REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA E COMÉRCIO EXTERIOR
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0015774-0

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0015774-0

(22) Data do Depósito: 21/11/2000

(43) Data da Publicação do Pedido: 31/05/2001

(51) Classificação Internacional: H04Q 7/38

(30) Prioridade Unionista: 23/11/1999 US 09/447,761

(54) Título: MÉTODO E APARELHO PARA RESPECTIVAMENTE FORNECER E MANTER UMA DETERMINADA ASSOCIAÇÃO DE SEGURANÇA DURANTE UMA TRANSFERÊNCIA DO TERMINAL MÓVEL

(73) Titular: NOKIA CORPORATION, Companhia Finlandesa. Endereço: Keilalahdentie 4, FIN-02150 Espoo, Finlândia (FI).

(72) Inventor: JUHA ALA-LAURILA; HARRI HANSEN; JUHA SALVELA

Prazo de Validade: 10 (dez) anos contados a partir de 16/06/2015, observadas as condições legais.

Expedida em: 16 de Junho de 2015.

Assinado digitalmente por:
Júlio César Castelo Branco Reis Moreira
Diretor de Patentes

"MÉTODO E APARELHO PARA RESPECTIVAMENTE FORNECER E MANTER UMA DETERMINADA ASSOCIAÇÃO DE SEGURANÇA DURANTE UMA TRANSFERÊNCIA DO TERMINAL MÓVEL."

Campo da Invenção

Esta invenção se relaciona aos sistemas de radiocomunicação, onde uma rede de área local sem fios (WLAN - Wireless Local Area Network) é um exemplo não-limitativo. Mais especificamente, esta invenção relaciona ao fornecimento de segurança na informação, quando um terminal móvel é transferido de uma primeira estação base ou ponto de acesso (PA) para uma segunda estação base ou ponto de acesso (PA).

Descrição da Técnica Anterior

Em uma configuração mínima, um sistema de comunicação é formado por uma estação transmissora e uma estação receptora que são interconectadas por um canal de comunicação. Os sinais de comunicação gerados pela estação transmissora são transmitidos no canal de comunicação e recebidos pela estação receptora.

Em um sistema de comunicação de rádio, ao menos uma parte do canal de comunicação é formada por uma parte do espectro eletromagnético. A mobilidade aumentada das comunicações é permitida em um sistema de comunicação de rádio, porque uma conexão de estrutura cabeada ou fixa, não é requerida entre as estações, transmissora e receptora.

Um sistema de comunicação celular do qual um sistema de telefonia celular é um exemplo, é um exemplo de um sistema de comunicação de rádio. Quando o terminal móvel de um assinante em um sistema de comunicação celular é posicionado fisicamente em quase qualquer local ao longo de uma área que é cercada pela infra-estrutura de rede do sistema de comunicação celular, o terminal móvel é capaz de comunicar através do sistema de comunicação celular com outro terminal móvel.

A infra-estrutura de rede de um sistema de comunicação sem fio exemplar, inclui estações bases fisicamente aparte espaçadas ou pontos de acesso (PAs), o qual cada um inclui um transceptor. Em tal sistema exemplar, cada estação base ou PA define uma área geográfica ou uma célula do sistema de comunicação. Como o primeiro terminal móvel é usado para comunicar com o segundo terminal móvel, e como o primeiro terminal móvel

viaja ou move entre as células do sistema, a comunicação ininterrupta é possível pela manipulação sobre as comunicações de uma estação base para outra estação base. Tal transferência de comunicação é fornecida por um processo de transferência.

Uma rede de área local de alta performance de rádio tal como HIPERLAN tipo–2 (High Performance radio Local Area Network) suporta três tipos de transferência. O HIPERLAN/2 fornece comunicações de alta velocidade (tipicamente uma taxa de dados de 25 Mb/s) entre os dispositivos portáteis e o IP de Banda Larga, nas redes ATM e UMTS, e é capaz de suportar as aplicações de mídia múltiplas, com a aplicação típica sendo interna. O HIPERLAN/2 provê acesso local sem fio às redes de infra-estrutura diferentes (por exemplo, IP, ATM e UMTS) pelos terminais em movimento e estacionários, que interagem com os pontos de acesso que, em troca, normalmente são conectados a um IP, a backbone ATM ou UMTS. Vários pontos de acesso são solicitados para os serviços de rede. A rede sem fio como um todo, suporta as transferências das conexões entre os pontos de acesso para fornecer mobilidade. Ambientes operacionais típicos incluem as redes empresariais e as redes de premissa doméstica. Uma avaliação das redes de acesso HIPERLAN/2 é fornecida pelo Instituto Europeu de Normas de telecomunicações (ETSI) no documento DTR/BRAN-00230002, 1998, incorporado aqui por referência.

Dependendo da decisão de transferência do terminal móvel, a transferência de setor (setor-interno), a transferência de rádio (transceptor de ponto de acesso interno/ transferência do ponto de acesso interno), a transferência de rede (ponto de acesso interno/ transferência de rede interna) ou uma transferência forçada pode ocorrer de acordo com o HIPERLAN/2.

Antes da execução de transferência, o terminal móvel deve agrupar as medidas pertinentes na freqüência que é usada pelo ponto de acesso atual, como também nas freqüências que são usadas pelos pontos de acesso que são candidatos a uma transferência. As medidas na freqüência de serviço podem ser transportadas pelo terminal móvel, enquanto este é sincronizado ao ponto de acesso atual. Contudo, de forma a medir a freqüência dos pontos de acesso vizinhos, o terminal móvel deve estar temporariamente afastado do ponto de acesso atual.

Durante o procedimento de afastamento do terminal móvel, o terminal móvel

é temporariamente desconectado do ponto de acesso atual, de forma que o terminal móvel possa executar as medidas nos pontos de acesso vizinhos. Durante este tempo, nenhuma comunicação entre o terminal móvel e o ponto de acesso atual é possível. Como parte deste procedimento de afastamento, o terminal móvel diz o ponto de acesso atual que estará ausente para os n-quadros. Durante este período de afastamento, o terminal móvel não pode ser alcançado pelo ponto de acesso atual. Depois do período de afastamento, o ponto de acesso atual pode ativar uma sucessão ativa do terminal móvel para conferir se o terminal móvel está disponível.

Durante o setor de transferência, o ponto de acesso do setor da antena é alterado, e o mesmo ponto de acesso controla toda a transferência. Depois de uma transferência de setor bem sucedida, o terminal móvel comunica pelo novo setor.Uma transferência de rádio relaciona os pontos de acesso que têm mais de um transceptor por ponto de acesso, por exemplo, dois transceptores de ponto de acesso e um controlador de ponto de acesso. A transferência de rádio é executada quando o terminal móvel move de uma área de cobertura de um ponto de acesso para outra área de cobertura que é servida pelo mesmo ponto de acesso. Uma vez que a transferência de rádio possa ser executada dentro da camada de controle de enlace de dados (CCED), os protocolos da camada superior (CS) não são envolvidos. Quando o terminal móvel detecta a necessidade para uma transferência para outro controlador de ponto de acesso, o terminal móvel ainda pode sincronizar o ponto de acesso atual. Neste caso, o terminal móvel pode notificar o seu controlador de ponto de acesso, que o terminal móvel executará uma transferência a outro controlador de ponto de acesso. No caso de uma transferência de rádio, toda a informação pertinente sobre conexões entrantes, os parâmetros de segurança, etc. estarão disponíveis no ponto de acesso, de forma que esta informação não seja re-negociada.

Uma transferência de rede é transportada quando o terminal móvel move de um ponto de acesso para outro ponto de acesso. Uma vez que o terminal móvel deixa a área de serviço de, por exemplo, um enlace de controle de rádio (ECR), a transferência de rede envolve a camada de convergência (CC) e o CS (quando for necessário), como também a DLCI. Para manter a associação e as conexões CS, uma sinalização específica através da backbone pode ser necessária. Quando o terminal móvel detecta a necessidade para

transferência para outro ponto de acesso (alvo), o terminal móvel ainda pode ser sincronizado ao ponto de acesso atual. Neste caso, o terminal móvel pode notificar que o ponto de acesso atual executará uma transferência para outro ponto de acesso. O ponto de acesso notificado deixará de transmitir para àquele terminal móvel, mas manterá associação durante um tempo especificado, quando indicado.

A transferência forçada dá uma oportunidade ao ponto de acesso atual para ordenar um certo terminal móvel para deixar a célula do ponto de acesso atual. Uma transferência forçada é iniciada pelo ponto de acesso que envia um sinal de Transferência_Força ao terminal móvel. Em um procedimento, o terminal móvel executa uma transferência normal e deixa a sua célula antiga, indiferente de se esta encontra uma célula nova. Em um segundo procedimento, o terminal móvel tem a oportunidade para voltar ao ponto de acesso antigo se a transferência falhar.

Para outra discussão das características da HIPLERLAN/2 veja as Redes de Acesso de Rádio de Banda Larga (BRAN - Broadband Radio Access Networks); Especificação Funcional HIPERLAN tipo 2; Controle de Enlace de rádio (CER) que são fornecidos pela organização de padronização ETSI, incorporada aqui por referência.

Vários tipos de sistemas de comunicação sem fios foram implementados, e outros foram propostos, para abrangir áreas geográficas limitadas, por exemplo, uma área limitada que é cercada por um edifício ou por um escritório dentro de um edifício. Os sistemas de comunicação sem fios, tal como as redes micro-celulares, as redes privadas, e WLANs são exemplos de tais sistemas.

Os sistemas de comunicação sem fios são tipicamente construídos de acordo com os padrões, que são promulgados por um corpo regulador ou quase-regulador. Por exemplo, o padrão IEEE 802.11 promulgado pelo IEEE (Instituto de Engenharia elétrica e Eletrônica) é um padrão de rede de área local sem fios (WLAN) que geralmente pertence à rede de área local sem fio comercial de 2. 4 GHz. O padrão 802.11 especifica uma interface entre o terminal sem fio e uma estação base ou ponto de acesso, como também entre os terminais sem fios. Os padrões que pertencem à camada física e à camada de controle de acesso ao meio (CAM) são agrupadas em tal padrão. Este padrão permite um compartilhamento médio automático entre os dispositivos diferentes que incluem as camadas

físicas compatíveis. A transferência de dados assíncrona é provida para o padrão, geralmente por meio da camada CAM, utilizando o acesso múltiplo por detecção de portadora com esquema de comunicação que evita colisão (CSMA/CA - Carrier Sense Multiple Access/ Collision Avoidance).

Enquanto o padrão IEEE 802.11 para as comunicações sem fio, através do uso dos terminais móveis é construído para ser mutuamente operável de acordo com tal padrão, o padrão não provê uso adequado para os serviços sem fios em tempo real. Por exemplo, em uma implementação do padrão, uma perda significante de qualidade é às vezes experimentada durante a transferência de comunicações de um PA para outro PA. Números excessivos de quadros de dados são suscetíveis de serem perdidos ou retardados, resultando na perda de qualidade de comunicação, ou mesmo no término das comunicações. Os modos operacionais diferentes do agrupado no padrão IEEE 802.11 são solicitados então, para particularmente os serviços sem fio em tempo real. As funções proprietárias foram propostas, as quais permitem uma qualidade melhorada das comunicações quando comparada com a operação do padrão IEEE 802.11 existente. Os PAs e os terminais móveis que são operáveis para executar tais funções proprietárias, são referenciados como sendo capaz de modo proprietário.

Contudo, ambas as extremidades de um par de comunicações, consistindo em um terminal móvel e o PA, pelos quais o terminal móvel comunica, deve ser capaz de operar no modo proprietário. Se ambas as extremidades do par de comunicações, não estiverem juntas operáveis de acordo com o modo proprietário, a operação convencional para o padrão IEEE 802.11 é solicitada. Então, antes de permitir que ambas as extremidades do par de comunicações operem no modo proprietário, uma determinação deve ser feita da habilidade de ambas às extremidades do par de comunicações juntas serem operáveis de acordo com o modo proprietário.

O pedido de patente copendente mencionado acima fornece um aparelho que é operável para identificar se ambas as extremidades do par de comunicações são operáveis juntas no modo proprietário, o aparelho que opera para ativar ambas as extremidades do par de comunicações operam no modo proprietário quando for determinado que uma compatibilidade-par sai, e o aparelho logo após opera para manter a operação no modo

proprietário durante os procedimentos de transferência devendo o terminal móvel mover de uma célula que é servida pelo primeiro PA à uma célula que é servida pelo segundo PA.

Em adição às características valiosas que são fornecidas pelo aparelho deste pedido de patente copendente, seria desejável restabelecer uma associação de segurança tal como quando ocorre uma transferência de PA-para-PA.

Muitos clientes, e ambientes particularmente empresariais, solicitam um alto grau de segurança de dados, e esta segurança de dados não pode ser comprometida pelo uso de uma instalação WLAN. Desde então o acesso ao WLAN não pode ser fisicamente restringido, é habitual usar métodos de criptografia para proteger os dados transmitidos e os elementos de rede. Os padrões Internet IEEE 802.11 atual e o ITEF oferecem dois mecanismos complementares para fornecer comunicações de dados seguras sobre um enlace sem fios, isto é um Protocolo de Segurança da Internet (IPSEC).O IPSEC é um protocolo de segurança baseado em IP, que fornece uma comunicação segura entre os dois servidores IP. Um uso comum do protocolo IPSEC está nas construções das Redes Privadas Virtuais (VPNs).

Nos sistemas WLAN, o protocolo IPsec pode ser usado para fornecer segurança de extremo a extremo para os pacotes de dados, esta segurança sendo fornecida pela autenticação e/ou codificação dos pacotes de dados transmitidos. O IPsec usa uma criptografia simétrica que requer uso da mesma chave de codificação e/ou autenticação em ambas as extremidades do enlace de comunicação. Os protocolos de gerenciamento da chave seletora tal como TCI pode ser usado para gerar as chaves simétricas para uma pilha IPsec.

Enquanto o protocolo de gerenciamento da chave Troca de Chave Internet (TCI) é útil para o estabelecimento de uma associação de segurança a nível IP, durante uma associação de terminal móvel/ ponto de acesso inicial, quando a necessidade para uma transferência de comunicação ocorre, o uso do TCI ou de outros protocolos semelhantes infligem uma demora de tempo considerável ao realizar a transferência desde que tais protocolos solicitem a troca de mensagens múltiplas, o seu uso de codificação da chave pública requer um processamento muito pesado. Como a transferência do tráfego de carga útil pode ser resumida apenas após uma associação de segurança ativa, foi estabelecido entre o novo-PA e o terminal móvel, o uso do protocolo de gerenciamento da chave TCI ou

outros protocolos que apresentam problemas durante a transferência.

Quando qualquer protocolo de segurança com uma chave de codificação dinâmica, isto é uma chave dinâmica dependente da sessão, é aplicado entre um terminal móvel e um PA, este é desejável para achar um mecanismo para a transferência de uma associação de segurança ativa de um PA para outro PA, quando o terminal móvel move dentro da área de cobertura que é fornecida pela rede ou sistema de rádio sem fio.

Esta no âmbito desta informação de fundo a presente invenção fornece um método/aparelho de baixo ou curto retardo para o gerenciamento da chave e do re-estabelecimento de associação de segurança durante uma transferência de comunicação WLAN, em que não haja nenhuma necessidade para modificar a associação de segurança de extremo a extremo durante a transferência (por exemplo, as conexões de carga útil IPsec entre o terminal móvel e o servidor), e onde a transferência afeta apenas as funções de segurança entre o terminal móvel e o PAs novo e antigo.

Resumo da Invenção

Esta invenção relaciona às comunicações de rádio, para o padrão WLAN de 2.4 GHz IEEE 802.11, para as redes de área local de alta performance de rádio (HIPERLANs), para o padrão ETSI HIPERLAN tipo 2, e para a associação de segurança do nível IPSEC entre o terminal sem fio e os elementos de rede. A invenção é utilizada em qualquer rede sem fio baseada em IP, exemplos dos quais inclui ETSI BRAN e o IEEE 802.11. Em adição, a invenção é utilizada quando o terminal móvel move entre duas entidades de roteadores IPSEC, onde um terminal sem fio comunica com um ponto terminal, que não é um ponto de acesso sem fio.

A presente invenção provê um método/aparelho eficiente para restabelecer uma associação de segurança existente quando um evento de transferência ocorre em um sistema de comunicação de rádio, tal como o IEEE 802.11 ou o HIPERLAN. A operação desta invenção aumenta o desempenho de transferência, e minimiza o retardo que é associado com a re-negociação de uma associação de segurança entre um PA novo e o terminal móvel.

A invenção provê um modo eficiente para manter uma associação de segurança estabelecida entre o terminal móvel e a rede de comunicação sem fio, quando

uma transferência ocorrer dentro da rede. Um exemplo de utilização da invenção é uma WLAN que possui um Protocolo de Segurança Internet (IPsec) baseado na associação de segurança entre o PAs e os terminais móveis que estão dentro da WLAN. Contudo, a invenção também utiliza para manter qualquer tipo de associação de segurança dinâmica, tal como as funções de segurança do nível de rádio da HIPERLAN/2.

De acordo com a invenção, a autenticação de um terminal móvel durante um evento de transferência é alcançada por um procedimento de desafio/resposta. De acordo com este procedimento de desafio/resposta, o PA novo envia um desafio ao terminal móvel, ao que o terminal móvel (TM) responde enviando uma resposta ao PA novo.

Uma chave de autenticação para ambas as extremidades do par de comunicações que é composto de um terminal móvel e um PA, é gerada originalmente por um protocolo de gerenciamento de chave seletora, por exemplo, a Troca de Chave Internet (TCI). As associações de segurança são transferidas entre os vários PAs que estão dentro do sistema de comunicação sem fio, para evitar a necessidade por uma nova e diferente troca de chave durante cada transferência.

As chaves e as suas informações relacionadas são solicitadas por um PA novo durante o processo de transferência, e as chaves e outras informações do PA antigo para o PA novo, em uma ou mais mensagens de transferência que passam entre o PA antigo e o PA novo. A troca de desafios de autenticação e as suas respostas são integradas na sinalização de transferência que ocorre entre o PA novo e o terminal móvel, que estão envolvidos na transferência.

De acordo com uma característica da invenção, as mensagens são as mensagens de controle de acesso ao meio (CAM).

Deverá ser observado que esta característica da invenção de fornecer a autenticação do ponto de acesso é desejável, mas é uma característica opcional.

Enquanto uma conexão segura é preferida entre os pontos de acesso, tal característica não é solicitada pelo espírito e escopo da invenção.

Estas e outras características e vantagens da invenção serão aparentes ao técnico no assunto em referência à descrição detalhada a seguir da invenção, onde a descrição faz referência aos desenhos.

Breve Descrição das Figuras

Figura 1 – é uma apresentação de um sistema de comunicação, no qual uma incorporação da presente invenção é operável.

Figura 2 – é uma apresentação de um processo de transferência direto de acordo com a invenção.

Figura 3 – é uma apresentação de um processo de transferência de retorno de acordo com a invenção.

Figuras 4a a 4c – fornecem outra apresentação do processo de transferência direto da Figura 2.

Figuras 5a a 5c – fornecem outra apresentação do processo de transferência de retorno da Figura 3.

Figura 6 – é uma apresentação da transferência forçada HIPERLAN/2 de acordo com a invenção.

Figura 7 – é uma apresentação da transferência direta da HIPERLAN/2 de acordo com a invenção.

Descrição Detalhada da Invenção

A Figura 1 é um exemplo de um sistema de comunicação que fornece as comunicações de rádio com e entre uma pluralidade de terminais móveis, dos quais o terminal móvel 12 é um exemplo. Em outro exemplo, um ponto de acesso cobre a interface de rádio e a ponte de rede fixa, com o ponto de acesso conectado à rede fixa, este exemplo não requer a UCC apresentada na Figura 1. O sistema de comunicação 10 forma uma WLAN que proporciona as comunicações de rádio com uma pluralidade de terminais móveis 12, como agrupado no padrão IEEE 802.11, como também, potencialmente, de acordo com o modo proprietário de operação, como é descrito no pedido de patente copendente mencionado acima. Outros sistemas de comunicação são análogos, e operação da presente invenção também é operável nos outros sistemas de comunicação.

A WLAN 10 inclui uma pluralidade de PAs aparte espaçados 14 e 114, que são individualmente localizados nas duas localizações geográficas aparte espaçadas. Enquanto apenas dois PAs 14, 114 apresentados, e na prática atual um maior número de PAs são utilizados. Os PAs 14, 114 algumas vezes são referenciados como estações base ou

dispositivos de antena remotos (DARs). O termo "ponto de acesso", "PA", ou "ap" deverão geralmente ser usados aqui para identificar os dispositivos que formam os pontos de acesso à infra-estrutura de rede do sistema de comunicação 10. O termo "terminal móvel", "TM"ou "tm"deverão geralmente ser usados para identificar os dispositivos que formam os pontos de acesso para os pontos de acesso.

Cada um dos PAs 14, 114 incluem um circuito transceptor de rádio 16 que é capaz de transmitir/receber os sinais de comunicação de rádio com os terminais móveis 12, quando os terminais móveis são posicionados dentro de uma taxa de comunicação de um PA particular. Geralmente, um terminal móvel 12 comunica com um PA 14, 114 quando o terminal móvel é posicionado dentro de uma área geográfica ou célula 18, 118, que está próxima a e definida por um determinado ponto de acesso. Na Figura 1, a célula 18 é associada com o ponto de acesso 14, o terminal móvel 12 reside dentro da célula 18, e a célula 118 é associada com o ponto de acesso 114. Note que no modo seletor 34, é incluído apenas quando uma implementação da invenção usa as mensagens de nível de enlace de rádio proprietário, esta não sendo uma implementação solicitada da invenção.

Os pontos de acesso 14, 114 são acoplados a uma unidade de controle central (UCC) 22. A UCC 22 é tipicamente um HUB ou um roteador IP. A UCC 22 fornece para as conexões uma rede backbone de comunicação externa 24. Embora não apresentados, outros dispositivos de comunicação, tal como outras estações de comunicação e as outras redes de comunicação são tipicamente acoplados a rede backbone de comunicação 24. Deste modo, um caminho de comunicação pode ser formado para fornecer as comunicações entre o terminal móvel 12 e as estações de comunicação que são acopladas, diretamente ou indiretamente, à rede backbone de comunicação 24. Além disso, a comunicação local entre uma pluralidade de terminais móveis 12 é permitida. Em uma comunicação entre os pares de terminais móveis 12, o caminho de comunicação formado entre eles inclui dois enlaces de rádio separados.

Os PAs 14, 114 incluem os elementos de controle 28, que executam várias funções de controle relacionadas a operação dos respectivos PAs. Na Figura 1, os elementos de controle 28 são cada um apresentado para incluir um comparador 32, um modo seletor 34, e um determinador de disponibilidade de transferência 36, cujos elementos de controle

são funcionais e implementados da maneira desejada, como, por exemplo, os algoritmos que são executáveis pelo circuito de processamento. Em outra implementação, as funções que são executadas através de tais elementos são localizadas em outro lugar, tal como o terminal móvel 12 como indicado pelo bloco 28', ou pela UCC 22 como indicado pelo bloco 28". Assim, as funções executadas pelos elementos de controle podem ser distribuídas entre os vários dispositivos diferentes.

Note que de acordo com a invenção, o comparador 32 inclui funções de segurança, e o bloco 28 inclui as funções de controle de acesso ao meio (CAM).

Na construção e disposição da Figura 1, e como ensinado pelo pedido de patente copendente acima mencionado, um par de comunicações que consiste em um PA 14, 114 e um terminal móvel 12 são operáveis de acordo com o modo-padrão IEEE 802.11, quando é determinado que o par de comunicações não estão ambos no modo-proprietário compatível, ou eles são operáveis conforme o modo-proprietário quando for determinar que ambos os membros do par de comunicações são capazes do modo-proprietário. Para produzir este resultado, um comparador 32 recebe os identificadores que identificam o modo-operável do terminal móvel e o ponto de acesso que forma um par de comunicações. O modo seletor 34 então seleciona o modo-padrão de operação ou o modo-proprietário de operação, para a comunicação entre o terminal móvel e o ponto de acesso.

Como a posição física de um terminal móvel 12 altera de célula 18 para célula 118 durante uma determinada sessão de comunicação, o terminal móvel 12 deixa a primeira área 18 geográfica que é servida pelo PA 14, e então entra na segunda área 118 geográfica que é servida pelo PA 114. De célula-para-célula ou o movimento de área-a-área requer uma transferência de comunicações do antigo-PA 14 que é associado com a primeira área 18 para o novo-PA 114 que é associado com a segunda área 118, permitindo então a comunicação contínua com o terminal móvel 12.

O determinador de disponibilidade de transferência 36 provê indicações ao terminal móvel 12 dos PAs disponíveis, para os quais uma transferência de comunicações é possível, esta disponibilidade sendo contida em uma lista 38 do ponto de acesso disponível que contém as identidades dos PAs que estão disponíveis para a transferência de comunicações.

A lista 38 do ponto de acesso disponível pode ser comunicada aos terminais móveis 12 a intervalos de tempo selecionados, ou a lista 38 de ponto de acesso pode ser fornecida a cada terminal móvel 12 quando o terminal móvel é ativado inicialmente, ou um prefixo de rede ou uma lista de prefixos de rede podem ser usados para fornecer a mesma meta.

Nesta descrição da invenção será assumidos que uma associação de segurança (AS) existe entre terminal móvel 12 e o PA 14 atual ou antigo. Quer dizer, será assumido que o terminal móvel 12 e o PA 14 compartilham o mesmo jogo comum de chaves e outras informações que são necessárias para alcançar a função(s) de segurança. De acordo com a invenção, esta associação de segurança estabelecida e compartilhada é transferida do antigo-PA 14 para o novo-PA 114, em um modo seguro, quando o terminal móvel move da célula 18 para a célula 118. Esta transferência é feita de uma maneira muito rápida minimizando o número de mensagens que são necessárias para efetuar a transferência, e eliminando o uso da codificação da chave pública. Como resultado, a interrupção de uma transferência de tráfego de carga útil para e do terminal móvel 12 é minimizado, e qualquer interrupção deste tipo é muito importante para os serviços em tempo real, como Voz sobre o IP (VOIP) e a distribuição de vídeo.

De acordo com a invenção, uma chave de autenticação ou a associação de segurança para ambas as extremidades do enlace de comunicação (isto é o enlace que envolve o terminal móvel 12 e o PA 14) é gerado por um protocolo de gerenciamento de chave, tal como o TCI, sendo observado que o protocolo de troca de chave Diffie-Hellman também pode ser utilizado.

Depois, quando o terminal móvel 12 move da célula 18 e do seu PA 14 para célula 118 e para o seu PA 114, a autenticação durante o processo de transferência é alcançada pelo procedimento de desafio/resposta simples da invenção. Além disso, as associações de segurança são transferidas entre o antigo-PA 14 e o novo-PA 114, evitando assim a necessidade por uma nova troca de chave durante a transferência do antigo-PA 14 para o novo-PA 114.

Durante o procedimento de desafio/resposta, o novo-PA 118 envia um desafio ao terminal móvel 12, ao que o terminal móvel 12 envia uma resposta para o novo

PA 118. Em adição, o terminal móvel 12 autentica o novo-PA 118 de uma maneira semelhante durante a transferência.

As chaves e as informações relacionadas são solicitadas pelo novo-PA 14, ao que eles são transferidos do antigo-PA 14 para o novo-PA 114 nas mensagens de transferência. Similarmente, a troca do desafio de autenticação e as suas respostas são integradas na sinalização de transferência que ocorre entre o novo-PA 114 e o terminal móvel 12.

A Figura 2 apresenta um processo 20 de transferência direta (TR) de acordo com a invenção, esta sendo uma incorporação preferida da invenção. No processo 20 de transferência direta, a sinalização de transferência é enviada entre o terminal móvel (TM ou tm) 12 e o novo ponto de acesso (PA ou pa) 114. Este tipo de transferência é especialmente útil quando o enlace de rádio 21 é perdido sem advertência anterior.

A Figura 3 apresenta um processo 30 de transferência de retorno (TR) de acordo com a invenção. No processo 30 de transferência de retorno, a transferência é solicitada através do terminal móvel 12 em comunicação com o antigo-PA 14, este resultando em uma sucessão de mensagem um pouco diferente da que é apresentada na Figura 2. Durante a transferência de retorno, uma opção benéfica é usar a mensagem 31 de interface de rádio, que transporta o desafio de autenticação do antigo-PA 14 para terminal móvel 12 também dispara a transferência 33 de retorno. Isto é, o desafio de autenticação 31 é usado para indicar o terminal móvel 12, que este deveria desconectar do antigo-PA 14 e conectar ao novo-PA 114, onde uma associação de segurança 35 (AS) já foi preparada para o terminal móvel 12.

Como usado aqui, o termo "antigo-PA" significa um ponto de acesso, tal como o ponto de acesso 14 com o qual o terminal móvel 12 está comunicando originalmente ou atualmente. Então, o termo "antigo-PA" também significa o "atual-PA" com o qual o terminal móvel 12 está comunicando no momento que a transferência de comunicação é requerida.

Como usado aqui, o termo "novo-PA" significa um ponto de acesso tal como o ponto de acesso 114 com o qual o terminal móvel 12 deve começar a comunicar porque o terminal móvel moveu geograficamente de uma célula 18 antiga para uma célula

118 nova. Então, o termo "novo-PA" significa um "futuro-PA" com o qual o terminal móvel 12 comunicará após uma transferência de comunicação tiver sido completado.

Nas Figuras 2 e 3, os nomes da mensagem IEEE 802.11 são usados, e os parâmetros adicionais das mensagens de transferência são apresentados. Contudo, esta denominação das mensagens não é crítica ao escopo desta invenção, uma vez que a invenção pode ser realizada em outros sistemas que o IEEE 802.11. O uso das mensagens CAM (controle de acesso ao meio) estendidas nas Figuras 2 e 3, transportam os parâmetros adicionais sobre as interfaces de rádio, é, contudo benéfico no fato de que a necessidade para enviar as mensagens adicionais é evitada.

Para garantir a segurança, é desejável que mensagens que transportam as chaves sejam cifradas. Então, a transferência de associação de segurança ou AS e o outro tráfego de controle entre os PAs 14, 114, são apresentados como sendo codificados e autenticados pelo IPsec.

Os meios específicos onde é determinado que terminal móvel 12 tem fisicamente movido em relação às células 18, 118, tal que a transferência seja requerida, não é crítico à presente invenção. Por exemplo, o procedimento pode ser análogo ao usado nos sistemas celulares de divisão de tempo convencionais, que usam os procedimentos de transferência assistidos móveis. Em geral, o terminal móvel 12 sintoniza aos canais de controle das estações bases ou PAs das células adjacentes, tal como as células 18, 118, por exemplo a intervalos temporizados. A intensidade do sinal, ou alguma outra característica do sinal, tal como uma taxa de erro de bit dos sinais que são radiodifusados nestes canais de controle, são então medidos ou detectados através do terminal móvel 12. Os sinais ascendentes que são baseados nesta medida do terminal móvel 12 são enviados então pelo terminal móvel à rede 10, ao que a rede 10 determina se uma transferência de comunicação deveria ser efetuada. Quando esta é determinada, a transferência é requerida, e as instruções são enviadas ao terminal móvel 12, e o processo de transferência de comunicação da Figura 2 ou da Figura 3 inicia.

As Figuras 4a a 4c fornecem outra apresentação do processo 20 de transferência direto, em que a transferência de comunicação do terminal móvel 12 é fornecida em relação do antigo-PA 14 e do novo-PA 114, quando o terminal móvel move da

célula 18 para célula 118. Nesta figura um terminal móvel ou TM é também referenciado usando o termo "tm", e um ponto de acesso ou PA é também referenciado usando o termo "pa". Com referência à Figura 4a, o processo 20 de transferência direta é iniciado no terminal móvel 12 pelo saída sim 400 do evento 401, indicando que a transferência é requerida. O terminal móvel 12 opera agora a função 402 para ativar a sua função de transferência de rádio.

A função 403 do terminal móvel 12 gera um desafio para o novo-PA 114, ao que a função 404 onde uma mensagem SOL_REASSOCIAÇÃO_CAM que contém "desafio_tm" é enviada para o novo PA 114.

Na função 405, o novo-PA 114 aceita a mensagem 404, ao que o novo-PA 114 opera a função 406 para enviar um pedido de transferência para o antigo-PA 14.

O antigo-PA 14 opera agora a função 407 para recuperar os parâmetros de associação de segurança AS, AS de seu banco de dados de associação de segurança. O antigo-PA 14 opera então a função 408, para enviar um pedido de transferência que contém os parâmetros AS, AS para o novo-PA 114.

Com referência à Figura 4b, o novo-PA 1 14 opera agora a função 409, para criar uma associação de segurança (AS), e opera a função 410 para gerar um desafio para autenticar o terminal móvel 12, e opera a função 411 para calcular uma resposta ao "desafio_tm" que estava contido na mensagem 404 da Figura 4a, e opera a função 412 para enviar uma mensagem SOL_AUTENTICAÇÃO_CAM para o terminal móvel 12. A mensagem 412 contém a "resposta_pa" que foi calculada pela operação da função 411, contém o "desafio_pa"que foi gerado pela operação da função 410, e contém a "outra informação".

O terminal móvel 12 opera agora a função 413, para atualizar os seus parâmetros de associação de segurança, opera a função 414 para calcular uma resposta ao "desafio_pa" que foi recebido por via de mensagem 412, e opera a função 415 para comparar a "resposta_pa" que foi recebida por meio da mensagem 412 à resposta correta ou esperada.

Quando a comparação executada através da função 415 produz uma comparação correta, a função 416 opera para autenticar o novo-PA 114, a função 417 opera

para enviar uma mensagem RESP_AUTENTICAÇÃO_CAM para o novo-PA 114, esta mensagem que contém a "resposta_tm" foi calculada na função 414.

Com referência agora à Figura 4c, na função 418 o novo-PA 114 opera para comparar a "resposta_tm" recebida por meio da mensagem 417 para a resposta correta ou própria, e quando esta comparação produz uma comparação correta, a função 419 opera para autenticar o terminal móvel 12. O novo-PA 114 opera então a função 420 para enviar uma mensagem RESP_REASSOCIAÇÃO_CAM para o terminal móvel 12, ao que transferência é completada e o terminal móvel 12 opera depois a função 421 para retomar seu tráfego de carga útil usando o novo-PA 114.

As Figuras 5ª-5c fornecem outra apresentação do processo 30 de transferência de retorno, em que a transferência de comunicação é provida para o terminal móvel 12 relativo ao antigo-PA 14 e ao novo-PA 114. Nesta figura um terminal móvel ou TM é também referenciado para usar o termo "tm", e o ponto de acesso ou PA é também referenciado para usar o termo "pa".

Com referência à Figura 5a, o processo 30 de transferência de retorno é iniciado no terminal móvel 12 pela saída sim 500 do evento 501, indicando que a transferência é requerida. O terminal móvel 12 opera agora a função 502 para enviar um pedido de transferência para o antigo-PA 14.

Quando mensagem 502 é recebida no antigo-AP 14, a função 503 aceita a mensagem, a função 504 opera para recuperar os parâmetros de associação de segurança AS, AS de sua base de dados de associação de segurança (AS), e a função 505 opera para enviar um pedido de transferência que contém os parâmetros AS, AS para o novo-PA 114.

Usando os parâmetros AS, AS que foram recebidos na mensagem 505, o novo-PA114 agora opera a função 506 para criar a sua própria associação de segurança (AS). O novo-PA 114 opera então a função 507 para gerar um desafio para autenticar o terminal móvel 12, e na função 508 um pedido de transferência é enviado ao antigo-PA 14, este pedido 508 incluindo o "desafio_pa" que foi gerado na função 507, e a "outra informação".

Com referência agora à Figura 5b, com relação à mensagem 508, o antigo-PA 14 opera a função 509 para enviar uma mensagem DESASSOCIAÇÃO_CAM para o

terminal móvel 12, esta mensagem contém o "desafio_pa" e a "outra_informação" que era do antigo-PA 14 recebida do novo-PA 114 por via de mensagem 508.

Em resposta à mensagem 509, o terminal móvel 12 ativa a sua função de transferência de rádio 510. Na função 511 o terminal móvel 12 atualiza agora os seus parâmetros de associação de segurança, na função 511 o terminal móvel 12 opera para calcular uma resposta para a parte "desafio_pa" das mensagens 508 e 509, na função 513 o terminal móvel 12 opera para gerar um desafio para autenticar o novo-PA 114, e na função 514 o terminal móvel 12 envia uma mensagem SOL_REASSOCIAÇÃO_CAM ao novo-PA 114. A mensagem 514 contém a "resposta_tm" que foi calculada na função 511, o "desafio_tm" foi gerado na função 512, e a "outra informação".

Com referência agora à Figura 5c, a função 515 provê a autenticação do terminal móvel 12, a função 516 compara a "resposta_tm" que foi recebida através da mensagem 513 para a resposta correta ou esperada, a função 517 calcula uma resposta para o "desafio_tm" que foi recebido por meio da mensagem 513, e a função 518 opera para enviar uma mensagem APER_RESP_REASSOCIAÇÃO_CAM para o terminal móvel 12, a mensagem contendo a "resposta_pa" que foi calculada através da função 517.

Na função 519 o terminal móvel 12 opera para autenticar o novo-PA 114 comparando na função 520 a "resposta_pa" contida na mensagem 518 com a resposta correta ou esperada, e como resultado desta comparação correta, a função 521 faz com que o terminal móvel 12 retome o tráfego de carga útil usando o novo PA 114.

Do anterior pode ser visto que a presente invenção provê um método/aparelho provê a segurança de informação quando a comunicação com um determinado terminal móvel 12 é manipulada sobre o primeiro ponto de acesso 14 para o um segundo ponto de acesso 114. O sistema de comunicação 10 é provido possuindo uma pluralidade de pontos de acesso, cada ponto de acesso servindo a uma área geográfica diferente que está dentro de uma área geográfica global que é servida através do sistema de comunicação, e uma pluralidade de terminais móveis 12 são fornecidos onde os terminais móveis são individualmente e fisicamente móveis dentro de toda a área geográfica global e entre as áreas geográficas diferentes.

No processo/aparelho de transferência da invenção, primeiro é detectado

quando um determinado terminal móvel 12 move de uma influência de comunicação com o primeiro ponto de acesso 14 em uma influência de comunicação com o segundo ponto de acesso 114 (veja 401 da Figura 4a e 501 da Figura 5a).

Quando tal movimento é detectado, os parâmetros de associação de segurança do primeiro ponto de acesso 14 (veja 407 da Figura 4a e 504 da Figura 5a), uma associação de segurança é criada no segundo ponto de acesso 114 de acordo com os parâmetros de associação de segurança recuperados (veja 409 da Figura 4b e 506 da Figura 5a), e uma associação de segurança criada no terminal móvel 12 determinado de acordo com os parâmetros de associação de segurança recuperados (veja 413 da Figura 4b e 510 da Figura 5b).

Em adição, quando tal movimento é detectado, um desafio-ponto-acesso-autenticação é enviado de um determinado terminal móvel 12 para o segundo ponto de acesso 114 (veja 404 da Figura 4a e 513 da Figura 5b), e um desafio-terminal-móvel-autenticação é enviado do segundo ponto de acesso 114 para um determinado terminal móvel 12 (veja 412 da Figura 4b e 508 da Figura 5a). Note que o desafio-ponto-acesso anteriormente descrito é uma característica opcional da invenção.

Em resposta ao desafio-ponto-acesso-autenticação que é recebido de um determinado terminal móvel 12, o segundo ponto de acesso 114 gera agora uma resposta-ponto-acesso-autenticação (veja 411 da Figura 4b e 516 da Figura 5c), e esta resposta-ponto-acesso-autenticação é enviada a um determinado terminal móvel 12 (veja 412 da Figura 4b e 517 da Figura 5c).

Em resposta ao desafio-terminal-móvel-autenticação que é recebido do segundo ponto de acesso 114, um determinado terminal móvel 12 agora calcula uma resposta-termianl-móvel-autenticação (veja 4 da Figura 4b e 511 da Figura 5b), e esta resposta-termianl-móvel-autenticação é enviada para o segundo ponto de acesso 114 (veja 417 da Figura 4b e 513 da Figura 5b).

A primeira comparação em um determinado terminal móvel 12, agora opera para comparar a resposta-ponto-acesso-autenticação que é recebida do segundo ponto de acesso 114 uma resposta correta ou esperada (veja 41 da Figura 4b e 519 da Figura 5c), e a segunda comparação no segundo ponto de acesso 114, agoa opera para comparar a resposta-

termianl-móvel-autenticação que é recebida de um determinado terminal móvel 12 para a resposta correta ou esperada (veja 418 da Figura 4c e 515 da Figura 5c).

Finalmente, a comunicação é iniciada entre um determinado terminal móvel 12 e o segundo ponto de acesso 114 baseado no resultado da primeira comparação e na segunda comparação (veja 421 da Figura 4c e o 520 da Figura 5c).

As Figuras 6 e 7 apresentam duas incorporações adicionais da invenção. Enquanto os detalhes específicos das incorporações das Figuras 6 e 7 diferem nos detalhes específicos desta, os conteúdos das incorporações das Figuras 6 e 7 serão prontamente aparentes por meio de uma comparação às incorporações das Figuras 2, 3, 4a- 4b e 5a- 5b da invenção.

Enquanto a invenção foi descrita em detalhes enquanto fazia referência às incorporações preferidas, nenhuma parte desta descrição detalhada pode ser tomada como uma limitação ao espírito e escopo da invenção, visto que é conhecido que outros técnicos no assunto podem visualizar outras incorporações que estão dentro do espírito e escopo desta invenção, então a invenção é geralmente conhecida como definida pelas reivindicações apensas.

REIVINDICAÇÕES

1. Método (20) para fornecer segurança na informação quando a comunicação com um determinado terminal móvel (12) é transferida do primeiro ponto de acesso (14) para o segundo ponto de acesso (114), em que o método compreende os passos de:

- fornecer um sistema de comunicação (10) possuindo uma pluralidade de pontos de acesso (14, 114), cada ponto de acesso servido a uma área geográfica diferente (18, 118) dentro de toda a área geográfica que é servida pelo sistema de comunicação;

- fornecer uma pluralidade de terminais móveis (12) que são cada um fisicamente móvel dentro de toda área geográfica e entre as diferentes áreas geográficas (18, 118);

- detectar (401) quando um determinado terminal móvel move de uma influência de comunicação com o primeiro ponto de acesso para uma influência de comunicação com o segundo ponto de acesso;

CARACTERIZADO pelo fato de que o método ainda compreende os passos de:

- responder ao passo de detectar através da recuperação (407) dos parâmetros de associação de segurança do primeiro ponto de acesso (14), pela criação (409) de uma associação de segurança no segundo ponto de acesso (114) de acordo com os parâmetros de associação de segurança recuperados, e pela criação de uma associação de segurança de um determinado terminal móvel (12) de acordo com os parâmetros de associação de segurança recuperados; e

- iniciar (421) a comunicação entre um determinado terminal móvel (12) e o segundo ponto de acesso (114) baseado no passo de resposta.

2. Método (20) de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende os passos de:

- responder ao passo de detecção (401) pelo envio (404) de um desafio-ponto-acesso-autenticação (412) do terminal móvel determinado (12) para o segundo ponto de acesso (114), e pelo envio (412) de um desafio-terminal-móvel-autenticação do segundo ponto de acesso (114) para um determinado terminal móvel (12);

- gerar (410) uma resposta-ponto-acesso-autenticação para o segundo ponto

de acesso (114) em resposta ao desafio-ponto-acesso-autenticaçãorecebido do terminal móvel (12);

- enviar (412) a resposta-ponto-acesso-autenticação para um determinado terminal móvel;

- gerar (414) uma resposta-terminal-móvel-autenticação para um determinado terminal móvel (12) em resposta ao desafio-terminal-móvel-autenticação recebido do segundo ponto de acesso;

- enviar (417) a resposta-terminal-móvel- autenticação para o segundo ponto de acesso;

- comparar primeiro (415) a resposta-ponto-acesso-autenticação à uma resposta correta em um determinado terminal móvel;

- comparar em segundo (418) a resposta-terminal-móvel-autenticação à uma resposta correta no segundo ponto de acesso; e

- iniciar (420) a comunicação entre um determinado terminal móvel e o segundo ponto de acesso baseado na primeira etapa de comparação e na segunda etapa de comparação.

3. Método (20) de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que uma pluralidade de terminais móveis (12) possuem uma camada de controle de acesso ao meio e de camadas físicas compatíveis, e onde as mensagens são as mensagens de controle de acesso ao meio.

4- Método (20) de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que as mensagens são transmitidas dentro de uma rede área local sem fio tal como o IEEE 802.11 ou as mensagens de múltiplo acesso da HIPERLAN/2 (rede de área local de alta performance de rádio/do tipo 2).

5- Método (20) de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que o sistema de comunicação (10) é um sistema de comunicação WLAN (rede de área local sem fio) onde o protocolo de segurança é usado para fornecer uma segurança de extremo-a-extremo para os pacotes de dados.

6- Método (20) de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a segurança de extremo-a-extremo é fornecida pela autenticação e/ou

codificação dos pacotes de dados, onde o protocolo de segurança fornece uma criptografia simétrica solicitando o uso de uma mesma codificação e/ou chave de autenticação em ambas as extremidades de um enlace de comunicação.

7- Método (20) de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que o protocolo de gerenciamento de chave seletora opera para gerar as chaves simétricas para o protocolo de segurança.

8- Método (20) de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que compreende os passos de:

- fornecer uma sessão dependente da chave de codificação dinâmica entre um determinado terminal móvel e o segundo ponto de acesso; e

- transferir uma associação de segurança ativa do primeiro ponto de acesso para o segundo ponto de acesso quando um terminal móvel move dentro de uma área de cobertura de comunicação que é fornecida pelo sistema de comunicação.

9 - Método (20) de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que compreende os passos de:

- fornecer o sistema de comunicação (10) tal como a rede de área local;

- fornecer um servidor dentro da rede de área local;

- fornecer uma chave de gerenciamento e de reestabelecimento da associação de segurança dentro da rede de área local durante a transferência de comunicação, sem solicitar uma modificação para uma associação de segurança de extremo-a-extremo, quando uma comunicação que continua durante a transferência de comunicação, tal que a transferência de comunicação realize apenas as funções de segurança entre o terminal móvel e o primeiro e o segundo pontos de acesso.

10- Método (20) de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que a rede de área local inclui o Protocolo de Segurança Internet baseado na associação de segurança entre uma pluralidade de pontos de acesso (14, 114) e uma pluralidade de terminais móveis (12).

11- Método (20) de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a chave de autenticação é fornecida para ambas as extremidades de um par de comunicação que é feito de um determinado terminal móvel (12) e do primeiro e do

segundo pontos de acesso (14, 114), a chave de autenticação sendo gerada pelo protocolo de gerenciamento de chave seletora.

12- Método (20) de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a chave de autenticação ou de associação de segurança existe entre um determinado terminal móvel (12) e o primeiro ponto de acesso (14) de acordo com o protocolo de gerenciamento de chave seletora; e onde as associações de segurança são transferidas entre uma pluralidade de pontos de acesso (14, 114) de forma a evitar a necessidade entre uma pluralidade de pontos de acesso (14, 114) de forma a evitar a necessidade para uma nova troca de chave durante a transferência de comunicação.

13- Método (20) de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que o protocolo de gerenciamento de chave seletora é um TCI, e onde as associações de segurança são transferidas entre o primeiro ponto de acesso (14) e o segundo ponto de acesso (114) de forma a evitar a necessidade para uma nova troca de chave durante a transferência de comunicação do primeiro ponto de acesso (14) para o segundo ponto de acesso (114).

14- Método (20) de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que inclui o passo de codificar as mensagens para transportar as chaves.

15- Aparelho para manter uma determinada associação de segurança em um sistema de radiocomunicação (10), em que quando uma transferência de comunicação ocorre quando um terminal móvel (12) move fisicamente da primeira área geográfica (18) que é servida pelo primeiro ponto de acesso de comunicação (14) para a segunda área geográfica (118) que é servida pelo segundo ponto de acesso de comunicação (114), o terminal móvel (12) inicialmente forma o primeiro par de comunicações com o primeiro ponto de acesso de comunicação (14), e após a transferência de comunicação do terminal móvel formando o segundo par de comunicações com o segundo ponto de aceso de comunicação (114), cada membro do primeiro par de comunicações (12 – 14) possuindo uma determinada associação de segurança associada com o aparelho, o aparelho compreende:

- primeiro dispositivo (40) no terminal móvel (12) para detectar a necessidade para iniciar a transferência de comunicação;

- segundo dispositivo (45) dentro do sistema de radiocomunicação (10) e responsável ao primeiro dispositivo (40) detectando a necessidade para iniciar a transferência de comunicação para estabelecer uma determinada associação de segurança no segundo ponto de acesso de comunicação (114);

CARACTERIZADO pelo fato de que ainda compreende:

- terceiro dispositivo (403) no terminal móvel (12) para gerar o desafio-ponto-acesso como uma função de uma determinada associação de segurança, e para enviar o desafio-ponto-acesso para o segundo ponto de acesso de comunicação;

- quarto dispositivo (410) no segundo ponto de acesso de comunicação para gerar o desafio-terminal-móvel como uma função de uma determinada associação de segurança estabelecida no segundo ponto de acesso de comunicação, e para enviar o desafio-terminal-móvel para o terminal móvel;

- quinto dispositivo (414) no terminal móvel e responsável pelo desafio-terminal-móvel para gerar a resposta do terminal móvel como uma função de uma determinada associação de segurança, e para enviar a resposta do terminal móvel para o segundo ponto de acesso de comunicação;

- sexto dispositivo (409) no segundo ponto de acesso de comunicação e responsável pelo desafio-ponto-acesso para gerar uma resposta do ponto de acesso como uma função de uma determinada associação de segurança estabelecida no segundo ponto de acesso de comunicação, e para enviar a resposta do ponto de acesso para o terminal móvel;

- sétimo dispositivo no terminal móvel e responsivo para a resposta do ponto de acesso para determinar se a resposta do ponto de acesso está correta como uma função de uma determinada associação de segurança;

- oitavo dispositivo (418) no segundo ponto de acesso de comunicação (114) e responsivo para a resposta do terminal móvel para determinar se a resposta do terminal móvel está correta como uma função de uma determinada associação de segurança estabelecida no segundo ponto de acesso de comunicação; e

- nono dispositivo (420) dentro do sistema de radiocomunicação (10) e responsivo ao oitavo e nono dispositivos para estabelecer a transferência de comunicação

quando ambas a resposta do terminal móvel e a resposta do ponto de acesso estiverem corretas.

16- Aparelho de acordo com a reivindicação 15, **CARACTERIZADO** pelo fatp de que o sistema de radiocomunicação (10) é selecionado do grupo IEEE 802.11 e da HIPERLAN (rede de área local de alta performance de rádio).

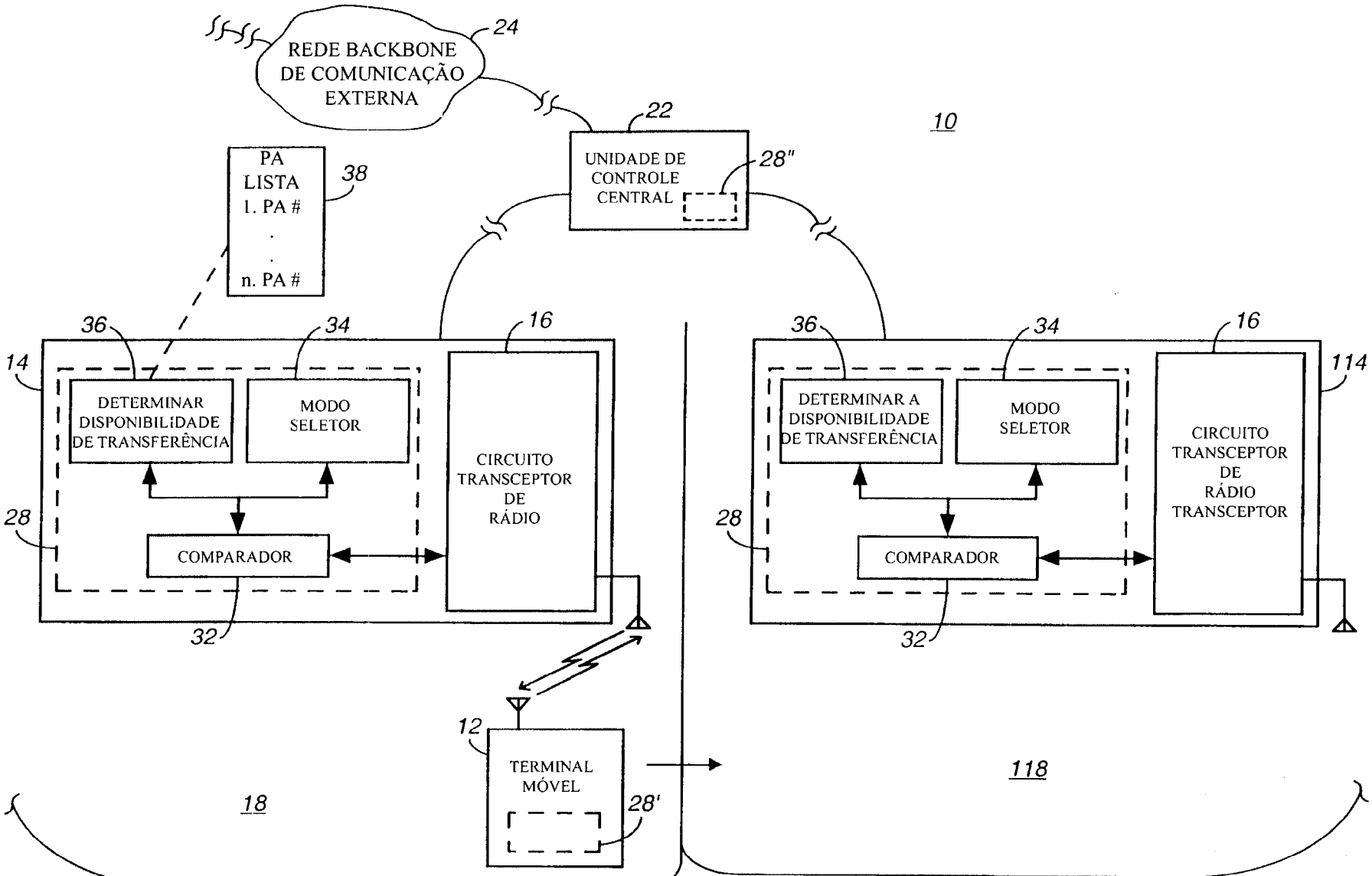
REDE BACKBONE DE COMUNICAÇÃO EXTERNA
24
22
10
UNIDADE DE CONTROLE CENTRAL
28"
PA LISTA
1. PA #
.
.
n. PA #
38
36
34
16
14
DETERMINAR DISPONIBILIDADE DE TRANSFERÊNCIA
MODO SELETOR
CIRCUITO TRANSCEPTOR DE RÁDIO
28
COMPARADOR
32
DETERMINAR A DISPONIBILIDADE DE TRANSFERÊNCIA
MODO SELETOR
CIRCUITO TRANSCEPTOR DE RÁDIO TRANSCEPTOR
114
12
TERMINAL MÓVEL
28'
18
118

FIG. 1

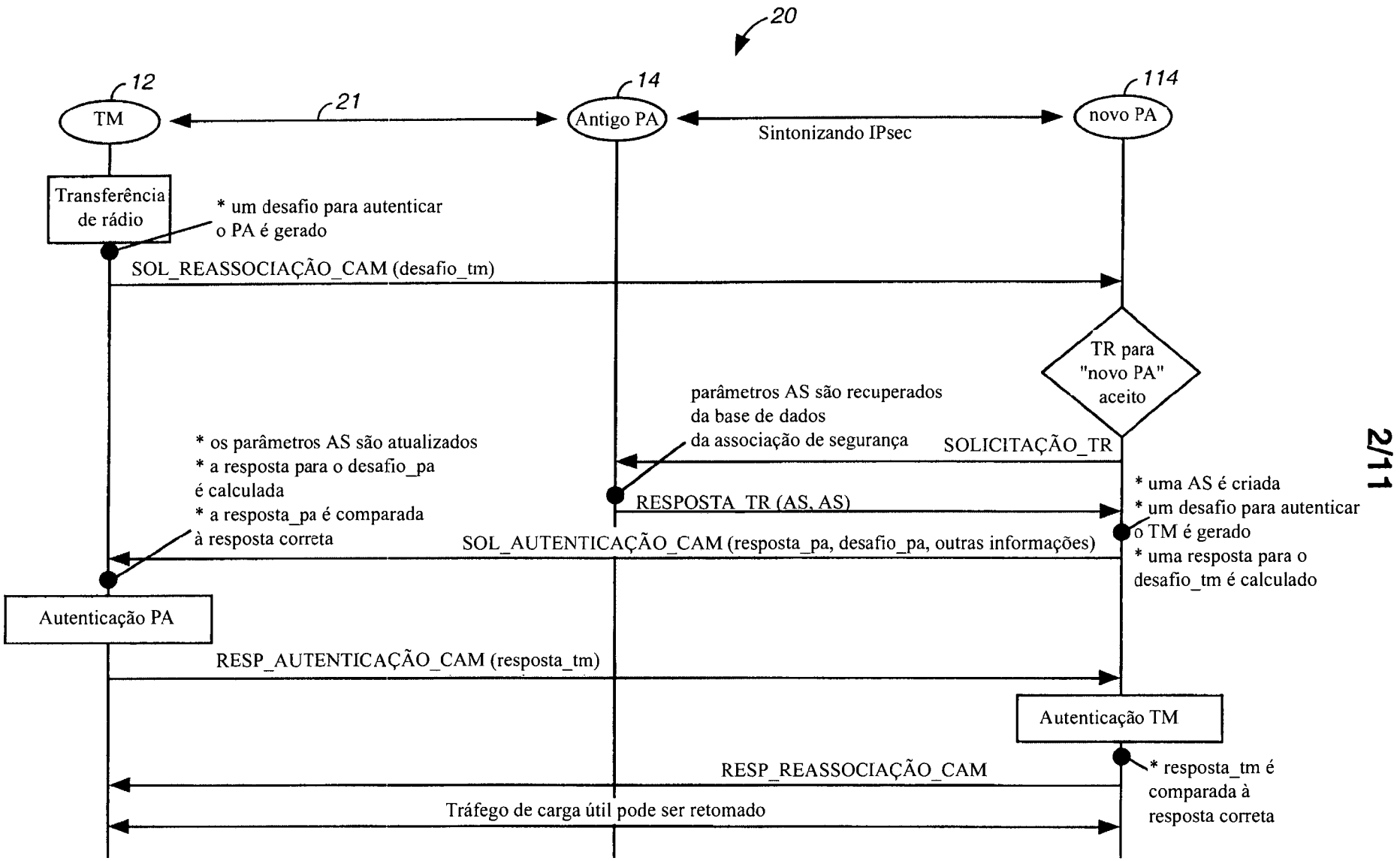
20
12
TM
21
14
Antigo PA
Sintonizando IPsec
114
novo PA
Transferência de rádio
* um desafio para autenticar o PA é gerado
SOL_REASSOCIAÇÃO_CAM (desafio_tm)
TR para "novo PA" aceito
parâmetros AS são recuperados da base de dados da associação de segurança
SOLICITAÇÃO_TR
* os parâmetros AS são atualizados
* a resposta para o desafio_pa é calculada
* a resposta_pa é comparada à resposta correta
RESPOSTA_TR (AS, AS)
* uma AS é criada
* um desafio para autenticar o TM é gerado
* uma resposta para o desafio_tm é calculado
SOL_AUTENTICAÇÃO_CAM (resposta_pa, desafio_pa, outras informações)
Autenticação PA
RESP_AUTENTICAÇÃO_CAM (resposta_tm)
Autenticação TM
* resposta_tm é comparada à resposta correta
RESP_REASSOCIAÇÃO_CAM
Tráfego de carga útil pode ser retomado

FIG. 2

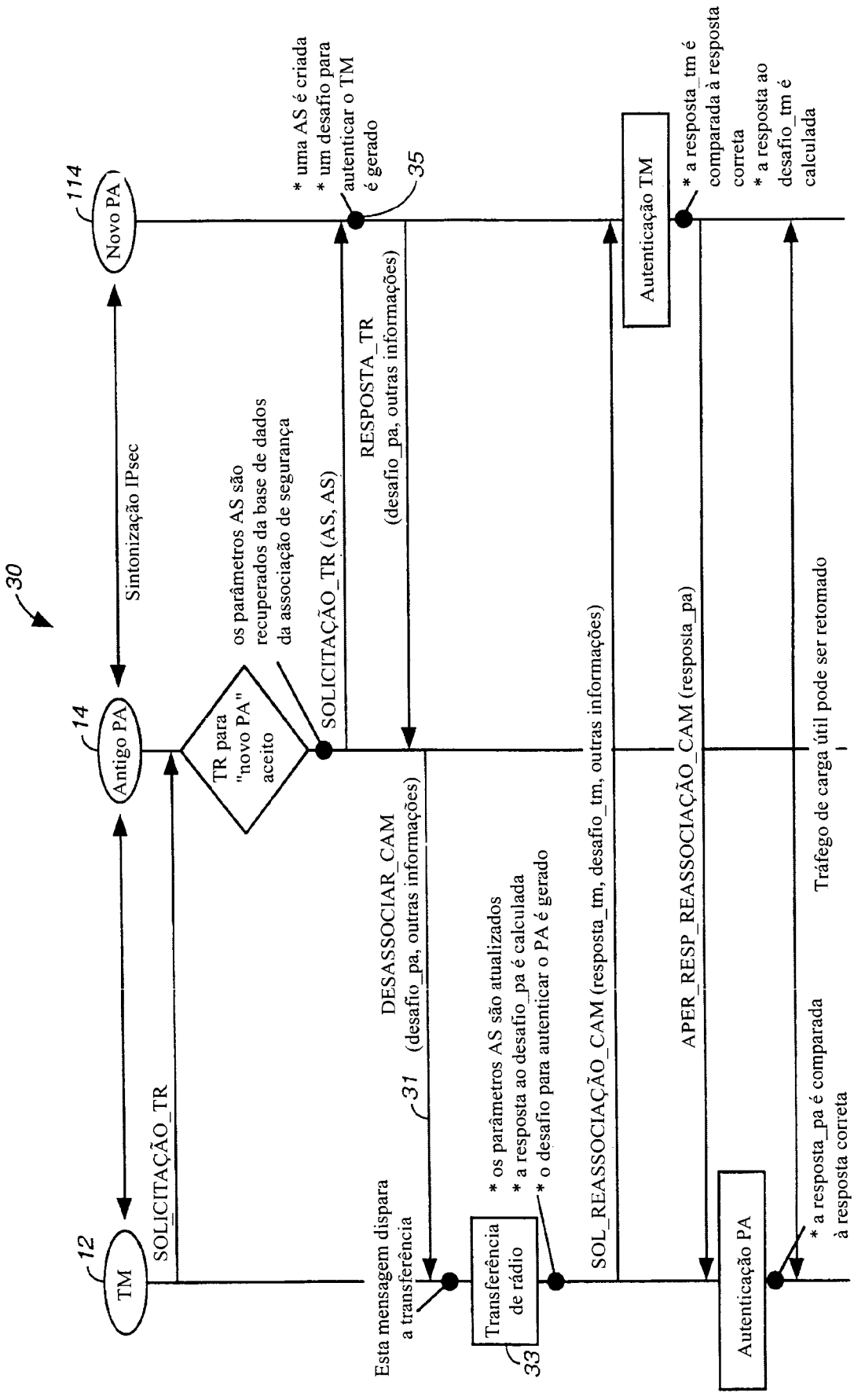
30
12
TM
14
Antigo PA
114
Novo PA
Sintonização IPsec
SOLICITAÇÃO_TR
TR para "novo PA" aceito
os parâmetros AS são recuperados da base de dados da associação de segurança
SOLICITAÇÃO_TR (AS, AS)
* uma AS é criada
* um desafio para autenticar o TM é gerado
35
RESPOSTA_TR (desafio_pa, outras informações)
DESASSOCIAR_CAM (desafio_pa, outras informações)
31
Esta mensagem dispara a transferência
Transferência de rádio
33
* os parâmetros AS são atualizados
* a resposta ao desafio_pa é calculada
* o desafio para autenticar o PA é gerado
SOL_REASSOCIAÇÃO_CAM (resposta_tm, desafio_tm, outras informações)
Autenticação TM
* a resposta_tm é comparada à resposta correta
* a resposta ao desafio_tm é calculada
APER_RESP_REASSOCIAÇÃO_CAM (resposta_pa)
Autenticação PA
* a resposta_pa é comparada à resposta correta
Tráfego de carga útil pode ser retomado

FIG. 3

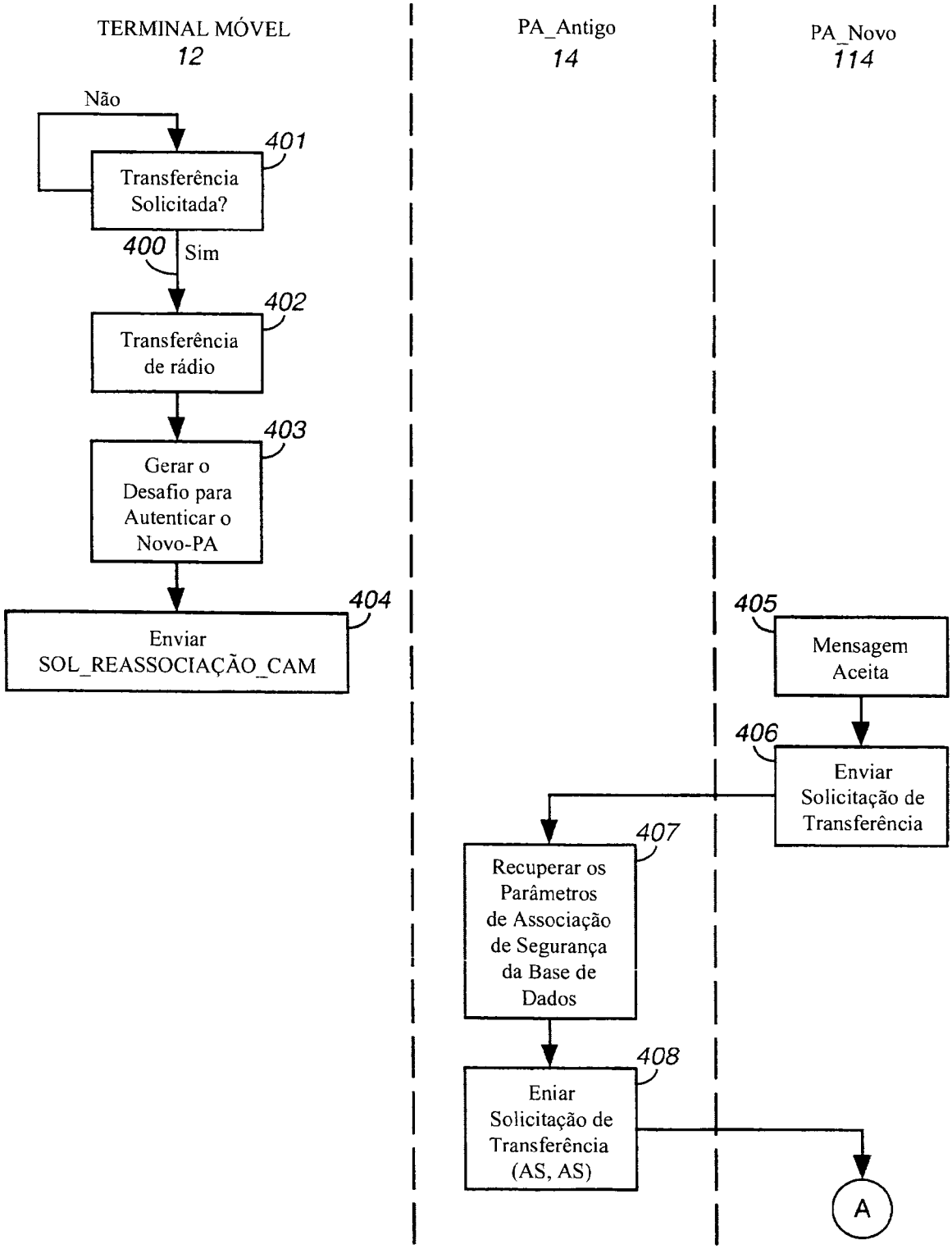
TERMINAL MÓVEL
12
PA_Antigo
14
PA_Novo
114
Não
401
Transferência Solicitada?
400
Sim
402
Transferência de rádio
403
Gerar o Desafio para Autenticar o Novo-PA
404
Enviar SOL_REASSOCIAÇÃO_CAM
405
Mensagem Aceita
406
Enviar Solicitação de Transferência
407
Recuperar os Parâmetros de Associação de Segurança da Base de Dados
408
Eniar Solicitação de Transferência (AS, AS)
A

FIG. 4A

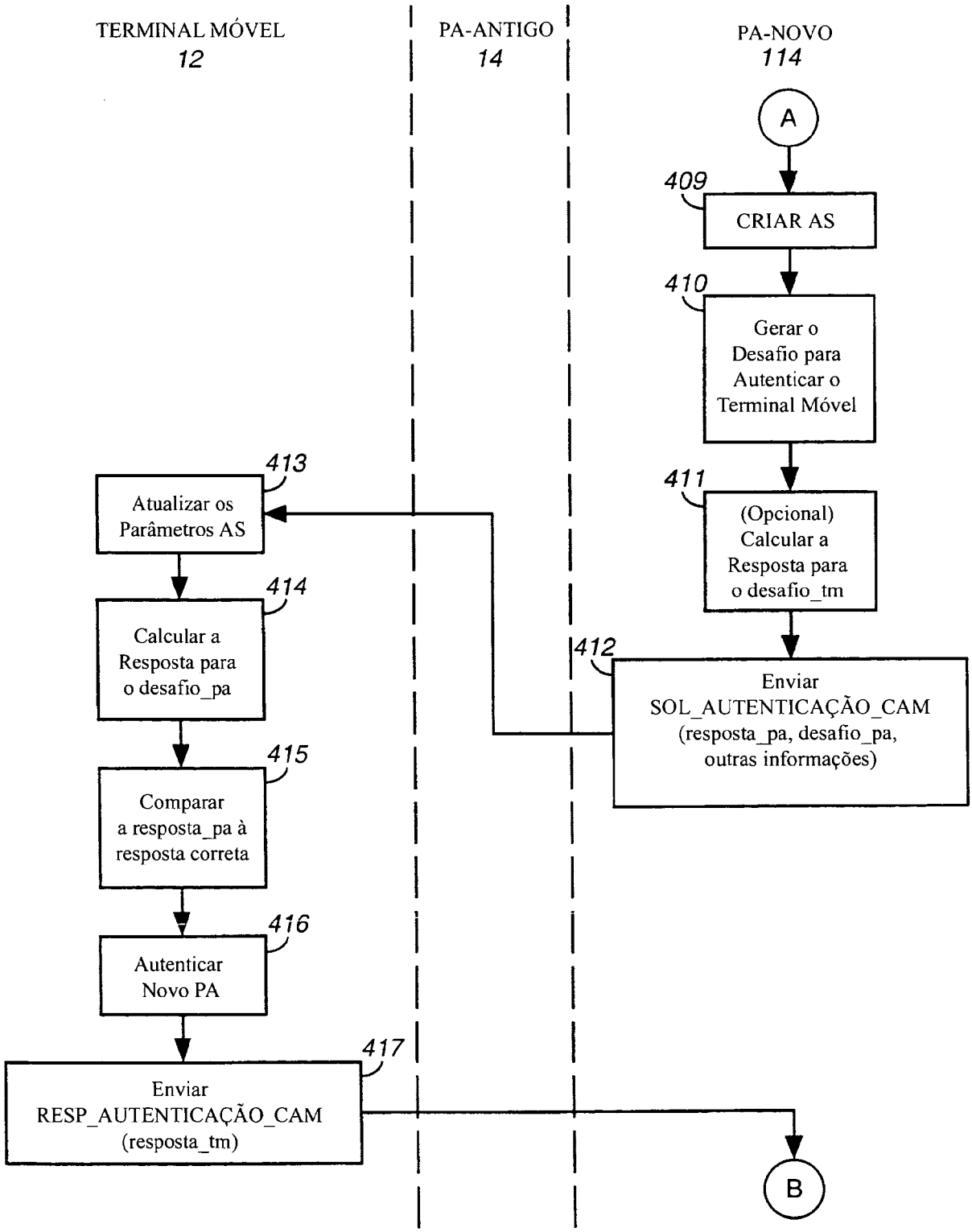
TERMINAL MÓVEL
12
PA-ANTIGO
14
PA-NOVO
114
A
409
CRIAR AS
410
Gerar o Desafio para Autenticar o Terminal Móvel
411
(Opcional) Calcular a Resposta para o desafio_tm
412
Enviar SOL_AUTENTICAÇÃO_CAM (resposta_pa, desafio_pa, outras informações)
413
Atualizar os Parâmetros AS
414
Calcular a Resposta para o desafio_pa
415
Comparar a resposta_pa à resposta correta
416
Autenticar Novo PA
417
Enviar RESP_AUTENTICAÇÃO_CAM (resposta_tm)
B

FIG. 4B

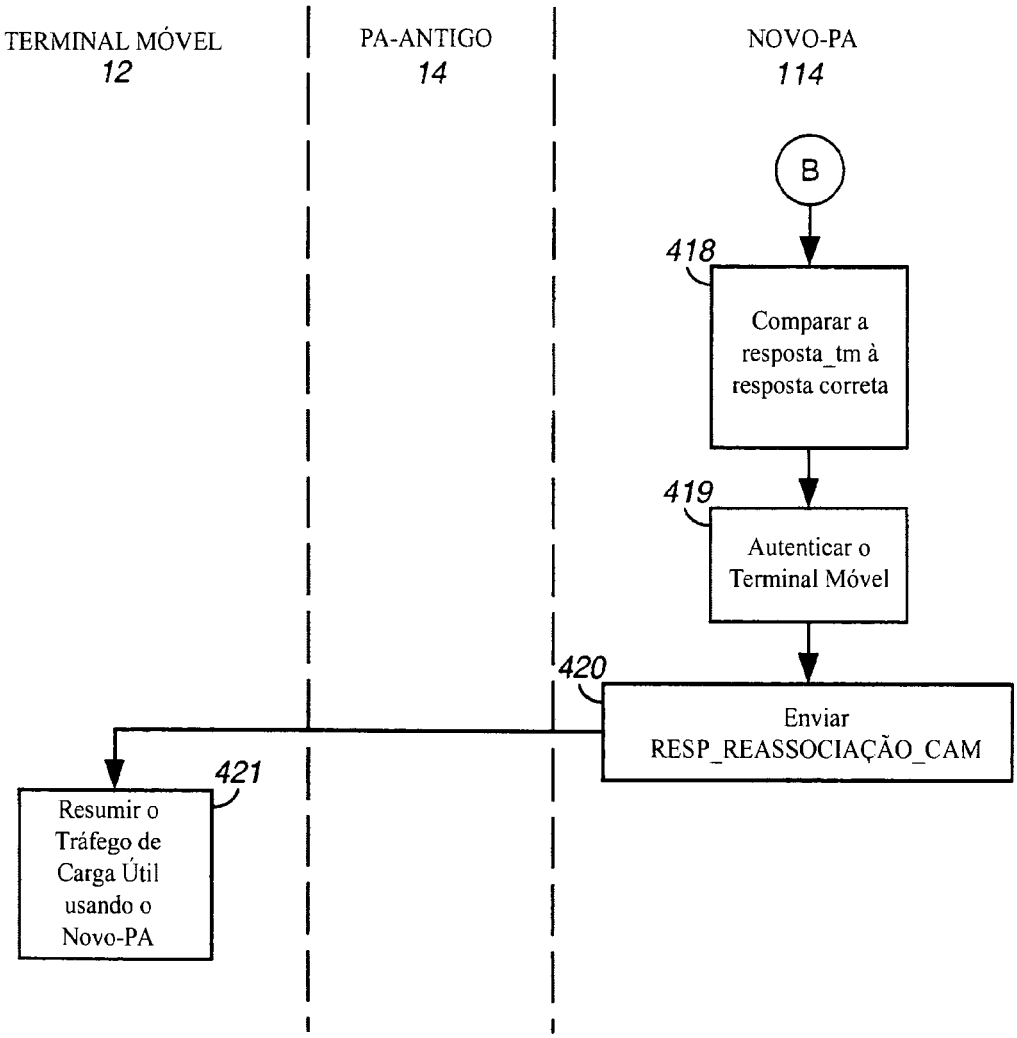
TERMINAL MÓVEL
12
PA-ANTIGO
14
NOVO-PA
114
B
418
Comparar a resposta_tm à resposta correta
419
Autenticar o Terminal Móvel
420
Enviar RESP_REASSOCIAÇÃO_CAM
421
Resumir o Tráfego de Carga Útil usando o Novo-PA

FIG. 4C

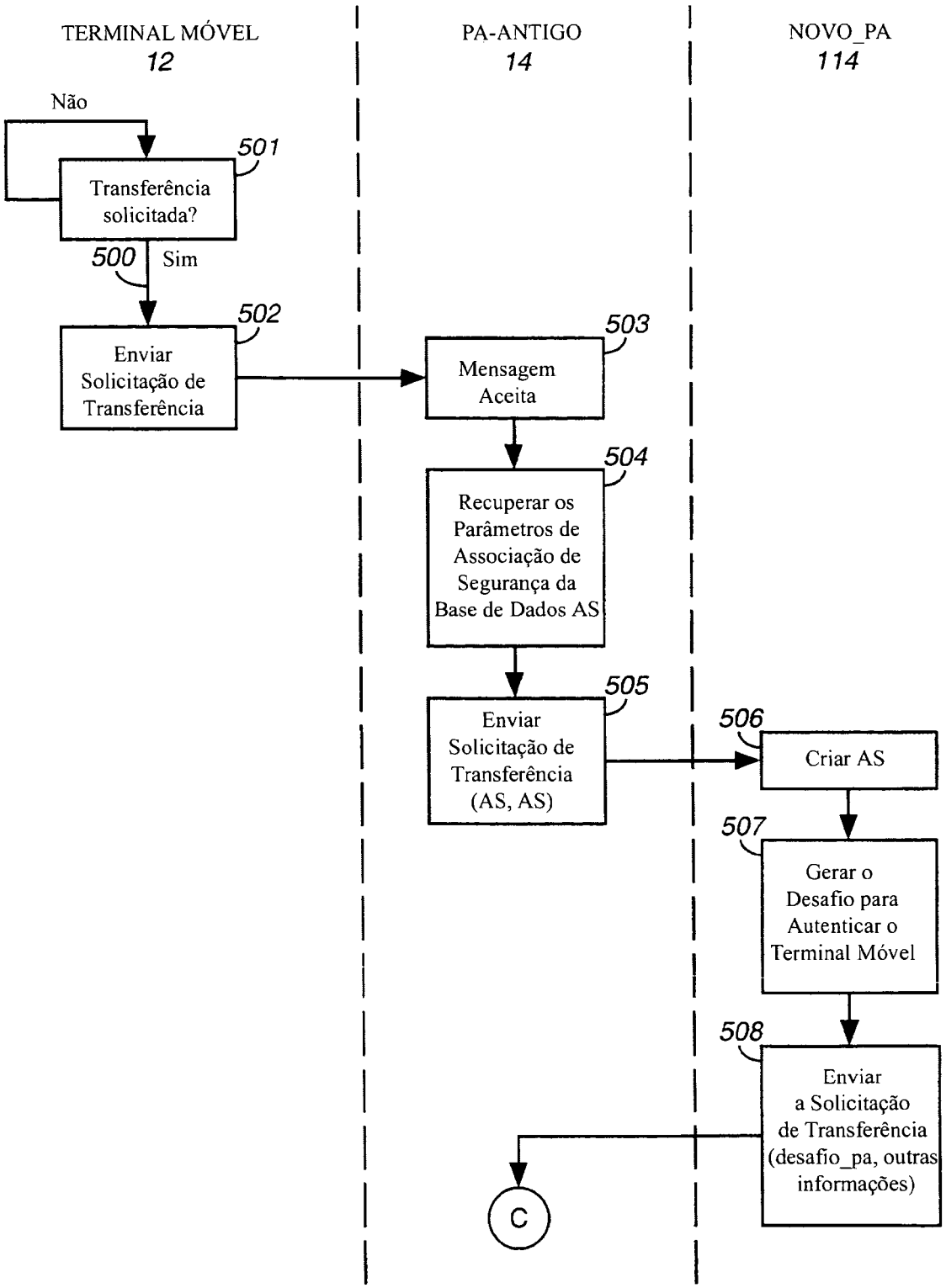
TERMINAL MÓVEL
12
PA-ANTIGO
14
NOVO_PA
114
Não
501
Transferência solicitada?
500
Sim
502
Enviar Solicitação de Transferência
503
Mensagem Aceita
504
Recuperar os Parâmetros de Associação de Segurança da Base de Dados AS
505
Enviar Solicitação de Transferência (AS, AS)
506
Criar AS
507
Gerar o Desafio para Autenticar o Terminal Móvel
508
Enviar a Solicitação de Transferência (desafio_pa, outras informações)
C

FIG. 5A

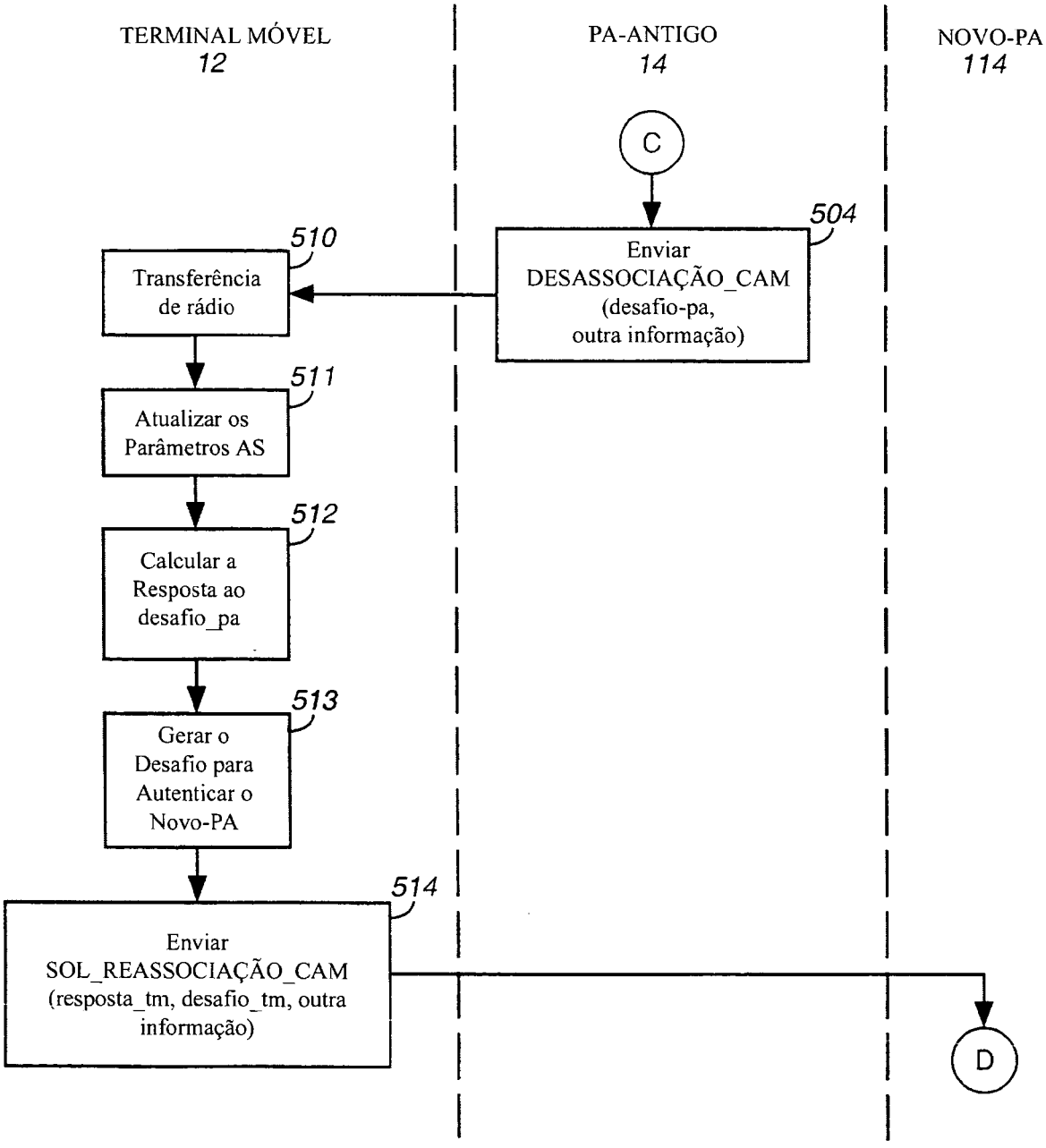
TERMINAL MÓVEL
12
PA-ANTIGO
14
NOVO-PA
114
C
504
Enviar
DESASSOCIAÇÃO_CAM
(desafio-pa,
outra informação)
510
Transferência
de rádio
511
Atualizar os
Parâmetros AS
512
Calcular a
Resposta ao
desafio_pa
513
Gerar o
Desafio para
Autenticar o
Novo-PA
514
Enviar
SOL_REASSOCIAÇÃO_CAM
(resposta_tm, desafio_tm, outra
informação)
D

FIG. 5B

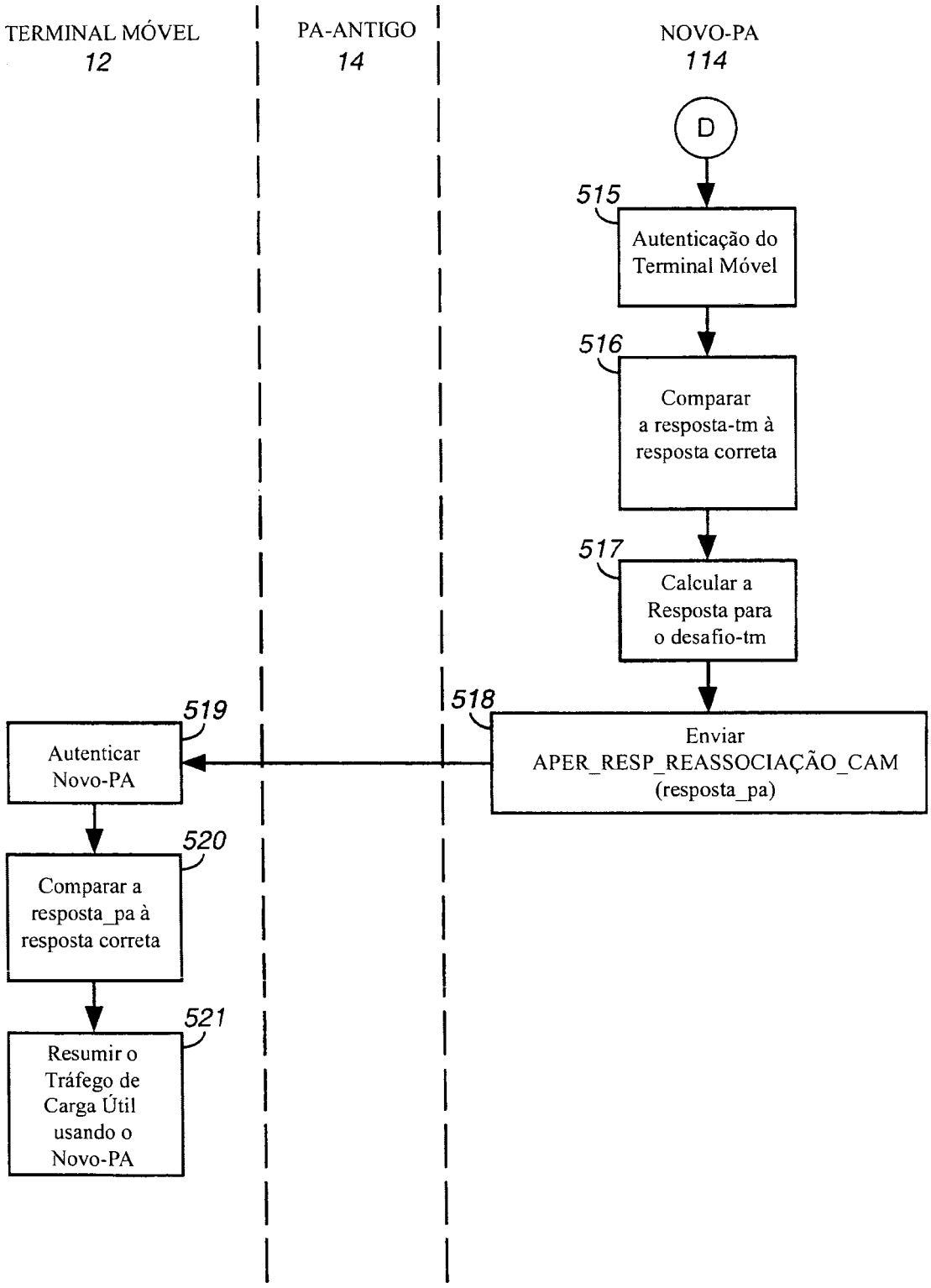
TERMINAL MÓVEL
12
PA-ANTIGO
14
NOVO-PA
114
D
515
Autenticação do Terminal Móvel
516
Comparar a resposta-tm à resposta correta
517
Calcular a Resposta para o desafio-tm
518
Enviar APER_RESP_REASSOCIAÇÃO_CAM (resposta_pa)
519
Autenticar Novo-PA
520
Comparar a resposta_pa à resposta correta
521
Resumir o Tráfego de Carga Útil usando o Novo-PA

FIG. 5C

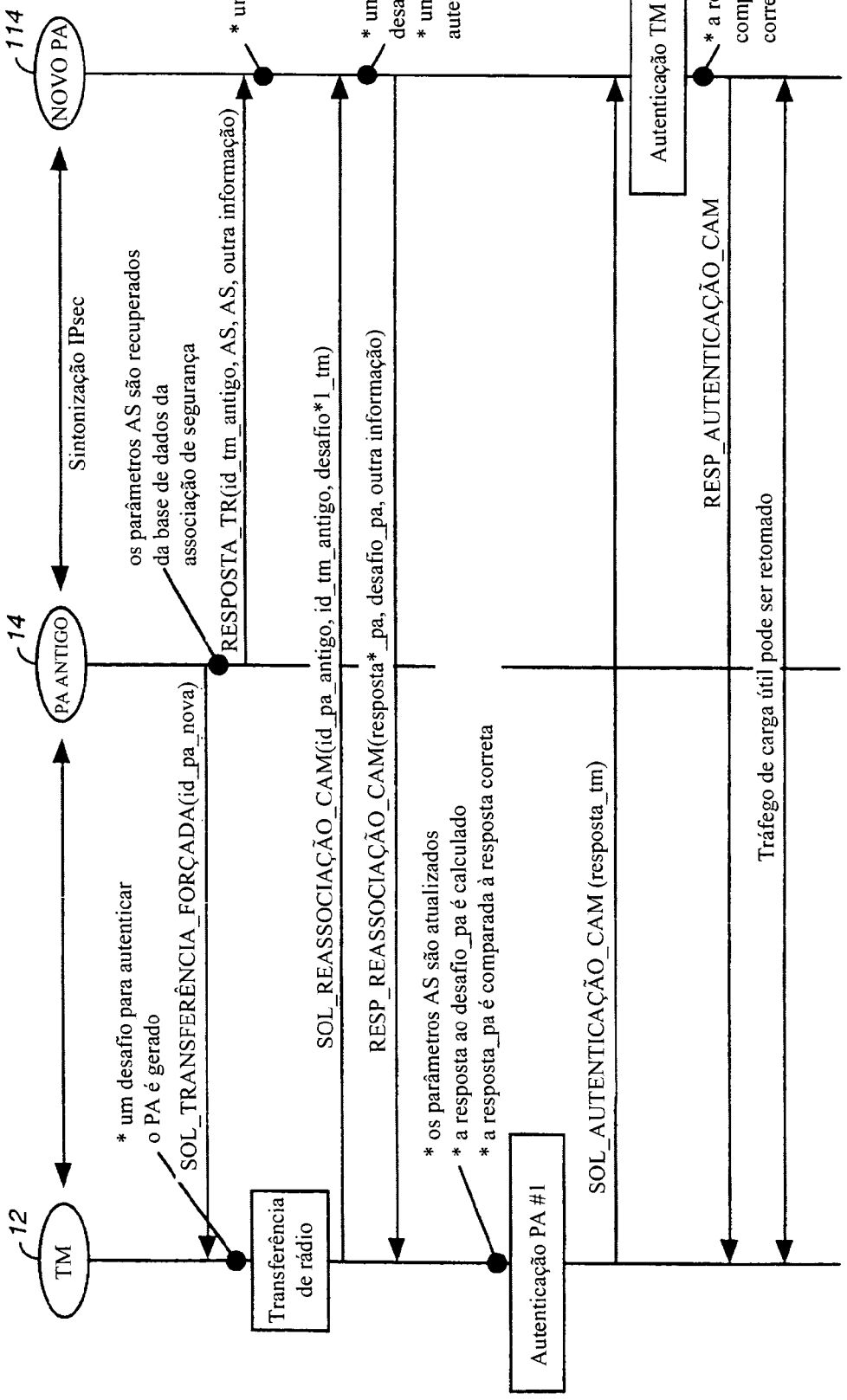
12
TM
14
PA ANTIGO
114
NOVO PA
Sintonização IPsec
* um desafio para autenticar o PA é gerado
SOL_TRANSFERÊNCIA_FORÇADA(id_pa_nova)
os parâmetros AS são recuperados da base de dados da associação de segurança
* uma AS é criada
RESPOSTA_TR(id_tm_antigo, AS, AS, outra informação)
Transferência de rádio
SOL_REASSOCIAÇÃO_CAM(id_pa_antigo, id_tm_antigo, desafio*1_tm)
* uma resposta ao desafio_tm é calculada
* um desafio para autenticar o TM é gerado
RESP_REASSOCIAÇÃO_CAM(resposta*_pa, desafio_pa, outra informação)
* os parâmetros AS são atualizados
* a resposta ao desafio_pa é calculado
* a resposta_pa é comparada à resposta correta
Autenticação PA #1
SOL_AUTENTICAÇÃO_CAM (resposta_tm)
Autenticação TM
* a resposta_tm é comparada à resposta correta
RESP_AUTENTICAÇÃO_CAM
Tráfego de carga útil pode ser retomado

FIG. 6

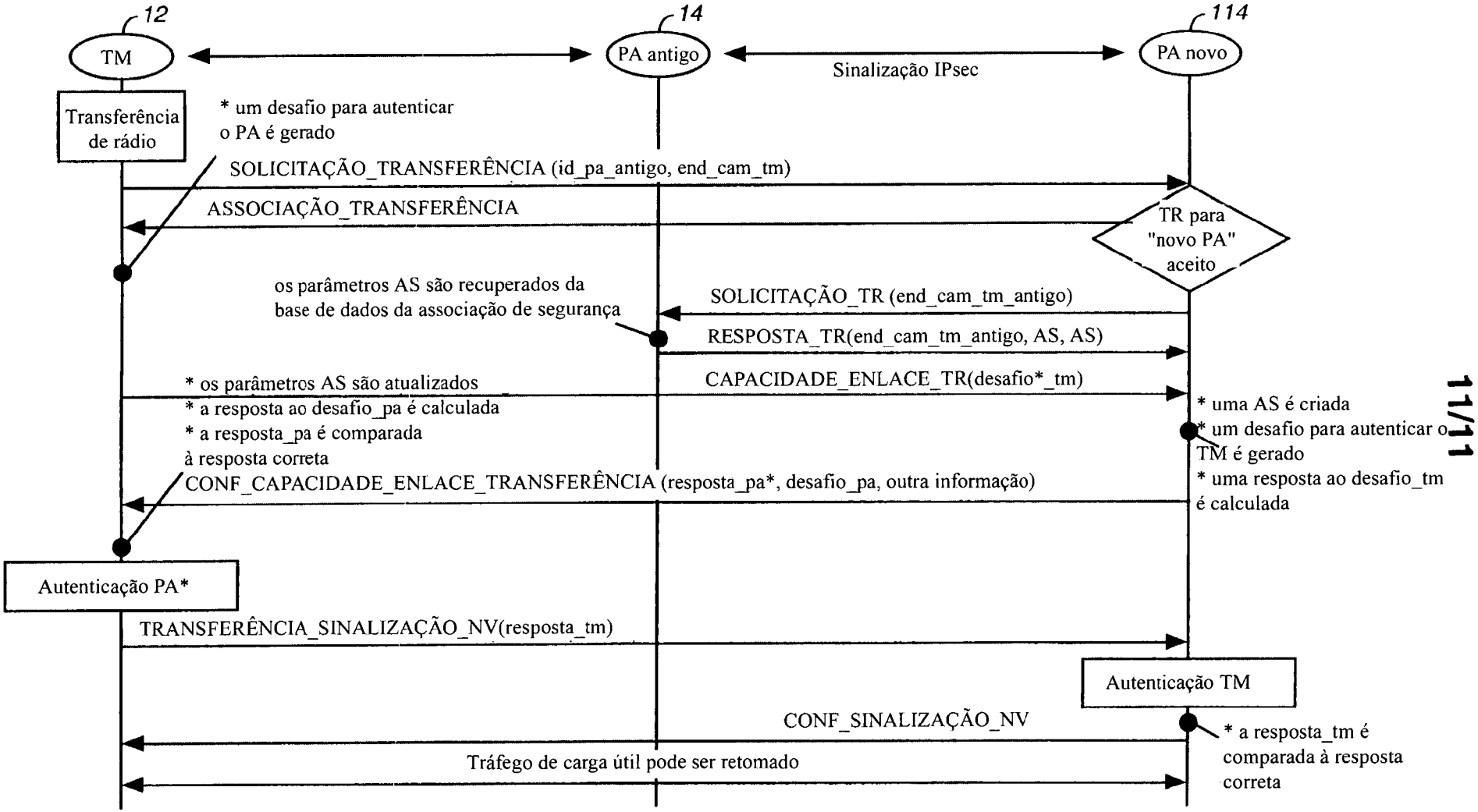
12
TM
14
PA antigo
Sinalização IPsec
114
PA novo
Transferência de rádio
* um desafio para autenticar o PA é gerado
SOLICITAÇÃO_TRANSFERÊNCIA (id_pa_antigo, end_cam_tm)
ASSOCIAÇÃO_TRANSFERÊNCIA
TR para "novo PA" aceito
os parâmetros AS são recuperados da base de dados da associação de segurança
SOLICITAÇÃO_TR (end_cam_tm_antigo)
RESPOSTA_TR(end_cam_tm_antigo, AS, AS)
* os parâmetros AS são atualizados
* a resposta ao desafio_pa é calculada
* a resposta_pa é comparada à resposta correta
CAPACIDADE_ENLACE_TR(desafio*_tm)
* uma AS é criada
* um desafio para autenticar o TM é gerado
* uma resposta ao desafio_tm é calculada
CONF_CAPACIDADE_ENLACE_TRANSFERÊNCIA (resposta_pa*, desafio_pa, outra informação)
Autenticação PA*
TRANSFERÊNCIA_SINALIZAÇÃO_NV(resposta_tm)
Autenticação TM
CONF_SINALIZAÇÃO_NV
* a resposta_tm é comparada à resposta correta
Tráfego de carga útil pode ser retomado

FIG. 7

RESUMO

"MÉTODO E APARELHO PARA RESPECTIVAMENTE FORNECER E MANTER UMA DETERMINADA ASSOCIAÇÃO DE SEGURANÇA DURANTE UMA TRANSFERÊNCIA DO TERMINAL MÓVEL."

Uma associação de segurança existente é re-estabelecida quando um evento de transferência de comunicação ocorre em um sistema de comunicação de rádio, tal como o IEEE 082.11 ou o HIPERLAN, onde a associação de segurança existente entre o terminal móvel e a rede de comunicação sem fio é mantida quando a transferência de comunicação ocorre dentro da rede. A autenticação durante o evento de transferência é alcançada pelo procedimento de desafio/resposta. De acordo com o procedimento de desafio/resposta cada membro de um par de comunicações, que é feito de um novo ponto de acesso e, o terminal móvel que está experimentando uma transferência para um novo ponto de acesso, envia o desafio para o outro membro do par de comunicações. Cada membro do par de comunicações então calcula a resposta para o seu desafio recebido, e estas respostas são enviadas de volta para o outro membro do par de comunicações. Cada membro do par de comunicações então compara a sua resposta recebida à resposta correta. Quando estas comparações estiverem corretas, a comunicação de carga útil começa entre o segundo ponto de acesso e o terminal móvel.