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

(11) PI 0811296-7 B1

(22) Data do Depósito: 07/05/2008

(45) Data de Concessão: 02/06/2020

(54) Título: MÉTODO E EQUIPAMENTO PARA MÚLTIPLAS AUTENTICAÇÕES BASEADAS EM EAP EM UM SISTEMA DE COMUNICAÇÃO SEM FIO E MEMÓRIA LEGÍVEL POR COMPUTADOR

(51) Int.Cl.: H04L 29/06; H04W 12/06.

(52) CPC: H04L 63/06; H04L 63/08; H04L 63/105; H04W 12/06.

(30) Prioridade Unionista: 01/05/2008 US 12/113,860; 07/05/2007 US 60/916,530.

(73) Titular(es): QUALCOMM INCORPORATED.

(72) Inventor(es): RAVINDRA PATWARDHAN; VIDYA NARAYANAN; FATIH ULUPINAR; LAKSHMINATH REDDY DONDETI; PARAG ARUN AGASHE; PEERAPOL TINNAKORNSRISUPHAP; RAYMOND TAH-SHENG HSU; JUN WANG.

(86) Pedido PCT: PCT US2008062966 de 07/05/2008

(87) Publicação PCT: WO 2008/137965 de 13/11/2008

(85) Data do Início da Fase Nacional: 06/11/2009

(57) Resumo: "MÉTODO E EQUIPAMENTO PARA SUPORTE EFICIENTE PARA MÚLTIPLAS AUTENTICAÇÕES" Um método para múltiplas autenticações baseadas em EAP em um sistema de comunicação sem fio é descrito. No método, uma primeira chave de sessão mestre (MSK) é gerada em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo. Uma primeira chave de sessão temporal (TSK) é gerada a partir da primeira chave de sessão mestre (MSK) . Uma segunda autenticação baseada em EAP é realizada, utilizando a primeira chave de sessão temporal (TSK), para um acesso de segundo tipo. O acesso de primeiro tipo e o acesso de segundo tipo são providos após as primeira e segunda autenticações baseadas em EAP serem concluídas com sucesso.

"MÉTODO E EQUIPAMENTO PARA MÚLTIPLAS AUTENTICAÇÕES BASEADAS EM EAP EM UM SISTEMA DE COMUNICAÇÃO SEM FIO E MEMÓRIA LEGÍVEL POR COMPUTADOR"

FUNDAMENTOS

CAMPO

[0001] A presente invenção refere-se de maneira geral a comunicações sem fio e, mais especificamente, a múltiplas autenticações.

FUNDAMENTOS

[0002] Os sistemas de comunicação sem fio são amplamente desenvolvidos para prover diversos tipos de conteúdo de comunicação tais como voz, dados e etc. Estes sistemas podem ser sistemas de acesso múltiplo capazes de suportar comunicação com múltiplos usuários pelo compartilhamento de recursos de sistema (por exemplo, largura de banda e potência de transmissão). Os exemplos de tais sistemas de acesso múltiplo incluem sistemas de acesso múltiplo por divisão de código (CDMA), sistemas de acesso múltiplo por divisão de tempo (TDMA), sistemas de acesso múltiplo por divisão de frequência (FDMA), sistemas 3GPP LTE e sistemas de acesso múltiplo por divisão de frequência ortogonal (OFDMA).

[0003] Geralmente, um sistema de comunicação de acesso múltiplo sem fio pode simultaneamente suportar comunicação para múltiplos terminais sem fio. Cada terminal se comunica com uma ou mais estações base via transmissões nos links direto e reverso. O link direto (ou downlink) se refere ao link de comunicação das estações base para os terminais e o link reverso (ou uplink) se refere a link de comunicação dos terminais para as estações base. Este link

de comunicação pode ser estabelecido pelo sistema de única-entrada e única-saída, múltiplas-entradas e única-saída ou múltiplas-entradas e múltiplas-saídas (MIMO).

SUMÁRIO

[0004] Um aspecto da presente invenção pode residir em um método para múltiplas autenticações baseadas em EAP em um sistema de comunicação sem fio. No método, uma primeira chave de sessão mestre (MSK) é gerada em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo. Uma primeira chave de sessão temporária (TSK) é gerada a partir da primeira chave de sessão mestre (MSK). Uma segunda autenticação baseada em EAP é realizada, com a utilização da primeira chave de sessão temporária (TSK), para um acesso de segundo tipo. O acesso de primeiro tipo e acesso de segundo tipo são providos após a primeira e a segunda autenticações baseadas em EAP serem concluídas com sucesso.

[0005] Em mais aspectos detalhados da invenção, o método pode compreender adicionalmente gerar uma segunda chave de sessão mestre (MSK) na segunda autenticação baseada em EAP. Em adição, o método pode compreender adicionalmente gerar uma segunda chave de sessão temporária (TSK) a partir da segunda chave de sessão mestre (MSK). A segunda chave de sessão temporária (TSK) pode ser utilizada em uma terceira autenticação. Alternativamente, o método pode compreender adicionalmente utilizar a primeira chave de sessão temporária (TSK) para uma terceira autenticação baseada em EAP se uma segunda chave de sessão mestre (MSK) não for gerada na segunda autenticação baseada em EAP. A primeira e a segunda

autenticações baseadas em EAP podem ser parte de uma única sessão.

[0006] Em outros aspectos mais detalhados da invenção, o método pode compreender adicionalmente gerar uma mensagem indicadora para indicar se a primeira e a segunda autenticações baseadas em EAP são concluídas com sucesso. A mensagem indicadora pode possuir um valor de 1 para indicar uma conclusão bem-sucedida das primeira e segunda autenticações baseadas em EAP, e um valor de 0 para indicar que a primeira e a segunda autenticações baseadas em EAP não foram concluídas. A mensagem indicadora pode ser um flag *ValidPMKExists* .

[0007] Além disso, a primeira autenticação baseada em EAP pode incluir uma mensagem de Solicitação/Identidade de EAP que inclui um primeiro tipo de autenticação, e a segunda autenticação baseada em EAP pode incluir uma mensagem de Solicitação/Identidade de EAP que inclui um segundo tipo de autenticação. O método pode compreender adicionalmente gerar uma primeira chave raiz de domínio específico (DSRK) na primeira autenticação baseada em EAP, gerar uma segunda chave raiz de domínio específico (DSRK) na segunda autenticação baseada em EAP, e realizar uma re-autenticação baseada em EAP de pelo menos um dentre o acesso de primeiro tipo ou acesso de segundo tipo utilizando pelo menos uma dentre a primeira DSRK e a segunda DSRK. O acesso de primeiro tipo pode estar associado a um terminal de acesso (AT), e o acesso de segundo tipo pode estar associado a um usuário. Alternativamente, o acesso de primeiro tipo está associado a um dispositivo particular, e o acesso de segundo tipo

está associado a um servidor particular. Ademais, o acesso de primeiro tipo pode compreender o acesso a uma rede via rádio, e o acesso de segundo tipo pode compreender o acesso através de um provedor de serviço de internet (ISP).

[0008] Um outro aspecto da invenção pode residir em um equipamento para múltiplas autenticações baseadas em EAP operável em um sistema de comunicação sem fio, o equipamento compreendendo: meios para gerar uma primeira chave de sessão mestre (MSK) em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo, meios para gerar uma primeira chave de sessão temporária (TSK) a partir da primeira chave de sessão mestre (MSK), meios para realizar de uma segunda autenticação baseada em EAP, utilizando a primeira chave de sessão temporária (TSK), para um acesso de segundo tipo, e meios para prover o acesso de primeiro tipo e do acesso de segundo tipo após as primeira e segunda autenticações baseadas em EAP serem concluídas com sucesso.

[0009] Ainda um outro aspecto da invenção, pode residir um produto de programa de computador compreendendo um meio legível por computador que compreende um código para fazer com que um computador gere uma primeira chave de sessão mestre (MSK) em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo, código para fazer com que um computador gere uma primeira chave de sessão temporária (TSK) a partir da primeira chave de sessão mestre (MSK), código para fazer com que um computador realize uma segunda autenticação baseada em EAP, utilizando a primeira chave de sessão temporária (TSK), para um acesso de segundo tipo e um

código para fazer com que um computador proveja o acesso de primeiro tipo e o acesso de segundo tipo após a primeira e a segunda autenticação baseada em EAP serem concluídas com sucesso.

[0010] Ainda, outro aspecto da invenção pode residir em um equipamento para múltiplas autenticações baseadas em EAP operáveis em um sistema de comunicação sem fio, o equipamento compreendendo um processador, configurado para: gerar uma primeira chave de sessão mestre (MSK) em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo, gerar uma primeira chave de sessão temporária (TSK) a partir da primeira chave de sessão mestre (MSK), realizar uma segunda autenticação baseada em EAP, utilizando a primeira chave de sessão temporária (TSK), para um acesso de segundo tipo, prover acesso de primeiro tipo e acesso de segundo tipo após as primeira e segunda autenticações baseadas em EAP serem concluídas com sucesso, e uma memória acoplada ao processador para armazenar dados.

BREVE DESCRIÇÃO DOS DESENHOS

[0011] As características, natureza e vantagens da presente descrição se tornarão evidentes a partir da descrição detalhada mencionada abaixo quando adotada em conjunto com os desenhos nos quais os caracteres de referência similares se identificam correspondentemente por todo o documento e em que:

[0012] A Figura 1 ilustra um sistema de comunicação de acesso múltiplo sem fio de acordo com uma modalidade;

[0013] A Figura 2 é um diagrama de blocos de um sistema de comunicação;

[0014] A Figura 3 ilustra um exemplo de múltiplas autenticações; e

[0015] A Figura 4 ilustra um exemplo de múltiplas autenticações e utilização de DSRK.

DESCRIÇÃO DETALHADA

[0016] As técnicas descritas no presente documento podem ser utilizadas por diversas redes de comunicação sem fio tais como redes de Acesso Múltiplo por Divisão de Código (CDMA), redes de Acesso múltiplo por Divisão de Tempo (TDMA), redes de Acesso Múltiplo por Divisão de Frequência (FDMA), redes FDMA Ortogonal (OFDMA), redes FDMA de Única Portadora (SC-FDMA), etc. Os termos "redes" e "sistemas" são frequentemente utilizados de modo intercambiável. Uma rede CDMA pode implantar uma tecnologia via rádio tais como Acesso de Rádio Terrestre Universal (UTRA), cdma2000, etc. A UTRA inclui CDMA de banda larga (W-CDMA) e Taxa de Chips Baixa (LCR). A cdma2000 abrange os padrões IS-2000, IS-95 e IS-856. Uma rede TDMA rede pode implantar uma tecnologia via rádio tal como o sistema global para comunicação móvel (GSM). Uma rede OFDMA pode implantar uma tecnologia via rádio tal como UTRA evoluído (E-UTRA), IEEE 802.11, IEEE 802.16, IEEE 802.20, Flash-OFDM, etc. UTRA, E-UTRA e GSM são partes do Sistema Universal de Telecomunicações Móveis (UMTS). A Evolução a Longo Prazo (LTE) é um lançamento iminente de UMTS que usa E-UTRA. UTRA, E-UTRA, GSM, UMTS e LTE descritas nos documentos de uma organização chamada "Projeto de Parceria para a Terceira Geração" (3GPP). A cdma2000 é descrita em

documentos de uma organização chamada "Projeto de Parceria para a Terceira Geração 2" (3GPP2). Estas diversas tecnologias e padrões de rádio são conhecidos na técnica. A título de esclarecimento, certos aspectos das técnicas são descritos abaixo para LTE, e a terminologia LTE é utilizada em grande parte da descrição abaixo.

[0017] O acesso múltiplo por divisão de frequência de única portadora (SC-FDMA), que utiliza modulação com portadora única e equalização de domínio da frequência, é uma técnica. A SC-FDMA possui desempenho similar e, essencialmente, a mesma complexidade total que aquela do sistema OFDMA. O sinal de SC-FDMA possui uma relação potência pico/média (PAPR) mais baixa devido a sua estrutura de única portadora inerente. A SC-FDMA tem atraído bastante atenção, especialmente nas comunicações por uplink onde a PAPR mais baixa beneficia amplamente o terminal móvel em termos de eficiência de potência de transmissão. Isto é atualmente uma concepção de trabalho para o esquema de acesso múltiplo por uplink em Evolução a Longo Prazo 3GPP (LTE) ou UTRA evoluído.

[0018] Com referência à Figura 1, é ilustrado um sistema de comunicação de acesso múltiplo sem fio de acordo com uma modalidade. Um ponto de acesso 100 (AP) inclui múltiplos grupos de antenas, um inclui 104 e 106, outro inclui 108 e 110 e um adicional inclui 112 e 114. Na Figura 1, somente duas antenas são mostradas para cada grupo de antenas, entretanto, mais ou menos antenas podem ser utilizadas para cada grupo de antenas. O terminal de acesso 116 (AT) está em comunicação com as antenas 112 e 114, onde as antenas 112 e 114 transmitem informações para

o terminal de acesso 116 sobre o link direto 120 e recebem informações a partir do terminal de acesso 116 sobre o link reverso 118. O terminal de acesso 122 está em comunicação com as antenas 106 e 108, onde as antenas 106 e 108 transmitem informações para o terminal de acesso 122 sobre o link direto 126 e recebem informações do terminal de acesso 122 sobre o link reverso 124. Em um sistema de duplexação por divisão de frequência (FDD), os links de comunicação 118, 120, 124 e 126 podem utilizar uma frequência diferente para comunicação. Por exemplo, o link direto 120 pode utilizar uma frequência diferente da utilizada pelo link reverso 118.

[0019] Um ponto de acesso pode ser uma estação fixa utilizada para se comunicar com os terminais e pode também ser chamada de um ponto de acesso, Nó B ou alguma outra terminologia. Um terminal de acesso (AT) pode também ser chamado de terminal de acesso, equipamento de usuário (UE), dispositivo de comunicação sem fio, terminal, terminal de acesso ou alguma outra terminologia.

[0020] A autenticação de um dispositivo, por exemplo, um terminal de acesso, assegura que somente os dispositivos, usuários e etc. autorizados possuem acesso a uma rede particular. A autenticação pode se referir à autenticação do dispositivo, autenticação de serviço, etc. Em um exemplo, múltiplas autenticações podem ser requeridas para uma sessão particular. Por exemplo, isto pode ser requerido para autenticar tanto um dispositivo como um servidor para rede acesso em um setor. Múltiplas autenticações podem ser requeridas, por exemplo, quando o AT necessita realizar a autenticação de acesso a um

provedor de acesso à rede via rádio e a autenticação de ISP para o provedor de rede de IP. Em outro exemplo, as autenticações de dispositivo e usuário podem ser realizadas. Os exemplos aqui descritos reduzem a possibilidade de um terminal de acesso obter acesso sem realizar todas as autenticações.

[0021] Em um exemplo, quando múltiplas autenticações são requeridas, por exemplo, duas, uma primeira chave pode ser gerada e utilizada para codificação e decodificação, uma segunda chave pode, então, ser gerada, utilizada para codificar/decodificar e, então, as chaves podem ser combinadas. Em outro exemplo, a autenticação serial pode ser realizada. Na autenticação serial, uma primeira chave pode ser gerada na primeira autenticação, e, então, a segunda autenticação pode ser realizada com a utilização da chave gerada na primeira autenticação. Neste exemplo, não se requer a combinação de chaves, e isto pode levar a uma implantação de autenticação mais simples em sistemas de comunicação.

[0022] As múltiplas autenticações podem estar mutuamente vinculadas onde uma chave de sessão temporária (TSK) da última autenticação protege as autenticações subsequentes. Por exemplo, uma TSK gerada em uma primeira autenticação pode ser requerida em uma segunda autenticação. Em outro exemplo, no caso de re-autenticação, poderá ser necessária somente uma única autenticação.

[0023] Os exemplos aqui descritos provêm suporte à autenticação múltipla. Em um exemplo, pode ser requerida a vinculação das autenticações para segurança. No presente contexto, os nós ou autenticadores de acesso devem

permitir que o AT obtenha serviço somente após todas as autenticações terem sido concluídas com sucesso. Em outro exemplo, a re-autenticação eficiente é provida sendo que múltiplas autenticações não precisam ser repetidas.

[0024] A Figura 3 ilustra um exemplo de múltiplas autenticações que são executadas (run) uma após a outra. Conforme ilustrado, a troca de EAP inicial é feita claramente, para Solicitação/Identidade de EAP (Tipo-Autenticação). Subsequentemente, uma sessão é assegurada. Na Figura 3, a primeira autenticação deve ser geradora de chave. Em outras palavras, isto é obrigatório para gerar uma chave de sessão mestre (MSK), aqui, "MSK1". Subsequentemente, um protocolo de troca de chave (KEP) gera uma chave de sessão temporária (TSK), por exemplo, TSK1 da MSK, conforme ilustrado, MSK1. A TSK derivada após a primeira autenticação protege a segunda autenticação de EAP. Se duas ou mais autenticações foram geradoras de chave, a última MSK se torna a MSK atual. Em um exemplo, uma segunda autenticação pode ou não gerar uma segunda MSK. Se uma segunda MSK for gerada na segunda autenticação, o KEP utiliza a segunda MSK para gerar uma segunda TSK, por exemplo, TSK2. A segunda TSK pode, então, ser utilizada para a proteção de mensagens subsequentes (dados gerados). Se uma segunda MSK não for gerada na segunda autenticação, a TSK gerada anteriormente, por exemplo, TSK1 ainda pode ser utilizada.

[0025] Continuando com o exemplo da Figura 3, o controlador de rede via rádio de serviço (S-RNC) força o KEP com a utilização da MSK atual. O S-RNC usa o flag *ValidPMKExists* para indicar a outros membros de conjunto

ativo se ambas autenticações estão concluídas ou não. Os novos membros de conjunto ativo aguardam pela atualização da sessão com o flag *ValidPMKExists* ligado antes de executar o ERP (protocolo de re-autenticação de EAP) e/ou KEP (protocolo de troca de chave por interface aérea). O flag *ValidPMKExists* pode alternar entre 1 e 0, sendo que 1 indica que ambas as sessões estão concluídas e 0 representa que elas ainda não estão concluídas. Uma sessão pode compreender diversas autenticações. Por exemplo, uma terceira autenticação pode ser requerida. No presente contexto, uma terceira MSK pode ser gerada e utilizada pelo KEP para derivar uma terceira TSK. Se uma terceira MSK não for gerada na terceira autenticação, uma TSK anterior pode ser utilizada, por exemplo, TSK2, $TSK_{anterior}$, etc.

[0026] Os novos membros de conjunto ativo podem executar o ERP, porém podem, então, aguardar para executar o KEP até depois que o flag *ValidPMKExists* estiver ligado. Em um exemplo, se somente um dos métodos de EAP for gerador de chave, uma troca de ERP pode ser permitida para outra eBS para conceber a utilização da DSRK estabelecida pelo primeiro método de EAP. Entretanto, até que o AT finalize todas as autenticações necessárias, o AT pode não ser permitido a acessar a rede. Portanto, a troca de KEP pode ser atrasada até então. Em outro exemplo, se mais de um método de EAP for gerador de chave, o ERP também é operado utilizando a última DSRK produzida.

[0027] A Figura 4 ilustra um exemplo de múltiplas autenticações e utilização da chave raiz de domínio específico (DSRK). A DSRK pode ser utilizada para re-autenticação. Conforme ilustrado, a DSRK da última troca

de EAP pode ser utilizada para re-autenticação. O AAA-L não pode correlacionar as DSRKs e armazena ambas. Espera-se que o AT utilize a DSRK correta.

[0028] Em outro aspecto, um AT com mau comportamento finaliza a primeira autenticação com o S-RNC. Isto também pode adicionar um AN ao conjunto ativo. No presente contexto, isto pode obter a sessão com MSK1' do S-RNC ou realizar ERP com DSRK1. O AAA-L não sabe se um AT finalizou múltiplas autenticações.

[0029] A redução pode ser no nível de interface aérea ou através de servidores de rede backend. No nível de interface aérea, o S-RNC espera que o AT finalize o número esperado de autenticações. O S-RNC pode proporcionar uma sessão para um novo AN, porém na sessão há um flag *ValidPMKExists* que irá indicar que a PMK ainda não foi estabelecida. O S-RNC pode proporcionar uma sessão para qualquer AN, uma vez que *getsession* não pode conter um cookie de segurança antes do EAP ser concluído. No presente, o S-RNC irá se assegurar de que a sessão é atualizada após o EAP (um ou múltiplos) ser concluído. O novo AN irá esperar por outra atualização de sessão com este valor do flag alternado antes de realizar o ERP (Opcional) e o KEP. Adicionalmente, o novo AN não irá permitir a transferência de dados antes de a TSK estar estabelecida.

[0030] Através dos servidores de rede backend, o S-RNC espera que o AT finalize o número de autenticações esperado. Se o AT finalizar menos que o número esperado de autenticações, o S-RNC pode fechar a sessão ou enviar uma notificação ao AAA-L que detém a DSRK. No presente

contexto, o AAA-L envia uma notificação para quaisquer ANs que possam ter derivado rMSK da DSRK. Os ANs fecham, então, a sessão não autorizada com o AT.

[0031] Como referência novamente à Figura 1, cada grupo de antenas e/ou área na qual elas são projetadas para se comunicarem é frequentemente chamado de setor do ponto de acesso. Na modalidade, cada um dos grupos de antena é projetado para se comunicar com o terminal de acessos em um setor das áreas cobertas pelo ponto de acesso 100.

[0032] A Figura 2 é um diagrama de blocos de uma modalidade de um sistema transmissor 210 (também conhecido como ponto de acesso) e um sistema receptor 250 (também conhecido como terminal de acesso) em um sistema MIMO 200. No sistema transmissor 210, os dados de tráfego para um número de fluxos de dados é provido a partir de uma fonte de dados 212 para um processador de dados de transmissão (TX) 214.

[0033] Em uma modalidade, cada fluxo de dados é transmitido por uma respectiva antena de transmissão. O processador de dados TX 214 formata, codifica e intercala os dados de tráfego para cada fluxo de dados com base em um esquema de codificação particular selecionado para que o fluxo de dados proveja dados codificados.

[0034] Os dados codificados para cada fluxo de dados podem ser multiplexados com dados piloto utilizando técnicas de OFDM. Os dados piloto são tipicamente um padrão de dados conhecido que é processado por uma maneira conhecida e pode ser utilizado no sistema receptor para estimar a resposta de canal. Os dados codificados e piloto

multiplexados para cada fluxo de dados são, então, modulados (isto é, mapeados por símbolo) com base em um esquema de modulação particular (por exemplo, BPSK, QSPK, M-PSK ou M-QAM) selecionado para que o fluxo de dados proveja símbolos de modulação. A taxa de dados, codificação e modulação para cada fluxo de dados podem ser determinadas por instruções realizadas pelo processador 230.

[0035] Os símbolos de modulação para todos os fluxos de dados são, então, providos para um processador MIMO TX 220, que pode processar adicionalmente os símbolos de modulação (por exemplo, para OFDM). O processador MIMO TX 220 fornece, então, N_T fluxos de símbolo de modulação para N_T transmissores (TMTR) 222a a 222t. Em certas modalidades, o processador MIMO TX 220 aplica ponderações de conformação de feixe aos símbolos dos fluxos de dados e à antena a partir de qual o símbolo está sendo transmitido.

[0036] Cada transmissor 222 recebe e processa um respectivo fluxo de símbolos para prover um ou mais sinais analógicos e ainda condiciona (por exemplo, amplifica, filtra e converte ascendentemente) os sinais analógicos para prover um sinal modulado adequado para transmissão pelo canal MIMO. Os N_T sinais modulados dos transmissores 222a a 222t são, então, transmitidos a partir de N_T antenas 224a a 224t, respectivamente.

[0037] No sistema receptor 250, os sinais modulados transmitidos são recebidos por N_R antenas 252a a 252r e o sinal recebido de cada antena 252 é provido para um respectivo receptor (RCVR) 254a a 254r. Cada receptor 254 condiciona (por exemplo, filtra, amplifica e converte descendentemente) um respectivo sinal recebido, digitaliza

o sinal condicionado para prover amostras e processa adicionalmente as amostras para prover um fluxo de símbolos "recebido" correspondente.

[0038] Um processador de dados RX 260 recebe e processa, então, os N_R fluxos de símbolos recebidos dos N_R receptores 254 com base em uma técnica de processamento de receptor particular para prover N_T fluxos de símbolos "detectados". O processador de dados RX 260 demodula, deintercala e decodifica, então, cada fluxo de símbolos detectados para recuperar os dados de tráfego para os fluxos de dados. O processamento pelo processador de dados RX 260 é complementar ao realizado pelo processador MIMO TX 220 e pelo processador de dados TX 214 no sistema transmissor 210.

[0039] Um processador 270 determina periodicamente qual matriz de pré-codificação utilizar (discutida abaixo). O processador 270 formula uma mensagem de link reverso que compreende uma porção do índice de matriz e uma porção do valor de classificação.

[0040] A mensagem de link reverso pode compreender diversos tipos de informações relacionadas ao link de comunicação e/ou ao fluxo de dados recebido. A mensagem de link reverso é, então, processada por um processador de dados TX 238, que também recebe os dados de tráfego para um número de fluxos de dados de uma fonte de dados 236, modulada por um modulador 280, condicionada por transmissores 254a a 254r e transmitida de volta ao sistema transmissor 210.

[0041] No sistema transmissor 210, os sinais modulados do sistema receptor 250 são recebidos por antenas

224, condicionados por receptores 222, demodulados por um demodulador 240 e processados por um processador de dados RX 242 para extrair a mensagem de link reverso transmitida pelo sistema receptor 250. O processador 230 determina, então, qual matriz de pré-codificação utilizar para determinar os pesos de conformação de feixe e, então, processar a mensagem extraída.

[0042] Entende-se que a ordem ou hierarquia específica das etapas nos processos descritos é um exemplo de abordagens exemplificativas. Com base nas preferências de projetado, deve ficar entendido que a ordem ou hierarquia específica das etapas nos processos podem ser reorganizadas, enquanto permanecem incluídas no escopo da presente descrição. O método em anexo reivindica os elementos presentes nas diversas etapas em uma ordem de amostra e não se limita à ordem ou hierarquia específica apresentada.

[0043] Aqueles versados na técnica entenderão que as informações e sinais podem ser representados utilizando-se qualquer uma dentre uma variedade de tecnologias e técnicas diferentes. Por exemplo, dados, instruções, comandos, informações, sinais, bits, símbolos e chips que possam ter sido mencionados por toda a descrição acima podem ser representados por voltagens, correntes, ondas eletromagnéticas, campos ou partículas magnéticas, campos ou partículas ópticas ou qualquer combinação destes.

[0044] Os versados na técnica irão ainda observar que diversas etapas de blocos, módulos, circuitos e algoritmos lógicos ilustrativas aqui descritas em conjunto com as modalidades descritas podem ser implantadas

como hardware eletrônico, software de computador ou combinações de ambos. Para ilustrar claramente esta intercambialidade de hardware e software, diversos componentes, blocos, módulos, circuitos e etapas ilustrativos foram descritos acima geralmente em termos de funcionalidade. Se tal funcionalidade for implementada como hardware ou software depende das restrições de aplicação e projeto específicos impostas pelo sistema como um todo. Os versados podem implantar a funcionalidade descrita de várias maneiras para cada aplicação particular, porém tais decisões de implantação não devem ser interpretadas como ocasionadoras de um afastamento do escopo da presente descrição.

[0045] Os diversos blocos, módulos e circuitos lógicos ilustrativos descritos em conjunto com as modalidades aqui descritas podem ser implantados ou realizados com um processador de aplicação geral, um processador de sinal digital (DSP), um circuito integrado de aplicação específica (ASIC), um arranjo de porta programável em campo (FPGA) ou outro dispositivo lógico programável, porta discreta ou transistor lógico, componentes de hardware discreto ou qualquer combinação destes projetada para realizar as funções aqui descritas. Um processador de propósito geral pode ser um microprocessador, mas, alternativamente, o processador pode ser qualquer processador, controlador, microcontrolador ou máquina de estado convencionais. Um processador também pode ser implantado como uma combinação de dispositivos computacionais, por exemplo, uma combinação de um DSP e um microprocessador, uma pluralidade de microprocessadores, um

ou mais microprocessadores em conjunto com um núcleo DSP ou qualquer outra configuração.

[0046] Em uma ou mais modalidades exemplificativas, as funções descritas podem ser implantadas em hardware, software, firmware ou qualquer combinação destes. Se implantadas em software, as funções podem ser armazenadas ou transmitidas por uma ou mais instruções ou códigos em um meio legível por computador. Os meios legíveis por computador incluem tanto meios de armazenamento como meios de comunicação de computador que incluem qualquer meio que facilita a transferência de um programa de computador de um local para outro. Um meio de armazenamento pode ser qualquer meio disponível que pode ser acessado por um computador. Por meio de exemplo, e sem limitação, tal meio legível por computador pode compreender RAM, ROM, EEPROM, CD-ROM ou outro armazenamento em disco óptico, armazenamento em disco magnético ou outro dispositivo de armazenamento magnético, ou qualquer outro meio que possa ser usado para portar ou armazenar o código de programa desejado na forma de estrutura de instruções ou dados e que possa ser acessado por um computador. Em adição, qualquer conexão é designada apropriadamente pelo meio legível por computador. Por exemplo, se o software for transmitido de um website, servidor ou outra fonte remota utilizando um cabo coaxial, cabo de fibra óptica, par trançado, linha digital de assinantes (DSL) ou tecnologias sem fio tais como infravermelho, rádio e microondas, então, o cabo coaxial, cabo de fibra óptica, par trançado, linha digital de assinantes (DSL) ou tecnologias sem fio tais como infravermelho, rádio e microondas estão incluídos na

definição de meio. Disquete ou disco, conforme aqui utilizado, inclui disco compacto (CD), disco a laser, disco óptico, disco versátil digital (DVD), disquete e disco blu-ray onde os disquetes usualmente reproduzem os dados magneticamente, enquanto os discos reproduzem os dados opticamente com lasers. As combinações das considerações acima devem também estar incluídas no escopo do meio legível por computador.

[0047] As etapas de um método ou algoritmo descrito em conjunto com as modalidades aqui descritas podem ser incorporadas diretamente em hardware, em um módulo de software executado por um processador ou em uma combinação dos dois. Um módulo de software pode estar presente em uma memória RAM, memória flash, memória ROM, memória EPROM, memória EEPROM, registradores, disco rígido, um disco removível, um CD-ROM ou qualquer outra forma de meio de armazenamento conhecida na técnica. Um meio de armazenamento exemplificativo é acoplado ao processador, tal processador pode ler as informações de e gravar as informações no meio de armazenamento. Alternativamente, o meio de armazenamento pode ser integral ao processador. O processador e o meio de armazenamento podem residir em um ASIC. O ASIC pode residir em um terminal do usuário.

[0048] A descrição anterior das modalidades descritas é provida para habilitar que qualquer indivíduo versado na técnica produza ou use a presente descrição. Diversas modificações nestas modalidades estarão prontamente evidentes para os versados na técnica, e os princípios genéricos aqui definidos podem ser aplicados em outras modalidades sem que se afaste do espírito ou do

escopo da descrição. Dessa forma, a presente descrição não se destina a estar limitada às modalidades aqui mostradas, mas está acordada ao escopo mais amplo consistente com princípios e recursos novos aqui descritos.

REIVINDICAÇÕES

1. Método para múltiplas autenticações baseadas em EAP em um sistema de comunicação sem fio, o método caracterizado pelo fato de que compreende:

gerar uma primeira chave de sessão mestre (MSK) em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo;

gerar uma primeira chave de sessão temporária (TSK) a partir da primeira chave de sessão mestre (MSK);

realizar uma segunda autenticação baseada em EAP, utilizando a primeira chave de sessão temporária (TSK), para um acesso de segundo tipo; e

prover acesso de primeiro tipo e acesso de segundo tipo após a primeira e a segunda autenticações baseadas em EAP serem concluídas com sucesso.

2. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que o método compreende adicionalmente gerar uma segunda chave de sessão mestre (MSK) na segunda autenticação baseada em EAP.

3. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 2, caracterizado pelo fato de que o método compreende adicionalmente gerar uma segunda chave de sessão temporária (TSK) a partir da segunda chave de sessão mestre (MSK).

4. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 3, caracterizado pelo fato de que a segunda chave de sessão temporária (TSK) é usada em uma terceira autenticação baseada em EAP.

5. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que o método compreende adicionalmente utilizar a primeira chave de sessão temporária (TSK) para uma terceira autenticação baseada em EAP caso uma segunda chave de sessão mestre (MSK) não seja gerada na segunda autenticação baseada em EAP.

6. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que a primeira e a segunda autenticações baseadas em EAP são parte de uma única sessão.

7. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que o método compreende adicionalmente gerar uma mensagem indicadora para indicar se a primeira e a segunda autenticações baseadas em EAP foram concluídas com sucesso.

8. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 7, caracterizado pelo fato de que a mensagem indicadora possui um valor de 1 para indicar conclusão bem sucedida das primeira e segunda autenticações baseadas em EAP, e um valor de 0 para indicar que as primeira e segunda autenticações baseadas em EAP não foram concluídas.

9. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 8, caracterizado pelo fato de que a mensagem indicadora é um flag *ValidPMKExists* .

10. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que o método compreende adicionalmente gerar uma

mensagem indicadora para indicar se múltiplas autenticações baseadas em EAP foram concluídas com sucesso.

11. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que a primeira autenticação baseada em EAP inclui uma mensagem de Solicitação/Identidade de EAP que inclui um primeiro tipo de autenticação, e a segunda autenticação baseada em EAP inclui uma mensagem de Solicitação/Identidade de EAP que inclui um segundo tipo de autenticação.

12. Método para múltiplas autenticações baseadas em EAP, de acordo com a reivindicação 1, caracterizado pelo fato de que o método compreende adicionalmente:

gerar uma primeira chave raiz de domínio específico (DSRK) na primeira autenticação baseada em EAP;

gerar uma segunda chave raiz de domínio específico (DSRK) na segunda autenticação baseada em EAP;

realizar uma re-autenticação baseada em EAP de pelo menos um dentre o acesso de primeiro tipo ou o acesso de segundo tipo utilizando pelo menos uma entre a primeira DSRK e a segunda DSRK.

13. Equipamento (210, 250) para múltiplas autenticações baseadas em EAP operável em um sistema de comunicação sem fio (200), o equipamento (210, 250) caracterizado pelo fato de que compreende:

meios para gerar uma primeira chave de sessão mestre (MSK) em uma primeira autenticação baseada em EAP para um acesso de primeiro tipo;

meios para gerar uma primeira chave de sessão temporária (TSK) a partir da primeira chave de sessão mestre (MSK);

meios para realizar uma segunda autenticação baseada em EAP, utilizando a primeira chave de sessão temporária (TSK), para um acesso de segundo tipo; e

meios para prover acesso de primeiro tipo e acesso de segundo tipo após a primeira e a segunda autenticações baseadas em EAP serem concluídas com sucesso.

14. Equipamento (210, 250), de acordo com a reivindicação 13, caracterizado pelo fato de que compreende:

um processador (230, 270).

15. Memória legível por computador caracterizada pelo fato de que contém gravado na mesma o método conforme definido em qualquer uma das reivindicações 1 a 12.

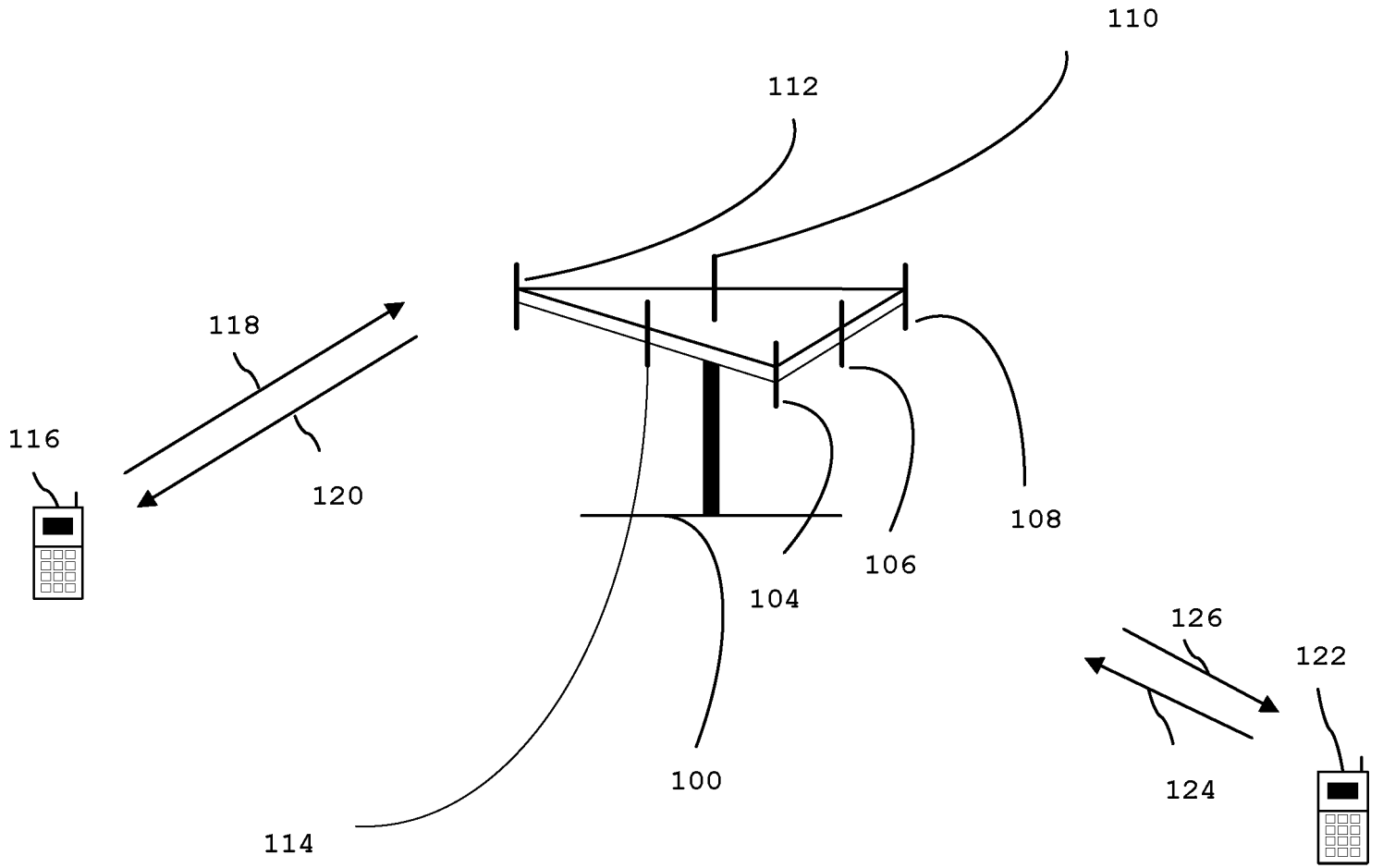

FIGURA 1

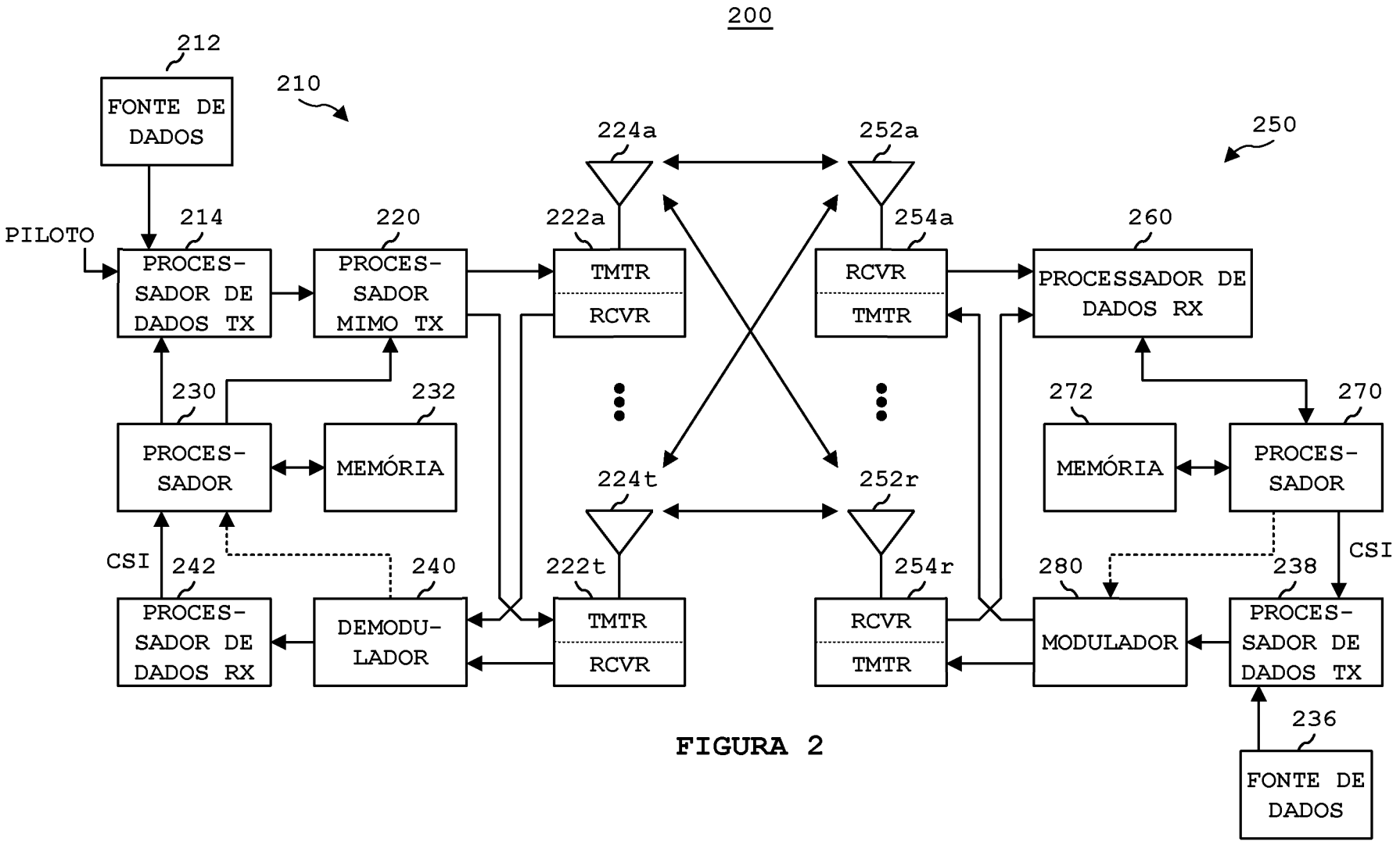
200
212
FONTE DE DADOS
210
250
224a
252a
PILOTO
214
220
222a
254a
260
PROCES-SADOR DE DADOS TX
PROCES-SADOR MIMO TX
TMTR
RCVR
RCVR
TMTR
PROCESSADOR DE DADOS RX
230
232
272
270
PROCES-SADOR
MEMÓRIA
MEMÓRIA
PROCES-SADOR
224t
252r
CSI
242
240
222t
254r
280
238
CSI
PROCES-SADOR DE DADOS RX
DEMODU-LADOR
TMTR
RCVR
RCVR
TMTR
MODULADOR
PROCES-SADOR DE DADOS TX
236
FONTE DE DADOS

FIGURA 2

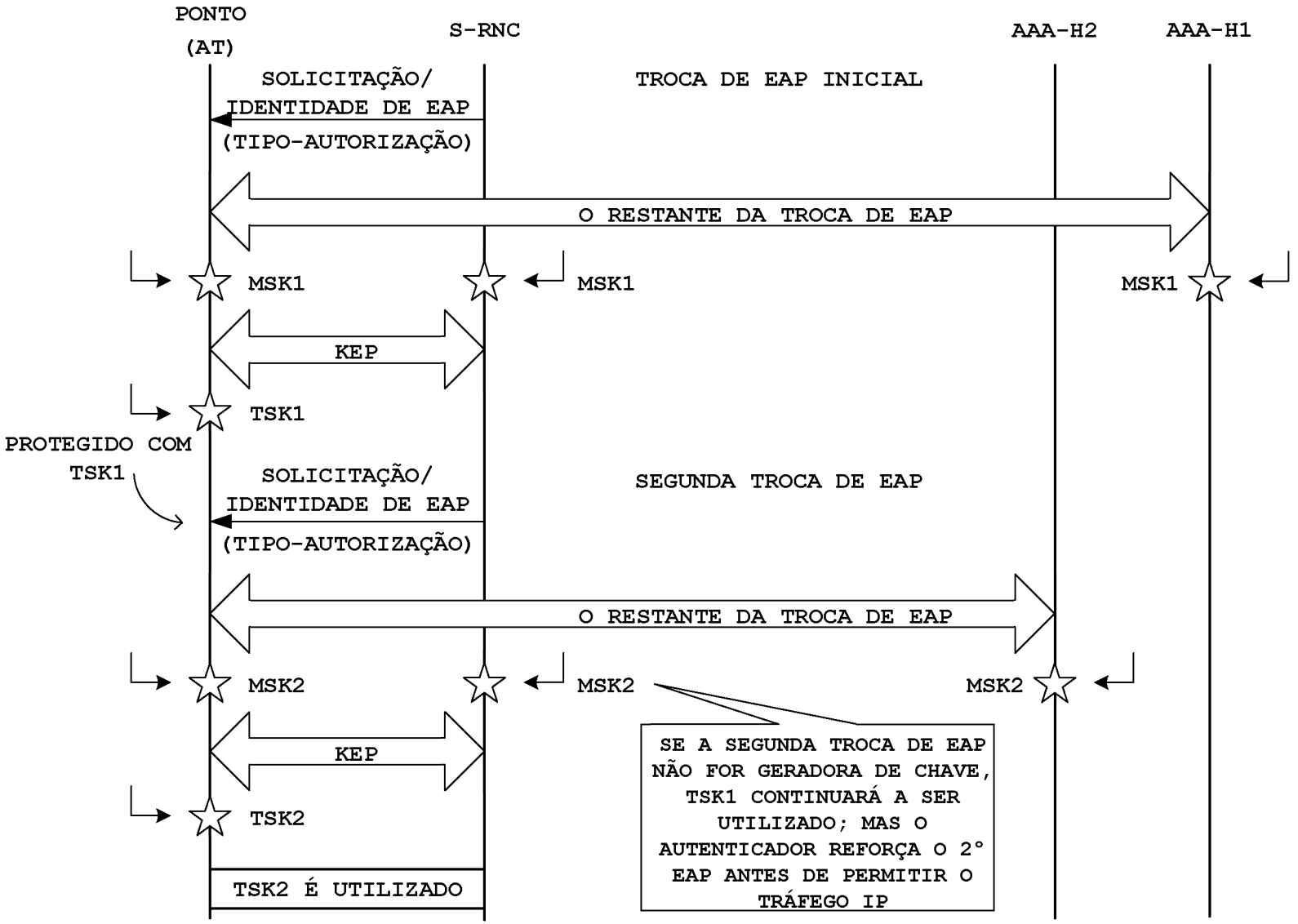
PONTO
(AT)
S-RNC
AAA-H2
AAA-H1
SOLICITAÇÃO/
IDENTIDADE DE EAP
(TIPO-AUTORIZAÇÃO)
TROCA DE EAP INICIAL
O RESTANTE DA TROCA DE EAP
MSK1
MSK1
MSK1
KEP
TSK1
PROTEGIDO COM
TSK1
SOLICITAÇÃO/
IDENTIDADE DE EAP
(TIPO-AUTORIZAÇÃO)
SEGUNDA TROCA DE EAP
O RESTANTE DA TROCA DE EAP
MSK2
MSK2
MSK2
KEP
TSK2
TSK2 É UTILIZADO
SE A SEGUNDA TROCA DE EAP NÃO FOR GERADORA DE CHAVE, TSK1 CONTINUARÁ A SER UTILIZADO; MAS O AUTENTICADOR REFORÇA O 2° EAP ANTES DE PERMITIR O TRÁFEGO IP

FIGURA 3

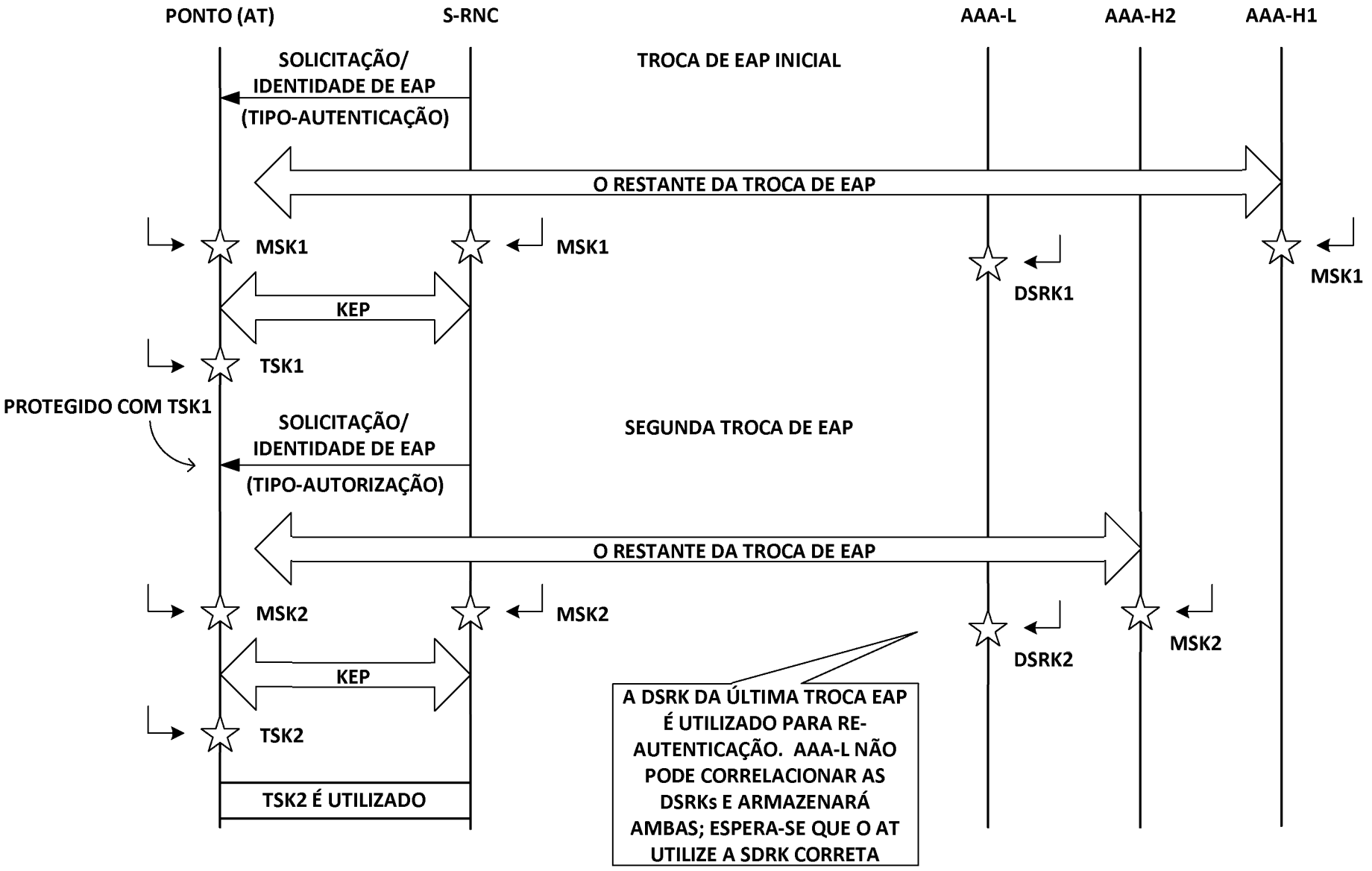
PONTO (AT)
S-RNC
AAA-L
AAA-H2
AAA-H1
SOLICITAÇÃO/
IDENTIDADE DE EAP
(TIPO-AUTENTICAÇÃO)
TROCA DE EAP INICIAL
O RESTANTE DA TROCA DE EAP
MSK1
MSK1
DSRK1
MSK1
KEP
TSK1
PROTEGIDO COM TSK1
SOLICITAÇÃO/
IDENTIDADE DE EAP
(TIPO-AUTORIZAÇÃO)
SEGUNDA TROCA DE EAP
O RESTANTE DA TROCA DE EAP
MSK2
MSK2
DSRK2
MSK2
KEP
TSK2
TSK2 É UTILIZADO
A DSRK DA ÚLTIMA TROCA EAP É UTILIZADO PARA RE-AUTENTICAÇÃO. AAA-L NÃO PODE CORRELACIONAR AS DSRKs E ARMAZENARÁ AMBAS; ESPERA-SE QUE O AT UTILIZE A SDRK CORRETA

FIGURA 4