



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

(11) PI 0808892-6 B1



(22) Data do Depósito: 04/03/2008

(45) Data de Concessão: 24/09/2020

(54) Título: MÉTODO DE OPERAÇÃO DE UM PONTO DE MALHA PARA ESTABELECEER ASSOCIAÇÕES SEGURAS EM UMA REDE DE COMUNICAÇÃO

(51) Int.Cl.: H04L 29/06; H04W 12/00; H04W 12/06; H04W 84/18.

(52) CPC: H04L 63/0869; H04W 12/003; H04W 12/06; H04W 84/18.

(30) Prioridade Unionista: 12/03/2007 US 60/894,261; 26/02/2008 US 12/037,547.

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

(72) Inventor(es): ANTHONY J. BRASKICH; CHARLES R. BARKER, JR.; STEPHEN P. EMEOTT; GUENAE L. T. STRUTT.

(86) Pedido PCT: PCT US2008055739 de 04/03/2008

(87) Publicação PCT: WO 2008/112455 de 18/09/2008

(85) Data do Início da Fase Nacional: 14/09/2009

(57) Resumo: MÉTODO PARA ESTABELECEER ASSOCIAÇÕES SEGURAS EM UMA REDE DE COMUNICAÇÃO É revelado um método para autenticação de segurança em uma rede sem fio. É fornecido um método de uma rede de malha ad hoc para dois dispositivos para determinar rapidamente papéis (isto é, qual é o autenticador e qual é o suplicante) enquanto estabelece uma associação de segurança. A invenção provê ainda a inclusão de informações de chave cache no processo de negociação de papel e a aplicação de negociação de papel em uma estabelecimento de comunicações de três sentidos encurtado.

MÉTODO DE OPERAÇÃO DE UM PONTO DE MALHA PARA ESTABELECE ASSOCIAÇÕES SEGURAS EM UMA REDE DE COMUNICAÇÃO

Campo da Invenção

A presente invenção refere-se genericamente a
5 comunicações sem fio e mais particularmente ao
estabelecimento de associações seguras entre dispositivos
que operam em uma rede de comunicação.

Antecedentes

Uma rede sem fio baseada em infraestrutura inclui,
10 tipicamente, uma rede de comunicação com gateways fixa e
cabeada. Muitas redes sem fio baseadas em infraestrutura
empregam uma unidade móvel, ou um hospedeiro, que se
comunica com uma estação base fixa que é acoplada a uma
rede cabeada. A unidade móvel pode se mover geograficamente
15 enquanto se comunica através de um enlace sem fio com a
estação base. Quando a unidade móvel se move para fora do
alcance de uma estação base, pode se conectar ou se
“transferir” para uma estação base nova e iniciar
comunicação com a rede cabeada através da estação base
20 nova.

Em comparação com redes sem fio baseadas em
infraestrutura, como redes celulares ou redes de satélite,
redes ad hoc são redes de autoformação que podem operar na
ausência de qualquer infraestrutura fixa, e em alguns casos
25 a rede ad hoc é formada inteiramente de nós móveis. Uma
rede ad hoc inclui, tipicamente, um número de unidades
potencialmente móveis, geograficamente distribuídas, às
vezes mencionadas como “nós”, que são conectadas sem fio
entre si por um ou mais enlaces (por exemplo, canais de
30 comunicação de radiofrequência). Os nós podem se comunicar

mutuamente através de uma mídia sem fio sem o suporte de uma rede cabeada ou baseada em infraestrutura.

Uma rede de malha sem fio é uma coleção de nós ou dispositivos sem fio organizados em um modo descentralizado para fornecer extensão de faixa mediante permissão para que os nós sejam alcançados através de múltiplos saltos. Em uma rede de múltiplos saltos, pacotes de comunicação enviados por um nó de fonte podem ser retransmitidos através de um ou mais nós intermediários antes de atingir um nó de destino. Uma grande rede pode ser realizada utilizando pontos de acesso inteligentes (IAP) que fornecem nós sem fio com acesso a um "backhaul" cabeado.

Redes ad hoc sem fio podem incluir tanto nós roteáveis (de malha) como nós não roteáveis (não de malha). Nós de malha ou "roteáveis" são dispositivos que podem seguir um protocolo sem fio padrão como Institute of Electrical and Electronics Engineers (IEEE) 802.11s ou 802.16j. Esses dispositivos são responsáveis por remeter pacotes para/a partir dos dispositivos proxy que são associados aos mesmos. Nós não de malha ou "não roteáveis" são dispositivos que seguem um protocolo sem fio padrão como IEEE 802.11 a, b, e, g ou IEEE 802.14, porém, não participando em nenhum tipo de roteamento. Esses dispositivos são "representados" por dispositivo de malha que estabelece rotas para eles.

À medida que as redes de comunicação sem fio se tornam mais predominantes, a segurança continua a ser uma preocupação principal tanto para provedores de rede de comunicação como usuários finais. Isso é mais evidente ao utilizar uma rede sem fio móvel onde o ambiente de

segurança pode oferecer os maiores desafios uma vez que dados podem ser prontamente recebidos e manipulados por muitos nós. Os enlaces de rádio utilizados em uma rede sem fio expõem a sinalização e dados que atravessam a rede a pretensos espiões e/ou hackers. Em uma rede sem fio de múltiplos saltos, isso requer que cada enlace nos dispositivos de malha tenha uma associação de segurança única estabelecida através do processo de gerenciamento de chave e autenticação de múltiplos saltos. Então, os quadros de ar no enlace podem ser protegidos com as associações de segurança estabelecidas.

As soluções de segurança hoje em dia estabelecem tipicamente uma associação de segurança entre um servidor de autenticação e um nó unindo a rede. Infelizmente, pode demorar dez segundos para o nó concluir a autenticação com um servidor de autenticação. Quando um nó une uma rede ad hoc e estabelece um enlace seguro com um de seus vizinhos, é vantajoso fornecer um mecanismo de segurança acelerado que permite rapidamente enlaces seguros entre o nó e outros nós vizinhos que também são membros da rede.

Breve Descrição das Figuras

As figuras em anexo, onde numerais de referência similares se referem a elementos funcionalmente similares ou idênticos em todas as várias vistas e que juntamente com a descrição detalhada abaixo são incorporados em e formam parte do relatório descritivo, servem para ilustrar adicionalmente várias modalidades e explicar vários princípios e vantagens tudo de acordo com a presente invenção.

A figura 1 é uma rede de comunicação de exemplo para

implementação de algumas modalidades da presente invenção.

A figura 2 ilustra um diagrama de fluxo de mensagem de acordo com algumas modalidades da presente invenção.

A figura 3 ilustra mais detalhe do diagrama de fluxo de mensagem da figura 2 de acordo com algumas modalidades da presente invenção.

As figuras 4, 5 e 6 são fluxogramas que ilustram operações de exemplo de um ponto de malha na rede da figura 1 de acordo com algumas modalidades da presente invenção.

Técnicos versados reconhecerão que elementos nas figuras são ilustrados para simplicidade e clareza e não foram traçados necessariamente em escala. Por exemplo, as dimensões de alguns dos elementos nas figuras podem ser exageradas em relação a outros elementos para ajudar a melhorar a compreensão das modalidades da presente invenção.

Descrição Detalhada

Antes de descrever em detalhe modalidades que estão de acordo com a presente invenção, deve ser observado que as modalidades residem principalmente em combinações de etapas de método e componentes de aparelho relacionados ao estabelecimento de associações seguras em uma rede sem fio ad hoc. Por conseguinte, os componentes de aparelho e etapas de método foram representados onde apropriado por símbolos convencionais nos desenhos, mostrando somente aqueles detalhes específicos que são pertinentes à compreensão das modalidades da presente invenção de modo a não obscurecer a revelação com detalhes que serão prontamente evidentes para aqueles com conhecimentos comuns na técnica tendo o benefício da descrição da presente

invenção.

Nesse documento, termos relacionais como: primeiro e segundo; superior e inferior, e similares, podem ser utilizados exclusivamente para distinguir uma entidade ou
5 ação de outra entidade ou ação sem exigir necessariamente ou indicar qualquer tal relação efetiva ou ordem entre tais entidades ou ações. Os termos, "compreende," "compreendendo" ou qualquer outra variação dos mesmos, pretendem cobrir uma inclusão não exclusiva, de tal modo
10 que um processo, método, artigo, ou aparelho que compreende umalista de elementos não inclui somente aqueles elementos, porém pode incluir outros elementos não listados expressamente ou inerentes a tal processo, método, artigo ou aparelho. Um elemento prosseguido por "compreende ...um"
15 não, impede, sem mais limitações, a existência de elementos idênticos adicionais no processo, método, artigo, ou aparelho que compreende o elemento.

Será reconhecido que modalidades da invenção descritas aqui podem ser compreendidas de um ou mais processadores
20 convencionais e instruções de programa armazenadas exclusivas que controlam um ou mais processadores para implementar, em combinação com certos circuitos não processadores, algumas, a maioria ou todas as funções de estabelecer associações seguras em uma rede sem fio ad hoc
25 descrita aqui. Os circuitos não processadores podem incluir, porém não são limitados a, um receptor de rádio, um transmissor de rádio, acionadores de sinal, circuitos de relógio, circuitos de fonte de energia, e dispositivos de entrada de usuário. Como tal, essas funções podem ser
30 interpretadas como etapas de um método para executar o

estabelecimento de associações seguras em uma rede sem fio ad hoc. Alternativamente, algumas ou todas as funções poderiam ser implementadas por uma máquina de estado que não tem instruções de programa armazenadas, ou em um ou mais circuitos integrados de aplicação específica (ASICs), nos quais cada função ou algumas combinações de certas das funções é implementada como lógica customizada. Evidentemente, uma combinação das duas abordagens poderia ser utilizada. Desse modo, métodos e meios para essas funções foram descritos aqui. Além disso, espera-se que aqueles com conhecimentos comuns, não obstante esforço possivelmente significativo e as muitas opções de desenho motivadas, por exemplo, por tempo disponível, tecnologia atual e considerações econômicas, quando guiado pelos conceitos e princípios revelados aqui serão prontamente capazes de gerar tais instruções de software e programas e ICs com experimentação mínima.

Em redes ad hoc é desejável, e muitas vezes necessário, estabelecer pelo menos um e em muitos casos vários enlaces não-hierárquicos com um ou mais pontos de malha não-hierárquica (MP). MPs não transmitirão quadros de dados ou quadros de gerenciamento diferentes daqueles utilizados para estabelecimento de enlace até que o enlace não-hierárquico tenha sido estabelecido com sucesso. O MP deixa cair os tais quadros a partir de um MP não-hierárquico se considerar que o enlace não é estabelecido.

Um MP deve ser capaz de estabelecer pelo menos um enlace de malha com um MP não-hierárquico, e pode ser capaz de estabelecer muitos tais enlaces simultaneamente. É possível que haja mais MPs não-hierárquicos candidatos do

que o dispositivo é capaz de manter enlaces não-hierárquicos simultaneamente. Nesse caso, o MP seleciona com quais MPs estabelecer enlaces não-hierárquicos baseado em alguma medida de qualidade de sinal ou outra informação recebida de MPs vizinhos, candidatos.

O MP inicia o protocolo de estabelecimento de enlace não-hierárquico, por exemplo, nos casos como os dois seguintes cenários. Em cada um desses cenários, o MP recebe um comando pela entidade de gerenciamento de estação (SME)

IEEE 802.11. Em um primeiro cenário, o MP não atingiu o número máximo de vizinhos e deseja aceitar novas conexões.

Nesse cenário, um comando Abrir passivo faz com que o MP inicie uma ocorrência de protocolo de estabelecimento de enlace e ouça solicitações de conexão que entram. Em uma

modalidade exemplar da invenção, o comando Abrir passivo é um primitivo `MLME-PassivePeerLinkOpen().request`. Em um segundo cenário, o MP acorda com o perfil transportado em um sinalizador ou uma resposta de sonda a partir de um MP não-hierárquico e não atingiu o número máximo de vizinhos.

Um comando Abrir Ativo é expedido que faz com que o MP inicie uma ocorrência de protocolo de estabelecimento de enlace com o MP não-hierárquico identificado como `peerId` e envie ativamente uma solicitação de conexão para esse MP não-hierárquico. Em uma modalidade exemplar da invenção, o comando Abrir ativo é um primitivo `MLME-ActivePeerlinkOpen(peerId).request`.

O MP também pode terminar a ocorrência de protocolo, por exemplo, como nos três cenários a seguir. Em um primeiro cenário, o MP encontra falha durante o procedimento de estabelecimento de enlace não-hierárquico.

Como resultado, o MP envia uma solicitação de fechar conexão. Em um segundo caso, o MP recebe uma solicitação de fechar conexão a partir do MP não-hierárquico. Em um terceiro caso, a conexão é fechada porque o MP recebe um
5 sinal de cancelar enlace não-hierárquico. O SME 802.11 pode emitir um comando Cancelar Enlace não-hierárquico. Em uma modalidade exemplar da invenção, o comando Cancelar Enlace não-hierárquico é um primitivo MLME-CancelPeerLink().request. Esse sinal pode ser acionado por
10 algum evento interno. Por exemplo, o MP descobre a falha de transmissão de dados.

A presente invenção provê um meio eficiente de estabelecer um enlace não-hierárquico entre dois membros de uma rede sem fio ad hoc através de um estabelecimento de
15 comunicações de estabelecimento de enlace não-hierárquico enquanto simultaneamente estabelece uma associação de segurança entre os dois. O objetivo é definir um estabelecimento de comunicações utilizando o número menor de mensagens possíveis enquanto provê autenticação mútua,
20 transporte de forma segura e deriva chaves de sessão, e assegura negociação de papel previsível.

A presente invenção provê um método de executar uma associação de segurança conjunta e estabelecimento de comunicações de enlace não-hierárquico em uma arquitetura
25 de associação de segurança de malha eficiente (EMSA). O método requer três mensagens, a saber, uma abertura de enlace não-hierárquico, uma configuração de enlace não-hierárquico e uma resposta de enlace não-hierárquico, no caso em que um dos dois pontos de malha inicie o
30 estabelecimento de comunicações, ou quatro mensagens, a

saber, duas de abertura de enlace não-hierárquico e duas confirmações de enlace não-hierárquico, no evento de ocorrer uma abertura simultânea. O método inclui suporte embutido para negociação de série de segurança e um
5 procedimento de determinação de papel 802.1X, que provê suporte aperfeiçoado para chaves armazenadas em cache, mesmo no caso das duas partes não poder recuperar chaves a partir de um distribuidor de chave de malha EMSA (MKD).

A figura 1 ilustra uma rede sem fio ad hoc 100, de
10 acordo com algumas modalidades da presente invenção. A rede sem fio ad hoc 100, por exemplo, pode ser uma rede de arquitetura habilitada de malha (MEA) ou uma rede 802.11 (isto é, 802.11a, 802.11b, 802.11g ou 802.11s). Será reconhecido por aqueles com conhecimentos comuns na técnica
15 que a rede de comunicação 100, de acordo com a presente invenção, pode compreender, alternativamente, qualquer rede de comunicação empacotada onde pacotes são remetidos através de múltiplos saltos sem fio. Por exemplo, a rede sem fio ad hoc 100 pode ser uma rede que utiliza protocolos
20 de dados de pacote como OFDMA (acesso múltiplo por divisão de frequência ortogonal), TDMA (acesso múltiplo por divisão de tempo), GPRS (Serviço de rádio de pacote geral), e EGPRS (GPRS aperfeiçoado). Adicionalmente, cada salto sem fio da rede de comunicação empacotada 100 pode empregar o mesmo
25 protocolo de dados de pacote que os outros saltos, ou um protocolo de dados de pacote exclusivo por salto.

Como ilustrado na figura 1, a rede de comunicação 100 inclui uma pluralidade de pontos de malha 102-1 até 102-n (mencionados também como nós 102 ou nós móveis 102 ou
30 dispositivos de comunicação 102), e pode, porém não é

exigido, incluir uma rede fixa 104 tendo uma pluralidade de pontos de acesso inteligentes (IAP) 106-1, 106-23, ..., 106-n (mencionados genericamente como nós 106 ou pontos de acesso 106), para fornecer pontos de malha 102 com acesso à rede fixa 104. A rede fixa 104 pode incluir, por exemplo, uma rede de acesso local de núcleo (LAN), e uma pluralidade de servidores e roteadores de gateway para fornecer nós de rede com acesso a outras redes, como outras redes ad-hoc, uma rede de telefone comutada pública (PSTN) e Internet. A rede de comunicação 100 pode incluir ainda uma pluralidade de roteadores fixos ou móveis 107-1 até 107-n (mencionados genericamente como roteadores 107 ou nós 107 ou dispositivos de comunicação 107) para rotear pacotes de dados entre outros nós 102, 106 ou 107. Observa-se que para fins dessa discussão, os nós discutidos acima podem ser coletivamente mencionados como "nós 102, 106 e 107" ou simplesmente "nós" ou alternativamente como "dispositivos de comunicação."

Como reconhecido por aqueles versados na técnica, os nós 102, 106 e 107 são capazes de comunicarem entre si direta ou indiretamente. Ao comunicar indiretamente, um ou mais outros nós 102, 106 ou 107, pode operar como um roteador ou roteadores para remeter ou retransmitir pacotes sendo enviados entre nós.

Serviços de associação de segurança de malha eficientes são utilizados para estabelecer segurança de enlace entre dois Pontos de malha (MPs) 102 em uma rede de malha sem fio 100. Serviços de EMSA são fornecidos através do uso de uma hierarquia de malha sem fio, uma hierarquia de chaves derivadas que é estabelecida através do uso de

uma Chave pré-compartilhada (PSK) ou quando um MP executa autenticação IEEE 802.1X utilizando um método de autenticação de protocolo de autenticação extensível (EAP).

A presente invenção inclui um mecanismo de autenticação que suporta o estabelecimento eficiente de associações de segurança entre MPs. Esse mecanismo pode operar em papéis de suplicante de malha ou autenticador de malha, dependendo das capacidades e preferências do MP e capacidades e preferências de seus vizinhos. Um autenticador de malha é um ponto de malha que provê autenticação antes de permitir que outro ponto de malha tenha acesso à rede. Em uma modalidade exemplar da presente invenção, o autenticador de malha é um autenticador 802.1X. Um suplicante de malha é um ponto de malha que solicita acesso à rede. Faz isso por associação a, e então autenticação de si próprio, um autenticador. Em uma modalidade exemplar da presente invenção, o suplicante de malha é um suplicante 802.1X.

Ao operar no papel de autenticador de malha, um ponto de malha pode permitir que pontos de malha de suplicante unam uma de malha e estabeleçam associações de segurança a si próprio e a outros membros da rede. Durante um estabelecimento de comunicações EMSA, um MP desempenhará o papel de Suplicante 802.1X, e o outro desempenhará o papel de Autenticador 802.1X. A presente invenção inclui ainda um procedimento de determinação de papel 802.1X para determinar durante um estabelecimento de comunicações de EMSA quais papéis são atribuídos a todos os MP. Esse procedimento permite que o papel de autenticador de malha e suplicante de malha sejam exclusivamente atribuídos a um

único MP antes da conclusão do estabelecimento de comunicações de EMSA.

A figura 2 ilustra um diagrama de fluxo de mensagem 200, de acordo com algumas modalidades da presente invenção. Especificamente, a figura 2 ilustra estabelecimento de enlace não-hierárquico utilizando o estabelecimento de comunicações EMSA abreviado entre dois pontos de malha 102-1, 102-2 na rede 100. Um MP que inicia o estabelecimento de comunicações EMSA abreviado envia uma mensagem aberta de enlace não-hierárquico 205 que contém um elemento de informação de Associação de Segurança de malha (MSAIE), um elemento de informação de Capacidade de Segurança de malha (MSCIE) e um elemento de informação de rede de segurança robusto (RSNIE), onde o RSNIE contém uma lista de identificação Chave Mestre em pares (PMKID). A lista PMKID contém um ou duas entradas que identificam a Chave ou Chaves Mestre em pares de Autenticador de malha compartilhado (PMK-MA) disponíveis para assegurar o enlace não-hierárquico. A mensagem Abertura de enlace Não-hierárquico solicita que um enlace seja estabelecido entre o remetente e o receptor de Abertura de Enlace Não-hierárquico. No estabelecimento de comunicações EMSA abreviado que inclui a mensagem de configuração de enlace não-hierárquico 210 e mensagem de resposta de enlace não-hierárquico 215 da presente invenção, a determinação de papéis depende das informações permutadas na(s) mensagem(ns) de abertura de enlace não-hierárquico 205. O estabelecimento de comunicações EMSA abreviado permite que um MP estabeleça uma chave transiente em pares (PTK) com um autenticador de malha, utilizando a hierarquia de chave de

malha que estabeleceu durante Autenticação EMSA inicial.

A figura 3 ilustra mais detalhe da operação de pontos de malha 102-1 e 102-2 durante um estabelecimento de enlace não-hierárquico 300. Como ilustrado, a operação inicia com o bloco 305 no qual o ponto de malha 102-1 determina que um enlace não-hierárquico deve ser configurado. Pode ocorrer após receber um sinalizador, por exemplo. Nesse ponto um comando de Abertura Ativa é emitido para iniciar configuração de enlace não-hierárquico. A seguir, no bloco 310, o ponto de malha 102-1 seleciona um número utilizado uma vez e série de códigos e identifica chaves mestre disponíveis. Mais especificamente, no bloco 310, após receber uma Abertura ativa, o MP 102-1: (a) seleciona um número utilizado uma vez (campo de Número utilizado uma vez local de MSAIE); (b) seleciona 1 série de códigos em pares do qual o não-hierárquico suporta (MSAIE); (c) determina se a função de Autenticador de malha local (MA) tem um PMK de autenticador de malha armazenado em cache (PMK-MA) criado por não-hierárquico; e caso positivo, insere PMK distribuidor de chave de malha (PMK-MKD)Name identificando uma chave da qual o PMK-MA cache é derivado no RSNIE (Lista PMKID); (d) insere o PMK-MKDName identificando uma chave criada por esse MP durante Autenticação de EMSA inicial no RSNIE (Lista PMKID) (Observação: A lista PMKID tem 1 ou 2 entradas); e (e) constroi uma mensagem de abertura de enlace não-hierárquico contendo: MSCIE, MSAIE, & RSNIE. O ponto de malha 102-1 então envia uma mensagem de abertura de enlace não-hierárquico 205 para o ponto de malha 102-2.

A seguir, no bloco 315, o ponto de malha 102-2, após receber a mensagem de abertura de enlace não-hierárquico

205: (a) examina RSNIE e MSCIE, e determina se deseja configurar um enlace com o par não-hierárquico 102-1; caso negativo, o ponto de malha 102-2 envia uma mensagem de fechar enlace não-hierárquico (não mostarda); (b) faz um procedimento de determinação de papel 802.1X (a ser descrito posteriormente), isso determina o PMK-MA a ser utilizado; (c) recupera o PMK-MA se necessário e se atua no papel de autenticador 802.1X; e (d) seleciona um número utilizado uma vez e computa o PTK.

A seguir, no bloco 320, o ponto de malha 102-2 identifica a chave usada. Após determinação de papel 802.1X e computação de PTK, o ponto de malha 102-1: (a) constrói seu RSNIE incluindo o PMK-MAName no campo de lista PMKID; (b) constrói o MSAIE contendo: ambos os números utilizado uma vez, o identificador do autenticador 802.1X, a seleção de série (suplicante escolhe) (observação: se o suplicante faz a escolha com base na capacidade de rede não-hierárquica; se autenticador, ecoa a escolha da rede não-hierárquica a partir da mensagem de abertura de enlace não-hierárquico), a chave temporal de grupo criptografada (GTK), o PMK-MKDName identificando o PMK-MKD do qual o PMK-MA é derivado, e o código de integridade de mensagem (MIC) sobre vários elementos de informação (IEx). O ponto de malha 102-2 envia uma mensagem de configuração de enlace não-hierárquico 210 contendo: MSCIE, RSNIE e MSAIE parar o ponto de malha 102-1. A mensagem de configuração de enlace não-hierárquico 210 é protegida utilizando o MIC.

A seguir, no bloco 325, quando o ponto de malha 102-1 recebe a mensagem de configuração de enlace não-hierárquico 210, o ponto de malha 102-1 verifica o papel 802.1X

utilizando o procedimento de determinação de papel 802.1X, computa o PTK, e verifica o MIC e conteúdo de mensagem. Após receber a mensagem de configuração de enlace não-hierárquico 210, o ponto de malha 102-1: (a) se autenticador 802.1X e se necessário, recupera o PMK-MA utilizando o PMK-MKDName incluído; (b) computa o PTK utilizando os números utilizados uma vez e o PMK-MA; (c) verifica o MIC; (d) verifica se a seleção de série de códigos é suportada e se foi selecionada pelo suplicante 802.1X; e (f) decriptografa o GTK. Se algum componente não for verificado, então o ponto de malha 102-1 envia uma mensagem fechar enlace não-hierárquico (não mostrada). A mensagem Fechar enlace não-hierárquico tenta fechar a conexão entre os dois MPs.

De outro modo, a seguir, no bloco 330, o ponto de malha 102-1 constroi e envia de volta uma mensagem de resposta de enlace não-hierárquico 215 similar à mensagem de configuração de enlace não-hierárquico 210 e abre uma porta para comunicação com o ponto de malha 102-2. Especificamente, após verificar a mensagem de configuração de enlace não-hierárquico 210, o ponto de malha 102-1: (a) constroi seu RSNIE incluindo o PMK-MAName no campo de lista PMKID; (b) constroi o MSAIE contendo: ambos os números utilizados uma vez, o identificador do autenticador 802.1X, a seleção de série de códigos do suplicante, o GTK criptografado, o PMK-MKDName identificando o PMK-MKD do qual o PMK-MA é derivado, e o MIC através de vários IEs. O ponto de malha 102-1 envia uma resposta de enlace não-hierárquico 215 que contém: MSCIE, RSNIE e MSAIE. O ponto de malha 102-1 também instala PTK e GTK. O ponto de malha

102-1 então abre uma porta 802.1X para comunicação com o ponto de malha 102-2.

Para concluir o estabelecimento, no bloco 335, após receber a resposta de enlace não-hierárquico 215, o ponto de malha 102-2 verifica o MIC, verifica se o RSNIE e o MSCIE casam aqueles anteriormente recebidos (na mensagem de abertura de enlace não-hierárquico 205), verifica se as seleções de série de códigos/autenticação e gerenciamento de chave (AKM) são suportadas e são aquelas selecionadas pelo suplicante 802.1X, e decriptografa o GTK. Se algum componente não for verificado, o ponto de malha 102-2 envia uma mensagem fechar enlace não-hierárquico (não mostrado). O ponto de malha 102-2 então instala PTK e GTK. O ponto de malha 102-1 então abre uma porta 802.1X para comunicação com rede não-hierárquica 102-1. Em uma modalidade (não mostrada), o ponto de malha 102-2 pode enviar uma mensagem de confirmação de enlace não-hierárquico adicional para o ponto de malha 102-1 após receber uma mensagem de resposta de enlace não-hierárquico 215 e verificar o conteúdo. Uma pessoa com conhecimentos comuns na técnica reconhece que a presença ou ausência de tal mensagem de confirmação não altera o escopo da presente invenção.

O processo de estabelecimento de comunicações descrito com relação às figuras 2 e 3 provê um procedimento de determinação de papel 802.1X exclusivo. O estabelecimento de comunicações permite uso de chaves caches em todos os cenários. O estabelecimento de comunicações utiliza hierarquia de chave derivada de EMSA no local. O estabelecimento de comunicações provê opções de partida de protocolo flexível.

A figura 4 é um fluxograma que ilustra uma operação de exemplo de um ponto de malha 102 de acordo com algumas modalidades da presente invenção. Especificamente, a figura 4 ilustra um cenário de abertura ativa 400 no qual um ponto de malha 102 envia uma mensagem de abertura de enlace não-hierárquico para estabelecer ativamente um enlace com um par não-hierárquico.

Como ilustrado na figura 4, a operação 400 começa com a Etapa 405 com um comando de Abertura ativa para o A vizinho. A seguir, na etapa 410, o ponto de malha envia uma mensagem de abertura de enlace não-hierárquico contendo MSAIE e RSNIE para o A vizinho. Então, na etapa 415, o ponto de malha espera receber uma mensagem do A vizinho. Em uma modalidade (não mostrada) um processo de tempo de espera é incluído para assegurar a robustez do processo. Após o MP ter enviado uma mensagem de Abertura de Enlace não-hierárquico, porém não recebeu uma mensagem de configuração de Enlace não-hierárquico correspondente, MessageTimer, é definido. Se o MP não recebeu a configuração de Enlace não-hierárquico quando o temporizador termina, o MP envia uma mensagem de Fechar Enlace não-hierárquico para fechar o enlace. (não mostrado).

O MP vizinho pode rejeitar a mensagem Fechar Enlace não-hierárquico se contiver um identificador de ocorrência descasado. O identificador de ocorrência recebido é considerado um descasamento em três casos. No caso um, o MP ainda não tem um identificador de registro de ocorrência para o MP de rede não-hierárquica. No caso dois, a mensagem contém o valor aleatório no campo de ID de Enlace Local,

porém não casa com o PeerLinkID registrado localmente. No caso três, o valor no campo ID de Enlace não-hierárquico (se não for nulo) não casa com o registro local de LocalLinkID. No resto dos casos, o identificador de ocorrência é considerado um casamento, e o MP aceita a mensagem. Ao fazer isso, o MP registra o ID de enlace a partir do MP não-hierárquico.

A seguir, na etapa 420, o ponto de malha determina se uma mensagem recebida é uma mensagem de abertura de enlace não-hierárquico. Quando a mensagem é uma mensagem de abertura de enlace não-hierárquico, a operação continua com a Etapa 425 na qual o ponto de malha processa a mensagem incluindo verificar o conteúdo de mensagem. Em uma modalidade, o ponto de malha também faz a determinação de papel 802.1X. Em algumas modalidades, o MP rejeita a mensagem de Abertura de Enlace não-hierárquico se contiver um identificador de ocorrência descasado ou os parâmetros de configuração na mensagem recebida não forem aceitáveis pelo MP. O identificador de ocorrência contido na Abertura de Enlace não-hierárquico contém somente o ID de enlace fornecido pela rede não-hierárquica. É considerado um descasamento quando o MP tem o registro local do PeerLinkID e não casa com o valor recebido no campo ID de Enlace Local. Além do identificador de ocorrência, a mensagem de Abertura de Enlace não-hierárquico contém parâmetros de configuração. O MP pode rejeitar a mensagem se esses parâmetros não casarem com a configuração local e programa. Em outras modalidades, o MP aceita a mensagem e registra as configurações recebidas que são úteis para operações após o enlace ter sido estabelecido. O ponto de malha pode

armazenar também o valor recebido no campo ID de Enlace Local como PeerLinkId se o ponto de malha não tiver ainda um registro.

A seguir, na etapa 430, o ponto de malha deriva PTK.

5 Então, na etapa 435, o ponto de malha envia uma mensagem de confirmação de enlace não-hierárquico protegido utilizando o PTK. A seguir, na etapa 440, o ponto de malha espera por uma mensagem de confirmação de enlace não-hierárquico a partir do A vizinho (isto é, par não-hierárquico). Em uma
10 modalidade (não mostrada) um processo de tempo de espera é incluído. Após o MP ter enviado uma mensagem de Confirmação de Enlace não-hierárquico, porém não receber uma mensagem de Confirmação de Enlace não-hierárquico correspondente, um temporizador, MessageTimer, é definido. Se o MP não recebeu
15 a Confirmação de Enlace não-hierárquico quando o temporizador expira, o MP enviará uma mensagem Fechar Enlace não-hierárquico para fechar o enlace. (não mostrado).

A seguir, na etapa 445, o ponto de malha determina se
20 o MIC e conteúdo da mensagem de confirmação de enlace não-hierárquico são válidos. Caso negativo, a operação cicla de volta para a Etapa 440. O MP pode rejeitar a mensagem de Confirmação de Enlace não-hierárquico se contiver um identificador de ocorrência descasado ou os parâmetros de
25 configuração na mensagem recebida não forem aceitáveis pelo MP. É considerado um descasamento do identificador de ocorrência se o valor no campo ID de Enlace não-hierárquico da mensagem recebida não casar com o LocalLinkId registrado localmente, ou o valor no campo ID de Enlace Local da
30 mensagem recebida não casar com o PeerLinkId registrado

localmente (se o MP tiver um registro local de PeerLinkID). Além do identificador de ocorrência, a mensagem de Confirmação de Enlace não-hierárquico contém também parâmetros de configuração. O MP pode rejeitar a mensagem se os parâmetros recebidos não casarem com a configuração local e programa, ou se não forem compatíveis com os parâmetros recebidos em uma mensagem anterior.

Se o MIC e conteúdo forem válidos, a operação continua para a etapa 450 na qual o ponto de malha instala PTK e GTK; e abre uma porta para comunicação com o A vizinho. A operação então termina.

Voltando para a etapa 420, quando a mensagem não é uma mensagem de abertura de enlace não-hierárquico, a operação continua para a etapa 455 na qual o ponto de malha determina se a mensagem é uma mensagem de configuração de enlace não-hierárquico. Se a mensagem não for uma mensagem de configuração de enlace não-hierárquico, a operação retorna à etapa 415. Se a mensagem for uma mensagem de configuração de enlace não-hierárquico, a operação continua para a etapa 460 na qual o ponto de malha deriva PTK, se necessário. A seguir, na etapa 465, o ponto de malha determina se o MIC e conteúdo da mensagem de configuração de enlace não-hierárquico são válidos. Se não forem válidos, a operação cicla de volta para a etapa 415. Se válidos, a operação continua para a etapa 470 na qual o ponto de malha envia uma mensagem de respostas de enlace não-hierárquico protegida pelo PTK. A seguir, na etapa 450, o ponto de malha instala PTK e GTK e abre uma porta para comunicação com o A vizinho. A operação então termina.

A figura 5 é um fluxograma que ilustra uma operação de

exemplo de um ponto de malha 102 de acordo com algumas modalidades da presente invenção. Especificamente, a figura 5 ilustra um cenário de abertura passiva 500 no qual um ponto de malha 102 ouve uma mensagem de abertura de enlace não-hierárquico, e responde para configurar um enlace.

Como ilustrado na figura 5, a operação 500 começa com a etapa 505 na qual o ponto de malha recebe uma mensagem de abertura de enlace não-hierárquico a partir do A vizinho. A seguir, na etapa 510, o ponto de malha processa a mensagem de abertura de enlace não-hierárquico incluindo verificar seu conteúdo. Em algumas modalidades, o ponto de malha também faz a determinação do papel 802.1X. A seguir, na etapa 515, o ponto de malha seleciona um número utilizado uma vez local e deriva PTK. A seguir, na etapa 520, o ponto de malha envia uma mensagem de configuração de enlace não-hierárquico protegida utilizando o PTK. A seguir, na etapa 525, o ponto de malha espera uma mensagem de resposta de enlace não-hierárquico a partir do A vizinho (isto é, par não-hierárquico). Em uma modalidade (não mostrada) um processo de tempo de espera é incluído para assegurar a robustez do processo. Após o MP enviar uma mensagem de configuração de Enlace não-hierárquico, porém não receber uma mensagem de Resposta de Enlace não-hierárquico correspondente, um temporizador, MessageTimer, é definido. Se o MP não recebeu a Resposta de Enlace não-hierárquico quando o temporizador termina, o MP enviará uma mensagem Fechar Enlace não-hierárquico para fechar o enlace. (não mostrado).

A seguir, na etapa 530, o ponto de malha verifica o MIC e outro conteúdo de mensagem de uma mensagem de

resposta de enlace não-hierárquico recebida. A seguir, na etapa 535, é determinado se o conteúdo foi ou não verificado. Quando o conteúdo não é verificado, a operação cicla de volta para a etapa 525. Quando o conteúdo é verificado, a operação continua para a etapa 540 na qual o ponto de malha instala PTK e GTK e abre uma porta para comunicação com o A vizinho. A operação então termina.

De acordo com algumas modalidades da presente invenção, nas operações das figuras 4 e 5, quando o processamento de mensagem encontra qualquer erro ou o MP toma a decisão local de fechar o enlace, o MP envia uma mensagem Fechar Enlace não-hierárquico para fechar o enlace. O MP espera algum tempo para fechar o enlace totalmente. Esse período de tempo atrativo pode ser governado por um temporizador - CancelTimer. Antes de o CancelTimer expirar, o MP continua a responder a qualquer mensagem de Abertura de Enlace não-hierárquico adicional a partir do MP não-hierárquico por enviar de volta a mensagem Fechar Enlace não-hierárquico. Quando o CancelTimer expirar, o MP eventualmente fecha o enlace liberando o recurso local alocado para a ocorrência de enlace. Esse mecanismo permite que o processo recupere rapidamente da falha.

A figura 6 é um fluxograma que ilustra uma operação de exemplo 600 de um ponto de malha 102, de acordo com algumas modalidades da presente invenção. Especificamente, a figura 6 ilustra um procedimento de determinação de papel 802.1X 600 em um ponto de malha de acordo com algumas modalidades da presente invenção. A operação 600 da figura 6 pode ser incluída, por exemplo, como detalhe adicional das etapas

315 e 325 da figura 3, etapa 425 da figura 4, e etapa 510 da figura 5, conforme anteriormente aqui descrito. A determinação de papel 802.1X atribui os papéis de autenticador 802.1X e suplicante 802.1X para os MPs, baseado na presença de chaves armazenadas em cache e a configuração dos MPs. Também determina o PMK-MA a ser utilizado para assegurar o enlace.

Como ilustrado na figura 6, a operação 600 começa com a etapa 605 na qual o ponto de malha determina se pelo menos um ponto de malha pode ser um autenticador de malha (MA) (isto é, um bit de autenticador de malha é definido). Se nenhum ponto de malha pode ser um autenticador de malha, a operação continua até a etapa 610 na qual o ponto de malha envia uma mensagem de fechar enlace não-hierárquico. A operação então termina.

Quando pelo menos um autenticador de malha é identificado na etapa 605, a operação continua para a etapa 615 na qual o ponto de malha determina se o PMKID local é válido. Para determinar se o PMKID local é válido, o ponto de malha examina a LIsta de PMKID recebida a partir de um MP não-hierárquico em uma mensagem de abertura de enlace não-hierárquico. Se a LIsta PMKID contiver duas entradas, e uma entrada corresponde a um PMK-MA que foi criado pelo ponto de malha durante Autenticação de EMSA inicial, então o PMKID local é válido. Quando o PMKID local não é válido, ou quando a LIsta de PMKID recebida a partir de um MP não-hierárquico contém somente uma única entrada, a operação continua até a etapa 620 na qual o ponto de malha determina se existe uma chave não-hierárquica armazenada em cache. Para determinar se uma chave não-hierárquica armazenada em

cache existe, o ponto de malha examina a Lista PMKID a partir de um MP não-hierárquico em uma mensagem de abertura de enlace não-hierárquico. Se a entrada que corresponde a um PMK-MA que foi criada pelo MP não-hierárquico durante sua Autenticação de EMSA inicial identificar uma chave que é localmente armazenada em cache no ponto de malha, então a chave não-hierárquica armazenada em cache existe. Quando uma chave não-hierárquica armazenada em cache existe, a operação continua até a etapa 625 na qual o ponto de malha de processamento é identificado como o autenticador 802.1X. A operação então termina.

Voltando à etapa 615, quando o PMKID local é válido, a operação continua até a etapa 630 na qual o ponto de malha determina se uma chave não-hierárquica armazenada em cache existe. Quando nenhuma chave não-hierárquica armazenada em cache existe, a operação continua até a etapa 635 na qual o MP não-hierárquico é identificado como o autenticador 802.1X. A operação então termina.

Voltando para a etapa 620, quando nenhuma chave não-hierárquica armazenada em cache existe, a operação continua até a etapa 640 na qual o ponto de malha determina se o par não-hierárquico é conectado a um MKD. Quando o par não-hierárquico é conectado ao MKD, a operação continua até a etapa 645 na qual o ponto de malha determina se é conectado ao MKD. Quando o ponto de malha também é conectado ao MKD, a operação continua até a etapa 650 na qual o ponto de malha compara o Controle de Acesso de mídia não-hierárquica (MAC) com seu MAC local. Quando o MAC não-hierárquico é menor do que o MAC local, a operação continua com a etapa 655 na qual o ponto de malha de processamento é

identificado como o autenticador 802.1X. Alternativamente, quando o MAC não-hierárquico é maior do que o MAC local, a operação continua com a etapa 660 na qual o ponto de malha não-hierárquico é identificado como o autenticador 802.1X.

5 Após as duas etapas 655 e 660, a operação termina.

Voltando à etapa 645, quando o ponto de malha de processamento não é conectado ao MKD, a operação continua até a etapa 665 na qual o ponto de malha não-hierárquico é identificado como o autenticador 802.1X. A operação então
10 termina.

Voltando à etapa 640, quando o par não-hierárquico não é conectado ao MKD, a operação continua até a etapa 670 na qual é determinado se o ponto de malha de processamento é conectado ao MKD. Quando o ponto de malha de processamento
15 é conectado ao MKD, a operação continua até a etapa 680 na qual o ponto de malha de processamento é identificado como o autenticador 802.1X. A operação então termina.

Quando, na etapa 670, o ponto de malha de processamento não é conectado ao MKD, a operação continua
20 até a etapa 610 na qual o ponto de malha envia uma mensagem de Fechar enlace não-hierárquico. A operação então termina.

A presente invenção, como descrito aqui, provê um método em uma rede de malha ad hoc para dois dispositivos para determinar rapidamente papéis (isto é, que é o
25 autenticador e que é o suplicante) enquanto estabelecem uma associação de segurança. A invenção provê a inclusão de informações de chave armazenada em cache no processo de determinação de papel e a aplicação de determinação de papel em um estabelecimento de comunicações de três
30 sentidos encurtado.

No relatório descritivo acima, modalidades específicas da presente invenção foram descritas. Entretanto, uma pessoa com conhecimentos comuns na técnica reconhece que várias modificações e alterações podem ser feitas sem se afastar do escopo da presente invenção. Por conseguinte, o relatório descritivo e figuras devem ser considerados em um sentido ilustrativo em vez de restritivo, e todas essas modificações pretendem ser incluídas no escopo da presente invenção.

REIVINDICAÇÕES

1. Método de operação de um ponto de malha para estabelecer associações seguras em uma rede de comunicação, compreendendo:

5 enviar uma mensagem de abertura de enlace não-hierárquico para um nó vizinho;

receber uma mensagem de resposta a partir do nó vizinho em resposta à mensagem de abertura de enlace não-hierárquico;

10 caracterizado por:

processar a mensagem de resposta utilizando uma primeira operação quando a mensagem de resposta é uma mensagem de abertura de enlace não-hierárquico;

15 processar a mensagem de resposta utilizando uma segunda operação quando a mensagem de resposta é uma mensagem de configuração de enlace não-hierárquico;

instalar uma chave transiente em partes (PTK) e uma chave temporal de grupo criptografado (GTK) como resultado da primeira operação ou da segunda operação; e

20 abrir uma porta para comunicação com o nó vizinho.

2. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que a mensagem de abertura de enlace não-hierárquico inclui um elemento de informação de associação de segurança de malha (MSAIE) e um elemento de
25 informação de rede de segurança robusto (RSNIE).

3. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que a primeira operação compreende:

30 processar a mensagem de resposta incluindo verificar o conteúdo de mensagem de resposta;

derivar o PTK;

enviar uma mensagem de confirmação de enlace não-hierárquico protegida utilizando o PTK;

receber uma mensagem de confirmação de enlace não-hierárquico de nó A vizinho partir do nó vizinho;

determinar se o código de integridade de mensagem (MIC) e o conteúdo da mensagem de confirmação de enlace não-hierárquico de nó vizinho são válidos; e

continuar a instalação de PTK e etapa GTK quando o código de integridade de mensagem (MIC) e o conteúdo da mensagem de confirmação de enlace não-hierárquico são válidos.

4. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que a segunda operação compreende:

derivar o PTK quando necessário;

determinar se o código de integridade de mensagem (MIC) e o conteúdo da mensagem de configuração de enlace não-hierárquico são válidos; e

quando o MIC e conteúdo da mensagem de configuração de enlace não-hierárquico são válidos:

enviar uma mensagem de resposta de enlace não-hierárquico protegida pelo PTK; e

continuar para a etapa de instalar PTK e GTK.

5. Método, de acordo com a reivindicação 1, caracterizado por compreender ainda antes da etapa de recepção:

esperar por receber a mensagem de resposta a partir do nó vizinho por um período de tempo; e

enviar uma mensagem de enlace não-hierárquico para

fechar o enlace quando nenhuma mensagem de resposta é recebida durante o período de tempo.

6. Método, de acordo com a reivindicação 3, caracterizado pelo fato de que a etapa de processamento
5 compreende ainda:

executar uma determinação de papel 802.1X incluindo:

atribuir um papel de um autenticador 802.1X e um papel de um suplicante 802.1X a cada um do ponto de malha e nó vizinho com base na presença de uma ou mais chaves
10 armazenadas em cache e uma configuração de cada um do ponto de malha e nó vizinho.

7. Método, de acordo com a reivindicação 6, caracterizado pelo fato de que a atribuição de um papel de um autenticador 802.1X e um papel de um suplicante 802.1X
15 para os pontos de malha com base na presença de uma ou mais chaves armazenadas em cache compreende:

atribuir o papel do autenticador 802.1X ao nó vizinho quando uma identificação local de Chave mestre em pares (PMKID) é válida e uma chave não-hierárquica não é
20 armazenada em cache; e

atribuir o papel do autenticador 802.1X ao ponto de malha quando o PMKID local não é válido e a chave não-hierárquica é armazenada em cache.

8. Método, de acordo com a reivindicação 7, caracterizado por compreender ainda:
25

determinar se o PMKID local é válido mediante:

examinar uma Lista de PMKID recebida a partir do nó vizinho em uma mensagem de abertura de enlace não-hierárquico; e

30 quando a Lista PMKID contém duas entradas, e uma

entrada corresponde a um PMK-MA que foi criado pelo ponto de malha durante Autenticação EMSA inicial, então o PMKID local é válido.

9. Método, de acordo com a reivindicação 7,
5 caracterizado pelo fato de que o ponto de malha determina se a chave não-hierárquica armazenada em cache existe por:

examinar uma Lista PMKID recebida a partir do nó vizinho em uma mensagem de abertura de enlace não-hierárquico; e

10 quando a entrada que corresponde a uma Chave Mestre em partes de Autenticador de malha (PMK-MA) que foi criada pelo nó vizinho durante sua autenticação de associação de segurança de malha eficiente, inicial, (EMSA) identifica uma chave que é localmente armazenada em cache no ponto de
15 malha, então a chave não-hierárquica armazenada em cache existe.

10. Método, de acordo com a reivindicação 6,
caracterizado pelo fato de que a atribuição de um papel de um autenticador 802.1X, e um papel de um suplicante 802.1X,
20 aos pontos de malha com base na configuração de cada um dos pontos de malha, compreende:

atribuir o papel de autenticador 802.1X ao ponto de malha quando o nó vizinho não é conectado a um distribuidor de chave de malha (MKD) e o ponto de malha é conectado ao
25 MKD;

atribuir o papel de autenticador 802.1X ao nó vizinho quando o nó vizinho é conectado ao MKD e o ponto de malha não é conectado ao MKD;

atribuir o papel de autenticador 802.1X ao ponto de
30 malha quando o nó vizinho e o ponto de malha são conectados

ao MKD e o MAC local é maior do que o MAC de nó vizinho; e atribuir o papel de autenticador 802.1X ao nó vizinho quando o nó vizinho e o ponto de malha são conectados ao MKD e o MAC local é menor do que o MAC do nó vizinho.

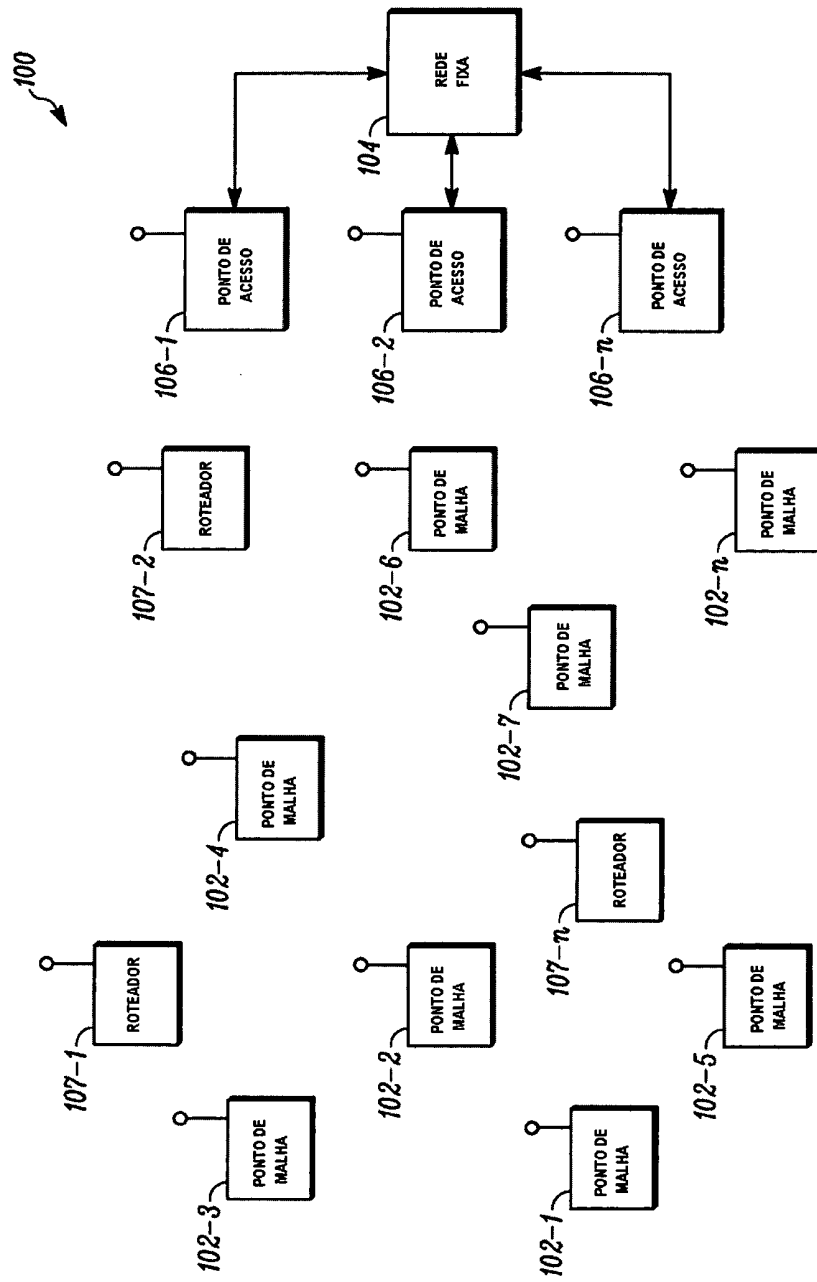
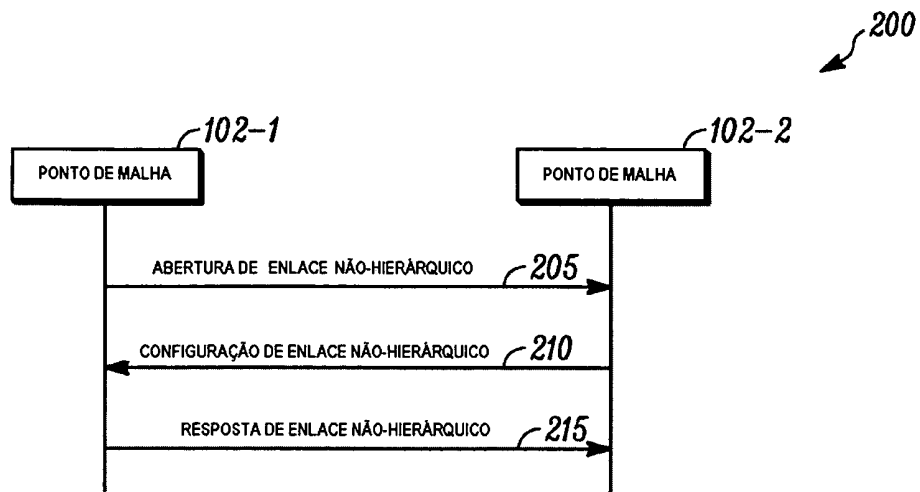


FIG. 1

*FIG. 2*

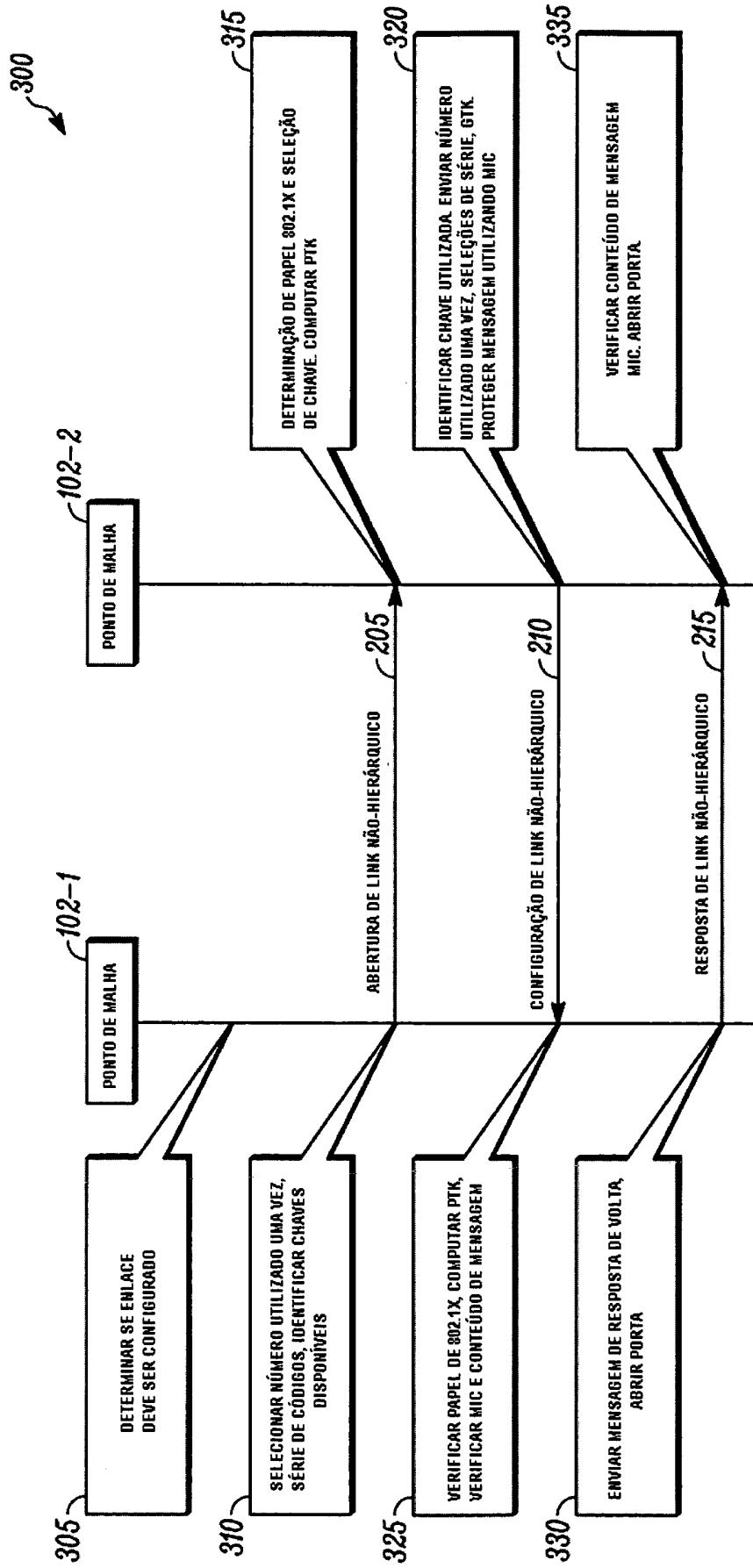
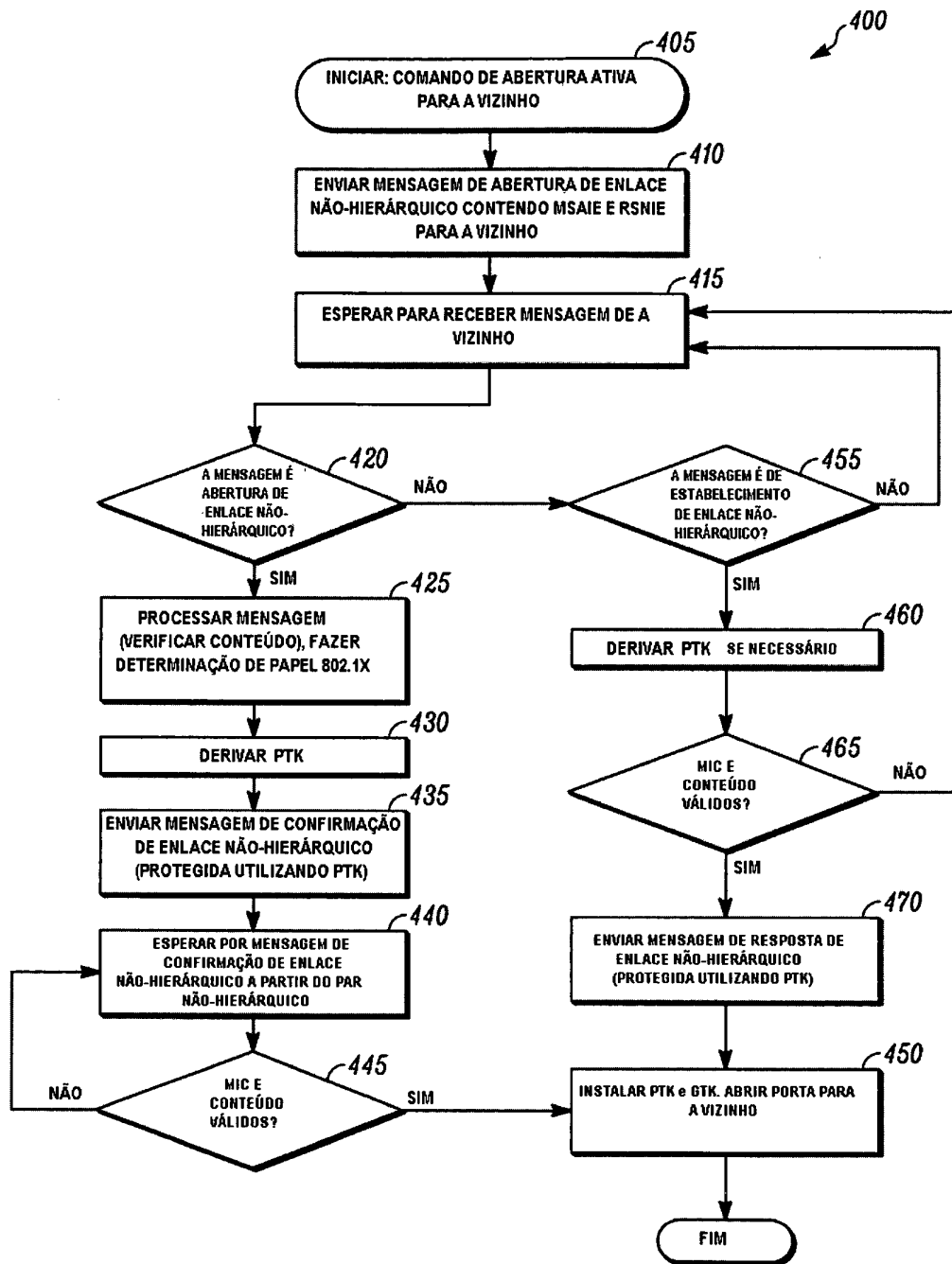


FIG. 3



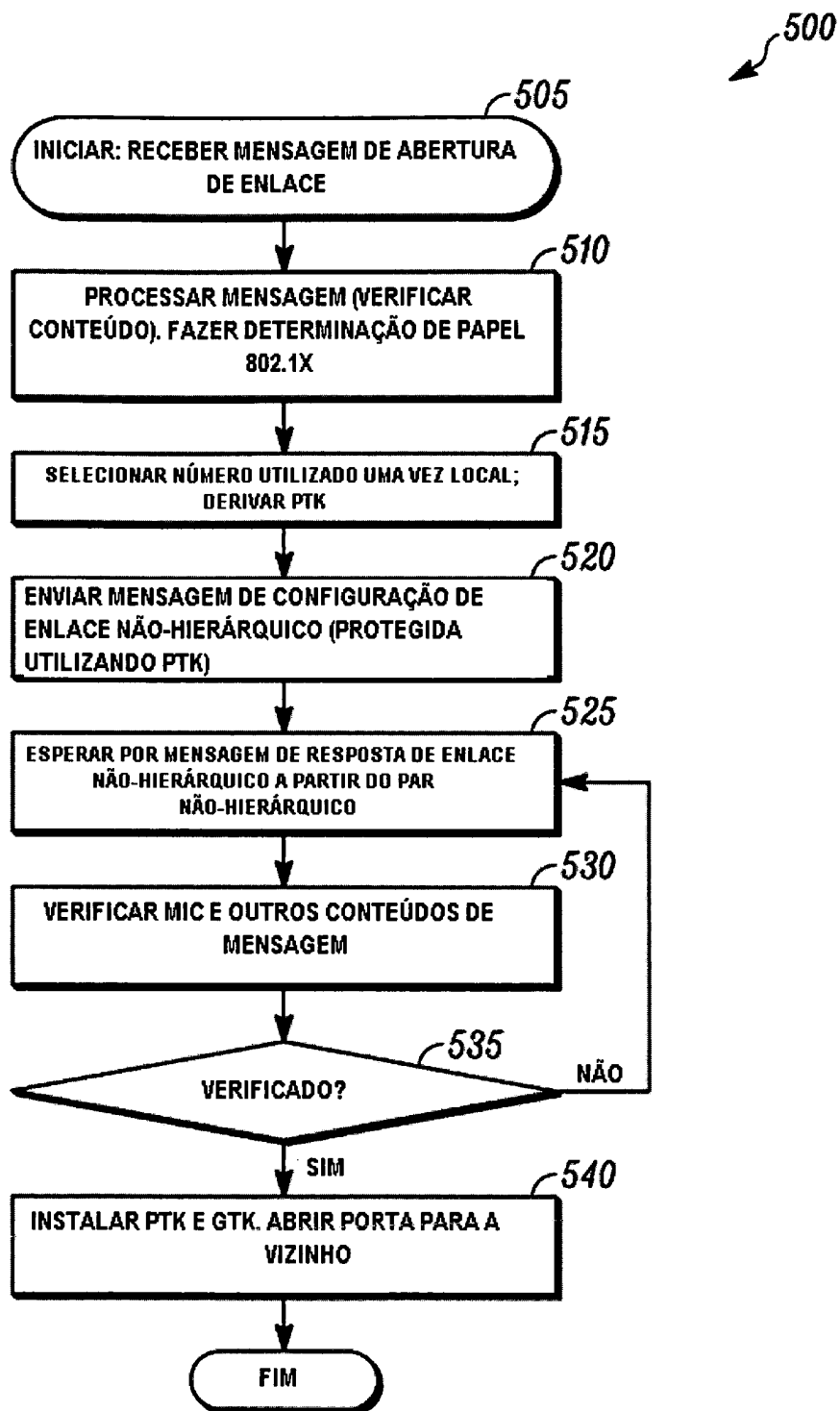


FIG. 5

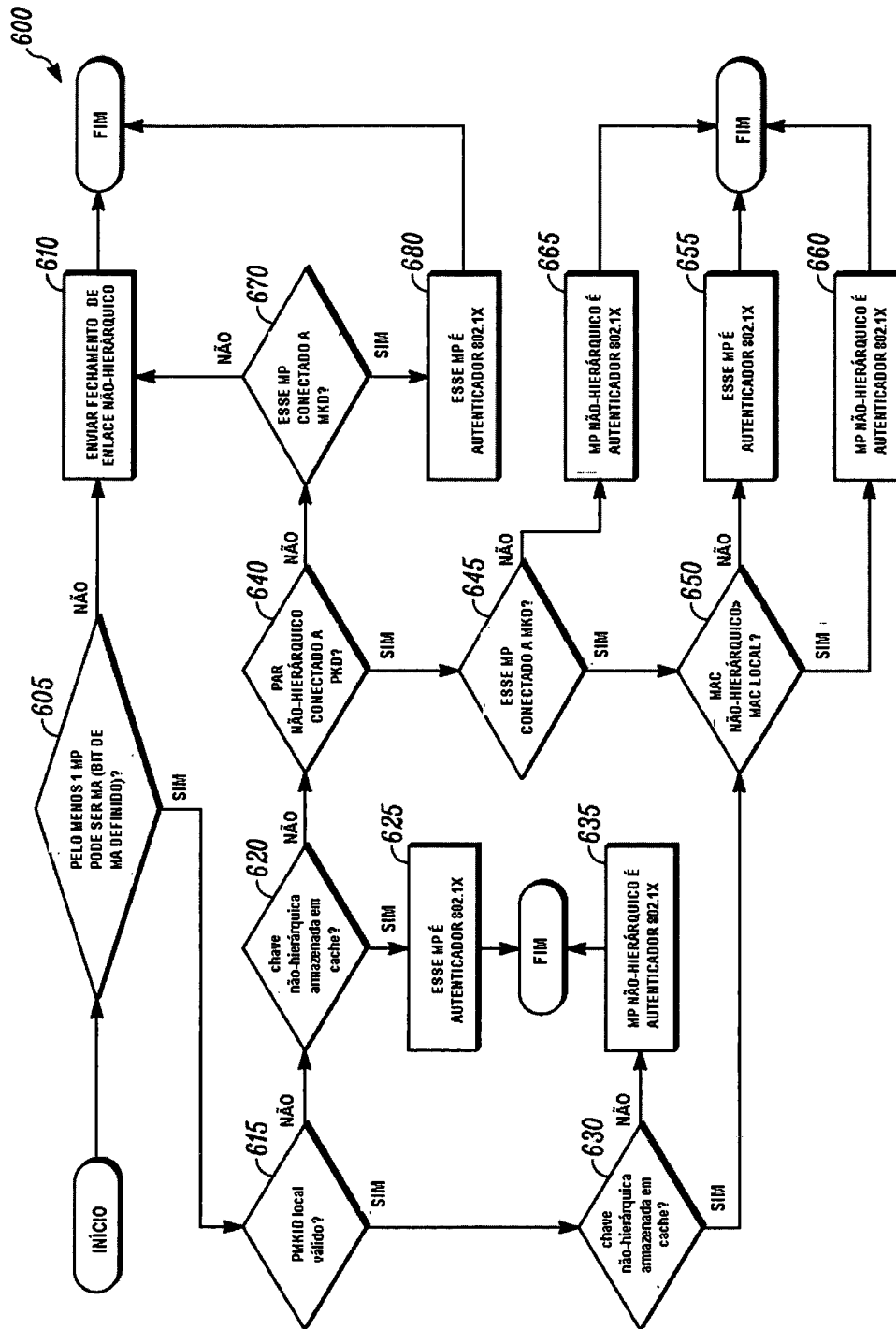


FIG. 6