República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI0609993-9 A2**

BRPI0609993A2

(22) Data de Depósito: 20/04/2006
(43) Data da Publicação: 18/10/2011
(RPI 2128)

(51) Int.Cl.:
H04L 29/06
H04L 12/22

(54) Título: MÉTODO PARA PROVER INCAPACIDADE DE LIGAÇÃO À UM NÓ MÓVEL EM UMA SESSÃO COM UM NÓ CORRESPONDENTE, NÓ MÓVEL, E, NÓ CORRESPONDENTE

(30) Prioridade Unionista: 04/04/2006 US 11/396706, 22/04/2005 US 60/673786, 31/05/2005 US 60/685396

(73) Titular(es): TELEFONAKTIEBOLAGET LM ERICSSON (publ)

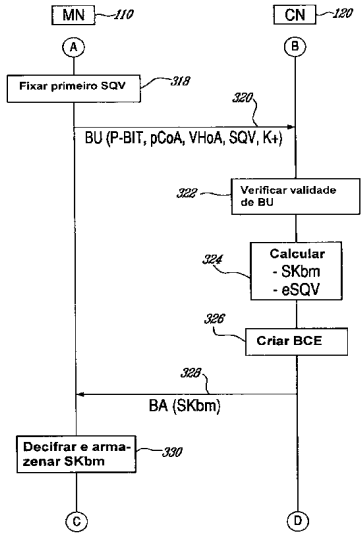
(72) Inventor(es): SURESH KRISHNAN, Wassim Haddad

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT IB2006051233 de 20/04/2006

(87) Publicação Internacional: WO 2006/111938de 26/10/2006

(57) Resumo: MÉTODO PARA PROVER INCAPACIDADE DE LIGAÇÃO A UM NÓ MÓVEL EM UMA SESSÃO COM UM NÓ CORRESPONDENTE, NÓ MÓVEL, E, NÓ CORRESPONDENTE. Um método, um nó correspondente e um nó móvel provêem anonimato e incapacidade de ligação a um nó móvel em uma sessão com um nó correspondente. Valores de seqüência, calculados baseados em dados secretos, são adicionados a atualizações enviadas do nó móvel para o nó correspondente e são usados pelo nó correspondente para autenticar atualizações do nó móvel. Um endereço doméstico do nó móvel não é exposto explicitamente. Um endereço de cuidado esperado é calculado no nó correspondente e usado pelo nó correspondente para enviar pacotes de dados ao nó móvel.



"MÉTODO PARA PROVER INCAPACIDADE DE LIGAÇÃO A UM NÓ MÓVEL EM UMA SESSÃO COM UM NÓ CORRESPONDENTE, NÓ MÓVEL, E, NÓ CORRESPONDENTE"

Fundamento da Invenção

Campo da Invenção

A presente invenção relaciona-se a um método, um nó móvel e um nó correspondente, para suportar anonimato do nó móvel enquanto em uma sessão com o nó correspondente.

Descrição da Arte Relacionada

IP móvel versão 4 (IPv4 Móvel, IP Móvel, MIPv4 ou MIP) e a versão atual de IPv6 Móvel (MIPv6) são construídas para prover mobilidade a hospedeiro ou Nó Móvel (MN). Os outros nós, normalmente chamados Nós Correspondentes (CNs), são normalmente vistos como hospedeiros fixos. Referência é feita agora à Figura 1, que mostra uma arquitetura de rede de MIPv6 como sugerida pela especificação de MIPv6 atual achada em um Pedido Para Comentário (RFC) número 3775 da Força-Tarefa de Engenharia da Internet (IETF). Como pode ser visto na Figura 1, uma rede de IP 100 inclui um MN 110 em comunicação com um CN 120 em uma ligação que provê um caminho direto 122. O caminho direto 122 será não provavelmente composto de só uma conexão física direta, mas em lugar disso representa uma série de ligações entre equipamentos de roteamento habilitando transparentemente a comunicação entre eles. O modo que a série de ligações é usada para transportar tráfego entre o MN 110 e o CN 120 é irrelevante contanto que comunicação de IP entre eles possa ser estabelecida.

O MN 110 tem um endereço doméstico de 128 bits nomeado permanentemente válido em sua rede doméstica 127, qual endereço doméstico é alocado na iniciação do MN 110 na rede doméstica 127. O endereço doméstico inclui um prefixo de sub-rede, que é de 64 bits de comprimento, e um identificador de interface, que também é de 64 bits de comprimento. O

mecanismo de alocação é bem conhecido na arte anterior. O MN 110 está ademais em comunicação com um Agente Doméstico (HA) 130 localizado em sua rede doméstica 127. Entre outras funcionalidades, o HA 130 mantém registro de um endereço estrangeiro do MN 110 válido fora da rede doméstica 127. O endereço estrangeiro é chamado Cuidado de Endereço (CoA) no contexto de MIPv6, e também inclui 128 bits. O CoA nomeado ao MN 110 muda em tempo quando o MN 110 se move de uma rede para outra. O registro mantido pelo HA 130, chamado ligação no contexto de MIPv6, liga o CoA ao endereço doméstico. Uma Entrada de 'Cache' de Ligação (BCE) incluindo o endereço doméstico e o CoA do nó móvel também é mantido no CN 120 para o propósito de alcançar o MN 110. O HA 130 também é responsável por rotear tráfego recebido no endereço doméstico ao MN 110. O tráfego recebido é remetido pelo HA 120 em uma ligação 125 para o MN 110. Todo o tráfego enviado na ligação 125, de acordo com MIPv6, é codificado para assegurar, entre outras coisas, confidência de credenciais trocadas periodicamente entre o MN 110 e o HA 130.

As linhas seguintes resumem como o conceito de MIPv6 se aplica em uma situação típica. Por exemplo, o MN 110 está em sessão de IP bidirecional, com o CN 120 no caminho direto 122. Quando o MN 110 se move de uma primeira rede doméstica a uma rede visitada, como ilustrado por uma seta 135 na Figura 1, o MN 110 adquire um primeiro CoA. Esta modificação em estado de endereçamento do MN 110 deve ser anunciada ao CN 120. A fim de anunciar a aquisição de seu primeiro CoA, o MN 110 envia uma primeira BU, incluindo o HoA, o primeiro CoA e um número de seqüência de 64 bits (SQN), para o CN 120 no caminho direto 122. O CN 120, na recepção da primeira BU, cria um BCE para a sessão, onde armazena o HoA, o primeiro CoA e o SQN. O CN 120 então envia um primeiro BA ao MN 110. Recepção do primeiro BA no MN 110 indica uma conclusão bem sucedida do anúncio da modificação do estado de endereçamento.

Quando o MN 110, enquanto a sessão ainda está em andamento, se move para uma segunda rede visitada, ele adquire um segundo CoA e envia ao CN 120 uma segunda BU levando o segundo CoA. A segunda BU também inclui o HoA e um novo SQN, cujo valor é aumentado monotonicamente sobre o SQN anterior. O CN 120 reconhece o BCE para a sessão por uso do HoA. O CN 120 atualiza o BCE sobrescrevendo o primeiro CoA com o segundo CoA e sobrescrevendo o SQN com o SQN recentemente recebido. O CN 120 rejeita a segunda BU se ela incluir um SQN que não é aumentado monotonicamente sobre o valor de seqüência armazenado previamente no BCE. O SQN é significado prover uma proteção contra um nó malicioso que poderia querer tomar a sessão enviando uma BU com o HoA do MN 110 e um CoA diferente para o nó malicioso. O nó malicioso poderia não enviar o próprio SQN e por esse meio ser detectado. Porém, a proteção oferecida pelo SQN é marginal no máximo: um nó malicioso pode enviar qualquer número de falsas BUs com vários valores de SQN até que uma BU seja aceita e respondida com um BA.

Outro problema com o método acima mencionado de informar o CN 120 de movimentos do MN 110 é que o HoA e os vários valores de CoA nomeados ao MN 110 são expostos no caminho direto 122 levando as várias mensagens de BU. Um nó malicioso localizado neste caminho poderia identificar o MN 110 e rastrear em tempo real seus movimentos pela Internet. Este tipo de atividade constituiria uma séria violação da privacidade do MN 110.

Haveria vantagens claras de ter um método, um nó móvel e um nó correspondente para prover uma capacidade para o nó correspondente para evitar expor uma identidade do nó móvel a qualquer terceiro e evitar um ataque de um nó fingindo ser o nó móvel legítimo.

Sumário da Invenção

É portanto um objetivo amplo desta invenção prover um

método, um nó móvel e um nó correspondente para prover anonimato e incapacidade de ligação ao nó móvel enquanto em uma sessão com o nó correspondente. Mensagens de atualização enviadas do nó móvel ao nó correspondente incluem um valor de seqüência, só conhecido pelo nó móvel e pelo nó correspondente, que não pode ser predito por um terceiro malicioso.

Um primeiro aspecto da presente invenção é dirigido a um método para prover incapacidade de ligação a um nó móvel que envia mensagens de atualização a um nó correspondente enquanto o nó correspondente e o nó móvel estão em uma sessão. Uma primeira atualização inclui um valor de seqüência fixado pelo nó móvel. O nó correspondente calcula um valor de seqüência esperado, usando um algoritmo baseado pelo menos em parte no valor de seqüência recebido, e o armazena em uma entrada de tabela para a sessão. Ao enviar uma segunda atualização, o nó móvel calcula um novo valor de seqüência, usando o mesmo algoritmo e o mesmo valor de seqüência precedente como usado pelo nó correspondente na recepção da primeira atualização. O nó correspondente recebe a segunda atualização incluindo o novo valor de seqüência e o usa para localizar a entrada de tabela. O nó correspondente aceita a segunda atualização se o novo valor de seqüência recebido casar com um valor de seqüência esperado em uma entrada de tabela. O achado da entrada de tabela incluindo o valor de seqüência esperado que casa com o novo valor de seqüência recebido autentica a segunda atualização. Outros dados na segunda atualização, por exemplo incluindo novos dados de endereço, são usados para atualizar o conteúdo da entrada de tabela.

Um segundo aspecto da presente invenção é dirigido a um método para esconder um endereço doméstico do nó móvel em mensagens de atualização.

Um terceiro aspecto da presente invenção é dirigido a um método para ademais prover anonimato do nó móvel em uma sessão mudando

um valor de um endereço enviado ao nó correspondente a toda atualização.

Um quarto aspecto da presente invenção é dirigido a um nó móvel para preservar anonimato e incapacidade de ligação de terceiros maliciosos potenciais.

Um quinto aspecto da presente invenção é dirigido a um nó correspondente para prover a um de nó móvel anonimato e incapacidade de ligação de terceiros maliciosos potenciais.

Breve Descrição dos Desenhos

Para um entendimento mais detalhado da invenção, para objetivos adicionais e vantagens disso, referência pode ser feita agora à descrição seguinte, tomada junto com os desenhos acompanhantes, em que:

Figura 1 é uma representação da arte anterior de uma arquitetura de Protocolo de Internet Móvel versão 6;

Figura 2 mostra uma representação de um método para estabelecer uma sessão com uma chave de autenticação secreta entre um nó móvel e um nó correspondente;

Figuras 3a, 3b, 3c e 3d mostram um diagrama de seqüência de um método exemplar para prover anonimato a um nó móvel em uma sessão com um nó correspondente;

Figura 4 mostra um nó móvel exemplar construído de acordo com a presente invenção; e

Figura 5 mostra um nó correspondente exemplar construído de acordo com a presente invenção.

Descrição Detalhada

Os ensinamentos inovadores da presente invenção serão descritos com referência particular a vários usos exemplares e aspectos da concretização preferida. Porém, deveria ser entendido que esta concretização provê só alguns exemplos dos muitos usos vantajosos dos ensinamentos inovadores da invenção. Em geral, declarações feitas na especificação do

presente pedido não limitam necessariamente nenhum dos vários aspectos reivindicados da presente invenção. Além disso, algumas declarações podem se aplicar a algumas características inventivas, mas não a outras. Na descrição das figuras, mesmos numerais representam mesmos elementos da invenção.

A presente invenção provê um método, um nó móvel (MN) e um nó correspondente (CN) para prover anonimato e incapacidade de ligação ao MN enquanto em uma sessão com o CN. Se ou não o MN está localizado em uma rede doméstica quando a sessão é estabelecida primeiro, o MN envia uma atualização ao CN para pedir a criação de uma entrada de tabela para a sessão. Se o MN estiver localizado em uma rede estrangeira, ele adquire um cuidado de endereço (CoA) da rede estrangeira e o envia na atualização. O CN armazena o CoA em sua entrada de tabela. Se, porém, o MN estiver localizado em sua rede doméstica, ele envia seu endereço doméstico (HoA) como um 'pseudo-CoA', como se este endereço fosse um CoA. Declarado de outro modo, o MN da presente invenção atua no CN como se ele sempre estivesse localizado em uma rede estrangeira, a fim de sempre estabelecer a entrada de tabela no CN.

O MN da presente invenção não expõe seu HoA quando o MN está em uma rede estrangeira. Também finge que seu HoA é um CoA quando está localizado em sua rede doméstica. O valor do pseudo-CoA resultante muda com toda a atualização. Portanto, o CN não é capaz de confiar em um valor de HoA estável do MN para identificar a entrada de tabela para a sessão. Um novo ponteiro para identificar a entrada de tabela é requerido agora. O MN e o CN da presente invenção usam um novo valor de seqüência (SQV) para substituir o número de seqüência (SQN). O SQV não é aumentado monotonicamente de uma atualização à próxima. O SQV, que tem um mesmo comprimento de 64 bits como o SQN, é em lugar disso recalculado com toda atualização nova por uso de informação secreta só conhecida pelo MN e pelo CN. Isto previne um terceiro malicioso, de seguir um rastro das várias

atualizações por ter tentado seguir um valor de SQN crescente monotonicamente. Em um aspecto da presente invenção, o SQV é enviado pelo MN em cada nova atualização. O CN usa o SQV recebido para localizar a entrada de tabela para a sessão em andamento com o MN. Realmente, o SQV é agora usado no CN como o novo ponteiro para identificar a entrada de tabela para a sessão.

O MN e o CN da presente invenção também usam informação secreta só conhecida por eles mesmos para modificar valores de endereço do MN. Isto ademais provê privacidade e anonimato ao MN.

No contexto da presente invenção, o MN pode incluir um telefone celular móvel, um assistente pessoal, um laptop e similar, em que o MN inclui pelo menos uma interface de acesso e preferivelmente suporta MIPv6.

O CN pode ser um servidor, por exemplo um servidor da web ou um servidor de Protocolo de Iniciação de Sessão (SIP), ou qualquer computador. O CN também poderia ser outro MN, que pode ser opcionalmente outro MN. O CN preferivelmente suporta MIPv6.

A fim de prover uma base para uma descrição da concretização preferida da presente invenção, referência é feita agora à Figura 2, que mostra uma representação de um método para estabelecer uma sessão com uma chave de autenticação secreta entre o MN e o CN. O MN 110 está associado com uma rede doméstica, que é uma porção doméstica da rede de IPv6 100 (também chamada rede doméstica 127). O MN 110 tem um primeiro endereço de IPv6 ou HoA válido na porção doméstica da rede de IPv6 100. O HoA também serve para associar o MN 110 a um Agente Doméstico (HA) 130 localizado na rede doméstica. O HA é um nó na rede doméstica, em que o MN tem uma assinatura. Quando a assinatura para o MN 110 é estabelecida na rede doméstica, o HA 130 define o HoA e o aloca ao MN 110. Todo o tráfego endereçado ao HoA é roteado primeiro ao HA 130,

que o remete ao MN 110.

O MN 110 também tem um par de chaves assimétricas incluindo uma chave privada (K-) e uma chave pública (K+). O funcionamento detalhado de criptografia de chave dupla é bem conhecido na arte anterior. É considerado que propriedade da K+ pelo MN 110 é provável. A prova de propriedade pode ser feita, por exemplo, usando uma Autoridade de Certificado, que é um terceiro confiável assegurando propriedade da K+. Outra solução, que não requer o uso de um terceiro é usar a K+ já usada para outros mecanismos criptográficos. Um exemplo de um tal mecanismo é o mecanismo de endereço gerado criptograficamente (CGA), que também habilita prova de propriedade de um endereço de IPv6 gerado com ele.

Quando o MN 110 se move em uma porção visitada da rede de IPv6 100 (etapa 220), um segundo endereço de IPv6 ou Cuidado de Endereço (CoA), válido na porção visitada, é provido ao MN 110 por um nó de serviço da porção visitada (etapa 222). O CoA é fixado além do HoA. O CoA é usado para alcançar o MN 110 diretamente. O modo no qual o CoA é fixado ao MN 110 é bem conhecido na arte.

O MN 110 precisa informar o CN 120 de seu CoA recentemente adquirido. Isto é alcançado enviando uma mensagem de estabelecimento 224 do MN 110 endereçada ao CN 120 pelo HA 130 (isto é, roteada do HA 130 para o CN 120). A mensagem de estabelecimento 224 também pode ser chamada uma Atualização de Pré-ligação ou PBU. A mensagem de estabelecimento 224 anuncia o CoA. A mensagem de estabelecimento inclui o HoA e o CoA do MN e, pode ademais incluir a K+ do MN.

Na recepção da mensagem de estabelecimento 224, o CN 120 testa a capacidade de alcance do CoA e a capacidade de alcance do HoA do MN 110. Isto é alcançado enviando do CN 120 um primeiro teste de endereço 228 para o MN 110 endereçado ao HoA. Um segundo teste de endereço 230

endereçado ao CoA é enviado do CN 120.

Na recepção do primeiro teste de endereço 228 e do segundo teste de endereço 230, o MN 110 envia uma única atualização 232. A atualização 232 é assinada pelo MN 110 usando a K-. A atualização 232 também pode ser chamada uma Atualização de Ligação (BU). O HoA, o CoA e um SQN são incluídos na atualização 232. Como a atualização 232 é a primeira atualização enviada para esta sessão, o SQN pode ser fixado a qualquer valor pelo MN 110.

Recepção da atualização 232 no CN 120 completa o teste do CoA e HoA. Ao receber a atualização 232, o CN 120 cria um BCE, onde armazena o HoA, o CoA e o SQN.

O CN 120 ademais envia um reconhecimento 234 ao MN 110 endereçado ao CoA. O reconhecimento 234 inclui uma chave de autenticação secreta (SKbm) codificada no reconhecimento 234 usando a K+ do MN 110. A SKbm é provavelmente para ser gerada pelo CN 120. O reconhecimento 234 também pode ser chamado um Reconhecimento de Ligação (BA). Na recepção do reconhecimento 234, o MN 110 decifra a SKbm usando a K-. Depois disso, ambos o CN 120 e o MN 110 têm a mesma SKbm para autenticar a comunicação entre eles na etapa 236.

A K+ do MN 110 pode ser anunciada tanto enviando a K+ na mensagem de estabelecimento 224, na atualização 232, ou em qualquer combinação de mensagens 224 e 232.

Tendo descrito agora anteriormente um método geral de estabelecer uma sessão entre o MN e o CN, um aspecto da concretização preferida da presente invenção será descrito agora por referência às Figuras 3a, 3b, 3c e 3d, que mostram um diagrama de seqüência de um método exemplar para prover anonimato a um nó móvel em uma sessão com um nó correspondente. É primeiro determinado na etapa 300, antes do estabelecimento de uma sessão, se o MN 110 está em uma rede doméstica ou

em uma rede estrangeira. Se o MN 110 estiver na rede doméstica, ele fixa um pseudo-cuidado de endereço (pCoA) igual a seu endereço doméstico (HoA) na etapa 302. Se o MN 110 estiver em uma rede estrangeira, ele deve adquirir primeiro um cuidado de endereço (CoA) na etapa 304 e então fixar seu pCoA igual ao CoA na etapa 306. O MN 110 então calcula um Endereço Doméstico Virtual (VHoA) na etapa 308. O método preferido para calcular o VHoA é usar um mecanismo de reedição bem conhecido, em que o VHoA é calculado como por equação (1):

$$VHoA = SHA (pCoA) \quad (1)$$

onde: 'SHA' é uma função de reedição.

Outros métodos de computar o VHoA também são possíveis. Isto inclui usar outros mecanismos de reedição, além do algoritmo de Padrão de Reedição Segura (SHA) bem conhecido. É preferível, por razões de privacidade que o HoA atual ou CoA nomeado ao MN 110 não possa ser detectado facilmente por análise do valor de VHoA obtido na etapa 308.

O MN 110 ademais fixa uma indicação de privacidade, ou bit P, na etapa 310. O MN 110 então envia ao CN 120 uma mensagem de estabelecimento, por exemplo uma mensagem de Atualização Pré-ligação (PBU) no contexto de uma implementação de MIPv6, na etapa 312. A mensagem de estabelecimento inclui o VHoA e o pCoA, e, preferivelmente, o bit P.

Enquanto a mensagem de estabelecimento como mostrada na Figura 2 incluía o HoA e o CoA do MN 110, esta mensagem de estabelecimento difere no tipo de endereços enviados nela. O VHoA que é enviado em vez do HoA não é um endereço roteável. O pCoA que é enviado em vez do CoA é um endereço roteável e pode ter de fato um valor igual ao HoA ou ao CoA.

O CN 120 recebe a mensagem de estabelecimento na etapa 312. Na etapa 314, o CN 120 sabe da presença do bit P que o VHoA não é um

endereço doméstico real e assim decide saltar qualquer teste de endereço doméstico. Sem o bit P, o CN 120 poderia tentar fazer um teste de endereço doméstico, detectar uma falha, determinar baseado na falha que o VHoA não é um endereço doméstico real, e simplesmente continuar com a próxima etapa. O bit P é portanto um aspecto opcional da presente invenção. Na etapa 316, o CN 120 envia um teste de cuidado de endereço, ou Teste de Pré-ligação (PBT) no contexto de uma implementação de MIPv6, para o MN 110.

Na etapa 318, o MN 110 fixa um primeiro valor de seqüência (SQV) para a sessão. O valor do SQV pode ser fixado a qualquer valor neste momento, mas é preferivelmente escolhido de forma que case com um formato de um campo padrão, tal como por exemplo o número de seqüência (SQN) de uma Atualização de Ligação (BU) em MIPv6. O MN 110 envia para o CN 120 na etapa 320 uma atualização, tal como uma mensagem de BU, incluindo o bit P, o pCoA, o VHoA, o SQV e, preferivelmente, uma chave pública (K+) do MN 110. Em um aspecto alternado da concretização preferida da invenção, o pCoA pode ser modificado sobrescrevendo seus 64 bits menos significantes, incluindo uma parte de identificador de interface, pelo SQV. Neste caso, o SQV é enviado vantajosamente só como uma parte do pCoA. Na etapa 322, o CN 120 preferivelmente verifica a autenticidade da mensagem de BU por uso da K+. O CN 120 calcula uma chave secreta compartilhada (SKbm) na etapa 324. O CN 120 também calcula um valor de seqüência esperado (eSQV), preferivelmente baseado na SKbm e no SQV recebido, como por equação (2):

$$eSQV = SHA((SQV) + Primeiro(128, SHA(SKbm))) \quad (2)$$

onde: 'SQV' é o SQV prévio, isto é, SQV recebido na última atualização;

'Primeiro (tamanho, entrada)' é uma função usada para indicar truncamento dos dados de entrada de forma que só os primeiros bits de tamanho permaneçam para serem usados.

Outros métodos de calcular o eSQV também cairiam dentro da

extensão da presente invenção, já que o valor de eSQV não pode ser predito facilmente do valor de SQV.

Na etapa 326, o CN 120 cria uma entrada de tabela para a sessão com o MN 110, a entrada de tabela sendo uma Entrada de 'Cache' de Ligação (BCE) no contexto de uma implementação de MIPv6. A entrada de tabela armazena o eSQV, o pCoA, o VHOA, a K+ e a SKbm. Na etapa 328, o CN 120 envia um reconhecimento para o MN 110, incluindo a SKbm. No contexto de uma implementação de MIPv6, o reconhecimento tomaria a forma de um Reconhecimento de Ligação (BA). O MN 110 decifra e armazena a SKbm na etapa 330. Depois disso, como mostrado na etapa 332, o CN 120 pode enviar pacotes de dados para o MN 110 usando o pCoA como um endereço de roteamento. Pacotes de dados são preferivelmente codificados por uso da SKbm.

Na etapa 334, o MN 110 muda de localização enquanto a sessão com o CN 120 ainda está em andamento. O MN 110 calcula um SQV novo na etapa 336, usando o mesmo método como usado pelo CN 120 na etapa 324, que preferivelmente usa a equação (2). O MN 110 então fixa um novo valor para o pCoA nas etapas 338, 340, 342 e 344, da mesma maneira como quando a sessão era inicialmente fixada. De uma mesma maneira como no caso da primeira atualização, o pCoA pode opcionalmente ser modificado sobrescrevendo seus 64 bits menos significantes com o novo SQV. Neste caso também, o SQV é enviado só como uma parte do pCoA. Porque o MN 110 mudava de local na etapa 334, o novo pCoA é necessariamente diferente do valor prévio nomeado ao pCoA. Um novo valor do VHoA é calculado na etapa 346, reusando o mesmo método como na etapa 308.

O MN 110 envia para o CN 120 na etapa 348 uma nova atualização, incluindo o mesmo bit P e os novos valores para o pCoA, VHoA e SQV. Preferivelmente, a K+ também é incluída.

Na etapa 350, o CN 120 tenta achar uma entrada de tabela em

que o valor de eSQV casa, ou é igual ao SQV recentemente recebido. Se nenhum for achado, a mensagem de atualização é ignorada e o processo termina na etapa 352. Um casamento achado é indicativo que o CN 120 autenticou corretamente a mensagem de atualização recentemente recebida porque um SQV com um valor igual só poderia ser calculado pelo MN 110 por uso de informação secreta. O CN 120 calcula novos valores a serem entrados na entrada de tabela na etapa 354. Um novo valor de eSQV é calculado da mesma maneira como na etapa 324, baseado no SQV recentemente recebido. Um cuidado de endereço esperado (eCoA) é calculado, também na etapa 354, como por equação (3):

eCoA (iid) = Primeiro (64, SHA ((SHA (SKbm) | Prefixo de Sub-rede de pCoA))) (3)

onde:

'iid' é a parte de identificador de interface do eCoA;

'pCoA' é o pseudo-cuidado de endereço do MN enviado na atualização; e

'Prefixo de Sub-rede de pCoA' se torna um prefixo de sub-rede do eCoA.

O valor de eCoA precisa permanecer um endereço de IP roteável. Equação (3) calcula a parte de identificador de interface do eCoA requerido. O valor de eCoA atual é obtido de pré-anexar o valor de eCoA(iid) ao prefixo de sub-rede de pCoA. Conseqüentemente, o eCoA inclui um prefixo de sub-rede roteável e só a parte de iid foi modificada.

Ainda na etapa 354, um endereço doméstico virtual esperado (eVHoA) é calculado como por equação (4):

eVHoA = SHA (eCoA) (4)

O eCoA e eVHoA poderiam ser computados com outros métodos, contanto que os valores obtidos confiram anonimato razoável ao MN 110 e contanto que o eCoA preserve o prefixo de sub-rede do pCoA. Na concretização preferida, o mecanismo para calcular o eVHoA, como

publicado na equação (4), é idêntico ao mecanismo para calcular o VHoA, como na equação (1).

O CN 120 atualiza a entrada de tabela na etapa 356 sobrescrevendo o eSQV prévio com o novo valor para o eSQV, sobrescrevendo o pCoA prévio com o eCoA, e sobrescrevendo o VHoA prévio com o eVHoA.

Na etapa 358, o CN 120 envia um novo reconhecimento para o MN 110. Responsivo a recibo do novo reconhecimento, o MN 110 calcula na etapa 360 uma cópia do eCoA e uma cópia do eVHoA, usando algoritmos idênticos como aqueles usados pelo CN 120.

Depois disso, como mostrado na etapa 362, o CN 120 pode enviar pacotes de dados para o MN 110 usando o eCoA como um endereço de roteamento.

Da descrição anterior das Figuras 3a-3d, pode ser visto que a identidade real do MN 110 é, tanto quanto possível, não exposta ao CN ou a qualquer invasor malicioso. Se o MN 110 primeiro estabeleceu a sessão de sua rede doméstica, seu endereço doméstico só foi exposto na primeira atualização, onde estava fingindo ser um cuidado de endereço. Atualizações subseqüentes, indicativas dos movimentos e atividades de um nó móvel, não seriam ligáveis ou correlatáveis por invasor malicioso porque a presente invenção usa valores de seqüência que não são incrementados monotonicamente.

Igualmente, assalto da sessão enviando uma atualização de um terceiro fica praticamente impossível porque o terceiro não pode predizer o próximo valor de seqüência que será aceito pelo CN 120.

Uma construção exemplar de um MN 110 como usado nas figuras precedentes, será descrita agora por referência à Figura 4, que mostra um MN 110 exemplar construído de acordo com a presente invenção. O MN 110 pode ser implementado em hardware, software, ou qualquer combinação disso. O MN 110 inclui uma interface de acesso 410, uma memória 420, um

processador 430, uma lógica de comunicação 440, um operador de pacote 450 e aplicativos 460.

A interface de acesso 410 é usada para se comunicar com CNs por uma conexão à rede doméstica e, quando longe de uma rede doméstica, por uma conexão a redes estrangeiras. Em um MN 110 exemplar, a interface de acesso 410 poderia ser uma interface de CDMA2000, uma interface de WLAN, uma interface de Acesso Múltiplo por Divisão de Código de Banda Larga, uma interface de Serviço de Dados de Pacote Geral, uma interface de WiMAX, uma interface de EV-DO, e similares.

A memória 420 armazena um endereço doméstico permanente (HoA), um cuidado de endereço (CoA), um pseudo-cuidado de endereço (pCoA), um endereço doméstico virtual (VHoA), um cuidado de endereço esperado (eCoA), que é de fato uma cópia de um eCoA calculado no CN 120, um endereço doméstico virtual (eVHoA), que é de fato uma cópia de um eVHoA calculado no CN 120, uma chave secreta compartilhada decifrada (SKbm), uma chave pública (K+) e uma chave privada (K-) e um valor de seqüência (SQV).

O processador 430 fixa um bit de privacidade (bit P) e preferivelmente inclui três mecanismos de reedição distintos para implementar os algoritmos das equações (1), (2) e (3) usadas em calcular o VHoA, o SQV e cópias do eCoA e eVHoA.

A lógica de comunicação 440 adquire o CoA quando o MN 110 está em uma rede estrangeira. A lógica de comunicação também controla o envio da mensagem de estabelecimento, o PBT, a atualização e a BU pela interface de acesso 410, como também recebe da interface de acesso 410 o teste de endereço, o PBT, o reconhecimento e o BA.

O operador de pacote 450 envia carga útil para o CN 120 pela interface de acesso 410 e recebe carga útil adicional do CN 120, também pela interface de acesso 410. O operador de pacote 450 provê a carga útil recebida

aos aplicativos 460 e recebe de aplicativos 460 carga útil a ser enviada para o CN 120. Os aplicativos 460 incluem quaisquer aplicativos achados comumente em um nó móvel e são bem conhecidos na arte.

Quando o MN 110 estabelece uma sessão com CN 120, a lógica de comunicação 440 determina primeiro se interface de acesso 410 está conectada por uma rede doméstica ou uma rede estrangeira. Se o MN 110 estiver em uma rede estrangeira, a lógica de comunicação adquire um CoA e o armazena em memória 420. Em qualquer caso, a lógica de comunicação estabelece um pCoA, tanto igual ao CoA, se presente, ou ao HoA, e o armazena na memória 420. Processador 430 então calcula o VHoA, preferivelmente usando a equação (1), e o armazena em memória 420. Processador 430 também fixa o bit P. Lógica de comunicação 440 envia uma mensagem de estabelecimento para o CN 120, por interface de acesso 410. A mensagem de estabelecimento inclui o bit P, o pCoA e o VHoA.

Quando uma mensagem de teste de endereço chega do CN 120 pela interface de acesso 410, a lógica de comunicação 440 decodifica a mensagem. Pede ao processador 430 para prover um SQV. Como nenhum valor de SQV prévio está nesse momento armazenado em memória 420, o processador 430 fixa o SQV a qualquer valor que obedece um formato de um campo de SQV em uma atualização. Lógica de comunicação 440 lê a K+ de memória 420 e pede a interface de acesso 410 para enviar uma atualização, incluindo o bit P, o pCoA, o VHoA, o SQV e a K+, para CN 120.

Quando um reconhecimento chega do CN 120 pela interface de acesso 410, a lógica de comunicação 440 decodifica a mensagem. Processador 430 decifra a SKbm usando a K- lida de memória 420, e armazena o resultado em memória 420.

A sessão sendo estabelecida agora completamente entre o MN 110 e o CN 120, dados de pacote são trocados entre os dois nós. O MN 110 recebe e envia dados de pacote pela interface de acesso 410. Operador de

pacote 450 processa os pacotes recebidos e provê os dados recebidos a aplicativos 460. Processamento no operador de pacote 450 pode ademais incluir codificar pacotes de partida e pacotes de chegada decifrando usando a SKbm lida de memória 420. Aplicativos 460 também provêem dados para operador de pacote 450 para enviar para o CN 120 pela interface de acesso 410.

No evento que a interface de acesso 410 relata uma mudança de conexão para uma rede de serviço, indicativa de uma mudança de localização para MN 110, a lógica de comunicação 440 avalia novamente se a interface de acesso 410 está agora conectada pela rede doméstica ou uma nova rede estrangeira. Se o MN 110 estiver na nova rede estrangeira, a lógica de comunicação adquire um novo CoA e o armazena em memória 420. Em qualquer caso, a lógica de comunicação estabelece um novo pCoA, tanto igual ao novo CoA, se presente, ou ao HoA, e o armazena na memória 420. Lógica de comunicação 440 pede ao processador 430 para prover um SQV. Processador 430 lê o valor de SQV de memória 420 e o usa como uma base para computar um novo SQV, preferivelmente usando equação (2). Lógica de comunicação 440 arranja para enviar uma nova atualização para CN 120, incluindo notavelmente o novo SQV e o novo pCoA. Quando a lógica de comunicação 440 detecta que um reconhecimento foi recebido, seguindo a segunda atualização, pede para o processador 430 computar uma cópia de eCoA, preferivelmente usando a equação (3), e uma cópia de eVHoA, preferivelmente usando a equação (4). Processador 430 então armazena as cópias de eCoA e de eVHoA em memória 420.

Uma construção exemplar de um CN 130 como usado nas Figuras precedentes, será descrita agora por referência à Figura 5, que mostra CN 120 exemplar construído de acordo com a presente invenção. O CN 120 pode ser implementado em hardware, software, ou qualquer combinação disso, como é bem conhecido na arte. O CN 120 pode ser um nó móvel.

O CN 120 inclui uma porta de entrada 510, uma porta de saída 520, uma tabela 530, entradas 540 em tabela 530, um processador 550, uma lógica de comunicação 560, um operador de pacote 570 e aplicativos 580.

Porta de entrada 510 recebe mensagens tal como a mensagem de estabelecimento, a atualização, a PBU ou a BU. Porta de saída 520 envia mensagens tal como o teste de endereço, o reconhecimento, o PBT ou o BA. Dependendo da tecnologia de acesso usada pelo CN 120, a porta de entrada 510 e a porta de saída 520 podem formar uma única entidade.

Tabela 530 inclui uma entrada 540, que pode ser por exemplo um BCE, para cada sessão com um MN 110. Cada entrada de tabela inclui um valor de seqüência esperado (eSQV), que também é usado como um ponteiro 542 para identificar uma entrada dentro da tabela inteira 530. Cada entrada de tabela ademais inclui um pseudo-cuidado de endereço (pCoA), que também pode levar um valor de um cuidado de endereço esperado (eCoA), um endereço doméstico virtual (VHoA), que também pode levar um valor de um endereço doméstico virtual esperado (eVHoA), uma chave pública (K+) e uma chave secreta compartilhada (SKbm) para o MN 110.

Processador 550 calcula a SKbm e executa a autenticação de mensagens. Processador 550 preferivelmente também inclui três mecanismos de reedição distintos para implementar os algoritmos das equações (2), (3) e (4) usadas em calcular o eSQV, o eCoA e o eVHoA.

A lógica de comunicação 560 controla recepção da mensagem de estabelecimento, o PBT, a atualização e o BU pela porta de entrada 510, como também envia pela porta de saída 520 o teste de endereço, o PBT, o reconhecimento e o BA. Para localizar uma das entradas 540 para operar dados recebidos em uma mensagem, a lógica de comunicação 560 varre pela tabela 530 e procura por uma entrada 540 incluindo o eSQV que casa, ou é igual a um SQV recebido como uma parte da mensagem.

O operador de pacote 570 envia carga útil para o MN 110 pela

porta de saída 520 e recebe carga útil adicional do MN 110 pela porta de entrada 510. O operador de pacote 570 provê a carga útil recebida aos aplicativos 580 e recebe de aplicativos 580 carga útil a ser enviada para o MN 110. Os aplicativos 580 incluem quaisquer aplicativos achados comumente em um nó correspondente e são bem conhecidos na arte.

Quando uma mensagem de estabelecimento é recebida por porta de entrada 510, a lógica de comunicação 560 detecta a presença de um bit P. Por causa da presença deste indicador, a lógica de comunicação 560 elege para não testar um campo de endereço doméstico da mensagem de estabelecimento, que inclui o VHoA. Lógica de comunicação 560 instrui a porta de saída 520 para enviar um teste de endereço, tal como um PBT, para o MN 110, a um endereço indicado por um campo de pCoA da mensagem de estabelecimento.

Quando uma atualização é recebida por porta de entrada 510, a lógica de comunicação 560 uma vez mais detecta a presença do bit P. Este bit P indica que uma sessão está sendo estabelecida pedindo anonimato. Indica ademais que um campo de endereço doméstico da mensagem de atualização contém um VHoA não roteável. Também indica que um campo de número de seqüência foi substituído com um SQV que precisa ser usado como um ponteiro 542 para identificar uma entrada de tabela para a sessão. Lógica de comunicação 560 instrui o processador 550 para autenticar a atualização, usando uma K+ recebida na atualização. Lógica de comunicação 560 ademais instrui o processador 550 para calcular uma SKbm. Lógica de comunicação 560 então instrui o processador 550 para calcular um eSQV, baseado no valor de SQV recebido na atualização, preferivelmente usando a equação (2). Lógica de comunicação então cria uma entrada 540 na tabela 530, a entrada 540 incluindo o eSQV, o SKbm, a K+ e ademais incluindo um valor de pCoA e um valor de VHoA recebido como uma parte da atualização. Lógica de comunicação 560 então instrui a porta de saída 520 para enviar um

reconhecimento, tal como BA, para o MN 110, a um endereço indicado agora pelo pCoA armazenado na entrada de tabela 540. O reconhecimento ademais inclui a SKbm.

A sessão agora sendo estabelecida completamente entre o MN 110 e o CN 120, dados de pacote são trocados entre os dois nós. O CN120 recebe dados de pacote por porta de entrada 510 e envia dados de pacote por porta de saída 520. Pacotes são enviados para o MN 110 por uso do valor de pCoA armazenado na entrada de tabela 540. Operador de pacote 570 processa os pacotes recebidos e provê os dados recebidos para aplicativos 580. Processamento no operador de pacote 570 pode ademais incluir codificar pacotes de partida e decifrando pacotes de chegada usando a SKbm lida de entrada de tabela 540. Aplicativos 580 também provêem dados para operador de pacote 570 para enviar para o MN 110 pela porta de saída 520.

Uma atualização adicional pode ser recebida por porta de entrada 510, como resultado de uma mudança de localização no CN 110. Lógica de comunicação 560 uma vez mais detecta a presença do bit P. Lógica de comunicação 560 lê um novo valor de SQV da atualização e varre por tabela 530 para achar uma entrada 540 cujo ponteiro 542 é igual ao SQV recentemente recebido. Se nenhum for achado, isto pode ser indicativo de uma nova sessão sendo estabelecida por outro nó móvel. Se, porém, esta atualização adicional for um resultado de uma tentativa por um nó malicioso para seqüestrar a sessão, essa atualização adicional não pode autenticar e a mensagem é ignorada.

Quando a entrada de tabela 540 é achada, cujo ponteiro 542, consistindo no eSQV previamente armazenado, casa com o SQV recentemente recebido, a lógica de comunicação instrui o processador 550 para calcular um novo valor de eSQV, baseado no valor de eSQV prévio. O novo eSQV é armazenado em entrada de tabela 540. Então, a lógica de comunicação 560 pede ao processador 550 para calcular um eCoA e um

eVHoA, preferivelmente usando as equações (3) e (4). Lógica de comunicação 560 sobrescreve, na entrada de tabela 540, o pCoA anterior com o novo eCoA e o VHoA anterior com o novo eVHoA. Lógica de comunicação 560 então instrui a porta de saída 520 para enviar um reconhecimento para o MN 110, a um endereço indicado pelo eCoA agora armazenado na entrada de tabela 540.

A sessão entre o MN 110 e o CN 120 continua, dados de pacote agora sendo enviados para o MN 110 por uso do valor de eCoA armazenado na entrada de tabela 540.

Embora vários aspectos da concretização preferida do método, do nó móvel e do nó correspondente da presente invenção tenham sido ilustrados nos Desenhos Acompanhantes e descritos na Descrição Detalhada precedente, será entendido que a invenção não está limitada à concretização exposta, mas é capaz de numerosos rearranjos, modificações e substituições sem partir do espírito da invenção como será publicado e definido pelas reivindicações seguintes.

REIVINDICAÇÕES

1. Método para prover incapacidade de ligação a um nó móvel em uma sessão com um nó correspondente, caracterizado pelo fato de compreender as etapas de:

enviar uma primeira atualização de dito nó móvel para dito nó correspondente, dita primeira atualização incluindo um primeiro valor de seqüência;

calcular em dito nó correspondente um valor de seqüência esperado baseado pelo menos em parte em dito primeiro valor de seqüência, usando um primeiro mecanismo de reedição;

criar em dito nó correspondente uma entrada de tabela para dita sessão, dita entrada de tabela para armazenar dito valor de seqüência esperado;

calcular em dito nó móvel um segundo valor de seqüência baseado pelo menos em parte em dito primeiro valor de seqüência, usando dito primeiro mecanismo de reedição;

enviar de dito nó móvel para dito nó correspondente uma segunda atualização incluindo dito segundo valor de seqüência; e

identificar em dito nó correspondente dita entrada de tabela olhando por dita tabela por um casamento entre dito valor de seqüência esperado e dito segundo valor de seqüência.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender ainda as etapas de:

responsivo à dita primeira atualização, calcular em dito nó correspondente uma chave secreta compartilhada para dito nó móvel;

armazenar dita chave secreta compartilhada em dita entrada de tabela;

enviar uma confirmação de dito nó correspondente para dito nó móvel, dita confirmação incluindo dita chave secreta compartilhada; e

armazenar dita chave secreta compartilhada em dito nó móvel antes de enviar dita segunda atualização.

3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que:

dita primeira atualização adicionalmente inclui um primeiro pseudo-endereço de cuidado igual a um endereço doméstico se dito nó móvel estiver em uma rede doméstica para dito nó móvel ou igual a um endereço de cuidado se dito nó móvel estiver em uma rede estrangeira;

dita entrada de tabela adicionalmente armazena dito primeiro pseudo-endereço de cuidado;

dita segunda atualização adicionalmente inclui um segundo pseudo-endereço de cuidado igual a dito endereço doméstico se dito nó móvel estiver em dita rede doméstica para dito nó móvel ou igual a um novo endereço de cuidado se dito nó móvel estiver em uma nova rede estrangeira;

dita segunda atualização é enviada responsiva a uma mudança de uma localização de dito nó móvel; e

dito entrada de tabela sobrescreve dito pseudo-endereço de cuidado com dito segundo pseudo-endereço de cuidado.

4. Método de acordo com a reivindicação 3, caracterizado pelo fato de que:

dito primeiro valor de seqüência é incluído em dito primeiro pseudo-endereço de cuidado; e

dito segundo valor de seqüência é incluído em dito segundo pseudo-endereço de cuidado.

5. Método de acordo com a reivindicação 3, caracterizado pelo fato de que adicionalmente provém anonimato, em que:

dito nó móvel calcula um endereço doméstico virtual baseado pelo menos em parte em dito primeiro pseudo-endereço de cuidado;

dita primeira atualização adicionalmente inclui dito endereço

doméstico virtual e uma indicação de privacidade;

dita etapa de calcular em dito nó correspondente dito valor de seqüência esperado é responsivo à dita indicação de privacidade em dita primeira atualização;

dito nó correspondente armazena dito endereço doméstico virtual em dita entrada de tabela; e

dito nó correspondente usa dito primeiro pseudo-endereço de cuidado e dito endereço doméstico virtual para enviar pacotes para dito nó móvel até que dito nó correspondente receba dita segunda atualização.

6. Método de acordo com a reivindicação 5, caracterizado pelo fato de compreender ainda as etapas de:

responsivo à dita segunda atualização incluindo dita indicação de privacidade, calcular em dito nó correspondente um valor de seqüência esperado adicional baseado pelo menos em parte em dito segundo valor de seqüência;

calcular em dito nó correspondente um endereço de cuidado esperado, baseado pelo menos em parte em dito segundo pseudo-endereço de cuidado;

calcular em dito nó correspondente um endereço doméstico virtual esperado baseado pelo menos em parte em dito endereço de cuidado esperado;

atualizar dita entrada de tabela armazenando dito valor de seqüência esperado adicional, dito endereço de cuidado esperado e dito endereço doméstico virtual esperado;

enviar uma confirmação adicional de dito nó correspondente para dito nó móvel;

calcular em dito nó móvel uma cópia de dito endereço de cuidado esperado, baseado pelo menos em parte em dito segundo pseudo-endereço de cuidado;

calcular em dito nó móvel uma cópia de dito endereço doméstico virtual esperado baseado pelo menos em parte em dita cópia de dito endereço de cuidado esperado; e

usar em dito nó correspondente dito endereço de cuidado esperado e dito endereço doméstico virtual esperado para enviar pacotes para dito nó móvel até que dito nó correspondente receba dita segunda atualização.

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que:

dita etapa de calcular em dito nó correspondente dito valor de seqüência esperado adicionalmente inclui calcular baseado pelo menos em parte em dita chave secreta compartilhada;

dita etapa de calcular em dito nó móvel dito segundo valor de seqüência adicionalmente inclui calcular baseado pelo menos em parte em dita chave secreta compartilhada;

dita etapa de calcular em dito nó correspondente dito valor de seqüência esperado adicional adicionalmente inclui calcular baseado pelo menos em parte em dita chave secreta compartilhada e usar dito primeiro mecanismo de reedição;

dita etapa de calcular em dito nó correspondente dito endereço de cuidado esperado adicionalmente inclui calcular baseado pelo menos em parte em dita chave secreta compartilhada e usar um segundo mecanismo de reedição;

dita etapa de calcular em dito nó móvel dita cópia de dito endereço de cuidado esperado adicionalmente inclui calcular baseado pelo menos em parte em dita chave secreta compartilhada e usar dito segundo mecanismo de reedição;

dita etapa de calcular em dito nó móvel dito endereço doméstico virtual usa um terceiro mecanismo de reedição;

dita etapa de calcular em dito nó correspondente dito endereço

doméstico virtual esperado usa dito terceiro mecanismo de reedição; e

dita etapa de calcular em dito nó móvel dita cópia de dito endereço doméstico virtual esperado usa dito terceiro mecanismo de reedição.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que:

dito nó correspondente ignora dita segunda atualização se dito segundo valor de seqüência não casar com qualquer valor de seqüência esperado em qualquer entrada de tabela.

9. Método de acordo com a reivindicação 1, caracterizado pelo fato de que:

dita atualização adicionalmente inclui uma chave pública de dito nó móvel; e

dito nó correspondente autentica dita primeira atualização baseado em dita chave pública.

10. Nó móvel, caracterizado pelo fato de compreender:

uma memória para armazenar um primeiro valor de seqüência e um segundo valor de seqüência;

um processador para calcular dito primeiro valor de seqüência, para armazenar dito primeiro valor de seqüência em dita memória, para ler dito primeiro valor de seqüência de dita memória, para calcular dito segundo valor de seqüência por uso de um primeiro mecanismo de reedição, baseado pelo menos em parte em dito primeiro valor de seqüência, e para armazenar em dita memória dito segundo valor de seqüência;

uma interface de acesso para enviar para um nó correspondente uma primeira atualização incluindo dito primeiro valor de seqüência e uma segunda atualização incluindo dito segundo valor de seqüência; e

uma lógica de comunicação para controlar uma sessão com dito nó correspondente, dita lógica de comunicação pedindo dito processador

para calcular dito primeiro e dito segundo valores de seqüência e pedindo dita interface de acesso para enviar dita primeira e dita segunda atualizações.

11. Nó móvel de acordo com a reivindicação 10, caracterizado pelo fato de que:

dita interface de acesso é para receber uma confirmação de dito nó correspondente, dita confirmação incluindo uma chave secreta compartilhada;

dito processador é para descriptografar dita chave secreta compartilhada; e

dita memória é para armazenar dita chave secreta compartilhada descriptografada.

12. Nó móvel de acordo com a reivindicação 10, caracterizado pelo fato de que:

dito primeiro mecanismo de reedição adicionalmente calcula dito segundo valor de seqüência baseado pelo menos em parte em dita chave secreta compartilhada;

dito processador adicionalmente inclui um segundo mecanismo de reedição para calcular um endereço doméstico virtual baseado pelo menos em parte em um pseudo-endereço de cuidado;

dito processador adicionalmente inclui um terceiro mecanismo de reedição para calcular um endereço de cuidado esperado baseado pelo menos em parte em dito pseudo-endereço de cuidado e baseado pelo menos em parte em dita chave secreta compartilhada; e

dito segundo mecanismo de reedição é adicionalmente para calcular um endereço doméstico virtual esperado baseado pelo menos em parte em dito endereço de cuidado esperado.

13. Nó móvel de acordo com a reivindicação 10, caracterizado pelo fato de que:

dito lógica de comunicação é para controlar envio de dita

primeira atualização no estabelecimento de dita sessão;

dita lógica de comunicação é para detectar uma mudança de localização de dito nó móvel; e

dito lógica de comunicação é para controlar envio de dita segunda atualização responsivo à dita mudança de localização.

14. Nó móvel de acordo com a reivindicação 13, caracterizado pelo fato de que:

dita lógica de comunicação é para determinar se dita sessão é estabelecida por uma conexão de dita interface de acesso para uma rede doméstica ou para uma rede estrangeira;

dito lógica de comunicação é para adquirir um endereço de cuidado se dita sessão estiver sendo servida através de dita rede estrangeira;

dita lógica de comunicação é para estabelecer um pseudo-endereço de cuidado, dito pseudo-endereço de cuidado sendo igual a dito endereço de cuidado se dita sessão estiver sendo servida por dita rede estrangeira, dito pseudo-endereço de cuidado sendo igual a um endereço doméstico de dito nó móvel se dita sessão estiver sendo servida por dita rede doméstica; e

dita primeira atualização inclui dito pseudo-endereço de cuidado.

15. Nó móvel de acordo com a reivindicação 14, caracterizado pelo fato de que:

dita lógica de comunicação é para estabelecer um novo pseudo-endereço de cuidado responsivo à dita mudança de localização;

dito novo pseudo-endereço de cuidado é igual a um novo endereço de cuidado se dito nó móvel for servido agora por uma nova rede estrangeira responsiva à dita mudança de localização, dito pseudo-endereço de cuidado é igual a dito endereço doméstico de nó móvel dito se dita sessão for servida agora por dita rede doméstica responsivo à dita mudança de

localização; e

dita segunda atualização inclui dito novo pseudo-endereço de cuidado.

16. Nó correspondente, caracterizado pelo fato de compreender:

uma porta de entrada para receber uma primeira atualização incluindo um primeiro endereço e um primeiro valor de seqüência, dita primeira atualização sendo para uma sessão com um nó móvel, e para receber uma segunda atualização para dita sessão, dita segunda atualização incluindo um segundo endereço e um segundo valor de seqüência;

um processador para calcular um valor de seqüência esperado baseado pelo menos em parte em dito primeiro valor de seqüência, usando um primeiro mecanismo de reedição, e para calcular um novo valor de seqüência esperado baseado pelo menos em parte em dito segundo valor de seqüência;

uma tabela para armazenar uma entrada de tabela para dita sessão com dito nó móvel, em que dita entrada de tabela inclui dito primeiro endereço e um ponteiro para dita entrada de tabela, dito ponteiro sendo igual a dito valor de seqüência esperado, para sobrescrever em dita entrada de tabela dito ponteiro com dito novo valor de seqüência esperado, e para sobrescrever em dita entrada de tabela dito primeiro endereço com um endereço de cuidado esperado baseado pelo menos em parte em dito segundo endereço; e

uma lógica de comunicação para controlar dita sessão, dita lógica de comunicação para olhar por dita tabela por uma entrada incluindo um valor de dito ponteiro igual a dito primeiro valor de seqüência, para criar dita entrada de tabela se nenhum valor de dito ponteiro igual a dito primeiro valor de seqüência for achado em dita tabela, para pedir dito processador para calcular dito valor de seqüência esperado, para achar dita entrada de tabela incluindo dito ponteiro igual a dito segundo valor de seqüência, e para pedir dito processador para calcular dito novo valor de seqüência esperado.

17. Nó correspondente de acordo com a reivindicação 16, caracterizado pelo fato de que:

dito processador é para adicionalmente calcular uma chave secreta compartilhada para dita sessão com dito nó móvel;

dita entrada de tabela é para adicionalmente armazenar dita chave secreta compartilhada;

dito nó correspondente adicionalmente inclui uma porta de saída para enviar confirmações para dito nó móvel, responsivo à dita primeira e segunda atualizações, ditas confirmações incluindo dita chave secreta compartilhada.

18. Nó correspondente de acordo com a reivindicação 17, caracterizado pelo fato de que:

dito primeiro mecanismo de reedição calcula ditos valores de seqüência esperados baseado pelo menos em parte em dita chave secreta compartilhada;

dito processador adicionalmente inclui um segundo mecanismo de reedição para calcular dito endereço de cuidado esperado baseado pelo menos em parte em dita chave secreta compartilhada;

dito processador adicionalmente inclui um terceiro mecanismo de reedição para calcular um endereço doméstico virtual baseado pelo menos em parte em endereço de cuidado esperado; e

dita entrada de tabela é para adicionalmente armazenar dito endereço doméstico virtual.

19. Nó correspondente de acordo com a reivindicação 17, caracterizado pelo fato de compreender ainda:

um operador de pacote para enviar por dita porta de saída pacotes de dados para dito nó móvel usar dito endereço de cuidado esperado.

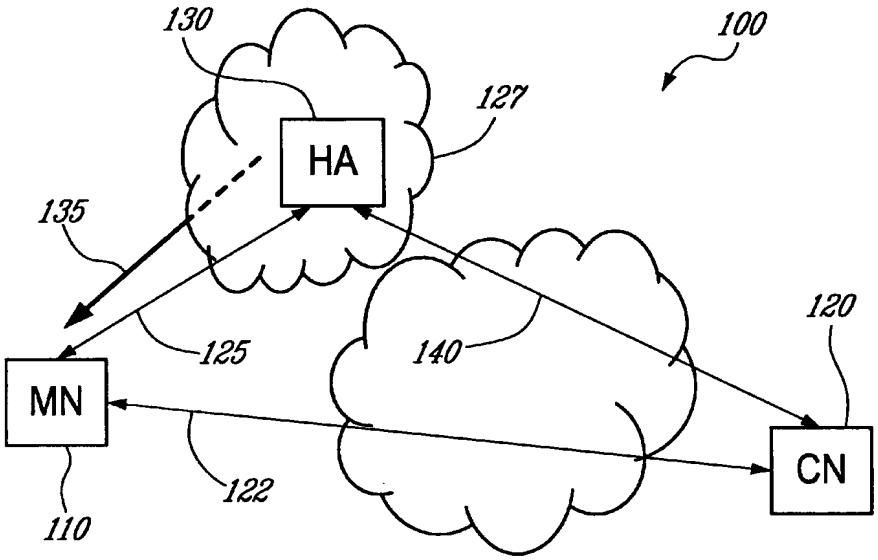


Fig. 1 Técnica anterior

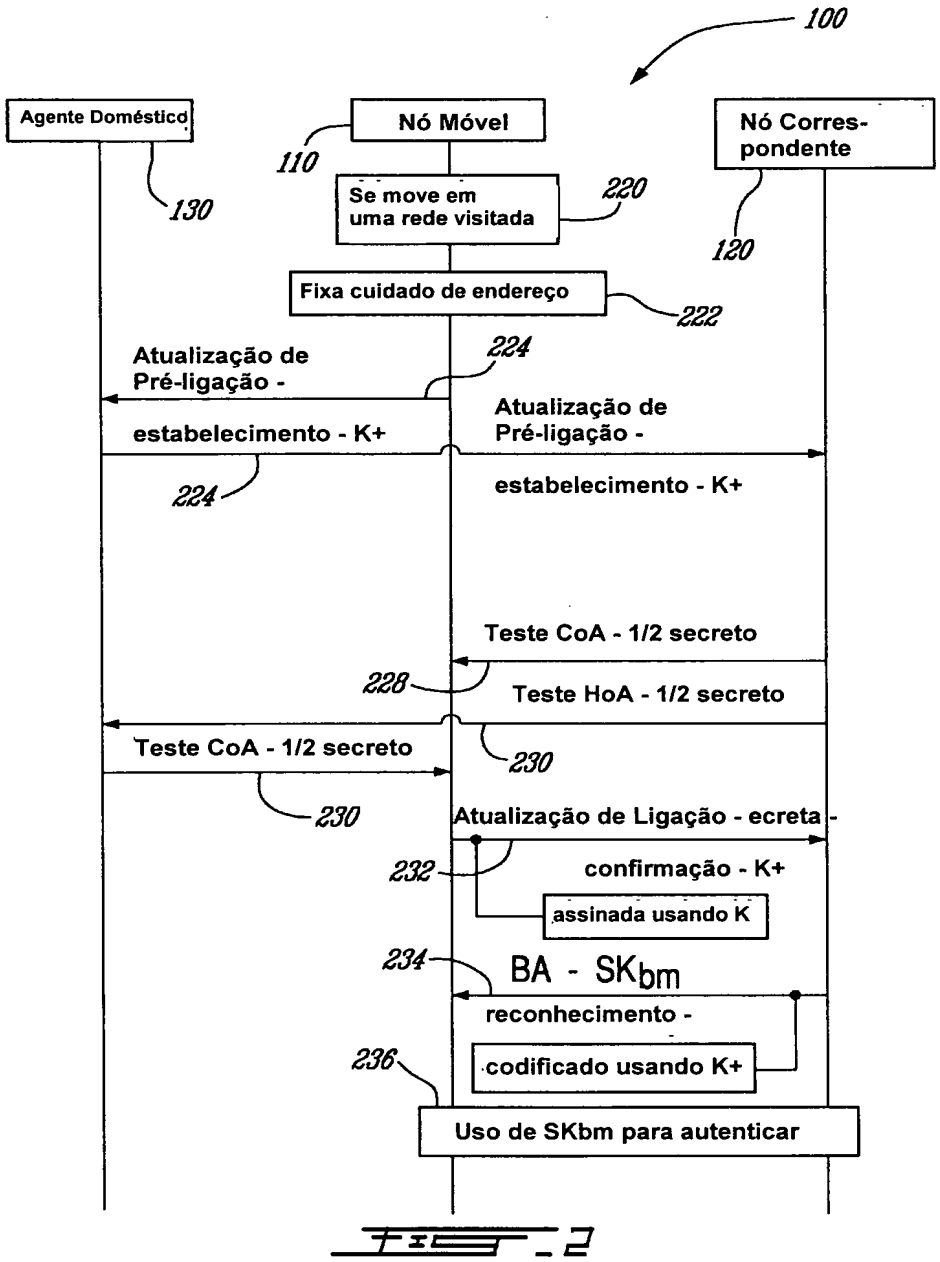

100
Agente Doméstico
Nó Móvel
Nó Corres-pondente
110
130
120
Se move em uma rede visitada
220
Fixa cuidado de endereço
222
224
Atualização de Pré-ligação - estabelecimento - K+
224
Atualização de Pré-ligação - estabelecimento - K+
Teste CoA - 1/2 secreto
228
Teste HoA - 1/2 secreto
Teste CoA - 1/2 secreto
230
230
Atualização de Ligação - ecreta -
232
confirmação - K+
assinada usando K
234
BA - SKbm
reconhecimento -
codificado usando K+
236
Uso de SKbm para autenticar

Fig. 2

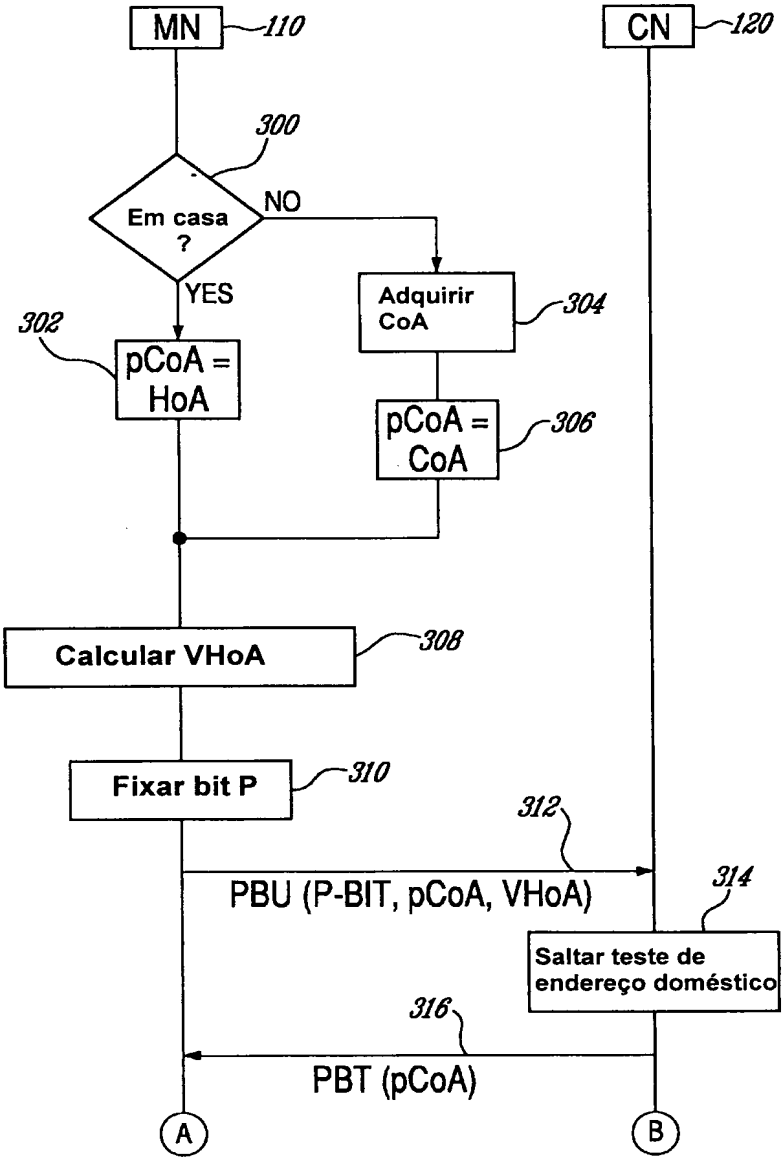

MN
110
CN
120
300
Em casa ?
NO
YES
Adquirir CoA
304
302
pCoA = HoA
pCoA = CoA
306
Calcular VHoA
308
Fixar bit P
310
312
PBU (P-BIT, pCoA, VHoA)
314
Saltar teste de endereço doméstico
316
PBT (pCoA)
A
B

Fig. 3a

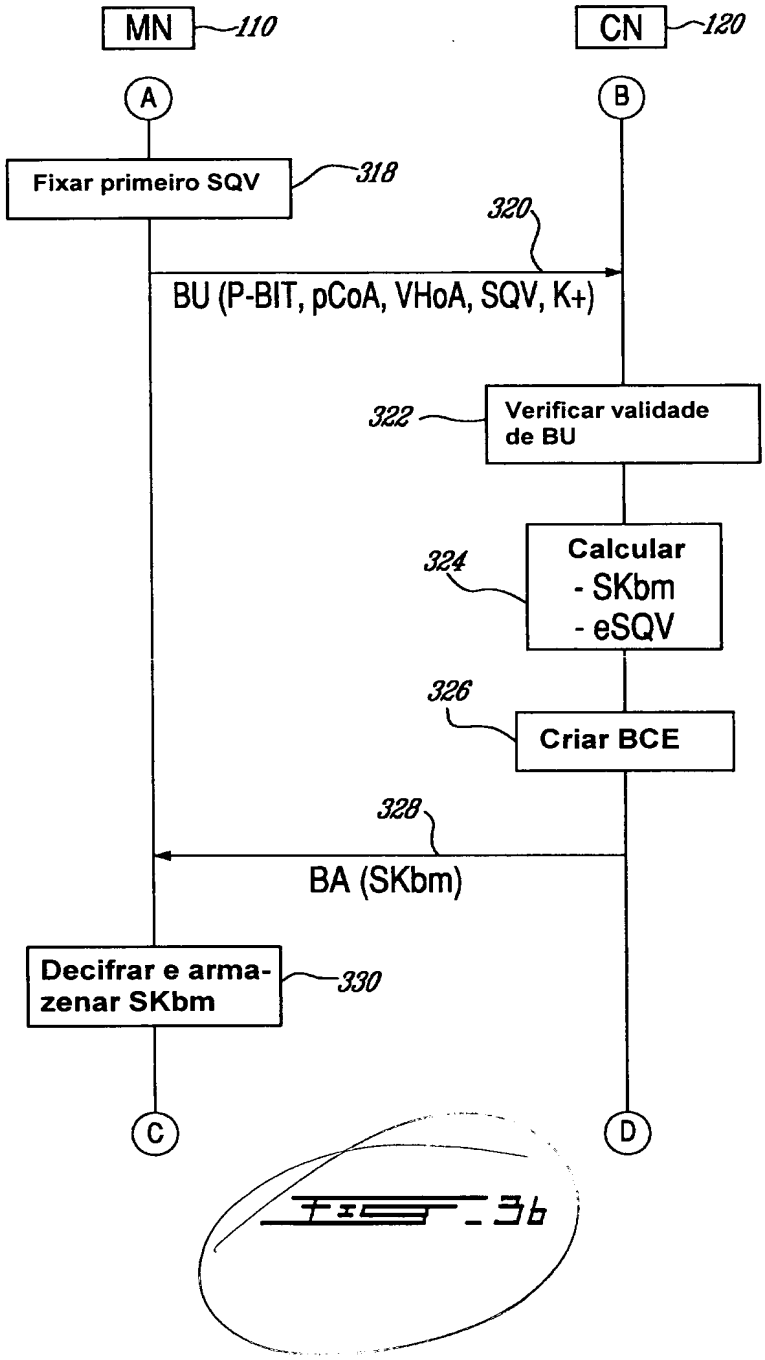

MN
110
CN
120
A
B
Fixar primeiro SQV
318
320
BU (P-BIT, pCoA, VHoA, SQV, K+)
322
Verificar validade de BU
324
Calcular
- SKbm
- eSQV
326
Criar BCE
328
BA (SKbm)
Decifrar e armazenar SKbm
330
C
D

Fig. 3b

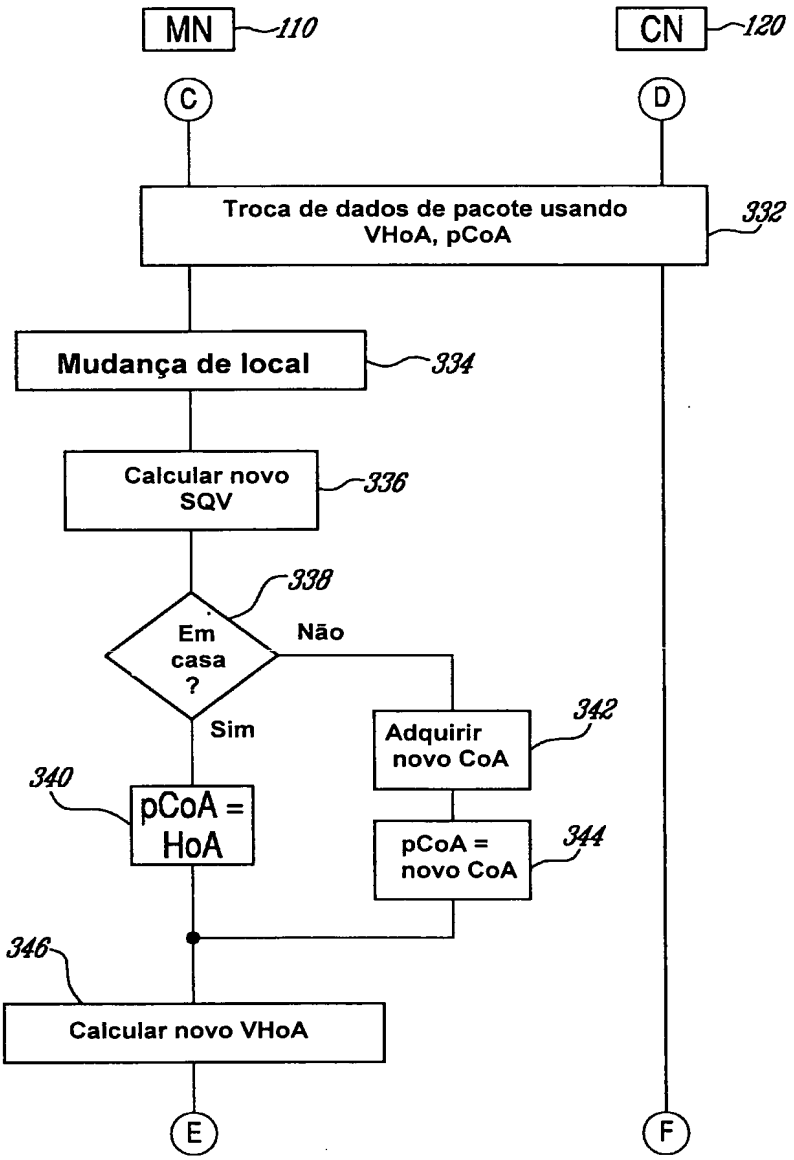

MN
110
CN
120
C
D
Troca de dados de pacote usando VHoA, pCoA
332
Mudança de local
334
Calcular novo SQV
336
338
Em casa ?
Não
Sim
Adquirir novo CoA
342
340
pCoA = HoA
pCoA = novo CoA
344
346
Calcular novo VHoA
E
F

Fig. 3c

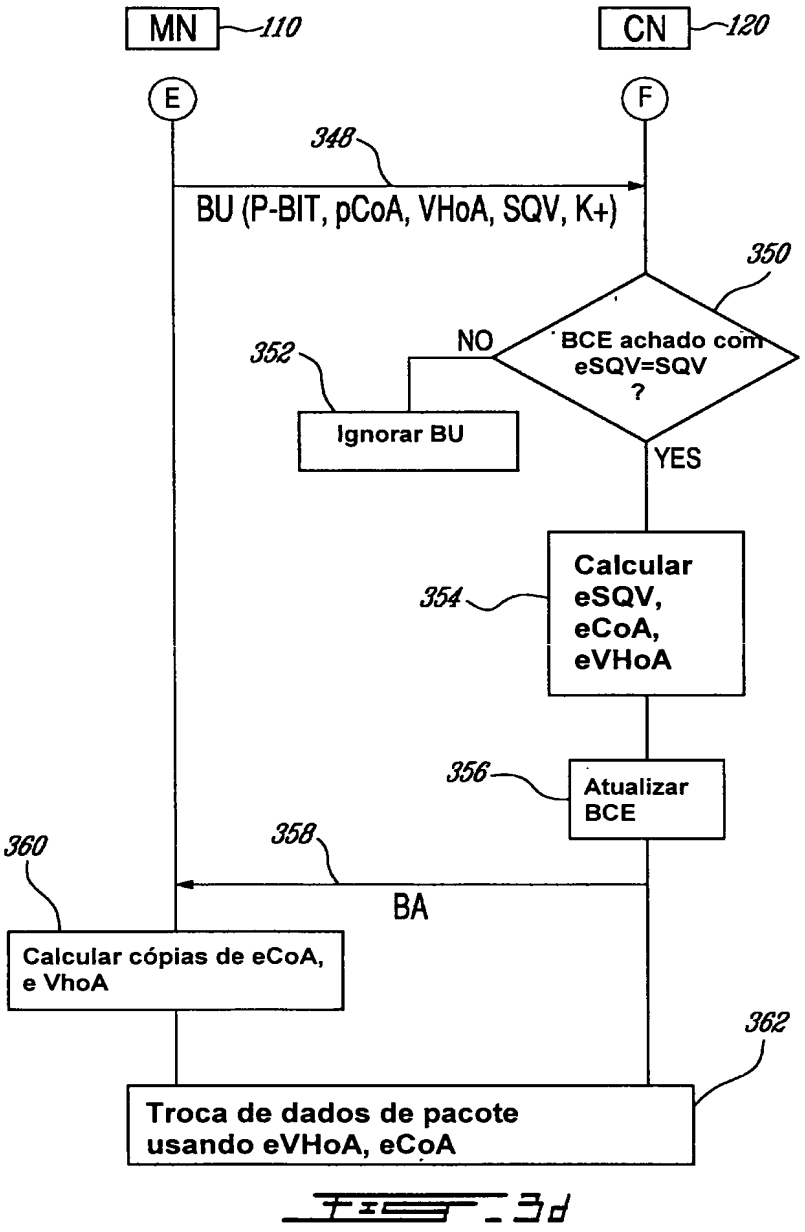

MN
110
CN
120
E
F
348
BU (P-BIT, pCoA, VHoA, SQV, K+)
350
BCE achado com eSQV=SQV ?
NO
352
Ignorar BU
YES
Calcular eSQV, eCoA, eVHoA
354
356
Atualizar BCE
358
BA
360
Calcular cópias de eCoA, e VhoA
362
Troca de dados de pacote usando eVHoA, eCoA

Fig. 3d

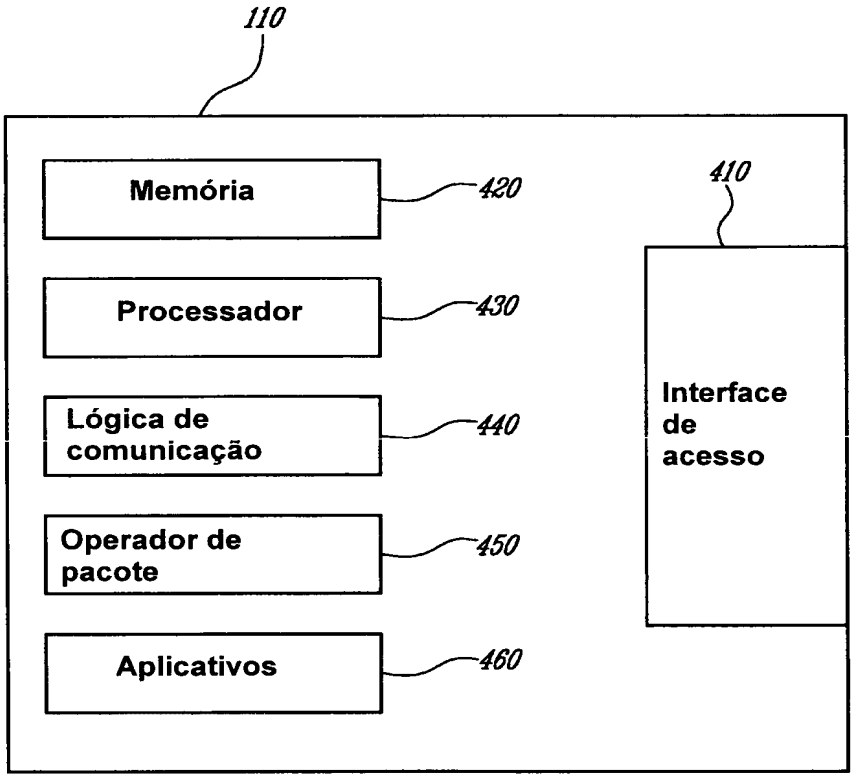

110
Memória
420
Processador
430
Lógica de comunicação
440
Operador de pacote
450
Aplicativos
460
410
Interface de acesso

Fig. 4

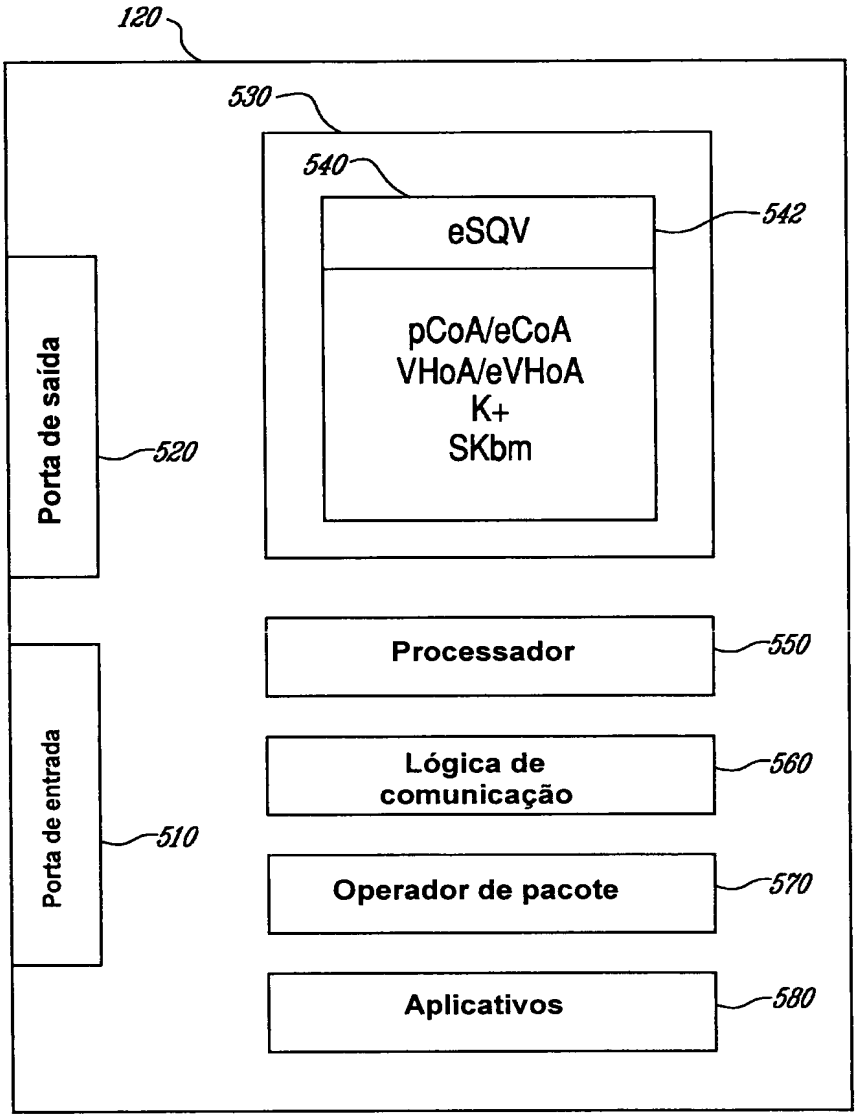

120
530
540
eSQV
542
pCoA/eCoA
VHoA/eVHoA
K+
SKbm
Porta de saída
520
Processador
550
Lógica de comunicação
560
Porta de entrada
510
Operador de pacote
570
Aplicativos
580

Fig. 5

PI0609993-9

RESUMO

"MÉTODO PARA PROVER INCAPACIDADE DE LIGAÇÃO A UM NÓ MÓVEL EM UMA SESSÃO COM UM NÓ CORRESPONDENTE, NÓ MÓVEL, E, NÓ CORRESPONDENTE"

Um método, um nó correspondente e um nó móvel provêem anonimato e incapacidade de ligação a um nó móvel em uma sessão com um nó correspondente. Valores de seqüência, calculados baseados em dados secretos, são adicionados a atualizações enviadas do nó móvel para o nó correspondente e são usados pelo nó correspondente para autenticar atualizações do nó móvel. Um endereço doméstico do nó móvel não é exposto explicitamente. Um endereço de cuidado esperado é calculado no nó correspondente e usado pelo nó correspondente para enviar pacotes de dados ao nó móvel.