



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

(11) PI 0716507-2 B1



(22) Data do Depósito: 26/07/2007

(45) Data de Concessão: 10/12/2019

(54) Título: MÉTODO DE AUTENTICAÇÃO DE SEGURANÇA E DE GERENCIAMENTO DE CHAVE E MÉTODO PARA COMUNICAÇÃO ENTRE UM MANTENEDOR DE CHAVE DE NÍVEL DE TOPO E UM MANTENEDOR DE CHAVE DE NÍVEL UM

(51) Int.Cl.: H04L 9/08; H04L 9/32; H04W 12/04; H04L 29/06; H04W 12/06; (...).

(52) CPC: H04L 9/0844; H04L 9/321; H04W 12/04; H04L 63/064; H04W 12/0602; (...).

(30) Prioridade Unionista: 07/09/2006 US 11/470.887.

(73) Titular(es): MOTOROLA SOLUTIONS, INC..

(72) Inventor(es): HEYUN ZHENG; CHARLES R. BARKER, JR.; AMIT GANDHI; KEITH J. GOLDBERG; SAMER S. HANNA; SURONG ZENG.

(86) Pedido PCT: PCT US2007074422 de 26/07/2007

(87) Publicação PCT: WO 2008/030667 de 13/03/2008

(85) Data do Início da Fase Nacional: 05/03/2009

(57) Resumo: AUTENTICAÇÃO DE SEGURANÇA E GERENCIAMENTO DE CHAVE DENTRO DE UMA REDE MULTI-HOP SEM FIO BASEADA EM INFRAESTRUTURA Um sistema e um método da autenticação da segurança e do esquema da gerência chave em uma rede sem fio multi-hop fornecidos nisto com um modelo de segurança hop-by-hop. O esquema adapta a hierarquia 802.11r chave na rede engrenada do AP. Nesta aproximação, um suporte chave superior (ROKH) deriva e prende a chave por pares mestra da parte superior (PMK_O) para cada dispositivo sem fios do suplicant após o processo de autenticação. Todo o authenticator AP toma ao nível um papel chave do suporte (R1KH) e recebe a chave por pares mestra seguinte do nível (PMK_1) de ROKH. A chave da protecção de dados do nível de ligação é derivada de PMK 1 através do aperto de mão da maneira 802 .11i 4.

MÉTODO DE AUTENTICAÇÃO DE SEGURANÇA E DE GERENCIAMENTO DE
CHAVE E MÉTODO PARA COMUNICAÇÃO ENTRE UM MANTENEDOR DE
CHAVE DE NÍVEL DE TOPO E UM MANTENEDOR DE CHAVE DE NÍVEL UM
Campo da Invenção

5 A presente invenção se refere geralmente a comunicações sem fio e, mais particularmente, a uma autenticação de segurança e a um gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura.

10 Antecedentes

Uma rede sem fio baseada em infraestrutura tipicamente inclui uma rede de comunicação com gateways fixos e com fio. Muitas redes sem fio baseadas em infraestrutura empregam uma unidade móvel ou host, a qual se comunica com
15 uma estação base fixa que é acoplada a uma rede com fio. A unidade móvel pode se mover geograficamente enquanto está se comunicando por um enlace sem fio com a estação base. Quando a unidade móvel se move para fora de alcance de uma estação base, ela pode se conectar ou "transferir de ponto
20 a ponto" para uma nova estação base e começar uma comunicação com a rede com fio através da nova estação base.

Em comparação com redes sem fio baseadas em infraestrutura, tais como redes celulares ou redes por
25 satélite, as redes *ad hoc* são redes de autoformação as quais podem operar na ausência de qualquer infraestrutura fixa e, em alguns casos, a rede *ad hoc* é formada inteiramente por nós móveis. Uma rede *ad hoc* tipicamente inclui várias unidades móveis potencialmente distribuídas
30 geograficamente, às vezes referidas como "nós", os quais

são conectados de forma sem fio a cada outro por um ou mais enlances (por exemplo, canais de comunicação de frequência de rádio). Os nós podem se comunicar uns com os outros por uma mídia sem fio sem o suporte de uma rede baseada em 5 infraestrutura ou com fio.

Conforme as redes de comunicações se tornam mais prevalentes, a segurança continua a ser uma preocupação principal de provedores de rede de comunicação e usuários finais. Isto é mais evidente quando se usa uma rede sem fio 10 móvel em que o ambiente de segurança pode oferecer os maiores desafios, uma vez que os dados podem ser prontamente recebidos e manipulados por muitos nós. Os enlances de rádio usados em uma rede sem fio expõem a sinalização e os dados atravessando a rede a bisbilhoteiros e/ou a supostos hackers. Em uma rede sem fio de salto 15 múltiplo, isto requer que cada enlace nos dispositivos em malha (mesh) tenha uma associação de segurança única estabelecida através do processo de autenticação de salto múltiplo e de gerenciamento de recurso. Então, os quadros 20 de ar no enlace podem ser protegidos com as associações de segurança estabelecidas.

Breve Descrição dos Desenhos

As figuras associadas, onde números de referência iguais se referem a elementos idênticos ou funcionalmente 25 similares por todas as vistas separadas e os quais em conjunto com a descrição detalhada abaixo são incorporados em e fazem parte do relatório descritivo, servem para ilustração adicional de várias modalidades e para explicação dos vários princípios e vantagens, tudo de 30 acordo com a presente invenção.

A FIG. 1 ilustra uma rede sem fio de salto múltiplo baseada em infraestrutura de exemplo de acordo com algumas modalidades da presente invenção.

5 A FIG. 2 ilustra um formato de mensagem de exemplo de algumas modalidades da presente invenção.

A FIG. 3 é um fluxograma que ilustra um processo de distribuição de chave e de autorização de papel de acordo com algumas modalidades da presente invenção.

10 A FIG. 4 ilustra um procedimento de autenticação de acordo com algumas modalidades da presente invenção.

A FIG. 5 é um fluxograma de mensagem que ilustra mensagens de autenticação trocadas entre os vários elementos da rede da FIG. 1, de acordo com algumas modalidades da presente invenção.

15 A FIG. 6 ilustra maiores detalhes da troca de mensagem da FIG. 5 de acordo com algumas modalidades da presente invenção.

Os técnicos versados apreciarão que elementos nas figuras são ilustrados por simplicidade e clareza e não foram desenhados necessariamente em escala. Por exemplo, as dimensões de alguns dos elementos nas figuras podem ser exageradas em relação a outros elementos, para se ajudar a melhorar o entendimento das modalidades da presente invenção.

25 Descrição Detalhada

Antes de se descreverem em detalhes as modalidades que estão de acordo com a presente invenção, deve ser observado que as modalidades residem primariamente em combinações de etapas de método e componentes de aparelho relacionados à
30 autenticação de segurança e ao gerenciamento de chave.

Assim sendo, os componentes de aparelho e as etapas de método foram representados, onde apropriado, por símbolos convencionais nos desenhos, mostrando apenas aqueles detalhes específicos que são pertinentes para o
5 entendimento das modalidades da presente invenção, de modo a não se obscurecer a exposição com detalhes que serão prontamente evidentes para aqueles de conhecimento comum na técnica, tendo o benefício da descrição aqui.

Neste documento, termos relacionais tais como primeiro
10 e segundo, topo e fundo e similares podem ser usados unicamente para se distinguir uma entidade ou ação de uma outra entidade ou ação, sem necessariamente requerer ou implicar qualquer relação ou ordem real como essa entre tais entidades ou ações. Os termos "compreende",
15 "compreendendo" ou qualquer outra variação dos mesmos são pretendidos para cobrirem uma inclusão não exclusiva, de modo que um processo, método, artigo ou aparelho que compreende uma lista de elementos não inclua apenas aqueles elementos, mas também inclua outros elementos não
20 expressamente listados ou inerentes nesse processo, método, artigo ou aparelho. Um elemento seguido por "compreende... um" não impede, sem maiores restrições, a existência de elementos idênticos adicionais no processo, método, artigo ou aparelho que compreende o elemento.

25 Será apreciado que modalidades da invenção descritas aqui podem ser compreendidas por um ou mais processadores convencionais e instruções de programa armazenadas únicas que controlam um ou mais processadores para a implementação, em conjunto com certos circuitos não de
30 processador, de algumas, da maioria ou de todas as funções

de autenticação de segurança e de gerenciamento de chave descritas aqui. Os circuitos não de processador podem incluir, mas não estão limitados a um receptor de rádio, um transmissor de rádio, controladores de sinal, circuitos de relógio, circuitos de fonte de potência e dispositivos de entrada de usuário. Como tal, estas funções podem ser interpretadas como etapas de um método para a realização de autenticação de segurança e de gerenciamento de chave. Alternativamente, algumas ou todas as funções poderiam ser implementadas por uma máquina de estado que não tenha instruções de programa armazenadas, ou em um ou mais circuitos integrados específicos de aplicação (ASICs), nos quais cada função ou algumas combinações de certas funções são implementadas como uma lógica personalizada.

Obviamente, uma combinação das duas abordagens poderia ser usada. Assim, métodos e meios para estas funções foram descritos aqui. Ainda, é esperado que alguém de conhecimento comum, não obstante possivelmente motivados por esforço significativo e muitas escolhas de projeto, por exemplo, tempo disponível, tecnologia atual e considerações econômicas, quando guiado pelos conceitos e princípios mostrados aqui serão prontamente capazes pela geração de instruções de software e programas e ICs com experimentação mínima.

A presente invenção provê um esquema de autenticação de segurança e de gerenciamento de chave para uma rede sem fio de salto múltiplo baseada em infraestrutura com um modelo de segurança de salto por salto. Os blocos de construção básicos da presente invenção são IEEE 802.11i e IEEE 802.1x. Para a transferência rápida, os recursos em

802.11r são incluídos.

O IEEE 802.1x é uma nova tecnologia que provê uma capacidade de escalonamento quase ilimitada com uma supervisão de administração mínima. Ele também permite que
5 métodos de autenticação diferentes sejam selecionados pelos usuários ou pelas operadoras. Na presente invenção, uma Segurança de Camada de Transporte Tunelada (TTLS) é usada para o usuário e a autenticação de dispositivo, devido a sua segurança forte relativa e ao custo de emprego mais
10 baixo. Para os dispositivos, uma autenticação de Segurança de Camada de Transporte (TLS) é um recurso opcional.

Para uma autenticação centralizada e um suporte a 802.11r, o mantenedor de chave de nível de topo (R0KH) para a hierarquia de chave de 802.11r é projetado para estar
15 localizado na rede com fio. O transporte de mensagem entre o mantenedor de chave de nível de topo (nível zero) e os mantenedores de chave de nível 2 (R1KH) pode ser na camada 2 ou na camada de Protocolo de Internet (IP).

Na presente invenção, uma hierarquia de chave baseada
20 em 802.11r é adaptada dentre os pontos de acesso em malha, os quais assumem o papel dos mantenedores de chave de nível um. O fluxo de mensagem de gerenciamento de segurança dentre mantenedores de chave é provido. O gerenciamento de chave pode suportar estações sem fio em conformidade com
25 802.11i e 802.11r. Ele também pode suportar pontos de acesso virtuais com possíveis identificadores de conjunto de serviço múltiplos (SSID) empregados. O fluxo de mensagem de segurança dentre mantenedores de chave de nível zero e de nível um pode ser transportado pela camada 2 ou pela
30 camada 3, dependendo da localização de mantenedor de chave

de nível zero. Quando todos os mantenedores de chave de nível zero são empregados no mesmo segmento de camada 2 com os mantenedores de chave de nível 1, o transporte de comunicação de camada 2 pode ser usado e, caso contrário, o transporte de comunicação de camada 3 deve ser usado. Uma Chave de Distribuição de Chave (KDK) é derivada durante o processo de autenticação inicial e usada para assegurar o material de chave transportado a partir do mantenedor de chave de nível de topo para os mantenedores de chave de próximo nível. O papel do mantenedor de chave de nível um R1KH é autorizado pelo mantenedor de chave de nível de topo com base na informação de autorização a partir do Servidor de Autenticação.

Um sistema e um método de esquema de autenticação de segurança e de gerenciamento de chave em uma rede sem fio de salto múltiplo são providos aqui, com um modelo de segurança de salto por salto. O esquema adapta a hierarquia de chave de 802.11r na rede de ponto de acesso (AP) em malha. Nesta abordagem, um mantenedor de chave de nível de topo (R0KH) deriva e mantém a Chave Mestra Formada em Pares de topo (PMK_0) para cada dispositivo sem fio requerente após o processo de autenticação. Todos os pontos de acesso de autenticador (AP) assumem o papel de mantenedor de chave de nível um (R1KH) e recebem a Chave Mestra Formada em Pares de próximo nível (PMK_1) a partir do mantenedor de chave de nível de topo R0KH. A chave de proteção de dados de nível de enlace é derivada a partir de PMK_1 através de um aperto de mão de 4 vias, tal como um aperto de mão de 4 vias de 802.11i.

A FIG. 1 ilustra uma rede sem fio de salto múltiplo

baseada em infraestrutura de exemplo 100 de acordo com algumas modalidades da presente invenção. Na rede de exemplo 100 da FIG. 1, os canais de comunicação de nível 2 dentre os mantenedores de chave são usados e um mantenedor 5 de chave de nível de topo R0KH é anexado a um comutador de Ethernet central. Assim, o mantenedor de chave de nível de topo R0KH está no mesmo segmento de L2 com todos os dispositivos de ponto de acesso inteligente controlado (IAP) e ponto de acesso de malha (MAP). Um cliente de 10 serviço de usuário de discagem de autenticações remotas (RADIUS) e um autenticador de 802.1X também são implementados na rede 100, de acordo com algumas modalidades da presente invenção.

Será apreciado por aqueles de conhecimento comum na 15 técnica que quando os canais de comunicação de camada de IP são usados para o mantenedor de chave de nível de topo R0KH e o mantenedor de chave de nível um R1KH, o R0KH pode estar localizado em qualquer localização. De acordo com uma implementação de exemplo, R0KH está localizado no mesmo 20 host que o sistema de gerenciamento de rede. Todos os dispositivos de R1KH conectados ao mesmo R0KH são identificados através de um Identificador de Domínio de Mobilidade (MDI), o qual é anunciado em todos os quadros de sinal de orientação.

25 Conforme ilustrado, a rede 100 inclui um ou mais pontos de acesso de malha 135-n (MAP), os quais são usados para roteamento de pacotes de dados de um ou mais pontos de acesso inteligentes 130-n (IAP) para um ou mais dispositivos de assinante sem fio 140-n (SD) (também 30 referidos como estações (STA)). Um ou mais IAPs 130-n então

roteiam os pacotes para um comutador de Ethernet central 125 acoplado de forma comunicativa a um roteador central 115, e um mantenedor de chave de nível de topo (R0KH) 120. O roteador central 115 é acoplado através de uma espinha dorsal (backbone) com fio 110 para um servidor de autenticação 105. Embora apenas os percursos dos dispositivos de assinante (SD) para a rede com fio 125 sejam mostrados, será apreciado por aqueles de conhecimento comum na técnica que conexões em malha podem ser estabelecidas, desde que dois dispositivos vizinhos, tais como o dispositivo de assinante 140-1 e o dispositivo de assinante 140-2 possam se comunicar um com o outro.

O servidor de autenticação 105 funciona para prover serviços de autenticação para o R0KH 120 e será descrito a partir deste ponto. Em geral, o servidor de autenticação 105 realiza uma função de autenticação necessária para se checarem as credenciais de um requerente em nome do autenticador e indica se o requerente está autorizado a acessar serviços de autenticador. Em uma modalidade da presente invenção, o servidor de autenticação 105 está localizado na seção de rede com fio em que a segurança física do host pode ser provida. Por exemplo, o servidor de autenticação 105 pode ser um servidor de serviço de usuário de discagem de autenticações remotas (RADIUS) habilitado para protocolo de autenticação extensível - Segurança de Camada de Transporte tunelada / protocolo de autenticação extensível - protocolo de camada de transporte (EAP-TTLS / EAP-TLS) para uma autenticação centralizada.

Conforme será apreciado por aqueles de conhecimento comum na técnica, os dispositivos de assinante 140-n na

rede 100 podem ser requeridos para o envio e a recepção de dados encriptados. Qualquer dispositivo na rede 100 requerendo / desejando acesso aos serviços oferecidos pelo sistema de autenticador é referido como um requerente. Um
5 dispositivo que autentica um outro dispositivo (requerente) o qual requer / deseja usar os serviços protegidos pelo autenticador é referido como um autenticador. O autenticador faz cumprir um controle de acesso com base no resultado do autenticador.

10 Conforme será apreciado por aqueles de conhecimento comum na técnica, cada nó na rede 100 (isto é, os IAPs 130-n, os MAPs 135-n e os SDs 140-n) é autenticado para a rede 100, antes de se unir à rede em malha. As credenciais para a autenticação podem ser com base, por exemplo, em uma
15 senha, uma identificação (I.D.) de cartão de módulo de identidade de assinante (SIM) ou outra I.D. que seja única para o nó em particular e seja armazenada no servidor de autenticação 105. Cada nó usa esta relação com o servidor de autenticação 105 para autenticação para um MAP ou IAP em
20 malha seguro de um salto, o qual estabeleceu uma conexão segura com o R0KH 120. O R0KH 120 usará os serviços de autenticação providos pelo servidor de autenticação 105. O servidor de autenticação 105 também ajuda ao nó em particular que esteja se autenticando para o
25 estabelecimento de uma relação confiável com seus nós vizinhos pela distribuição de um material de chave mestra de sessão que é encriptado para o R0KH 120. O R0KH 120 deriva as Chaves Mestras Formadas em Pares de nível zero e de nível um (PMK_0, PMK_1). O R0KH 120 também mantém PMK_0
30 e envia PMK_1 para o MAP ou IAP de autenticador, o qual

está assumindo o papel de um mantenedor de chave de nível um.

Em uma modalidade da presente invenção, a rede 100 incorpora uma operabilidade de IEEE 802.11r. O 802.11r
5 provê transições de BSS ("Conjunto de Serviço Básico") rápidas. O 802.11r assim facilita a conectividade a bordo de veículos em movimento, com transferências rápidas de uma estação base para uma outra gerenciadas de uma maneira sem emendas. A aplicação primária atualmente divisada para o
10 padrão 802.11r é em VoIP ("voz por IP" ou telefonia baseada em Internet) através de telefones móveis projetados para funcionarem com redes de Internet sem fio, ao invés de (ou além de) redes celulares padronizadas.

O 802.11r refina o processo de transição de um cliente
15 móvel, conforme ele se move entre os pontos de acesso. O protocolo permite que um cliente sem fio estabeleça um estado de segurança e de qualidade de serviço (QoS) em um novo ponto de acesso, antes de fazer uma transição, o que leva a uma perda de conectividade e uma perturbação de
20 aplicação mínimas. As mudanças gerais no protocolo não introduzem quaisquer novas vulnerabilidades de segurança. Isto preserva o comportamento de estações e pontos de acesso atuais. O 802.11r provê mecanismos para roaming de clientes móveis para comunicação com pontos de acesso
25 candidatos, estabelecimento de associações de segurança e reserva de recursos de QoS.

De acordo com a presente invenção, na rede 100 da FIG. 1, uma hierarquia de chave baseada em 802.11r é aplicada a um AP em malha, desse modo tornando uma transferência
30 rápida possível para um ou mais APs móveis. Nesta

hierarquia de chave, uma chave de nível de topo PMK_0 é gerada no R0KH 120 a partir do material de chave mestra recebido a partir do servidor de autenticação 105. No próximo nível, uma PMK_1 é derivada no R0KH 120 a partir da PMK_0. A PMK_1 é entregue para o R1KH. A chave transiente formada em pares (PTK) é derivada a partir de PMK_1 entre o requerente e o autenticador através de um aperto de mão de 4 vias de 802.11i. De acordo com algumas modalidades da presente invenção, o mantenedor de chave de nível de topo R0KH 120 está localizado na seção de rede com fio e afixado ao comutador de Ethernet central 125 e todos os outros pontos de acesso em malha (MAP) 135-n e os IAPs 130-n assumirão o papel de mantenedor de chave de nível um.

Em alguns empregos da presente invenção, o R0KH 120 pode estar contido em cada IAP 130-n, desse modo todo o MAP 135-n associado àquele IAP 130-n será R1KH sob aquele R0KH 120. (não mostrado) Quando os canais de comunicação de camada de IP são usados para R0KH e R1KH, os R0KH e R1KH podem estar localizados em um segmento de camada 2 diferente.

Proxy de EAPOL dentre Mantenedores de Chave

Um protocolo de exemplo usado para comunicações entre os nós e o servidor 105 é um EAP (Protocolo de Autenticação Extensível). O protocolo de EAP define um formato de mensagem e um aperto de mão de troca para suporte de múltiplos métodos de autenticação. O EAP tipicamente roda diretamente por camadas de enlace de dados, tal como um Protocolo de Ponto a Ponto (PPP) ou IEEE 802, sem requerer um IP. O EAP provê seu próprio suporte para duplicação e eliminação e retransmissão, mas confia em garantias de

ordenação de camada mais baixa. Uma fragmentação não é suportada no EAP em si. Contudo, métodos de EAP individuais podem suportar uma fragmentação, tal como EAP-TLS, onde dados de certificado longos precisam ser transmitidos em vários pacotes. Para 802.1X, por exemplo, as mensagens de EAP entre o requerente de autenticação e o R0KH 120 são encapsuladas em formatos de mensagem de EAPOL (EAP por rede de área local (LAN)). O EAP é flexível e extensível no suporte de múltiplos mecanismos de autenticação, tais como senha de usuário, autenticação baseada em certificado, senha de uso único, ficha de autenticação ou cartão inteligente, e similares. Ele provê um veículo para negociação e uso de mecanismos de autenticação apropriados incluindo aqueles os quais derivam um material de chaveamento no nó e o servidor de autenticação 105.

Um procedimento de autenticação começa quando um nó transmite uma requisição de autenticação usando, por exemplo, um Protocolo de Autenticação Extensível (EAP) compreendendo pacotes de EAP Por Rede de Área Local (EAPOL). O processo de autenticação envolve vários pacotes de EAPOL serem transmitidos e recebidos, começando com um pacote de começo de EAP e terminando com um pacote de mensagem de sucesso de EAP ou um pacote de mensagem de falha de EAP. O servidor de autenticação armazena as credenciais de autenticação de um dispositivo móvel (tipicamente denominado um Requerente) que está sendo autenticado. Os servidores de autenticação também podem ser conectados a outros servidores de autenticação para a obtenção de credenciais de autenticação de Requerente que não estejam armazenadas localmente.

Quando a hierarquia de chave de 802.11r é usada para o gerenciamento de chave, as mensagens de EAPOL para a autenticação e o gerenciamento de chave têm que ser transportadas entre o mantenedor de chave de nível de topo 5 R0KH e o mantenedor de chave de próximo nível R1KH.

A FIG. 2 ilustra um formato de mensagem 200 para uso na operação de algumas modalidades da presente invenção. Especificamente, a FIG. 2 ilustra uma encapsulação de mensagem de EAP para um quadro de com de mantenedor de 10 chave de L2 de acordo com algumas modalidades da presente invenção. O cabeçalho de Controle de Acesso a Midia (MAC) 205 contém os endereços de MAC de origem e de destino de cada salto. O cabeçalho de Roteamento *Ad hoc* (AHR) 210 contém os endereços de MAC de origem e de destino do 15 autenticador e o dispositivo final de rota em malha (isto é, R1KH e R0KH). Um id de protocolo especial é colocado no campo de id de protocolo de cabeçalho de AHR 210 para representação do pacote de proxy de EAPOL. Um endereço de MAC de requerente 220 também é incluído entre o cabeçalho 20 de AHR 210 e o pacote de EAPOL 230 no formato de mensagem 200. O formato de mensagem 200 inclui um indicador (flag) de i/r 215 no primeiro byte do corpo de carga útil de malha para suporte de requerentes de 802.11i e 802.11r. O formato de mensagem ainda inclui um item de informação de SSID 225 25 para suporte de APs virtuais. O endereço de MAC de requerente 220 é necessário para o R0KH 120 conhecer qual dispositivo requerente de modo a ser capaz de ligar a PMK_0 e a PMK_1 àquele requerente em particular. Quando o indicador (flag) de i/r 215 indica um requerente de 30 802.11i, o R0KH 120 deriva a PMK com base no padrão 802.11i

e entrega a PMK para o R1KH. Quando o indicador (flag) de i/r 215 indica um requerente de 802.11r, o R0KH 120 deriva a PMK_0 e a PMK_1 com base na hierarquia de chave de 802.11r e entrega a PMK_1 para o autenticador (R1KH). O
5 SSID 225 é necessário para a derivação de PMK_0 e de PMK_1. Para APs virtuais, o requerente pode selecionar um SSID a partir de um número de SSIDs disponíveis.

De acordo com a presente invenção, quando as mensagens dentre mantenedores de chave são transportadas na camada de
10 rede, o quadro de EAPOL 230 juntamente com os campos de i/r 215, de SPA 220 e SSID 225 são colocados na carga útil de pacote de IP (protocolo de internet). Adicionalmente, o envio do endereço de MAC de mantenedor de chave também é incluído na carga útil de IP, o que é necessário para a
15 derivação de PMK_1.

Conforme é bem conhecido na técnica, conforme ilustrado na FIG. 2, o quadro de EAPOL 230 inclui uma versão de protocolo 235, a qual é um número binário não sinalizado, cujo valor é a versão do protocolo de EAPOL. O
20 quadro de EAPOL 230 ainda inclui um tipo de pacote 240, o qual é um número binário não sinalizado, cujo valor determina o tipo de pacote conforme se segue: a) EAP-packet; b) EAPOL-Start; c) EAPOL- Logoff; d) EAPOL-Key; e) EAPOL-Encapsulated-ASF-Alert. O quadro de EAPOL 230 ainda
25 inclui um comprimento de corpo de pacote 245, o qual é um binário não sinalizado, cujo valor define o comprimento em octetos do campo de corpo de pacote. O quadro de EAPOL 230 também inclui um corpo de pacote 250, o qual é apresentado, se o tipo de pacote contiver o valor EAP-Packet, EAPOL-Key;
30 caso contrário, ele não é apresentado.

Conforme é bem conhecido na técnica, conforme ilustrado na FIG. 2, o corpo de pacote de EAP 250 inclui um campo de código 255, o qual identifica o tipo de pacote de EAP. Os códigos de EAP são atribuídos conforme se segue: 1 = Requisição; 2 = Resposta; 3 = Sucesso; 4 = Falha. O corpo de pacote de EAP 250 ainda inclui um campo de identificador 260, o qual ajuda na combinação de respostas com requisições. O corpo de pacote de EAP 250 ainda inclui um campo de comprimento 265, o qual indica o comprimento do pacote de EAP incluindo os campos de Código 255, Identificador 260, Comprimento 265 e de Dados 275. O corpo de pacote de EAP 250 ainda inclui um campo de tipo 270. O campo de tipo indica o tipo da requisição ou da resposta. Isto pode ser um tipo de identidade ou um método de autenticação em particular. O corpo de pacote de EAP 250 também inclui um campo de dados de tipo 275. O formato do campo de dados 275 é determinado pelo campo de dados de tipo 275. O formato do campo de dados 275 é determinado pelo campo de Código 255 e pelo campo de tipo 270.

20 Chave de Distribuição de Chave e Autorização de Papel

Conforme será apreciado por aqueles de conhecimento comum na técnica, há dois tipos de dispositivos requerentes na rede 100. Os dois tipos de dispositivos requerentes na rede 100 são os dispositivos de MAP 135-n e os dispositivos de STA 140-n. De acordo com algumas modalidades da presente invenção, os dispositivos de MAP 135-n funcionam como R1KH para a hierarquia de chave de 802.11r. Para proteção da distribuição de PMK_1 a partir do mantenedor de chave de topo R0KH 120 para R1KH, uma Chave de Distribuição de Chave formada em pares (KDK) é derivada para cada par de R0KH e

MAP/IAP, conforme ilustrado na FIG. 3.

A FIG. 3 é um fluxograma que ilustra um processo de distribuição de chave e de autorização de papel 300 de acordo com algumas modalidades da presente invenção.

5 Conforme ilustrado na FIG. 3, a operação começa com uma etapa de autenticação inicial 305. A autenticação inicial, por exemplo, pode ser uma autenticação de TTLS ou TLS inicial. Em seguida, na Etapa 310, o R0KH 120 obtém os atributos de autorização a partir do servidor de autenticação 105 na mensagem de "sucesso de autenticação" final para o requerente autenticado. Em seguida, na Etapa 315, é determinado se o atributo de papel de requerente autenticado é um mantenedor de chave de nível um, quando o atributo de papel de requerente autenticado é um mantenedor de chave de nível um, o processo continua para a Etapa 320, na qual o R0KH e o R1KH requerente iniciam um aperto de mão de 4 vias no estilo de 8902.11i com PMK_0 para a derivação da KDK.

Em seguida, na Etapa 320, a KDK é derivada como:

20 KDK = KDF-KDKLen(PMK_0, "KDK Key derivation", SNonce || ANonce || AA || SPA).

onde:

- KDF-256 é definida na Seção 8.5.A.3 de 802.11r.
- SNonce é um número randômico gerado por R1KH, e
- 25 • ANonce é um número randômico gerado por R0KH.
- Os dois números randômicos são trocados durante duas primeiras mensagens do aperto de mão de 4 vias.
- AA é o endereço de MAC de R0KH
- SPA é o endereçamento e MAC de R1KH.

30 Será apreciado por aqueles de conhecimento comum na

técnica que, quando R1KH se move, a KDK fica a mesma, a menos que R0KH inicie um novo aperto de mão de quatro vias de KDK.

Autenticação e Iniciação de Reautenticação

5 A FIG. 4 ilustra um procedimento de autenticação 400 de acordo com algumas modalidades da presente invenção. Conforme ilustrado na FIG. 4, a operação começa com um nó 135-n se ativando na Etapa 405. Em seguida, na Etapa 415, o nó ouve / varre os quadros de sinal de orientação a partir
10 de seus dispositivos vizinhos, os quais podem ser um MAP 135-n ou um IAP 130-n. Em seguida, na Etapa 415, o nó seleciona um IAP ou um MAP para começar o processo de autenticação pela escolha de um dispositivo que tenha indicado que ele tem uma conexão com um servidor de
15 autenticação 105. Em seguida, na Etapa 420, uma primeira autenticação é completada para o nó com o dispositivo de MAP vizinho selecionado. Na Etapa 524, após a primeira autenticação, o nó pode iniciar uma reautenticação com outros dispositivos de MAP vizinhos os quais foram
20 autenticados e conectados a um IAP no mesmo domínio de mobilidade. Esta reautenticação usa um processo de transferência rápida de 802.11r para se evitar uma transação de autenticação plena.

Fluxo de Mensagem de Autenticação

25 A FIG. 5 é um fluxograma de mensagem 500 que ilustra mensagens de autenticação trocadas entre vários elementos da rede da FIG. 1 de acordo com algumas modalidades da presente invenção. Especificamente, a FIG. 5 é um fluxograma de mensagem 500 que ilustra mensagens trocadas
30 entre um dispositivo requerente e um MAP (ou IAP) de R1KH.

A porta controlada de 802.1x de MAP de R1KH é desbloqueada para aquelas mensagens a partir de um dispositivo não autenticado.

Um MAP de R1KH é um dispositivo de MAP ou de IAP o qual tem uma conexão segura para um R0KH; e é presumido já autenticado. Ele assumirá o papel de R1KH para o dispositivo requerente.

No cenário de exemplo do diagrama 500 da FIG. 5, o MAP1 de R1KH 135-1 e o MAP2 de R1KH 135-2 já estão autenticados e têm uma conexão segura com R0KH 120. Eles podem ser, por exemplo, um salto múltiplo a partir de R0KH 120, conforme ilustrado pelo percurso de salto múltiplo 505 da FIG. 5. O requerente (isto é, o dispositivo 140-1) neste cenário de exemplo, ainda não foi autenticado para o MAP1 de R1KH 135-1 e o MAP2 de R1KH 135-2, os quais são os vizinhos de um salto do requerente.

Neste cenário de exemplo, as mensagens entre R0KH 120 e o servidor de autenticação 105 são transportadas pelo protocolo de serviço de usuário de discagem de autenticação remota (RADIUS) baseado em Protocolo de Datagrama de Usuário (UDP). As mensagens são protegidas pelo uso de um esquema de modulação e de codificação de segurança de protocolo RADIUS. Ainda, neste cenário de exemplo, as mensagens de autenticação entre R1KH 135-1 e R0KH 120 são transportadas pelo mecanismo de criação de proxy de protocolo de autenticação extensível por rede de área local (EAPOL) e os materiais de chave são protegidos com KDK entre o R0KH e o R1KH. O R1KH 135-1 notifica o R0KH 120 do SSID selecionado pelo requerente 140-1 para uma implementação de ponto de acesso (AP) virtual.

Conforme ilustrado na FIG. 5, o processo de autenticação começa quando o requerente 140-1 inicia uma requisição de associação 510 com seu MAP1 vizinho 135-1. Em resposta, o MAP1 135-1 envia uma resposta de associação 515. Por exemplo, o processo de autenticação 802.1x será começado pelo requerente 140-1 (EAPOL-Start a partir do requerente), se a autenticação de EAP de 802.1X 520 for selecionada através das duas primeiras mensagens de associação. Após uma autenticação de EAP de 802.1x bem sucedida, uma MSK será entregue a partir do servidor de autenticação 105 para o R0KH 120 na mensagem de Acesso Aceito em conjunto com o pacote de EAP-Success e outras atribuições de autorização. Após obter MSK, o R0KH 120 computa uma PMK_0 e uma PMK_1, conforme descrito no padrão 802.11r.

Para decidir se um processo de derivação de KDK é ou não para ser conduzido, o R0KH 120 checa o papel do requerente a partir dos atributos de autorização retornados a partir do servidor de autenticação de back end 105. Se o requerente 140-1 tiver um papel de R1KH, a troca de mensagem de derivação de KDK 525 será conduzida. Caso contrário, nenhum processo de derivação de KDK será iniciado para o requerente 140-1.

Para a geração dos nomes únicos para a PMK_0 e a PMK_1, o R0KH 120 gera um número randômico denominado ANonce a ser usado para a derivação do nome de PMK_0 e do nome de PMK_1. Este ANonce é enviado para o MAP1 135-1 em conjunto com a PMK_1 e o nome de PMK_1 na mensagem 530. O ANonce é para ser usado por MAP1 135-1 no aperto de mão de 4 vias com o requerente 140-1. O requerente 140-1 então

usará o mesmo ANonce para derivar os mesmos nomes de chave.

Após receber a PMK_1 530 a partir do R0KH 120, o MAP1 inicia um aperto de mão de 4 vias 535 com o requerente 140-1 para a geração de uma PTK para proteção do enlace entre o
5 requerente 140-1 e o MAP3 135-3 (não mostrado na FIG. 5). Após isso, o MAP1 135-1 e o requerente 140-1 podem se comunicar em um enlace seguro 540.

A FIG. 6 ilustra uma troca de mensagem detalhada de exemplo 600, conforme descrito previamente aqui na FIG. 5,
10 quando a autenticação de 802.1x é EAP-TTLS, de acordo com algumas modalidades da presente invenção. Conforme ilustrado na FIG. 6, o requerente 140-1 envia um quadro EAPOL-start 605 para o MAP1 de R1KH 135-1, quando uma autenticação de 802.1x é selecionada. O R1KH 135-1 então
15 transporta este quadro 610 para o R0KH 120. O R0KH 120 assume o controle de todo o fluxo de mensagem entre o requerente 140-1 e o servidor de autenticação 105. O MAP1 de R1KH 135-1 implementa uma máquina de estado de nova tentativa para o EAPOL-Start para envio para o R0KH 120. A
20 última mensagem PMK_1 ACK 615 completa a máquina de estado em R0KH 120. A última mensagem 620 a partir de R0KH 120 para R1KH 135-1 contém PMK_1, R1Name e Anonce. Se o requerente 140-1 for um dispositivo de 802.11i, apenas a PMK de 802.11i será entregue para o R1KH 135-1.

25 Reautenticação (Transição Rápida)

Com referência de volta à FIG. 5, após a primeira autenticação com o MAP1 135-1, o requerente 140-1 pode iniciar um processo de reautenticação (transferência rápida) com quaisquer dispositivos de MAP vizinhos 135-n,
30 os quais tenham anunciado uma conexão segura com um

servidor de autenticação 105 e estejam no mesmo domínio de mobilidade. O processo de reautenticação segue uma transição de BSS rápida de 802.11r; mecanismo de base pelo ar. A requisição de reautenticação inclui R0Name, R1Name, 5 SNonce e seu nome de mantenedor de chave de nível de topo associado R0KH-ID. R0Name e R1Name também são para serem incluídos.

Conforme ilustrado na FIG. 5, após o procedimento de autenticação ser completado entre o requerente 140-1 e o 10 MAP1 135-1, o requerente 140-1 inicia um procedimento de reautenticação com seu próximo dispositivo vizinho R1KH MAP2 135-2. Por exemplo, uma primeira mensagem com transferência rápida 545 é enviada a partir do requerente 140-1 para o MAP2 135-2. Em resposta, o MAP2 135-2 envia 15 uma requisição de PMK 550 para o R0KH 120 requisitando a PMK_1 correspondente a partir do R0KH 120, se ele não mantiver aquela PMK_1 identificada por R1Name. A requisição de PMK_1 para o R0KH deve incluir o R0Name. Em resposta, o R0KH 120 envia a PMK_1 555 para o MAP2 135-2. 20 Após isso, o MAP2 135-2 envia a segunda mensagem para o requerente 140, quando o MAP2 135-2 obtiver a PMK_1 correspondente. O requerente 140-1 e o MAP2 135-2 completam as mensagens de transferência rápida 560 e resultam em um enlace seguro 565. Será apreciado por aqueles de 25 conhecimento comum na técnica que esta reautenticação de transferência rápida pode ser repetida para qualquer número de dispositivos de MAP ou de IAP no alcance de comunicação (na vizinhança) do requerente.

No relatório descritivo precedente, modalidades 30 específicas da presente invenção foram descritas. Contudo,

alguém de conhecimento comum na técnica aprecia que várias modificações e mudanças podem ser feitas, sem que se desvie do escopo da presente invenção, conforme estabelecido nas reivindicações abaixo. Assim sendo, o relatório descritivo e as figuras devem ser considerados em um sentido ilustrativo, ao invés de restritivo, e pretende-se que todas essas modificações sejam incluídas no escopo da presente invenção. Os benefícios, as vantagens, as soluções para problemas e qualquer (quaisquer) elemento(s) que possam fazer com que qualquer benefício, vantagem ou solução ocorram ou se tornem mais pronunciados não devem ser construídos como recursos críticos, requeridos ou essenciais ou elementos de qualquer uma ou de todas as reivindicações. A invenção é definida unicamente pelas reivindicações em apenso, incluindo quaisquer emendas feitas durante a pendência deste pedido e todos os equivalentes daquelas reivindicações, conforme emitido.

REIVINDICAÇÕES

1. Método de autenticação de segurança e de gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, o método caracterizado pelo
5 fato de compreender:

inicialmente, a autenticação de um requerente incluindo a determinação de um ou mais atributos de papel de requerente autenticado com um servidor de autenticação;

a obtenção de um ou mais atributos de autorização a
10 partir do servidor de autenticação por um mantenedor de chave de nível de topo;

determinar se o atributo de papel de requerente autenticado é um mantenedor de chave de nível um pelo mantenedor de chave de nível de topo;

15 iniciar um aperto de mão de quatro vias entre o mantenedor de chave de nível de topo e o requerente com uma chave mestra formada em pares (PMK)_0 para a derivação de uma Chave de Distribuição de Chave (KDK) quando o atributo de papel de requerente autenticado for um mantenedor de
20 chave de nível um; e

quando o atributo de papel de requerente autenticado não for um mantenedor de chave de nível um:

a comunicação de uma chave mestra formada em pares de nível um (PMK)_1 a partir do mantenedor de chave
25 de nível de topo para um mantenedor de chave de nível um,

a iniciação de um aperto de mão de quatro vias entre o mantenedor de chave de nível um e o requerente com a chave mestra formada em pares de nível um (PMK)_1 para a geração de um enlace de comunicação seguro entre o
30 requerente e o mantenedor de chave de nível um, e

a comunicação no enlace seguro entre o mantenedor de chave de nível um e o requerente.

2. Método de autenticação de segurança e de gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, de acordo com a reivindicação 1, caracterizado pelo fato de o aperto de mão de quatro vias entre o mantenedor de chave de nível de topo e o mantenedor de chave de nível um compreender um aperto de mão de quatro vias no estilo de 802.11i para a derivação de uma KDK entre o mantenedor de chave de nível de topo e o mantenedor de chave de nível um; e ainda onde o aperto de mão de quatro vias entre o mantenedor de chave de nível um e o requerente compreende um aperto de mão de quatro vias no estilo de 802.11i para a derivação de uma chave transiente formada em pares (PTK) entre o mantenedor de chave de nível um e o requerente.

3. Método de autenticação de segurança e de gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, de acordo com a reivindicação 1, caracterizado pelo fato de a KDK ser derivada como:

$$KDK = KDF\text{-}KDKLen(PMK_0, \text{"KDK Key derivation"}, SNonce || ANonce || AA || SPA).$$

onde:

25 KDF-256 é um número pré-definido,
 SNonce é um número randômico gerado pelo requerente,
 ANonce é um número randômico gerado pelo mantenedor de chave de nível de topo,
 os dois números randômicos são trocados durante duas
 30 primeiras mensagens do aperto de mão de quatro vias,

AA é o endereço de MAC de mantenedor de chave de nível de topo, e

SPA é o endereço de MAC de requerente.

4. Método de autenticação de segurança e de gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, de acordo com a reivindicação 1, caracterizado pelo fato de a etapa de autenticação inicial incluir uma comunicação de uma mensagem de "sucesso de autenticação" final, e ainda onde um ou mais atributos de autorização são obtidos a partir da mensagem de "sucesso de autenticação" final.

5. Método de autenticação de segurança e de gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, de acordo com a reivindicação 1, caracterizado pelo fato de o método ainda compreender:

a iniciação de uma reautenticação com um outro mantenedor de chave de nível um pelo requerente, onde o outro mantenedor de chave de nível um foi autenticado e conectado ao mantenedor de chave de nível de topo em um mesmo domínio de mobilidade, onde a reautenticação compreende:

a comunicação de uma mensagem usando um processo de transferência rápida a partir do requerente para o outro mantenedor de chave de nível um;

a comunicação da chave mestra formada em pares de nível um (PMK)₁ a partir do mantenedor de chave de nível de topo para o outro mantenedor de chave de nível um;

a conclusão de uma transferência rápida entre o outro mantenedor de chave de nível um e o requerente usando

a chave mestra formada em pares de nível um (PMK)_1 para a geração de um enlace de comunicação seguro entre o requerente e o outro mantenedor de chave de nível um; e

a comunicação no enlace seguro entre o outro mantenedor de chave de nível um e o requerente.

6. Método para comunicação entre um mantenedor de chave de nível de topo e um mantenedor de chave de nível um para uma autenticação de segurança e um gerenciamento de chave em uma rede de salto múltiplo sem fio baseada em infraestrutura, caracterizado pelo fato de compreender:

a comunicação de uma mensagem tendo um formato de mensagem que compreende:

um cabeçalho de Controle de Acesso a Mídia (MAC) contendo um endereço de MAC de origem e de destino de pelo menos um salto;

um cabeçalho de Roteamento *Ad hoc* (AHR) contendo:

um endereço de MAC de origem e um de destino do mantenedor de chave de nível um e do mantenedor de chave de nível de topo, e

uma identificação de protocolo representando um pacote de proxy de protocolo de autenticação extensível por uma rede de área local (EAPOL);

um endereço de MAC de requerente;

um indicador (flag) de i/r que é um indicador de padrão 802.11i ou 802.11r; e

um identificador de conjunto de serviço (SSID).

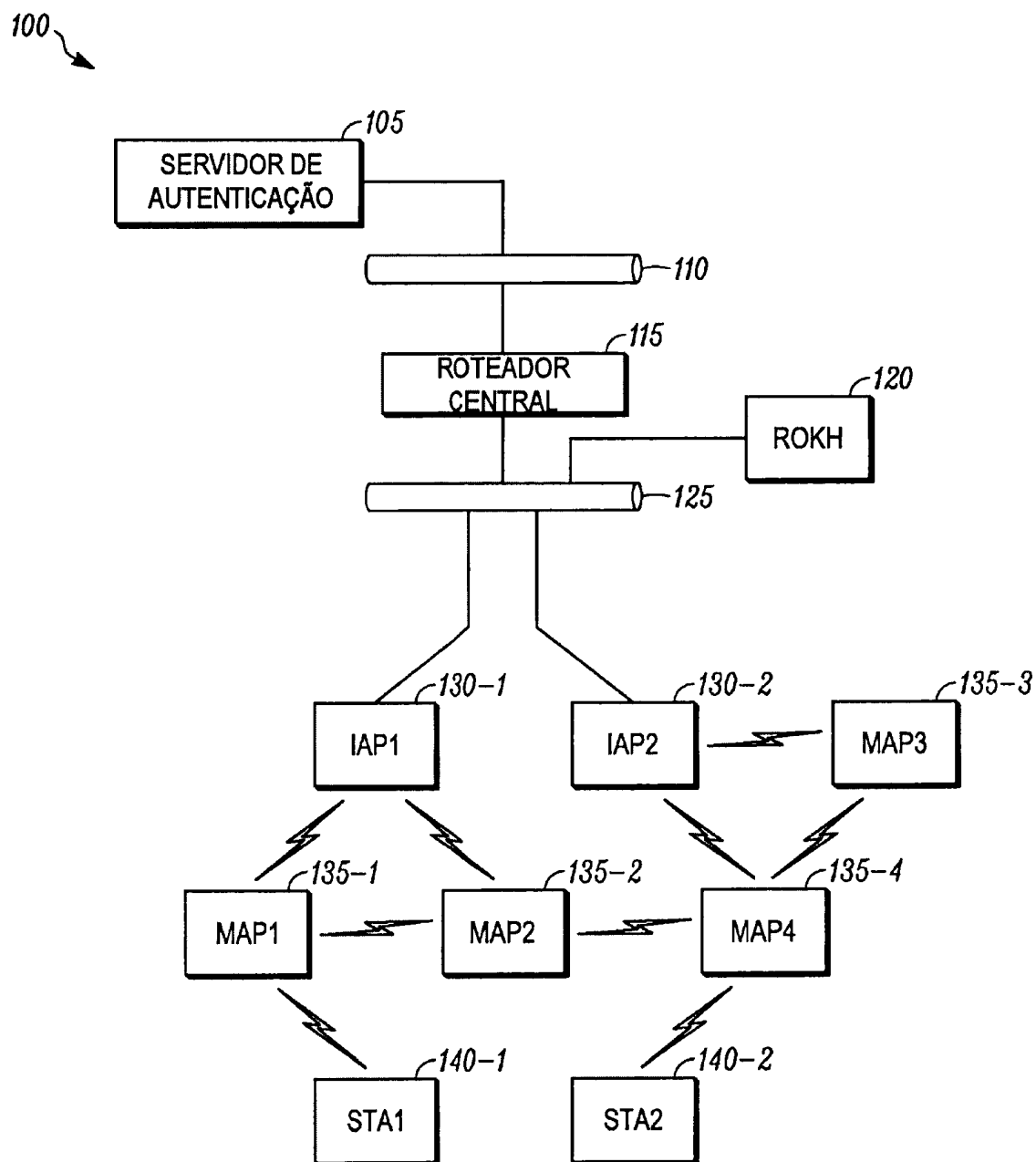
7. Método, de acordo com a reivindicação 6, caracterizado pelo fato de o endereço de MAC de requerente identificar qual dispositivo requerente ligar a uma chave mestra formada em pares_0 (PMK_0) e uma PMK_1.

8. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de o indicador (flag) de i/r indicando um requerente de 802.11i identificar que a PMK é derivada com base no padrão 802.11i e a PMK é para ser
5 enviada para um R1KH.

9. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de o indicador (flag) de i/r indicando um requerente de 802.11r identificar que PMK_0 e PMK_1 são derivadas com base em uma hierarquia de chave de
10 802.11r e a PMK_1 é para ser entregue para o autenticador.

10. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de o SSID ser usado para derivação de PMK_0 e PMK_1 para um ponto de acesso virtual, e ainda onde um requerente seleciona um SSID a partir de uma
15 pluralidade de SSIDs disponíveis.

11. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de a mensagem ser transportada em uma camada de comunicação selecionada a partir do grupo que compreende uma camada 2 e uma camada 3, e
20 ainda onde quando o formato de mensagem é colocado na carga útil de pacote de protocolo de internet (IP), um endereço de MAC de R1KH ser adicionado em conteúdos de mensagem.

*FIG. 1*

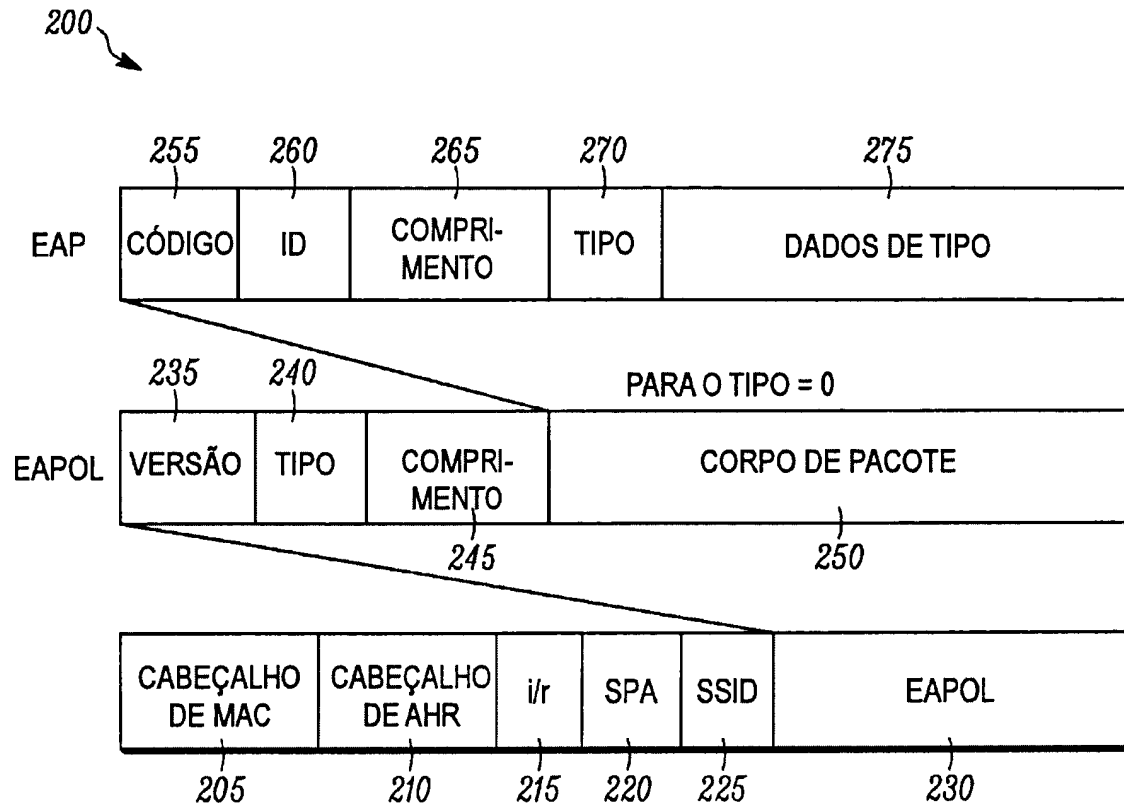


FIG. 2

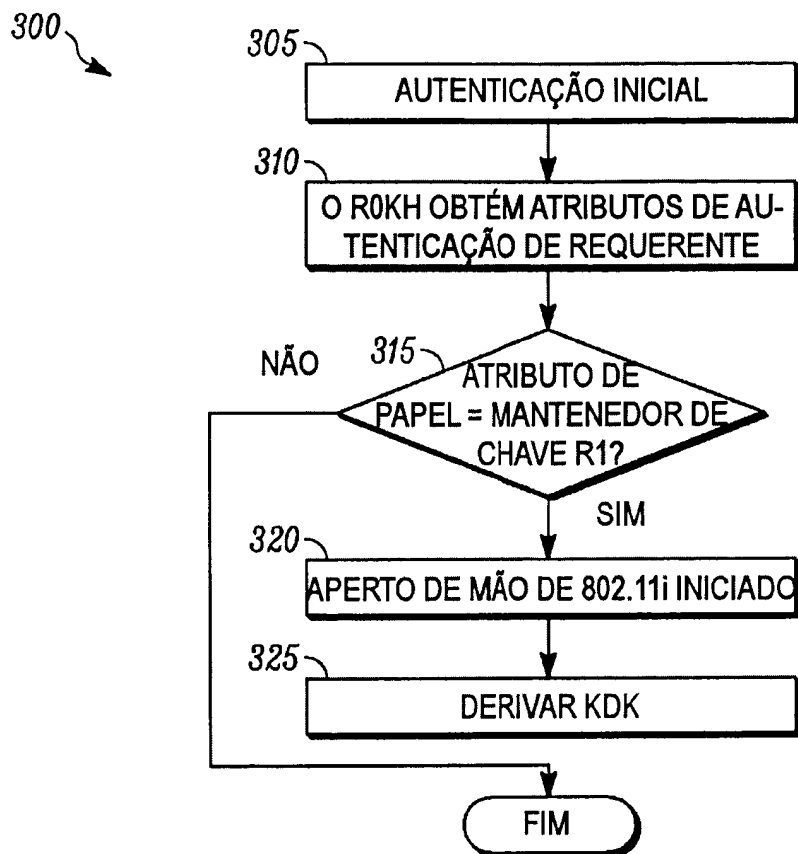


FIG. 3

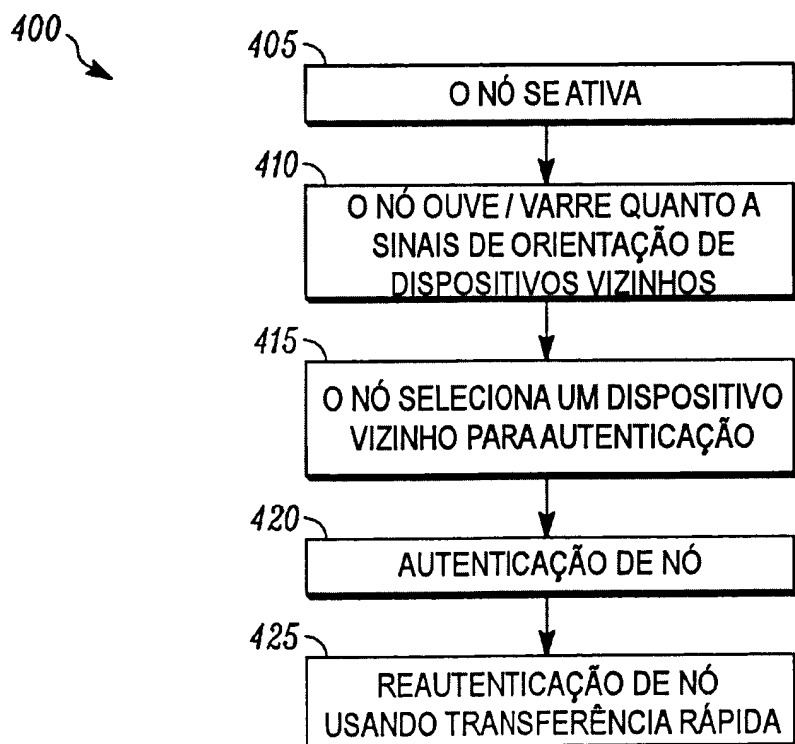


FIG. 4

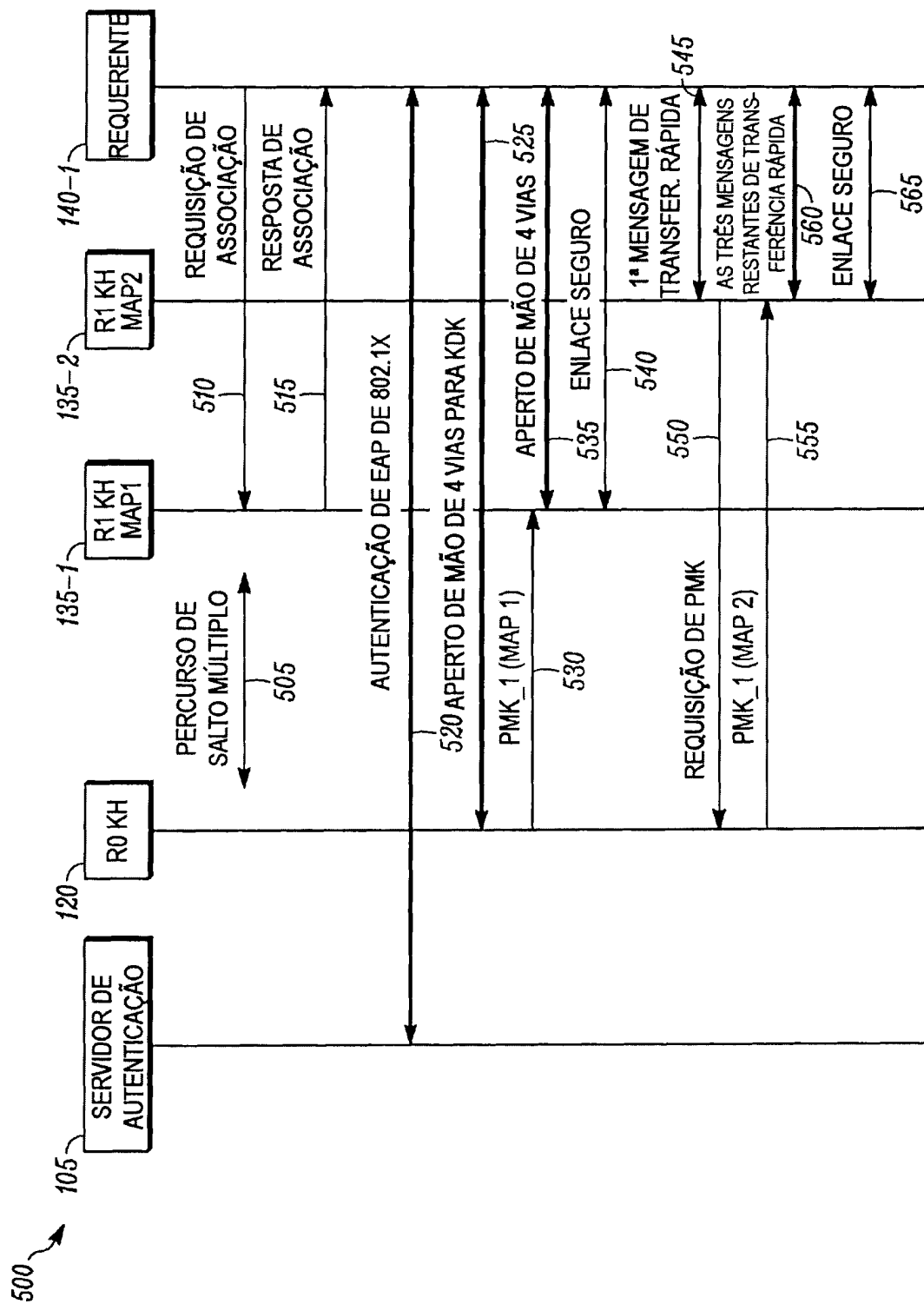


FIG. 5

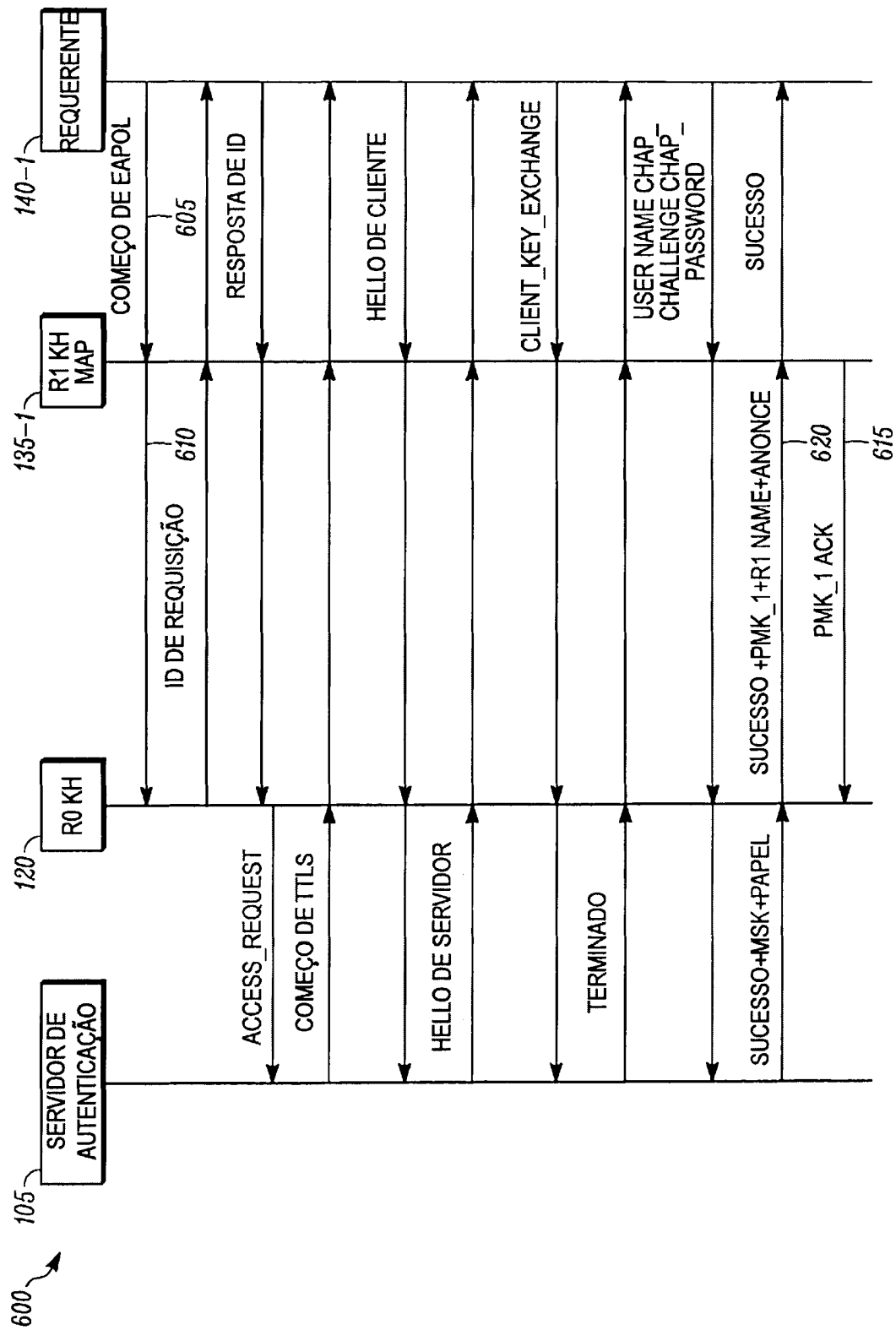


FIG. 6