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

(11) PI 0313412-1 B1

(22) Data do Depósito: 13/08/2003

(45) Data de Concessão: 21/03/2017

(54) Título: GERENCIAMENTO DE CHAVE DE SESSÃO PARA LAN PÚBLICA SEM FIO SUPORTANDO MÚLTIPLOS OPERADORES VIRTUAIS

(51) Int.Cl.: H04L 9/08; H04L 29/06; H04W 84/12; H04W 12/06; H04W 76/02; H04W 74/00; H04W 12/04; H04W 88/08; H04W 48/18

(52) CPC: H04L 9/0844,H04L 63/18,H04W 84/12,H04W 12/06,H04W 76/02,H04W 74/00,H04W 12/04, H04L 2209/80,H04L 63/08,H04W 88/08,H04W 48/18,H04L 63/06

(30) Prioridade Unionista: 14/08/2002 US 60/403.495

(73) Titular(es): THOMSON LICENSING S.A.

(72) Inventor(es): JUNBIAO ZHANG

"GERENCIAMENTO DE CHAVE DE SESSÃO PARA LAN PÚBLICA SEM FIO SUPORTANDO MÚLTIPLOS OPERADORES VIRTUAIS"

CAMPO DA INVENÇÃO

A presente invenção em geral refere-se a comunicações de rede e, mais particularmente, a um mecanismo para gerenciar acesso a chaves de sessão em um ambiente público de rede local sem fio (WLAN) que suporta operadores virtuais terceirizados.

FUNDAMENTOS DA TÉCNICA

Soluções de Contabilidade, Autorização, Autenticação (AAA) de rede local sem fio (WLAN) corrente não fornecem suporte adequado para operadores de WLAN para manter relações comerciais com múltiplos operadores virtuais, e em particular, com relação a gerenciamento de chaves de sessão usadas para acesso de WLAN. Falha em controlar e gerenciar as chaves de sessão poderia resultar em problemas de segurança potencial e gerenciamento.

WLANs estão cada vez mais sendo desenvolvidas em pontos ativos tais como hotéis, aeroportos e cafés. Uma solução de AAA (contabilidade, Autorização, Autenticação) confiável e eficiente seria de grande importância para permitir acesso público seguro de LAN sem fio. Em particular, tal solução de AAA deve ser capaz de suportar um conceito de operador virtual em que provedores terceirizados tais como ISPs, operadoras de celular e provedores de cartão pré-pago oferecem serviços de AAA para WLANs públicas e usuários sem fio. Desta maneira, usuários sem fio não têm que abrir uma conta ou pagar por crédito cada vez que se dirigem a um pon-

to ativo diferente; em vez disto, eles pode usar contas de ISP existentes, contas de celular ou um cartão pré-pago adquirido em qualquer lugar para ter acesso a WLAN pública. Isto poderia significantemente aumentar as oportunidades comerciais para os operadores de WLAN bem como operadores virtuais terceirizados. No entanto, as soluções de acesso de LAN sem fio corrente são todas designadas para configurações locais tais como um ambiente corporativo em que somente um único servidor de autenticação é usado. Por exemplo, o corpo de padrão IEEE 802.11 escolhe IEEE 802.1x como a solução para controle de acesso de WLAN, e os modelos de uso corrente utilizam servidores de autenticação para controlar a s atribuições de chave de sessão. Enquanto isto é suficiente para um ambiente corporativo ou similar, é certamente problemático em ponto ativo público onde múltiplos servidores de autenticação que pertencem a entidades comerciais diferentes podem coexistir. É muito difícil, se de todo possível, para estes servidores de autenticação coordenar atribuições de chave para um ponto de acesso.

Distribuições de chave correntes serão agora descritas. Em um cenário, um usuário de móvel em um ponto ativo público de WLAN não tem uma relação de confiança anterior com o ponto de acesso de WLAN. O usuário pretende usar um provedor de serviço terceirizado (por exemplo, um provedor de serviço de Internet (ISP)) como uma entidade de ponte de confiança. Um provedor de serviço pode ser referido como um operador virtual. O usuário mantém uma conta com este operador virtual, que tem uma relação comercial com o operador de

WLAN. Porque o usuário tem uma relação de confiança estabelecida com o operador virtual, ele é capaz de autenticar-0se com o operador virtual em uma maneira segura. O operador virtual então transmite com segurança uma chave de sessão para o usuário bem como ao ponto de acesso de WLAN (porque o operador virtual também tem uma relação de confiança com a WLAN). Devido a esta chave de sessão compartilhada, a LAN sem fio então conhece que o usuário é autorizado a acessar a rede e assim garante acesso ao usuário. Note que neste esquema, o operador virtual cede a chave de sessão desde que tenha uma relação de confiança com o usuário e a WLAN.

A chave de sessão é usada para acesso local e deve ser local ao ponto de acesso de WLAN, por exemplo cedido e mantido pelo ponto de acesso. Quando múltiplos operadores virtuais estão presentes, o esquema de gerenciamento de chave mencionado acima é problemático em pelo menos duas áreas. Primeiro, para o operador virtual, é freqüentemente problemático para ceder e gerenciar chaves de sessão para dezenas de milhares de pontos de acesso pertencendo a entidades diferentes, isto é, para acomodar algoritmos de criptografia diferentes e comprimentos de chave para tipos diferentes de pontos de acesso. Em segundo lugar, para o ponto de acesso, pode ser difícil certificar-se de que múltiplos operadores virtuais cedem chaves de sessão em uma maneira consistente, por exemplo tem que se certificar que dois usuários não estão usando a mesma chave cedida por dois operadores virtuais diferentes ao mesmo tempo.

Uma dificuldade chave é que o ponto de acesso não

compartilha um segredo com o usuário sem fio, assim não é seguro enviar diretamente uma chave de sessão do ponto de acesso para o usuário. Em uma solução para este problema é que o operador virtual notifica o ponto de acesso (AP) sobre a chave pública do usuário em autenticação de usuário bem sucedida. O AP então criptografa a chave de sessão usando a chave pública do usuário e então envia o resultado ao usuário. Desde que somente que o usuário específico é capaz de decriptografar a chave de sessão usando sua chave privada correspondente, a chave de sessão pode ser estabelecida com segurança entre o AP e o usuário sem fio. No entanto, este esquema exige o uso de chaves pública/privada, que pode não ser compatível com os métodos de autenticação atuais entre o usuário sem fio e o servidor de autenticação. É provável que o usuário tem que manter dois tipos diferentes de chaves (chave privada para decriptografar a chave de seção e chave do tipo senha para autenticar com o servidor de autenticação). Isto não somente aumenta a complexidade de software de cliente, mas também aumenta a dificuldade em manter com segurança as chaves. Adicionalmente, este esquema não funciona com IEEE 802.1x, que está se tornando um padrão em segurança de WLAN.

Portanto, existe uma necessidade para uma solução em que as chaves são atribuídas e gerenciadas localmente por um ponto de acesso, ainda usuários sem fio são capazes de obter com segurança a chave de sessão sem uma relação de confiança anterior com o ponto de acesso.

SUMÁRIO DA INVENÇÃO

A invenção descreve um mecanismo eficaz e eficiente para endereçar este problema. As chaves de sessão são atribuídas e gerenciadas localmente pelas chaves de WLAN (desde que estas chaves são usadas para controle de acesso local), ainda podem ser distribuídas com segurança para os usuários sem fio que somente mantêm uma relação de confiança com seus operadores virtuais correspondentes.

Um método para gerenciamento de chave de sessão para redes locais sem fio inclui estabelecer um primeiro canal seguro entre um ponto de acesso e um operador virtual, e sugerir uma chave de seção para o operador virtual do ponto de acesso. Um segundo canal de segurança é estabelecido entre o operador virtual e um usuário, e a chave de sessão é enviada pelo operador virtual para permitir comunicações entre o ponto de acesso e o usuário.

Um sistema para gerenciamento de chave de sessão para redes locais sem fio inclui um ponto de acesso, que estabelece um primeiro canal seguro entre o ponto de acesso e um operador virtual. Uma chave de sessão é sugerida ao operador virtual a partir do ponto de acesso. O operador virtual estabelece um segundo canal seguro entre ele e um usuário na autenticação do usuário, o operador virtual ajustando a chave de sessão para permitir comunicações entre o ponto de acesso e o usuário.

BREVE DESCRIÇÃO DOS DESENHOS

As vantagens, natureza e vários aspectos adicionais da invenção parecerão mais completamente na considera-

ção das modalidades ilustrativas a serem descritas agora em detalhe em conexão com os desenhos anexos em que:

a Figura 1 é um sistema exemplar de acordo com uma modalidade da presente invenção;

a Figura 2 é um fluxograma de etapas ilustrativas para implementar o método para gerenciamento de chave de sessão de acordo com uma modalidade da presente invenção; e

a Figura 3 é um diagrama de outro método ilustrativo para gerenciamento de chave de sessão para redes locais sem fio de acordo com outra modalidade da presente invenção.

Deve ser entendido que os desenhos são para propósitos de ilustrar os conceitos da invenção e não são necessariamente a única configuração possível para ilustrar a invenção.

DESCRIÇÃO DETALHADA DA INVENÇÃO

A presente invenção em geral se refere a comunicações de rede e, mais particularmente, a um mecanismo para gerenciar as chaves de sessão de acesso em um ambiente público de rede local sem fio (WLAN) que suporta operadores virtuais terceirizados. Tais operadores virtuais podem incluir Provedores de Serviço de Internet (ISPs), operadoras de celular, ou provedores de cartão pré-pago. Para maximizar fontes de receita, uma rede local sem fio (WLAN) pública pode manter a relação comercial com múltiplos operadores virtuais.

É para ser entendido que a presente invenção é descrito em termos de sistemas de WLAN, tais como aqueles que cumpre,m com os padrões IEEE 802.11, Hiperplan 2, e/ou

banda ultra-larga; no entanto, a presente invenção é muito mais ampla e pode ser aplicável a outros esquemas de gerenciamento de sistema para outros sistemas de comunicações. Em adição, a presente invenção pode ser aplicável a qualquer sistema de rede incluindo telefone, cabo, computador (Internet), satélite, etc.

Referindo-se agora em detalhe específico aos desenhos em que numerais de referência iguais identificam elementos similares ou idênticos por todas as várias vistas, e inicialmente a Figura 1, uma rede local sem fio (WLAN) 14 inclui um ponto de acesso 30 para um ponto ativo de WLAN 31. WLAN 14 pode empregar, por exemplo padrões de IEEE 802.11 e HIPERLAN2. WLAN 14 pode incluir uma barreira de proteção 22 entre redes externas, tal como, por exemplo, a Internet 7. Usuários finais ou unidades móveis 40 podem acessar operadores virtuais 62 da WLAN 14 através da Internet 7 usando, por exemplo, túneis HTTPS ou outros canais seguros 64, como será descrito aqui.

Disperso entre ou dentro de células de uma rede celular são redes locais sem fio 14. De acordo com a presente invenção, uma chave de sessão 60 é enviada de um operador virtual 62 a um usuário 40. Operadores virtuais 62 podem incluir Provedores de Serviço de Internet (ISPs), operadoras de celular, ou provedores de cartão pré-pago ou outras entidades, que fornecem serviços sobre uma rede de comunicações. Para maximizar fontes de receita, uma rede local sem fio (WLAN) pública pode manter relação comercial com os múltiplos operadores virtuais. No entanto, mantendo uma plurali-

dade de operadores virtuais é difícil enquanto mantém a segurança de sistema adequada.

Porque o operador virtual 62 e o usuário (MS 40) compartilham um segredo, tal como um canal seguro ou usando um pedaço de informação ou código compartilhado, a chave 60 pode ser transmitida através de um canal seguro 64 entre eles. No entanto, em vez de ter o operador virtual 62 determinando e mantendo a chave de sessão 60, as chaves são escolhidas por pontos de acesso de WLAN 30 e então sugeridas ao operador virtual. As chaves podem ser escolhidas por uma pluralidade de métodos, incluindo, por exemplo, geração de número randômico, selecionado de um número pré-armazenado de chaves, etc.

Referindo-se à Figura 2, uma modalidade para implementar a presente invenção é ilustrativamente descrita como se segue. No bloco 102, um usuário (terminal móvel (MT)) solicita acesso de LAN sem fio em um ponto de acesso (AP) 30 e especifica um operador virtual (VO) 62. No bloco 104, o AP 30 estabelece um canal seguro SC_1 com o operador virtual 62. Toda a comunicação subseqüente entre o AP 30 e o operador virtual 62 será através de SC_1. No bloco 106, o usuário estabelece um canal seguro SC_2 com o operador virtual 62 e se autentica com o operador virtual através de SC_2. Isto pode incluir colocar a chave de sessão em espera até a autenticação de usuário bem sucedida.

No bloco 108, o operador virtual, na autenticação de usuário bem sucedida, notifica o AP 30 sobre o resultado e requer ao AP 30 uma chave de sessão 60 através de SC_1. Se a

chave de sessão está em espera, pode ser removida da espera se a autenticação não é bem sucedida. No bloco 110, o AP 30 escolhe uma chave de sessão 60 e envia para o operador virtual 62 através de SC_1. No bloco 112, o operador virtual envia esta chave de sessão para o usuário através de SC_2. No bloco 114, o usuário e o AP 30 começa usando a chave de sessão para a comunicação subseqüente entre eles (canal seguro SC_3).

Referindo-se à figura 3, o método como mostrado na Figura 2 pode ser ainda aperfeiçoado para velocidade e eficiência como ilustrado. Em vez de o operador virtual requerer a chave de sessão depois da autenticação bem sucedida, o AP 30 fornece uma chave de sessão sugerida logo depois de SC_1 é estabelecida e coloca esta chave "em espera" na memória 24 no ponto de acesso 30. Na autenticação de usuário bem sucedida, o AP 30 é notificado pelo operador virtual e começa usando esta chave para SC_3. No caso de uma autenticação bem sucedida (por exemplo, depois de um certo número de tentativas mal sucedidas pelo usuário), o AP 30 é também notificado e remove a chave da lista "em espera" 24. Isto impede o ataque de negativa de serviço em que um atacante faz continuamente tentativas de autenticação mal sucedidas. Se o AP não é notificado sobre a autenticação mal sucedida, as chaves sugeridas empilhariam no armazenamento de memória do AP. As etapas de autenticação podem incluir o seguinte.

Na etapa 202, um usuário solicita o acesso de LAN sem fio em um AP 30 e especifica o operador virtual 62. Na etapa 204, AP 30 estabelece um canal seguro SC_1 com o operador virtual 62. Toda a comunicação subseqüente entre o AP e

o operador virtual será através de SC_1. Na etapa 206, o AP envia uma chave de sessão sugerida ao operador virtual 62 e coloca esta chave "em espera". Na etapa 208, o usuário estabelece um canal seguro SC_2 com o operador virtual 62 e autentica-se com o operador virtual 62 através de SC_2 no bloco 209. Na etapa 210, o operador virtual 62 notifica o AP 30 sobre o resultado da autenticação, e o AP 30 remove a chave sugerida da lista de "em espera". No bloco 212, no caso de autenticação bem sucedida, o operador virtual 62 envia a chave de sessão para o usuário. No bloco 214, o usuário e o AP 30 começa usando a chave de sessão para a comunicação subseqüente entre eles (canal seguro SC_3).

A razão que o método da Figura 3 é mais eficiente porque economiza uma viagem de ida e volta de tempo de comunicação do método da Figura 2, por exemplo, o operador virtual não tem que esperar até o fim da autenticação, para requerer o APO para a chave de sessão, então notificar o usuário sobre a chave, pode ser feito em paralelo com a etapa 208. Assim, um retardo de viagem de ida e volta total é evitado. Em outras modalidades a etapa 206, pode ser realizada seqüencialmente com a etapa 208.

É para ser entendido que a presente invenção pode ser implementada em várias formas de hardware, software, firmware, processadores de propósito especial, ou uma combinação do mesmo, por exemplo, dentro de um terminal móvel, ponto de acesso, e/ou uma rede de celular. De preferência, a presente invenção é implementada como uma combinação de hardware e software. Além do mais, o software é de preferên-

cia implementado como um programa de aplicação de modo tangível incorporado em um dispositivo de armazenamento de programa. O programa de aplicação pode ser descarregado a, e executado por, uma máquina compreendendo qualquer arquitetura adequada. De preferência, a máquina é implementada em uma plataforma de computador tendo um hardware tal como uma ou mais unidades de processamento central (CPU), uma memória de acesso randômico (RAM), e interface(s) de entrada/saída (I/O). A plataforma de computador também inclui um sistema de operação e código de microinstrução. Os vários processos e funções descritos aqui podem tanto ser parte do código de microinstrução ou parte do programa de aplicação (ou uma combinação dos mesmos), que é executado por meio do sistema de operação. Em adição, vários outros dispositivos periféricos podem ser conectados à plataforma de computador tal como um dispositivo de armazenamento de dados adicional e um dispositivo de impressão.

É para ser entendido que, porque alguns dos componentes de sistema constituintes e etapas de método descritos nas Figuras anexas podem ser implementados no software, as conexões atuais entre os componentes do sistema (ou etapas do processo) podem diferir dependendo da maneira em que a presente invenção é programada. Dado os ensinamentos aqui, alguém versado na técnica relacionada será capaz de considerar estas e outras implementações e configurações da presente invenção.

Tendo descrito as modalidades preferidas para o gerenciamento de chave de sessão para LAN sem fio pública

suportando múltiplos operadores virtuais (que pretendem ser ilustrativos e não limitantes), nota-se que modificações e variações podem ser feitas por pessoas versadas na técnica à luz dos ensinamentos acima. É portanto para ser entendido que mudanças podem ser feitas nas modalidades particulares da invenção descrita, que estão dentro do escopo e espírito da invenção quando delineado pelas reivindicações anexas. Tendo assim descrito a invenção com os detalhes e particularidade exigidos pelas leis de patente, o que é reivindicado e desejado, protegido pelas Cartas Patente é descrito nas reivindicações anexas.

REIVINDICAÇÕES

1. Método para gerenciar uma chave de sessão usada para permitir comunicações entre um terminal móvel (40) e um ponto de acesso (30) em uma rede local sem fio “WLAN” (31), **CARACTERIZADO** pelo fato de compreender as etapas de:

Receber (102) uma solicitação para acessar a WLAN (31) a partir do terminal móvel;

Determinar (102) um operador virtual associado com a solicitação de acesso;

Estabelecer (104) um primeiro canal seguro entre o ponto de acesso (30) e o operador virtual;

Solicitar (106) autenticação do usuário do operador virtual por meio do primeiro canal seguro, onde o operador virtual se comunica com o terminal móvel (40) por meio de um segundo canal seguro para autenticar o terminal móvel;

Selecionar (110) uma chave de sessão e enviar a chave de sessão para o operador virtual por meio do primeiro canal seguro (110), onde o operador virtual envia (112) a chave de sessão para o terminal móvel (40) por meio do segundo canal seguro; e

Comunicar (114) com o terminal móvel (40) usando a chave de sessão.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a etapa de solicitar autenticação de usuário (106) é realizada em paralelo com a etapa de selecionar (110) e enviar a chave de sessão.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a etapa de comunicação (114)

compreende comunicar-se com o terminal móvel (40) usando a chave de sessão ao receber a notificação de autenticação de usuário bem sucedida do operador virtual.

4. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a etapa de selecionar uma chave de sessão (110) compreende colocar a chave de sessão em espera até a notificação da autenticação de usuário bem sucedida do operador virtual, e na notificação remover a chave de sessão da espera e enviar a chave de sessão ao operador virtual.

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** adicionalmente pelo fato de compreender a etapa de remover a chave de sessão da espera se a autenticação for bem sucedida.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a etapa de selecionar (110) uma chave de sessão e enviar a chave de sessão para o operador virtual por meio do primeiro canal seguro é realizada somente depois de receber a notificação de autenticação de usuário bem sucedida do operador virtual.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o operador virtual inclui um de um Provedor de Serviço de Internet, um provedor de celular e um provedor de cartão de crédito.

8. Aparelho para gerenciar uma chave de sessão usada para permitir comunicações entre um terminal móvel (40) e uma rede local sem fio WLAN (31), **CARACTERIZADO** pelo fato de compreender:

um dispositivo para receber (102) uma solicitação para acessar a WLAN (31) a partir do terminal móvel (40);

um dispositivo para determinar (102) um operador virtual associado à solicitação de acesso;

um primeiro dispositivo para se comunicar com o operador virtual por meio de um primeiro canal seguro, o primeiro dispositivo de comunicação solicitando (106) a autenticação de usuário do operador virtual por meio do primeiro canal seguro, onde o operador virtual se comunica com o terminal móvel (40) por meio de um segundo canal seguro para autenticar o terminal móvel (40);

um dispositivo, acoplado ao primeiro dispositivo de comunicação, para selecionar (110) uma chave de sessão e enviar a chave de sessão para o operador virtual por meio do primeiro canal seguro, onde o operador virtual envia (110) a chave de sessão para o terminal móvel (40) por meio do segundo canal seguro; e

um segundo dispositivo para se comunicar (114) com o terminal móvel (40) usando a chave de sessão.

9. Aparelho, de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o primeiro dispositivo de comunicação solicita autenticação de usuário em paralelo com o dispositivo de selecionar selecionando e enviando a chave de sessão.

10. Aparelho, de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que o segundo dispositivo de comunicação se comunica com o terminal móvel (40) usando a

chave de sessão ao receber a notificação de autenticação de usuário bem sucedida do operador virtual.

11. Aparelho, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o dispositivo de seleção coloca a chave de sessão em espera até a notificação de autenticação de usuário bem sucedida do operador virtual, e na notificação remove a chave de sessão da espera e envia a chave de sessão para o operador virtual.

12. Aparelho, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que o dispositivo de seleção remove a chave de sessão da espera se a autenticação for bem sucedida.

13. Aparelho, de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o dispositivo de seleção seleciona uma chave de sessão e envia a chave de sessão para o operador virtual por meio do primeiro canal seguro somente depois de receber a notificação de autenticação de usuário bem sucedida do operador virtual.

14. Aparelho, de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o operador virtual inclui um de um Provedor de Serviço de Internet, um provedor de celular, e um provedor de cartão de crédito.

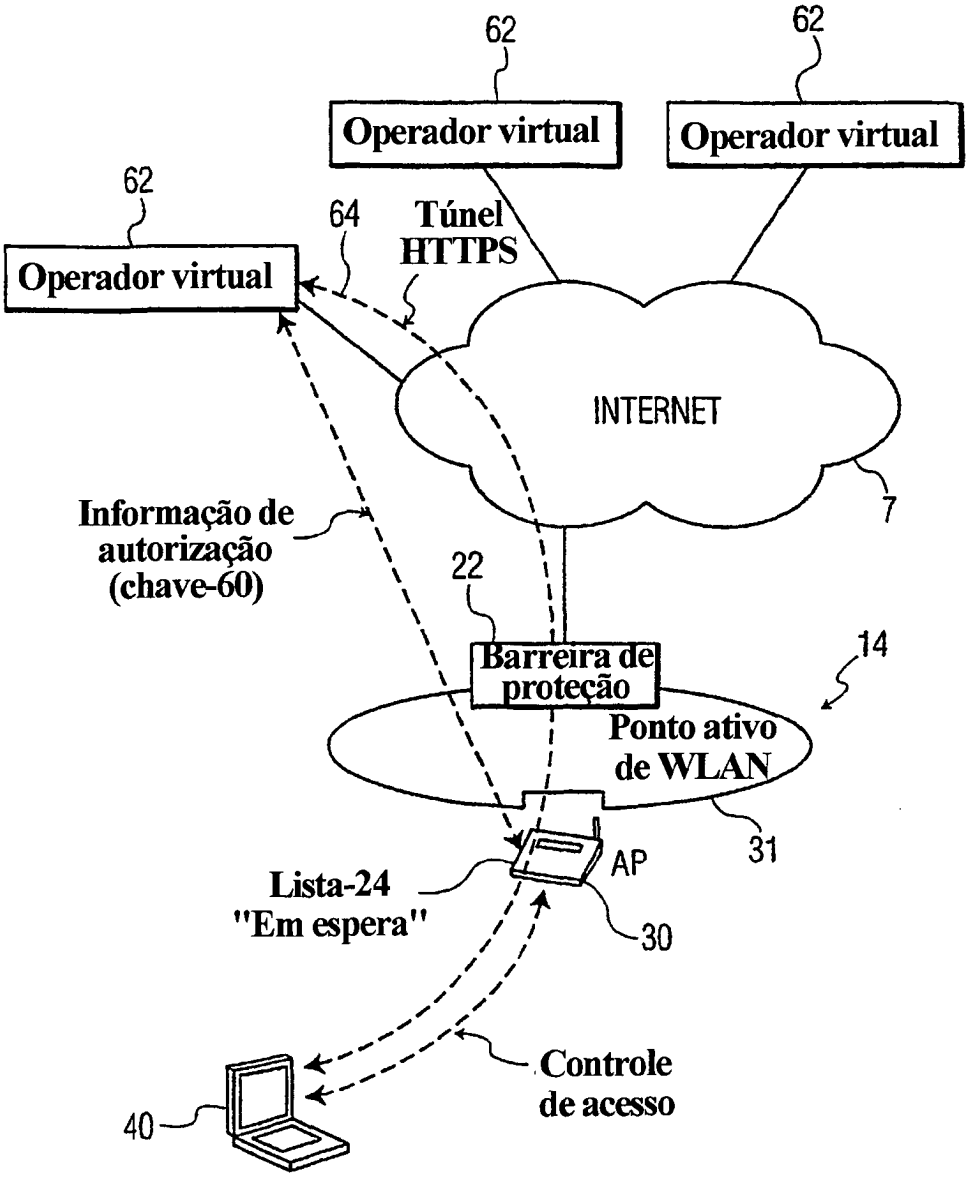
62
62
Operador virtual
Operador virtual
62
64
Túnel
HTTPS
Operador virtual
INTERNET
7
Informação de
autorização
(chave-60)
22
Barreira de
proteção
14
Ponto ativo
de WLAN
31
AP
Lista-24
"Em espera"
30
Controle
de acesso
40

FIG. 1

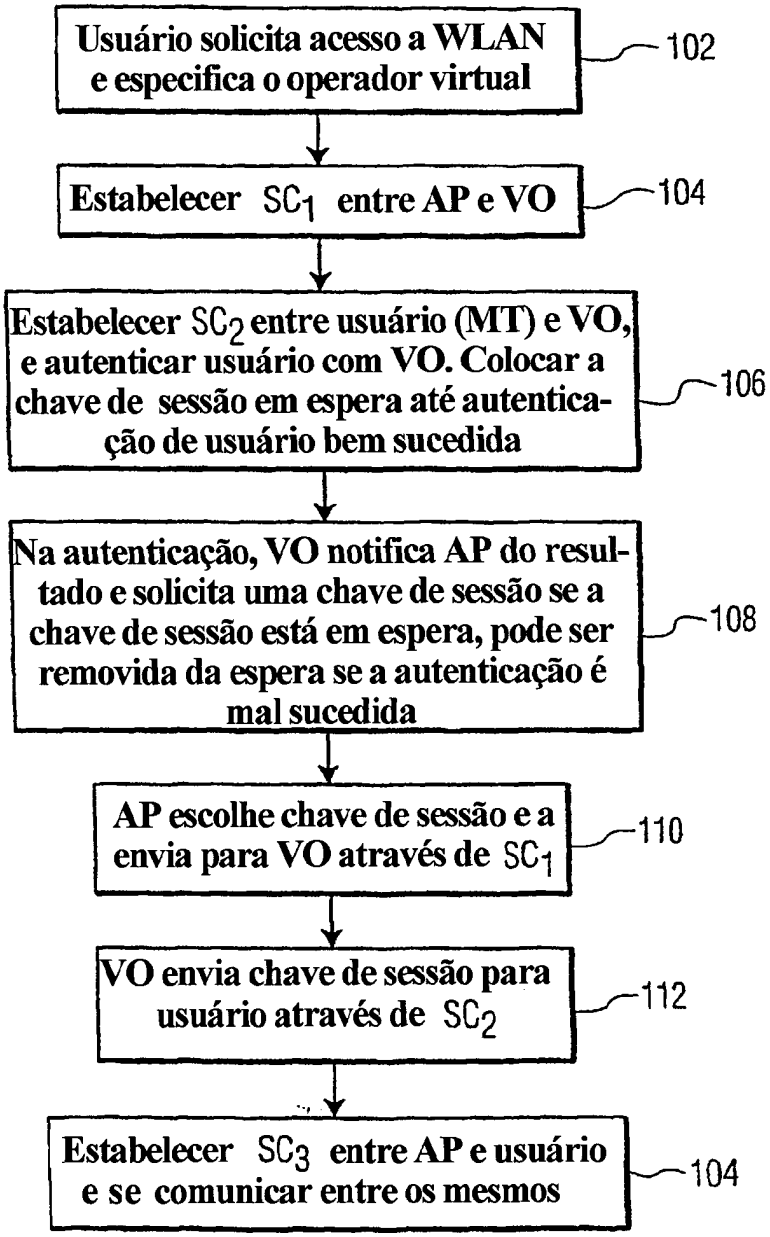
Usuário solicita acesso a WLAN e especifica o operador virtual
102
Estabelecer SC_1 entre AP e VO
104
Estabelecer SC_2 entre usuário (MT) e VO, e autenticar usuário com VO. Colocar a chave de sessão em espera até autenticação de usuário bem sucedida
106
Na autenticação, VO notifica AP do resultado e solicita uma chave de sessão se a chave de sessão está em espera, pode ser removida da espera se a autenticação é mal sucedida
108
AP escolhe chave de sessão e a envia para VO através de SC_1
110
VO envia chave de sessão para usuário através de SC_2
112
Estabelecer SC_3 entre AP e usuário e se comunicar entre os mesmos
104

FIG. 2

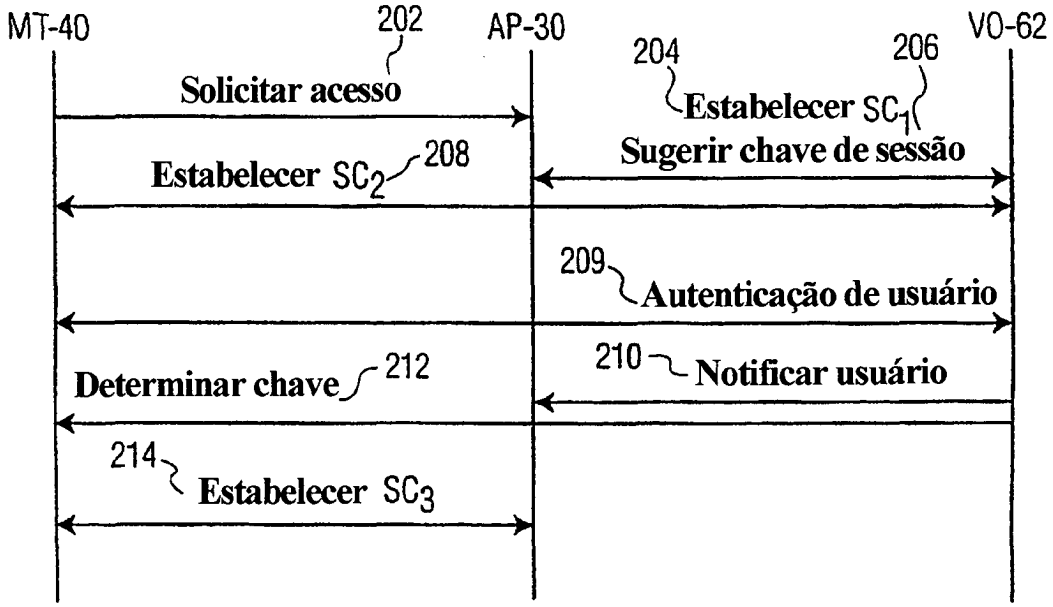
MT-40
202
AP-30
204
206
VO-62
Solicitar acesso
Estabelecer SC1
Sugerir chave de sessão
Estabelecer SC2
208
209
Autenticação de usuário
Determinar chave
212
210
Notificar usuário
214
Estabelecer SC3

FIG. 3

RESUMO

"GERENCIAMENTO DE CHAVE DE SESSÃO PARA LAN PÚBLICA SEM FIO SUPORTANDO MÚLTIPLOS OPERADORES VIRTUAIS"

Um método e aparelho para gerenciar uma chave de sessão para permitir que um terminal móvel acesse uma rede local sem fio (WLAN). A invenção prepara-se para estabelecer um primeiro canal seguro entre um ponto de acesso e um operador virtual, e sugerir uma chave de sessão para o operador virtual a partir do ponto de acesso. Um segundo canal seguro é estabelecido entre o operador virtual e um usuário, e a chave de sessão é enviada para o usuário por meio do segundo canal seguro na autenticação de usuário bem sucedida. O terminal móvel acessa a WLAN usando a chave de sessão.