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

(11) PI 0711079-0 B1

BRPI0711079B1

(22) Data do Depósito: 17/04/2007

(45) Data de Concessão: 08/10/2019

(54) Título: MÉTODOS PARA FORNECER COMUNICAÇÃO SEGURA ENTRE DISPOSITIVOS AD-HOC E PARA OPERAÇÃO DE UM DISPOSITIVO DE COMUNICAÇÃO E DISPOSITIVO DE COMUNICAÇÃO DE MODO DUAL

(51) Int.Cl.: H04L 9/08; H04L 29/06; H04W 12/06; H04W 84/18; H04W 92/02.

(52) CPC: H04L 9/0822; H04L 9/0825; H04L 9/0833; H04L 63/065; H04L 63/08; (...).

(30) Prioridade Unionista: 28/04/2006 US 11/380.809.

(73) Titular(es): MOTOROLA SOLUTIONS, INC.; PURDUE UNIVERSITY.

(72) Inventor(es): JEFFREY D. BONTA; HONG YON LACH; BHARAT BHARGAVA; XIAOXIN WU.

(86) Pedido PCT: PCT US2007066755 de 17/04/2007

(87) Publicação PCT: WO 2007/127637 de 08/11/2007

(85) Data do Início da Fase Nacional: 28/10/2008

(57) Resumo: MÉTODO E SISTEMA PARA FORNECER COMUNICAÇAO SEGURA AUXILIADA POR TELEFONES CELULARES DE UMA PLURALIDADE DE DISPOSITIVOS AD-HOC Um método para fornecer comunicação segura entre uma pluralidade de dispositivos ad-hoc inclui autenticar um ou mais primeiros dispositivos dentro de uma primeira rede; autenticar um o mais segundos dispositivos dentro de uma segunda rede; transmitir uma chave de grupo para os primeiros dispositivos autenticados e para os segundos dispositivos autenticados; estabelecer uma rede ad-hoc por pelo menos um dos primeiros dispositivos autenticados e pelo menos um dos segundos dispositivos autenticados utilizando a chave de grupo; e comunicar dentro da rede ad- hoc entre o pelo menos um dos primeiros dispositivos autenticados e o pelo menos um dos segundos dispositivos autenticados.

MÉTODOS PARA FORNECER COMUNICAÇÃO SEGURA ENTRE DISPOSITIVOS AD-HOC E PARA OPERAÇÃO DE UM DISPOSITIVO DE COMUNICAÇÃO E DISPOSITIVO DE COMUNICAÇÃO DE MODO DUAL

CAMPO DA INVENÇÃO

A presente invenção relaciona-se genericamente a sistemas de comunicação sem fio e, em particular, a comunicação segura entre uma pluralidade de dispositivos de comunicação *ad-hoc*.

HISTÓRICO

Uma rede sem fio com base em infra-estrutura tipicamente inclui uma rede de comunicação com portais fixos e fiados. Muitas redes sem fio com base na infra-estrutura empregam uma unidade móvel ou hospedeiro que se comunica com uma estação base fixa que é acoplada a uma rede fiada. A unidade móvel pode deslocar-se geograficamente enquanto ela estiver se comunicando por um enlace sem fio com a estação base. Quando a unidade móvel se desloca para fora do alcance de uma estação base, ela poderá conectar ou "transferir" para uma nova estação base e inicia a comunicação com a rede fiada através da nova estação base.

Em comparação com as redes sem fio com base na infra-estrutura, essas redes celulares ou redes de satélite, redes *ad-hoc* são redes auto-formadas que podem operar na ausência de qualquer infra-estrutura fixa, e em alguns casos a rede *ad-hoc* é formada inteiramente de nós móveis. Uma rede *ad-hoc* tipicamente inclui um número de unidades potencialmente móveis distribuídas geograficamente, às vezes referidas como "nós", que são conectadas de modo sem fio uma a outra por um ou mais enlaces (por exemplo, canais

de comunicação de freqüência de rádio). Os nós podem comunicar uns com os outros por uma mídia sem fio sem o suporte de uma rede fiada ou com base na infra-estrutura. Enlaces ou conexões entre esses nós podem mudar dinamicamente de maneira arbitrária à medida que os nós existentes se deslocam dentro da rede *ad-hoc*, à medida que novos nós participam ou entram na rede *ad-hoc*, ou à medida que os nós existentes deixam ou saem da rede *ad-hoc*.

Recentemente houve um interesse crescente na integração de redes sem fio. Exemplos de redes integradas incluem Advanced Mobile Phone Service (AMPS - Serviço de Telefonia Móvel Avançado) combinado com redes celulares IS-95, Global Positioning System (GPS - Sistema de Posicionamento Global) aplicado em redes celulares, redes combinadas de satélite e celular, e rede combinada celular e de área local sem fio (LAN).

Recentemente, a integração de redes celulares e redes *ad-hoc* também vem ganhando interesse. Será apreciado que a construção de redes *ad-hoc* é dependente de uma densidade adequada de dispositivos *ad-hoc*. Será ainda apreciado que em uma área em que há densidade suficiente de aparelhos de mão capazes de unir-se a uma rede *ad-hoc*, poderá haver uma variedade de fabricantes de aparelhos de mão e uma variedade de provedores de serviço de aparelhos de mão. Um problema neste ambiente é que cada provedor de serviço não está acostumado a participar ou cooperar com outros provedores de serviço. Portanto, qualquer tentativa de estabelecer uma rede *ad-hoc* que contenha aparelhos de mão de múltiplos provedores de serviço provavelmente será bloqueada. Uma razão para bloquear a formação *ad-hoc* é a

preocupação com a segurança dos assinantes do provedor de serviço e preocupação para a utilização não autorizada de serviços fornecidos pelo provedor de serviço (por exemplo, um serviço de jogos ou de correspondência eletrônica).

DESCRIÇÃO SUCINTA DAS FIGURAS

As figuras acompanhantes, em que números de referência iguais referem-se a elementos idênticos ou funcionalmente similares por todas as visões separadas e que junto com a descrição detalhada abaixo são aqui incorporados e formam parte da especificação, servem para ainda ilustrar várias versões e explicar vários princípios e vantagens tudo de acordo com a presente invenção.

A Figura 1 é uma rede de comunicação exemplar de acordo com algumas versões da invenção.

A Figura 2 é um dispositivo de comunicação exemplar para operação dentro da rede de comunicação de acordo com algumas versões da presente invenção.

A Figura 3 é um fluxograma que ilustra uma operação exemplar da rede de comunicação da Figura de acordo com algumas versões da presente invenção.

A Figura 4 é um fluxograma que ilustra uma operação exemplar do dispositivo de comunicação da Figura 2 de acordo com algumas versões da presente invenção.

A Figura 5 é um diagrama de fluxo de mensagem que ilustra a operação exemplar da rede da Figura 1 de acordo com algumas versões da presente invenção.

Artesãos habilitados apreciarão que elementos nas figuras são ilustrados quanto à simplicidade e clareza e não foram necessariamente desenhados em escala. Por exemplo, as dimensões de alguns dos elementos nas figuras

poderão ser exageradas em relação a outros elementos para ajudar a melhorar a compreensão das versões da presente invenção.

DESCRIÇÃO DETALHADA

Antes de descrever em detalhe versões que estão de acordo com a presente invenção, deve-se observar que as versões residem essencialmente em combinações de etapas de métodos e componentes de aparelho relacionados ao fornecimento de comunicação segura auxiliada por celular de uma pluralidade de dispositivos *ad-hoc*. Assim, os componentes do aparelho e as etapas de métodos foram representados quando apropriados por símbolos convencionais nos desenhos, mostrando apenas aqueles detalhes específicos que são pertinentes à compreensão das versões da presente invenção de modo a não obscurecer a revelação com detalhes que serão prontamente aparentes para aqueles de habilidade ordinária na tecnologia tendo o benefício da descrição aqui apresentada.

Neste documento, termos relacionais como primeiro e segundo, superior e inferior, e assemelhados, poderão ser utilizados unicamente para distinguir uma entidade ou ação de outra entidade ou ação sem necessariamente exigir ou implicar qualquer relação ou ordem verdadeira assim entre essas entidades ou ações. Os termos "compreende", "compreender" ou qualquer outra variação destes, pretendem cobrir uma inclusão não=exclusiva, tal que um processo, método, artigo, ou aparelho que compreende uma lista de elementos não inclui apenas aqueles elementos mas poderá incluir outros elementos não expressamente listados ou inerentes a esse processo, método, artigo, ou aparelho. Um

elemento precedido de "compreende ... um", sem maiores restrições, não impede a existência de elementos idênticos adicionais no processo, método, artigo ou aparelho que compreende o elemento.

Será apropriado que versões da invenção aqui descritas poderão ser compreendidas de um ou mais processadores convencionais e instruções de programa armazenadas singulares que controlem o um ou mais processadores para implementar, em conjunto com certos circuitos não-processadores, parte, a maioria, ou a totalidade das funções de fornecer comunicação segura auxiliada por celular de uma pluralidade de dispositivos *ad-hoc* aqui descritos. Os circuitos de não-processador poderão incluir, mas não estão a eles limitados, um receptor de rádio, um transmissor de rádio, acionadores de sinal, circuitos de cronômetros, circuitos de fonte de energia, e dispositivos de entrada do usuário. Como tal, essas funções poderão ser interpretadas como etapas de um método para efetuar a comunicação segura auxiliada por celular de uma pluralidade de dispositivos *ad-hoc*. Alternativamente, parte ou a totalidade das funções poderiam ser implementadas por uma máquina de estado que não possui nenhuma instrução de programa armazenada, ou em uma ou mais circuitos integrados específicos da aplicação (ASICs), em que cada função ou algumas combinações de certas das funções são implementadas como lógica sob medida. Naturalmente, uma combinação das duas abordagens poderia ser utilizada. Assim, métodos e meios para essas funções foram aqui descritos. Ainda, é esperado que alguém de habilidade ordinária, apesar de possivelmente esforço significativo e muitas opções de

projeto motivadas, por exemplo, pelo tempo disponível, a tecnologia atual, e considerações econômicas, quando orientado pelos conceitos e princípios aqui revelados será prontamente capaz de gerar essas instruções e programas de software e circuitos integrados (ICs) com um mínimo de experimentação.

A presente invenção provê a aplicação de chaves utilizadas em uma rede hierárquica (por exemplo, rede *ad-hoc* 802.11 sobreposta com uma rede de área ampla contendo um centro de serviço para a distribuição das chaves. Especificamente, a presente invenção utiliza uma estrutura de chave hierárquica para permitir que aplicações privadas utilizam repasses de operações de serviço iguais e desiguais ou de apenas operadores de serviço iguais. O método inclui a renovação periódica das teclas para excluir as teclas de usuários não-pagantes ou chaves bandidas. Várias chaves são gerenciadas pelo conjunto de mão e um centro de serviço de sobreposição (por exemplo, o Registrador de Localização Residencial Celular(HLR)). Cada chave tem funcionalidade singular que permite coletivamente a cooperação par-a-par entre dispositivos de aparelhos de mão, mesmo se os dispositivos de aparelhos de mão tiverem fabricantes diferentes e/ou provedores de serviço diferentes.

A Figura 1 é uma rede de comunicação exemplar 100 de acordo com algumas versões da invenção. Como é ilustrado, a rede de comunicação 100 é compreendida de pelo menos duas redes celulares, uma primeira rede celular 105 e uma segunda rede celular 110. Será apreciado por aqueles de habilidade ordinária na tecnologia que a rede de

comunicação 100 pode ser compreendida de qualquer duas ou mais redes de comunicação incluindo redes celulares (conforme ilustrado), redes de telefones sem fio, redes de área local sem fio, redes de rádio bilaterais e assemelhados. Será ainda apreciado que cada uma das redes dentro da rede de comunicação 100 pode ser operada por um provedor de serviço singular não associado um ao outro. Cada provedor de serviço tipicamente não participa ou coopera com outros provedores de serviço dentro da rede de comunicação.

Será apreciado por aqueles de habilidade ordinária na tecnologia que a primeira rede celular 101 e a segunda rede celular 110 da Figura 1 pode operar de acordo com pelo menos um de várias normas. Essas normas incluem protocolos de sistema de comunicação analógico, digital, ou de modo dual, como, mas sem a eles se limitar, o Advanced Mobile Phone System (AMPS), o Narrowband Advanced Mobile Phone System (NAMPS), o Global System for Mobile Communications (GSM), o sistema celular digital IS-136 Time Division Multiple Access (TDMA), o sistema celular digital IS-95 Code Division Multiple Access (CDMA), o sistema CDMA 2000, o sistema Wideband CDMA (W-CDMA), O Personal Communications System (PCS), o sistema Third Generation (3G), o Universal Mobile Telecommunications System (UMTS), e variações e evoluções desses protocolos. Na descrição seguinte, o termo "rede celular" refere-se a qualquer um dos sistemas mencionados acima ou um equivalente.

De acordo com a presente invenção, cada uma das redes celulares inclui um centro de serviço de segurança para gerenciar a comunicação segura dentro de cada rede celular.

Por exemplo, a primeira rede celular 105 inclui um primeiro centro de serviço de segurança 130 e a segunda rede celular 110 inclui um segundo centro de serviço de segurança 135.

Como é ilustrado na Figura 1, uma pluralidade de dispositivos de comunicação operam dentro de cada uma das duas ou mais redes celulares. Por exemplo, os dispositivos de comunicação 115-n (incluindo 115-1, 115-2, 115-3, 115-4, 115-5 conforme é ilustrado) operam dentro da primeira rede celular 105. De modo similar, os dispositivos de comunicação 120-n (incluindo 120-1, 120-2, 120-3, e 120-4 conforme é ilustrado) operam dentro da segunda rede celular 105. Será apreciado por alguém de habilidade ordinária na tecnologia que cada um dos dispositivos de comunicação 115-n e 120-n pode ser um telefone celular móvel, um terminal de dados de rádio móvel, um telefone celular móvel tendo um terminal de dados anexado ou integrado, um dispositivo de mensagem bilateral, ou um equivalente conforme apropriado para operar dentro de cada uma das redes da rede de comunicação 100. De modo similar, o dispositivo de comunicação pode ser qualquer outro dispositivo eletrônico como um assistente digital pessoal ou um computador laptop tendo capacidade para a comunicação sem fio. Na descrição seguinte, o termo "dispositivo de comunicação" refere-se a qualquer combinação dos dispositivos mencionados acima ou um equivalente.

De acordo com a presente invenção, pelo menos alguns dos dispositivos de comunicação 115-n são capazes de comunicar dentro de mais de uma rede de comunicação como a pri9meira rede celular 105 e uma rede *ad-hoc* 125. Por exemplo, como é ilustrado na Figura 1, os dispositivos de

comunicação 115-2, 115-3, 115-4, e 115-5 operam dentro tanto da primeira rede celular 105 como da rede *ad-hoc* 125. De modo similar, pelo menos alguns dos dispositivos de comunicação 120-n são capazes de se comunicar dentro de mais de uma rede de comunicação como a segunda rede celular 110 e da rede *ad-hoc* 125. Por exemplo, como é ilustrado na Figura 1, os dispositivos de comunicação 120-2, 120-3, e 120-4 operam dentro tanto da segunda rede celular 110 como da rede *ad-hoc* 125.

Será apreciado por aqueles de habilidade ordinária na tecnologia que a rede *ad-hoc* 125 pode ser uma rede de arquitetura ativada de malha (MEA) ou uma rede 802.11 (isto é, 802.11a, 802.11b, ou 802.11g). Será apreciado por aqueles de habilidade ordinária na tecnologia que a rede *ad-hoc* 125 pode alternativamente compreender qualquer rede de comunicação pacotizada. Por exemplo, a rede de comunicação 100 pode ser uma rede que utiliza protocolos de dados de pacote como TDMA (acesso múltiplo de divisão por tempo), GPRS (Serviço de Rádio de Pacote Geral), e EGPRS (Enhanced GPRS)

A rede *ad-hoc* 125 inclui uma pluralidade de nós móveis (referidos geralmente como nós ou nós móveis ou dispositivos de comunicação) como os dispositivos de comunicação 115-3, 115-4, 115-5, 120-2. 120-3, e 120-4 conforme é ilustrado na Figura 1. Ainda, a rede *ad-hoc* pode, mas não é obrigada a fazê-lo, incluir uma rede fixa tendo uma pluralidade de pontos de acesso inteligentes (IAP) para fornecer nós com acesso à rede fixa (não mostrado). A rede fixa 104 pode incluir, por exemplo, uma rede de acesso local cerne (LAN),e uma pluralidade de

servidores e de roteadores de portais para fornecer nós de rede com acesso a outras redes, como outras redes *ad-hoc*, uma rede de telefonia comutada pública 9PSTN) e a Internet. A rede *ad-hoc* 125 ainda pode incluir uma pluralidade de roteadores fixos para rotear pacotes de dados entre outros nós (não mostrado). É observado que para fins desta discussão, os nós discutidos acima podem ser referidos coletivamente como "nós" ou alternativamente como "dispositivos de comunicação".

Como pode ser apreciado por alguém de habilidade na tecnologia, os nós dentro da rede *ad-hoc* 125 são capazes de se comunicar uns com os outros diretamente, ou através de um ou mais outros nós que operam como roteador ou roteadores para os pacotes que estão sendo enviados entre nós. Cada nó comunica com outros nós vizinhos utilizando um enlace de transmissão e um enlace de recepção associado ao nó e cada um dos nós vizinhos.

A Figura 2 é um dispositivo de comunicação exemplar 200 para operação dentro da rede de comunicação 100 de acordo com algumas versões da presente invenção. O dispositivo de comunicação 200, por exemplo, pode ser o dispositivo de comunicação 115-n e 120-n conforme está ilustrado na Figura 1. De acordo com a presente invenção, o dispositivo de comunicação 200 é um dispositivo de modo dual. Apenas por meio de exemplo, o dispositivo de comunicação 200 pode ser capaz de operação dentro tanto da rede *ad-hoc* 125 como uma das redes celulares 105, 110 da Figura 1.

O dispositivo de comunicação 200 inclui hardware de dispositivo convencional (não representado por

simplicidade) como interfaces de usuário, circuitos de alerta, telas, e assemelhados, que são integradas em uma armação compacta.

O dispositivo de comunicação 200 ainda inclui uma antena celular 205 e um transceptor celular 210 para comunicar com a rede celular 105, 110. A antena celular 205 intercepta sinais transmitidas de uma ou mais redes celulares 105, 110 e transmite sinais para a uma o mais redes celulares 105, 110. A antena celular 205 é acoplada ao transceptor celular 210, que emprega técnicas de demodulação convencionais para receber os sinais de comunicação. O transceptor celular 210 é acoplado a um processador 225 e é reativo aos comandos do processador 225. Quando o transceptor celular 210 recebe um comando do processador 225, o transceptor celular 210 envia um sinal através da antena celular 205 para uma ou mais das redes celulares 105, 110. Em uma versão alternativa (não mostrada), o dispositivo de comunicação 200 inclui uma antena de recepção e um receptor para receber sinais de uma ou mais das redes celulares 105, 110 e uma antena de transmissão e um transmissor para transmitir sinais para uma ou mais das redes celulares 105, 110. Será apreciado por alguém de habilidade ordinária na tecnologia que outros diagramas de blocos eletrônicos similares do mesmo ou de tipo alternativo pode ser utilizado para o bloco celular do dispositivo de comunicação 200.

O dispositivo de comunicação 200 ainda inclui uma antena *ad-hoc* 215 e um transceptor *ad-hoc* 220 para comunicar dentro da rede *ad-hoc* 125. A antena *ad-hoc* 215 intercepta os sinais transmitidos de um ou mais nós dentro

da rede *ad-hoc* 125 e transmite sinais para o um ou mais nós dentro da rede *ad-hoc* 125. A antena *ad-hoc* 215 é acoplado ao transceptor *ad-hoc* 220 que emprega técnicas de demodulação convencionais para receber e transmitir sinais de comunicação, como sinais pacotizados, de e para o dispositivo de comunicação 200 sob o controle do processador 225. Os sinais de dados pacotizados podem, por exemplo, incluir informação de voz, de dados ou de multimídia, e sinais de controle pacotizados, incluindo informação de atualização do nó. Quando o transceptor *ad-hoc* 220 recebe um comando do processador 225, o transceptor *ad-hoc* 220 envia uma sinal através da antena *ad-hoc* 215 para um ou mais nós dentro da rede *ad-hoc* 125. Em uma versão alternativa (não mostrada), o dispositivo de comunicação 200 inclui uma antena de recepção e um receptor para receber sinais da rede *ad-hoc* 125 e uma antena de transmissão e um transmissor para transmitir sinais para a rede *ad-hoc* 125. Será apreciado por alguém de habilidade ordinária na tecnologia que outros diagramas de bloco eletrônico similar do mesmo ou de tipo alternativo pode ser utilizado para o bloco *ad-hoc* do dispositivo de comunicação 200.

Acoplado ao transceptor celular 210 e o transceptor *ad-hoc* 220, está o processador 225 utilizando técnicas de processamento de sinal convencional para processar mensagens recebidas. Será apreciado por alguém de habilidade ordinária na tecnologia que processadores adicionais podem ser utilizados conforme necessário para lidar com os requisitos de processamento do processador 225.

De acordo com a presente invenção, o processador 225 inclui um processador de autenticação 235 para autenticar várias comunicações de e para o dispositivo de comunicação 200. Ainda de acordo com a presente invenção, o processador 225 inclui um processador de aplicação 240 para processar vários programas de aplicação de software dentro do dispositivo de comunicação 200. Será apreciado por aqueles de habilidade ordinária na tecnologia que o processador de autenticação 235 e o processador de aplicação 240 pode, cada um, ser codificado duro ou programado dentro do dispositivo de comunicação 200 durante a fabricação, ode ser programado pelo ar quando da assinatura do cliente, ou pode ser uma aplicação baixada.Será apreciado que outros métodos de programação podem ser utilizados para programar cada um do processador de autenticação 235 e o processador de aplicação 240 dentro do dispositivo de comunicação 200. Será ainda apreciado por alguém de habilidade ordinária na tecnologia que cada um do processador de autenticação 235 e o processador de aplicação 240 pode ser circuito de hardware dentro do dispositivo de comunicação 200. De acordo com a presente invenção, cada um do processador de autenticação 235 e do processador de aplicação 240 pode estar contido dentro do processador 225 conforme ilustrado, ou alternativamente pode ser um bloco individual operativamente acoplado ao processador 225 (não mostrado).

Para efetuar as funções necessárias do dispositivo de comunicação 200, o processador 225 é acoplado à memória 230, que preferivelmente inclui uma memória de acesso aleatório (RAM), a memória de apenas leitura (ROM), a memória de apenas leitura programável e apagável (EEPROM) e

memória flash.

A memória 230, de acordo com a presente invenção, inclui locais de armazenamento para o armazenamento de uma ou mais chaves e informação de controle 245 e uma ou mais aplicações 250. De acordo com a presente invenção, a uma ou mais chaves 245 podem incluir, sem a elas ser limitadas, uma chave secreta 255, uma chave de grupo geral 260, uma chave de grupo de serviço 265, um recuo de atraso de re-autenticação 270, uma chave pública 275, uma chave de sessão 280, e um tempo de re-chaveamento 285, cada um dos quais será descrito em detalhe abaixo.

Será apreciado por aqueles de habilidade ordinária na tecnologia que a memória 230 pode ser integrada dentro do dispositivo de comunicação 200, ou alternativamente, pode ser pelo menos parcialmente contido dentro de uma memória externa como o dispositivo de armazenamento de memória. O dispositivo de armazenamento de memória, por exemplo, pode ser um cartão de módulo de identificação do assinante (SIM). O cartão SIM é um dispositivo eletrônico que tipicamente inclui uma unidade de microprocessador e uma memória adequada para encapsular dentro de um pequeno cartão de plástico flexível. O cartão SIM inclui adicionalmente alguma forma de interface para comunicar com o dispositivo de comunicação 200.

A Figura 3 é um fluxograma que ilustra a operação exemplar da rede de comunicação da Figura 1 de acordo com algumas versões da presente invenção. Como é ilustrado, algumas das comunicações envolvidas com a operação exemplar são comunicações de rede celular 305, e algumas das comunicações envolvidas com a operação exemplar são

comunicações de rede *ad-hoc* 310.

A operação da Figura 3 inicia com a etapa 310 em que cada dispositivo de comunicação autentica a si próprio com o centro de serviço de segurança associado da rede celular em que ele opera. Por exemplo, cada um dos dispositivos de comunicação 115-n autentica a si próprio com o primeiro centro de serviço de segurança 130 da rede 100. De modo similar, cada um dos dispositivos de comunicação 120-n autentica a si próprio com o segundo centro de serviço de segurança 135 da rede 100. Com referência ao dispositivo de comunicação 200, o processador de autenticação 235 recupera a chave secreta 255 e a chave pública 275 da memória 230, criptografa a chave pública 275 com a chave secreta 255, e envia a chave pública criptografada para o centro de serviço de segurança associado através do transceptor celular 210 e a antena celular 205. Na presente invenção, a chave secreta 255 está embutida no aparelho de mão por ocasião da fabricação e é conhecida apenas pelo centro de serviço de segurança associado. O centro de serviço de segurança associado descriptografa a chave pública 275 utilizando sua cópia conhecida da chave secreta 255 e armazena a chave pública para uso futuro.

A seguir, na etapa 315, uma chave de grupo geral é transmitida para todos os dispositivos autenticados. A mesma chave de grupo geral é transmitida para todos os dispositivos de comunicação autenticados dentro da rede 100 independentemente do provedor de serviço/rede celular em que o dispositivo de comunicação opera. Por exemplo, o centro de serviço de segurança 130 transmite a chave de grupo geral para cada dispositivo de comunicação 115-n em

resposta a autenticação do dispositivo de comunicação 115-n. De modo similar, o centro de serviço de segurança 135 transmite a chave de grupo geral para cada dispositivo de comunicação 120-n em resposta a autenticação do dispositivo de comunicação 120-n. A chave de grupo geral é criptografada utilizando a chave secreta 255 correspondente ao dispositivo de comunicação 115-n ou 120-n que está sendo autenticado. Em uma versão alternativa, a chave de grupo geral é criptografada utilizando a chave pública 275 correspondente ao dispositivo de comunicação 115-n ou 120-n que está sendo autenticado. Com referência ao dispositivo de comunicação 200, a chave de grupo geral criptografada 260 é recebida através da antena celular 205 e do transceptor celular 210, descriptografada pelo dispositivo de comunicação 200, e armazenada pelo processador 225 na memória 230 para uso futuro pelo dispositivo de comunicação. De acordo com a presente invenção, todos os dispositivos de comunicação que operam dentro da rede *ad-hoc* 125 tendo a chave de grupo geral 260 doravante (etapa 320) podem utilizar a chave de grupo geral 260 para intercambiar com segurança pacotes de controle através da rede *ad-hoc* 125 uns com os outros.

A seguir, na etapa 325, cada centro de serviço de segurança transmite uma chave de grupo de serviço para todos os dispositivos de comunicação autenticados, operando dentro da mesma rede celular. Por exemplo, o primeiro centro de serviço de segurança 130 transmite uma primeira chave de grupo de serviço para os dispositivos de comunicação autenticados 115-n; e o segundo centro de serviço de segurança 130 transmite uma segunda chave de

grupo de serviço para os dispositivos de comunicação autenticados 120-n. A chave de grupo de serviço é criptografada utilizando a chave secreta 255 correspondente ao dispositivo de comunicação 115-n ou 120-n que está sendo autenticado. Em uma versão alternativa, a chave de grupo de serviço é criptografada utilizando a chave pública 275 correspondente ao dispositivo de comunicação 115-n ou 120-n que está sendo autenticado. Com referência ao dispositivo de comunicação 200, a chave de grupo de serviço criptografada 265 é recebida através da antena celular 205 e o transceptor celular 210, descriptografada pelo dispositivo de comunicação 200, e armazenada pelo processador 225 na memória 230 para utilização futura pelo dispositivo de comunicação 200. De acordo com a presente invenção, todos os dispositivos de comunicação que operam dentro da mesma rede celular tendo a mesma chave de grupo de serviço, daí em diante (etapa 330) pode utilizar a chave de grupo de serviço para intercambiar com segurança pacotes de dados e de controle através da rede *ad-hoc* uns com os outros.

A seguir, na etapa 335, cada centro de serviço de segurança transmite um recuo de retardo de re-autenticação para todos os dispositivos de comunicação autenticados que operam dentro da mesma rede celular. Por exemplo, o primeiro centro de serviço de segurança 130 transmite um primeiro recuo de retardo de re-autenticação para os dispositivos de comunicação autenticados 115-n; e o segundo centro de serviço de segurança 130 transmite um segundo recuo de retardo de re-autenticação para os dispositivos de comunicação autenticados 120-n. Com referência ao

dispositivo de comunicação 200, o recuo de retardo de re-autenticação 270 é recebido através da antena celular 205 e do transceptor celular 210, e armazenado pelo processador 225 na memória 230 para utilização futura pelo dispositivo de comunicação 200. De acordo com a presente invenção, este recuo de retardo de re-autenticação é selecionado aleatoriamente para cada dispositivo de comunicação autenticado. Ele representa um tempo de retardo que o dispositivo de comunicação autenticado precisará esperar antes dele gerar uma nova solicitação de autenticação. Na etapa 340, quando a hora atual for pelo menos igual ao tempo de recuo de retardo de re-autenticação, a operação então circula de volta para as etapas 315 e 325. Então a re-autenticação é gerada após receber uma irradiação de rede para restabelecer uma chave de grupo geral 260 e a chave de grupo de serviço 265. Este método permite a renovação periódica das chaves para excluir as chaves de usuário não-pagador ou as chaves de bandidos.

Com referência agora de volta à comunicação dentro da rede *ad-hoc* 125, após a chave de grupo geral ter sido recebida pelos vários dispositivos de comunicação no modo dual autenticados, a rede *ad-hoc* 125 pode ser estabelecida na etapa 345 como é bem conhecido na tecnologia. Em outras palavras, a rede *ad-hoc* 125 pode ser estabelecida para incluir os dispositivos de comunicação 115-2, 115-3, 115-4, 115-5, 120-2, 120-3, e 120-4 utilizando a tecla de grupo geral 260 para criptografar os pacotes de controle para descoberta da rota. A seguir, na etapa 350, a comunicação entre os vários dispositivos participantes na rede *ad-hoc* 125 ocorre com segurança através de um canal de comunicação

de rede *ad-hoc* associado. Por exemplo, os mesmos dispositivos de provedor de serviço intercambiam pacotes de controle e de dados na etapa 330.

Será apreciado que periodicamente uma nova chave de grupo de serviço e/ou uma nova chave geral de grupo será transmitida para mudar as chaves. Na etapa 355, o centro de serviço de segurança irradia uma mensagem de alerta de re-chaveamento para cada dispositivo de comunicação. Esta mensagem de alerta contém um tempo de re-chaveamento futuro pelo qual todos os dispositivos de comunicação precisam ter completado um procedimento de re-autenticação. Este tempo de re-chaveamento futuro é depois do que o tempo atual mais o recuo de retardo de re-autenticação máximo recebido por qualquer dispositivo de comunicação. Com referência ao dispositivo de comunicação 200, o recuo de retardo de re-autenticação 270 é utilizado como um recuo de tempo do tempo atual pelo qual quando da expiração, o dispositivo de comunicação 200 iniciará um procedimento de re-autenticação conforme definido anteriormente nas etapas 310, 315, e 325. O centro de serviço de segurança só autenticará aqueles dispositivos de comunicação que têm permissão de participar na rede *ad-hoc* 125. Como foi definido anteriormente na etapa 315, cada centro de serviço de segurança transmite uma chave de grupo geral para todos os dispositivos de comunicação autenticados que operam dentro da rede 100 independentemente do provedor de serviço/rede celular em que o dispositivo de comunicação opera. Como foi definido anteriormente na etapa 325, cada centro de serviço de segurança transmite uma chave de grupo de serviço para todos os dispositivos de comunicação autenticados que

operam dentro da mesma rede celular. Todas as chaves recebidas do centro de serviço de segurança são entregues a cada dispositivo de comunicação através de um controle de celular ou canal de dados. Na etapa 360, cada dispositivo de comunicação autenticado determina se o tempo atual é ou não igual ao tempo de re-chaveamento comunicado 285. Quando o tempo atual for o tempo de re-chaveamento 285, o processo flui de volta para a etapa 315 e o dispositivo de comunicação começará a utilizar a nova chave de grupo geral e a nova chave de grupo de serviço para todas as comunicações futuras quando o tempo atual for igual ao tempo de re-chaveamento 285. Será apreciado por aqueles de habilidade ordinária na tecnologia que embora a Figura 3 ilustre uma versão exemplar em que a nova chave de grupo geral e a nova chave de grupo de serviço são comunicadas a ou após o tempo de rechaveamento 285, alternativamente, a nova chave de grupo geral e a nova chave de grupo de serviço podem ser comunicadas e armazenadas dentro dos dispositivos de comunicação em qualquer tempo anterior ao tempo de rechaveamento 285.

A Figura 4 é um fluxograma que ilustra uma operação exemplar do dispositivo de comunicação 200 da Figura 2, de acordo com algumas versões da presente invenção. Especificamente, a Figura 4 ilustra uma operação exemplar da etapa 350 de comunicação da Figura 3 de acordo com algumas versões da presente invenção.

A operação da Figura 4 tem início com a etapa 400 em que o dispositivo de comunicação 200 lança uma aplicação. Por exemplo, o processador de aplicação 240 lança uma aplicação armazenada na memória da aplicação 250. A seguir,

na etapa 405, o dispositivo de comunicação 200 identifica um dispositivo par para a aplicação. Por exemplo, o processador de aplicação 240 identifica o dispositivo par dos dados da aplicação armazenada na memória de aplicação 250. A seguir, na etapa 410, o dispositivo de comunicação 200 recebe uma chave pública 275 e uma chave de sessão 280 para partilhar uma aplicação com o dispositivo par através da rede celular em que tanto o dispositivo de comunicação como o dispositivo par operam. Por exemplo, um dispositivo de comunicação fonte 200 solicita a utilização da utilização conjunta de uma aplicação entre ele próprio e um dispositivo par identificado. O centro de serviço de segurança transmite uma chave de sessão e uma chave pública para o dispositivo par para o dispositivo de comunicação (a chave pública do dispositivo par e chave de sessão são criptografadas com a chave pública do dispositivo de comunicação 200). A seguir, na etapa 415, o dispositivo de comunicação 200 autentica o dispositivo par com a chave pública recebida. Em uma versão da presente invenção, os cabeçalhos de comunicação do enlace de dados e os cabeçalhos de comunicação da camada de rede são criptografados com a chave de grupo geral, a solicitação de autenticação é criptografada com a chave de grupo de serviço, e o conteúdo da solicitação de autenticação (por exemplo, a chave pública do dispositivo de comunicação fonte 200) é criptografada com a chave pública do dispositivo par. Isto permite que qualquer dispositivo autenticado na rede *ad-hoc* (independentemente da rede celular a qual pertence) rotear a solicitação de autenticação para o dispositivo par. Além disso, o fato de

que uma autenticação está sendo tentada é conhecido apenas dos dispositivos de comunicação na rede celular que contém o dispositivo de comunicação fonte 200. Será apreciado por aqueles de habilidade ordinária na tecnologia que as outras realizações do uso dessas chaves estão também dentro do escopo da invenção. O dispositivo par responderá à solicitação de autenticação utilizando a chave pública do dispositivo de comunicação fonte 200 bem como as outras chaves conforme acabado de descrever. A seguir, na etapa 420, o dispositivo de comunicação criptografa uma chave de sessão com a chave pública do dispositivo par em uma solicitação de sessão de aplicação. A seguir, na etapa 425, o dispositivo de comunicação criptografa a chave de sessão com a chave pública do dispositivo par em uma solicitação de sessão de aplicação. A seguir, na etapa 425, o dispositivo de comunicação intercambia a chave de sessão com o dispositivo par através da rede *ad-hoc*. Por meio de exemplo em uma versão da presente invenção, os cabeçalhos de comunicação de enlace de dados e os cabeçalhos de comunicação da camada de rede são criptografados com a chave de grupo geral, a solicitação de sessão de aplicação é criptografada com a chave de grupo de serviço, e o conteúdo da solicitação de sessão de aplicação (isto é, a chave de sessão) é criptografada com a chave pública do dispositivo par. Isto permite que qualquer dispositivo autenticado na rede *ad-hoc* (independentemente da rede celular a que pertença) rotear a solicitação de sessão de aplicação ao dispositivo par. Além disso, o fato de que a solicitação de sessão de aplicação está sendo tentada é conhecida apenas dos dispositivos de comunicação na rede

celular que contém o dispositivo de comunicação de fonte 200. Ademais, a chave de sessão é conhecida apenas do dispositivo de comunicação alvo 200 e o dispositivo par. Será apreciado por aqueles de habilidade ordinária na tecnologia que outras realizações da utilização dessas chaves também estão dentro do escopo da invenção. Mais uma vez, o dispositivo par responderá à solicitação de sessão de aplicação utilizando a chave pública do dispositivo de comunicação fonte 200 bem como outras chaves conforme acabado de descrever. A seguir, na etapa 430, o dispositivo de comunicação criptografa os pacotes de aplicação com o dispositivo par utilizando a chave de sessão e a chave de grupo de serviço recebidas anteriormente. A seguir, na etapa 435, o dispositivo de comunicação e o dispositivo par comunicam pelo canal de comunicação da rede *ad-hoc* para processar as várias operações da aplicação. Como foi exemplificado anteriormente, cada uma da chave de grupo geral, chave de grupo de serviço, chaves públicas e chave de sessão são utilizadas para comunicar em segurança entre o dispositivo de comunicação fonte 200 e o dispositivo par protegendo elementos da comunicação considerados necessários pelo dispositivo de comunicação e o provedor de serviço para os dispositivos de comunicação.

A Figura 5 é um diagrama de fluxo de mensagem que ilustra uma operação exemplar de uma rede 500 de acordo com algumas versões da presente invenção. A rede 500 inclui uma primeira rede celular 505 e uma segunda rede celular 510. A primeira rede celular 505 inclui um primeiro centro de serviço de segurança 515 e vários dispositivos de comunicação incluindo o dispositivo A 520, o dispositivo B

525 e o dispositivo C 530. A segunda rede celular 510 inclui um segundo centro de serviço de segurança 540 e vários dispositivos de comunicação incluindo o dispositivo D 535.

Para fins do cenário exemplar da Figura 5, dois usuários, o dispositivo A 520 e o dispositivo B 525 querem partilhar conteúdo através do dispositivo C 530. Como é ilustrado, o dispositivo A 520, o dispositivo B 525, e o dispositivo C 530 operam todos na mesma rede celular (a rede celular 505) utilizando o mesmo provedor de serviço. Neste cenário exemplar, os usuários A e B querem que seus dados de aplicação sejam privados, mas eles querem que o dispositivo C efetue intermediações para eles. Outrossim, A, B e C querem todos que o controle e os dados sejam seguros do usuário D (dispositivo D 535 que opera em uma rede celular diferente 510). Para possibilitar isto, o dispositivo A 520, o dispositivo B 525, e o dispositivo C 530, possuem, cada um, uma chave de grupo geral e uma primeira chave do primeiro grupo de serviço de rede celular conhecida pelo primeiro centro de serviço de segurança 515. O dispositivo D 535 também conhece a mesma chave de grupo geral conhecida pelo dispositivo A 520, o dispositivo B 525, e o dispositivo C 530, mas conhece apenas a segunda chave de grupo de serviço da rede celular. Se o dispositivo A 520, o dispositivo B 525, e o dispositivo C 530 quiserem utilizar o dispositivo D 535 como um intermediador, eles utilizariam a chave de grupo geral para a descoberta da rota e as intermediações de pacote cru através do endereço Media Access Control (MAC) do dispositivo D, mas utilizariam a chave de grupo de serviço da primeira rede

celular para controle de camadas mais altas e pacotes de dados.

Como é ilustrado no fluxo de operação da Figura 5, em operação 545, cada um do dispositivo A 520, o dispositivo B 525, o dispositivo C 530, e o dispositivo D 535 inicialmente energizarão e começarão um procedimento de autenticação utilizando uma chave secreta ou certificado, por exemplo, que está embutido no conjunto de mão por ocasião da fabricação. Esta autenticação é efetuada com seus respectivos centros de serviço de segurança (isto é, o primeiro centro de serviço de segurança 515 para o dispositivo A 520, o dispositivo B 525, o dispositivo C 530, e o segundo centro de serviço de segurança 540 para o dispositivo D 535). A seguir, na operação 550, uma vez autenticados, cada um do dispositivo A 520, o dispositivo B 525, o dispositivo C 530, e o dispositivo D 535 são designados uma chave de grupo geral. A seguir, na operação 555, cada um do dispositivo A 520, o dispositivo B 525, e o dispositivo C 530 recebe uma chave de grupo de serviço do primeiro centro de serviço de segurança 515; e o dispositivo D 535 recebe uma chave de grupo de serviço do segundo centro de serviço de segurança 540.

A seguir, na operação 560, cada um do dispositivo A 520, o dispositivo B 525, o dispositivo C 530, e o dispositivo D 535 utiliza a chave de grupo geral para intercambiar informação de controle e encontrar uma rota do dispositivo A 520 para o dispositivo B 525 através do dispositivo C 530 e o dispositivo D 535. A seguir, na operação 565, o dispositivo A 520 intercambia uma solicitação com o primeiro provedor de serviço celular para

iniciar uma aplicação (por exemplo, correspondência eletrônica com o dispositivo B 525). A seguir, na operação 570, o primeiro centro de serviço de segurança 515 verifica se o dispositivo B 525 está autorizado a utilizar o serviço de correspondência eletrônica e então fornece a chave pública para o dispositivo B 525 ao dispositivo A 520. A seguir, na operação 575, utilizando esta chave pública, o dispositivo A 520 e o dispositivo B 525 intercambiam uma chave de sessão para a aplicação de correspondência eletrônica bem como a chave pública para o dispositivo A 520. A seguir, na operação 580, utilizando a chave de grupo de serviço da rede celular, a chave de grupo geral, e a chave de sessão, dados são criptografados ao nível apropriado de encapsulamento dos pacotes de dados sendo intercambiados entre o dispositivo A 520 e o dispositivo B 525 através do dispositivo C 530 e do dispositivo D 535 através de uma rede *ad-hoc* comum conforme estabelecido na operação 560. O dispositivo C 530 e o dispositivo D não são capazes de decodificar os pacotes de dados, mas são inteiramente capazes de cooperar para servir as necessidades de intermediação do dispositivo A 520 e do dispositivo B 525.

Embora não seja ilustrado, será apreciado por alguém de habilidade ordinária na tecnologia que, em ocasião posterior, o primeiro centro de serviço de segurança 515 poderá irradiar uma solicitação para gerar uma nova chave de grupo geral, uma nova primeira chave de grupo de serviço da rede celular, ou uma nova chave de sessão ou chave de aplicação para o dispositivo A 520 e o dispositivo B 525. Esta solicitação especifica um tempo de rechaveamento

futuro que todos os dispositivos autenticados atualizarão suas chaves respectivas. Para efetuar a geração de novas chaves, a solicitação disparará cada um do dispositivo A 520, o dispositivo B 525, o dispositivo C 530, e o dispositivo D 535 para iniciar um novo procedimento de autenticação utilizando suas respectivas chaves secretas ou certificados. A autenticação de cada dispositivo ocorre em pontos aleatórios no tempo antes do tempo de rechaveamento futuro. O recuo aleatório no tempo tem por base um parâmetro recebido durante a autenticação anterior. Esta operação é necessária para ter certeza de qualquer assinante não-pagante não está mais capacitado a participar ou fazer escuta em redes *ad-hoc* gerenciadas pela rede celular. Ou, se o usuário A ou o usuário B parassem de pagar pela aplicação de correspondência eletrônica, esta chave de aplicação atualizada também impede que eles utilizam mais a aplicação.

A presente invenção conforme aqui descrita fornece um sistema e método para tornar atraente e seguro para os aparelhos de mão de um provedor de serviço cooperar com aparelhos de mão de outro provedor de serviço para estabelecer uma rede *ad-hoc* e permitir a intermediação de pacotes através de seus assinantes.

Na especificação anterior, versões específicas da presente invenção foram descritas. No entanto, alguém de habilidade ordinária na tecnologia aprecia que várias modificações e mudanças podem ser feitas sem desviar do escopo da presente invenção conforme explicitado nas reivindicações abaixo. Assim, a especificação e as figuras devem ser consideradas em sentido ilustrativo e não no

sentido restritivo, e todas essas modificações pretendem ser incluídas dentro do escopo da presente invenção. Os benefícios, vantagens, soluções de problemas, e quaisquer elementos que poderão causar qualquer benefício, vantagem ou solução a ocorrer ou tornar-se mais acentuada não devem ser interpretadas como recursos ou elementos críticos, obrigatórios ou essenciais de qualquer uma ou de todas as reivindicações. A invenção é definida unicamente pelas reivindicações apensas incluindo quaisquer emendas feitas durante a pendência desta aplicação e todos os equivalentes daquelas reivindicações conforme emitidas.

REIVINDICAÇÕES

1. Método para fornecer comunicação segura entre uma pluralidade de dispositivos *ad-hoc*, o método **caracterizado** pelo fato de compreender:

autenticar um ou mais primeiros dispositivos (115-1, 115-2, 115-3, 115-4, 115-5) dentro de uma primeira rede (105);

autenticar um ou mais segundos dispositivos (120-1, 120-2, 120-3, 120-4) dentro de uma segunda rede (110);

transmitir uma chave de grupo para os primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5) e para os segundos dispositivos autenticados (120-1, 120-2, 120-3, 120-4);

estabelecer uma rede *ad-hoc* (125) por pelo menos um dos primeiros dispositivos autenticados (115-2, 115-3, 115-4, 115-5) e pelo menos um dos segundos dispositivos autenticados (120-2, 120-3, 120-4) utilizando a chave de grupo; e

comunicar dentro da rede *ad-hoc* (125) entre o pelo menos um dos primeiros dispositivos autenticados (115-2, 115-3, 115-4, 115-5) e o pelo menos um dos segundos dispositivos autenticados (120-2, 120-3, 120-4);

comunicar dentro da primeira rede (105) pelos primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5) utilizando uma primeira chave de grupo de serviço; e

comunicar dentro da segunda rede (110) pelos segundos dispositivos autenticados (120-1, 120-2, 120-3, 120-4) utilizando uma segunda chave de grupo de serviço.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a primeira rede (105) compreende uma primeira rede celular operada por um primeiro provedor de serviço; e

em que a segunda rede (110) compreende uma segunda rede celular operada por um segundo provedor de serviço.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de a etapa de estabelecer a rede *ad-hoc* compreender o pelo menos um dos primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5) e o pelo menos um dos segundos dispositivos autenticados (120-1, 120-2, 120-3, 120-4) intercambiar pacotes de controle criptografados com a chave de grupo para a descoberta da rota.

4. Método, de acordo com a reivindicação 2, **caracterizado** pelo fato de que a primeira rede (105) incluir um primeiro centro de serviço de segurança (130), em que a etapa de autenticar um ou mais primeiros dispositivos (115-1, 115-2, 115-3, 115-4, 115-5) compreende cada um do um ou mais primeiros dispositivos (115-1, 115-2, 115-3, 115-4, 115-5) autenticando a si próprio com o primeiro centro de serviço de segurança (130); e

em que a segunda rede inclui um segundo centro de serviço de segurança (135) e em que a etapa de autenticar um ou mais segundos dispositivos (120-1, 120-2, 120-3, 120-4) compreende cada um dos um ou mais segundos dispositivos (120-1, 120-2, 120-3, 120-4) autenticando a si próprio com o segundo centro de serviço de segurança (135).

5. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que ainda compreende transmitir

um tempo de recuo de retardo de re-auntenticação para os primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5); e

re-autentificar os primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5) em um tempo pelo menos igual ao tempo de recuo de retardo de re-autenticação.

6. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que ainda compreende:

transmitir uma mensagem de re-chaveamento incluindo um tempo de re-chaveamento para os primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5); e

gerar uma re-autenticação de pelo menos um dos primeiros dispositivos autenticados (115-1, 115-2, 115-3, 115-4, 115-5) quando um tempo atual for pelo menos igual ao tempo de re-chaveamento.

7. Método de operação de um dispositivo de comunicação de modo dual (200), o método **caracterizado** pelo fato de compreender:

autenticar o dispositivo de comunicação de modo dual (200) dentro de uma rede celular (105);

receber uma chave de grupo geral através da rede celular (105);

comunicar dentro de uma rede *ad-hoc* (125) utilizando a chave de grupo geral para intercambiar em segurança pacotes de controle com um ou mais outros dispositivos que operam dentro da rede *ad-hoc* (125);

receber uma chave de grupo de serviço de um centro de serviço de segurança (130) através da rede celular (105); e

utilizar a chave de grupo de serviço para intercambiar em segurança pacotes de controle e de dados com um ou mais outros dispositivos celulares.

8. Método de operação de um dispositivo de comunicação de modo dual, de acordo com a reivindicação 7, **caracterizado** pelo fato de que a etapa de autenticar compreende:

transmitir uma chave secreta do dispositivo de comunicação de modo dual (200) para o centro de serviço de segurança (130) através da rede celular (105).

9. Dispositivo de comunicação de modo dual **caracterizado** pelo fato de ter meios configurados para executar as etapas conforme definidas na reivindicação 7 ou 8.

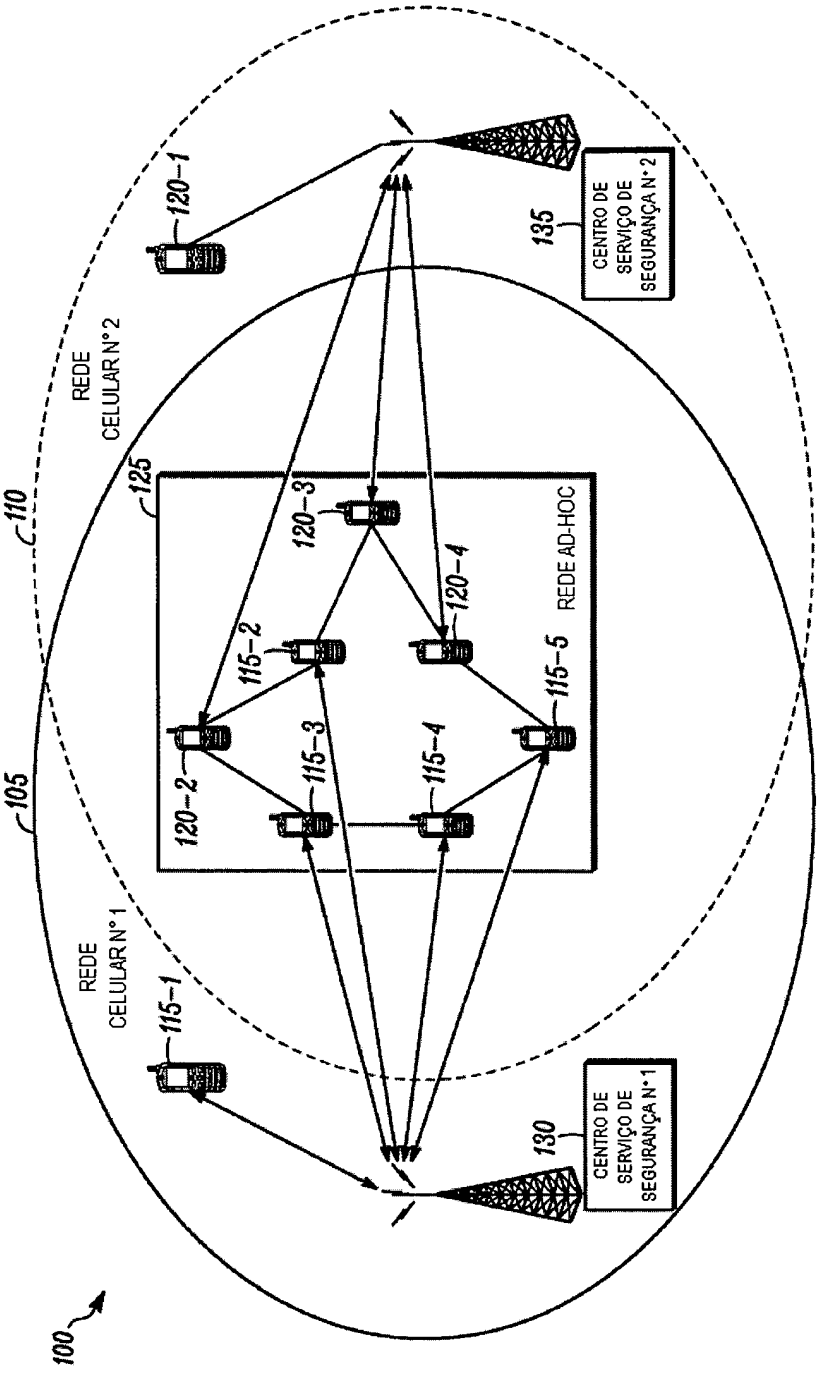
100
105
110
REDE CELULAR N° 1
REDE CELULAR N° 2
125
REDE AD-HOC
115-1
115-2
115-3
115-4
115-5
120-1
120-2
120-3
120-4
130
135
CENTRO DE SERVIÇO DE SEGURANÇA N° 1
CENTRO DE SERVIÇO DE SEGURANÇA N° 2

FIG. 1

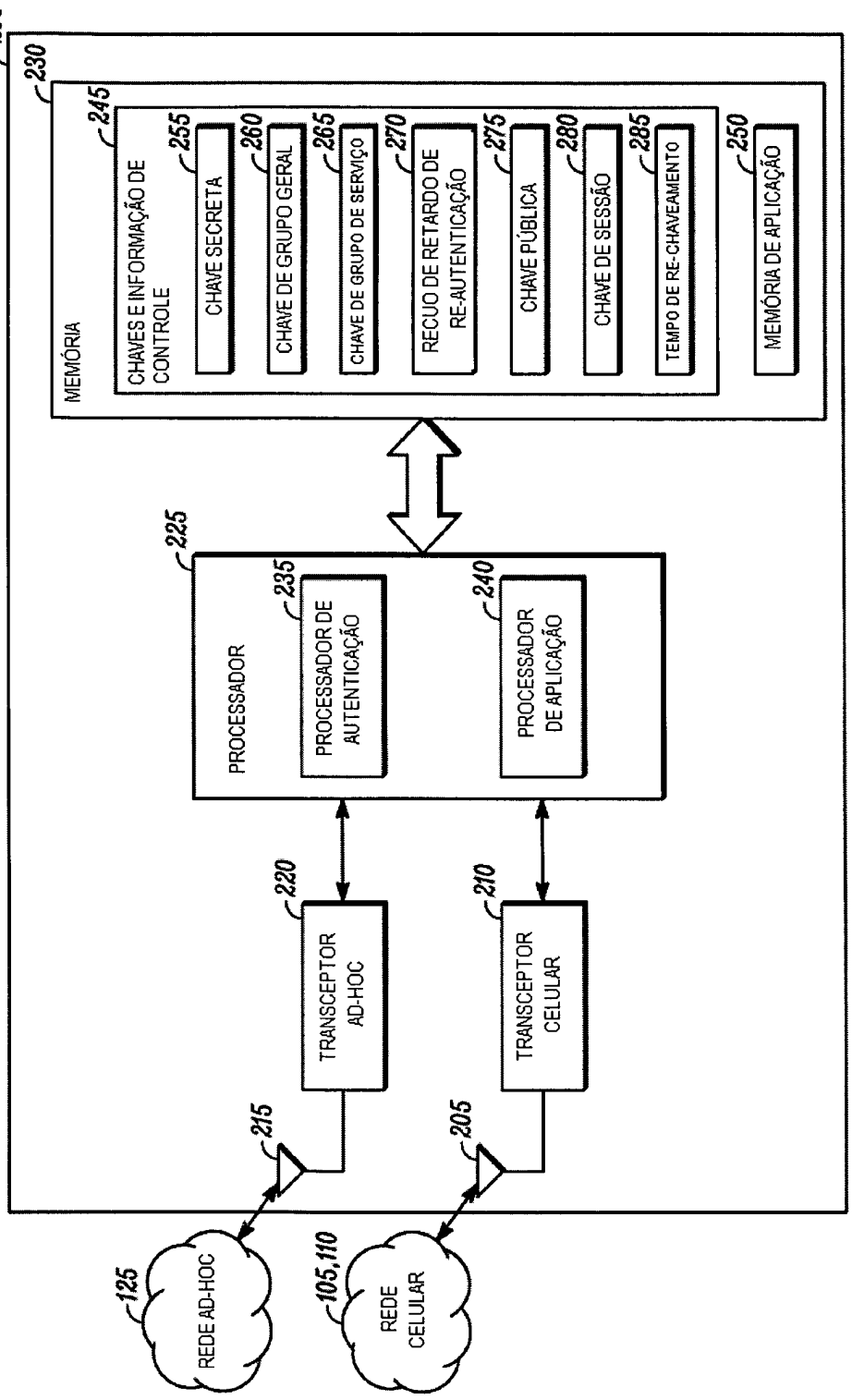
200
230
MEMÓRIA
245
CHAVES E INFORMAÇÃO DE CONTROLE
255
CHAVE SECRETA
260
CHAVE DE GRUPO GERAL
265
CHAVE DE GRUPO DE SERVIÇO
270
RECUO DE RETARDO DE RE-AUTENTICAÇÃO
275
CHAVE PÚBLICA
280
CHAVE DE SESSÃO
285
TEMPO DE RE-CHAVEAMENTO
250
MEMÓRIA DE APLICAÇÃO
225
PROCESSADOR
235
PROCESSADOR DE AUTENTICAÇÃO
240
PROCESSADOR DE APLICAÇÃO
220
TRANSCEPTOR AD-HOC
210
TRANSCEPTOR CELULAR
215
205
125
REDE AD-HOC
105,110
REDE CELULAR

FIG. 2

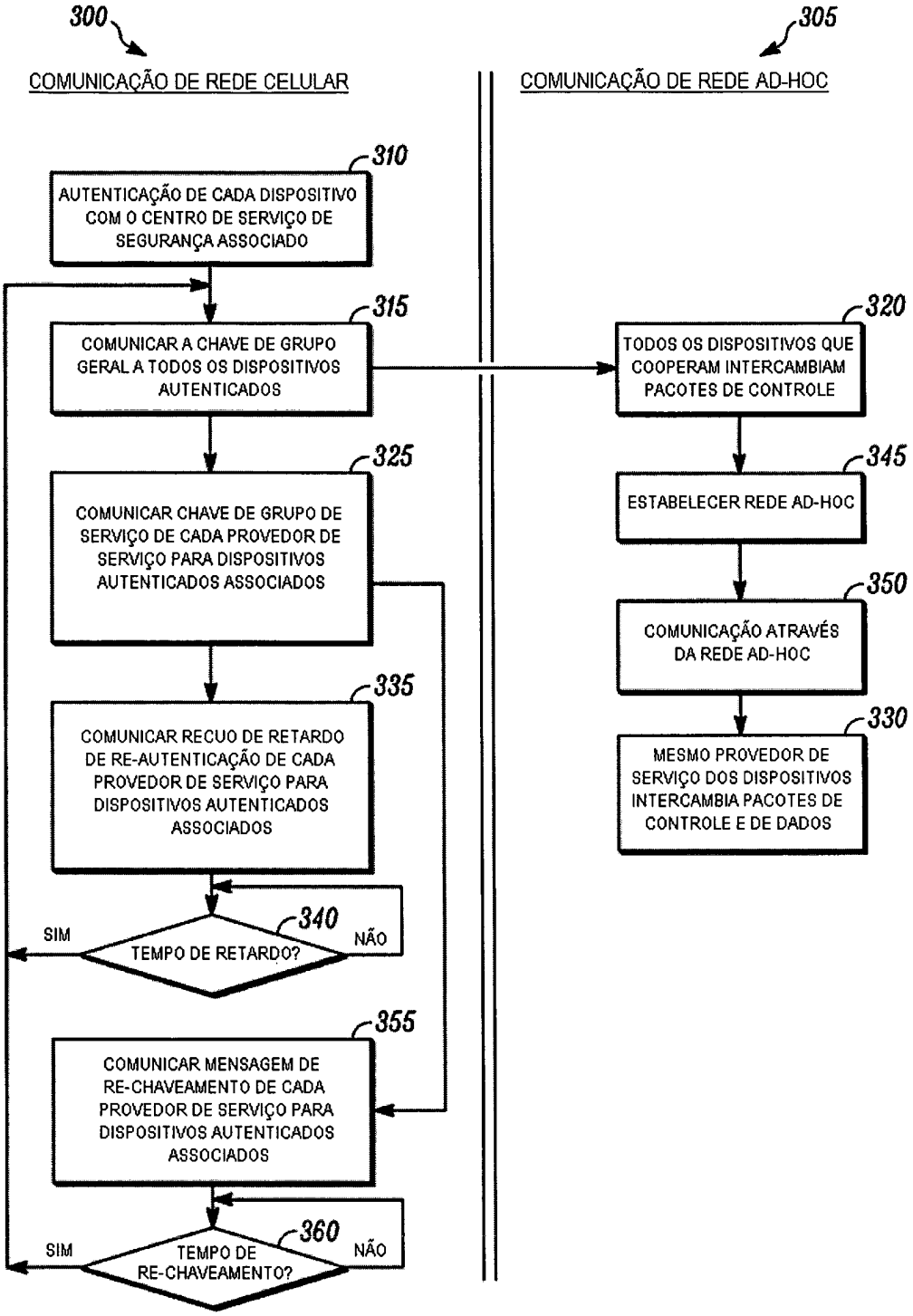
300
COMUNICAÇÃO DE REDE CELULAR
305
COMUNICAÇÃO DE REDE AD-HOC
310
AUTENTICAÇÃO DE CADA DISPOSITIVO COM O CENTRO DE SERVIÇO DE SEGURANÇA ASSOCIADO
315
COMUNICAR A CHAVE DE GRUPO GERAL A TODOS OS DISPOSITIVOS AUTENTICADOS
320
TODOS OS DISPOSITIVOS QUE COOPERAM INTERCAMBIAM PACOTES DE CONTROLE
325
COMUNICAR CHAVE DE GRUPO DE SERVIÇO DE CADA PROVEDOR DE SERVIÇO PARA DISPOSITIVOS AUTENTICADOS ASSOCIADOS
345
ESTABELECER REDE AD-HOC
350
COMUNICAÇÃO ATRAVÉS DA REDE AD-HOC
335
COMUNICAR RECUO DE RETARDO DE RE-AUTENTICAÇÃO DE CADA PROVEDOR DE SERVIÇO PARA DISPOSITIVOS AUTENTICADOS ASSOCIADOS
330
MESMO PROVEDOR DE SERVIÇO DOS DISPOSITIVOS INTERCAMBIA PACOTES DE CONTROLE E DE DADOS
340
TEMPO DE RETARDO?
SIM
NÃO
355
COMUNICAR MENSAGEM DE RE-CHAVEAMENTO DE CADA PROVEDOR DE SERVIÇO PARA DISPOSITIVOS AUTENTICADOS ASSOCIADOS
360
TEMPO DE RE-CHAVEAMENTO?
SIM
NÃO

FIG. 3

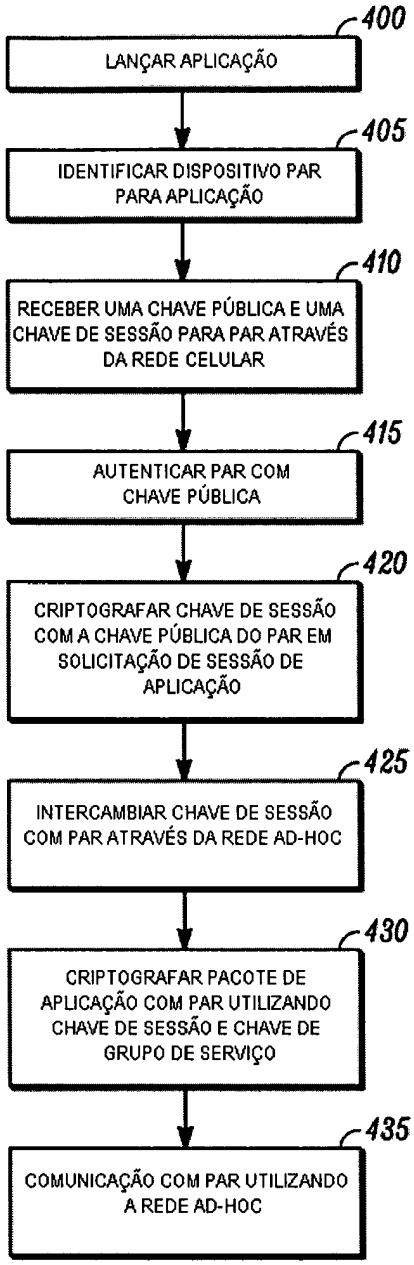
400
LANÇAR APLICAÇÃO
405
IDENTIFICAR DISPOSITIVO PAR PARA APLICAÇÃO
410
RECEBER UMA CHAVE PÚBLICA E UMA CHAVE DE SESSÃO PARA PAR ATRAVÉS DA REDE CELULAR
415
AUTENTICAR PAR COM CHAVE PÚBLICA
420
CRIPTOGRAFAR CHAVE DE SESSÃO COM A CHAVE PÚBLICA DO PAR EM SOLICITAÇÃO DE SESSÃO DE APLICAÇÃO
425
INTERCAMBIAR CHAVE DE SESSÃO COM PAR ATRAVÉS DA REDE AD-HOC
430
CRIPTOGRAFAR PACOTE DE APLICAÇÃO COM PAR UTILIZANDO CHAVE DE SESSÃO E CHAVE DE GRUPO DE SERVIÇO
435
COMUNICAÇÃO COM PAR UTILIZANDO A REDE AD-HOC

FIG. 4

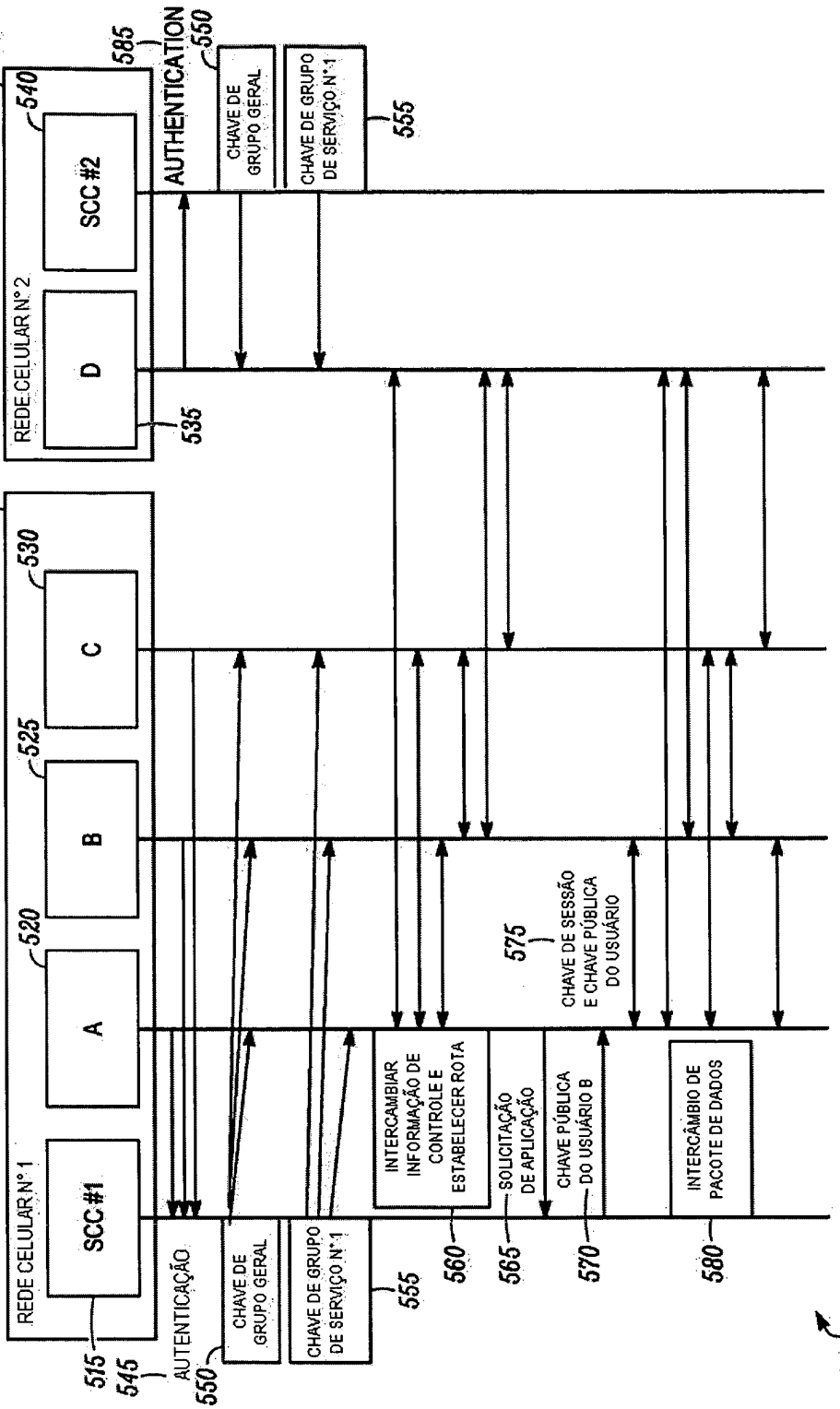
REDE CELULAR N° 1
SCC #1
A
B
C
REDE CELULAR N° 2
D
SCC #2
AUTHENTICATION
AUTENTICAÇÃO
CHAVE DE GRUPO GERAL
CHAVE DE GRUPO DE SERVIÇO N° 1
INTERCAMBIAR INFORMAÇÃO DE CONTROLE E ESTABELECER ROTA
SOLICITAÇÃO DE APLICAÇÃO
CHAVE PÚBLICA DO USUÁRIO B
CHAVE DE SESSÃO E CHAVE PÚBLICA DO USUÁRIO
INTERCÂMBIO DE PACOTE DE DADOS
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585

FIG. 5