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

(11) PI 0616347-5 B1

(22) Data do Depósito: 01/08/2006

(45) Data de Concessão: 09/04/2019

(54) Título: MÉTODO DE SINCRONIZAÇÃO DE CONTAGEM DE PROTEÇÃO DE INTEGRIDADE

(51) Int.Cl.: H04W 12/10; H04L 29/06.

(52) CPC: H04W 12/10; H04L 63/12.

(30) Prioridade Unionista: 29/09/2005 US 11/238,503.

(73) Titular(es): GOOGLE TECHNOLOGY HOLDINGS LLC.

(72) Inventor(es): HUI ZHAO; PADMAJA PUTCHA.

(86) Pedido PCT: PCT US2006029943 de 01/08/2006

(87) Publicação PCT: WO 2007/040781 de 12/04/2007

(85) Data do Início da Fase Nacional: 25/03/2008

(57) Resumo: MÉTODO DE SINCRONIZAÇÃO DE CONTAGEM DE PROTEÇÃO DE INTEGRIDADE. O método de sincronização de contagem de proteção de integridade (200) inicia (210) uma nova conexão quando o equipamento do usuário (UE) já está no modo conectado com uma rede. Se novas chaves de segurança estão pendentes, o EU envia (250) um valor START de zero em uma mensagem de transferência direta inicial. Se nenhuma chave de segurança nova estiver pendente, o UE envia (240) um valor START não zero com base em um Universal Subscriber Interface Module (USIM) . Enviar um valor START de zero quando novas chaves de segurança estão pendentes no EU força o valor de contagem de integridade COUNT-1 da rede a casar com o valor COUNT-1 de zero no UE, que impede a falha no estabelecimento de chamada devido à incapacidade de passar uma verificação de segurança de proteção de integridade.

MÉTODO DE SINCRONIZAÇÃO DE CONTAGEM DE PROTEÇÃO DE INTEGRIDADE

Campo Da Revelação

Esta revelação relaciona-se genericamente à comunicação por radiotelefone e, em particular, à verificação de integridade de mensagens de sinalização entre uma estação móvel e uma rede.

Histórico Da Revelação

De acordo com a Especificação Técnica 25,331 do Projeto de Parceria de Terceira Geração (3GPP), o Equipamento do Usuário (UE) pode iniciar uma conexão de sinalização utilizando um procedimento de transferência direta inicial (IDT) que inclui calcular um valor START para um procedimento de comando no modo de segurança. Este valor START é enviado do UE para sua rede de comunicação, e a rede utiliza o valor START recebido para inicializar uma variável COUNT-I que é utilizada para proteção de integridade de mensagens entre o UE e a rede.

No entanto, se falhas na conexão causam a liberação da conexão de sinal antes do procedimento de comando do modo de segurança completar, o valor START enviado em um IDT poderá não ser o mesmo que o valor START utilizado no UE, e a verificação de integridade para mensagens poderia falhar. Tentativas subseqüentes de estabelecer uma conexão substituta utilizando o procedimento IDT também falharão devido à incapacidade de sustentar a proteção de integridade.

Há uma oportunidade para o UE compensar pelos erros no casamento COUNT para melhorar as chances de que uma conexão substituta terá sucesso. Os vários aspectos, recursos e

vantagens da revelação tornar-se-ão mais inteiramente aparentes para aqueles dotados de habilidade ordinária na tecnologia quando da cuidadosa consideração dos desenhos seguintes e da descrição detalhada acompanhante.

A publicação do pedido de patente Europeu EP A 1448009 descreve um método para gerenciamento de valores START durante um procedimento Inter-RAT de maneira a prevenir a exclusão de novos conjuntos de chaves. O dispositivo sem fio primeiro completa, de modo bem-sucedido, um procedimento Inter-RAT, que é tanto uma entrega Inter-RAT, quanto uma reseleção de célula Inter-RAT ou uma ordem de mudança de célula Inter-RAT a partir de um procedimento UTRAN. O dispositivo sem fio então determina se um USIM está presente. Se o USIM está presente, o dispositivo sem fio determina se um novo conjunto de chave de segurança foi recebido e não usado para funções de cifragem e integridade durante uma conexão RRC atual. Se um novo conjunto de chaves estiver presente e não ser usado, o dispositivo sem fio armazena um valor 0 no USIM como um valor START de segurança para o domínio CN associado com a conexão RRC.

A publicação do pedido de patente US 2003/0235212 descreve um método para sincronização de um valor START para uma Portadora de Rádio que é criada por um procedimento de setup de Portadora de Rádio iniciado pelo UTRAN e realizado em conjunto com um procedimento de relocação SRNS. A UE recebe uma mensagem de setup de Portadora de Rádio a partir da UTRAN e concede um primeiro valor START para START_VALUE_TO_TRANSMIT variável de acordo com as HFNs de todas as RBs estabelecidas no primeiro domínio. A UE utiliza o START_VALUE_TO_TRANSMIT variável

para estabelecer um HFN da nova Portadora de Rádio.

Descrição Sucinta Dos Desenhos

A Figura 1 mostra um sistema 3GPP simplificado com o Equipamento do Usuário e uma rede de acordo com uma versão.

A Figura 2 mostra um fluxograma de um método de sincronização de contagem para o Equipamento de Usuário mostrado na Figura 1 de acordo com uma versão geral.

A Figura 3 mostra um fluxograma de um método de sincronização de contagem para o Equipamento do Usuário mostrado na Figura 1 de acordo com uma primeira versão detalhada.

A Figura 4 mostra um primeiro diagrama de fluxo de sinal exemplar para o método de sincronização de contagem no sistema 3GPP mostrado na Figura 1 de acordo com a primeira versão detalhada.

A Figura 5 mostra um fluxograma de um método de sincronização de contagem para o Equipamento do Usuário mostrado na Figura 1 de acordo com a segunda versão detalhada.

A Figura 6 mostra um segundo diagrama de fluxo de sinal exemplar para um método de sincronização de contagem no sistema 3GPP mostrado na Figura 1 de acordo com a segunda versão detalhada.

Resumo da Revelação

De acordo com a revelação da invenção, é fornecido um método de sincronização de contagem de proteção de integridade conforme definido nas respectivas reivindicações.

Descrição Detalhada

Um método de sincronização de contagem de proteção de

integridade sincroniza o valor COUNT-I da rede 3GPP com o valor COUNT-I do Equipamento do Usuário 3GPP mesmo quando a conexão de sinalização é liberada após o término bem-sucedido do procedimento de modo de segurança. Este método dá às tentativas de re-conexão uma chance maior de obter sucesso e impede as falhas no estabelecimento de chamadas devido à incapacidade de efetuar a proteção de integridade. Um ponto de decisão com base em se chaves não utilizadas de uma tentativa de conexão anterior estão disponíveis em um UE assegura que os valores COUNT de proteção de integridade para o UE e a rede serão sincronizados.

A Figura 1 mostra um sistema 3GPP simplificado 100 com o Equipamento do Usuário (UE) 180 e uma rede 190 de acordo com uma versão. Nas versões discutidas, um sistema de comunicação sem fio 3GPP é mostrado; no entanto, os princípios revelados poderão ser aplicados a outros tipos de sistemas de comunicação sem fio incluindo versões futuras do sistema 3GPP. O UE 180, às vezes referido como um dispositivo móvel ou uma estação móvel, pode ser um radiotelefone, um laptop com conexão sem fio, um dispositivo de mensagem sem fio, ou outro tipo de dispositivo de comunicação sem fio compatível com a rede 190. O UE 180 tem ou está acoplado a um Universal Subscriber Interface Module (USIM - Módulo de Interface de Assinante Universal) 185.

A rede 190 inclui uma rede cerne comutada por circuito (CS) 196 bem como uma rede cerne comutada por pacote (PS) 198. A rede cerne CS 196 e a rede cerne PS 198 operam independentemente uma da outra. Por exemplo, a rede cerne OS poderá ter uma conexão de chamada estabelecida com o UE

180, e a rede cerne CS poderá iniciar uma conexão de chamada em ocasião posterior que não é coordenada com a conexão da rede cerne PS. A rede cerne CS 196 e a rede cerne PS 198 se juntam em uma entidade Radio network Controller (RNC – Controladora de Rede de Rádio) 194, radio resource control (RRC – Controle de Recurso de Rádio) e radio link control (RLC – Controle de Enlace de Rádio) dentro da rede 190 e assim tanto as mensagens OS como CS são transmitidas através de um enlace de comunicação sem fio 110 para o UE 180. O UE 180 também se comunica com a rede 190 através do enlace de comunicação sem fio 110.

A Figura 2 mostra um fluxograma 200 de um método de sincronização de contagem para o UE 180 mostrado na Figura 1 de acordo com uma versão geral. Na etapa 210, o UE 180 inicia uma nova conexão quando o UE já está em modo conectado com segurança (também denominado de proteção de integridade). Dois cenários são comuns. No primeiro cenário, o UE já está conectado à rede cerne comutada por circuito (CS) 196 mostrada na Figura 1 e está iniciando uma chamada comutada por pacote (PS) na etapa 210. No segundo cenário, o UE já está conectado à rede cerne PS 198 mostrada na Figura 1 e está iniciando uma chamada CS na etapa 210.

Na etapa 230, o UE 180 verifica por chaves pendentes não utilizadas ao verificar uma variável binária PENDING_NEW_KEYS armazenada em uma memória, como a memória de acesso aleatório (RAM) do UE 180. Chaves novas pendentes estão presentes quando um procedimento de autenticação é completado com sucesso entre o UE 180 e a rede 190 para uma conexão particular. A ausência de novas chaves indica que

nenhum procedimento de autenticação entre o UE 180 e a rede 190 foi completado para aquela conexão particular.

Se nenhuma chave estiver pendente, conforme determinado pela etapa 230, o UE 180 transmite uma mensagem Initial Direct Transfer (IDT) tendo um valor START não zero determinado do Universal Subscriber Interface Module (USIM) 185 do UE 180 de acordo com procedimentos EGPP TS 25.331 existentes, e o fluxo termina na etapa 290.

Se novas chaves estão pendentes, conforme determinado pela etapa 230, o UE 180 transmite uma mensagem IDT tendo um valor START de '0'. O valor START zero indica para a rede que seu valor COUNT-I existente deve ser refixado para zero para a conexão recém iniciada. O fluxo então termina na etapa 290.

De acordo com os procedimentos 3GPP TS 25.331 existentes, se novas chaves estão pendentes no UE 180, o valor COUNT-I do UE é refixado para zero. Enviar o valor START de '0' para a rede 190 na etapa 350 força o valor COUNT-I da rede a casar com o valor COUNT-I zero no UE 180. Se um valor START não zero fosse enviado sob essas circunstâncias, então o valor COUNT-I do UE seria zero e o COUNT-I da rede seria não zero, que resultaria em falha no estabelecimento da chamada devido à incapacidade de passar na verificação de proteção de integridade.

A Figura 3 mostra um fluxograma de um método de sincronização de contagem para o Equipamento do Usuário mostrado na Figura 1 de acordo com uma primeira versão detalhada. A Figura 3 é muito semelhante à Figura 2 exceto que a etapa 310 especifica que o UE inicie uma conexão CS quando o UE já está no modo conectado PS com segurança. Um

exemplo de fluxo de sinal deste cenário é mostrado na Figura 4.

A Figura 4 mostra um primeiro diagrama de fluxo de sinal exemplar 400 para o método de sincronização de contagem no sistema 3GPP 100 mostrado na Figura 1 de acordo com a primeira versão detalhada. Neste primeiro exemplo, a liberação da conexão de sinalização CS 470 ocorre após o procedimento de autenticação CS completar com sucesso. Em vez de incluir um valor START não zero, a mensagem de atualização de localização CS 480 do procedimento de transferência direta inicial (IDT) inclui um valor START de 0.

Este primeiro diagrama de fluxo de sinal exemplar 400 mostra três camadas em um UE 480: uma camada de controle de recurso de rádio (RRC) 484, uma camada de gerenciamento de mobilidade (MM) no domínio comutado por circuito 486, e uma camada de gerenciamento de mobilidade GPRS (GMM) no domínio comutado por pacote 488. A camada MM 486 utilizada no domínio CS é análoga à camada GMM 488 no domínio PS; ambas são camadas de gerenciamento de mobilidade.

Três camadas de uma rede 490 também estão mostrados no primeiro diagrama de fluxo de sinal exemplar 400. A rede 490 tem uma camada de controle de recurso de rádio (RRC) 494 que é a contraparte da camada RRC 484 no UE 480. A rede 490 também tem uma rede cerne CS 496 e uma rede cerne PS 498, mostrados na FIG. 1 como rede cerne CS 196 e rede cerne de PS 198. Como foi dito anteriormente, a rede cerne CS 496 e a rede cerne PS 498 operam independentemente uma da outra.

Uma mensagem de atualização de localização CS 420

gerada pela camada MM comutada por circuito 486 dispara o estabelecimento de conexão RRC 410 entre o UE 480 e a rede 490 utilizando várias mensagens. Durante o estabelecimento da conexão RRC 410, o UE 480 envia à rede 490 valores START ($START_{CS}$, $START_{PS}$) do USIM. O valor $START_{CS}$ do UE é utilizado para iniciar o valor COUNT-I_{CS} da rede para a conexão CS, e o valor $START_{PS}$ do UE é utilizado para iniciar o valor COUNT-I_{PS} para a conexão PS. Como foi dito anteriormente, o valor COUNT-I da rede e o valor COUNT-I correspondente no UE são utilizados para efetuar a proteção de integridade quando o UE e a rede estão em modo de segurança.

A seguir, a mensagem de atualização de localização CS 420 gerada pela camada MM comutada por circuito 486 é transmitida da camada RRC 484 do UE 480. A mensagem é recebida na camada RRC 494 da rede 490 e encaminhada para a rede cerne CS 496 para processamento. No lado de comutação por pacote, uma mensagem de solicitação de afixação 430 é gerada na camada GMM 488 comutada por pacote e transmitida da camada RRC 484 do UE 480. A rede 490 recebe a mensagem e a envia da camada RRC 494 para a rede cerne PS 498. A mensagem de atualização de localização CS 420 e a mensagem de solicitação de afixação PS 430 não são coordenadas uma com a outra e podem ocorrer em qualquer seqüência no tempo.

Em resposta à mensagem de solicitação de afixação PS 430, a rede 490 envia uma mensagem de solicitação de autenticação e de cifragem 440. A solicitação de autenticação e de cifragem é gerada pela rede cerne PS 498 e enviada através da camada RRC 494. O UE 480 recebe a mensagem em sua camada RRC 484 e a encaminha para a camada GMM 488 para processamento. Uma vez completado o

processamento, a camada GMM 488 produz uma mensagem de resposta de autenticação e de cifragem 445, que é enviada para a camada RRC 484 para transmissão pelo UE 480. A mensagem 445 é recebida pela camada RRC 494 da rede 490 e passada para o cerne PS 498.

No momento, em resposta à mensagem de atualização de localização 420, a rede cerne CS 496 iniciou uma mensagem de solicitação de autenticação 450. A MM 486 do UE 480 responde com uma mensagem de resposta de autenticação CS 455 para a conexão CS. A mensagem de resposta de autenticação 455 é encaminhada da camada RRC 494 da rede 490 para o cerne CS 496.

Após a mensagem de resposta de autenticação e de cifragem PS 455 ser recebida pelo cerne PS 498 da rede 490, o cerne PS 498 envia uma mensagem de comando de modo de segurança PS 460 para iniciar a proteção de integridade para a conexão PS entre o UE 480 e a rede 490. Quando a camada RRC 484 do UE 480 recebe a mensagem de comando de modo de segurança PS 460 da camada RRC 494 da rede, o UE 480 inicia a proteção de integridade. Quando a iniciação do modo de segurança é completada na camada RRC 484, o UE 480 notifica a rede 490 utilizando a mensagem completada de modo de segurança PS 465 e notifica sua camada GMM comutada por pacote 488 utilizando uma mensagem 467.

Neste ponto, a conexão de sinalização CS é liberada 470 antes do término bem sucedido do procedimento de modo de segurança CS, e as chaves CS permanecem sem uso. Se uma conexão CS for originada novamente, o UE 480 envia uma transferência direta inicial (IDT) ao enviar uma mensagem de atualização de localização 480 que inclui o valor

$START_{CS}$ de 0. O UE 480 utilizará as chaves CS não utilizadas quando um procedimento de modo de segurança CS for iniciado. O valor START zero na mensagem de atualização de localização 480 forçará o valor COUNT-I_{CS} da rede a refixar para zero, que então casará com o valor COUNT-I_{CS} zero no UE 480.

Quando o valor COUNT-I_{CS} da rede e o COUNT-I_{CS} do UE casam, a conexão de substituição CS recém iniciada pode utilizar as chaves de segurança da conexão anterior para estabelecer proteção de integridade e o estabelecimento de chamada não falhará devido à incapacidade de sustentar o modo de segurança.

Sem o fluxograma 300 mostrado na Figura 3, a mensagem de atualização de localização 480 teria incluído o valor $START_{CS}$ do USIM de acordo com procedimentos IDT padrão. O valor $START_{CS}$ do USIM teria sido um valor não zero que teria causado um erro de casamento entre o valor COUNT-I_{CS} da rede e o valor COUNT-I_{CS} do UE, o que teria impedido a chamada da re-conexão de ser bem-sucedida.

A Figura 5 mostra o fluxograma do método de sincronização de contagem para o Equipamento do Usuário mostrado na Figura 1, de acordo com uma segunda versão detalhada. A Figura 5 é muito similar à Figura 2, exceto que a etapa 510 especifica que o UE inicia uma conexão PS quando o UE já está no modo conectado CS com segurança. O exemplo de fluxo de sinal deste cenário é mostrado na Figura 6.

A Figura 6 mostra um segundo diagrama de fluxo de sinal exemplar 600 para o método de sincronização de contagem no sistema 3GPP 100 mostrado na Figura 1 de acordo

com a segunda versão detalhada. Neste segundo exemplo, uma liberação de conexão de sinalização PS 670 ocorre após o procedimento de autenticação PS completa com sucesso. Em vez de incluir um valor START não zero, a mensagem de solicitação de afixação PS 680 do procedimento de transferência direta inicial (IDT) inclui um valor START de 0.

Este segundo diagrama de fluxo de sinal exemplar 600 mostra três camadas no UE 680: uma camada de controle de recurso de rádio (RRC) 684, uma camada de gerenciamento de mobilidade no domínio comutado por circuito (MM) 686, e uma camada de gerenciamento de mobilidade GPRS no domínio comutado por pacote (GMM) 688. A camada MM 686 utilizada no domínio CS é análoga à camada GMM 688 no domínio PS; ambas são camadas de gerenciamento de mobilidade.

Três camadas de uma rede 690 também são mostradas no primeiro diagrama de fluxo de sinal exemplar 600. A rede 690 tem uma camada de controle de recurso de rádio (RRC) 694, que é a contraparte da camada RRC 684 no UE 680. A rede 690 também tem uma rede cerne CS 696 e uma rede cerne PS 698, que são mostradas na Figura 1 como a rede cerne CS 196 e a rede cerne PS 198. Como foi dito anteriormente, a rede cerne CS 696 e a rede cerne PS 698 operam independentemente uma da outra.

Uma mensagem de atualização de localização CS 620 gerada pela camada MM comutada por circuito 686 dispara o estabelecimento de conexão RRC 610 entre o UE 680 e a rede 690 utilizando várias mensagens. Durante o estabelecimento da conexão RRC 610, o UE 680 envia à rede 690 valores START ($START_{CS}$, $START_{PS}$) do USIM. O valor $START_{CS}$ do UE é utilizado

para iniciar o valor COUNT-I_{CS} da rede para a conexão CS, e o valor $START_{PS}$ do UE é utilizado para iniciar o valor COUNT-I_{PS} da rede para a conexão PS. Como foi dito anteriormente, o valor COUNT-I da rede e o valor COUNT-I correspondente no UE são utilizados para efetuar proteção de integridade quando o UE e a rede estão em modo de segurança.

A seguir, a mensagem de atualização de localização CS 620 gerada pela camada MM comutada por circuito 686 é transmitida da camada RRC 684 do UE 680. A mensagem é recebida na camada RRC 694 da rede 690 e encaminhada para a rede cerne CS 696 para processamento. No lado de comutação por pacote, uma mensagem de solicitação de afixação 630 é gerada na camada GMM comutada por pacote 688 e transmitida da camada RRC 684 do UE 680. A rede 690 recebe a mensagem e a envia da camada RRC 694 para a rede cerne PS 698. A mensagem de atualização de localização CS 620 e a mensagem de solicitação de afixação PS 630 não são coordenadas uma com a outra e podem ocorrer em qualquer seqüência no tempo.

Em resposta à mensagem de solicitação de afixação PS 630, a rede 690 envia uma mensagem de solicitação de autenticação e de cifragem 640. A solicitação de autenticação e de cifragem é gerada pela rede cerne PS 698 e enviada através da camada RRC 694. O UE 680 recebe a mensagem em sua camada RRC 684 e a encaminha para a camada GMM 688 para processamento. Uma vez terminado o processamento, a camada GMM 688 produz uma mensagem de resposta de autenticação e de cifragem 645, que é enviada para a camada RRC 684 para transmissão pelo UE 680. A mensagem 645 é recebida pela camada RRC 694 da rede 690 e

passada para o cerne PS 698.

Entrementes, em resposta à mensagem de atualização de localização 620, a rede cerne CS 696 iniciou uma mensagem de solicitação de autenticação 650. O MM 686 do UE 680 responde com uma mensagem de resposta de autenticação CS 655 para a conexão CS. A mensagem de resposta de autenticação 655 é encaminhada da camada RRC 694 da rede 690 para a camada CS 696.

Após a mensagem de resposta de autenticação CS 655 ser recebida pela camada CS 696 da rede 690, a camada CS 696 envia uma mensagem de comando em modo de segurança 660 para iniciar a proteção de integridade para a conexão CS entre o UE 680 e a rede 690. Quando a camada RRC 684 do UE 680 recebe a mensagem de comando em modo de segurança CS 660 da camada RRC 694 da rede, o UE 680 inicia a proteção de integridade. Quando a iniciação do modo de segurança é completado na camada RRC 684, o UE 680 notifica a rede 690 utilizando a mensagem completa em modo de segurança CS 665 e notifica sua camada MM comutada por circuito 686 utilizando a mensagem 667.

Neste ponto, a conexão de sinalização PS é liberada 670 antes do término bem-sucedido do procedimento em modo de segurança, e as chaves de segurança permanecem não utilizadas. Se uma conexão PS é originada novamente, o UE 680 envia uma transferência direta inicial (IDT) ao enviar uma mensagem de solicitação de afixação 680 incluindo o valor $START_{PS}$ de 0. O UE 680 utilizará as chaves PS não utilizadas quando o procedimento em modo de segurança PS é iniciado. O valor START zero na mensagem de solicitação de afixação 680 forçará que o valor COUNT-I_{PS} seja zero, que

então casará com o valor COUNT-I_{PS} zero no UE 680.

Quando o valor COUNT-I_{PS} da rede e o COUNT-I_{PS} do UE casam, a conexão de substituição PS recém iniciada pode utilizar as chaves de segurança da conexão anterior para estabelecer a proteção de integridade e o estabelecimento da chamada não falhará devido a uma incapacidade de sustentar o modo de segurança.

Sem o fluxograma 500 mostrado na Figura 5, a mensagem de solicitação de afixação 680 teria incluído o valor $START_{PS}$ do USIM de acordo com procedimentos IDT padrão. O valor STARTPS do USIM poderia ser um valor não zero que teria causado um erro no casamento entre o valor COUNT-IPS da rede e o valor COUNT-IPS do UE, que teria impedido a chamada de re-conexão de ter sucesso.

Assim, o método de sincronização de contagem sincroniza o valor COUNT-I da rede com o valor COUNT-I do UE mesmo quando a conexão de sinalização é liberada antes do término bem-sucedido do procedimento de modo de segurança. Este método dá às tentativas de re-conexão uma chance maior de ter sucesso e impede falhas no estabelecimento de chamadas devido a uma incapacidade de efetuar a proteção de integridade. Ao acrescentar um ponto de decisão com base em se chaves não utilizadas de uma tentativa de conexão anterior estão disponíveis no UE, o método assegura que os valores COUNT de proteção de integridade para o UE e a rede serão sincronizados.

Embora esta revelação inclua o que são considerados atualmente como sendo as versões preferidas e melhores modos da invenção descritos de maneira a estabelecer a posse da mesma pelos inventores e que permite aqueles de

habilidade ordinária na tecnologia fazer e utilizar a invenção, será compreendido e apreciado que há muitos equivalentes às versões preferidas aqui reveladas e que modificações e variações poderão ser feitas sem desviar do escopo da invenção, que não são para serem limitados pelas versões preferidas e sim pelas reivindicações apensas, incluindo quaisquer emendas feitas durante a pendência desta aplicação e todos os equivalentes daquelas reivindicações conforme emitidas.

É ainda compreendido que a utilização de termos relacionais como primeiro e segundo, e assemelhados, são utilizados unicamente para distinguir uma de outra entidade, item, ou ação sem necessariamente exigir ou implicar em qualquer efetivo relacionamento ou ordem desses entre essas entidades, itens ou ações. Boa parte da funcionalidade inventiva e muitos dos princípios inventivos são mais bem implementados em programas ou instruções em software. É esperado que alguém de habilidade ordinária, apesar do possivelmente significativo esforço e muitas opções de projeto motivadas, por exemplo, pelo tempo disponível, pela tecnologia atual, e por considerações econômicas, quando orientado pelos conceitos e princípios aqui revelados serão prontamente capazes de gerar essas instruções e programas de software com um mínimo de experimentação. Portanto, maior discussão desse software, se houver, será limitada no interesse da brevidade e da minimização de qualquer risco de obscurecer os princípios e conceitos de acordo com a presente invenção.

REIVINDICAÇÕES

1. Método de sincronização de contagem de proteção de integridade compreendendo:

estabelecer uma conexão RRC entre um equipamento de usuário e uma rede; e

iniciar, através do equipamento de usuário, uma segunda conexão de sinalização a um segundo domínio na rede enquanto o equipamento do usuário já tem uma primeira conexão de sinalização a um primeiro domínio na rede, tanto a primeira conexão de sinalização como a segunda conexão de sinalização utilizam a conexão RRC;

o método sendo **caracterizado** por:

determinar se novas chaves de segurança do segundo domínio estão pendentes no equipamento do usuário;

enviar um valor START de 0 em uma mensagem de transferência direta inicial, se novas chaves de segurança estiverem pendentes no equipamento do usuário; e

manter a conexão RRC entre o equipamento de usuário e a rede.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de determinar se novas chaves de segurança estão pendentes no equipamento do usuário compreender:

conferir por uma variável no equipamento do usuário que indica que chaves de segurança não utilizadas estão pendentes.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato da rede ser uma rede de Projeto de Parceria de Terceira Geração.

4. Método, de acordo com a reivindicação 1,

caracterizado pelo fato de ainda compreender:

enviar um valor START não zero na mensagem de transferência direta inicial, se nenhuma chave de segurança nova estiver pendente no equipamento do usuário.

5. Método, de acordo com a reivindicação 4, **caracterizado** pelo fato do valor START não zero ser determinado a partir de um Universal Subscriber Interface Module.

6. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato do segundo domínio ser um domínio comutado por pacote e o primeiro domínio ser um domínio comutado por circuito.

7. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato do segundo domínio ser um domínio comutado por circuito e o primeiro domínio ser um domínio comutado por pacote.

8. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender:

liberar uma conexão de sinalização para o segundo domínio antes de completar um procedimento de modo de segurança, antes da etapa de inicialização.

9. Método, de acordo com a reivindicação 8, **caracterizado** pelo fato do primeiro domínio ser comutado por pacote e o segundo domínio ser comutado por circuito.

10. Método, de acordo com a reivindicação 8, **caracterizado** pelo fato do primeiro domínio ser comutado por circuito e o segundo domínio ser comutado por pacote.

11. Método, de acordo com a reivindicação 8, **caracterizado** pelo fato de ainda compreender:

enviar uma mensagem de transferência direta inicial

com um valor START não zero no segundo domínio, se nenhuma chave de segurança nova estiver pendente para o segundo domínio.

12. Método, de acordo com a reivindicação 11, **caracterizado** pelo fato do valor START não zero ser derivado de um Universal Subscriber Interface Module.

33
RJ.

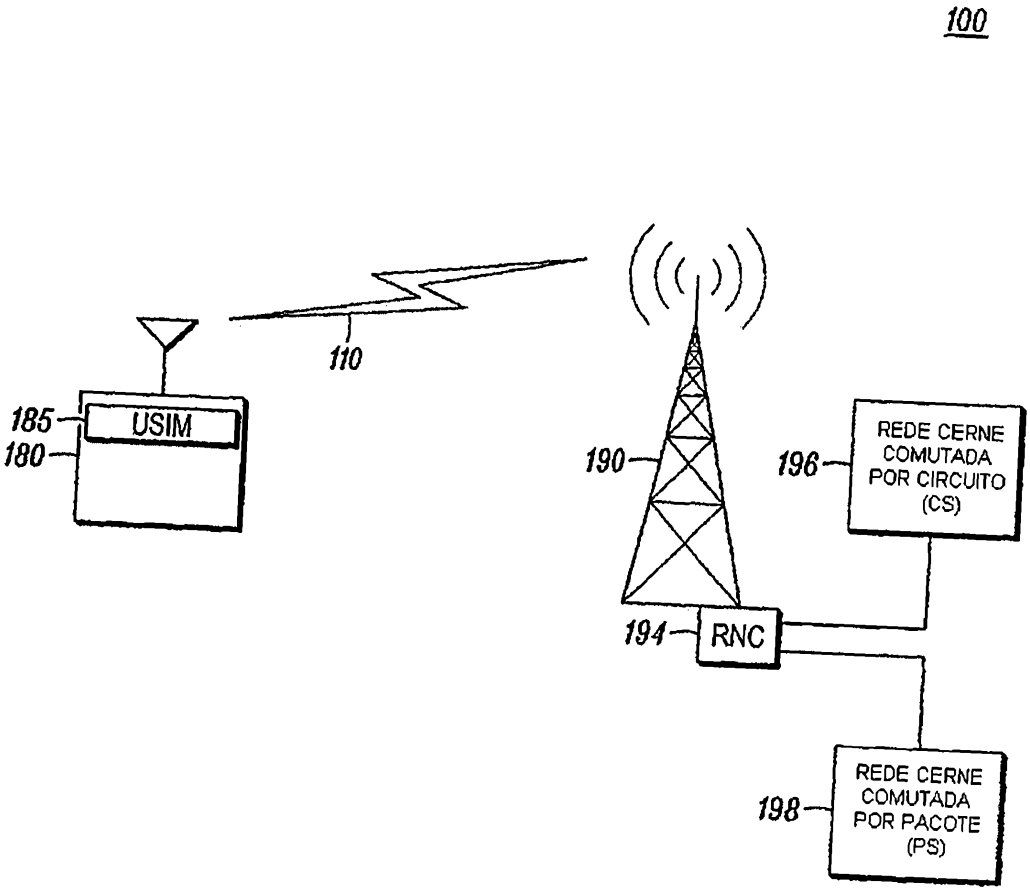
100
110
185
USIM
180
190
196
REDE CERNE COMUTADA POR CIRCUITO (CS)
194
RNC
198
REDE CERNE COMUTADA POR PACOTE (PS)

FIG. 1

200

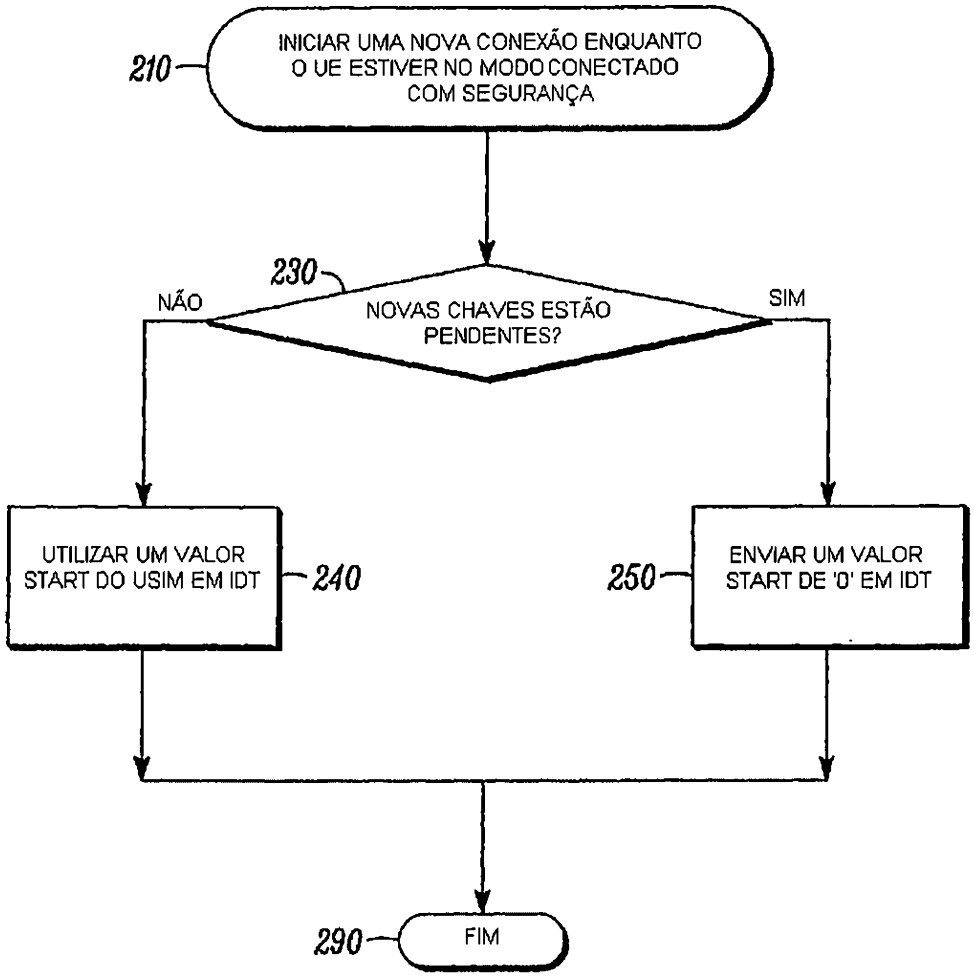
210
INICIAR UMA NOVA CONEXÃO ENQUANTO O UE ESTIVER NO MODO CONECTADO COM SEGURANÇA
230
NÃO
NOVAS CHAVES ESTÃO PENDENTES?
SIM
UTILIZAR UM VALOR START DO USIM EM IDT
240
250
ENVIAR UM VALOR START DE '0' EM IDT
290
FIM

FIG. 2

300

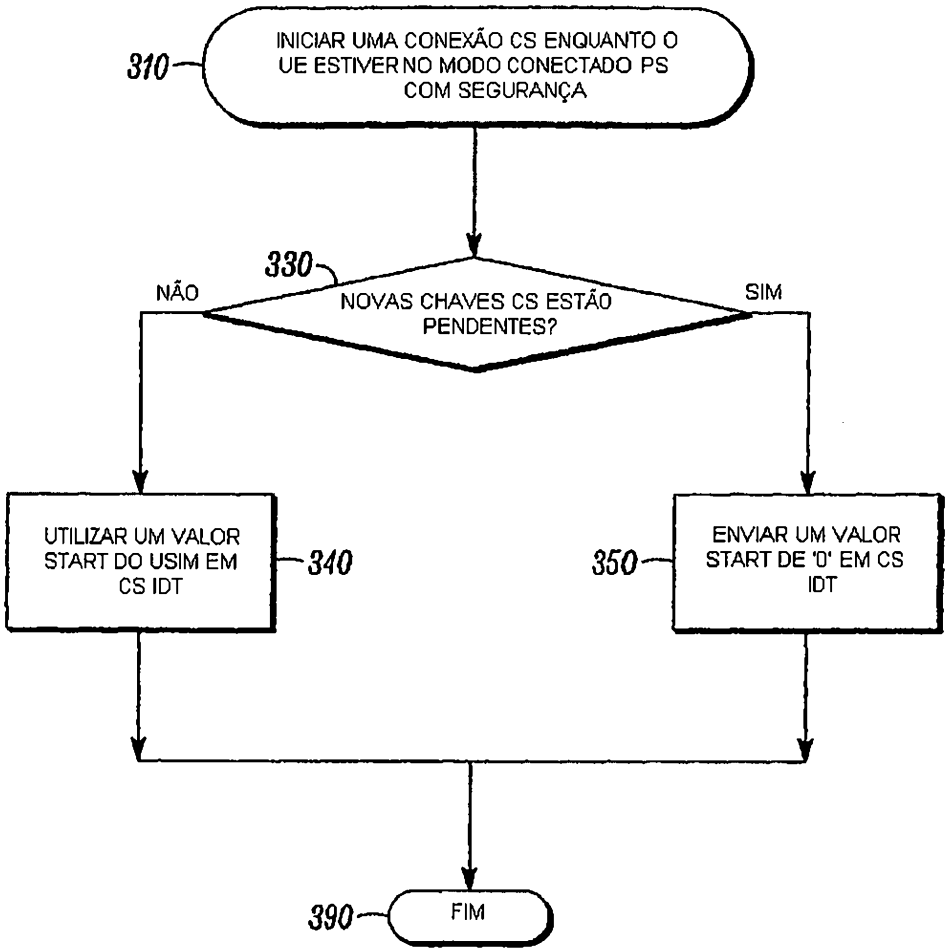
310
INICIAR UMA CONEXÃO CS ENQUANTO O UE ESTIVER NO MODO CONECTADO PS COM SEGURANÇA
330
NOVAS CHAVES CS ESTÃO PENDENTES?
NÃO
SIM
UTILIZAR UM VALOR START DO USIM EM CS IDT
340
350
ENVIAR UM VALOR START DE '0' EM CS IDT
390
FIM

FIG. 3

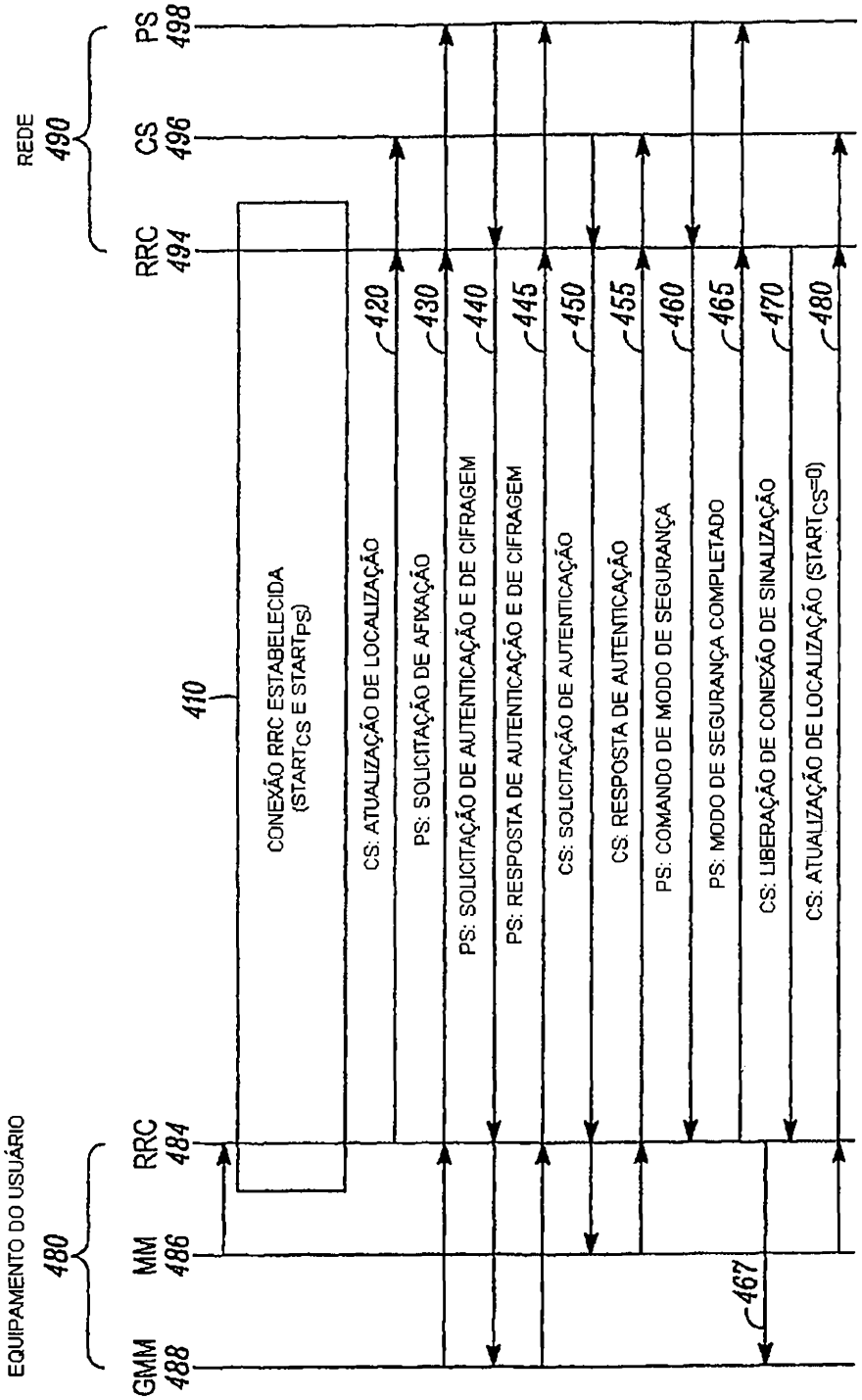
400
EQUIPAMENTO DO USUÁRIO
480
GMM 488
MM 486
RRC 484
REDE
490
RRC 494
CS 496
PS 498
410
CONEXÃO RRC ESTABELECIDA (START$_{CS}$ E START$_{PS}$)
CS: ATUALIZAÇÃO DE LOCALIZAÇÃO 420
PS: SOLICITAÇÃO DE AFIXAÇÃO 430
PS: SOLICITAÇÃO DE AUTENTICAÇÃO E DE CIFRAGEM 440
PS: RESPOSTA DE AUTENTICAÇÃO E DE CIFRAGEM 445
CS: SOLICITAÇÃO DE AUTENTICAÇÃO 450
CS: RESPOSTA DE AUTENTICAÇÃO 455
PS: COMANDO DE MODO DE SEGURANÇA 460
PS: MODO DE SEGURANÇA COMPLETADO 465
467
CS: LIBERAÇÃO DE CONEXÃO DE SINALIZAÇÃO 470
CS: ATUALIZAÇÃO DE LOCALIZAÇÃO (START$_{CS}$=0) 480

FIG. 4

37
RJ.

500

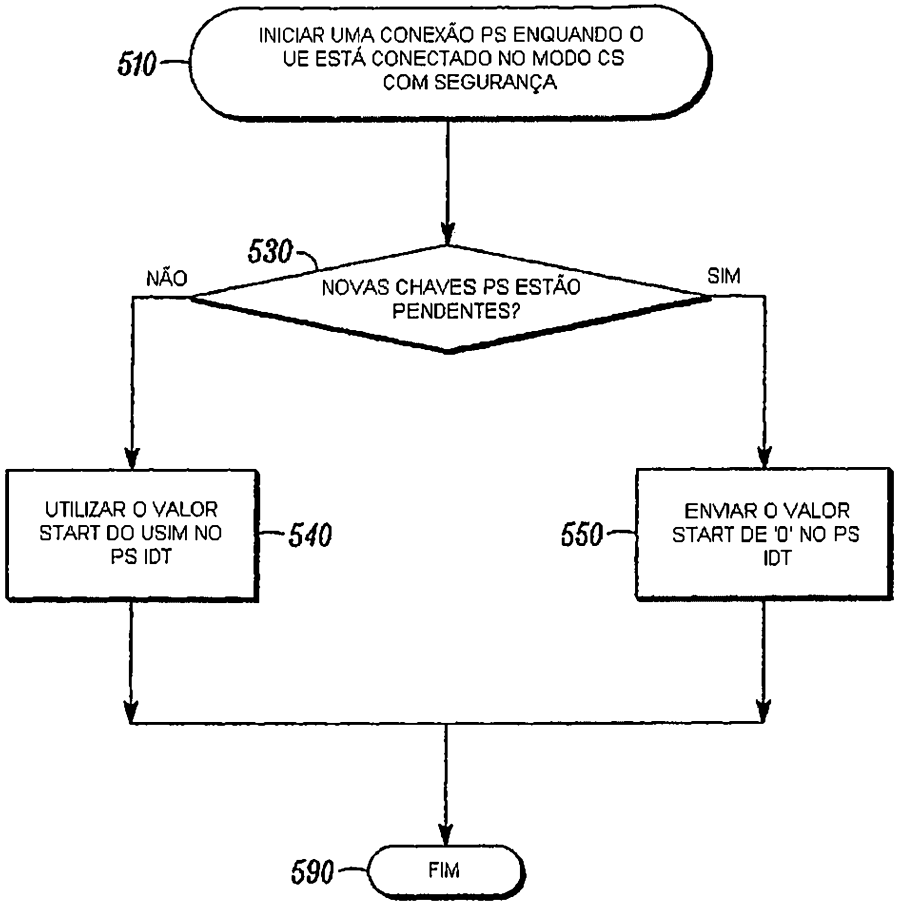

FIG. 5

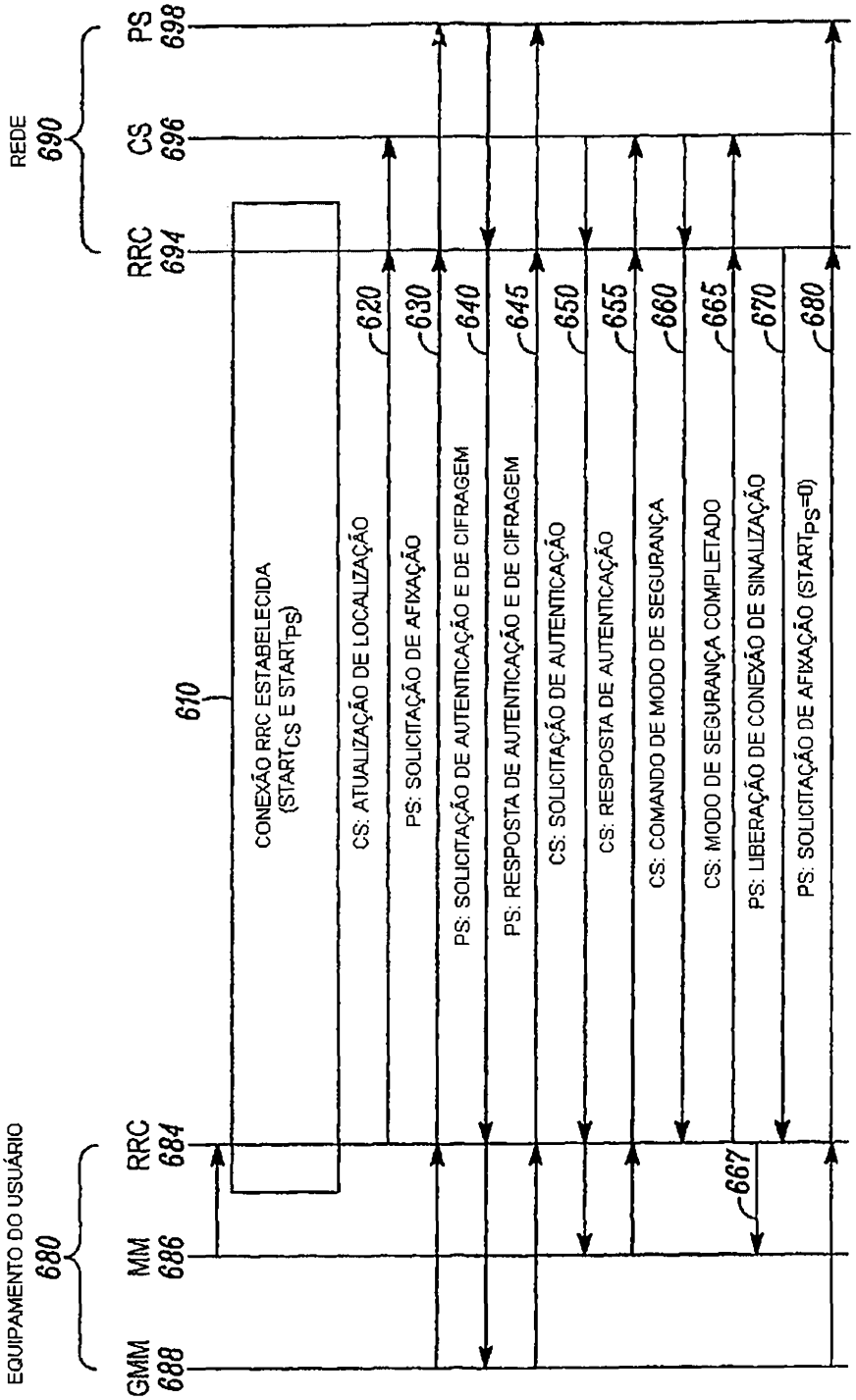
600
EQUIPAMENTO DO USUÁRIO
680
GMM 688
MM 686
RRC 684
REDE
690
RRC 694
CS 696
PS 698
610
CONEXÃO RRC ESTABELECIDA (START$_{CS}$ E START$_{PS}$)
620
CS: ATUALIZAÇÃO DE LOCALIZAÇÃO
630
PS: SOLICITAÇÃO DE AFIXAÇÃO
640
PS: SOLICITAÇÃO DE AUTENTICAÇÃO E DE CIFRAGEM
645
PS: RESPOSTA DE AUTENTICAÇÃO E DE CIFRAGEM
650
CS: SOLICITAÇÃO DE AUTENTICAÇÃO
655
CS: RESPOSTA DE AUTENTICAÇÃO
660
CS: COMANDO DE MODO DE SEGURANÇA
665
CS: MODO DE SEGURANÇA COMPLETADO
667
670
PS: LIBERAÇÃO DE CONEXÃO DE SINALIZAÇÃO
680
PS: SOLICITAÇÃO DE AFIXAÇÃO (START$_{PS}$=0)

FIG. 6