



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

(11) PI 0215728-4 B1

(22) Data do Depósito: 01/05/2002

(45) Data de Concessão: 07/06/2016



(54) Título: MÉTODO PARA PERMITIR UMA AUTENTICAÇÃO BASEADA EM SIM, CONTROLADOR DE ACESSO, TERMINAL SEM FIO E SISTEMA DE TELECOMUNICAÇÃO

(51) Int.Cl.: H04W 12/06; H04L 12/28; H04W 80/00; H04W 84/12

(52) CPC: H04W 12/06; H04L 12/2859; H04W 80/00; H04W 84/12

(73) Titular(es): TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

(72) Inventor(es): JESÚS ANGEL DE GREGORIO RODRIGUEZ, MIGUEL ANGEL MONJAS LLORENTE

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA PERMITIR UMA AUTENTICAÇÃO BASEADA EM SIM, CONTROLADOR DE ACESSO, TERMINAL SEM FIO E SISTEMA DE TELECOMUNICAÇÃO"**

5 CAMPO DA INVENÇÃO

A presente invenção refere-se geralmente a mecanismos de autenticação e de criptografia em cenários de Rede de Área Local sem Fio. Mais particularmente, a invenção refere-se a um dispositivo, sistema e métodos para uma autenticação baseada em SIM e a mecanismos de criptografia de uma camada 2 para proteger o caminho de comunicação a partir do Equipamento Terminal em diante.

ANTECEDENTE

Em 1999, a especificação 802.11b foi publicada pelo IEEE para acesso de Rede de Área Local Sem Fio (WLAN) em taxas de 11 Mbps. Este padrão tornou-se amplamente suportado pela indústria e possui uma enorme base instalada nas companhias empresariais, bem como pontos ativos publicamente acessíveis tal como aeroportos, hotéis, cafés e assim por diante.

Esta especificação 802.11b oferece até alguma extensão mecanismos de controle de autenticação e de acesso, bem como de confidencialidade, mas somente no caminho sem fio. A este respeito, dois métodos de autenticação são definidos neste padrão, a saber, "Sistema Aberto" e "Chave Compartilhada".

Quando o Sistema Aberto é utilizado, uma placa WLAN no Equipamento Terminal (TE) anuncia que ela deseja associar-se com o Ponto de Acesso WLAN (daqui para frente abreviado como AP). Nenhuma autenticação é executada e somente mecanismos básicos de controle de acesso são utilizados, como por exemplo, filtros de Controle de Acesso de Mídia (MAC) e Identificadores de Conjunto de Serviços (SSID).

Estes filtros MAC são dispostos para trabalhar de modo que somente placas WLAN cujo endereço MAC pertença a uma lista mantida pelo AP, tal como uma Lista de Controle de Acesso (ACL), sejam permitidos

de se associarem com o AP. Este mecanismo de controle de acesso possui uma utilidade limitada, desde que a identidade da entidade tentando se associar não realmente pertence a um usuário, mas ao invés disso ao próprio equipamento. Se um terminal ou placa for furtado, não existe autenticação baseada no usuário para impedir acesso aos recursos pelo equipamento furtado. Adicionalmente, à medida que os endereços MAC da placa WLAN sempre aparecem nos cabeçalhos dos quadros WLAN, fraudar o endereço MAC é um ataque trivial. Isto é de relevância especial, desde que a maioria das placas WLAN no mercado pode alterar seu endereço MAC apenas por utilizar o dispositivo de software.

O outro mecanismo de controle de acesso é o Identificador de Conjunto de Serviços (SSID) mencionado acima, o qual é um código alfanumérico que identifica a instância da WLAN com a qual o Equipamento Terminal (TE) está tentando se associar. Um dado AP somente permite a associação de placas WLAN que proporcionam um SSID correto. Entretanto, como este identificador é normalmente difundido pelos APs, e igualmente sem alterar o valor preestabelecido estabelecido pelo vendedor, este mecanismo de controle de acesso é, novamente, sem dúvida sem uso desde que uma pluralidade de ataques bem conhecidos possa ocorrer.

Um segundo método de autenticação mencionado acima é o assim chamado Chave Compartilhada. Este procedimento está embutido em um mecanismo de confidencialidade básica proporcionada pelo padrão de Privacidade Equivalente Com Fio (WEP), o qual é um algoritmo de criptografia simétrico baseado no RC4. Como tal, a autenticação é executada por se utilizar um mecanismo de pergunta - resposta, no qual ambas partes, a placa WLAN e o AP, apresentam para eles próprios uma mesma chave. Entretanto, esta chave é instalada e armazenada no Equipamento Terminal (TE) e por conseqüência, ela sofre das mesmas desvantagens como descritas quando se fala a cerca dos filtros MAC.

Além disso, uma série de documentos recentemente publicados tem apresentado a falha fundamental do próprio mecanismo de privacidade, ou seja, as falhas dos padrões WEP. Estas falhas começam com o uso de

chaves WEP estáticas, o que permite a um atacante descobrir as próprias chaves, desde que os vetores de inicialização dos algoritmos sejam enviados de forma clara dentro do quadro WEP. Uma série de ataques passivos, como, por exemplo, uma placa WLAN que somente fareja o tráfego, também permite deduzir as chaves.

No começo, parecia que apenas por renovar as chaves com um melhor gerenciamento de chave e por aumentar seu comprimento, por exemplo, de 40 para 128 bits, que o algoritmo poderia ser mais seguro ou, pelo menos, seguro o suficiente para alcançar uma segurança aceitável. Entretanto, mais e mais relatos recentes têm provado que o projeto do algoritmo como tal não proporciona um nível de segurança aceitável.

Atualmente, são feitos esforços pela indústria e pelos foros representativos para resolver as falhas nos padrões atualmente aplicáveis. O IEEE está atualmente definindo um novo padrão para aperfeiçoar os mecanismos de autenticação do 802.11b existentes e os resultados podem ser publicados como um assim chamado padrão 802.1x, um "Controle de Acesso de Rede Baseado em Porta", mas este trabalho ainda não está terminado. Além disso, esta maneira de se abordar somente leva em consideração a autenticação, de modo que um algoritmo de confidencialidade apropriado ainda é necessário. A este respeito, tendências correntes sugerem que um protocolo baseado no assim chamado protocolo de Sistema de Criptografia Avançada (AES) pode substituir o WEP. Contudo, o mecanismo de autenticação baseado em porta como sugerido na 802.1x possui um impacto significativos obre o sistema operacional do TE e nos software aplicáveis do AP, desde que o 802.1x apenas busca uma substituição para o mecanismo de autenticação baseado no WEP e para o próprio WEP.

Resumidamente, uma adoção massiva deste novo padrão 802.1x, com as falhas ainda não resolvidas mencionadas acima, irá levar a novos investimentos no equipamento WLAN, desde que todos os APs de uma dada WLAN teriam que ser substituídos ou, pelo menos, atualizados. Adicionalmente, e alguma coisa óbvia, qualquer mecanismo de confidencialidade somente proporciona proteção no caminho sem fio, ou seja, entre a

placa WLAN e o AP. Entretanto, o tráfego Ethernet correspondente além do AP não é de forma alguma criptografado.

Portanto, é um importante objetivo da presente invenção neste estágio, a provisão do dispositivo e métodos para permitir um mecanismo de autenticação eficaz dos usuários WLAN, bem como um mecanismo de criptografia completo por todo o caminho de comunicação começando a partir do Equipamento Terminal dos ditos usuários.

TÉCNICA RELACIONADA

Em resumo e como amplamente descrito acima, a autenticação nos padrões WLAN atualmente aplicáveis, a saber, 802.11. é não existente, ou baseada no dispositivo quando o endereço físico MAC da placa WLAN é utilizado para autenticar o TE. Isto é aparentemente impraticável para grandes disposições dado que uma criptografia obtida através do protocolo WEP como na WLAN, o qual é conhecido por sua fragilidade, não é encontrada a partir de diferentes setores apropriados para manter uma segurança aceitável.

A título de contraste, a autenticação nas redes móveis terrestres públicas mais recentes e convencionais como GSM, GPRS, ou UMTS seja feita por meio de um cartão SIM e por um conjunto de protocolos e algoritmos com segurança comprovada conhecidos como algoritmos de "Acordo de Autenticação e de Chave" (daqui para frente abreviado como AKA). A assim chamada autenticação baseada em SIM é baseada no usuário desde que uma SIM seja projetada para uso pessoal e protegida por um PIN de acesso.

Atualmente, operadores móveis desejam estender suas ofertas nas redes de acesso por incluir acesso de banda larga e a tecnologia WLAN torna isto possível com as taxas de acesso de até 11 Mbps, enquanto mantendo um custo de disposição extremamente baixo, principalmente devido ao uso de banda de espectro não licenciada na WLAN. Um operador móvel pode alcançar isto por instalar sua própria WLAN ou por assinar acordos com operadores WLAN existentes, mas em ambos os casos, os requerimentos de segurança devem ser pelo menos tão fortes quanto no caso de um

acesso móvel à rede principal dos operadores.

Para alcançar isto, um operador WLAN deve oferecer um mecanismo de autenticação e de criptografia que implique na posse de um cartão SIM. Este cartão SIM deve ser distribuída pelo operador móvel e pode ser o mesmo SIM utilizado para o acesso móvel, ou pode ser um SIM distribuído de propósito somente para acesso WLAN.

Uma WLAN convencional operada por uma terceira parte também pode ter seus próprios usuários locais e a autenticação a ser executada para o ditos usuários locais é totalmente até o operador WLAN. Por exemplo, esta autenticação para os usuários locais pode ser apenas baseada na identidade mais senha do usuário, ou mesmo absolutamente sem segurança. Entretanto, para estes usuários que assinaram com um operador móvel, a autenticação e outras questões de segurança através da dita WLAN devem ser comparáveis às na rede do operador móvel. Por outro lado, uma WLAN disposta e operada somente por um operador móvel deve negar acesso aos usuários não pertencendo a este operador móvel e devem somente implementar mecanismos de autenticação baseado em um cartão SIM.

Contudo, qualquer tentativa de introduzir mecanismos novos e seguros para autenticação e criptografia na WLAN deve ser direcionada para produzir o mínimo de impacto possível nos cenários WLAN correntes.

Uma tentativa muito interessante de resolver os problemas acima é descrita na publicação do pedido US 2002/0009199 com o título "Arranging Data Cipherring in a Wireless Telecommunication System". A instrução por trás deste pedido também apresenta um esquema de autenticação baseado em SIM.

Este esquema de autenticação baseado em SIM é, entretanto, pretendido para derivar uma chave de cifragem que é utilizada como a chave dos algoritmos WEP nativos da 802.11 para criptografia de tráfego entre o TE e o AP. A vantagem principal que este pedido introduz sobre as capacidades WEP existentes é a adição de um novo mecanismo para renovar as chaves uma vez por sessão. Além disso, este pedido é basicamente uma

versão modificada dos padrões WEP atuais e não resolve os problemas fundamentais declarados acima para a versão WEP original.

Contudo, setores diferentes na indústria têm estimado que ataques WEP bem conhecidos podem acertar uma chave WEP em menos do
5 que duas horas. Obviamente, se a chave WEP for estática e nunca renovada, como na versão WEP original, o problema é muito mais significativo. Por consequência, com a maneira de se abordar na US 2002/0009199, o problema está restrito aos limites da duração de uma dada sessão e se uma sessão se expandir além de poucas horas, o mesmo problema surge como
10 antes. Isto é claramente insuficiente para conceder níveis de segurança similares aos encontrados nas redes móveis terrestres públicas atuais.

A este respeito, é um objetivo da presente invenção a obtenção de um nível de segurança muito mais elevado permitindo ao operador escolher um algoritmo de criptografia que melhor se adapte às suas necessida-
15 des de segurança. Observa-se que normalmente existe uma negociação entre o nível de segurança e a performance. Portanto, aspectos adicionais como suportar chave com um comprimento de 128, 168, 256 bits, etc.; bem como suportar os algoritmos seguros mais recentes, como o AES por exemplo, e um procedimento de rotação de chave podem ser considerados outro
20 objetivo da presente invenção.

Além disso, de acordo com este pedido acima, US 2002/0009199, o caminho criptografado vai desde o Terminal Móvel até o AP, desde que o WEP seja somente aplicável para o caminho de rádio. A este respeito, o suporte para um caminho de criptografia a ser estabelecido
25 além do AP e cobrir também a parte com fio da WLAN, é um objetivo adicional da presente invenção.

Adicionalmente, o US 2002/0009199 esclarece que a designação de um endereço IP é feita antes de executar o processo de autenticação e por consequência, um usuário malicioso pode potencialmente iniciar
30 um conjunto inteiro de ataques bem conhecidos. Entretanto, se um usuário não tiver dispositivo para obter a conectividade IP antes de ter sido efetivamente autenticado, o risco diminuiria muito. Desse modo, é um objetivo adi-

cional da presente invenção a provisão de um mecanismo de autenticação para um usuário a ser realizado antes de fornecer a conectividade IP para o dito usuário.

Por outro lado, os pedidos US 2002/012433 e WO 01/76297, 5 descrevem, pelas mesmas modalidades exemplificativas comuns, um sistema onde um terminal adaptado sem fio pode se interconectar com uma rede móvel doméstica através de uma rede de acesso IP sem fio. A rede móvel doméstica sendo responsável por autenticar o usuário com uma autenticação baseada em SIM, enquanto que a rede de acesso IP sem fio permite ao 10 usuário acessar a rede Internet, uma vez autenticado. O terminal sem fio, a rede IP de acesso sem fio e a rede móvel todas comunicadas com um protocolo IP móvel. O sistema também compreende um Controlador de Acesso Público para controlar o acesso a partir de rede de acesso por radio para serviços de Internet. Este Controlador de Acesso Público aloca um endereço 15 IP para o terminal sem fio e autentica o terminal sem fio antes da conexão com a Internet ser estabelecida, e comunica mensagens de autenticação entre o terminal sem fio e a rede móvel doméstica. Além disso, a interface entre o terminal sem fio e o Controlador de Acesso Público é uma interface baseada em IP, em que o Controlador de Acesso Público e o terminal sem 20 fio são identificados pelos respectivos endereços IP de cada um. O fato do Controlador de Acesso Público e o terminal sem fio fazerem uso de um protocolo baseado em IP torna essencial que seja atribuído um endereço IP bem no começo, este endereço IP enviado do Controlador de Acesso Público para o terminal sem fio antes de estabelecer um canal de comunicação 25 seguro. Portanto, o mesmo problema como no pedido acima, US 2002/0009199, ocorre devido ao fato que a designação de um endereço IP é feita antes de rodar o processo de autenticação, e daí, um usuário malicioso pode potencialmente iniciar um conjunto completo de ataques bem conhecidos.

30 Em resumo, um importante objetivo da presente invenção é a provisão de um sistema, dispositivo e métodos para permitir uma autenticação de usuário baseada em SIM eficaz e para estabelecer um caminho de

criptografia completo, começando desde o TE, para usuários WLAN que são assinantes de uma rede móvel terrestre pública. Outro objetivo particularmente importante é que esta autenticação do usuário baseada em SIM pode ser executada antes de fornecer a conectividade IP para o dito usuário.

5 Um objetivo adicional da presente invenção é o suporte de chaves com comprimento variável, o uso de algoritmos de segurança à escolha do operador e a provisão de um procedimento de rotação de chave.

Ainda um objetivo adicional da presente invenção é a obtenção dos objetivos anteriores com um impacto mínimo sobre os cenários WLAN convencionais.

10 SUMÁRIO DA INVENÇÃO

Os objetivos da invenção são alcançados com um método para permitir uma autenticação baseada em SIM para usuários de uma rede de área local sem fio que são assinantes de uma rede móvel terrestre pública por meio de um mecanismo de autenticação de camada de ligação de dados (camada 2). Um importante aspecto deste método é que a conectividade IP somente é proporcionada para o usuário quando o processo de autenticação tiver completado com sucesso.

Os objetivos da invenção são assim alcançados com um método em que um terminal sem fio encontra um Ponto de Acesso acessível e requisita a associação com a rede de área local sem fio e o Ponto de Acesso aceita a requisição para isto. O terminal sem fio então inicia a descoberta de um Controlador de Acesso interposto entre o Ponto de Acesso e a rede móvel terrestre pública.

25 Então, o terminal sem fio envia o identificador do usuário imediatamente topo de um protocolo de camada 2 Ponto a Ponto para o Controlador de Acesso, o qual transfere o identificador do usuário recebido na parte de uma de um protocolo de camada 2 Ponto a Ponto para cima de um protocolo de autenticação residindo na camada de aplicação.

30 A seguir, o Controlador de Acesso envia o identificador do usuário para um Gateway de Autenticação na rede móvel terrestre pública para iniciar um procedimento de autenticação.

Uma vez que o processo de autenticação é iniciado, o Controlador de Acesso recebe um desafio de autenticação a partir da rede móvel terrestre pública via o Gateway de Autenticação; e transfere o desafio de autenticação recebida no mesmo protocolo na camada de aplicação para
5 baixo em direção a parte de cima do protocolo de camada 2 Ponto a Ponto. O desafio de autenticação é enviado pelo Controlador de Acesso para o terminal sem fio para derivar uma resposta de autenticação.

Então, o terminal sem fio pode enviar a resposta de autenticação imediatamente em cima de um protocolo de camada 2 Ponto a Ponto
10 para o Controlador de Acesso o qual transfere a resposta de autenticação recebida de um protocolo de camada 2 Ponto a Ponto para cima em direção ao protocolo de autenticação na camada de aplicação. A resposta de autenticação é enviada para o Gateway de Autenticação a partir do Controlador de Acesso que recebe uma chave de criptografia a partir da rede mó-
15 vel terrestre pública via o Gateway de Autenticação.

A seguir, o Controlador de Acesso extrai a chave de criptografia recebida no protocolo na camada de aplicação para criptografia adicional do caminho de comunicação com o terminal sem fio; e o Controlador de Acesso envia um endereço IP designado e outros parâmetros de configuração da
20 rede para o terminal sem fio.

Isto proporciona as vantagens de que o terminal móvel adiciona o mecanismo de autenticação de segurança, similar aos utilizados na rede de comunicação de rádio, em todo o caminho de comunicação, isto significando que ele obtém confidencialidade no caminho sem fio e no caminho
25 com fio. Os operadores podem estender suas redes de acesso, oferecer acesso de banda larga localizado (11 Mbps) por um custo muito baixo.

Também para alcançar os objetivos da presente invenção, é proporcionado um Controlador de Acesso que compreende um servidor Ponto a Ponto residindo em uma camada 2 OSI para comunicar-se com o
30 terminal sem fio; e um protocolo de autenticação residindo em uma camada de aplicação OSI para comunicar-se com a rede móvel terrestre pública. Além disso, este Controlador de Acesso adicionalmente compreende o dis-

positivo para transferir a informação recebida topo do protocolo de camada 2 Ponto a Ponto para cima em direção a um protocolo de autenticação apropriado residindo na camada de aplicação. Da mesma forma, o Controlador de Acesso também compreende o dispositivo para transferir a informação recebida no protocolo de autenticação residindo na camada de aplicação para baixo em direção a parte de cima do protocolo de camada 2 Ponto a Ponto.

De modo a totalmente alcançar os objetivos da invenção, também é proporcionado um terminal sem fio compreendendo funcionalidade par atuar como um cliente do protocolo da camada 2 Ponto a Ponto e possuindo um Protocolo de Autenticação Extensível topo deste protocolo de camada 2 Ponto a Ponto.

A solução geral proporcionada pela invenção resulta em um sistema de telecomunicação compreendendo uma rede de área local sem fio que inclui pelo menos um Ponto de Acesso, uma rede móvel terrestre pública, pelo menos um terminal de fio como dito acima, e o Controlador de Acesso dito acima.

BREVE DESCRIÇÃO DOS DESENHOS

Os aspectos, objetivos e vantagens da invenção irão se tornar aparentes pela leitura deste relatório descritivo em conjunto com os desenhos acompanhantes, nos quais:

A FIGURA 1 representa uma modalidade preferida de como um usuário de uma rede móvel convencional acessando através de uma WLAN, a qual pode ser acessada por usuários móveis e não móveis, pode ser autenticado por sua própria rede móvel e pode ter um caminho criptografado a partir do TE até sua própria rede móvel.

A FIGURA 2 apresenta uma arquitetura simplificada comparada com a na Figura 1 e aplicável a uma WLAN acessada somente por usuários de uma rede móvel terrestre pública.

A FIGURA 3 esquematicamente apresenta uma modalidade de um Controlador de Acesso compreendendo um Servidor PPPoE e um Cliente RADIUS onde o Protocolo de Autenticação Extensível reside.

A FIGURA 4 basicamente apresenta uma seqüência ilustrativa das ações realizadas a partir do TE até a rede móvel e por todas as entidades da WLAN para executar a autenticação do usuário baseada em SIM.

DESCRIÇÃO DETALHADA DAS MODALIDADES PREFERIDAS

5 O dito a seguir descreve modalidades atualmente preferidas do dispositivo, métodos e sistema para permitir uma autenticação do usuário baseada em SIM eficaz e para estabelecer um caminho de criptografia completo começando a partir do TE para usuários WLAN que são assinantes de uma rede móvel terrestre pública. De acordo com um aspecto da presente
10 invenção, esta autenticação do usuário baseada em SIM é executada antes de ter dado a conectividade IP para o dito usuário.

Portanto, o esboço geral de uma modalidade preferida é apresentado na FIGURA 1, apresentando um cenário geral onde assinantes de uma rede móvel terrestre pública (GSM/GPRS/UMTS), bem como outros
15 usuários não móveis locais, acessam uma rede de área local sem fio (WLAN). Este cenário geral na FIGURA 1 propõe uma arquitetura particularmente simples almejada para minimizar os impactos sobre uma WLAN convencional existente de modo a realizar um dos objetivos da presente invenção. Esta arquitetura bastante simples envolve diferentes entidades de
20 uma WLAN e de uma rede móvel terrestre pública, as quais são descritas a seguir. Além disso, a FIGURA 2 apresenta uma arquitetura igualmente mais simplificada de acordo com outra modalidade da presente invenção para uma WLAN fornecer acesso somente para assinantes de uma rede móvel terrestre pública e sem usuários WLAN locais.

25 Uma primeira entidade na FIGURA 1 e 2 é o Equipamento Terminal (TE), o qual é equipado com o hardware e software necessários para fazer interface com o cartão SIM do usuário bem como para enviar e receber a informação de sinalização requerida de acordo com o protocolo de Acordo de Autenticação e de Chave (AKA). O TE também inclui o software
30 necessário para implementar um Protocolo Ponto a Ponto através do protocolo Ethernet (PPPoE), do lado do cliente, por consequência com o RFC 2516.

A inclusão de tal cliente PPPoE permite o estabelecimento de uma sessão de Protocolo Ponto a Ponto com um servidor específico no domínio da WLAN. Esta é uma modalidade muito conveniente de modo a alavancar mecanismos de autenticação existentes, por exemplo, o Protocolo de Autenticação Extensível (EAP) e os protocolos de criptografia, como o Protocolo de Controle de Criptografia PPP (daqui para frente referido como "PPP criptografado") de acordo com o RFC 1968, que estende o caminho de criptografia ao longo da parte com fio da WLAN, assim oferecendo um nível de segurança muito mais elevado. Um componente como este Cliente PPPoE é uma parte principal para a solução proposta.

Outras entidades nos cenários nas FIGURAS 1 e 2 são os Pontos de Acesso que se comportam como estações de rádio padrão simples de acordo com o padrão 802.11b, sem qualquer lógica adicional. Diferente de outras soluções possíveis, como explicado com respeito ao futuro padrão 802.1x, a maneira de se abordar oferecida pela presente invenção permite a reutilização do hardware econômica existente ao invés de ter que substituir ou atualizar todos os APs presentes na WLAN. Estes APs inalterados podem executar neste cenário com suporte WEP desativado, desde que tal WEP oferece por ele próprio pouca segurança comparado com os mecanismos de segurança que são implementados topo da camada PPPoE.

De acordo com um aspecto da presente invenção, é proporcionada uma nova entidade, o Controlador de Acesso (daqui para frente referido como AC) tanto na FIGURA 1 como na 2 que compreende a funcionalidade do servidor PPPoE requerida. Este servidor PPPoE é automaticamente descoberto pelo Equipamento terminal (TE), por meio de um mecanismo embutido no protocolo PPPoE, a saber, através de uma troca de sinais iniciada por uma mensagem de difusão. Este Controlador de Acesso (AC) também compreende uma funcionalidade de cliente RADIUS que tem a responsabilidade de reunir as credenciais do cliente, recebidas através dos atributos EAP transportados topo de um PPP e enviar os mesmos a um Servidor de Autenticação WLAN (WLAN-AS) convencional, também através dos atributos EAP transportados agora sobre topo das mensagens RADIUS. Um

componente como este Controlador de Acesso (AC) também é uma parte principal para o propósito da presente solução.

5 Tanto o Controlador de Acesso como o cliente PPPoE mencionados acima, o qual está embutido no Equipamento Terminal, são entidades cooperativas pretendidas para envelopar um procedimento de autenticação de desafio-resposta bem como para estabelecer um caminho criptografado.

10 Uma entidade adicional presente somente no cenário mais geral apresentado na FIGURA 1 é um Servidor de Autenticação WLAN (WLAN-AS) que implementa a funcionalidade de um servidor de autenticação local para usuários WLAN locais, não pertencendo ao operador móvel e que pode ser assim autenticado por outro dispositivo, tal como um usuário simples e uma associação de senha. Este WLAN-AS também executa o papel de um proxy RADIUS, quando recebendo mensagens de autenticação a partir do Controlador de Acesso e enviando as mesmas para um Gateway de Autenticação (daqui para frente referido como AG) no domínio do operador da rede móvel terrestre pública.

20 O WLAN-AS é somente requerido para o propósito da presente invenção de modo a autenticar os próprios usuários WLAN que não são assinantes móveis da rede móvel terrestre pública. Por consequência, uma WLAN pretendida para fornecer acesso somente para assinantes de uma rede móvel pode livrar-se de tal entidade sem afetar a autenticação dos ditos assinantes móveis e o estabelecimento de um caminho criptografado, escopo da presente invenção. A este respeito, a FIGURA 2 apresenta uma modalidade de uma arquitetura simplificada para uma WLAN fornecendo acesso somente para assinantes de uma rede móvel terrestre pública como explicado acima onde o WLAN-AS desse modo não está incluído.

30 Ainda uma entidade adicional incluída nos cenários das Figuras 1 e 2 é o Gateway de Autenticação (daqui para frente referido como AG) sozinho ou provavelmente em cooperação com um Registro de Localização Inicial (HLR) para armazenar dados de usuário de assinantes móveis. Este Gateway de Autenticação (AG), sozinho ou em combinação com um HLR, atua como servidores backend de autenticação dentro do domínio do opera-

dor e estão encarregados de gerar vetores de autenticação de acordo com o protocolo AKA para redes móveis terrestres públicas mais recentes e convencionais tal como a GSM, GPRS e UMTS. Estes componentes, a saber, AG e HLR, podem ser entidades fisicamente separadas que se comunicam
5 uma com a outra pelo protocolo de Parte Móvel da Aplicação (MAP), ou elas podem ser uma única entidade lógica atuando como um servidor RADIUS e com a base de dados de assinantes embutida, junto com a implementação dos algoritmos necessários no AKA, tal como os bem conhecidos A5, A8 e assim por diante.

10 Na última maneira de abordar, a comunicação para o HLR por consequência não é necessária, como ilustrado em forma de exemplo na FIGURA 2.

Em resumo, o controlador de acesso, o cliente PPPoE mencionado acima, o qual é embutido no Equipamento Terminal, e este Gateway
15 de Autenticação são entidades principais para o propósito da presente invenção. A descrição particular para as funções residindo em tais entidades é meramente ilustrativa e de maneira não restritiva.

A FIGURA 3 apresenta camadas de protocolo diferentes envolvidas em um Controlador de Acesso (AC) com referência ao modelo de Interconexão de Sistema Aberto (OSI). O servidor PPPoE, residindo debaixo
20 de uma camada IP, compreendendo uma camada de protocolo PPPoE que naturalmente reside sobre uma camada Ethernet e possuindo embutido o EAP mencionado acima. Da mesma forma, o cliente RADIUS possuindo uma camada de protocolo RADIUS possuindo embutido o EAP, residindo
25 sobre uma camada UDP, ambos residindo sobre uma camada IP.

Por outro lado, a maneira na qual os diferentes elementos realizam alguns aspectos da presente invenção de acordo com modalidades atualmente preferidas é descrita abaixo com referência à seqüência de ações descritas na FIGURA 4.

30 O Equipamento Terminal (TE) mencionado acima é equipado com um Adaptador de Terminal Móvel (MTA) que permite o acesso a um cartão SIM tido por um terminal móvel. Este TE possui um transceptor para

comunicar-se (C-401, c-402) com um AP da WLAN e inclui a pilha de software apropriada para implementar o protocolo PPPoE de acordo com o RFC 2516.

O Controlador de Acesso (AC) possui um servidor PPPoE embutido. A descoberta do servidor PPPoE pelo cliente PPPoE é uma parte integral do próprio protocolo (C-403, C-404, C-405, C-406). A identidade utilizada pelo TE na ligação PPP (C-407, C-408) é um identificador de acesso de Rede (NAI), o qual é informado pelo usuário para estabelecer as sessões de discagem requeridas e cujo domínio é utilizado para identificar o usuário como um assinante de um dado operador móvel. Nenhuma senha é necessária, desde que a autenticação é feita por outro dispositivo. Alternativamente, ao invés de enviar um NAI, o IMSI poderia ser buscado a partir do cartão SIM e enviado como a identidade do usuário. Isto somente deve ser utilizado se enviar o IMSI em texto transparente for aceitável, o que pode não ser o caso.

Tendo recebido a identidade do usuário com ajuda dos mecanismos EAP, o Controlador de Acesso (AC) possui um cliente RADIUS para enviar (C-409) mensagens de autenticação para o servidor WLAN-AS. O Protocolo de Autenticação Extensível (EAP) é executado topo do PPP e do RADIUS, de modo a transportar a informação de autenticação entre o TE e o AG. O mecanismo de autenticação a ser utilizado dentro do EAP pode ser o AKA convencional utilizado em redes móveis terrestres públicas. Como já mencionado acima, o WLAN-AS atua como um servidor de autenticação para usuários WLAN habituais, cuja autenticação não é baseada na SIM e como um proxy de autenticação para aqueles usuários cuja parte de domínio do NAI identifica os mesmos como assinantes de uma rede móvel assim utilizando a autenticação baseada na SIM. Então, quando atuando como um proxy de autenticação, o WLAN-AS envia (C-410) as mensagens de autenticação recebidas para o Gateway de Autenticação (AG).

Quando o Gateway de Autenticação recebe (C-410) uma requisição de autenticação, solicita ao HLR um vetor de autenticação (C-411), triplete ou quinteto, por utilizar uma interface MAP. Para esta tarefa, o Ga-

teway de Autenticação (AG) tem que saber o IMSI do assinante cujo NAI foi enviado na mensagem RADIUS. Este IMSI pode ser descoberto por procurar em uma base de dados de diretórios, por exemplo. O HLR responde com a informação de autenticação requisitada (C-412) para o usuário.

5 Então, o AG encapsula o componente RAND do vetor de autenticação em um atributo EAP e envia o mesmo de volta através do WLAN-AS (C-413) para o AC (C-414) dentro de uma mensagem RADIUS. Observa-se que para o usuário de novas redes móveis como a UMTS, o envio de uma mensagem como AUTN também pode ser requerido.

10 O AC então envia (C-415) a informação EAP recebida para o TE em uma mensagem PPP. Observe que o AC comporta-se aqui como uma "passagem" da informação EAP entre os protocolos "portadores" tal como o PPP e o RADIUS.

15 Quando o TE recebe a informação EAP, extrai o número RAND e utiliza o mesmo para desafiar a SIM e gerar uma resposta (RES), que é então enviada de volta (C-416, C-417, C-418) para o AG via o EAP transmitido através do PPP e do RADIUS novamente. Como antes, para usuários UMTS, o TE primeiro autentica a rede, baseado no AUTN. Neste estágio, tem que ser observado que o TE gera a chave de criptografia seguindo os
20 algoritmos padrão definidos no AKA. Esta chave é utilizada como uma semente, a saber, material de formação de chave, para derivar uma ou várias chaves de sessão a serem utilizadas com o Protocolo de Controle de Criptografia PPP declarado no RFC 1968 e qualquer dos algoritmos de criptografia PPP existentes, por exemplo, o protocolo de criptografia DES-Triplo
25 PPP, RFC 2420.

 O AG recebe (C-418) a resposta EAP e verifica a validade do desafio. A chave de criptografia AKA (Kc) foi recebida anteriormente no vetor de autenticação a partir do HLR provavelmente em cooperação com um Centro de Autenticação (AuC) não descrito. O AG então comunica a chave
30 de criptografia AKA (Kc) para o AC (C-419, C-420) onde o servidor PPPoE reside. Isto pode ser feito em uma mensagem RADIUS acesso-aceitação onde o Sucesso-EAP é transmitido, mas desde que este comando EAP não

possa transportar quaisquer dados adicionais, um Atributo Específico de Vendedor (VSA) RADIUS pode ser uma opção valiosa.

- Neste estágio, o AC recebe (C-420) uma mensagem RADIUS Acesso-aceitação e requisita um endereço IP a partir de um servidor de Protocolo Dinâmico de Configuração de Hospedeiro (DHCP), este endereço IP sendo adicionalmente enviado para o TE. O AC segue o mesmo algoritmo que o TE para derivar chaves de sessão a partir da chave de criptografia AKA (Kc) a serem utilizadas com o Protocolo de Controle de Criptografia PPP e o algoritmo de criptografia PPP escolhido (3DES, por exemplo). O AC eventualmente envia (C-421) a mensagem de sucesso-EAP para o TE, junto com outros parâmetros de configuração destinados para o dito TE, tal como um endereço IP, uma máscara de rede IP, os servidores DNS e assim por diante. Então, a ligação PPP está totalmente estabelecida e pronta para entrar com a fase de rede.

REIVINDICAÇÕES

1. Método em um sistema de telecomunicação para permitir uma autenticação baseada em SIM para usuários de uma rede de área local sem fio que são assinantes de uma rede móvel terrestre pública, o método compreendendo as etapas de:

- (a) um terminal sem fio acessar a rede de área local sem fio através de um Ponto de Acesso acessível;
- (b) descobrir o Controlador de Acesso interposto entre o Ponto de Acesso e a rede móvel terrestre pública a partir de um terminal sem fio;
- (c) executar um procedimento de autenticação desafio-resposta baseado em SIM entre o terminal sem fio e a rede móvel terrestre pública através do Controlador de Acesso, o terminal sem fio provido de um cartão SIM e adaptado para ler dados do mesmo;

o método caracterizado pelo fato de que a aceitação de autenticação desafio-resposta na etapa (c) acontece antes de ter provido conectividade IP ao usuário, e são executadas:

- no topo de um protocolo de camada 2 Ponto-a-Ponto (PPPoE) entre o terminal sem fio e o Controlador de Acesso; e
- em um protocolo de autenticação residente na camada de aplicação entre a rede móvel terrestre pública e o Controlador de Acesso; e

sendo que o método compreende ainda as etapas de:

- (d) oferecer conectividade IP para o usuário no terminal sem fio, ao enviar um endereço IP designado e outros parâmetros de configuração da rede, uma vez que o dito usuário tenha sido autenticado de forma válida pela rede móvel terrestre pública.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a etapa (b) de descobrir um Controlador de Acesso inclui a etapa de estabelecer um sessão de Protocolo Ponto-a-Ponto entre um cliente de Protocolo Ponto-a-Ponto sobre Ethernet (PPPoE) no terminal sem fio e um servidor de Protocolo Ponto-a-Ponto sobre Ethernet (PPPoE) no Controlador de Acesso.

3. Método de acordo com a reivindicação 1, caracterizado pelo

fato de que a etapa (c) de executar o procedimento de autenticação desafio-resposta baseado em SIM inclui as etapas de:

(c1) enviar um identificador do usuário a partir do terminal sem fio para a rede móvel terrestre pública através do Controlador de Acesso;

5 (c2) receber um desafio de autenticação no terminal sem fio a partir da rede móvel terrestre pública via o Controlador de Acesso;

(c3) obter chave de criptografia e resposta de autenticação no terminal sem fio a partir do desafio recebido;

10 (c4) enviar a resposta de autenticação a partir do terminal sem fio para a rede móvel terrestre pública através do Controlador de Acesso;

(c5) receber no Controlador de Acesso uma chave de criptografia a partir da rede móvel terrestre pública; e

(c6) extrair a chave de criptografia recebida para encriptação adicional do caminho de comunicação com o terminal sem fio.

15 4. Método de acordo com a reivindicação 2, caracterizado pelo fato de que adicionalmente compreende a etapa de desviar a informação de autenticação recebida no topo de um protocolo de camada 2 Ponto-a-Ponto (PPPoE) em um nível superior a um protocolo de autenticação residente na camada de aplicação para submissões para a rede móvel terrestre pública.

20 5. Método de acordo com a reivindicação 4, caracterizado pelo fato de que adicionalmente compreende a etapa de desviar a informação de autenticação recebida em um protocolo de autenticação residente na camada de aplicação em um nível inferior no topo de um protocolo de camada 2 Ponto-a-Ponto (PPPoE) para submissões para o terminal sem fio.

25 6. Método de acordo com a reivindicação 3, caracterizado pelo fato de que adicionalmente compreende a etapa de estabelecer no terminal sem fio um caminho de criptografia simétrico utilizando as chaves de criptografia anteriormente obtidas no Controlador de Acesso e no terminal sem fio.

30 7. Método de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que a etapa (d) de enviar um endereço IP inclui uma etapa anterior de requisitar tal endereço IP a partir de um servidor de

Protocolo Dinâmico de Configuração de Host.

8. Método de acordo com qualquer uma das reivindicações 1 a 7, caracterizado pelo fato de que a comunicação entre o Controlador de Acesso e a rede móvel terrestre pública passa por um Gateway de Autenticação da dita rede móvel terrestre pública.

9. Método de acordo com qualquer uma das reivindicações 1 a 8, caracterizado pelo fato de que a comunicação entre o Controlador de Acesso e o Gateway de Autenticação de uma rede móvel terrestre pública passa por um Servidor de Autenticação da rede de área local sem fio encarregado de autenticar usuários locais da dita rede de área local sem fio que não são assinantes móveis.

10. Método de acordo com qualquer uma das reivindicações 1 a 9, caracterizado pelo fato de que o identificador do usuário na etapa c1) compreende um Identificador de Acesso de Rede.

11. Método de acordo com qualquer uma das reivindicações 1 a 10, caracterizado pelo fato de que o identificador do usuário na etapa c1) compreende uma Identidade de Assinante Móvel Internacional.

12. Método de acordo com qualquer uma das reivindicações 1 a 11, caracterizado pelo fato de que o protocolo de autenticação residente na camada de aplicação na etapa (c) é um Protocolo de Autenticação Extensível.

13. Método de acordo com a reivindicação 12, caracterizado pelo fato de que este Protocolo de Autenticação Extensível é transportado sobre um protocolo RADIUS.

14. Método, de acordo com a reivindicação 12, caracterizado pelo fato de que este Protocolo de Autenticação Extensível é transportado sobre um protocolo Diameter.

15. Controlador de Acesso para acessar um sistema de telecomunicação que compreende uma rede de área local sem fio incluindo pelo menos um Ponto de Acesso, uma rede móvel terrestre pública e pelo menos um Equipamento Terminal provido de um cartão SIM e adaptado para ler dados do assinante do mesmo, o Controlador de Acesso caracterizado pelo

fato de que compreende:

(a) um servidor de protocolo de camada 2 Ponto-a-Ponto (PPPoE) para comunicação com o terminal sem fio; e disposto para encapsular um procedimento de autenticação desafio-resposta baseado em SIM;

5 e

(b) um protocolo de autenticação residente em uma camada de aplicação OSI para comunicação com a rede móvel terrestre pública.

16. Controlador de Acesso de acordo com a reivindicação 15, caracterizado pelo fato de que adicionalmente compreende:

10 (a) meios para desviar a informação recebida no topo do protocolo de camada 2 Ponto-a-Ponto (PPPoE) em um nível superior ao protocolo de autenticação residente na camada de aplicação; e

(b) meios para desviar a informação recebida no protocolo de autenticação residente na camada de aplicação em um nível inferior no topo do protocolo de camada 2 Ponto-a-Ponto (PPPoE).

15 17. Controlador de Acesso de acordo com a reivindicação 16, caracterizado pelo fato de que adicionalmente compreende meios para requisitar um endereço IP a partir de um servidor de Protocolo Dinâmico de Configuração de Host, após um usuário ter sido autenticado com sucesso por sua rede móvel terrestre pública.

18. Controlador de Acesso de acordo com a reivindicação 17, caracterizado pelo fato de que é adaptado para comunicar-se com um terminal sem fio via um Ponto de Acesso.

19. Controlador de Acesso de acordo com a reivindicação 17, caracterizado pelo fato de que é adaptado para comunicar-se com uma rede móvel terrestre pública via um Gateway de Autenticação.

20. Controlador de Acesso de acordo com a reivindicação 17, caracterizado pelo fato de que é adaptado para comunicar-se com um Gateway de Autenticação via um Servidor de Autenticação responsável por autenticar os usuários locais de uma rede de área local sem fio.

21. Controlador de Acesso de acordo com qualquer uma das reivindicações de 15 a 20, caracterizado pelo fato de que o protocolo de au-

tenticação residente na camada de aplicação é um Protocolo de Autenticação Extensível.

22. Controlador de Acesso de acordo com a reivindicação 21, caracterizado pelo fato de que este Protocolo de Autenticação Extensível é transportado sobre um protocolo RADIUS.

23. Controlador de Acesso de acordo com a reivindicação 21, caracterizado pelo fato de que este Protocolo de Autenticação Extensível é transportado sobre um protocolo Diameter.

24. Terminal sem fio adaptado para realizar um procedimento de autenticação baseado em SIM, o terminal sem fio compreendendo funcionalidade para atuar como um cliente de protocolo de camada 2 Ponto-a-Ponto (PPPoE) e para manusear um Protocolo de Autenticação Extensível no topo deste protocolo de camada 2 Ponto-a-Ponto, terminal sem fio caracterizado pelo fato de que recebe um endereço IP após realizar um procedimento de autenticação baseado em SIM com sucesso, o endereço IP sendo utilizável para obter conectividade IP..

25. Sistema de telecomunicação compreendendo uma rede de área local sem fio que inclui pelo menos um Ponto de Acesso, uma rede móvel terrestre pública e pelo menos um Equipamento Terminal provido de uma cartão SIM e adaptada para ler dados do assinante do mesmo, caracterizado pelo fato de que ele adicionalmente compreende o Controlador de Acesso conforme definido nas reivindicações de 15 até 23 para permitir a autenticação de assinante baseada em SIM para usuários da rede de área local sem fio que são assinantes da rede móvel terrestre pública.

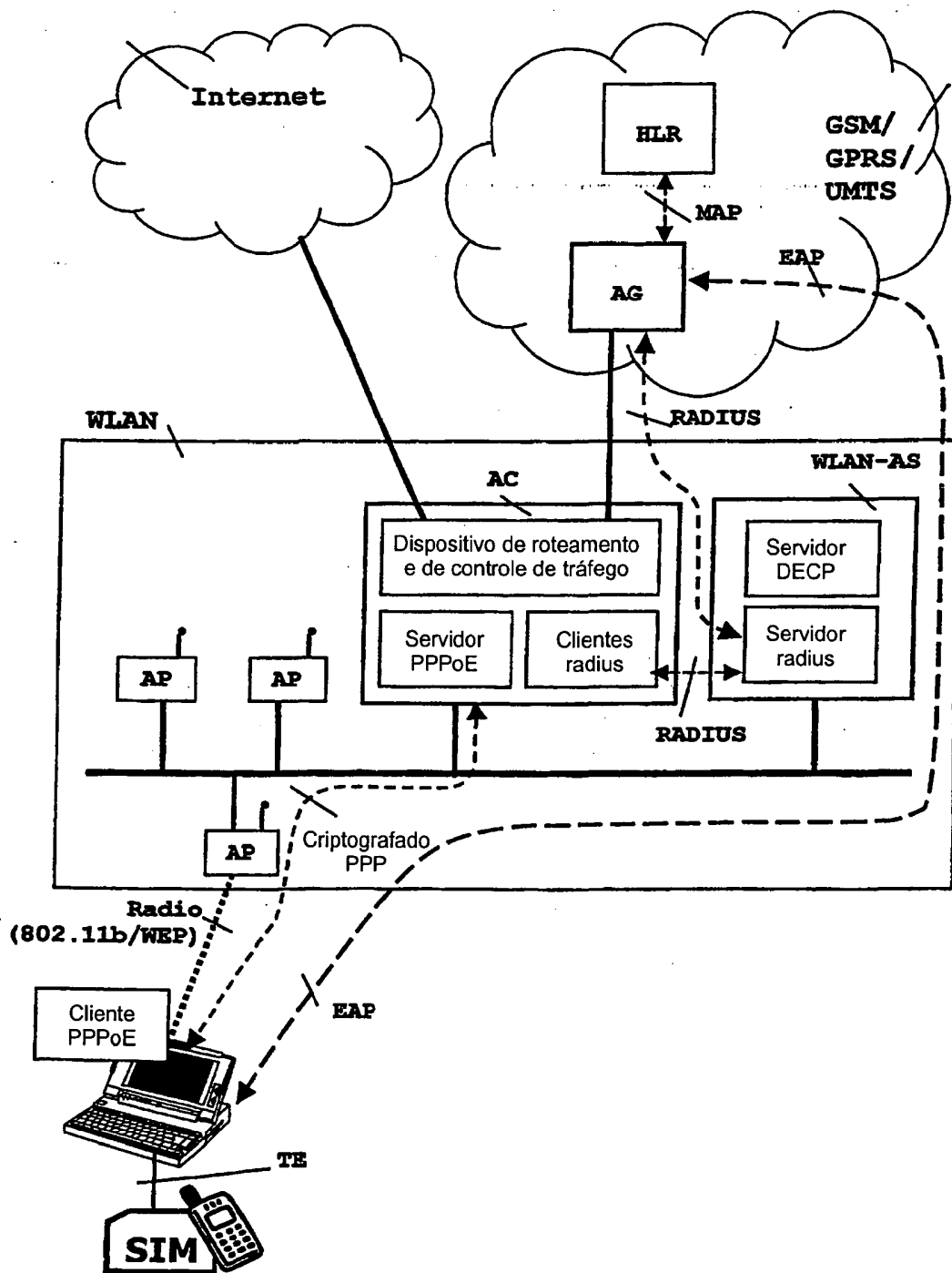


FIG.-1-

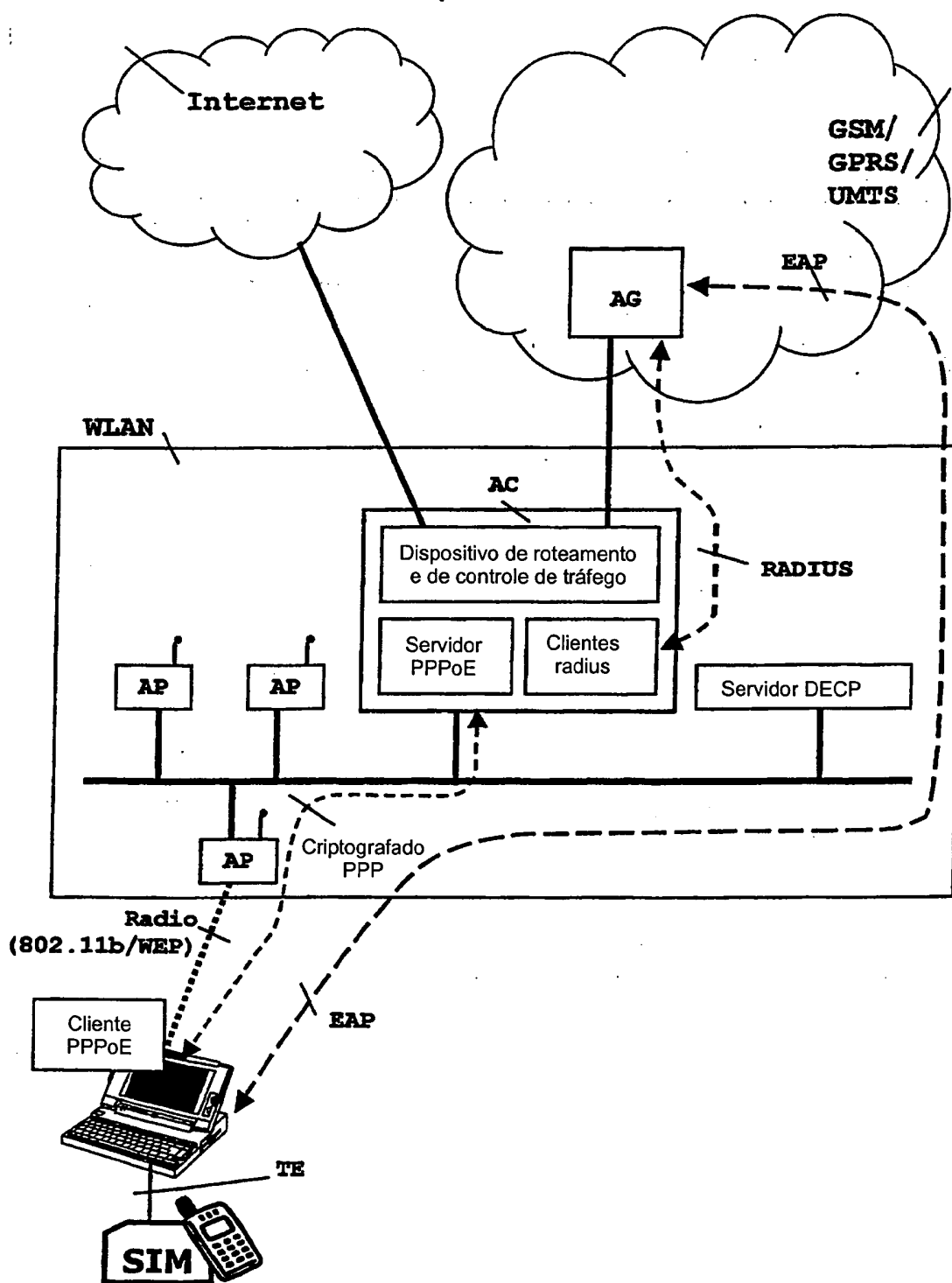


FIG.-2-

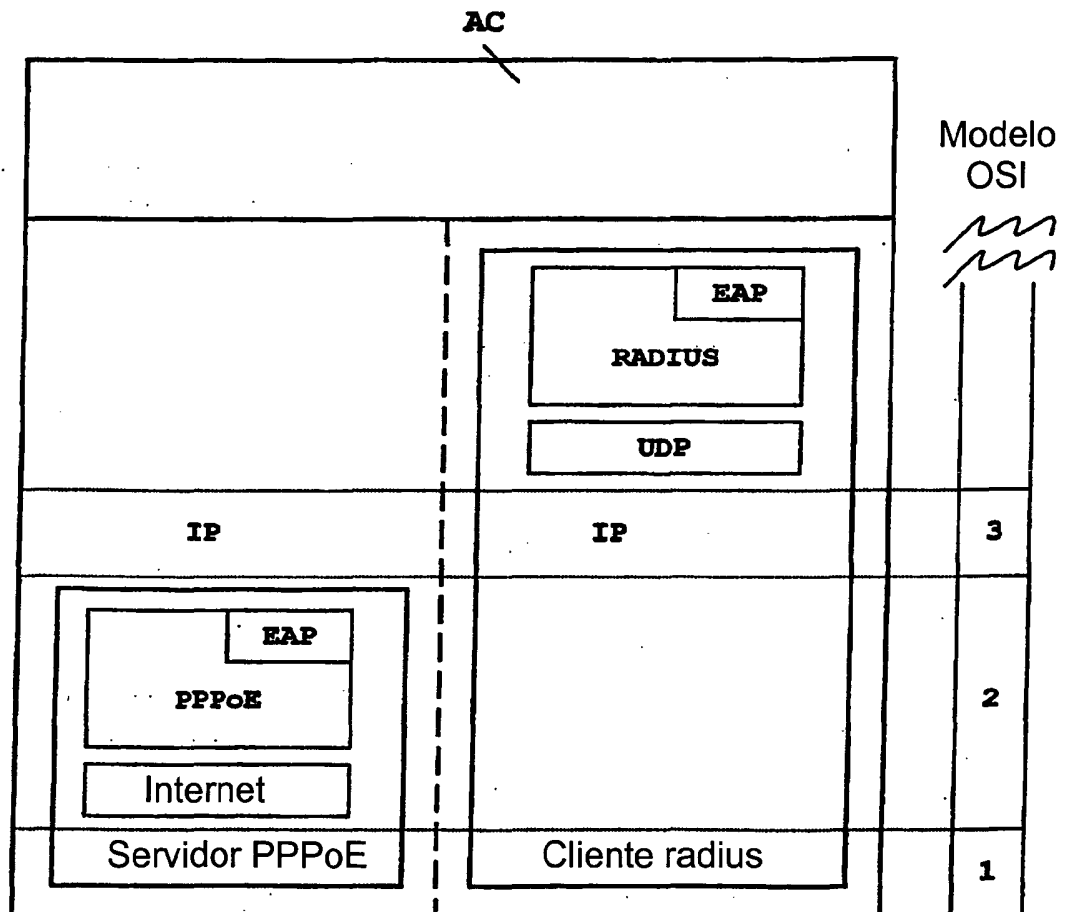


FIG.-3-

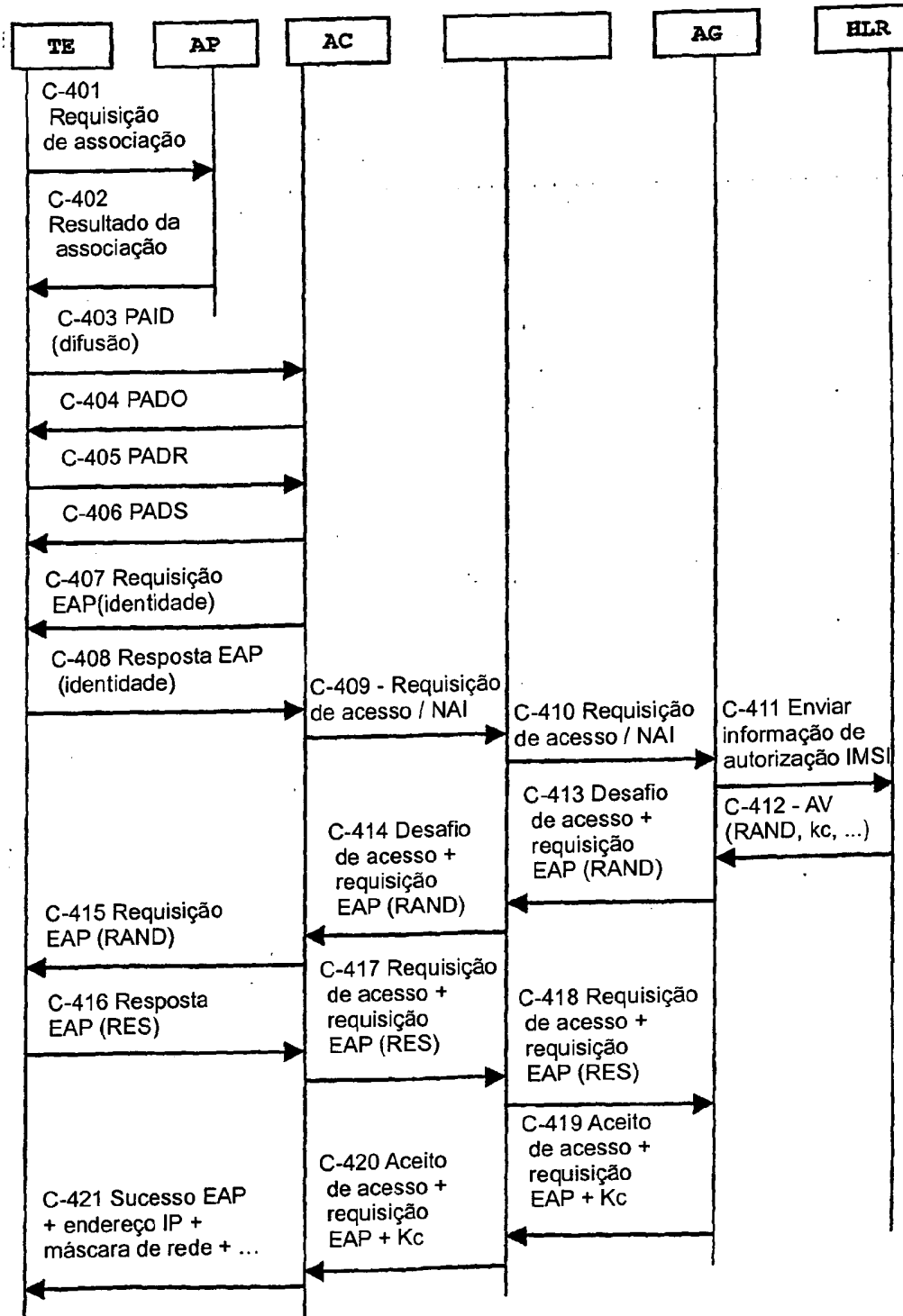


FIG.-4-

RESUMO

Patente de Invenção: **"MÉTODO PARA PERMITIR UMA AUTENTICAÇÃO BASEADA EM SIM, CONTROLADOR DE ACESSO, TERMINAL SEM FIO E SISTEMA DE TELECOMUNICAÇÃO"**.

5 A presente invenção refere-se a um método, controlador e sistema para executar uma autenticação baseada em SIM de um usuário acessando uma WLAN, sem ter provido ainda uma conectividade IP, junto com um mecanismo de criptografia de camada 2 para proteger o caminho entre o Equipamento Terminal e a rede Móvel. Portanto, a invenção proporciona um método para estabelecer um envelopamento de PPP para diálogos AKA entre o terminal e um Controlador de Acesso para acessar a rede móvel possuindo o SIM. A invenção também proporciona um Controlador de Acesso (AC) compreendendo um servidor Ponto-a-Ponto sobre Ethernet (PPPoE) para envelopamento de diálogos AKA a partir de um cliente PPP 10 instalado no terminal para o mesmo propósito, e também compreendendo um Roteador de Tráfego e um cliente RADIUS. O AC assim incluindo um cliente RADIUS é interposto entre um proxy RADIUS acessado a partir dos pontos de acesso (AP) na WLAN e a rede móvel onde a autenticação baseada em SIM é executada.