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

(21) **PI0902036-5 A2**

BRPI0902036A2

(22) Data de Depósito: 27/05/2009
(43) Data da Publicação: 08/02/2011
(RPI 2092)

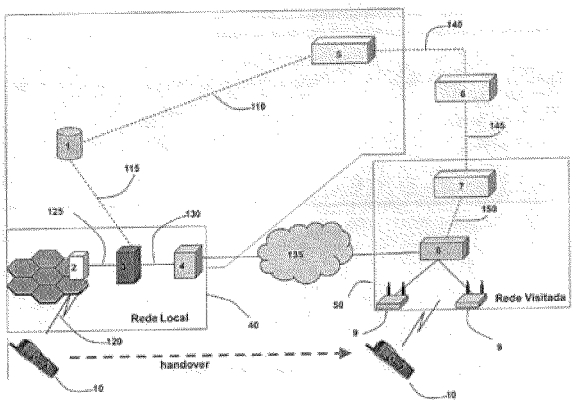
(51) Int.Cl.:
H04W 12/06

(54) Título: **SISTEMA E MÉTODO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS**

(73) Titular(es): Brasil Telecom S.A., Fundação Universidade de Brasília

(72) Inventor(es): Sebastião Boanerges Ribeiro Junior

(57) Resumo: SISTEMA E MÉTODO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS. A presente invenção refere-se a um sistema e a um método de autenticação com redução de atraso para interconexão de redes sem fio heterogêneas (40, 50), preferencialmente VVWAN celular e WLAN, com uma troca segura de chaves entre os elementos redes, utilizando-se de segredos específicos e compartilháveis para cada um dos elementos interconectados a e pela rede. Além disso, a presente invenção define uma arquitetura de rede baseada na introdução de um elemento funcional na rede VVWAN e em cada rede WLAN passível de ser visitada pelo terminal móvel (10), a este elemento funcional é dado o nome de Servidor de Distribuição de Chaves (SDC) (20, 30). O Servidor de Distribuição de Chaves (SDC) (20, 30) intro- duzido na arquitetura da presente invenção é responsável por realizar a distribuição antecipada das chaves de autenticação temporárias das redes WLAN elegíveis para receber o terminal móvel no handover seguinte.



Relatório Descritivo da Patente de Invenção para **"SISTEMA E MÉTODO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS".**

CAMPO DA INVENÇÃO

A presente invenção refere-se a um sistema e um método de autenticação para interconexão de redes sem fio heterogêneas, preferencialmente as redes heterogêneas WWAN celular e WLAN. A presente invenção proporciona uma arquitetura que compreende um procedimento de autenticação, de forma a permitir que a mesma seja realizada sem afetar o tempo de indisponibilidade do serviço.

DESCRIÇÃO DO ESTADO DA TÉCNICA

Ao longo do tempo, diferentes tecnologias de rede sem fio têm sido desenvolvidas para cobrir as diversas necessidades de comunicação. Esse desenvolvimento baseou-se, e ainda baseia-se, principalmente no raio de abrangência alcançado pelas redes. Assim, as redes WWAN (para a cobertura de regiões extensas), as redes WLAN (para instalações locais) e as redes WPAN (com cobertura pessoal) têm evoluído de forma contínua e distinta, com características inerentes à suas coberturas.

Além disso, a crescente oferta de serviços de voz e multimídia sobre redes de dados sem fio vem determinando a necessidade de otimização dos procedimentos de gerência de mobilidade, com a finalidade de reduzir o tempo de indisponibilidade da conexão do terminal à rede, e conseqüentemente, ao serviço. A premissa maior passou a ser a manutenção da percepção da qualidade do serviço pelo usuário final, de tal forma que a sua experiência com o serviço não seja alterada pelo fato do terminal ter realizado um handover vertical.

O handover vertical ocorre quando um terminal se desloca entre pontos de acesso que implementam diferentes tecnologias. Por envolver diferentes tecnologias, o handover vertical geralmente é iniciado pelo terminal após a conexão com a nova rede.

Atualmente, verifica-se que o handover vertical, no sentido WWAN para WLAN, implica na interrupção da comunicação por um tempo

significativo o suficiente para resultar em incômodo e em perda de informação do sistema por parte dos usuários, principalmente para aplicações de comunicação em tempo real, tais como voz e vídeo.

Uma solução normalmente adotada para solucionar o problema de interrupção da comunicação é manter a interface aérea da rede WWAN do terminal ligada simultaneamente à interface aérea WLAN. Assim, torna-se possível realizar a transferência da sessão ativa, e realizar o handover somente depois do terminal ter capacidade de encaminhar os pacotes IP pela interface aérea WLAN. Entretanto, essa implementação possui os seguintes problemas:

a) Elevado consumo de energia por manter os dois estágios rádio ligados simultaneamente, reduzindo o tempo de duração da carga da bateria do terminal móvel;

b) Complexidade e custo elevado no projeto do terminal, pois as duas interfaces aéreas necessitam ser totalmente independentes, com capacidade de encaminhar pacotes de forma independente. Além disso, os procedimentos de conexão e autenticação em uma das interfaces devem ocorrer enquanto a sessão continua ativa na outra; e

c) Potencial interrupção ou perda da comunicação caso haja um rápido decaimento do sinal da rede de origem antes de completada a realização do handover, visto que não há necessidade de otimização do tempo de conexão e autenticação na nova rede.

Algumas soluções alternativas para autenticação em redes WLAN no cenário de handover vertical já foram propostas. Os exemplos mais significativos são listados a seguir.

Na primeira delas, Li-Der Chou, W. C. Lai, Y. C. Lin, C. M. Huang e C. H. Lin Chou em sua obra "Signaling Traffic Volume Generated by Mobile and Personal Communications" propuseram a utilização de agentes inteligentes (IA - Intelligent Agents) que seriam enviados à rede para executar os procedimentos de conexão e autenticação com antecedência. Os agentes inteligentes para usuários (UIAs - User Intelligent Agents) poderiam ser configurados para se autenticar em nome do usuário e os agentes inteligentes

de servidor (SIA - Server Intelligent Agent) poderiam ser configurados para autenticar localmente os usuários. Para que esta proposta seja viabilizada, a chave de autenticação individual Ki armazenada no SIM e no HLR/AuC (Home Location Register/Authentication Center) deve ser compartilhada pelos agentes inteligentes, gerando uma vulnerabilidade no sistema e violando o princípio básico de segurança das redes GSM, que é a proteção da chave de autenticação individual Ki de acesso ou de leitura por qualquer aplicação não definida pelo 3GPP (3rd Generation Partnership Project).

Em uma outra solução, Scott C. H. Huang, Hao Zhu e Wensheng Zhang, em sua obra "SAP: Seamless Authentication Protocol for Vertical Handoff in Heterogeneous Wireless Networks" desenvolveram um protocolo de autenticação chamado de SAP (Seamless Authentication Protocol), Protocolo de Autenticação Contínua, em que dois servidores de autenticação compartilham uma chave privativa comum e secreta utilizada para gerar a chave temporária de handover. A rede de acesso WLAN armazena esta chave temporária e a utiliza para admitir o terminal por um curto período de tempo, evitando os atrasos associados à consulta e geração de vetores pela rede WWAN. O tempo de validade da autenticação temporária deve ser o suficiente para permitir que a associação completa seja efetuada em paralelo à sessão ativa. Esta solução possui qualidades que podem ser exploradas, como a autenticação transparente, mas também cria uma vulnerabilidade adicional ao permitir a autenticação de vários terminais com um mecanismo que utiliza uma única chave comum.

Deste modo, a presente invenção proporciona uma arquitetura que soluciona os problemas ainda existentes de forma mais eficiente, alterando a arquitetura de autenticação na rede WLAN de maneira a reduzir o tempo de indisponibilidade da comunicação durante o handover para um valor inferior ao perceptível pelos usuários do sistema. Com esta solução, evitam-se também os problemas inerentes das outras alternativas descritas acima.

OBJETIVOS DA INVENÇÃO

O objetivo da presente invenção é, portanto, proporcionar um

método seguro de troca de chaves entre os elementos da arquitetura de redes, definindo um segredo específico para cada terminal móvel e a rede de acesso WLAN assim como definir uma forma de compartilhamento segura deste segredo.

Outro o objetivo da presente invenção é diminuir o atraso evidenciado durante o procedimento de autenticação. Assim, a presente invenção visa minimizar as principais causas do atraso na realização do handover vertical, a saber: o tempo de espera para receber as chaves da rede caseira do assinante e a utilização de enlaces sobre a Internet para encaminhar as mensagens de autenticação até o servidor AAA da rede caseira, para verificar o resultado retornado pelo terminal.

BREVE DESCRIÇÃO DOS DESENHOS

A presente invenção, juntamente com seus objetivos, características e vantagens adicionais, será mais bem entendida a partir da seguinte descrição dos desenhos que ilustram, a título exemplificativo, o melhor modo de execução considerado para realizá-la, a saber:

a figura 1 ilustra um modelo esquemático de uma das arquiteturas de autenticação já conhecidas do estado da técnica;

a figura 2 ilustra o modelo esquemático da nova arquitetura de autenticação proposta pela presente invenção, assim como seus componentes;

a figura 3 mostra o atraso médio para transmitir um pacote com controle de retransmissão sobre quadros da rede WLAN;

a figura 4 representa o modelo de filas para análise do atraso no sentido terminal-rede; e

a figura 5 representa o modelo de filas para análise do atraso no sentido rede-terminal.

DESCRIÇÃO DETALHADA DA INVENÇÃO

A Figura 1 da presente invenção ilustra como é a atual arquitetura de autenticação na interconexão das redes heterogêneas WWAN celular e WLAN. Basicamente, a figura 1 ilustra um modelo de autenticação entre uma rede GPRS HPLMN 40 e uma rede WLAN 50 visitada. Na figura 1, os

elementos interligados através de linhas tracejadas possuem interesse somente em tráfego de sinalização, enquanto que os elementos interligados através de linhas contínuas possuem interesse também em tráfego de dados, como por exemplo voz e multimídia.

A rede GPRS HPLMN 40, ou simplesmente WWAN, compreende uma unidade de registro de assinantes HLR (Home Location Register) 1 que é uma base de dados de registro de localização, na qual assinantes são subscritos com o propósito de gravar informações, tais como informação de subscrição e informação de localização. Um dos protocolos de comunicação que pode ser utilizado pelas interfaces com o HLR 1 é o protocolo para aplicações móveis MAP 110, 115 (Mobile Application Part), uma extensão específica para redes móveis da sinalização SS7, usada para comunicação entre elementos da rede CN (Core Network), utilizado na comutação de pacote, e para comunicação entre diferentes redes públicas de telefonia móvel PLMNs (Public Land Mobile Network).

A unidade HLR 1 comunica-se com a unidade SGSN 3 (Serving GPRS Supporting Node), que é o elemento central no domínio de comutação de pacote (Packet Switched) através de um protocolo MAP/SS7 115. Essa unidade SGSN 3 controla o estabelecimento de sessões de dados pelos terminais e contém dois tipos de informações relacionadas aos terminais sobre seu controle: de subscrição e de localização. Além disso, a unidade SGSN 3 comunica-se com a estação de transmissão 2 através da interface Gb 125. A estação de transmissão 2 é responsável por tratar o tráfego e a sinalização entre o terminal móvel 10 e a rede, no presente caso, WWAN.

Outro elemento presente na arquitetura atual é a unidade GGSN 4 (Gateway GPRS Support Node). Sua função é executar o roteamento do tráfego "entrante" e "sainte" e manter informações de subscrição e de localização que são recebidas através da HLR 1 e dos elementos SGSN 3, este último através da interface Gn 130.

As interfaces Gb 125, Gn 130, Gi 210 e Um 120 são interfaces padrões para troca de dados e sinalização definidas pelo 3GPP na especificação 3GPP TS 23.002.

O terminal móvel (MS) 10 consiste do equipamento físico que pode ser utilizado por um assinante da rede pública de telefonia móvel PLMN e sua comunicação com a rede WWAN 40 pode ser realizada através da interface rádio, por exemplo.

A rede ilustrada na figura 1 utiliza ainda a autenticação EAP-SIM, ou seja, utiliza o protocolo EAP para autenticação e distribuição de chaves utilizando o cartão SIM, assim como o processo de autenticação padrão definido para a rede GSM. O EAP-SIM baseia-se no mecanismo de desafio e resposta definido para o GSM, utilizando o algoritmo A3/A8 de autenticação e derivação de chave que é executável no cartão SIM. O desafio dado ao cartão SIM é um número randômico de 128 *bits* (RAND). O algoritmo do cartão SIM utiliza o RAND e a chave de autenticação individual Ki, armazenada internamente, como entradas para produzir uma resposta de 32 bits (SRES) e uma chave longa de 64 bits, ou chave cifrada Kc (cipher key), como saída.

Em contrapartida, a rede de acesso WLAN 50 é responsável por encapsular os pacotes de autenticação gerados pelo terminal móvel 10 em pacotes RADIUS e direcioná-los para o servidor AAA 5, 6, 7.

O servidor AAA 5, 6, 7, que é baseado em protocolo RADIUS, basicamente tem a função de identificar o terminal móvel 10 como sendo pertencente à rede HPLMN 40 e é responsável por disparar a requisição de autenticação. O acrônimo AAA significa autenticação, autorização e contabilização (Authentication, Authorization e Accounting) e RADIUS (Remote Authentication Dial In User Service) 140, 145, 150 é um protocolo definido pelo IETF para transportar as funções de AAA. O protocolo RADIUS 140, 145, 150 permite que um servidor de acesso de rede possa acessar um servidor centralizado e compartilhado para buscar serviços de AAA.

Com base nos padrões existentes e nas propostas de alteração conhecidas até o momento, foi possível definir algumas premissas básicas que devem ser seguidas por uma arquitetura de autenticação transparente em rede WLAN de forma a tornar a mesma aplicável nos cenários de handover vertical de terminais móveis executando aplicações de tempo real:

a) manter, no mínimo, o mesmo nível de segurança existente na

rede WWAN caseira do usuário;

b) não impactar negativamente na qualidade da sessão durante o handover, isso é, ter duração máxima de interrupção no handover de 40 ms, em conjunto com o procedimento de conexão;

c) poder realizar autenticação inicial na rede WLAN de forma independente do tempo de espera pelos vetores de autenticação retornados pela rede WWAN; e

d) não comprometer as chaves compartilhadas utilizadas pela rede WWAN (p. ex.: chave de autenticação individual Ki).

Com base nas condições acima e também com foco no fator de interoperabilidade com os sistemas atuais, a presente invenção também é igualmente compatível com o padrão IEEE 802.11i. Do ponto de vista do procedimento de autenticação, o suporte ao padrão 802.11i significa que a autenticação deve ser realizada através de mensagens EAP, independentemente do método ou mecanismo específico.

Assim, a presente invenção define uma arquitetura baseada na introdução de um elemento funcional na rede WWAN e em cada rede WLAN passível de ser visitada pelo terminal móvel, a este elemento funcional é dado o nome de Servidor de Distribuição de Chaves (SDC). O Servidor de Distribuição de Chaves (SDC) introduzido na arquitetura da presente invenção é responsável por realizar a distribuição antecipada das chaves de autenticação temporárias das redes WLAN elegíveis para receber o terminal móvel no handover seguinte. Com a introdução deste elemento e a alteração de alguns dos procedimentos de autenticação entre o terminal móvel e o servidor AAA da rede WLAN visitada, verifica-se a obtenção de uma redução significativa na interrupção do serviço, interrupção essa devida à autenticação durante o handover vertical.

Deste modo, a arquitetura da presente invenção continua permitindo a utilização de arquiteturas voltadas para o suporte às necessidades de roaming de assinantes WLAN e mantém as premissas de segurança definidas pelos padrões atuais, inclusive com a manutenção do algoritmo de autenticação em uso. Essa arquitetura de autenticação, objeto da presente in-

venção, é ilustrada em detalhes na figura 2.

Na rede caseira WWAN 40, o servidor de distribuição de chaves - SDC HPLMN 20 é conectado ao elemento GGSN 4 através da interface Gi 210 e possui, para fins de confidencialidade na transmissão de informação, algum mecanismo-padrão através de túnel IPSec. Na rede G-PRS/GSM/UMTS, o terminal móvel é autenticado segundo os métodos padrões definidos para redes 3GPP, considerando que nessas redes existem mecanismos nativos para garantir a segurança na troca de dados entre o terminal móvel e os elementos de rede, incluindo o GGSN 4. Além disso, o SDC HPLMN 20 também pode realizar uma conexão segura com o terminal móvel 10 registrado na rede de acesso WWAN 40, pois o mesmo pode ser colocado internamente na rede local onde se encontra a interface Gi 210.

Em contrapartida, na rede WLAN visitada 50, o servidor de distribuição de chaves SDC WLAN 30 opera na mesma rede do servidor AAA 7 e deve possuir, para fins de confidencialidade na transmissão de informações, algum mecanismo-padrão através de túnel IPSec.

Entre o SDC HPLMN 20 e os diversos SDC WLAN 30, é considerado haver também algum mecanismo de troca segura de dados 215, através de métodos padrões de criptografia.

Basicamente, o SDC WLAN 30 tem as funções de:

a) criar, sob requisição, novos pares de chaves de autenticação, aqui designadas como Ka, específicas e vinculadas a uma identificação específica do terminal móvel, como por exemplo: IMSI (International Mobile Subscriber Identity) registrado no cartão SIM (Subscriber Identity Module), também chamado de USIM (UMTS Subscriber Identity Module); e

b) enviar as chaves criadas para o SDC HPLMN 20 e para o servidor AAA 7 da rede WLAN visitada 50 através de conexão segura estática 215, 220, ou seja, previamente configurada.

Da mesma forma, o SDC HPLMN 20 tem basicamente as funções de:

a) requisitar uma chave de autenticação específica para o SDC WLAN 30 em nome do terminal da rede WWAN 40, a requisição sendo ba-

seada nas informações enviadas pelo terminal móvel de identificação do terminal móvel, de localização de célula do terminal móvel e, no SSID (informação de identificação da rede ou Service Set Identifier (IEEE 802.11)) da rede WLAN alvo 50;

b) manter a base de endereços do SDC WLAN 30 associada aos SSID específicos da rede WLAN 50 e a localização geográfica da rede WLAN 50. Essas informações são fundamentais para garantir a identificação unívoca da rede WLAN 50 e do SDC WLAN 30 associado; e

c) retornar para o terminal móvel 10 a chave de autenticação Ka criada pelo SDC WLAN 30.

Apenas a título exemplificativo da concretização preferida, o servidor AAA 7 comunica-se com o terminal móvel 10 preferencialmente através de um comutador wireless 8, que por sua vez comunica-se com pelo menos um ponto de acesso Wi Fi 9, através dos quais o terminal móvel 10 será comunicado. Importante ressaltar que os pontos de acesso Wi Fi 9 e os comutadores wireless 8 são elementos essenciais e amplamente encontrados em redes WLAN.

O protocolo de troca de informação entre o SDC HPLMN 20 e os terminais móveis 10 ainda registrados na rede WWAN 50 pode ser baseado em protocolo HTTP padrão. Entre os elementos SDC 20 e 30, as informações podem ser trocadas via arquivos XML e entre o SDC WLAN 30 e o servidor AAA 7, as informações podem ser trocadas via qualquer protocolo de troca de dados seguro suportado pelo servidor AAA 7.

O método de operação da arquitetura objeto da presente invenção baseia-se na troca antecipada de chaves temporárias de autenticação com o auxílio da rede WWAN 40. As chaves trocadas e armazenadas no terminal móvel 10 e no servidor AAA 7 são utilizadas para autenticar o terminal móvel 10 na rede WLAN 50, seguindo os princípios definidos pelo padrão IEEE 802.11i.

As funções executadas pelo terminal móvel 10 na arquitetura da presente invenção são:

a) solicitar, enquanto o terminal móvel 10 ainda está registrado

na rede WWAN 40, que o SDC HPLMN 20 requisite as chaves de autenticação para serem enviadas às redes WLAN 50 próximas. As redes WLAN 50 podem ser localizadas através de mecanismo-padrão de scanning da rede 802.11;

b) informar a identificação do terminal móvel 10 ao SDC, assim como o SSID da rede WLAN 50 visada e a célula da rede WWAN 40 em que ele se encontra;

c) receber as chaves de autenticação Ka retornadas pelo SDC HPLMN 20 através da rede GPRS e armazená-las em área segura enquanto permanecer no raio de alcance da possível rede WLAN 50 visada;

d) ao tomar a decisão de conectar na rede WLAN visada 50, utilizar a chave de autenticação Ka recebida na autenticação EAP-SIM no lugar da chave de autenticação individual Ki armazenada no cartão SIM para validação e geração do material utilizado na autenticação mútua. Esta primeira autenticação é temporária e deve ser feita através do envio de endereço de identificação (NAI) com domínio específico, de forma a informar a natureza temporária desta autenticação para o servidor AAA 7; e

e) iniciar o procedimento de autenticação completa utilizando os dados padrões originais armazenados no cartão SIM, realizados após a autenticação temporária bem-sucedida, do registro das aplicações na rede IMS e do completo restabelecimento da sessão.

Além disso, o servidor AAA 7 de autenticação da rede WLAN 50 deve suportar as seguintes funções:

a) realizar a autenticação temporária do terminal móvel 10 com base no endereço NAI retornado e na chave de autenticação Ka específica recebida do SDC WLAN 30;

b) para realizar a autenticação temporária, o servidor AAA 7 deve implementar o algoritmo A3/A8 para poder gerar os vetores de autenticação de forma autônoma do HLR 1 da rede WWAN 40, porém baseado no NAI do terminal móvel 10 e na chave de autenticação Ka recebida. Os vetores de autenticação podem ser gerados quando a chave Ka é recebida, com o objetivo de reduzir o atraso durante a autenticação temporária;

c) controlar o tempo de associação do terminal móvel após a realização da autenticação temporária e desconectar os terminais móveis incapazes de realizar autenticação completa após um período predefinido de tempo; e

d) enviar mensagens RADIUS accounting (contabilização dos dados) para o servidor AAA intermediário (não-mostrado), para registro das atividades no assinante em roaming. Apesar de não ter sido mostrado, o servidor AAA intermediário, que na figura 1 foi ilustrado como servidor AAA 6, encontra-se presente nestes tipos de rede com a finalidade de tarifação e cobrança, não estando relacionado diretamente com a função de autenticação inicial.

Além da arquitetura de autenticação proposta pela presente invenção, a rede WLAN 50 pode possuir uma topologia de servidores AAA descentralizados, com menos carga e mais próximos às redes de acesso, com o objetivo de diminuir o tempo de processamento de autenticação verificado nas medidas realizadas na presente invenção. As principais vantagens desta arquitetura de autenticação proposta são: a troca antecipada de chaves de autenticação específicas para cada terminal móvel, sem consumo do tempo de autenticação; a utilização de arquitetura de autenticação temporária sem a necessidade de realização de consulta em servidores AAA 5, 6 e bases HLR 1 externas à rede WLAN 50 durante o handover; e a utilização de chaves individuais específicas e exclusivas para cada terminal móvel 10 durante a autenticação temporária, aumentando o nível geral de segurança na rede WLAN 50 em relação às soluções do estado da técnica.

Com a arquitetura da presente invenção, o tempo de indisponibilidade do serviço durante o processo de handover vertical é reduzido para valores menores que os recomendados pelos padrões. Vale ressaltar que, como a troca de chaves de autenticação Ka ocorre antes do procedimento de handover, o tempo não é afetado. Esse tempo de autenticação durante o handover é bastante reduzido, por não necessitar de consulta à rede WWAN caseira e por não utilizar servidores AAA centralizados de alta capacidade e com enlaces IP via a rede Internet e sobre longas distâncias.

EXEMPLOS DE CONCRETIZAÇÃO DA PRESENTE INVENÇÃO:

Este exemplo ilustra a realização da modelagem analítica de uma arquitetura para autenticação em redes WLAN, onde é analisado o atraso na execução de handover vertical entre redes WWAN e WLAN com o objetivo de avaliar e quantificar o tempo de interrupção do serviço decorrente do acréscimo de autenticação do terminal baseada nos padrões IEEE 802.1x e IEEE 802.11i com a utilização de protocolo EAP-SIM pela rede WLAN.

A arquitetura foi modelada analiticamente para várias condições e taxas de transmissão através da utilização dos modos IEEE 802.11b e IEEE 802.11g.

Através dos resultados obtidos, avaliou-se o impacto da introdução na rede WLAN da autenticação baseada no padrão IEEE 802.11i no atraso da execução do handover vertical entre sistemas WWAN e WLAN oferecendo serviços convergentes multimídia.

i. Atraso de Transmissão em WLAN

As redes GPRS possuem elevada vulnerabilidade a ruído e elevada taxa de erro de bit (BER) devido ao seu uso externo. Para melhorar a performance nestas redes com relação à BER, são utilizados mecanismos de retransmissões baseados na camada de enlace, tal como o Radio Link Protocol ou RLP, que é utilizado sobre a camada MAC. Como as redes WLAN possuem uma largura de banda maior que as redes WWAN atuais e uma utilização geralmente interna (indoor), estes mecanismos de retransmissão não são utilizados.

Nos enlaces WLAN, alguns mecanismos de retransmissão podem ser realizados pelos protocolos superiores aos da camada de enlace, tais como: TCP, DHCP, EAP, etc. Para a análise aqui realizada, as seguintes premissas para as sessões fim a fim, relativas aos protocolos de camada de transporte com controle de retransmissão, são observadas: funcionamento em modo interativo e sem execução de retransmissão rápida (fast retransmit), ou seja, um pacote perdido sempre esgota o temporizador de round-trip (RTO).

As deduções a seguir são baseadas nos diversos modelos de atraso de transmissão de quadro e pacote, portanto já conhecidos do estado da técnica. Segundo o algoritmo de Karn, para os protocolos com controle de retransmissão, o valor de RTO é multiplicado por um fator constante *c* após cada retransmissão devido ao esgotamento do temporizador. Então, $RTO_{i+1} = c * RTO_i$, onde RTO_i é o *i*-ésimo valor do temporizador de retransmissão. Este efeito provoca o crescimento exponencial do RTO após cada retransmissão. Felizmente, os protocolos da camada de transporte, em sua grande maioria, não permitem um número infinito de retransmissão. Então, considerando que *n* retransmissões são necessárias para transmitir um pacote com sucesso, o atraso médio para transmitir um pacote é dado por:

$$\begin{aligned} & T' + RTO_1 + RTO_2 + \cdots + RTO_{N_m} \\ & T' + cRTO_o + c^2 RTO_o + \cdots + c^n RTO_o \\ & T' + cRTO_o \sum_{i=0}^{n-1} c^i \\ & T' + cRTO_o \frac{(1-c^n)}{(1-c)} \end{aligned} \qquad (1)$$

onde T' é o atraso de propagação fim a fim do pacote e RTO_o é o valor inicial do temporizador de retransmissão.

A taxa de perda de pacotes é dada por $q = 1-(1-p)^k$, onde *p* é a probabilidade de um quadro estar com erro no enlace aéreo (FER) e *k* é o número de quadros do enlace aéreo contidos no pacote. A probabilidade de transmitir um pacote com sucesso pode ser calculada como $(1-q)+(1-q)q+\cdots+(1-q)q^{N_m}-1 = 1-q^{N_m}$. Utilizando a equação anterior e a equação 1 pode-se obter o atraso médio para transmitir um pacote com controle de retransmissão sobre a interface WLAN com não mais que N_m tentativas de retransmissão como:

$$D' = (1-q)\left[D + cRTO_o \frac{1}{(1-c)} + (k-1)\tau\right] + \cdots + (1-q)q^{N_m-1}\left[D + cRTO_o \frac{(1-c^{N_m-1})}{(1-c)} + (k-1)\tau\right]$$

$$D' = D + (k-1)\tau + cRTOo \frac{(1-q)}{(1-c)}\left[\frac{(1-q^{N_m})}{(1-q)} - \frac{(1-q^{N_m}c^{N_m})}{(1-qc)}\right] \qquad (2)$$

onde *D* é o atraso de propagação fim a fim do quadro sobre enlace WLAN e *τ* é o tempo inter-quadro. A figura 3 ilustra o atraso médio cal-

culado pela equação 2, ou seja, o atraso médio para transmitir um pacote com controle de retransmissão sobre quadros da rede WLAN.

O padrão IEEE 802.11 especifica que o tamanho máximo do payload é de 8184 bits, ou 1023 bytes. Como para mensagens DHCP é possível ter um comprimento máximo de 548 bytes, isso significa que temos $k = 1$ tanto para 802.11b quanto para 802.11g. Para mensagens EAP temos um comprimento máximo de 280 bytes e como estas mensagens são transportadas diretamente sobre a camada de enlace na interface aérea WLAN e devido ao fato do protocolo EAP não suportar fragmentação, temos também $k = 1$. Considerando os dados acima e também que o valor típico de c é igual a 2, temos que a equação 2 pode ser simplificada para:

$$D' = D + 2RTO_o(1-q)\left[\frac{(1-2^{N_m}q^{N_m})}{(1-2q)} - \frac{(1-q^{N_m})}{(1-q)}\right] \quad (3)$$

O atraso médio de transmissão fim a fim do canal WLAN (D) estimado é igual 1,4 ms para canal de 11Mbps (IEEE 802.11b) e de 0,4 ms para canal de 54Mbps (IEEE 802.11g), para payload de 1500 bytes e 10 terminais compartilhando o canal, segundo cálculos realizados utilizando a metodologia proposta por Giuseppe Bianchi em seu paper *"Performance Analysis of the IEEE 802.11 Distributed Coordination Function"* publicado em pelo jornal do IEEE em março de 2000.

O valor inicial de *RTO* é estimado como sendo o valor de atraso de round-trip e o valor do número máximo de retransmissões (N_m) é estimado como dez, conforme indicado por Sajal Das, Enoch Lee, Kalyan Basu, Naveen Kakani e Sanjoy Das em seu artigo *"Performance optimization of VoIP calls over wireless links using H.323 protocol"* de 2003.

No processo de conexão à rede WLAN e de autenticação, temos quatro trocas de mensagens DHCP, cinco mensagens ARP (sendo três Gratuitous ARP, com intervalos de 0,5s e 1s entre elas, e um diálogo de requisição de endereço MAC (não considerado por ser realizado entre o tempo de espera de esgotamento de temporização das mensagens Gratuitous ARP) e 8 troca de mensagens EAP. Os tempos de atraso devido a estas trocas de mensagens podem ser calculados, respectivamente, como: $D_{DHCP} = 4D'_{DHCP}$;

$D_{ARP} = (3D'_{ARP} + ARP_{wait})$ e $D_{EAP} = 8D'_{EAP}$. Os valores D'_{DHCP}, D'_{ARP} e D'_{EAP} são calculados a partir da equação 3 com os valores de RTO_o e N_m específicos para cada um dos protocolos. O valor de ARP_{wait} total é de 1,5s (temporização de 0,5s mais 1s) para o cenário de utilização de terminais baseados em sistema operacional *Microsoft Windows Móbile*®. O valor acima foi obtido segundo informação fornecida pela *Microsoft* em http://support.microsoft.com/kb/199773/en-us.

ii. Atraso de Autenticação

No processo de handover do terminal as mensagens de autenticação são processadas por diversos elementos de rede e transportadas por diferentes protocolos, tais como EAP, RADIUS e MAP. O protocolo EAP é transportado diretamente sobre a rede 802.11, o protocolo RADIUS é transportado sobre IP em redes 802.3 e o protocolo MAP é transportado sobre rede de sinalização número 7 (SS7), através de enlaces TDM de 64 Kbps e de 2Mbps (enlace E1).

O atraso introduzido pelos elementos de rede pode ser calculado pela utilização da teoria clássica de filas para o sentido terminal-rede e rede-terminal, conforme ilustrado pelas figuras 4 e 5.

Ambos os casos possuem duas redes de filas abertas sem realimentação. Seguindo o proposto pelo Teorema de Burke, o atraso total de cada rede de fila em um sistema aberto pode ser calculado como a soma dos atrasos individuais de cada nó. Adicionalmente a esta consideração, as taxas de entrada em cada servidor não são devidos exclusivamente ao fluxo de mensagens de autenticação dos terminais realizando handover entre redes WWAN e WLAN, há outros fluxos de dados utilizando os mesmos servidores simultaneamente.

O tempo de atraso total para o processo de conexão na rede WLAN pode ser descrito como:

$$D_{CON} = D_{MH} + D_{DHCP} + D_{ARP} + D_{AP} + D_{DHCP\_Server} \quad (4)$$

Considerando-se que o processo de autenticação envolve troca de sinalização bidirecional com os elementos da rede, o tempo de atraso total para o processo de autenticação pode ser descrito como:

$$D_{AUT} = D_{MH} + D_{EAP} + D_{AP} + D_{AAA\_WLAN} + 4\Delta + D_{AAA\_INT} + D_{AAA\_WWAN} + D_{HLR} \quad (5)$$

O atraso de processamento devido ao terminal pode ser calculado como:

$$D_{MH} = \frac{1}{\mu - \lambda_{MH}} + \frac{1}{\mu' - \lambda_{MH'}} \quad (6)$$

Os atrasos de transmissão devido à interface WLAN são dados pelos componentes D_{DHCP}, D_{ARP} e D_{EAP} e são calculados conforme a equação 3 e segundo a descrição do tópico anterior sobre os atrasos de transmissão em WLAN.

O atraso de processamento devido aos elementos da rede de acesso WLAN pode ser calculado como:

$$D_{AP} = \frac{1}{\mu_{AP} - \lambda_{WLAN}} + \frac{1}{\mu_{AP'} - \lambda_{WLAN'}} \quad (7)$$

O atraso de processamento devido ao servidor de DHCP pode ser calculado como:

$$D_{DHCP\_Server} = \frac{\rho_{DHCP}}{(1 - \rho_{DHCP})}\left(\frac{2}{\lambda_{DHCP}}\right) \quad (8)$$

O atraso de processamento devido ao servidor AAA da rede WLAN para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_WLAN} = \frac{1}{\mu_{AAA\_WLAN} - \lambda_{AAA\_WLAN}} + \frac{1}{\mu_{AAA'\_WLAN} - \lambda_{AAA'\_WLAN}} \quad (9)$$

O atraso de processamento devido ao servidor AAA da rede intermediária para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_INT} = \frac{2}{\mu_{AAA} - \lambda_{AAA\_INT}} \quad (10)$$

O atraso de processamento devido ao servidor AAA da rede WWAN (HPLMN) para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_WWAN} = \frac{1}{\mu_{SS7} - \lambda_{AAA'\_WWAN}} + \frac{1}{\mu_{AAA} - \lambda_{AAA\_WWAN}} \quad (11)$$

O atraso de processamento devido à rede SS7 e ao HLR/AuC da rede WWAN (HPLMN) pode ser calculado como:

$$D_{HLR} = 2\Delta_{SS7} + \frac{\rho_{HLR}}{(1-\rho_{HLR})}\left(\frac{1}{\lambda_{HLR}} + \frac{1}{\lambda_{HLR'}}\right) \qquad (12)$$

O volume de tráfego inicial de autenticação via rede WLAN é muito menor que o existente na rede WWAN, pois a quantidade de usuários utilizando a rede WWAN é muito maior que a de usuários utilizando a rede WLAN. Devido a este fato, o atraso responsável pelo elemento HLR/AuC não é alterado pelo volume de tráfego de mensagens de autenticação incremental gerado pelos usuários na rede WLAN. Na implementação realizada, o valor do atraso relativo ao processamento do HLR foi medido em rede WWAN comercial, dimensionada para aproximadamente 3 milhões de assinantes. Nestas condições o atraso de processamento devido à rede SS7 e ao HLR/AuC da rede WWAN (HPLMN) para um par de mensagens de requisição e resposta pode ser alternativamente representado como:

$$D_{HLR} = 2\Delta_{SS7} + \Delta_{HLR} \qquad (13)$$

Os parâmetros utilizados nas equações anteriores e seus significados estão listados na tabela 1 a seguir.

Tabela 1 - Parâmetros usados no atraso de processamento

Parâmetro	Significado
μ	Taxa de processamento de mensagens do terminal para rede WLAN
μ'	Taxa de processamento de mensagens do terminal para aplicação
μ_{AP}	Taxa de processamento de mensagens da rede WLAN para Internet
$\mu_{AP'}$	Taxa de processamento de mensagens da rede WLAN para os terminais
μ_{AAA}	Taxa de processamento de mensagens dos servidores AAAs

Parâmetro	Significado
μ_{SS7}	Taxa de processamento de mensagens do servidor AAA para mensagens SS7
λ_{MH}	Taxa de chegada de mensagens da aplicação para terminal
$\lambda_{MH'}$	Taxa de chegada de mensagens no terminal da rede WLAN
λ_{WLAN}	Taxa de chegada de mensagens na rede WLAN pelos terminais
$\lambda_{WLAN'}$	Taxa de chegada de mensagens na rede WLAN pela Internet
λ_{DHCP}	Taxa de chegada de mensagens no servidor DHCP
λ_{AAA_WLAN}	Taxa de chegada de mensagens no servidor AAA pela rede WLAN
$\lambda_{AAA'\_WLAN}$	Taxa de chegada de mensagens no AAA (WLAN) pela rede intermediária
λ_{AAA_INT}	Taxa de chegada de mensagens no servidor AAA da rede intermediária
λ_{AAA_WWAN}	Taxa de chegada de mensagens no AAA (WWAN) pela rede intermediária
$\lambda_{AAA'\_WWAN}$	Taxa de chegada de mensagens no servidor AAA pela rede SS7
λ_{HLR}	Taxa de chegada de mensagens no HSS/AuC pela rede SS7
$\lambda_{HLR'}$	Taxa de chegada de mensagens no HSS em direção à rede SS7

Parâmetro	Significado
ρ_{DHCP}	Fator de utilização do servidor de DHCP
ρ_{HLR}	Fator de utilização do HLR
Δ_{SS7}	Atraso médio de mensagens na rede SS7
Δ_{HLR}	Atraso médio de processamento para consulta ao HLR/AuC
Δ	Atraso médio de mensagens pela Internet

O atraso total do processo de handover entre rede WWAN e WLAN é dado pela soma do atraso de conexão com o atraso de autenticação, ou seja:

$$D_{Handover} = D_{CON} + D_{AUT} \quad (14)$$

Com base nas equações demonstradas acima é possível calcular os atrasos de conexão e de autenticação de um terminal qualquer à rede WLAN, para diversas condições da rede de acesso.

Assim, com base na modelagem analítica desenvolvida, pode-se afirmar que o atraso de autenticação para a arquitetura proposta pode ser calculado como:

$$D'_{AUT} = D_{MH} + D_{EAP} + D_{AP} + D'_{AAA\_WLAN} \quad (15)$$

O valor de atraso para o servidor AAA da rede WLAN para a arquitetura proposta pode ser calculado como:

$$D'_{AAA\_WLAN} = \frac{n}{\mu_{AAA} - \lambda_{AAA\_WLAN}} \quad (16)$$

onde *n* é o número de pares de mensagens de requisição e resposta RADIUS para a arquitetura descrita, ou seja, três para o cenário de autenticação completa EAP-SIM e os demais parâmetros estando descritos na Tabela 1.

A tabela 2 mostra os valores dos parâmetros utilizados nas modelagens analíticas realizadas, considerando as condições de acesso a taxas de 11Mbps (IEEE 802.11b) e 54Mbps (IEEE 802.11g).

Tabela 2 - Parâmetros usados no atraso de processamento

Parâmetros	**802.11b (11Mbps)**	**802.11g (54Mbps)**
μ; $\mu_{AP'}$ *(nota 1)*	5,69 Mbps	14,42 Mbps
μ' *(nota 2)*	100 Mbps	100 Mbps
μ_{AP} *(nota 3)*	94,34 Mbps	94,34 Mbps
μ_{AAA}; μ_{AAA_WLAN}; μ_{AAA_WWAN} *(nota 8)*	160,14 pacotes/s	160,14 pacotes/s
$\mu_{AAA'\_WLAN}$ *(nota 8)*	79,761 pacotes/s	79,761 pacotes/s
λ_{MH} *(nota 5)*	15,22 Kbps	15,22 Kbps
$\lambda_{MH'}$ *(nota 1)*	5,69 Mbps	14,42 Mbps
λ_{DHCP} *(nota 6)*	1,20 Mbps	1,20 Mbps
λ_{WLAN}; $\lambda_{WLAN'}$ *(nota 7)*	100 Kbps	100 Kbps
λ_{AAA_INT}; λ_{AAA_WLAN} *(nota 8)*	124,27 pacotes/s	124,27 pacotes/s
$\lambda_{AAA'\_WLAN}$ *(nota 8)*	43,89 pacotes/s	43,89 pacotes/s
λ_{AAA_WWAN} *(nota 8)*	124,27 pacotes/s	124,27 pacotes/s
$\lambda_{AAA'\_WWAN}$ *(nota 11)*	3,93 Kbps	3,93 Kbps
ρ_{DHCP} *(nota 12)*	0,9	0,9
Δ_{SS7} *(nota 13)*	37,07 ms	37,07 ms
Δ_{HLR} *(nota 14)*	66,20 ms	66,20 ms
Δ *(nota 15)*	50 ms	50 ms

Notas:

(1) Calculado de acordo com metodologia desenvolvida por Bianchi em "Performance Analysis of the IEEE 802.11 Distributed Coordination Function" e considerando 10 terminais móveis utilizando simultaneamente o mesmo canal 802.11.

(2) Valor estimado para velocidade do barramento interno do terminal móvel.

(3) Valor efetivo (goodput) de taxa para interface 100BASE-T (Fast Ethernet) com MTU=1500 bytes, considerando o overhead devido ao protocolo TCP/IP e Ethernet.

(4) Múltiplo de 64Kbps (enlaces TDM) necessário para tratar o tráfego de autenticação entre servidor AAA da rede WWAN (HPLMN) e o HLR, via rede SS7.

(5) Calculado pelo tamanho total das mensagens de DHCP (Dynamic Host Configuration Protocol) e EAP trocados pelo terminal móvel.

(6) Considerado o tráfego gerado por um hotspot com 12 pontos de acersso (Access Points) - dado histórico médio de dimensionamento para cobertura de shopping-centers.

(7) Tráfego Internet estimado para um ponto de acesso com 10 terminais móveis conectados - dado histórico para dimensionamento de acesso WLAN.

(8) Valor obtido através das medidas realizadas em servidor AAA em rede real de produção.

(11) Resposta do HLR (protocolo MAP) às autenticações RADIUS, sobre enlaces TDM de 64Kbps.

(12) Valor estimado de fator de utilização para servidor DHCP (Dynamic Host Configuration Protocol).

(13) Valor medido em rede de sinalização em operação comercial do atraso médio de transmissão das mensagens de autenticação MAP SAI (Send Authentication Information).

(14) Valor medido em elemento em operação comercial do tempo gasto pela consulta ao elemento HLR/AuC.

(15) Valor estimado de atraso médio na Internet para enlaces terrestres de longa distância.

Os demais componentes da equação 15 são calculados conforme as equações 3, 6 e 7. Utilizando os valores listados na Tabela 2 e FER de 10%, obtém-se os seguintes valores de atraso de autenticação para a arquitetura da presente invenção, mostrados de forma comparativa com os resultados obtidos para os mecanismos de autenticação padrão:

Tabela 3 - Atrasos de autenticação previstos para a arquitetura com SDC proposta

Atraso de Autenticação	**11Mbps (802.11b)**	**54Mbps (802.11g)**
Autenticação Completa Padrão	1,16342 s	1,16044 s
Autenticação Rápida Padrão	0,68245 s	0,68022 s
Atraso de Autenticação (SDC)	88,55 ms	85,57 ms

Os valores de atraso calculados indicam uma melhora considerável no tempo de autenticação, com uma redução no atraso maior que 92% em ambos os casos. Apesar deste atraso ainda não está dentro do recomendado para interrupção de serviço durante o handover, o valor alcançado já se encontra na mesma ordem de grandeza do recomendado. Analisando os resultados com mais cuidado, verificou-se que, somente o tempo de processamento do servidor AAA contribui com 83,6 ms do tempo de atraso ilustrado na tabela 3. Isso é devido ao fato de terem sido utilizados os valores de taxa de processamento e de taxa de chegada, obtidos a partir de medições em servidor AAA centralizado e de grande porte.

Seguindo-se a premissa definida para a arquitetura da presente invenção, com servidores AAA descentralizados em servidores menores, obtém-se uma melhora no tempo de atendimento dos mesmos.

A arquitetura objeto da presente invenção também é utilizada em conjunto com a arquitetura IRAP de roaming de WLAN. Para isso, o servidor AAA intermediário não deve ser mais utilizado como proxy para as mensagens de autenticação temporária inicial, mas somente para a autenticação completa, realizada em paralelo com a sessão WLAN ativa do terminal e para tratamento de mensagens de RADIUS accounting.

iii. Análise dos Resultados

Com base nas medidas e nas modelagens analíticas realizadas, concluiu-se que os tempos gastos com os procedimentos padrões propostos para conexão e autenticação à rede WLAN não são compatíveis com o tempo máximo de interrupção no serviço de voz durante o handover conforme

recomendado por ETSI, que recomenda o máximo de 40 ms de interrupção do serviço de voz, bem abaixo dos resultados obtidos, conforme apresentado no exemplo, em que os tempos de conexão e de autenticação em redes WLAN podem atingir, em alguns casos, valores maiores que dois segundos. De uma maneira geral, esta interrupção do serviço tem duração suficiente para provocar a perda de informação durante a sessão multimídia de comunicação em tempo real estabelecida pelo usuário. Em outras palavras, isso significa que o tempo de interrupção do serviço observado torna o procedimento de handover perceptível pelo usuário final que esteja utilizando um serviço de comunicação multimídia em tempo real.

Em contrapartida, o resultado obtido pela modelagem analítica da presente invenção mostrou tempos de interrupção inferiores a 90ms, na mesma ordem de grandeza, portanto, do recomendado pelo ETSI.

Todavia, isso implica o entendimento de que a presente invenção e suas partes componentes descritas acima são apenas algumas das modalidades e exemplos de situações que poderiam ocorrer, o real escopo do objeto da invenção encontrando-se definido nas reivindicações.

REIVINDICAÇÕES

1. Sistema de autenticação para interconexão de redes sem fio heterogêneas (40, 50) compreendendo:

uma rede local (40) que compreende:

uma unidade de registro de assinantes (1) ;

uma unidade de estabelecimento de sessões de dados (3) que se comunica com a unidade de registro de assinantes (1) através de um protocolo específico (115);

uma unidade de roteamento de tráfego (4) que se comunica com a uma unidade de estabelecimento de sessões de dados (3) através de uma interface específica (130);

uma estação de transmissão (2) que se comunica com a uma unidade de estabelecimento de sessões de dados (3) através de uma interface específica (125) e com um terminal de acesso (10) através de uma outra interface específica (120);

uma rede visitada (50) que compreende:

pelo menos um servidor de autenticação, autorização e contabilização (7);

um comutador (8) que se comunica com um dos pelo menos um servidor de autenticação, autorização e contabilização (7) através de um protocolo (150);

pelo menos um ponto de acesso (9) que se comunica com o comutador (8) através de uma rede sem fio;

caracterizado pelo fato de que ainda compreende:

um servidor de distribuição de validadores (20) na rede local (40);

um servidor de distribuição de validadores (30) na rede visitada (50); e

em que os respectivos servidores (20, 30) são responsáveis pela criação e distribuição de pares de validadores vinculados a uma determinada identificação do terminal móvel (10) a ser autenticado.

2. Sistema, de acordo com a reivindicação 1, caracterizado pelo

fato de que o protocolo específico de comunicação entre a unidade de registro de assinantes (1) e a unidade de estabelecimento de sessões de dados (3) é preferencialmente um MAP/SS7 (115).

3. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que a interface específica de comunicação entre a unidade de roteamento de tráfego (4) e a unidade de estabelecimento de sessões de dados (3) é preferencialmente uma interface Gn (130) definida pela especificação 3GPP.

4. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que a interface específica de comunicação entre a estação de transmissão (2) e a unidade de estabelecimento de sessões de dados (3) é preferencialmente uma interface Gb (125) definida pela especificação 3GPP.

5. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que a interface específica de comunicação entre a estação de transmissão (2) e o terminal de acesso (10) é preferencialmente uma interface Um (120) definida pela especificação 3GPP.

6. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que o protocolo específico de comunicação entre o comutador (8) e um dos pelo menos um servidor de autenticação, autorização e contabilização (7) é preferencialmente um RADIUS/IP (150).

7. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que a comunicação entre o servidor (20) na rede local (40) e o servidor (30) na rede visitada (50) é realizada através de uma conexão segura estática (215) previamente configurada.

8. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de que compreende ainda servidores de autenticação, autorização e contabilização adicionais e descentralizados para diminuir o tempo de processamento de autenticação.

9. Método de autenticação de um terminal móvel (10) para interconectar redes sem fio heterogêneas (40,50) caracterizado pelo fato de que compreende as etapas de:

requisitar um validador em nome do terminal móvel (10);

criar um validador;

enviar para o terminal móvel (10) o validador criado; e

realizar a autenticação do terminar móvel (10) com base no validador criado.

10. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que a etapa de requisitar um validador compreende ainda as etapas de:

enviar uma primeira informação de identificação do terminal móvel (10) para o servidor (30) da rede visitada (50); e

requisitar ao servidor (30) da rede visitada (50) um validador para o terminal móvel (10) a partir do servidor (20) da rede local (40).

11. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que a etapa de criar um validador compreende ainda as etapas de:

criar pares de validadores específicos e vinculados a uma determinada identificação do terminal móvel (10).

12. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que a etapa de enviar para o terminal móvel (10) o validador criado compreende ainda as etapas de:

enviar por meio do servidor (20) da rede local (40) os validadores criados pelo servidor (30) da rede visitada (50) para o terminal móvel (10); e

enviar por meio do servidor (20) da rede local (40) os validadores criados para o servidor de autenticação, autorização e contabilização (7).

13. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa de realizar a autenticação do terminar móvel (10) com base no validador criado compreende ainda as etapas de:

armazenar os validadores recebidos no terminal móvel (10);

utilizar o validador recebido no terminal móvel (10) no lugar da chave de autenticação individual Ki armazenada no cartão SIM;

utilizar o validador armazenado no terminal móvel (10) para validação e geração da autenticação entre as redes local (40) e visitada (50);

enviar do terminal móvel (10) para o servidor de autenticação, autorização e contabilização (7) uma segunda informação de identificação; e

realizar a autenticação temporária do terminal móvel (10) no servidor de autenticação, autorização e contabilização (7) com base na segunda informação de autenticação recebida e no validador específico recebido do servidor de distribuição de chaves (30) da rede visitada (50).

14. Método, de acordo com a reivindicação 13, caracterizado pelo fato de que compreende ainda a etapa de:

gerar vetores de autenticação no servidor de autenticação, autorização e contabilização (7) com base na segunda informação de identificação do terminal móvel (10) e no validador recebido no mesmo.

15. Método, de acordo com a reivindicação 13 ou 14, caracterizado pelo fato de que a segunda informação de identificação do terminal móvel (10) compreende o endereço de autenticação NAI do terminal móvel (10).

16. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que compreende ainda a etapa de:

iniciar no terminal móvel (10) o procedimento de autenticação completa.

17. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que compreende ainda a etapa de:

controlar no servidor de autenticação, autorização e contabilização (7) o tempo de associação do terminal móvel (10) após a realização da autenticação temporária.

18. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que compreende ainda a etapa de desconectar o terminal móvel (10) incapaz de realizar autenticação completa após um período predefinido de tempo.

19. Método, de acordo com a reivindicação 11, caracterizado pelo fato de que a identificação do terminal móvel (10) compreende um IMSI registrado no cartão SIM/USIM.

20. Método, de acordo com a reivindicação 12, caracterizado pelo fato de que a etapa de enviar as chaves de autenticação para o servidor de (20) da rede local (40) e para o servidor de autenticação, autorização e

contabilização (7) é realizada através de conexão segura estática (215, 220).

21. Método, de acordo com a reivindicação 10, caracterizado pelo fato de que a etapa enviar uma primeira informação de identificação do terminal móvel (10) para o servidor (30) da rede visitada (50) compreende as informações de identificação do terminal móvel (10), de localização de célula do terminal móvel (10) e o SSID da rede alvo visitada (50).

22. Método, de acordo com a reivindicação 13, caracterizado pelo fato de que a etapa de armazenar os validadores recebidos no terminal móvel (10) compreende armazenar os validadores em uma área segura enquanto o terminal móvel (10) permanecer no raio de alcance da possível rede visitada (50).

23. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que a etapa de realizar a autenticação do terminal móvel (10) compreende ainda implementar preferencialmente o algoritmo A3/A8 para gerar vetores de autenticação de forma autônoma da unidade de registro de assinantes (1) da rede local (40).

24. Método, de acordo com a reivindicação 14, caracterizado pelo fato de que a etapa de gerar os vetores de autenticação inicia-se quando o validador é recebido no servidor de autenticação, autorização e contabilização (7).

25. Método, de acordo com a reivindicação 9, caracterizado pelo fato de que compreende ainda a etapa de enviar do servidor autenticação, autorização e contabilização (7) para o servidor autenticação, autorização e contabilização intermediário mensagens de contabilização para registro das atividades do terminal móvel (10) em roaming.

26. Método, de acordo com qualquer uma das reivindicações 9 a 25, caracterizado pelo fato de que a comunicação entre o servidor (20) na rede local (40) e o terminal móvel (10) é baseado preferencialmente no protocolo HTTP padrão.

27. Método, de acordo com qualquer uma das reivindicações 9 a 26, caracterizado pelo fato de que a comunicação entre o servidor (20) na rede local (40) e o servidor (30) na rede visitada (50) é realizada preferenci-

almente via arquivos XML.

28. Método, de acordo com qualquer uma das reivindicações 9 a 27, caracterizado pelo fato de que a comunicação entre o servidor (30) na rede visitada (50) e o servidor de autenticação, autorização e contabilização (7) é realizada via um protocolo (220) seguro de troca de dados suportado pelo servidor de autenticação, autorização e contabilização (7).

29.Método, de acordo com qualquer uma das reivindicações 9 a 28, caracterizado pelo fato de que o validador é uma chave de autenticação.

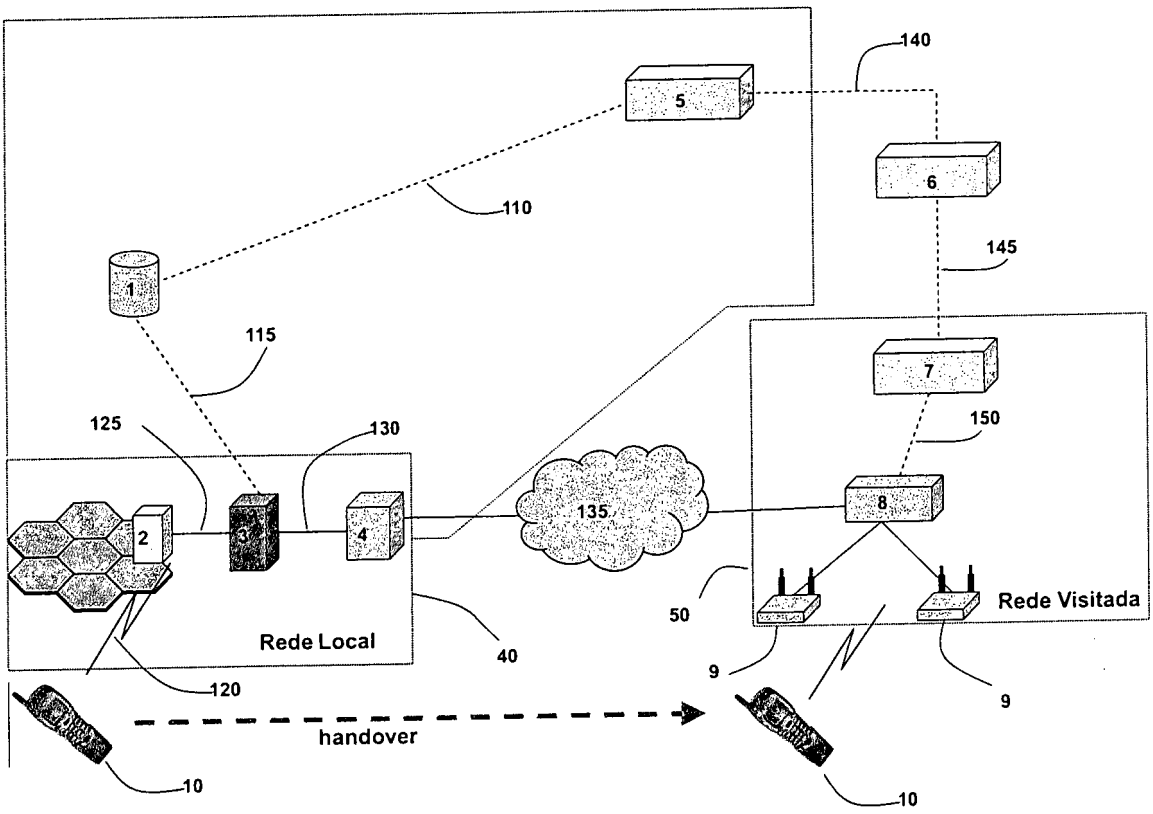

140
5
6
110
145
1
115
7
125
130
150
135
8
2
3
4
50
Rede Visitada
Rede Local
40
9
9
120
handover
10
10

FIG. 1

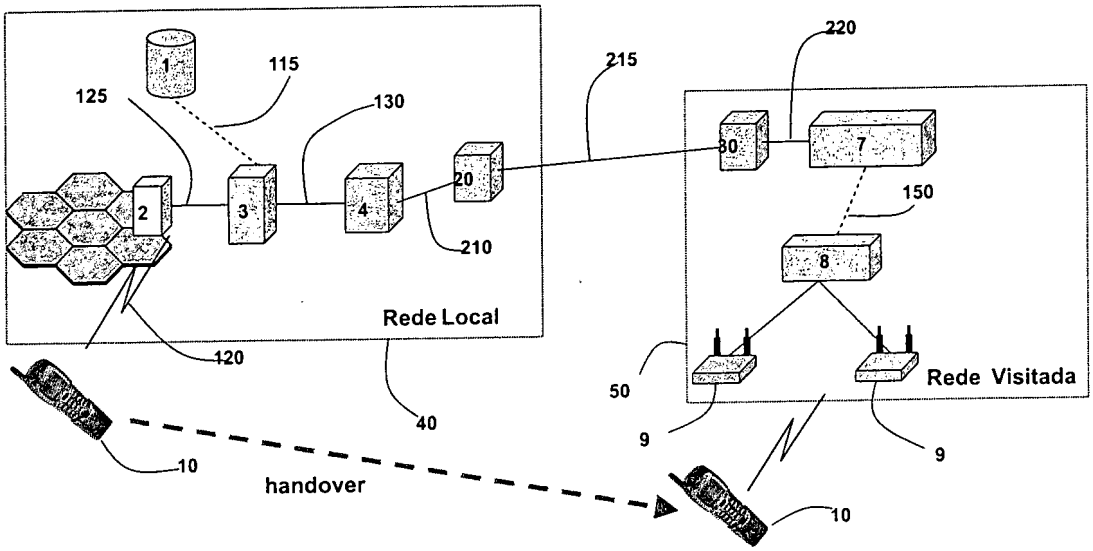

1
115
125
130
215
220
30
7
150
20
2
3
4
210
8
Rede Local
120
50
Rede Visitada
40
9
9
10
handover
10

FIG. 2

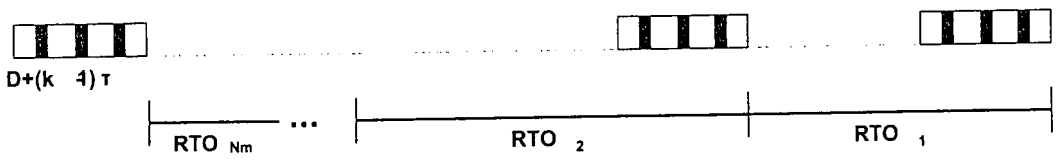

D+(k 1) T
RTO Nm
RTO 2
RTO 1

FIG. 3

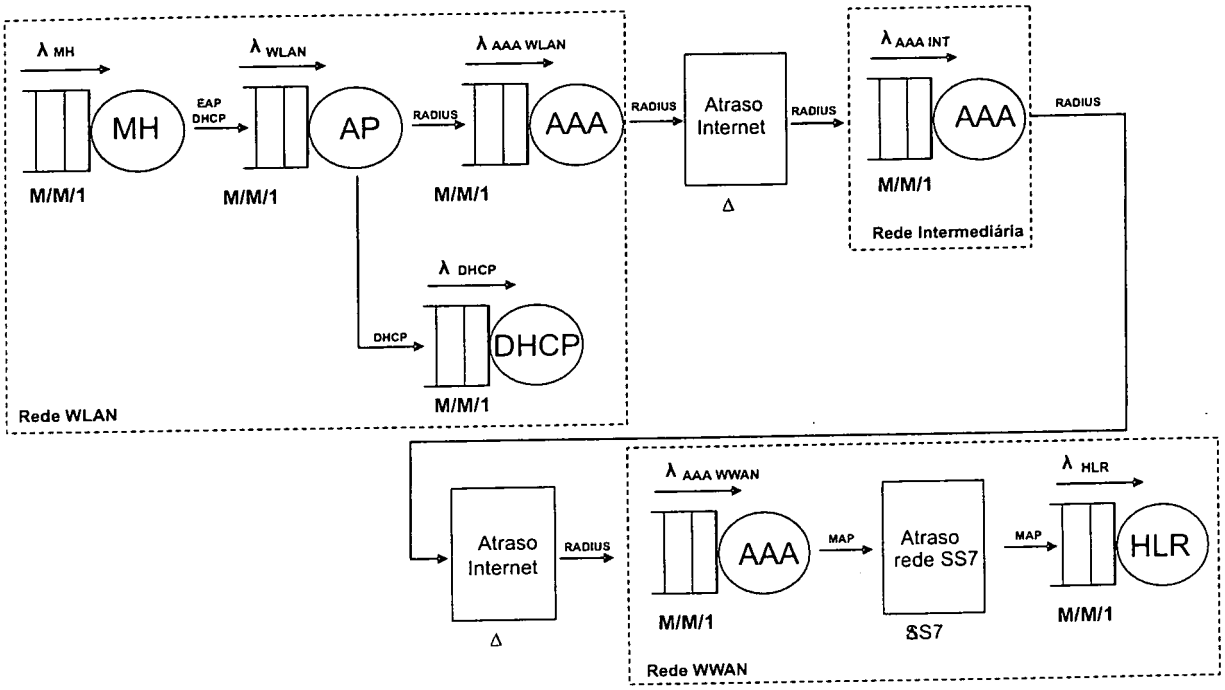

λ MH
λ WLAN
λ AAA WLAN
EAP
DHCP
RADIUS
MH
AP
AAA
M/M/1
M/M/1
M/M/1
RADIUS
Atraso
Internet
Δ
RADIUS
λ AAA INT
AAA
M/M/1
Rede Intermediária
RADIUS
λ DHCP
DHCP
DHCP
M/M/1
Rede WLAN
Atraso
Internet
Δ
RADIUS
λ AAA WWAN
AAA
M/M/1
MAP
Atraso
rede SS7
SS7
MAP
λ HLR
HLR
M/M/1
Rede WWAN

FIG. 4

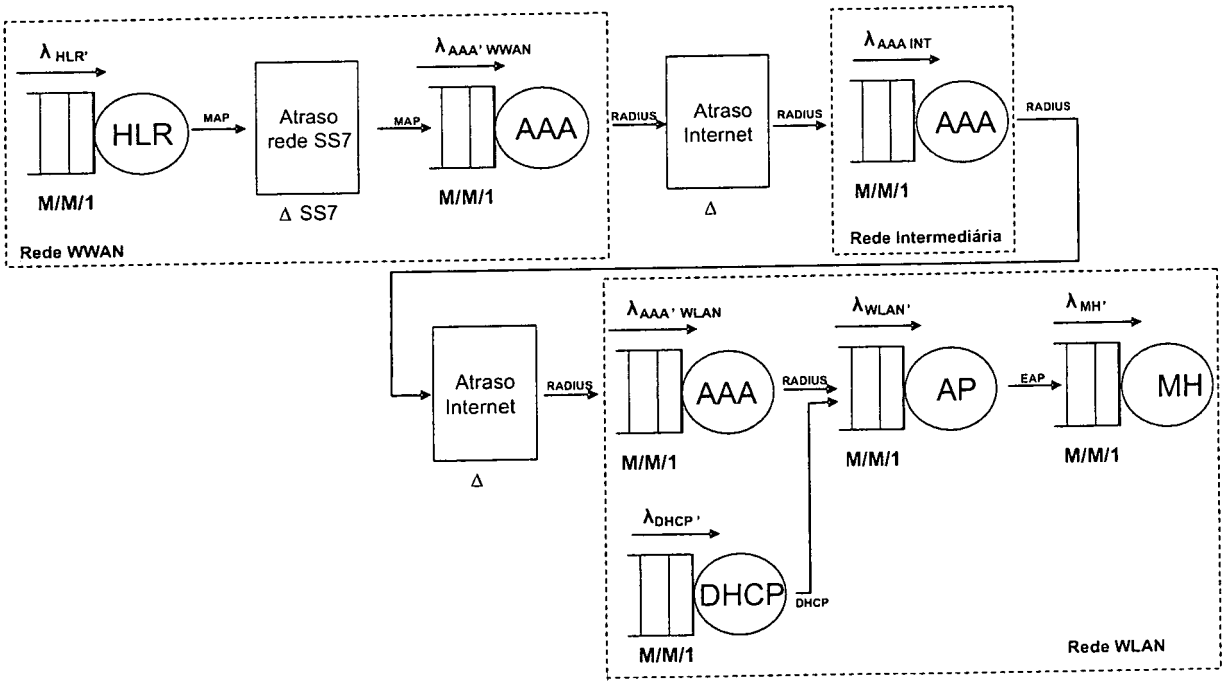

λ HLR'
HLR
M/M/1
MAP
Atraso
rede SS7
Δ SS7
λ AAA' WWAN
MAP
AAA
M/M/1
Rede WWAN
RADIUS
Atraso
Internet
Δ
RADIUS
λ AAA INT
AAA
M/M/1
Rede Intermediária
RADIUS
Atraso
Internet
Δ
RADIUS
λ AAA' WLAN
AAA
M/M/1
λ WLAN'
RADIUS
AP
M/M/1
λ MH'
EAP
MH
M/M/1
λ DHCP'
DHCP
DHCP
M/M/1
Rede WLAN

FIG. 5

RESUMO

Patente de Invenção: **"SISTEMA E MÉTODO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS".**

A presente invenção refere-se a um sistema e a um método de autenticação com redução de atraso para interconexão de redes sem fio heterogêneas (40, 50), preferencialmente WWAN celular e WLAN, com uma troca segura de chaves entre os elementos redes, utilizando-se de segredos específicos e compartilháveis para cada um dos elementos interconectados a e pela rede. Além disso, a presente invenção define uma arquitetura de rede baseada na introdução de um elemento funcional na rede WWAN e em cada rede WLAN passível de ser visitada pelo terminal móvel (10), a este elemento funcional é dado o nome de Servidor de Distribuição de Chaves (SDC) (20, 30). O Servidor de Distribuição de Chaves (SDC) (20, 30) introduzido na arquitetura da presente invenção é responsável por realizar a distribuição antecipada das chaves de autenticação temporárias das redes WLAN elegíveis para receber o terminal móvel no handover seguinte.