

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

(21) **PI0609971-8 A2**

(22) Data de Depósito: 30/03/2006
(43) Data da Publicação: 11/10/2011
(RPI 2127)



(51) *Int.Cl.:*
H04L 9/32
H04L 9/08
H04L 12/28

(54) Título: MÉTODO PARA GERENCIAR ACESSO A UMA REDE SEM FIO, SISTEMA, UM OU MAIS MEIOS LEGÍVEIS POR COMPUTADOR, TERMINAL MÓVEL, DISPOSITIVO DE CONTROLE DE ACESSO, E, MÉTODO PARA UM DISPOSITIVO CONFIÁVEL GERENCIAR ACESSO A UMA REDE SEM FIO

(30) Prioridade Unionista: 29/06/2005 US 11/169328, 04/04/2005 US 60/667661, 22/04/2005 US 60/673806, 29/06/2005 US 11/169328

(73) Titular(es): NOKIA CORPORATION

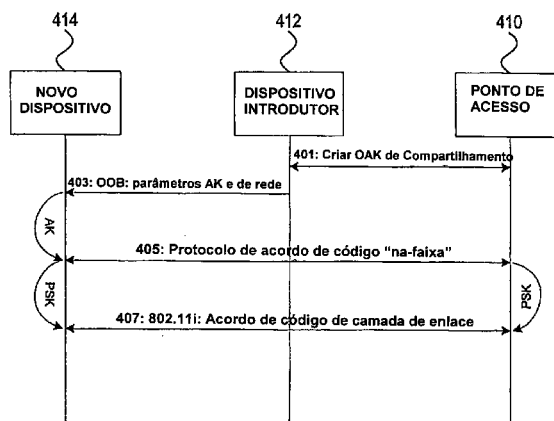
(72) Inventor(es): JAN-ERIK EKBERG, JARI TAKALA, KARI TI KOSTIAINEN, Nadarajah Asokan, PHILIP GINZBORG, SAMPO SOVIO, SEAMUS MOLONEY

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

(86) Pedido Internacional: PCT IB2006000695 de 30/03/2006

(87) Publicação Internacional: WO 2006/106393de 12/10/2006

(57) Resumo: MÉTODO PARA GERENCIAR ACESSO A UMA REDE SEM FIO, SISTEMA, UM OU MAIS MEIOS LEGÍVEIS POR COMPUTADOR, TERMINAL MÓVEL, DISPOSITIVO DE CONTROLE DE ACESSO, E, MÉTODO PARA UM DISPOSITIVO CONFIÁVEL GERENCIAR ACESSO A UMA REDE SEM FIO. São providos métodos e sistemas para gerenciar acesso a uma rede de área local sem fio. Um ponto de acesso sem fio (AP) pode usar uma abordagem unificada que utiliza um canal fora-da-banda para comunicar informação de chave de autenticação e endereço de rede a um dispositivo convidado, e utiliza um canal em-banda para estabelecer comunicações com o dispositivo convidado, e também provê suporte para configuração em-banda em todos os dispositivos. A capacidade de usar fora-da-banda onde possível provê um aumento de segurança e usabilidade, e a possibilidade de delegar acesso de um dispositivo para outro. A abordagem unificada deste modo provê também gerenciamento fácil de acesso de convidado à WLAN.



“MÉTODO PARA GERENCIAR ACESSO A UMA REDE SEM FIO, SISTEMA, UM OU MAIS MEIOS LEGÍVEIS POR COMPUTADOR, TERMINAL MÓVEL, DISPOSITIVO DE CONTROLE DE ACESSO, E, MÉTODO PARA UM DISPOSITIVO CONFIÁVEL GERENCIAR ACESSO A UMA REDE SEM FIO”

Este pedido reivindica prioridade para o Pedido U.S. provisório Ser. No. 60/667.661, depositado em 4 de Abril de 2005, intitulado “Easy, Flexible, and Secure Network Setup”, e Pedido U.S. provisório Ser. No. 60/673.806, depositado em 22 de Abril de 2005, intitulado “Secure, Easy and Flexible Network Setup”, cada um dos quais é aqui incorporado por referência.

CAMPO DA INVENÇÃO

A invenção relaciona-se em geral a computadores e redes de computadores. Mais especificamente, a invenção provê sistemas e métodos para a administração de redes sem fio, tal como um rede de área local sem fio (WLAN).

FUNDAMENTOS DA INVENÇÃO

Configurar uma rede sem fio doméstica, tal como uma rede de área local sem fio (WLAN), pode ser um processo muito difícil para a maioria dos usuários de computador, apresentando então um obstáculo significativo para a utilização eficiente das WLAN. Uma das dificuldades que os usuários encontram é determinar como melhor prover segurança de uma WLAN. Redes sem fio têm sido tipicamente protegidas por um único Código Pré Compartilhado (PSK). Entretanto, o uso de um único código secreto pré compartilhado requer que um usuário reconfigure a rede inteira, se o usuário deseja negar acesso futuro a um dispositivo que foi previamente autorizado para uso na WLAN. Embora o último padrão de LAN sem fio 802.11i (também conhecido como “WPA2”) suporta o uso de PSK múltiplos, alguns pontos de acesso (AP) não suportam o uso de PSK múltiplos. A

disponibilidade de PSK múltiplos habilita a revogação seletiva de associações de segurança, o que torna possível remover visitantes. 802.11i especifica a partir do PSK avançado, porém não especifica como os PSK são criados. Em adição, 802.11.i não especifica como agrupar os PSK ou como remover um PSK quando este não é mais necessário.

Outros protocolos 802.11.X especificam como os PMK (Códigos Mestre em Forma de Pares, que são similares aos PSK, exceto que um PMK é válido somente para uma única sessão). São criados usando um protocolo separado entre um dispositivo e um servidor de autenticação na rede. Entretanto, como o 802.11.i, o 802.11.X também não especifica como agrupar os PMK (remoção implícita no final da sessão).

Propostas existentes para resolver o problema de configuração de rede tentam explorar proximidade. Por exemplo, uma abordagem conhecida explora a proximidade física, usando um canal fisicamente seguro “fora-de-faixa” (OOB). O canal OOB pode ser baseado em NFC (Comunicação de Campo Próximo), infravermelho, *stick* de memória USB portátil ou qualquer outra tecnologia de comunicação que é baseada em proximidade física. OOB é usado para transferir o identificador de rede (por exemplo, um SSID) e um código compartilhado de um dispositivo para outro. Como o código transferido é usado diretamente como o PSK, não são necessários protocolos adicionais. Para adicionar um novo dispositivo à rede, a única interação de usuário necessária é tocar o novo dispositivo com uma “ficha”. A ficha pode ser um dispositivo de finalidade especial simples ou pode ser parte de um outro dispositivo, por exemplo, parte de um dispositivo de cliente WLAN que já esteja na rede. Figura 1 ilustra esta abordagem quando um “introdutor” admite um novo dispositivo na rede. Notar que o introdutor pode ser o próprio AP. Embora esta abordagem proveja interação de usuário intuitiva e permita delegação de acesso de um dispositivo para outro, o acesso de convidados permanece incômodo. Como o mesmo PSK é

usado por todos os dispositivos, a única maneira de remover acesso de convidados é remover todos os dispositivos da rede, e então adicionar dispositivos permitidos novamente, um por um.

5 Uma outra abordagem conhecida explora a proximidade do tempo usando configuração “na-faixa”. Uma proposta da *Broadcom* para Configuração Fácil Segura (SES) cai nesta categoria. Na SES, a configuração de rede é efetuada primeiramente colocando o AP em um modo de configuração, e então colocando o novo dispositivo em seu modo de configuração, por exemplo, pressionando uma tecla nos respectivos
10 dispositivos. Uma vez no modo de configuração, os dispositivos localizam um ao outro usando algum protocolo para acordo sobre um PSK. Figura 2 ilustra um exemplo de uma solução “na-faixa”. A disposição em pares do novo dispositivo e do AP na abordagem “na-faixa” é feita utilizando métodos de disposição em pares WLAN. Soluções “na-faixa” apresentam uma variedade
15 de problemas, incluindo a possibilidade de disposição em pares acidental com um dispositivo não pretendido e a ameaça de ataque “*man in the middle*” (porque o protocolo de acordo de código inicial não é autenticado). Em adição, o acesso de convidado é incômodo como no caso OOB, e nenhuma delegação de direitos de acesso de dispositivo a dispositivo é possível.

20 As abordagens OOB e “na-faixa” têm vantagens e desvantagens. A abordagem OOB é mais intuitiva e segura, mas devido ao hardware extra requerido, não é razoável esperar que todos os dispositivos terão canais “fora-de-faixa” adequados disponíveis. A abordagem “na-faixa” não permite a delegação de acesso e é menos segura, porém é menos
25 dispendiosa e é mais provável de começar a aparecer nos AP comerciais e dispositivos de cliente. Nenhuma das abordagens suporta gerenciamento de acesso de convidado fácil.

Então, seria um avanço na técnica prover métodos e sistemas que permitam configuração e administração de rede sem fio mais simples e

mais eficientes que superem as limitações e desvantagens acima.

BREVE SUMÁRIO DA INVENÇÃO

A seguir é apresentado um sumário simplificado da invenção, no sentido de prover um entendimento básico de alguns aspectos da invenção.

5 O sumário não é uma visão geral extensiva da invenção. Este não é destinado a identificar elementos chave ou críticos da invenção ou delinear o escopo da invenção. O sumário a seguir meramente representa alguns conceitos da invenção de uma forma simplificada como um prelúdio para a descrição mais detalhada provida abaixo.

10 Para superar limitações da técnica anterior descritas acima, e para superar outras limitações que serão aparentes pela leitura e entendimento da presente especificação, a presente invenção é direcionada a métodos e sistemas para gerenciar o acesso a uma rede de área local sem fio. Um ponto de acesso sem fio (AP) ou outro controlador de acesso pode usar uma
15 abordagem unificada que utiliza um canal “fora-de-faixa”, ou outro primeiro canal de comunicação, para comunicar código de autenticação e informação de endereço de rede a um dispositivo convidado, e utiliza um canal “na-faixa”, ou outro segundo canal de comunicação, para estabelecer comunicações com o dispositivo convidado, e também provê suporte para
20 configuração “na-faixa” em todos os dispositivos. A capacidade de usar “fora-de-faixa” onde possível, provê um aumento de segurança e usabilidade, e a possibilidade de delegar acesso de um dispositivo para outro. A abordagem unificada deste modo provê também gerenciamento fácil de acesso de convidado à WLAN.

25 De acordo com um primeiro aspecto da invenção, um método pode gerenciar acesso a um ponto de acesso sem fio (AP) ou outro controlador de acesso por um terminal móvel, onde o AP usa um canal de comunicação “fora-de-faixa” e um canal de comunicação “na-faixa”. Um código de autenticação (AK) correspondente ao terminal móvel é

estabelecido, e então enviado ao terminal móvel via canal “fora-de-faixa”. O AP recebe uma requisição de acordo de código do terminal móvel, via canal “na-faixa”, e estabelece um código de acesso correspondente ao terminal móvel, com base na requisição de acordo de código recebida, quando o terminal móvel é autorizado a acessar o AP. O AP autoriza o terminal móvel a se comunicar através do AP, na conclusão bem sucedida da etapa prévia. O AK é usado para autenticar o acordo de código.

De acordo com um outro aspecto da invenção, um método alternativo gerencia acesso a um ponto de acesso sem fio (AP) ou outro controlador de acesso por um terminal móvel, onde o AP usa um canal de comunicação “fora-de-faixa” e um canal de comunicação “na-faixa”. Um endereço do AP é enviado a um dispositivo mestre. Um código de autenticação de convidado (AK) correspondente ao terminal móvel é gerado, e informação correspondente é enviada ao terminal móvel a partir do dispositivo mestre. O terminal móvel envia um segundo AK ao AP, que compara o AK do convidado com o segundo AK. O AP concede acesso ao terminal móvel quando o segundo AK coincide com o AK do convidado.

De acordo com um outro aspecto da invenção, um novo terminal móvel pode ser adaptado para comunicação com a rede. O terminal móvel pode incluir um processador controlando a operação global do terminal móvel, um primeiro transceptor para enviar e receber comunicações através de um primeiro canal de comunicação, “na-faixa”, com um ponto de acesso sem fio (AP) ou outro controlador de acesso, e um receptor para receber comunicações através de um segundo canal de comunicação “fora-de-faixa” com o ponto de acesso sem fio (AP). O terminal móvel pode também incluir memória armazenando instruções executáveis por computador que, quando executadas pelo processador, fazem com que o terminal móvel execute um método para acessar uma rede de área local sem fio. O método pode executar etapas, recebendo um código de autenticação de convidado (AK) e um

endereço do AP sem fio via segundo canal de comunicação, e enviar o AK do convidado ao AP, via primeiro canal de comunicação, para estabelecer comunicações com o AP.

5 Aqueles especialistas na técnica verificarão que o acima é meramente uma introdução ao assunto descrito em mais detalhe abaixo.

BREVE DESCRIÇÃO DOS DESENHOS

10 Um entendimento mais completo da presente invenção e de certas vantagens desta, pode ser adquirido referindo-se à seguinte descrição, considerando os desenhos que a acompanham, nos quais números de referência iguais indicam características iguais, e onde:

Figura 1 ilustra um método “fora-de-faixa” da técnica anterior.

Figura 2 ilustra um método “na-faixa” da técnica anterior.

Figura 3 ilustra uma arquitetura de rede que pode ser usada de acordo com um ou mais aspectos ilustrativos da invenção.

15 Figura 4 ilustra um método unificado “fora-de-faixa”/“na-faixa” de acordo com um ou mais aspectos ilustrativos da invenção.

Figura 5 ilustra uma arquitetura de rede que pode ser usada de acordo com um ou mais aspectos ilustrativos da invenção.

Figura 6 ilustra um método de acordo com um protocolo SES.

20 DESCRIÇÃO DETALHADA DA INVENÇÃO

25 Na descrição seguinte das várias realizações ilustrativas, é feita referência aos desenhos anexos, que fazem parte desta, e que são mostrados por meio de ilustração de várias realizações de exemplo, nas quais a invenção pode ser praticada. Deve ser entendido que outras realizações podem ser utilizadas e modificações estruturais e funcionais podem ser feitas, sem se afastar do escopo da presente invenção.

Um ou mais aspectos da invenção podem ser usados no seguinte cenário ilustrativo. Com referência à Figura 3, em uma realização da invenção, um usuário adquire um novo ponto de acesso de LAN sem fio 301

de alta velocidade (ou outro controlador de acesso) e traz o dispositivo para sua casa. O usuário deseja conectar facilmente outros dispositivos sem fio 303, 305, 307, 309 ou 311, na residência, ao novo ponto de acesso 301, de tal modo que estes dispositivos possam usar a rede sem fio 302. Dispositivos sem fio são genericamente referidos aqui como terminais móveis, e podem incluir, porém não estão limitados a qualquer dispositivo com capacidades de comunicações sem fio, tais como telefones móveis, telefones inteligentes, aplicações domésticas, computadores *laptop*, computadores *desktop*, assistentes digitais pessoais, dispositivos de áudio/vídeo, televisões, “conversores set-top-box”, gravadores de vídeo pessoais, gravadores digitais pessoais, câmera digital, *camcorder* digital, dispositivo de memória pessoal, dispositivos de automação doméstica e/ou controle, sensores, veículos, e similares ou qualquer combinações destes.

Após conectar o ponto de acesso de LAN sem fio 301, o usuário conecta seu telefone móvel habilitado para o WLAN 309 ao novo ponto de acesso 301, simplesmente pressionando uma tecla em ambos os dispositivos (não mostrada). O AP 301 pode então ser colocado em uma prateleira ou outra localização apropriada, por exemplo, onde esteja fora de alcance de crianças ou outras fontes de dano ou ferimento. Para conectar um dos outros dispositivos domésticos sem fio à rede 302, tal como o estéreo doméstico 307, o usuário pode “tocar” aqueles dispositivos com o telefone móvel 309 ou (por pelo menos alguns dispositivos) pressionar uma tecla de configuração em ambos dispositivos 307 e AP 301 para conectá-los à rede 302. Mais tarde, se o vizinho do usuário comparece, o usuário pode gostar de exibir a rede 302 que adquiriu e permitir ao vizinho usar seu próprio telefone 311 para transferir alguma música para o estéreo doméstico 307. Isto pode ser obtido, por exemplo, tocando o telefone do vizinho 311 com o telefone do usuário 309. Quando o vizinho tiver visto o bastante e retornar a sua casa, o usuário pressiona uma tecla (não mostrada) no ponto de acesso 301, para

terminar a permissão temporária ao visitante que fora concedida ao vizinho, e assim o vizinho não pode mais controlar os dispositivos na residência do usuário. Alternativamente, o usuário pode usar seu telefone 309 para terminar a permissão temporária do visitante.

5 O cenário acima é ilustrativo para fins de descrever aspectos da invenção e não é limitante de modo algum. Conforme usado aqui, “tocar” se refere a uma interação baseada em proximidade entre dois dispositivos, onde a informação de configuração e/ou segurança é transferida ou autorizada de um dispositivo para o outro. No exemplo, “tocar” se refere a mover os
10 dispositivos fisicamente próximos um do outro, de tal modo que o canal OOB (NFC, comunicação sem fio de alcance curto, infravermelho, BlueTooth, UWB, Wi-Fi, RF ID, *stick* de memória USB, etc.) pode ser estabelecido e dados necessários trocados através do canal OOB. De acordo com um aspecto da invenção, uma abordagem unificada pode ser usada, a qual utiliza aspectos
15 de ambas abordagens OOB e “na-faixa”, permitindo deste modo suporte para a abordagem “na-faixa” em todos os dispositivos, mas também a capacidade de usar “fora-de-faixa” onde possível, para aumentar a segurança e usabilidade, e a possibilidade de delegar acesso de um dispositivo para outro. A abordagem unificada provê deste modo também fácil gerenciamento de
20 acesso de convidado à WLAN.

Figura 4 ilustra uma realização ilustrativa da invenção e um modo possível de obter esta unificação. Na etapa 401, o Ponto de Acesso 410 e Dispositivo Introdutor 412 criam e compartilham um código de autenticação original (OAK). O AP 410 e dispositivo 412 podem ser opcionalmente
25 porções do mesmo dispositivo. Na etapa 403, o dispositivo introdutor 412 provê a um novo dispositivo 414, via uma canal “fora-de-faixa”, o AK (onde $AK = f(OAK, AK-ID)$, conforme descrito adicionalmente aqui) e parâmetros de rede aplicáveis (por exemplo, endereço do AP, SSID). Usando o AK, na etapa 405, o novo dispositivo 414 e o ponto de acesso 410 usam um protocolo

de acordo de código para criar um código para o novo dispositivo. Finalmente, na etapa 407, o novo dispositivo 414 e o AP 410 executam procedimentos de código de camada de enlace, por exemplo, usando 802.11.i.

Conforme ilustrado na Figura 4, o PSK pode ser derivado de um protocolo de acordo de código “na-faixa”. Entretanto, se um canal “fora-de-faixa” está disponível, o canal OOB pode ser usado para transferir o código de autenticação (AK) e o endereço do AP 410 para o novo dispositivo 414, o que dispara o acordo de código “na-faixa” (isto é, o usuário não tem que pressionar qualquer tecla). O canal “fora-de-faixa” não está limitado a NFC, mas pode ser qualquer meio para passar o AK (e os parâmetros de rede, onde factível) ao Novo Dispositivo. O canal “fora-de-faixa” pode consistir de um Número de Identificação Pessoal (PIN) digitado pelo usuário.

O AP 410 pode ter dois tipos de “modos de recepção”. No primeiro modo de recepção “autenticado”, o AP 410 aceita requisições para acordos de código autenticados. O AK pode ser usado para autenticar o acordo de código, por padrão. Pressionando uma tecla no AP 410, o AP 410 pode ser colocado em um segundo modo de recepção “não autenticado”, por um tempo curto. O comportamento neste modo pode ser similar ao da abordagem Broadcom, descrita acima. A autenticação do acordo de código evita disposição em pares acidental e a possibilidade de ataques do tipo “*man-in-the-middle*”. Também, pode haver códigos de autenticação múltiplos (por exemplo, AK proprietário, AK familiar, AK convidado, etc.). Por exemplo, um AP pode ter três “fichas” cada uma contendo um código de autenticação diferente. O AP 410 pode categorizar associações de segurança baseadas em como foram autenticadas. Neste caso, uma operação de “remover todos os convidados” (por exemplo, um pressionamento longo da tecla) faz com que o AP 410 remova todas as associações de segurança feitas usando o código de autenticação de convidado ou nenhum código de autenticação. Quaisquer associações de segurança feitas usando outros códigos de autenticação,

entretanto, podem não ser removidas por esta operação. Isto permite gerenciamento efetivo e intuitivo de acesso de convidado.

Cada dispositivo pode ter um PSK dedicado, habilitando deste modo a revogação seletiva de associações de segurança. O PSK tem vida longa e é derivado da execução do protocolo e do valor de AK usado. Neste exemplo, os PSK podem ser rotulados e armazenados no AP com o nome do AK proprietário usado, permitindo então conhecimento de qual membro da família emitiu o acesso a qual convidado.

A delegação pode ser obtida com interação de usuário similar à solução OOB acima. Múltiplas formas de “endereços AP” podem ser incluídas em “parâmetros de rede”. Por exemplo, se o nome DNS do AP é incluído, o AP pode ser usado para acesso remoto à residência.

O AP não necessita ter uma interface “fora-de-faixa”, porque os códigos AK iniciais e parâmetros de rede podem ser fornecidos na forma de fichas passivas. Entretanto, se o AP tem uma interface “fora-de-faixa”, o AP pode usar aquela interface para emitir os códigos AK iniciais (AK proprietário) e parâmetros de rede de alguma forma limitada (por exemplo, uma vez após aquisição ou reset pleno). O AP pode usar a interface “fora-de-faixa” para receber códigos AK iniciais e parâmetros de rede do exterior (por exemplo, uma vez após aquisição ou reset pleno). A Tabela 1 seguinte sumariza diferentes possibilidades para geração e fornecimento dos AK e parâmetros de rede que podem ser usados de acordo com exemplos desta invenção.

Tabela 1 - Geração de Fornecimento de Código de Autenticação

GERAÇÃO DE PARÂMETRO	MECANISMO DE FORNECIMENTO	CANAL “FORA-DE-FAIXA” NO AP
AP gera os AK e parâmetros de rede	Fornecido separadamente (por exemplo, fichas NFC passivas, códigos PIN impressos na embalagem).	Não necessário

	Emitido via canal “fora-de-faixa” por um tempo limitado após reset pleno ou aquisição.	Necessário
	Emitido via canal “na-faixa” por um tempo limitado após reset pleno ou aquisição. (Menos seguro, mas poderia ser usado para evitar custos de hardware extra).	Não necessário
AP recebe os AK e parâmetros de rede de um dispositivo externo (por exemplo, telefone)	Recebido via canais “fora-de-faixa” por um tempo limitado após reset pleno ou aquisição.	Necessário
	Emitido via canal “na-faixa” por um tempo limitado após reset pleno ou aquisição. (Menos seguro, mas poderia ser usado para evitar custos de hardware extra).	Não necessário

Conforme mencionado acima, o canal “fora-de-faixa” não está limitado ao NFC. Exemplos adicionais de canais OOB incluem: SMS (Serviço de Mensagem Curta), MMS (serviço de geração de mensagem multimídia) ou serviços de geração de mensagens de telecomunicações similares. Usando SMS, um usuário pode tirar um contato de um livro de endereços, selecionar qual tipo de acesso autorizar e então enviar um SMS ao contato com o endereço AP e o AK. O dispositivo recebendo o SMS pode então executar as etapas 405 e 407 mostradas na Figura 4. Esta abordagem combinada preserva vantagens de ambas abordagens e habilita fácil gerenciamento de acesso de convidado.

Revogação: No caso mais simples, há somente um AK, e aquele AK pode ser usado para delegar acesso proprietário. Convidados podem ser admitidos usando uma disposição em pares não autenticada, como na abordagem Broadcom descrita acima. A diferença é que quando um

proprietário deseja remover acesso de convidado, a rede inteira não precisa ser recriada. Ao invés disso, exatamente os PSK que foram criados sem qualquer autenticação são removidos.

Quando o acesso de convidado é concedido usando um AK convidado, então quando este acesso de convidado deve ser revogado, o AP remove ou marca como inválido o PSK que foi usado pelo convidado durante seu primeiro eixo de rotação de acesso. Conforme mencionado acima, esta ação pode ser iniciada ou alcançada pressionando uma tecla no ponto de acesso ou outro controlador de acesso por um tempo predeterminado, o que revogará todo acesso de convidado à rede. Abordagens mais refinadas são também possíveis, sem se afastar desta invenção, mas da perspectiva de usabilidade de um usuário final, tal abordagem de uma tecla tem certas vantagens e atratividade. Alternativamente, remover ou marcar o PSK como inválido pode ser iniciado ou alcançado usando o dispositivo de usuário/introdutor 412, por exemplo, transmitindo uma requisição para revogação ao AP ou navegando em uma tabela de dispositivos de usuários/usuário autenticados/autenticado.

Mesmo após a revogação, convidados ainda manterão o AK válido, e então a possibilidade de obter um novo PSK usando uma requisição SES autenticada. No sentido de evitar isto, o AK usado por convidados é preferivelmente mudado como parte do procedimento de *reset* de acesso de convidado. Então, juntamente com a remoção dos PSK de convidado, o AP preferivelmente determina um novo AK para aceitar requisições SES autenticadas. Em adição, após este tipo de *reset* de AK, os dispositivos proprietários existentes são tornados capazes de conceder mais uma vez acesso a convidados.

Em geral, o AK é determinado por $AK = f(OAK, AK-ID)$, onde AK-ID pode ser qualquer parâmetro ou sub-função de parâmetros múltiplos. Três meios de permitir que dispositivos proprietários concedam

acesso a convidados incluem, por exemplo, procedimentos de marcação de tempo, número de seqüência, e transferência, como discutido adicionalmente abaixo. O AK-ID pode representar qualquer parâmetro único ou qualquer combinação de parâmetros com base em alguma função predefinida. Outros

5 parâmetros que podem ser incorporados no cálculo do AK-ID incluem, por exemplo, tipo de categoria, endereço MAC e nome ou ID de dispositivo de usuário. Aqueles especialistas na técnica verificarão que outros parâmetros podem também ou alternativamente ser usados em qualquer combinação. AK-ID pode ser considerado como uma estrutura de dados ou computação que

10 codifica várias informações de alguma maneira predeterminada.

Um AK pode, portanto, ser derivado de um OAK compartilhado entre o dispositivo de introdução e o aparelho, e uma ou mais outras variáveis armazenando informação adicional única para o novo dispositivo, e o endereço do AP como provido pelo dispositivo de introdução

15 para o novo dispositivo. Uma ou mais outras variáveis podem ser transferidas pelo novo dispositivo como parte do protocolo de acordo de código, de tal modo que o AP pode derivar o mesmo AK. O AK pode então ser usado para autenticar o protocolo de acordo de código, pois o AK não é ele próprio transferido. Outras abordagens ilustrativas são descritas abaixo.

20 Marcação de tempo: nesta abordagem, o AK convidado usado é uma função do tempo. Cada grupo (por exemplo, família, convidados, etc.) tem um “AK original” (OAK). O OAK não é divulgado durante a delegação. Ao invés disso, um AK transiente pode ser derivado do OAK, por exemplo, $AK = f(OAK, \text{tempo})$, onde OAK é como mencionado acima e o tempo

25 poderia ser qualquer valor baseado no tempo, por exemplo, milissegundos desde 1.1.1970 (Unix padrão). Ambos AP e os dispositivos proprietários/dispositivos mestre delegados podem calcular o mesmo AK usando esta função, e o dispositivo convidado recebe o AK e o apresenta ao AP juntamente com o identificador AK que inclui “tempo”. O ponto de

acesso pode aceitar requisições SES autenticadas somente quando é usado um AK que este reconhece. Os AK derivados terão então tempos de vida limitados, por exemplo, um dia. Isto implica em que os convidados somente tenham um dia no qual emitir as requisições SES autenticadas. Depois disso o

5 ponto de acesso não aceitará mais aquele AK. Uma desvantagem potencial com esta abordagem é que diferenças na sincronização de relógio entre o AP e os dispositivos delegados (que pode ser tal que o tempo do dispositivo é ajustado pelo usuário) pode causar inconsistências.

Número de seqüência: Esta abordagem envolve usar números

10 de seqüência ao invés de marcações de tempo, no sentido de evitar os problemas de sincronização de relógio mencionados acima. OAK é, como antes, e $AK = f(OAK, \text{número de seqüência})$. O AP mantém uma janela deslizante de números de seqüência aceitáveis. O AP atualiza a janela todas as vezes que recebe um novo número de seqüência. Como números de seqüência

15 possuem um tempo de vida curto, números de seqüência não usados antigos expirarão automaticamente. O resultado é que um AK pode somente ser usado por um curto período de tempo.

Transferência: nesta abordagem o AP gera um novo AK convidado quando o acesso de convidado deve ser reiniciado e os dispositivos

20 proprietários individuais então obtém o novo AK convidado a partir do AP, usando método “na-faixa” ou “fora-de-faixa”. Em tal cenário, os dispositivos proprietários têm conhecimento do AK proprietário, no sentido de permitir que desempacotem o novo AK convidado. Este método tem a desvantagem de que requer ação da parte dos usuários finais (ou dispositivos) no sentido de

25 obter o novo AK.

A invenção pode ser praticada em qualquer ambiente de rede adequado, e não está limitada a qualquer arquitetura de rede específica. Figura 5 apresenta uma outra amostra de ambiente de operação de rede na qual um ou mais aspectos ilustrativos da invenção podem ser praticados. O ponto de

acesso 501 incorpora um ponto de acesso de WLAN bem como acesso a Servidor(es) de WLAN e outras redes tal como a Internet 503. A primeira rede 505 pode incluir uma rede WLAN ou NFC, tal como RF ID. O dispositivo mestre 507 pode incluir um dispositivo de comunicação móvel ou dispositivo de controle remoto tendo acesso à primeira e segunda redes 505 e 509. A segunda rede 509 pode incluir um canal “fora-de-faixa” tal como NFC ou RF ID. A segunda rede 509 pode incluir alternativamente WLAN, rádio de curto alcance (por exemplo, BlueTooth) telecomunicação sem fio (SMS, MMS), IrDA e similares. O Novo Dispositivo 511 pode incluir um dispositivo de comunicação móvel, dispositivo de controle remoto, dispositivos periféricos, dispositivos eletrônicos de consumidor, ou outro dispositivo tendo acesso à segunda e terceira redes 509, 513. A terceira rede 513 pode incluir um canal “na-faixa” tal como a rede WLAN ou um canal “fora-de-faixa” como NFC ou RF ID.

Na arquitetura da Figura 5, onde um dos dispositivos tem um visor, por exemplo, um telefone móvel, quando o usuário “toca” a aplicação doméstica (por exemplo, um estéreo) o telefone móvel pode exibir uma imagem da aplicação transmitida da aplicação no visor do telefone. O usuário, pressionando uma tecla, pode mudar os parâmetros de rede somente para a aplicação mostrada no visor, dando então aos usuários um melhor entendimento de quais aplicações dispor em pares. No caso da WLAN, a disposição em pares é entre um dispositivo eletroacústico o ponto de acesso (e não entre dispositivos), mas a idéia não necessita ser limitada ao caso da WLAN. Neste caso, uma imagem do dispositivo pode ser exibida em um visor do AP, ou alternativamente uma imagem do AP pode ser exibida em um visor do dispositivo. A imagem pode ser transmitida na etapa 403 ou antes da etapa 403. A imagem pode ser fornecida via NFC ou qualquer outra rede de comunicação. Esta função requer significativo espaço de memória e poderia transformar o “toque” em “manter”, significando que o toque leva um tempo

mais longo. Como alternativa a exibir uma imagem, o telefone móvel pode exibir um nome de dispositivo, similar a dispositivos Bluetooth, preferivelmente com mais descrição, por exemplo, “conjunto de TV Philips”, “ponto de acesso WLAN da France Telecom”, “estéreo HiFi Sony”, “Nokia 6600”, “PDA do Sam”, etc.

Alguns dispositivos, entretanto, podem ter o mesmo nome pseudo único, então a conexão pode ser para/a partir de um outro dispositivo que não era pretendido. Tipicamente, o erro será detectado imediatamente, mas somente depois de pelo menos uma transmissão ter tido lugar, e os dados serem transmitidos ao dispositivo errado, e o receptor pretendido não ter recebido coisa alguma. Quando uma conexão sem fio entre dois telefones celulares é desejada, a prova de uma identidade de outra parte pode ser obtida da rede celular. Um telefone celular ou terminal móvel pode chamar o outro (sem a outra extremidade responder a chamada - significando que é grátis) para verificar o dispositivo. Isto é, para chamar o outro dispositivo, o chamador necessita conhecer o número da parte chamada. Em adição, a parte chamada é capaz de verificar o momento em que está sendo chamada, por exemplo, com base no ID chamador. Então, a prova de identidade dos dispositivos não é obviamente visível a partes externas.

Em uma realização da invenção, provar a identidade com uma chamada (não respondida) pode ser efetuada conforme segue: o dispositivo a ser autenticado (dispositivo A) envia seu número telefônico através de uma conexão sem fio (tal como Bluetooth ou WLAN) ao dispositivo que deseja se autenticar (dispositivo B). Uma aplicação de autenticação no dispositivo B aguarda algum tempo predeterminado ou randomicamente escolhido e disca para o dispositivo A via uma rede de telecomunicações sem fio. Quando o dispositivo A detecta a chamada, este imediatamente informa ao dispositivo B sobre a chamada, via uma conexão sem fio (tal como Bluetooth, WLAN). Uma aplicação de autenticação no dispositivo B pode agora decidir se a

resposta de A veio rápida o bastante para a chamada feita (durante alguma período predeterminado de tempo), fazendo deste modo com que B aprove a identidade de A (isto é, o número telefônico é enviado). Alternativamente ou adicionalmente, a identidade do dispositivo A, número telefônico e nome a partir do livre de endereço do dispositivo B, ou o número telefônico é apenas transmitido. Pode ser exibida ao usuário fazendo a conexão em um visor do dispositivo B e ser consultado sobre qual permissão deveria ser autorizada para a conexão. Esta técnica funciona mesmo se a rede não transmite o número telefônico do dispositivo A (por exemplo, se o número telefônico é secreto ou se o usuário está visitante em tal rede e o número não é transmitido). A autenticação mútua pode ser baseada no número telefônico do dispositivo A (se a rede o provê) ou em uma outra chamada da direção oposta. Este método pode ser útil, por exemplo, na etapa 403 na Figura 4. Uma realização alternativa da invenção, provando a identidade como uma chamada (não respondida) pode ser executada como segue: o dispositivo a ser autenticado (dispositivo A) envia seu número telefônico através de uma conexão de telecomunicação sem fio, ao dispositivo que deseja se autenticar (dispositivo B), isto é, o dispositivo A chama o dispositivo B. Uma aplicação de autenticação no dispositivo B armazena o número telefônico do dispositivo A em uma base de dados de acesso e aguarda algum tempo predeterminado ou randomicamente escolhido e disca para o dispositivo A via uma rede de telecomunicação sem fio. Quando o dispositivo A detecta a chamada, este informa imediatamente ao dispositivo B sobre a chamada, via uma conexão sem fio (tal como Bluetooth ou WLAN) incluindo o número telefônico do dispositivo B e seu próprio número telefônico. O número telefônico de A pode opcionalmente ser usado para computar o código usado para proteger a conexão sem fio. Uma aplicação de autenticação no dispositivo B pode verificar agora se o número telefônico do dispositivo A está na base de dados de acesso, se a resposta de A veio rápida o bastante para a chamada feita

(durante algum período predeterminado de tempo), fazendo deste modo com que B aprove a identidade de A (isto é, o número telefônico que este enviou). Este método é útil, por exemplo, na etapa 403 na Figura 4.

Adicionalmente, em uma realização da invenção, quando o dispositivo A informa ao dispositivo B sobre a chamada, via uma conexão Bluetooth, esta informação pode agora incluir o número telefônico do dispositivo B, o número telefônico do dispositivo A e também informação de identificação Bluetooth. O número telefônico de A pode ser usado opcionalmente para computar o código usado para proteger a conexão sem fio. Uma aplicação de autenticação no dispositivo B pode verificar se o número telefônico e a informação de identificação Bluetooth do dispositivo A estão na base de dados de acesso, se a resposta do dispositivo A veio rápida o bastante para a chamada feita (durante algum período predeterminado de tempo), fazendo deste modo com que o dispositivo B aprove a identidade do dispositivo A (isto é, o número telefônico que este enviou). A autenticação pode também ser feita verificando um par A (número telefônico, informação de identificação Bluetooth) na base de dados de acesso. Este método pode ser útil, por exemplo, na etapa 403 da Figura 4.

O método imediatamente descrito acima pode ser usado, por exemplo, nos seguintes exemplos de situações:

1) Um dispositivo de ponto de acesso WLAN (dispositivo B) e o novo dispositivo (dispositivo A) possuem capacidades de telecomunicação sem fio. Este acesso de telecomunicação sem fio é usado para compartilhar informação necessária para estabelecer acesso WLAN entre os dispositivos, como na etapa 403 na Figura 4. Neste caso, os dispositivos podem inicializar a configuração do acesso WLAN automaticamente após compartilhar a informação necessária. Alternativamente, a configuração do acesso WLAN pode ser iniciada manualmente pelo usuário.

2) O Gerente Mr. Marty senta-se em uma reunião com seus

clientes e percebe que não possui a última apresentação de seu produto armazenado em seu telefone inteligente. Ele envia uma mensagem SMS a sua secretária e pede a ela para enviá-la através de WLAN ad-hoc para seu telefone. Sua secretária inicia uma aplicação ad-hoc em seu telefone, que

5 inicia a conexão ad-hoc enviando seu número telefônico ao telefone de Marty, iniciando então a conexão. Marty aceita a conexão de sua secretária (esta é mostrada com base no número para o qual foi feita a chamada, ou foi destinada a ser feita para, dependendo dos ajustes de nível de segurança). Quando a conexão estiver feita, o arquivo pode ser enviado ao telefone

10 inteligente de Marty.

3) Quando um dispositivo A deseja fazer uma conexão com o dispositivo B, este cria uma conexão sem fio para o dispositivo B e os dispositivos trocam seus números telefônicos através da conexão. O UI nos telefones/dispositivos mostra o nome de usuário do dispositivo chamador (se

15 este está no livro de telefones do telefone) ou minimamente o número telefônico. O UI então solicita ao usuário se a conexão pode ser estabelecida ou autenticada. Durante a fase de autenticação, os dispositivos fazem uma chamada telefônica para o outro dispositivo, provando então com a chamada que o dispositivo é quem reivindica ser.

20 O método acima pode ser usado entre dispositivos que não estão fisicamente visíveis um ao outro, é suficiente que estes estejam dentro do alcance da conectividade sem fio. A conexão estabelecendo um processo é simples para o usuário, especialmente se o número telefônico do telefone chamado pode ser navegado a partir do livro telefônico (do ponto de vista do

25 usuário tornando a conexão tão fácil quanto fazer uma chamada).

De acordo com um aspecto da invenção, o acesso de rede pode ser baseado no AK e no endereço MAC de um dispositivo. Para permitir o acesso de rede ao novo dispositivo, um dispositivo de delegação pode dar o AK ao novo dispositivo “fora-de-faixa”, mas o dispositivo de delegação não

se comunica com o AP, nem há ali um protocolo de acordo de código especial entre o novo dispositivo e o AP. Quando o novo dispositivo contata o AP, o AP e o novo dispositivo derivam independentemente um novo PSK a partir do AK e o endereço MAC do dispositivo. Por exemplo, $PSK = f(AK, \text{endereço MAC})$, onde f é uma função de derivação de código adequada. Para revogar o acesso de rede a partir do dispositivo, o proprietário pode usar a interface de gerenciamento do AP para marcar o dispositivo alvo como “revogado”. Posteriormente, o PSK daquele dispositivo é removido e o AP pode adicionar um endereço MAC do dispositivo a uma lista de dispositivos revogados. Um dispositivo cujo endereço MAC esteja naquela lista não será capaz de estabelecer um PSK com o AP, isto é, não será capaz de executar a Etapa (1) acima, a menos que o acesso tenha sido novamente concedido ao dispositivo.

Uma vantagem desta abordagem é que o novo dispositivo e o AP podem derivar o PSK independentemente, sem novas mensagens de protocolo de acordo de código. O conhecimento do AK e endereço MAC do dispositivo é suficiente. Uma desvantagem desta abordagem, entretanto, é que o AP precisa não perder de volta os endereços MAC revogados. Também, esta abordagem é menos segura do que derivar o PSK do AK usando um protocolo de acordo de código, porque os endereços MAC podem ser forjados. Finalmente, permitir um dispositivo previamente revogado de volta na rede, requer que o delegador interaja com o AP para remover seu endereço MAC da lista de dispositivos revogados, requerendo deste modo conhecimento de um protocolo adicional.

De acordo com um outro aspecto da invenção, uma base de dados de dispositivos autenticados pode ser usada (ver tabela 2). O AP pode conter uma base de dados de dispositivos autenticados, por exemplo, uma tabela, armazenando (1) o endereço MAC de cada dispositivo que é parte da rede WLAN e (2) um código, PSK, que o AP compartilha com o dispositivo: {endereço MAC, PSK}. Quando um dispositivo contata o AP, o AP busca o

endereço MAC do dispositivo de contato da tabela e usa o PSK associado em comunicação com aquele dispositivo, se o endereço MAC é encontrado. Se o endereço MAC não é encontrado, o AP pode, por exemplo, recusar a se comunicar com o dispositivo, enviar uma mensagem predeterminada ao dispositivo, ou usar algum outro procedimento definido para dispositivos não autenticados. A base de dados de dispositivos autenticados pode incluir adicionalmente uma gravação de grupo de dispositivo (DG): {endereço MAC, PSK, DG}. O campo DG pode incluir, por exemplo, pelo menos um tipo e AK: por exemplo, DG = {Tipo, AK}. Tipo pode identificar um dispositivo, por exemplo, como “não autenticado”, em cujo caso o campo AK estaria vazio. Como um outro exemplo, o valor Tipo poderia ser “Convidado” em cujo caso o AK seria aquele reservado para convidados. Como um terceiro exemplo, o valor Tipo poderia ser “Doméstico” em cujo caso o AK será aquele reservado para dispositivos domésticos, tais como dispositivos eletrônicos de consumidor ou aplicações domésticas. Outros valores de Tipo podem incluir “Sensor” descrevendo diferentes sensores conectados ao AP. O número específico de tipos diferentes não é limitado. A gravação DG de um dispositivo é inicializada com base no valor do AK que o dispositivo conhece, por exemplo, quando aquele dispositivo se junta à rede. Adicionalmente, a base de dados pode ter uma coluna descrevendo a quem foram dados os direitos de acesso. Adicionalmente, o grupo de dispositivo pode incluir uma coluna para AK Original (OAK). A Tabela 2 mostra um exemplo de informação que pode ser incluída em uma base de dados de dispositivos autenticados. Outros valores de Tipo podem ser usados alternativamente, dependendo das necessidades do sistema, por exemplo, uma data de expiração associada a uma entrada de base de dados, para assegurar o cancelamento automático dos direitos do usuário (de outro modo pode ocorrer revogação quando um usuário é removido da base de dados ou quando o tempo de expiração é cancelado ou trocado). Um exemplo de uma base de dados de

dispositivos autenticados é mostrado abaixo na Tabela 2.

Tabela 2: Base de dados de dispositivos autenticados

Dado por (Autenticador)	Grupo de dispositivo (DG)				MAC	PSK	Nome do dispositivo
	Tipo	AK	OAK				
Dispositivo mestre	Não autenticado	-	-		MAC1	PSK1	Estéreo 1
Dispositivo mestre	Sensor	AK2	OAK3		MAC2	PSK2	Temperatura, quarto 1
Dispositivo mestre	Doméstico	AK9	OAK1		MAC9	PSK9	TV 1
Mãe	Convidado	AK3	OAK2		MAC3	PSK3	Telefone do Bob
Jack	Convidado	AK4	OAK2		MAC4	PSK4	Dispositivo de jogo do Pete
Jack	Convidado	AK5	OAK2		MAC5	PSK5	Reprodutor de música da Pate
Jane	Não autenticado	-	-		MAC6	PSK6	NN
Pai	Sensor	AK7	OAK3		MAC7	PSK7	Umidade, quarto 1
Pai	Convidado	AK8	OAK2		MAC8	PSK8	Câmera da Mary

Conforme descrito acima, quando um dispositivo contata o AP, o AP buscará o endereço MAC do dispositivo de contato a partir da base de dados de dispositivos autenticados e usará o PSK associado em comunicação com aquele dispositivo, se o endereço MAC é encontrado. A existência da gravação DG permite que o AP gerencie diferentes grupos de dispositivos. Por exemplo, sem o campo DG, a revogação do acesso de rede de um dispositivo convidado requer que o proprietário conheça o endereço MAC ou o PSK daquele dispositivo. Se este não conhece aqueles, então precisa encontrá-los (por exemplo, examinando os endereços MAC de todos os seus dispositivos domésticos) ou precisa mudar os valores de PSK de todos seus dispositivos, isto é, precisa explorar ou recodificar a totalidade da rede para revogar o dispositivo convidado.

Em contraste, consideremos a mesma operação a gravação DG está presente na Tabela AP. Quando o proprietário instrui o AP para revogar o acesso a todos os dispositivos convidados, o ponto AP simplesmente remove todas as gravações cujo campo “Tipo” DG é igual a “Convidado”.

- 5 Adicionalmente, informação sobre quem recebeu os direitos de acesso pode ser usada para tomar decisões inteligentes. Em um exemplo adicional, um dispositivo mestre pode acessar sem fio e gerenciar a base de dados de dispositivos autenticados. Alternativamente, a base de dados de dispositivos autenticados pode ser acessada por um computador pessoal em uma rede
- 10 doméstica WLAN. Uma revogação de um usuário pode acontecer removendo o usuário da lista ou cancelando ou mudando a data/horário de expiração do dispositivo do usuário. Alternativamente, a Tabela pode também incluir datas de expiração para dispositivos de usuário. Isto assegura o cancelamento automático de direitos de usuário. Alternativamente, o usuário pode usar o
- 15 campo “nome do dispositivo” para identificar os dispositivos cujo acesso deveria ser revogado.

- De acordo com um aspecto da invenção, a informação transferida usando o canal “fora-de-faixa” pode incluir um PSK derivado, uma senha randômica, ou um ou mais pares <tipo AK, versão AK, valor
- 20 AK>. “Tipo AK” pode ser um inteiro de tamanho fixo, opcionalmente com alguns valores reservados (por exemplo, 0 = visitante, 1 = proprietário). Versão AK é um número e seu conteúdo depende do esquema usado para revogação. Se os números de seqüência são usados como a base de revogação, a versão AK pode conter <ownerID +
- 25 sequenceNumberOwnerUsedWhenIssuingAK>. Se uma abordagem baseada no tempo é usada, a versão AK pode conter <ownerID | marcação de tempo de quando o AK foi emitido>. Se a revogação de convidados conduz a um novo AK convidado sendo criado no AP e proprietários necessitando transferir este novo AK, não há informação necessária neste campo.

Conforme discutido acima, Broadcom propôs SES. A proposta Broadcom pode ser modificada de acordo com um ou mais aspectos da invenção, onde o protocolo de acordo de código preferivelmente suporta autenticação opcional. A autenticação preferivelmente usa um AK, e as mensagens de protocolo preferivelmente são mudadas para identificar o tipo AK. (Se o último não é possível, somente dois grupos podem ser suportados: autenticado = proprietário, não autenticado = convidado). Quando o PSK resultante é armazenado, o tipo AK é também armazenado. Dois tipos de *reset* podem ser usados, um para remover todas as associações de segurança de convidado (por exemplo, pressionamento longo de tecla) e um segundo para reiniciar completamente o sistema. Também, o AP pode estar permanentemente em um modo onde pode aceitar requisições autenticadas para os PSK, isto é, não há equipamento para pressionamento de tecla no sentido de alcançar este modo.

O SecureEasySetup (SES), conforme descrito acima e, por exemplo, em www.broadcom.com/press/release.php?id=659800, é um protocolo simples para configurar conexões de WLAN seguras propostas pela Broadcom. O protocolo SES supõe que ambos dispositivo de cliente e ponto de acesso (AP) possuem uma tecla (a tecla pode ser uma tecla de software ou hardware ou chave, por exemplo, chave liga/desliga). No sentido de adicionar um novo dispositivo de cliente à rede WLAN, o usuário primeiramente pressiona uma tecla no AP e então no dispositivo de cliente. O resultado destes dois pressionamentos de tecla é que o cliente recebe um código WPA (“Acesso Protegido Wi-Fi”) e melhora nos sistemas e métodos descritos acima. Por exemplo, como será descrito abaixo, aspectos da presente invenção tornam o acesso de rede mais seguro e acessível ao usuário em situações fora de uma residência do usuário individual. Como exemplos ainda mais específicos, sistemas e métodos adequados podem ser providos para permitir que visitantes, por exemplo, em hotéis, restaurantes e similares,

acessem seguramente, temporariamente e facilmente o sistema de rede.

Ao habilitar o acesso de visitante a redes, hotéis, restaurantes e outros locais de acesso público, pode não ser desejável remover todas as contas de visitante a um dado tempo (ao invés disso, convidados ou visitantes da rede podem entrar e sair da rede em muitos instantes diferentes). Conseqüentemente, de acordo com pelo menos alguns exemplos da invenção, conforme descrito em mais detalhe abaixo, a informação de expiração pode ser adicionada a um ID de código de autenticação e/ou informação de expiração pode ser provida, via cálculo de um código de autenticação. Em alguns exemplos, se a informação de expiração = 0, isto pode ser usado para indicar que o AK não expira automaticamente.

Antes que os clientes possam ser adicionados a uma rede WLAN, o AP necessita gerar um código WPA e um SSID. Um código WPA é a especificação pela Aliança Wi-Fi baseada em uma versão do 802.11i. É pretendido haver uma medida provisória até que 802.11i esteja pronto. WPA-2 está destinado a ser 802.11i. 802.11i é um padrão IEEE oficial para segurança das LAN Sem Fio. Em sistemas e métodos de acordo com pelo menos alguns exemplos desta invenção, o código WPA é um código pré compartilhado entre o cliente WLAN e um ponto de acesso (também chamado aqui de um “PSK”). Um SSID é um identificador único para uma rede WLAN. Pontos de acesso (AP) radiodifundem o SSID.

Em pelo menos alguns exemplos desta invenção, um cliente pode ser adicionado a uma rede WLAN pressionando uma tecla provida no AP por um período de tempo estendido (por exemplo, cinco segundos). Enquanto o AP gera o código WPA e o SSID, fará piscar luzes de LED ou dar alguma outra indicação ao usuário. Se o AP possuía quaisquer disposições em pares existentes, estas serão removidas durante este processo. Uma vez que uma nova rede é gerada, os usuários podem adicionar novos dispositivos à rede, pressionando uma única tecla no AP e no dispositivo de cliente.

Figura 6 ilustra o protocolo para adicionar novos clientes em uma rede usando o protocolo SES. Na etapa 601, o pressionamento de uma tecla no AP 610 faz com que o AP entre no modo de recepção por algum período de tempo, por exemplo, dois minutos. Isto é, o AP aguarda em um estado pelo tempo em que está disponível para estabelecer comunicação em túnel seguro com um dispositivo de cliente. Na etapa 602, um pressionamento de tecla no dispositivo de cliente 611 inicia uma busca pelo cliente, para localizar um AP, por exemplo, AP 610, que está no modo de recepção. Depois do cliente 611 ter encontrado o AP 610, o cliente 611 estabelece um túnel seguro com o AP 610, na etapa 603. Se o AP já tiver criado um túnel seguro com um outro cliente, este não começará a assegurar o estabelecimento de túnel, mas ao invés disso replicará com uma advertência ou mensagem de erro. Na etapa 604, o cliente 611 recebe uma mensagem de protocolo para continuar o estabelecimento de túnel seguro. A mensagem de protocolo pode incluir o código WPA e SSID.

O protocolo SES da Figura 6 é amistoso e algo seguro. Entretanto, este ainda possui umas poucas deficiências, incluindo que a disposição em pares de cliente com um AP não pretendido é possível, disposição em pares de AP com um cliente não pretendido, são possíveis ataques “*man-in-the-middle*” e todas as disposições em pares são permanentes. Não é possível conceder acesso temporário, por exemplo, a visitantes. Algumas dessas vulnerabilidades supõem que há um outro AP possivelmente malicioso ou cliente presente e no modo de recepção (estes são denotados como “AP_OTHER” e “CLIENT_OTHER” na descrição abaixo). O AP que o usuário deseja dispor em pares com seu cliente é designado por “AP_OK” e seu cliente é designado por “CLIENT_OK” na descrição abaixo.

Então, vários melhoramentos podem ser feitos ao protocolo SES, de acordo com um ou mais aspectos da invenção. A disposição em pares de cliente com um AP não pretendido pode ser evitada de vários modos.

Primeiramente, se o cliente acha mais de um AP, o cliente pode abortar o procedimento de disposição em pares e alertar o usuário. Em segundo lugar, os pontos de acesso podem ser remetidos com nomes diferentes (tais como “Tigre” e “Leão”) que são retirados de um conjunto relativamente grande de nomes, e estes nomes podem ser impressos no topo do AP. Se o cliente encontra mais de um AP, o usuário pode então ser solicitado a selecionar o AP correto de uma lista de nomes. Esta característica pode auxiliar a reduzir acidentes. Se há mais de um AP com o mesmo nome, então o cliente pode ser adaptado para abortar o procedimento de disposição em pares.

Um cliente também pode dispor em pares com um AP não pretendido, se o usuário pressiona a tecla no dispositivo de cliente após o tempo predeterminado (por exemplo, dois minutos) a partir do pressionamento da tecla no dispositivo AP_OK, de tal modo que o dispositivo AP_OK não esteja mais no modo de recepção. Esta situação poderia ser evitada, por exemplo, se o AP desse alguma indicação (tal como luz piscando) quando está no modo de recepção e um tipo diferente de indicação (tal como luz constante por cinco segundos) quando a disposição em pares tiver sido estabilizada com sucesso. Deste modo, o usuário poderia verificar, após pressionar a tecla no cliente que a indicação no AP tenha mudado com sucesso do modo de recepção para o modo de disposição em pares. Também, o usuário do cliente pode ver, antes de pressionar a tecla de cliente, se o AP está no modo de recepção. Se uma disposição em pares bem sucedida não ocorre, mas ao invés disso o cliente tiver disposto em pares com “AP_OTHER”, então a disposição em pares incorreta pode ser removida manualmente do cliente.

Uma disposição em pares AP com um cliente não pretendido, pode ser evitada. Por exemplo, um AP pode dispor em pares com um “CLIENT_OTHER” se o usuário do “CLIENT_OTHER” pressiona a tecla em seu dispositivo de cliente mais rápido que o usuário do dispositivo de

“CLIENT_OK” pressiona sua tecla. Neste caso, uma mensagem de advertência pode ser enviada ao “CLIENT_OK”. Esta situação pode ser detectada e processada de uma variedade de modos diferentes. Por exemplo, a situação pode ser detectada se houver um protocolo de disposição em pares entre o CLIENTE e o AP e o AP continua a ouvir requisições de cliente por algum tempo, mesmo após um primeiro cliente completar com sucesso uma disposição em pares, por exemplo, até que o intervalo de tempo de disposição em pares (por exemplo, 2 minutos neste exemplo de sistema e método) se escoe. Se “CLIENT_OTHER” dispõe em pares primeiramente, então quando “CLIENT_OK” tenta dispor em pares com “AP_OK”, “AP_OK” retornará uma mensagem de advertência para “CLIENT_OK” indicando que a disposição em pares não é mais possível e a razão para isto (por exemplo, que um outro dispositivo já foi disposto em pares). Ao receber a mensagem de advertência, “CLIENT_OK” pode ser adaptado para exibir uma mensagem ao usuário, dizendo algo como “AP recusou-se a admitir seu dispositivo porque um outro dispositivo chegou antes de você. Pressione a tecla de cancelamento no AP por 3 segundos para tirar o outro dispositivo fora de sua rede AP” ou outra mensagem apropriada baseada no projeto do sistema.

Quando “CLIENT_OTHER” chega antes de “CLIENT_OK”, o AP pode não reconhecer “CLIENT_OK” e ou pode não reconhecer que um usuário errado (“CLIENT_OTHER”) foi disposto em pares (o AP pode não ter qualquer meio para reconhecer estas situações). Por esta razão, o AP pode não ser adaptado para tomar qualquer ação automaticamente, por si próprio, mas ao invés disso o AP envia uma mensagem de advertência pelo menos para o dispositivo de cliente tentando a última disposição em pares. Se “CLIENT_OK” recebe a mensagem de advertência, então o usuário do “CLIENT_OK” pode executar REMOVE_LAST_OPERATION descrita abaixo e/ou executar outras ações apropriadas. Se “CLIENT_OTHER” recebe a advertência, então por definição seu usuário não pode atuar na advertência

porque o usuário presumivelmente não terá acesso físico para fazer a função de REMOVE_LAST_OPERATION no AP (por exemplo, o usuário de cliente não autorizado presumivelmente não terá acesso físico ao AP).

5 Uma função REMOVE_LAST_OPERATION associada ao AP pode ser executada a qualquer tempo desejado, por exemplo, quando o usuário recebe uma mensagem de advertência no "CLIENT_OK" conforme descrito acima. Executar esta operação apaga, termina ou de outro modo elimina a disposição em pares não pretendida estabelecida com "CLIENT_OTHER", e opcionalmente torna novamente o AP disponível para
10 disposição em pares com "CLIENT_OK". A função REMOVE_LAST_OPERATION pode ser ativada, por exemplo, pressionando a mesma tecla SES por tempo mais longo ou mais curto que uma disposição em pares normal ou, se desejado, uma outra tecla pode ser provida para esta operação.

15 Ataques "*man in the middle*" podem ser evitados permitindo que o usuário compare as funções de "*hashing*" do código WPA em pares acordado. Por exemplo, se ambos cliente e o AP tem um único LED, os dispositivos poderiam apresentar a formação de "*hashing*" do código publico do AP um bit por vez com o LED (bit 1 poderia ser apresentado com uma luz
20 verde e bit 0 sem luz, por exemplo) para então assegurar que o cliente tenha disposto em pares com "AP_OK". Se ambos os dispositivos possuem pequenos visores, o "*hashing*" poderia ser representado como uma seqüência sonora (usando frequências diferentes ou diferentes amplitudes que representam 1 e 0). O AP pode radiodifundir uma lista de suas capacidades de
25 emissão de "*hashing*" e o cliente é suposto escolher uma da lista.

Este processo de comparação é opcional. Se o usuário nada faz após o protocolo SES normal, nenhuma comparação de funções de "*hashing*" será executada. Entretanto, se o usuário deseja comparar funções de "*hashing*", pode executar uma COMPARE_HASHES_OPERATION após o

protocolo SES normal. Se os usuários não usam COMPARE_HASHES_OPERATION, o mesmo nível de segurança que no SES original pode ser provido e obtido. O COMPARE_HASHES_OPERATION, entretanto, permite que um usuário
 5 consciente de segurança obtenha um nível mais alto de segurança contra um “*man in the middle*” ativo.

Uma vez que o usuário tenha executado COMPARE_HASHES_OPERATION, ambos dispositivos mostram a primeira parte da função de “*hashing*”. Se as partes da função de “*hashing*”
 10 são diferentes, um ataque de “*man in the middle*” ocorreu e o usuário pode ser orientado ou de outro modo saber executar REMOVE_LAST_OPERATION no AP. Se as partes de função de “*hashing*” são idênticas, o usuário pode fazer coisa alguma e esta disposição em pares será aceita. Alternativamente, o usuário pode selecionar NEXT_PART_OPERATION em ambos os
 15 dispositivos. Como resultado desta operação, ambos os dispositivos mostram a próxima parte da função de “*hashing*” e o usuário pode novamente escolher remover esta disposição em pares, aceitar esta disposição em pares nada fazendo, ou mudar para a próxima parte de função de “*hashing*”. Comparar funções de “*hashing*” usando saída de áudio pode ser uma abordagem
 20 amistosa desejável, porque o ouvido humano pode diferenciar mais facilmente entre seqüências sonoras que estão fora do tom ou fora de fase.

Quanto mais o usuário continua com este processo de comparação de funções de “*hashing*”, menor a possibilidade de um ataque de “*man in the middle*” bem sucedido. Comparar um bit reduz a possibilidade de
 25 ataque bem sucedido de 50 por cento. Comparar dois bits reduz a possibilidade de 75 por cento, e assim por diante. O protocolo de disposição em pares pode ser baseado, por exemplo, no MANA (“Manual de Autenticação para Dispositivos Sem Fio”, Gehrman e outros, Cryptobytes Spring 2004), que permite um alto nível de segurança contra ataques de “*man*

in the middle”, mesmo com valores de verificação relativamente curtos.

De acordo com um aspecto da invenção, o protocolo SES pode ser modificado para prover acesso temporário. O protocolo básico SES também permite que usuários adicionem dispositivos permanentemente na rede sem fio. Entretanto, seria uma melhoria também permitir acesso temporário, por exemplo, para visitantes, hóspedes de hotel, etc. Quando um visitante chega, o usuário pode dar seu acesso temporário à rede, por exemplo, executando uma ADD_VISITOR_OPERATION no AP ao invés de pressionar a tecla SES normal. Esta ação inicia a execução do protocolo SES normal e o visitante é requerido a pressionar a tecla em seu dispositivo, dentro do tempo predeterminado, por exemplo, dois minutos. Se a negociação SES é bem sucedida, o AP lembrará deste cliente como um visitante. Exemplos de modos pelos quais o acesso temporário pode ser provido são descritos acima.

O acesso temporário pode ser revogado de vários modos. Quando o usuário deseja remover todos os visitantes da rede, pode executar uma REMOVE_VISITORS_OPERATION no AP. Como resultado desta operação, o AP enviará um novo código WPA a todos os outros clientes pertencentes à rede, e os visitantes não receberão este novo código. A remoção de menos que todos os visitantes pode ser obtida conforme descrito acima.

De acordo com um aspecto da invenção, diferentes operações podem ser mapeadas para ações reais executadas pelo usuário. Aqueles especialistas na técnica verificarão que estes são apenas exemplos, e outros mapeamentos podem também ou alternativamente ser usados. Qualquer modo para mapear uma ação do usuário para AP ou funções de dispositivo de cliente podem ser usados, sem se afastar do escopo da invenção. Notadamente, as várias teclas descritas abaixo (por exemplo, as teclas “SES” e “Visitor”) podem estar localizadas diretamente no AP e/ou um outro dispositivo de controle operativamente acoplado ao AP (por exemplo, por

uma conexão sem fio, um controlador remoto, etc.), para uso, por exemplo, no caso em que o AP esteja localizado em uma localização remota ou difícil de alcançar. A Tabela 3 abaixo mostra exemplos de possíveis mapeamentos de operações de dispositivo para várias ações de usuário.

5 **Tabela 3: Mapeamentos de operações para ações**

Operação	Ações
REMOVE_LAST_OPERATION	Pressione a tecla SES por três segundos após disposição em pares
COMPARE_HASHES_OPERATION	Pressione a tecla SES brevemente após disposição em pares
NEXT_PART_OPERATION	Pressione a tecla SES brevemente quando a parte de função de "hashing" corrente está sendo mostrada
ADD_VISITOR_OPERATION	Pressione uma outra tecla (rotulada como Tecla "Visitor") brevemente
REMOVE_VISITORS_OPERATION	Pressione uma outra tecla (rotulada como Tecla "Visitor") por três segundos

O protocolo SES básico é atrativo porque é amistoso e relativamente seguro. Entretanto, ainda tem deficiências. Aspectos desta invenção provêm várias extensões ao protocolo SES básico, que tornam o protocolo mais seguro e útil, sem sacrificar a vantagem de usabilidade do SES. Deveria ser notado que estas extensões não complicam o protocolo SES normal do ponto de vista do usuário. O usuário pode eliminar disposições em pares não pretendidas acidentais com simples REMOVE_LAST_OPERATION, mas não é forçado a fazer isso.

15 Evitar ataques de "man in the middle" ativos é consideravelmente mais difícil e, em muitos cenários, ataques de "man in the middle" ativos não são realísticos. Em situações críticas de segurança, um usuário poderia avançado poderia, entretanto, usar o método de comparação de funções de "hashing" descrito acima, para melhorar a segurança do protocolo SES normal.

20 O ADD_VISITOR_OPERATION e

REMOVE_VISITORS_OPERATION provêm extensões plenas para o protocolo SES. Sem estes, o usuário não pode adicionar dispositivos de visitante e/ou tem que reconfigurar a rede inteira uma vez que o usuário deixa a rede.

5 Um ou mais aspectos da invenção podem ser realizados em instruções executáveis por computador, tal como em um ou mais módulos de programa, executados por um ou mais computadores ou outros dispositivos. Em geral, o programa inclui rotinas, programas, objetos, componentes, estruturas de dados, etc. que executam tarefas particulares ou implementam

10 tipos de dados abstratos particulares quando executados por um processador em um computador ou outro dispositivo. As instruções executáveis por computador podem ser armazenadas em um meio legível por computador tal como um disco rígido, disco óptico, meios de armazenagem removíveis, memória de estado sólido, RAM, etc. Como será verificado por um

15 especialista na técnica, a funcionalidade dos módulos do programa pode ser combinada ou distribuída conforme desejado, em várias realizações. Em adição, a funcionalidade pode ser realizada no todo ou em parte em firmware e hardware equivalentes, tais como circuitos integrados, arranjos de portas programáveis em campo (FPGA) e similares.

20 A presente invenção inclui qualquer nova característica ou combinação de características aqui descritas, seja explicitamente ou qualquer generalização destas. Embora a invenção tenha sido descrita com respeito a exemplos específicos incluindo modos presentemente preferidos para realizar a invenção, aqueles especialistas na técnica verificarão que há numerosas

25 variações e permutações dos sistemas e técnicas acima descritos. Então, o espírito e escopo da invenção deveria ser considerado amplamente conforme relatado nas reivindicações anexas.

REIVINDICAÇÕES

1. Método para gerenciar acesso a uma rede sem fio por um dispositivo terminal, caracterizado pelo fato de compreender etapas de:

5 a) o dispositivo terminal receber uma primeira chave de um dispositivo confiável da rede sem fio, via um primeiro canal de comunicação;

b) executar um protocolo de acordo de chave entre o dispositivo terminal e a rede sem fio via um segundo canal de comunicação, para determinar uma segunda chave correspondente ao dispositivo terminal autenticado usando a primeira chave;

10 c) autenticar o dispositivo terminal pela rede sem fio, usando a segunda chave; e

d) autorizar o terminal a acessar a rede sem fio, usando o segundo canal de comunicação na conclusão bem sucedida da etapa c).

15 2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa a) compreende gerar a primeira chave com base em uma função de uma terceira chave e pelo menos uma outra variável.

20 3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a pelo menos uma outra variável compreende um dentre uma marcação de tempo, um número de seqüência, um nome de dispositivo, um tipo de dispositivo, uma categoria de dispositivo, um endereço de dispositivo, e um tempo de vida de entrada do dispositivo.

25 4. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a primeira chave compreende uma chave de autenticação (AK), a segunda chave compreende uma chave pré-compartilhada (PSK) e a terceira chave compreende uma chave de autenticação original (OAK).

5. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a etapa b) compreende transferir a pelo menos uma outra variável como parte do protocolo de acordo de chave.

6. Método de acordo com a reivindicação 2, caracterizado pelo

fato de compreender adicionalmente determinar a terceira chave via protocolo de acordo de chave entre o dispositivo confiável e a rede sem fio.

5 7. Método de acordo com a reivindicação 6, caracterizado pelo fato de compreender adicionalmente o dispositivo confiável determinar a terceira chave e transmitir a terceira chave à rede sem fio.

8. Método de acordo com a reivindicação 6, caracterizado pelo fato de compreender adicionalmente a rede sem fio determinar a terceira chave e transmitir a terceira chave ao dispositivo confiável.

10 9. Método de acordo com a reivindicação 6, caracterizado pelo fato de compreender adicionalmente uma terceira parte determinar a terceira chave e transmitir a terceira chave para comunicação à rede sem fio e dispositivo confiável.

10. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender adicionalmente:

15 e) armazenar uma entrada correspondente ao dispositivo terminal em uma base de dados de acesso da rede sem fio.

11. Método de acordo com a reivindicação 10, caracterizado pelo fato de que a entrada compreende informação recebida do dispositivo terminal.

20 12. Método de acordo com a reivindicação 10, caracterizado pelo fato de que a etapa c) compreende consultar a base de dados de acesso quanto à entrada correspondente ao dispositivo terminal para determinar direitos de autenticação e acesso do dispositivo terminal.

25 13. Método de acordo com a reivindicação 10, caracterizado pelo fato de compreender adicionalmente:

f) revogar o acesso do dispositivo terminal à rede sem fio, com base na informação armazenada na entrada da base de dados de acesso.

14. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o primeiro canal de comunicação compreende

um canal de comunicação de campo próximo (NFC).

15. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o primeiro canal de comunicação compreende um serviço de envio de mensagem de telecomunicações.

5 16. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o segundo canal de comunicação compreende uma rede de área local sem fio (WLAN).

17. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a rede sem fio compreende uma rede de área
10 local sem fio (WLAN).

18. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender adicionalmente prover um controlador de acesso através do qual o dispositivo terminal acessa a rede sem fio na etapa d).

15 19. Método de acordo com a reivindicação 10, caracterizado pelo fato de compreender adicionalmente prover um controlador de acesso através do qual o dispositivo terminal acessa a rede sem fio na etapa d), e armazenar a base de dados de acesso no controlador de acesso.

20 20. Método de acordo com a reivindicação 1, caracterizado pelo fato de que na etapa a) o dispositivo confiável compreende um dispositivo de comunicações sem fio.

21. Método de acordo com a reivindicação 18, caracterizado pelo fato de que o dispositivo confiável compreende o controlador de acesso.

25 22. Método de acordo com a reivindicação 13, caracterizado pelo fato de que a etapa f) compreende revogar um segundo acesso do dispositivo terminal à rede sem fio.

23. Método de acordo com a reivindicação 13, caracterizado pelo fato de que a etapa f) compreende revogar todas as

entradas de base de dados de acesso coincidindo com um ou mais critérios especificados.

24. Método de acordo com a reivindicação 23, caracterizado pelo fato de que um ou mais critérios especificados
5 compreendem um tipo de grupo de dispositivo predefinido.

25. Método de acordo com a reivindicação 24, caracterizado pelo fato de que o tipo de grupo de dispositivo predefinido identifica um grupo de dispositivo correspondente a dispositivos convidados na rede sem fio.

10 26. Método de acordo com a reivindicação 23, caracterizado pelo fato de que o um ou mais critérios especificados compreendem um nome de dispositivo.

27. Sistema, caracterizado pelo fato de compreender:

15 um primeiro dispositivo confiável por uma rede sem fio, citado primeiro dispositivo armazenando instruções executáveis para transmitir uma primeira chave a um segundo dispositivo, via um primeiro canal de comunicação;

20 o segundo dispositivo não confiável pela rede sem fio, citado segundo dispositivo armazenando instruções executáveis para executar, via um segundo canal de comunicação, um protocolo de acordo de chave com um controlador de acesso da rede sem fio, para determinar uma segunda chave correspondente ao segundo dispositivo, onde o protocolo de acordo de chave autentica a segunda chave, usando a primeira chave;

25 o controlador de acesso armazenar instruções executáveis para autenticar o segundo dispositivo usando a segunda chave, e para autorizar o segundo dispositivo a acessar a rede sem fio na autenticação bem sucedida.

28. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que a primeira chave é gerada como uma função de uma terceira chave e pelo menos uma outra variável.

29. Sistema de acordo com a reivindicação 28, caracterizado pelo fato de que a pelo menos uma variável compreende um dentre uma marcação de tempo, um número de seqüência, um nome de dispositivo, um tipo de dispositivo, uma categoria de dispositivo, um endereço de dispositivo, e um tempo de vida de entrada do dispositivo.

30. Sistema de acordo com a reivindicação 28, caracterizado pelo fato de que a primeira chave compreende uma chave de autenticação (AK), a segunda chave compreende uma chave pré-compartilhada (PSK) e a terceira chave compreende uma chave de autenticação original (OAK).

31. Sistema de acordo com a reivindicação 28, caracterizado pelo fato de que a pelo menos uma outra variável é transferida como parte do protocolo de acordo de chave.

32. Sistema de acordo com a reivindicação 28, caracterizado pelo fato de que o primeiro dispositivo e o controlador de acesso determinam a terceira chave via um protocolo de acordo de chave.

33. Sistema de acordo com a reivindicação 32, caracterizado pelo fato de que o primeiro dispositivo determina a terceira chave e transmite a terceira chave ao controlador de acesso.

34. Sistema de acordo com a reivindicação 32, caracterizado pelo fato de que o controlador de acesso determina a terceira chave e transmite a terceira chave ao primeiro dispositivo.

35. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o controlador de acesso armazena adicionalmente instruções executáveis para armazenar uma entrada correspondente ao segundo dispositivo em uma base de dados de acesso da rede sem fio.

36. Sistema de acordo com a reivindicação 35, caracterizado pelo fato de que a entrada compreende informação recebida do

segundo dispositivo.

37. Sistema de acordo com a reivindicação 35, caracterizado pelo fato de que o controlador de acesso armazena instruções executáveis para consultar a base de dados de acesso para a entrada correspondente ao segundo dispositivo, para determinar direitos de autenticação e acesso do segundo dispositivo.

38. Sistema de acordo com a reivindicação 35, caracterizado pelo fato de que o controlador de acesso armazena instruções executáveis para revogar o acesso do segundo dispositivo à rede sem fio, com base na informação armazenada na entrada da base de dados de acesso.

39. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o primeiro canal de comunicação compreende um canal de comunicação de campo próximo (NFC).

40. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o primeiro canal de comunicação compreende um serviço de envio de mensagem de telecomunicações.

41. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o segundo canal de comunicação compreende uma rede de área local sem fio (WLAN).

42. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que a rede sem fio compreende uma rede de área local sem fio (WLAN).

43. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o primeiro dispositivo compreende um dispositivo de comunicações sem fio.

44. Sistema de acordo com a reivindicação 27, caracterizado pelo fato de que o primeiro dispositivo compreende o controlador de acesso.

45. Sistema de acordo com a reivindicação 38,

caracterizado pelo fato de que o controlador de acesso revoga o acesso do segundo dispositivo à rede sem fio, sem revogar o acesso de um terceiro terminal à rede sem fio.

5 46. Sistema de acordo com a reivindicação 38, caracterizado pelo fato de que o controlador de acesso revoga todas as entradas de base de dados de acesso coincidindo com um ou mais critérios especificados.

10 47. Sistema de acordo com a reivindicação 46, caracterizado pelo fato de que um ou mais critérios especificados compreendem um tipo de grupo de dispositivo predefinido.

 48. Sistema de acordo com a reivindicação 47, caracterizado pelo fato de que o tipo de grupo de dispositivo predefinido identifica um grupo de dispositivo correspondente a dispositivos convidados na rede sem fio.

15 49. Sistema de acordo com a reivindicação 46, caracterizado pelo fato de que o um ou mais critérios especificados compreendem um nome de dispositivo.

20 50. Método para gerenciar acesso a uma rede sem fio por um dispositivo terminal, caracterizado pelo fato de que a rede sem fio inclui um canal de comunicação em-banda, compreendendo as etapas de:

25 a) executar um protocolo de acordo de chave entre o dispositivo terminal e a rede sem fio via o canal de comunicação em-banda, para determinar uma primeira chave correspondente ao dispositivo terminal e autenticado comparando pelo menos uma parte de uma soma de verificação correspondente à primeira chave;

 b) autenticar o dispositivo terminal pela rede sem fio, usando a primeira chave; e

 c) autorizar o terminal a acessar a rede sem fio, na conclusão bem sucedida da etapa b).

51. Método de acordo com a reivindicação 50, caracterizado pelo fato de que a etapa a) compreende visualizar partes sucessivas da soma de verificação simultaneamente no dispositivo terminal e na rede sem fio.

5 52. Método de acordo com a reivindicação 50, caracterizado pelo fato de compreender adicionalmente revogar o acesso do dispositivo terminal à rede sem fio, com base na informação correspondente ao terminal, armazenada na base de dados de acesso.

10 53. Método de acordo com a reivindicação 52, caracterizado pelo fato de que a etapa de revogar compreende remover os direitos de acesso de um terminal cuja entrada é a mais recente na base de dados do controlador de acesso de acordo com uma única ação do usuário.

15 54. Método de acordo com a reivindicação 53, caracterizado pelo fato de que a etapa de revogar é iniciada recebendo entrada de usuário no controlador de acesso da rede sem fio.

55. Método de acordo com a reivindicação 54, caracterizado pelo fato de que a entrada de usuário compreende detectar que um usuário pressionou um botão predefinido de uma maneira predefinida em um controlador de acesso.

20 56. Um ou mais meios legíveis por computador, caracterizado(s) pelo fato de armazenar(em) instruções executáveis em computador para executar o método como definido na reivindicação 50.

57. Método para gerenciar acesso a uma rede sem fio por um dispositivo terminal, caracterizado pelo fato de compreender as etapas de:

25 a) o dispositivo terminal receber uma primeira chave de um dispositivo confiável da rede sem fio, via um primeiro canal de comunicação;

b) enviar uma requisição para um protocolo de acordo de chave para a rede sem fio;

c) executar o protocolo de acordo de chave para determinar

uma segunda chave correspondente à rede sem fio autenticada usando a primeira chave;

e) transmitir uma requisição para juntar-se à rede sem fio, onde a requisição compreende informação de autenticação com base na segunda
5 chave; e

f) receber confirmação para a requisição de junção.

58. Um ou mais meios legíveis por computador, caracterizado(s) pelo fato de armazenar(em) instruções executáveis em computador para executar o método como definido na reivindicação 57.

10 59. Terminal móvel, caracterizado pelo fato de compreender:

uma memória armazenando instruções executáveis por computador para executar um método para acessar uma rede sem fio, citado método compreendendo as etapas de:

15 a) o dispositivo terminal receber uma primeira chave de um dispositivo confiável da rede sem fio, via um primeiro canal de comunicação;

d) enviar uma requisição para um protocolo de acordo de chave para a rede sem fio;

20 e) executar o protocolo de acordo de chave para determinar uma segunda chave correspondente à rede sem fio autenticada usando a primeira chave;

g) transmitir uma requisição para juntar-se à rede sem fio, onde a requisição compreende informação de autenticação com base na segunda chave; e

h) receber confirmação para a requisição de junção.

25 60. Método para gerenciar acesso a uma rede sem fio por um controlador de acesso, caracterizado pelo fato de compreender as etapas de:

a) transmitir uma primeira chave de autenticação a um dispositivo terminal, via um primeiro canal de comunicação;

b) receber uma requisição para um protocolo de acordo de

chave a partir do dispositivo terminal;

c) executar o protocolo de acordo de chave para determinar uma segunda chave correspondente ao dispositivo terminal, e autenticado usando a primeira chave;

5 d) receber uma requisição do dispositivo terminal para juntar-se à rede sem fio;

e) autenticar a requisição usando a segunda chave; e

f) autorizar o terminal a acessar a rede sem fio usando um segundo canal de comunicação na conclusão bem sucedida da etapa e).

10 61. Um ou mais meios legíveis por computador, caracterizado(s) pelo fato de armazenar(em) instruções executáveis em computador para executar o método como definido na reivindicação 60.

62. Dispositivo de controle de acesso, caracterizado pelo fato de compreender:

15 uma memória armazenando instruções executáveis por computador para executar um método para acessar uma rede sem fio pelo controlador de acesso, citado método compreendendo as etapas de:

a) transmitir uma primeira chave de autenticação a um dispositivo terminal, via um primeiro canal de comunicação;

20 b) receber uma requisição para um protocolo de acordo de chave a partir do dispositivo terminal;

c) executar o protocolo de acordo de chave para determinar uma segunda chave correspondente ao dispositivo terminal, e autenticado usando a primeira chave;

25 d) receber uma requisição do dispositivo terminal para juntar-se à rede sem fio;

e) autenticar a requisição usando a segunda chave; e

f) autorizar o terminal a acessar a rede sem fio usando um segundo canal de comunicação na conclusão bem sucedida da etapa e).

63. Método para um dispositivo confiável gerenciar acesso a uma rede sem fio por um dispositivo terminal não confiável, caracterizado pelo fato de compreender etapas de:

- 5 a) compartilhar uma primeira chave com uma rede sem fio possuindo um controlador de acesso;
- b) escolher um valor para pelo menos uma variável;
- c) gerar uma segunda chave com base em uma função da primeira chave e pelo menos uma variável; e
- 10 d) transmitir a segunda chave ao dispositivo terminal não confiável via um primeiro canal de comunicação.

64. Um ou mais meios legíveis por computador, caracterizado(s) pelo fato de armazenar(em) instruções executáveis em computador para executar o método como definido na reivindicação 63.

65. Terminal móvel, caracterizado pelo fato de compreender:
- 15 uma memória armazenando instruções executáveis por computador para executar um método para acessar uma rede sem fio pelo controlador de acesso, citado método compreendendo as etapas de:

- 20 a) compartilhar uma primeira chave com uma rede sem fio possuindo um controlador de acesso;
- b) escolher um valor para pelo menos uma variável;
- c) gerar uma segunda chave com base em uma função da primeira chave e pelo menos uma variável; e
- d) transmitir a segunda chave ao dispositivo terminal não confiável via um primeiro canal de comunicação.

- 25 66. Método para gerenciar o acesso a uma rede sem fio por um controlador de acesso, caracterizado pelo fato de compreender as etapas de:

- a) compartilhar uma primeira chave com um dispositivo confiável;
- b) receber uma requisição para um protocolo de acordo de

chave de um dispositivo terminal não confiável;

c) executar o protocolo de acordo de chave para determinar uma segunda chave correspondente ao dispositivo terminal, citado protocolo de acordo de chave compreendendo

- 5
 - i. receber uma ou mais variáveis do dispositivo terminal,
 - ii. gerar a segunda chave baseado em uma função da primeira chave e uma ou mais variáveis, e
 - iii. autenticar a segunda chave determinado usando a primeira chave;

10 d) receber uma requisição do dispositivo terminal para juntar-se à rede sem fio;

e) autenticar a requisição da etapa d) usando a segunda chave;

f) autorizar o dispositivo terminal a acessar a rede sem fio na conclusão bem sucedida da etapa e).

15 67. Um ou mais meios legíveis por computador, caracterizado(s) pelo fato de armazenar(em) instruções executáveis em computador para executar o método como definido na reivindicação 66.

68. Dispositivo de controle de acesso, caracterizado pelo fato de compreender:

20 uma memória armazenando instruções executáveis por computador para executar um método para gerenciar o acesso a uma rede sem fio, citado método compreendendo as etapas de:

a) compartilhar uma primeira chave com um dispositivo confiável;

25 b) receber uma requisição para um protocolo de acordo de chave de um dispositivo terminal não confiável;

c) executar o protocolo de acordo de chave para determinar uma segunda chave correspondente ao dispositivo terminal, citado protocolo de acordo de chave compreendendo

- i. receber uma ou mais variáveis do dispositivo terminal,
 - ii. gerar a segunda chave baseado em uma função da primeira chave e uma ou mais variáveis, e
 - iii. autenticar a segunda chave determinado usando a primeira
- 5 chave;
- d) receber uma requisição do dispositivo terminal para juntar-se à rede sem fio;
 - e) autenticar a requisição da etapa d) usando a segunda chave;
 - f) autorizar o dispositivo terminal a acessar a rede sem fio na
- 10 conclusão bem sucedida da etapa e).

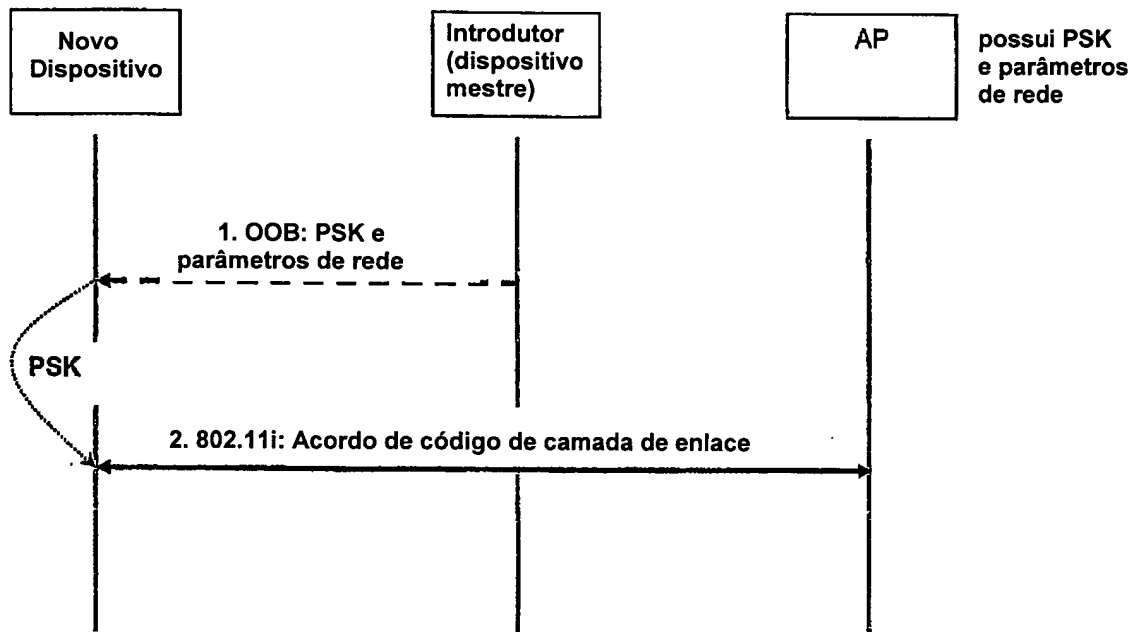


FIG. 1

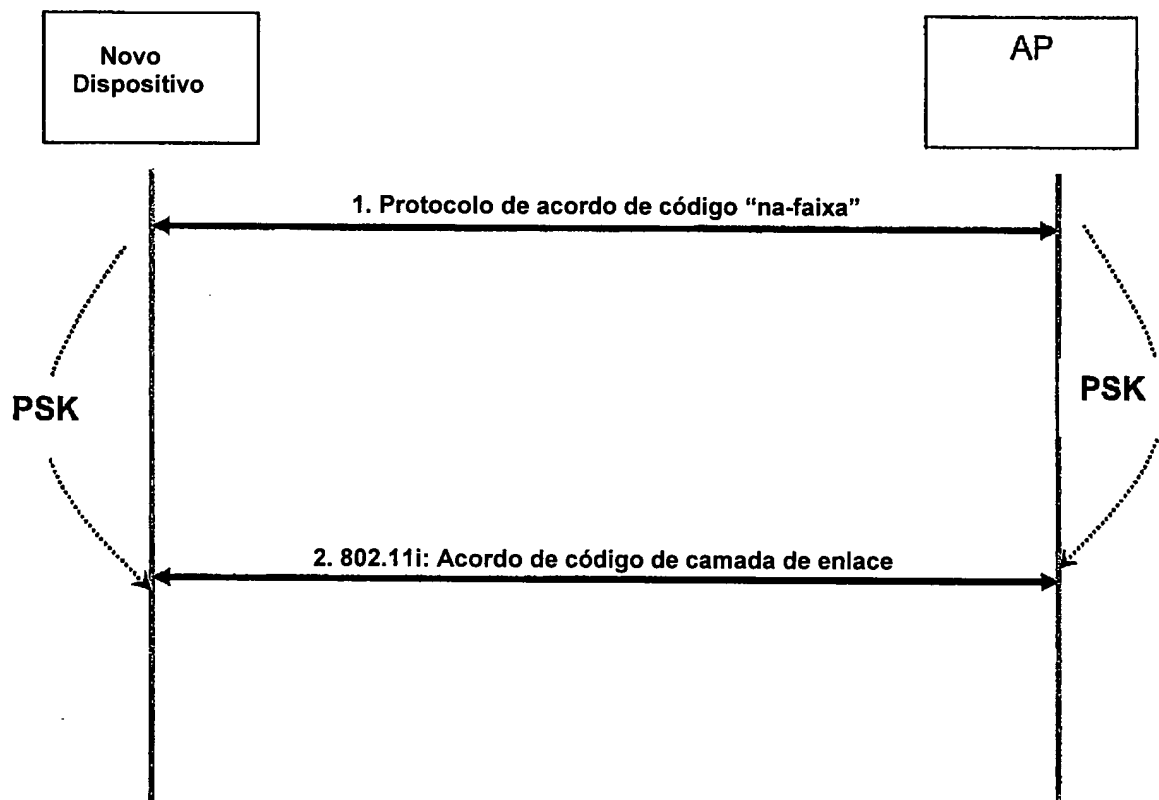


FIG. 2

(Técnica Anterior)

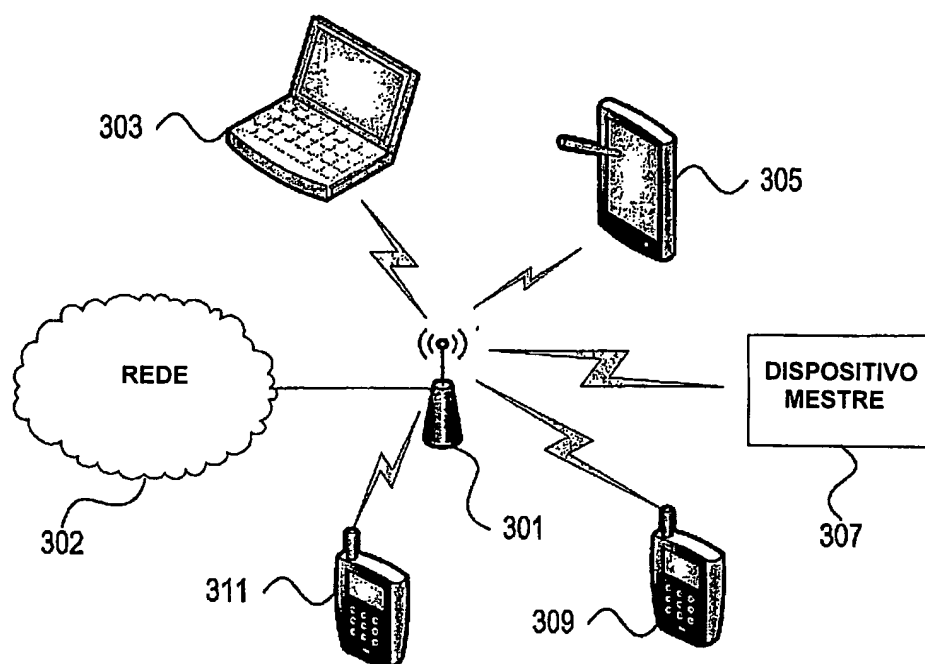


FIG. 3

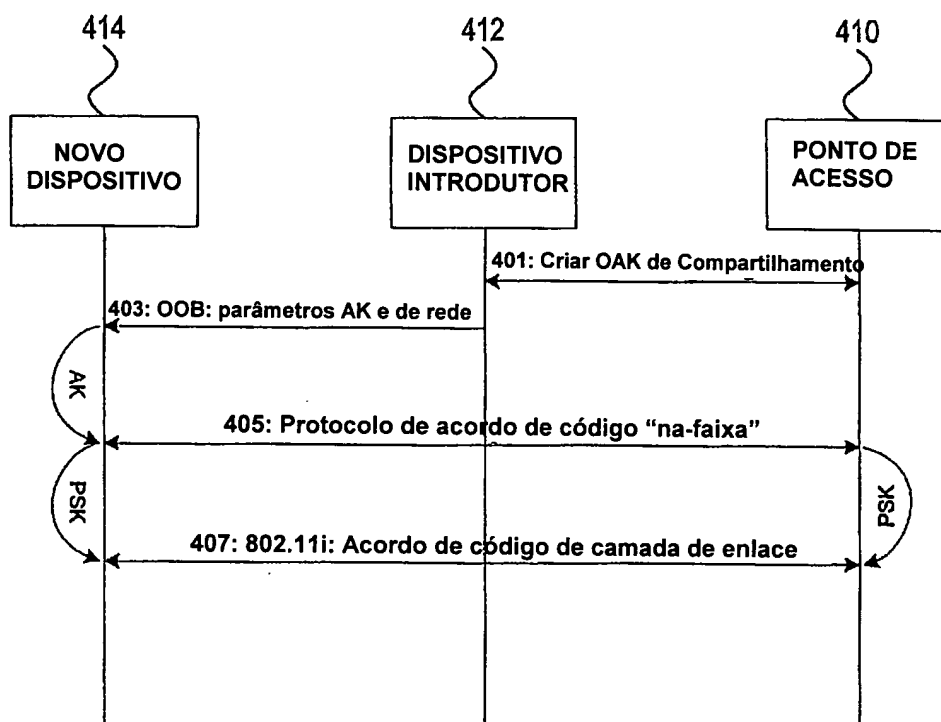


FIG. 4

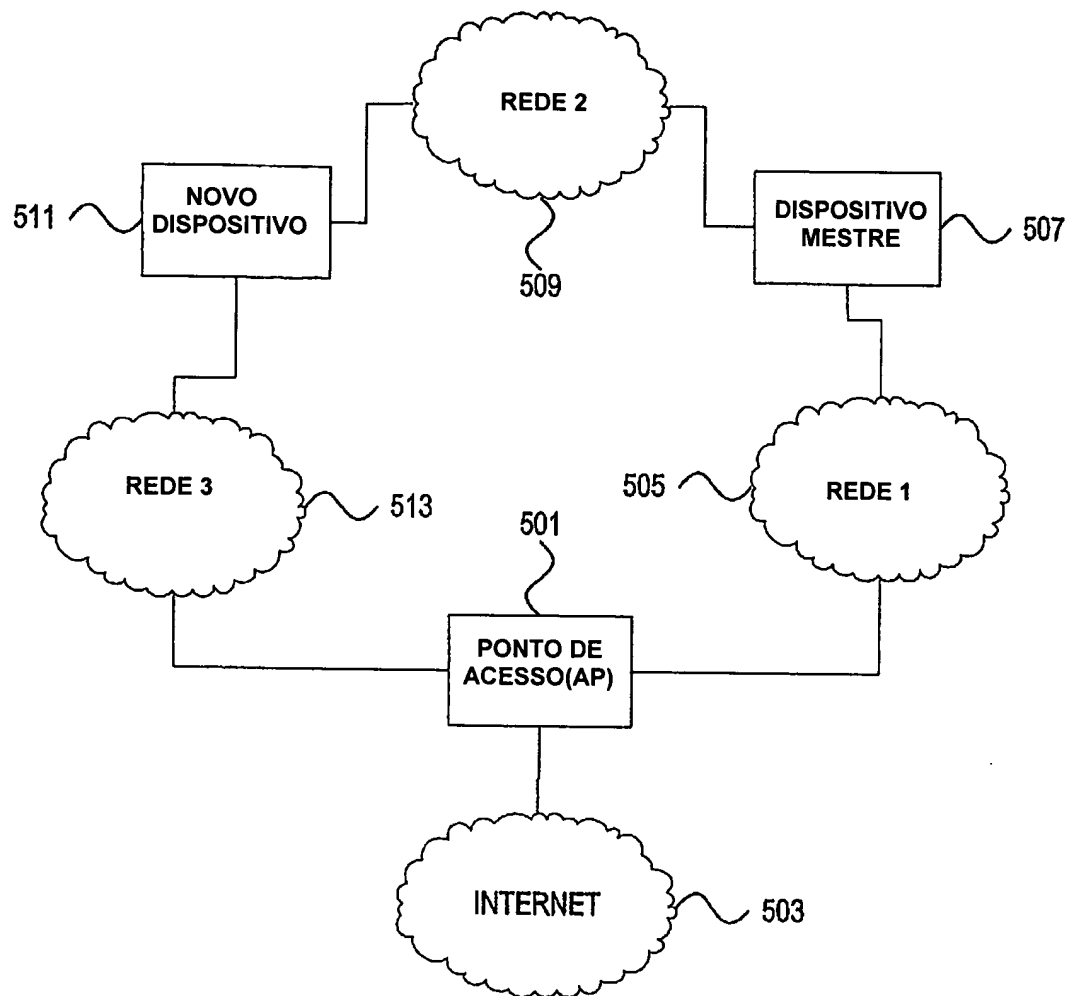


FIG. 5

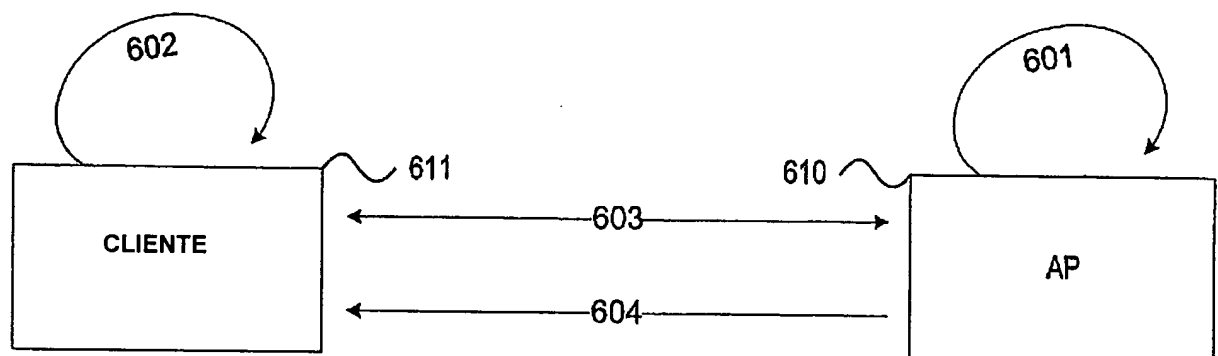


FIG. 6

RESUMO

“MÉTODO PARA GERENCIAR ACESSO A UMA REDE SEM FIO, SISTEMA, UM OU MAIS MEIOS LEGÍVEIS POR COMPUTADOR, TERMINAL MÓVEL, DISPOSITIVO DE CONTROLE DE ACESSO, E,
5 MÉTODO PARA UM DISPOSITIVO CONFIÁVEL GERENCIAR ACESSO A UMA REDE SEM FIO”

São providos métodos e sistemas para gerenciar acesso a uma rede de área local sem fio. Um ponto de acesso sem fio (AP) pode usar uma abordagem unificada que utiliza um canal fora-da-banda para comunicar
10 informação de chave de autenticação e endereço de rede a um dispositivo convidado, e utiliza um canal em-banda para estabelecer comunicações com o dispositivo convidado, e também provê suporte para configuração em-banda em todos os dispositivos. A capacidade de usar fora-da-banda onde possível provê um aumento de segurança e usabilidade, e a possibilidade de delegar
15 acesso de um dispositivo para outro. A abordagem unificada deste modo provê também gerenciamento fácil de acesso de convidado à WLAN.