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

(21) **PI 0711827-9 A2**

BRPI0711827A2

(22) Data de Depósito: 09/05/2007
(43) Data da Publicação: 17/01/2012
(RPI 2141)

(51) Int.Cl.:
H04N 7/167
H04N 7/24

(54) Título: SISTEMA E MÉTODO PARA DETERMINAR DINAMICAMENTE IDENTIFICADORES DE FLUXO EM UM SISTEMA DE TRANSPORTE MULTI-CRIPTOGRÁFICO

(30) Prioridade Unionista: 15/05/2006 US 11/383.375

(73) Titular(es): Scientific-Atlanta, Inc

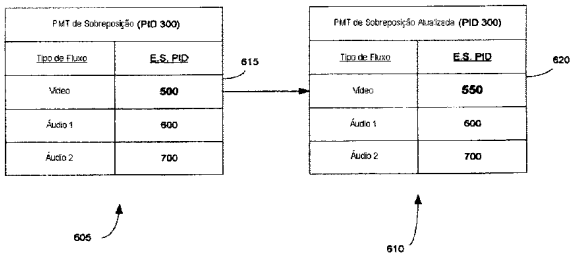
(72) Inventor(es): Neil B. Buchen, Thomas C. Wilson

(74) Procurador(es): Orlando de Souza

(86) Pedido Internacional: PCT US2007068532 de 09/05/2007

(87) Publicação Internacional: WO 2007/134089de 22/11/2007

(57) Resumo: SISTEMA E MÉTODO PARA DETERMINAR DINAMICAMENTE IDENTIFICADORES DE FLUXO EM UM SISTEMA DE TRANSPORTE MULTI- CRIPTOGRÁFICO. A presente invenção é adequada para utilização em um sistema multi-criptografado que determina dinamicamente identificadores de fluxo em um fluxo de sobreposição secundário dependendo dos identificadores no fluxo criptografado primário, O fluxo de entrada criptografado primário é monitorado para determinar a presença de todos os valores identificadores. Uma vez determinados os valores identificadores, os valores são armazenados em uma tabela de determinação e marcados como "em uso" para assegurar que esses valores identificadores não são determinados para qualquer um dos fluxos de sobreposição secundários. O fluxo criptografado primário é monitorado e a tabela de determinação é continuamente atualizada para detectar qualquer modificação ou conflitos nos valores identificadores, e os fluxos de sobreposição secundários são dinamicamente atualizados de acordo.



SISTEMA E MÉTODO PARA DETERMINAR DINAMICAMENTE IDENTIFICADORES DE FLUXO EM UM SISTEMA DE TRANSPORTE MULTI-CRIPTOGRÁFICO

CAMPO DA INVENÇÃO

A presente invenção relaciona-se genericamente ao campo de fluxos duais criptografados em um sistema de comunicação e, mais especificamente, no sentido de determinar dinamicamente informação de identificador de fluxo de um fluxo secundário no sistema.

HISTÓRICO DA INVENÇÃO

Sistemas de comunicação a cabo transmitem tipicamente fluxos de dados criptografados de acordo com um único esquema reservado. Assim, operadores de cabo precisam adquirir dispositivo de descriptografação, ou de mesa, que residem nas dependências do assinante, que descriptografam os fluxos de dados de acordo com o esquema de criptografia reservado. Obviamente, é benéfico para o operador de cabo e para o assinante ser capaz de oferecer múltiplos aparelhos de mesa com diferentes esquemas de descriptografação em vez de precisar selecionar apenas um único aparelho de mesa para o sistema. Sob esta ótica, o operador agora tem a opção de instalar um sistema de sobreposição, que permite múltiplos esquemas de criptografia e da mesma forma múltiplos dispositivos de descriptografia que descriptografa, cada um deles, um dos fluxos criptografados.

Em um sistema de sobreposição, no entanto, precauções especiais devem ser tomadas para assegurar que os fluxos de transporte multi-criptografados não estão em conflito nem colidem uns com os outros. Será apreciado que em um sistema

de comunicação convencional, há vários níveis de fluxos que compreendem um fluxo de transporte. Muito genericamente, o fluxo de transporte compreende uma pluralidade de programas em que cada um deles tem um número de programa. Cada um dos fluxos de programas compreende fluxos elementares de vídeo, de áudio ou de dados. Ademais, cada fluxo elementar compreende pacotes de vídeo, de áudio, ou de dados. O número de programa em uma tabela de associação de programa (PAT) identifica cada programa e uma tabela de mapa de programa (PMT) associada. Cada PMT então identifica os fluxos elementares com identificadores de pacote (PIDs). Os números de programa e os PIDs são escolhidos inicialmente de uma faixa fixa bem conhecida de números definidos na especificação MPEG. Portanto, existe uma chance de que dois fluxos de transporte separados vindo de diferentes provedores de serviço que são transmitidos utilizando o mesmo sistema, poderão incluir identificadores comuns (por exemplo, números de programa e PIDs) fazendo com que os dois fluxos se sobreponham, com isso apresentando número de programas e/ou pacotes de fluxos elementares que não possuem valores de fluxo identificadores singulares, mas são direcionados para dois dispositivos de descriptografação diferentes. Neste caso, o dispositivo de descriptografação recebe o fluxo criptografado com pacotes tendo esquemas de criptografia diferentes utilizando o mesmo identificador e poderá tentar descriptografar os fluxos errados, que então causaria vários problemas. Assim, existe uma necessidade de revelar, monitorar, e modificar dinamicamente os identificadores e as rotas de fluxo nos fluxos de transporte nesses sistemas para assegurar que os

conflitos não surjam.

DESCRIÇÃO SUCINTA DOS DESENHOS

A Figura 1 é um diagrama de blocos simplista de um sistema de sobreposição que transporta múltiplos fluxos criptografados com diferentes esquemas de criptografia para múltiplos dispositivos de descriptografação.

A Figura 2 ilustra uma tabela de associação de programa criptografado primário (PAT) que é transmitida periodicamente juntamente com o fluxo de transporte que os dispositivos de criptografação principais acessam para localizar um programa desejado e seus componentes no fluxo de transporte.

A Figura 3 ilustra uma PAT de sobreposição original que é transmitida periodicamente junto com o fluxo de transporte que tanto os dispositivos de criptografia secundário e principal acessam para localizar um programa desejado e seus componentes no fluxo de transporte.

A Figura 4 ilustra um PAT criptografado primário atualizado.

A Figura 5 ilustra um PAT de sobreposição atualizado tendo uma versão 2 de acordo com a presente invenção.

A Figura 6 ilustra uma tabela de mapa de programa de sobreposição original (PMT) e um PMT de sobreposição atualizado de acordo com a presente invenção.

A Figura 7 é um diagrama de blocos do dispositivo de processamento, ou de criptografação, e sistema de controle que monitora, detecta, e revisa quaisquer conflitos nos números de programa e/ou identificadores de pacotes de acordo com a presente invenção.

A Figura 8 é um diagrama de blocos de um dispositivo

de processamento de monitoramento PID que é adequado para utilização em uma Ethernet GIGA ou um ambiente comutado por pacote de acordo com a presente invenção.

DESCRIÇÃO DETALHADA DE UMA VERSÃO PREFERIDA

A presente invenção será descrita mais integralmente doravante com referência aos desenhos acompanhantes em que números iguais representam elementos iguais por todas as várias figuras, e em que uma versão exemplar da invenção é mostrada. No entanto, esta invenção poderá ser incorporada em muitas formas diferentes e não deve ser interpretada como sendo limitada às versões aqui apresentadas; em vez disso, as versões são fornecidas de modo que esta revelação seja integral e completa, e transmite inteiramente o escopo da invenção para aqueles habilitados na tecnologia. A presente invenção é descrita mais integralmente abaixo.

A presente invenção é adequada para utilização no sistema de comunicação de transporte MPEG que transmite múltiplos fluxos que utilizam esquemas de criptografia diferentes por um sistema a dispositivos de recepção dotados de múltiplos esquemas de descriptografia. A presente invenção permite que pelo menos dois dispositivos de descriptografia diferentes (por exemplo, um aparelho de mesa principal e um aparelho de mesa secundário) estejam localizados em um único sistema, que transmite fluxos tendo um esquema de criptografia principal e pelo menos outro esquema de criptografia (isto é, um esquema de criptografia de sobreposição, ou secundário). Cada aparelho de mesa é projetado para descriptografar quer o esquema de criptografia principal ou o secundário de cada vez. Antes de combinar os múltiplos fluxos criptografados para revelar

e monitorar os números de programa e os identificadores de pacote dos fluxos principal e secundário para assegurar que quaisquer conflitos nos fluxos de sobreposição e identificadores sejam corrigidos antes da transmissão. Mais especificamente, se um conflito for detectado (isto é, o fluxo primário e o fluxo secundário têm o mesmo número de programa e/ou identificador de pacote), a presente invenção modifica dinamicamente o identificador comum no fluxo secundário para um identificador diferente que é singular e não conflita com qualquer um dos fluxos criptografados primários associados. Assim, os múltiplos fluxos são transmitidos tendo diferentes números de programa e/ou identificadores de pacote. Adicionalmente, os dispositivos de descriptografia secundários, ou de sobreposição, no sistema são notificados do identificador modificado no fluxo secundário para assegurar o processamento apropriado e sua posterior exibição.

A Figura 1 é um diagrama de blocos simplista de um sistema de comunicação de sobreposição que transporta múltiplos fluxos criptografados com esquemas de criptografia diferentes para múltiplos dispositivos de descriptografação. Em uma instalação central de processamento de sinal, um dispositivo de criptografação de sobreposição 105, como, mas sem a eles se limitar, um modulador de modulação de amplitude de quadratura (QAM), recebe um fluxo de entrada criptografada principal 115 e um fluxo de entrada livre casado 120. Será apreciado que vários dispositivos de criptografia existem na central de processamento de sinal cada um deles recebendo uma cópia do fluxo de entrada criptografado primário e o fluxo de

entrada livre de acordo com configurações predeterminadas; no entanto, apenas um dispositivo de criptografia 105 é mostrado, por simplificação. O dispositivo de criptografação de sobreposição 105 manipula o fluxo de entrada criptografado primário 115 e o fluxo de entrada livre 120 para fornecer um fluxo criptografado dual parcial 125 (isto é, um fluxo de saída de sobreposição combinado). O fluxo de saída de sobreposição combinado 125 compreende pacotes selecionados do fluxo de entrada criptografado primário e pacotes casados do fluxo de entrada livre que foram criptografados com um esquema de criptografia secundário combinado com os pacotes restantes no fluxo de entrada livre. Por exemplo, 2% dos pacotes incluídos no fluxo criptografado primário são escolhidos do fluxo de entrada criptografado primário. Pacotes casados do fluxo de entrada livre são então criptografados com o esquema de criptografia secundário. Os 2% de pacotes criptografados primários e os 2% de pacotes criptografados secundários são então combinados para fornecer um fluxo de 4% de sobreposição criptografado combinado. O fluxo combinado de 4% é subseqüentemente com o fluxo de entrada livre restante de 98% para fornecer pacotes de conteúdo combinado de 102% no fluxo de saída de sobreposição combinado 125. O fluxo de saída de sobreposição combinado 125 é então fornecido para múltiplos dispositivos de descriptografação 130, 135, em que alguns dispositivos 130 poderão ter esquemas de descriptografação de acordo com o0 esquema de criptografia principal que descriptografam o conteúdo criptografado de 2% principal. Outros dispositivos 135 poderão ter esquemas de descriptografação de acordo com o esquema de

criptografia secundário que descriptografam o conteúdo criptografado de 2% do fluxo criptografado secundário. Será apreciado que ambos os dispositivos 130, 135 recebem e processam o fluxo livre de 98%. Mais informação relativa ao sistema de comunicação de criptografia dual pode ser encontrada no Pedido de Patente dos Estados Unidos número de série 10/629.839 intitulado "Methods and Apparatus for Providing a Partial Dual-Encrypted Stream in a Conditional Access System" requerido em 30 de julho de 2003, a revelação e os ensinamentos da qual são aqui incorporados por referência.

Um sistema de controle (CS) 140 fornece o gerenciamento, monitoramento e controle completo dos elementos do sistema e os serviços de irradiação fornecido aos usuários. Especificamente em um sistema de sobreposição, o sistema de controle 140 cuida da informação de provisionamento e de controle entre os dispositivos de descriptografia secundários 135 e o dispositivo de criptografia de sobreposição 105. Desta maneira, o CS 140 controla os números de programa de fluxo de saída enquanto o dispositivo de criptografia 105 controla todos os identificadores de pacote para o fluxo criptografado secundário. Assim, o CS 140 e o dispositivo de criptografia de sobreposição 105 descobrem e monitoram continuamente todos os números de programa e identificadores de pacote no fluxo criptografado primário e dependendo de quaisquer conflitos, os números de programa e os identificadores de pacote para o fluxo criptografado secundário são modificados dinamicamente para evitar quaisquer conflitos no fluxo de sobreposição de saída combinado 125.

A Figura 2 ilustra uma tabela de associação de programa (PAT) de entrada criptografada principal 200. Em um sistema de sobreposição, esta PAT é então analisada, recriada, combinada com informação de programa secundária, e então transmitida periodicamente juntamente com os demais componentes no fluxo de transporte 115. Os dispositivos de descriptografação primários 130 acessam o PAT de sobreposição combinado 305 para localizar um programa desejado e seus componentes no fluxo de transporte. Em um sistema de não sobreposição, os dispositivos de recepção 130 identificam e subseqüentemente recebem a PAT 200 por seu valor PID reservado de 0x0 203. A PAT 200 contém uma lista de todos os números de programas (PNs) disponíveis naquele fluxo de transporte e seus valores PID da tabela de mapeamento de programa (PMT) associada 210 para cada programa. O programa também é conhecido como uma sessão pois sessões referenciam um programa específico em um fluxo de transporte. Cada valor PID PMT 210, por exemplo, um valor PID PMT de 0x250, na PAT de entrada criptografada principal 200 é associada à PMT 215 que inclui os valores PID de fluxo elementar de 0x500, 0x510, e 0x520. Mais especificamente, a PMT 215, que é identificada pelo número de programa 0x20, e associada pelo valor PID PMT de 0x250, identifica os pacotes de vídeo e de áudio 220 para o programa associado. De acordo com a presente invenção, os dispositivos de descriptografação secundárias 135 não sintonizarão no programa 0x20 na PAT de entrada criptografada principal 200 e sua PMT associada e alternativamente aceitam seus valores PAT e PMT através de seus respectivos identificadores.

A Figura 3 ilustra uma tabela de associação de programa (PAT) de programa de sobreposição de saída original (PID 0x0) que é transmitida periodicamente junto com o fluxo de transporte que tanto os dispositivos de descriptografação secundário e principal acessam para localizar um programa desejado e seus componentes no fluxo de transporte. A PAT de sobreposição de saída 305 transportada no fluxo de sobreposição de saída combinado 125 inclui uma seção PAT que compreende a seção PAT criptografada de entrada principal inteira 315 junto com a seção PAT criptografada de programa de sobreposição acrescentada 325 para os dispositivos de descriptografação secundários 135. Como foi mencionado, os dispositivos de descriptografação secundários 135 são instruídos para sintonizar no fluxo de transporte para seus números de programa associados incluídos na PAT de sobreposição de saída 305 ao procurar pelo valor PID de 0x0 e subseqüentemente pesquisar a seção PAT criptografada do programa de sobreposição 325 para o número de programa desejado (PN). Os números de programa então identificam tabelas de mapeamento de programa (PMTs) por um valor PID que inclui identificadores de pacote para os pacotes de fluxo de programa no fluxo de sobreposição de saída combinado 125.

As seções PAT principal e secundária 315, 325, são combinadas no fluxo de saída de sobreposição combinado 125. A PAT de sobreposição de saída 305 é partilhada entre os dois sistemas de criptografia e conterá os programas PAT criptografados primários inteiros junto com os programas criptografados secundários ativos. O dispositivo de

criptografação 105 efetua o monitoramento PID de entrada criptografada principal para redeterminar dinamicamente os valores PID e de número de programa para evitar qualquer conflito com o fluxo criptografado primário 115 no fluxo de saída de sobreposição combinado 125. Será apreciado que a seção PAT do fluxo criptografado primário 315 permanece intocada e o fluxo criptografado primário flui sem qualquer conflito entre os fluxos criptografados principal e secundário.

A Figura 4 ilustra um número de programa atualizado na PAT criptografada principal 400. Em conjunto com a Figura 3, é observado que a PAT criptografada de entrada principal atualizada 400 agora tem um conflito de número de programa na seção PAT criptografada de programa de sobreposição 325 com o número de programa 0x40, que está ativo no fluxo criptografado secundário, e um conflito da PID PMT com o número de programa 0x60, que também está ativo no fluxo criptografado secundário. De acordo com a presente invenção, os conflitos são detectados antes de transmitir os fluxos criptografados principal e secundário.

A Figura 5 ilustra uma PAT de sobreposição atualizada 505 (versão 2) de acordo com a presente invenção. Devido ao conflito do número de programa 0x40, o número de programa de saída criptografada secundária 0x40 é modificado para um novo número de programa não utilizado 424; neste caso o número de programa 0x45 é utilizado. Ademais, o número de programa PAT de entrada criptografada atualizada 0x40 utiliza um valor PID PMT de 0x400. Portanto, o PID PMT do fluxo criptografado primário atualizado (isto é, 0x400) também conflita com o PID PMT (isto é, 0x400) associado ao

número de programa 0x60 no fluxo criptografado secundário. De acordo com a presente invenção, o conflito é detectado, e o PID PMT 0x400 é modificado para uma PID PMT não utilizada, que neste exemplo é o valor de 0x450. A PAT de sobreposição de saída atualizada 505 que inclui a seção PAT de entrada criptografada principal atualizada 520, a seção PAT criptografada de programa de sobreposição atualizada 515, e suas seções PMT associadas é então transmitida tanto para os dispositivos de descriptografação principal como secundário 130, 135.

A PAT de saída de sobreposição atualizada 505 tendo um número de versão incrementado é utilizada para sinalizar os dispositivos de descriptografação principal e secundário 130, 135 dos valores de fluxo de sobreposição modificados. Assim, os dispositivos de descriptografação principais 130 sintonizarão corretamente no número de programa 0x40 tendo um valor PID PMT de 0x400, e os dispositivos de descriptografação secundários 135 sintonizarão corretamente o fluxo de programa que utiliza o novo número de programa 0x45 tendo o valor PID PMT de 0x200. Será apreciado que a PID PMT associada ao número de programa revisto 0x45 poderá não modificar se os identificadores de pacote PMT não conflitarem com qualquer fluxo de entrada criptografada ativa utilizando o valor PID PMT de 0x200. Portanto, os pacotes elementares de vídeo e de áudio para o número de programa 0x45 ainda estão localizados em uma PMT que utiliza o valor PID de 0x200. Isto é apenas um exemplo e o algoritmo não é limitado ou obrigado a utilizar o mesmo valor PID PMT para o fluxo atualizado que agora utiliza o número de programa 0x45. Adicionalmente, os dispositivos de

descriptografação secundários 135 sintonizam corretamente no número de programa 0x60 tendo um valor PID PMT atualizado de 0x450.

A Figura 6 ilustra uma tabela de mapeamento de programa (PMT) de sobreposição original e uma PMT de sobreposição atualizada de acordo com a presente invenção. A PMT de sobreposição 605 tem um valor PID de 0x300 que é associado a um valor de número de programa de 0x50 mostrado na Figura 3. Neste exemplo, no entanto, o valor PID de vídeo de 0x500 conflita com a PID PMT criptografada principal 0x500 para o fluxo de vídeo principal como é mostrado na PMT criptografada principal 215 (Figura 2). De acordo com a presente invenção, o conflito é detectado e os valores PID de sobreposição conflitantes de 0x500 615 são modificados para um valor PID não utilizado de 0x550 620. A PMT de sobreposição atualizada 610 é então transmitida juntamente com o fluxo de saída de sobreposição combinado 125. As PIDs restantes na PMT 605 não exigem qualquer modificação, pois não há nenhum conflito.

A Figura 7 é um diagrama de blocos de um dispositivo de processamento, ou de criptografia 705 que monitora, detecta, e atualiza dinamicamente o fluxo criptografado secundário para corrigir quaisquer conflitos nos números de programas e/ou identificadores de pacote de acordo com a presente invenção. O dispositivo de processamento exemplar 705 inclui duas portas de entrada de interface serial assíncrona (ASI) que utilizam 8192 contadores de 32 bits em cada porta. Um banco de contadores 710 recebe o fluxo de entrada criptografado primário 115 e o fluxo de entrada livre casado 120 através das portas de entrada. Cada

contador 710 (1-n) é utilizado para monitorar a atividade PID do fluxo de entrada criptografada principal para todos os 8.192 valores PID disponíveis. Na fase de descoberta, cada contador é originalmente fixado em 0. Para cada número de programa e identificador de pacote presente no fluxo de entrada criptografado primário, um contador 710 (1-n) associado ao atual número de programa e cada identificador de pacote associado é incrementado por um. O dispositivo de processamento 705 monitora todos os valores do contador para detectar quais contadores 710 (1-n) têm um valor de zero e quais contadores 710 (1-n) têm um valor maior que zero. Pode então ser determinado que os contadores 710 (1-n) tendo o valor de zero não tiveram nenhuma atividade e estão disponíveis para os programas de sobreposição de saída e os identificadores de pacote para os fluxos de saída de sobreposição criptografada secundários. Quaisquer contadores 710 (1-n) tendo um valor de contador maior que zero indica atividade PID e estão atualmente em uso pelo fluxo criptografado primário e, portanto, não devem ser utilizados em qualquer fluxo de sobreposição secundário. Utilizando a informação PID descoberta, o dispositivo de processamento 705 ou designa inicialmente ou modifica as seções PAT e PMT para os fluxos de sobreposição secundários para utilizar valores que não conflitam com os valores de fluxo criptografado principais.

Em ocasião, um número de programa e/ou identificador de pacote no fluxo primário poderá mudar dinamicamente e começar a utilizar novos valores PID de fluxo e/ou de número de programa. Para esses casos, a fase de monitoramento continua a monitorar os contadores 710 (1-n)

por qualquer modificação atualizada. Assim, se um número de programa e/ou um identificador de pacote não utilizado anteriormente for posteriormente descoberto no fluxo de entrada criptografado primário e que o novo identificador está conflitando com um identificador já designado no fluxo de saída de sobreposição secundário, o dispositivo de processamento 705 atualiza a PAT e/ou a PMT para o fluxo de saída de sobreposição dependendo dos valores de fluxo que mudaram. A seção PAT e/ou PMT atualizada é então imediatamente transmitida no fluxo de saída de sobreposição combinada 125 para os dispositivos de descriptografação secundários 135 para sinalizar as mudanças no fluxo. Preferivelmente, o fluxo de entrada criptografada principal é portalizada até o PAT e/ou PMT de sobreposição atualizada serem transmitida e rotas de fluxo são atualizadas para assegurar nenhuma ruptura ou conflito antes da revisão. Adicionalmente, será apreciado que em algum ponto, os contadores 710 a-n poderão ficar cheios; em cujo ponto, os contadores 710 a-n poderão ser redefinidos e a fase de monitoramento continua com a identificação dos números de programa e os identificadores de pacote em uso.

Um seletor e mapeador de pacote crítico 720 seleciona pacotes críticos predeterminados do fluxo de entrada livre. Os pacotes críticos são então criptografados com o segundo esquema de criptografia. Os pacotes criptografados secundários são então mapeados tendo um valor PID apropriado nas tabelas PMT e/ou PAT de acordo com a presente invenção. As tabelas, os pacotes criptografados principal e secundário, e os pacotes livres são subseqüentemente multiplexados pelo multiplexador 725 para

fornecer um fluxo de sobreposição combinado 730.

Será apreciado que o dispositivo de processamento 705 da Figura 7 funciona bem em um ambiente ou produto que é limitado a um pequeno número de portas de entrada. O monitoramento da PID e do número de programa é efetuado após a energização do dispositivo de processamento 705 e continua para monitorar os fluxos de entrada criptografados primários de modo que o dispositivo de processamento 705 poderá detectar com rapidez qualquer mudança no PID dinâmico e/ou no número de programa que afetem o fluxo de saída de sobreposição combinado 125. Adicionalmente, é sabido que em um ambiente GIGA Ethernet ou de comutação por pacote, são projetados produtos para suportar um grande número de fluxos de entrada singulares quando comparado ao ambiente ASI, que normalmente só suporta um pequeno número de fluxos de entrada singulares. Portanto, seria necessária uma grande quantidade de memória para acompanhar os 8.192 contadores PID de 32 bits para cada um dos fluxos de entrada singulares em um ambiente GIGA Ethernet ou de comutação por pacote.

A Figura 8 é um diagrama de blocos de um dispositivo de processamento de monitoramento de PID contínuo 805 que é adequado para uso em um ambiente GIGA Ethernet ou de comutação por pacote de acordo com a presente invenção. Como vantagem, o dispositivo de processamento de monitoramento PID 805 é capaz de receber muitos mais fluxos GIGA Ethernet ou comutados por pacote que estão compreendidos no fluxo de entrada criptografada principal 115 enquanto não exige uma quantidade imoderada de memória. Adicionalmente, o monitoramento contínuo dos fluxos

detectará qualquer mudança no fluxo dinâmico após a energização inicial do dispositivo de processamento 805. Portanto, de acordo com a presente invenção, o dispositivo de processamento de monitoramento PID contínuo 805 passa inicialmente por uma fase de descoberta e então monitora continuamente o fluxo de entrada criptografada 115 para detectar qualquer mudança PID dinâmica n fluxo criptografado primário e efetua mudanças no fluxo sobreposto de saída 730, de acordo; com isso, evita PIDs duplicados que causam colisões no fluxo sobreposto combinado 730.

O dispositivo de monitoramento PID contínuo 805 inclui um processador 810 que recebe o fluxo criptografado primário 115. O processador 810 utiliza um único valor de bit, que corresponde valores de 16 bits que compreendem um PID, para cada PID e um método de refixação para determinar se qualquer um dos 8.192 fluxos PID estão ativos. Os contadores PID são continuamente atualizados para um estado fixado/ativo quando qualquer atividade PID for detectada. O algoritmo lê todos os contadores de bit PID, e então refixa todos os contadores, e entra de volta no modo de descoberta PID. Este método pegará a atividade PID que flutua entre ativa e não ativa de modo que os estados do contador PID não ficarão caducos. Utilizar o método de bit para indicar e armazenar a atividade PID economiza memória em comparação com o dispositivo de processamento 705 da Figura 7 e permite que 8.192 valores PID sejam armazenados em apenas 1024 bytes de memória. Inicialmente na energização do dispositivo de monitoramento PID 805, os valores PID do fluxo primário são descobertos e marcados como "em uso". Os

valores em uso são armazenados em uma tabela que indica que eles estão atualmente determinados, ou indisponíveis. Adicionalmente, valores PID não determinados ou livres são armazenados em uma tabela que pode ser utilizada pelo fluxo de sobreposição secundário.

Os sistemas e métodos aqui descritos resolvem quaisquer identificadores em duplicata ao continuamente monitorar e subseqüentemente modificar dinamicamente valores identificadores de fluxo. No entanto, há ocasiões em que as rotas físicas que transportam os fluxos dos dispositivos de criptografia múltipla 105 poderão precisar ser modificados para assegurar que não há nenhuma questão de fluxo cruzado com os dispositivos de descriptografia 130, 135 que estão atualmente observando o programa. Por meio de exemplo, suponha que um dispositivo de descriptografação secundário 135 está vendo um jogo de baseball no número de programa 0x17 com um PID de vídeo de 0x50 e um PID de áudio de 0x51. Devido a um conflito de PID com um canal adulto, que poderá ter acabado de ser acrescentado ao sistema, o dispositivo de processamento 705, 805 muda o número de programa de sobreposição 0x17 que tem as PIDs 0x500 e 0x501, respectivamente. Se o dispositivo de descriptografação 135 não mudar dinamicamente seus PIDs para as PIDs atualizadas, uma questão de fluxo cruzado surgirá e ele começará a descriptografar o canal adulto tendo PIDs 0x50 e 0x51. Portanto, é extremamente importante que os programas sejam recebidos apenas pelos dispositivos de descriptografia principal e secundário pretendidos 130, 135.

Assim, a conexão física entre a entrada e a saída do

dispositivo de processamento 705, 805 é modificada para eliminar a questão de fluxo cruzado. Se a rota permanecer aberta com os parâmetros originais após a mudança no fluxo, isto poderá criar a questão de fluxo cruzado pois a conexão física da entrada para a saída não está atualizada. O controle das rotas pode ser em um ASIC, em um FPGA, ou código em um processador As rotas são estabelecidas para passar os dados com base na informação no fluxo como valor PID, valor da porta User Datagram Protocol (UDP), e valor Internet Protocol (IP). Quando um valor de fluxo específico como o identificador mudar, o dispositivo de processamento 705, 805 reconhece a mudança e atualiza a rota para aquele fluxo.

Adicionalmente, um sistema e método primeiro-a-entrar primeiro-a-sair (FIFO) de PID de retorno é utilizado para armazenar valores PID que não são determinados de imediato a qualquer novo programa de sobreposição secundária que for criado. Em uma versão preferida, uma malha de PID de 16 bits é utilizada. No entanto, será apreciado que o tamanho pode ser escalonado dependendo do dispositivo de processamento 705, 805 e a aplicação. Cada entrada na malha PID conterá um valor PID para retornar à tabela de determinação PID. Após a malha PID FIFO encher, o código começa a retornar o valor PID mais antigo para um estado não determinado. Os valores PID também poderão ser armazenados em NVM e restaurados à tabela de determinação PID e retornar FIFO de PID após a energização do dispositivo de processamento 705, 805. Desta forma, questões de fluxo cruzado são minimizadas.

Será apreciado que modificações podem ser feitas na

versão da presente invenção que ainda está dentro do escopo da invenção. Adicionalmente, a presente invenção pode ser implementada utilizando hardware e/ou software que estão dentro do escopo de alguém habilitado na tecnologia. As versões da descrição foram apresentadas para fins de esclarecimento; no entanto, a invenção é definida pelas reivindicações seguintes.

REIVINDICAÇÕES

1. Método para determinar dinamicamente valores identificadores para um fluxo secundário dependendo de um fluxo primário em um fluxo de transporte multi-criptografado, em que os valores identificadores se enquadram dentro de uma faixa de valores, o método **caracterizado** pelo fato de compreender as etapas de:

receber um fluxo criptografado primário em um processador, em que o fluxo criptografado primário compreende pacotes criptografados primários;

revelar um valor identificador para cada pacote criptografado primário;

armazenar um valor de bit correspondente a cada valor identificador descoberto em uma tabela determinada;

com base em cada valor identificador descoberto na tabela determinada, designar um valor identificador disponível para cada pacote criptografado secundário compreendido de um fluxo criptografado secundário, em que o valor identificador disponível é escolhido de uma tabela disponível.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender a etapa de redefinir o valor de bit na tabela determinada de acordo quando o valor identificador for modificado ou acrescentado no fluxo criptografado primário.

3. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender a etapa de mapear o valor identificador designado de acordo com o valor de bit para um de uma tabela de associação de programa (PAT) e uma tabela de mapeamento de programa

(PMT), em que a PAT e a PMT são transmitidas junto com o fluxo de transporte multi-criptografado.

4. Método, de acordo com a reivindicação 3, **caracterizado** pelo fato de ainda compreender as etapas de:

monitorar continuamente os valores identificadores do fluxo criptografado primário;

redefinir o valor de bit na tabela determinada quando um valor identificador monitorado for mudado em um fluxo criptografado primário atualizado;

determinar se o valor de bit redefinido conflita com o identificador designado do fluxo criptografado secundário; e

modificar o identificador designado do fluxo secundário para um valor identificador designado atualizado tomada da tabela disponível para fornecer um fluxo criptografado secundário atualizado.

5. Método, de acordo com a reivindicação 4, **caracterizado** pelo fato de ainda compreender as etapas de:

remapear o identificador designado atualizado do fluxo secundário em um de PAT e PMT; e

transmitir um de PAT e PMT que compreende o identificador designado atualizado remapeado.

6. Método, de acordo com a reivindicação 4, **caracterizado** pelo fato de ainda compreender a etapa de:

bloquear a transmissão do fluxo criptografado primário atualizado enquanto o fluxo criptografado secundário é atualizado com mudanças de rota e um de PAT e PMT que compreende o identificador designado atualizado são transmitidos para uma pluralidade de dispositivos receptores.

7. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato das etapas ainda compreenderem:

receber o fluxo de transporte multi-criptografado em uma pluralidade de dispositivos receptores, em que a pluralidade de dispositivos receptores descriptografa um do fluxo criptografado primário e o fluxo criptografado secundário;

em cada um da pluralidade de dispositivos receptores, determinar se um programa desejado está em seu fluxo criptografado associado por um número de programa na PAT; e

descriptografar o programa desejado por um identificador de vídeo, de áudio, e de criptografação na PMT.

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

receber o fluxo criptografado primário do processador e um fluxo livre em um seletor de pacote;

determinar um pacote crítico do fluxo livre e seu pacote criptografado primário associado;

criptografar o pacote crítico determinado do fluxo livre com um esquema de criptografação secundário para fornecer o pacote criptografado secundário; e

assegurar que o pacote criptografado secundário tem o valor identificador designado que não conflita com o valor identificador descoberto do fluxo criptografado primário ao comparar o valor identificador do pacote criptografado primário a cada valor de bit na tabela determinada.

9. Método para determinar dinamicamente valores identificadores a um fluxo criptografado secundário dependendo de um fluxo criptografado primário **caracterizado**

pelo fato de compreender as etapas de:

receber um fluxo criptografado primário em um processador, em que o fluxo criptografado primário compreender pacotes criptografados primários;

determinar um valor identificador para cada pacote criptografado primário;

armazenar o valor identificador determinado em uma tabela determinada;

receber o fluxo criptografado primário e o fluxo livre casado em um seletor de pacote;

determinar um pacote crítico do fluxo livre e seu pacote criptografado primário associado.

criptografar o pacote crítico determinado do fluxo livre com um esquema de criptografia secundário para fornecer um pacote criptografado secundário;

designar um valor identificador secundário ao pacote criptografado secundário que não está presente na tabela determinada; e

transmitir um fluxo de sobreposição combinado a uma pluralidade de dispositivos receptores, em que o fluxo de sobreposição combinado compreender os pacotes críticos do fluxo criptografado primário, os pacotes criptografados secundários de um fluxo criptografado secundário, e uma parte restante do fluxo livre.

10. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de ainda compreender a etapa de redefinir o valor identificador na tabela determinada quando o valor identificador determinado para um pacote criptografado primário for pelo menos um de modificado, acrescentado, ou removido do fluxo criptografado primário.

11. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de ainda compreender as etapas de:

monitorar continuamente e revelar os valores identificadores do fluxo criptografado primário;

redefinir o valor identificador na tabela determinada quando o valor identificador descoberto para um pacote criptografado primário for pelo menos um de mudado, acrescentado, ou removido do fluxo criptografado primário;

identificar se o valor identificador descoberto conflita com um valor identificador designado secundário em um pacote secundário; e

modificar o valor identificador secundário designado para um valor identificador designado atualizado não presente na tabela determinada.

12. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de ainda compreender a etapa de mapear o valor identificador secundário designado a uma de PAT e PMT, em que a PAT e a PMT são transmitidas junto com o fluxo de sobreposição combinado.

13. Método, de acordo com a reivindicação 12, **caracterizado** pelo fato de ainda compreender as etapas de:

monitorar continuamente o fluxo criptografado primário por valores identificadores modificados em um fluxo criptografado primário atualizado;

detectar uma mudança no valor identificador do fluxo criptografado primário atualizado;

determinar se o valor identificador modificado conflita com um valor identificador igual do fluxo criptografado secundário;

remapear o identificador modificado do fluxo

criptografado secundário em um de PAT e PMT; e

modificar o valor identificador conflitante do pacote criptografado secundário para um valor identificador não utilizado disponível não encontrado em um do fluxo criptografado primário atualizado e fluxo secundário.

14. Método, de acordo com a reivindicação 13, **caracterizado** pelo fato de ainda compreender as etapas de:

bloquear a transmissão dos fluxos criptografados principal atualizado e secundário; e

transmitir a PAT e PMT remapeados.

15. Sistema de comunicação para transmitir um fluxo de transporte multi-criptografado, o fluxo de transporte multi-criptografado incluindo um fluxo primário, um fluxo secundário e um fluxo livre, cada um dos fluxos incluindo uma pluralidade de programas, cada um deles tendo um número de programa e uma pluralidade de pacotes, cada um deles tendo um identificador de pacote, o sistema de comunicação **caracterizado** pelo fato de compreender:

um dispositivo para determinar dinamicamente números de programa e identificadores de pacote para pacotes secundários compreendidos no fluxo secundário dependendo dos números de programa e identificadores de pacotes presentes no fluxo primário, o dispositivo compreendendo:

meio de monitorização para monitorar e detectar os números de programa e os identificadores de pacote presentes no fluxo primário; e

meio de processamento para designar os números de programa disponíveis e os identificadores de pacote disponíveis para os pacotes secundários;

em que o meio de monitorização monitora continuamente

o fluxo primário por quaisquer mudanças no número de programa e nos identificadores de pacote, e quando mudanças ocorrerem, o meio de processamento verifica por conflitos e subseqüentemente designa o pacote tendo um número de programa conflitante ou um identificador de pacote conflitante para um de um número de programa disponível e identificador de pacote.

16. Sistema de comunicação, de acordo com a reivindicação 15, **caracterizado** pelo fato do dispositivo transmitir uma PAT e PMTs iniciais incluindo os números de programa e identificadores de pacote, respectivamente, que permitem que uma pluralidade de dispositivos de recepção secundários aceitem corretamente o fluxo secundário, e em que no evento de uma redesignação no fluxo primário dinâmico, o dispositivo transmite pelo menos um de uma PAT revista e PMTs dependendo do conflito detectado.

17. Sistema de comunicação, de acordo com a reivindicação 16, **caracterizado** pelo fato de que no evento de um conflito, o dispositivo bloqueia a transmissão do fluxo primário e do fluxo secundário até a redesignação do fluxo secundário conflitante estar completa e as PAT e PMTs refletirem a redesignação são transmitidos para os dispositivos de recepção principal e secundário.

18. Sistema de comunicação, de acordo com a reivindicação 15, **caracterizado** pelo fato do meio de monitorização compreender um processador para designar um valor de bit a uma tabela indisponível correspondente ao valor do número de programa e um valor identificador de pacote quando presente no fluxo primário.

19. Sistema de comunicação, de acordo com a

reivindicação 18, **caracterizado** pelo fato do meio de processamento subseqüentemente designar um disponível de um número de programa e um identificador de pacote no fluxo secundário.

20. Sistema de comunicação, de acordo com a reivindicação 19, **caracterizado** pelo fato do meio de processamento detectar um valor identificador de pacote liberado que estava anteriormente em uso pelo fluxo primário e armazenar o valor identificador de pacote liberado em uma memória provisória para retardar sua disponibilidade.

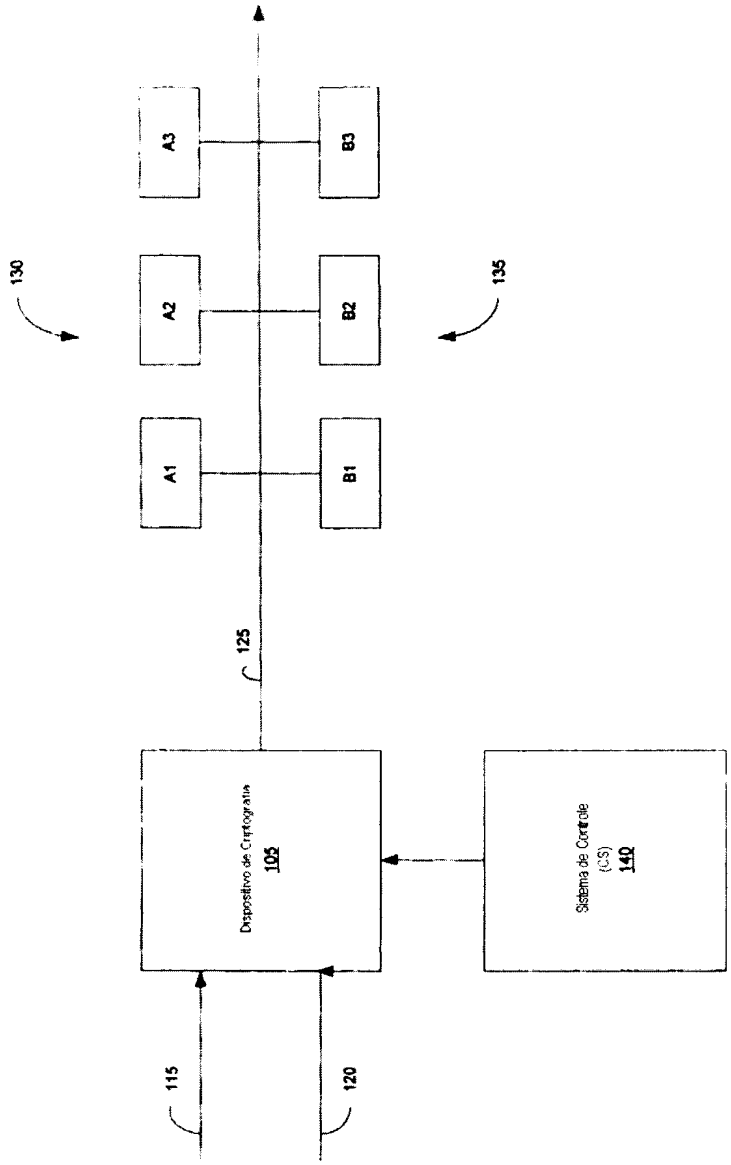

A3
B3
A2
B2
A1
B1
130
135
125
Dispositivo de Criptografia
105
Sistema de Controle
(CS)
140
115
120

FIG. 1

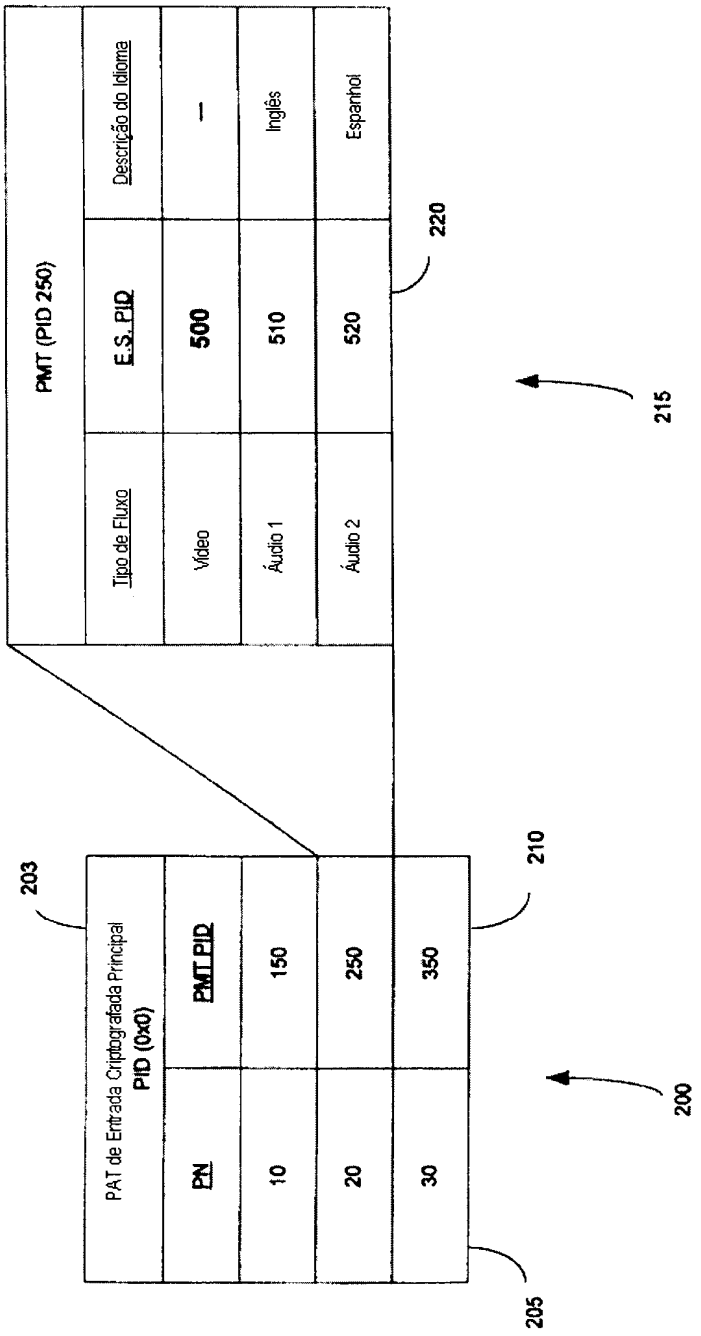

PAT de Entrada Criptografada Principal
PID (0x0)
PN
PMT PID
10
150
20
250
30
350
203
210
205
200
PMT (PID 250)
Tipo de Fluxo
E.S. PID
Descrição do Idioma
Vídeo
500
—
Áudio 1
510
Inglês
Áudio 2
520
Espanhol
220
215

FIG. 2

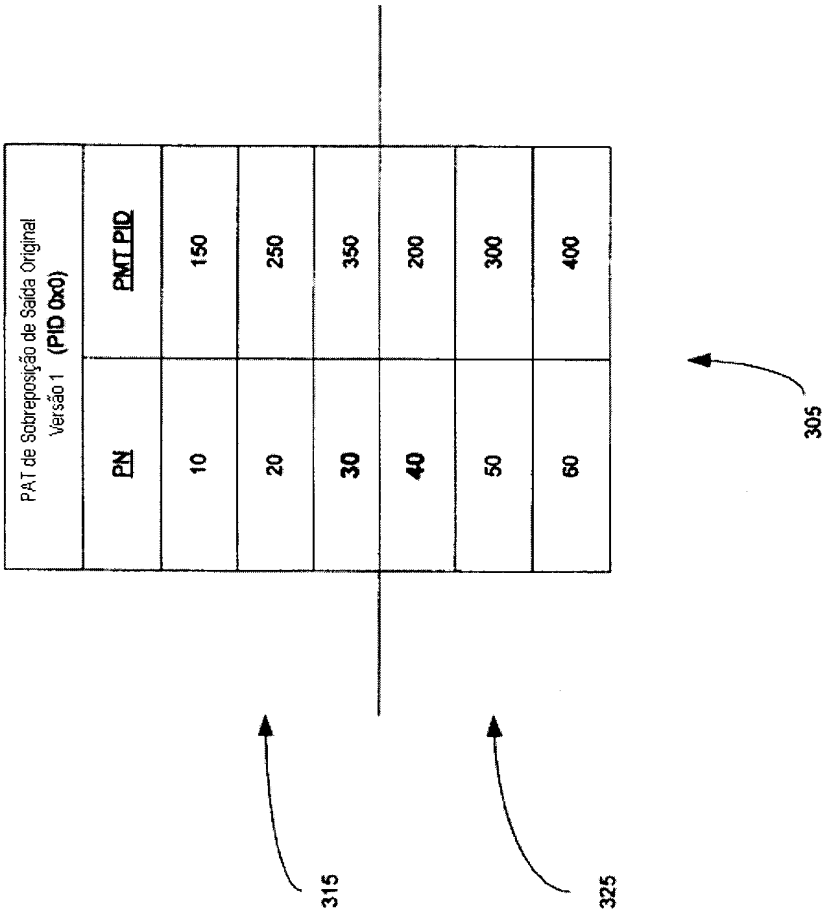

PAT de Sobreposição de Saída Original
Versão 1 (PID 0x0)
PN
PMT PID
10
150
20
250
30
350
40
200
50
300
60
400
305
315
325

FIG. 3

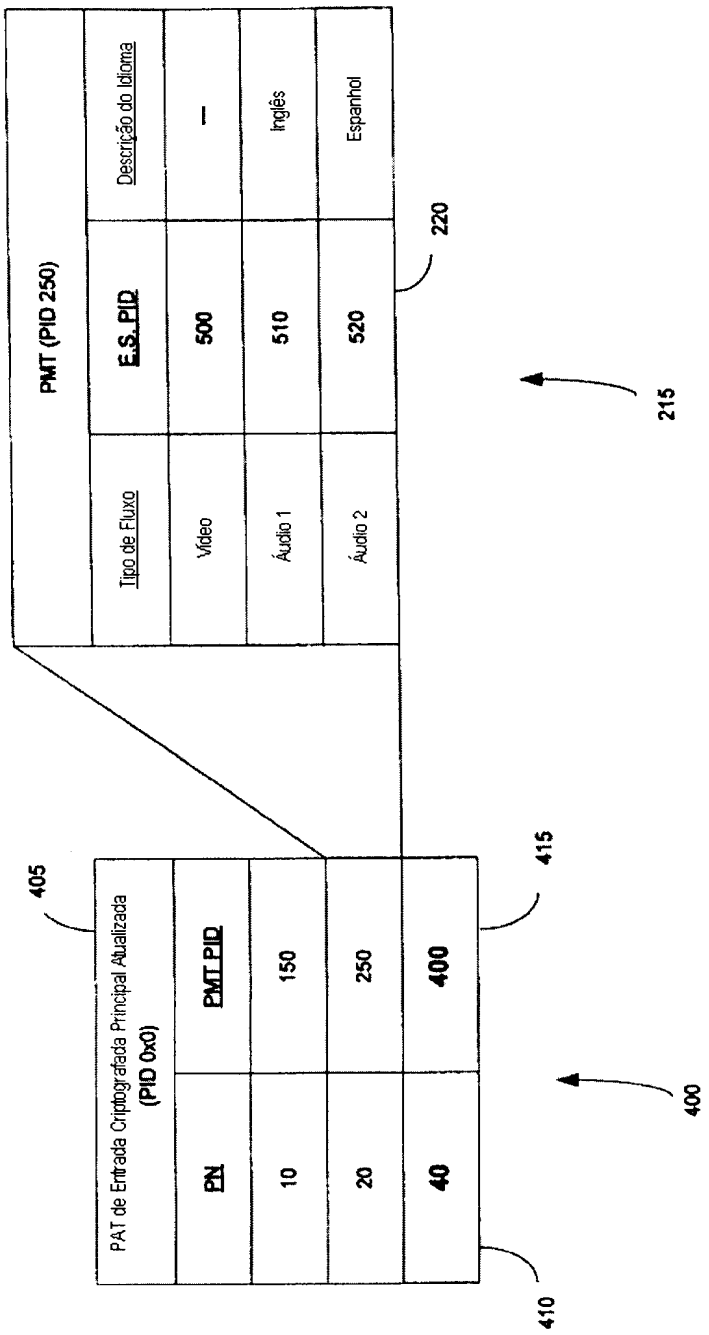

PAT de Entrada Criptografada Principal Atualizada (PID 0x0)
PN
PMT PID
10
150
20
250
40
400
405
410
415
400
PMT (PID 250)
Tipo de Fluxo
E.S. PID
Descrição do Idioma
Vídeo
500
—
Áudio 1
510
Inglês
Áudio 2
520
Espanhol
220
215

FIG. 4

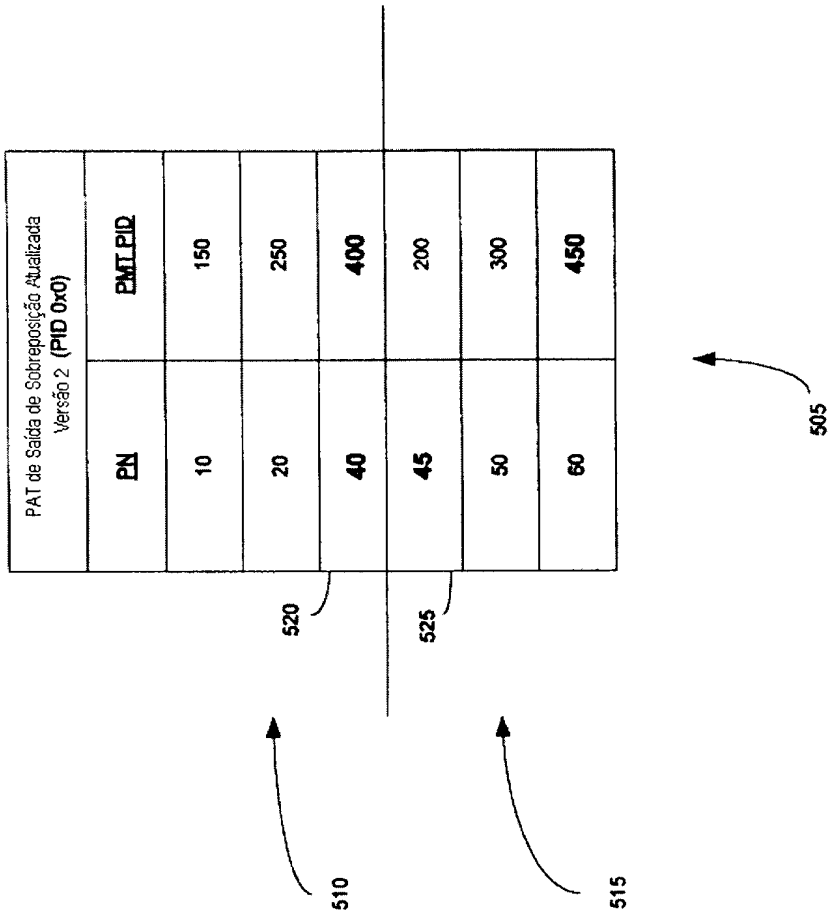

PAT de Saída de Sobreposição Atualizada
Versão 2 (PID 0x0)
PN
PMT PID
10
150
20
250
40
400
45
200
50
300
60
450
505
520
525
510
515

FIG. 5

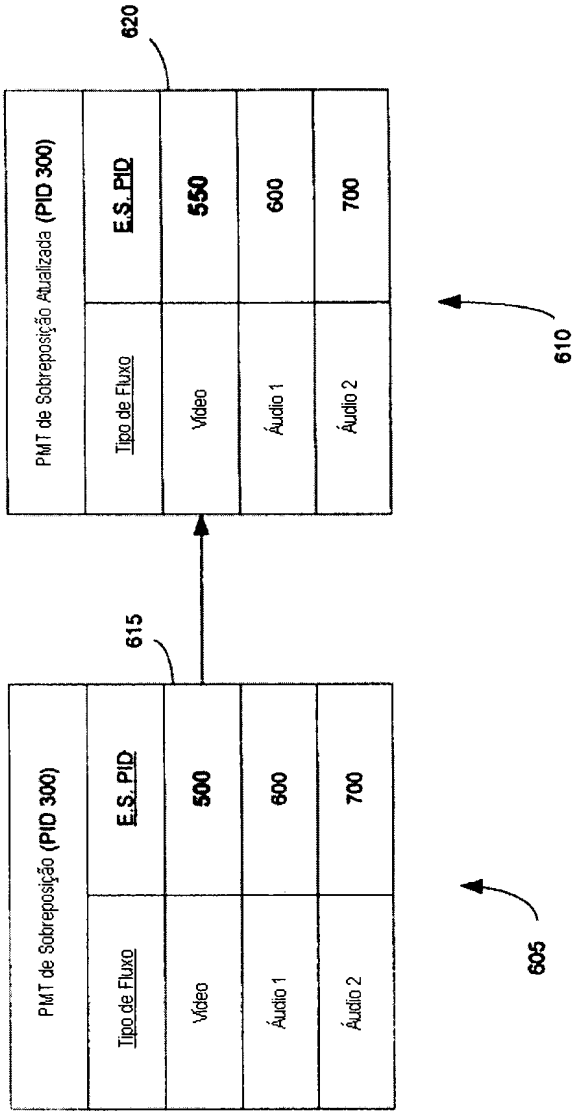

PMT de Sobreposição (PID 300)
Tipo de Fluxo
E.S. PID
Vídeo
500
Áudio 1
600
Áudio 2
700
615
605
PMT de Sobreposição Atualizada (PID 300)
Tipo de Fluxo
E.S. PID
Vídeo
550
Áudio 1
600
Áudio 2
700
620
610

FIG. 6

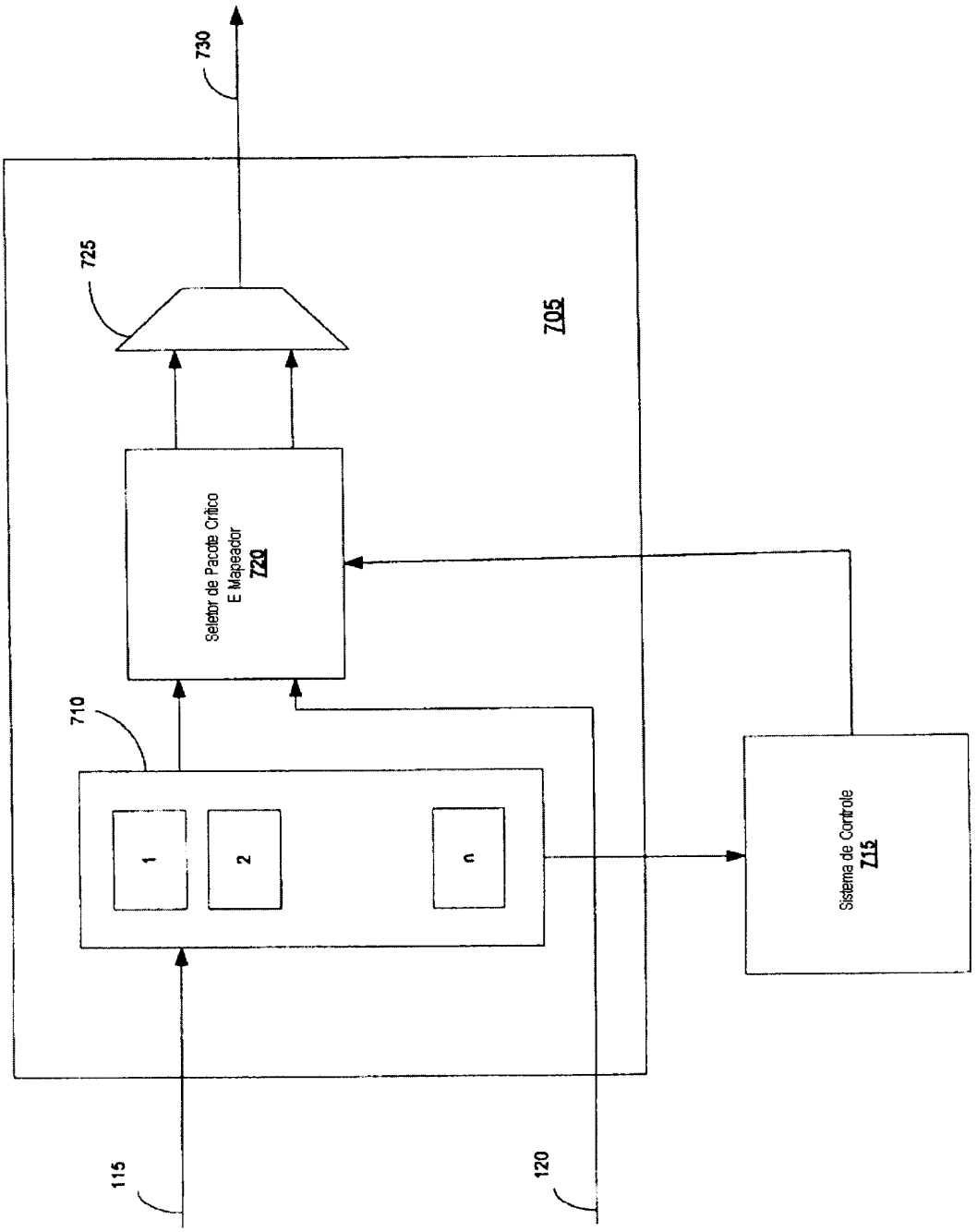

730
725
705
Seletor de Pacote Crítico
E Mapeador
720
710
1
2
n
Sistema de Controle
715
115
120

FIG. 7

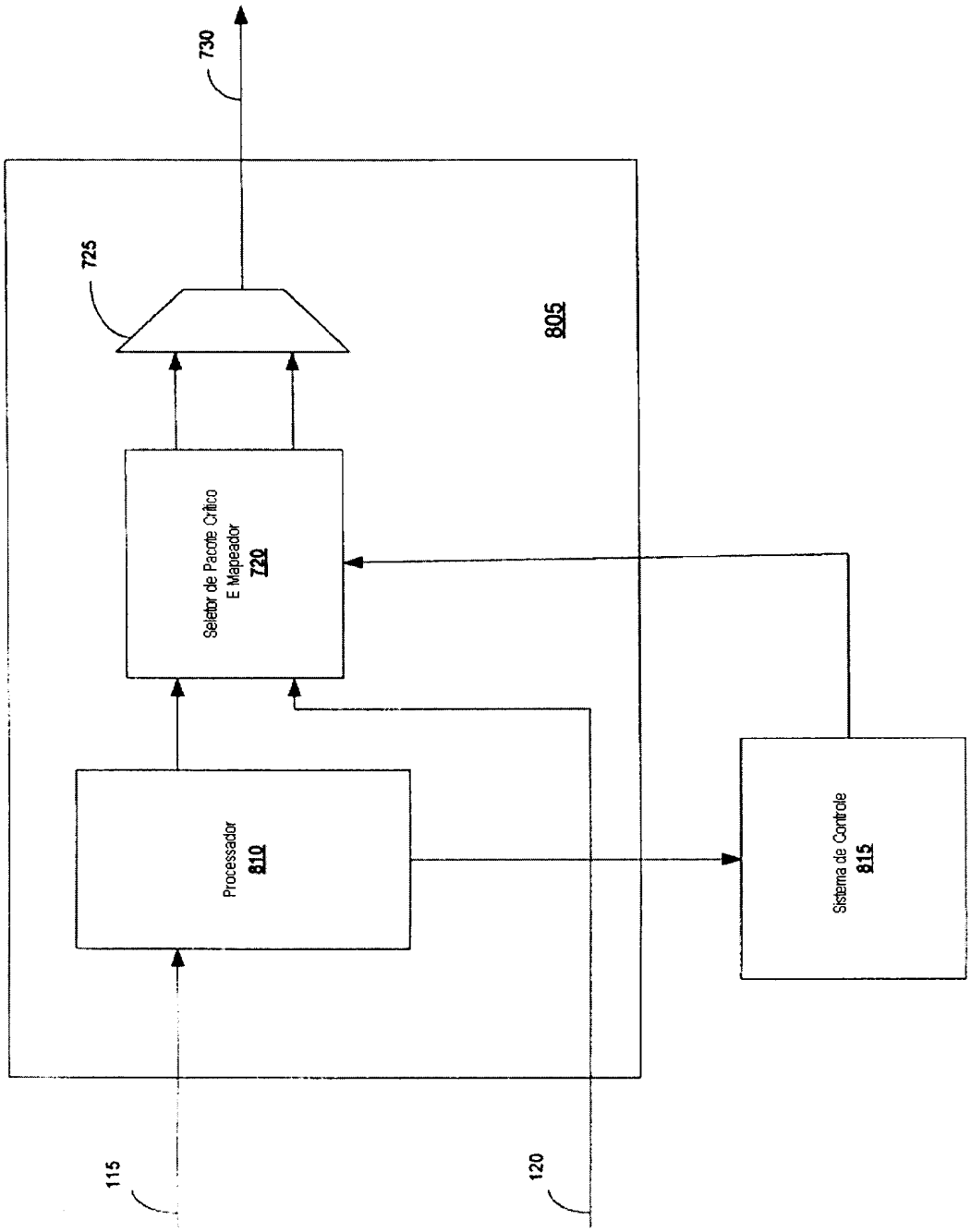

730
725
805
Seletor de Pacote Crítico
E Mapeador
720
Processador
810
Sistema de Controle
815
115
120

FIG. 8

SISTEMA E MÉTODO PARA DETERMINAR DINAMICAMENTE IDENTIFICADORES DE FLUXO EM UM SISTEMA DE TRANSPORTE MULTI-CRIPTOGRÁFICO

A presente invenção é adequada para utilização em um sistema multi-criptografado que determina dinamicamente identificadores de fluxo em um fluxo de sobreposição secundário dependendo dos identificadores no fluxo criptografado primário. O fluxo de entrada criptografado primário é monitorado para determinar a presença de todos os valores identificadores. Uma vez determinados os valores identificadores, os valores são armazenados em uma tabela de determinação e marcados como "em uso" para assegurar que esses valores identificadores não são determinados para qualquer um dos fluxos de sobreposição secundários. O fluxo criptografado primário é monitorado e a tabela de determinação é continuamente atualizada para detectar qualquer modificação ou conflitos nos valores identificadores, e os fluxos de sobreposição secundários são dinamicamente atualizados de acordo.

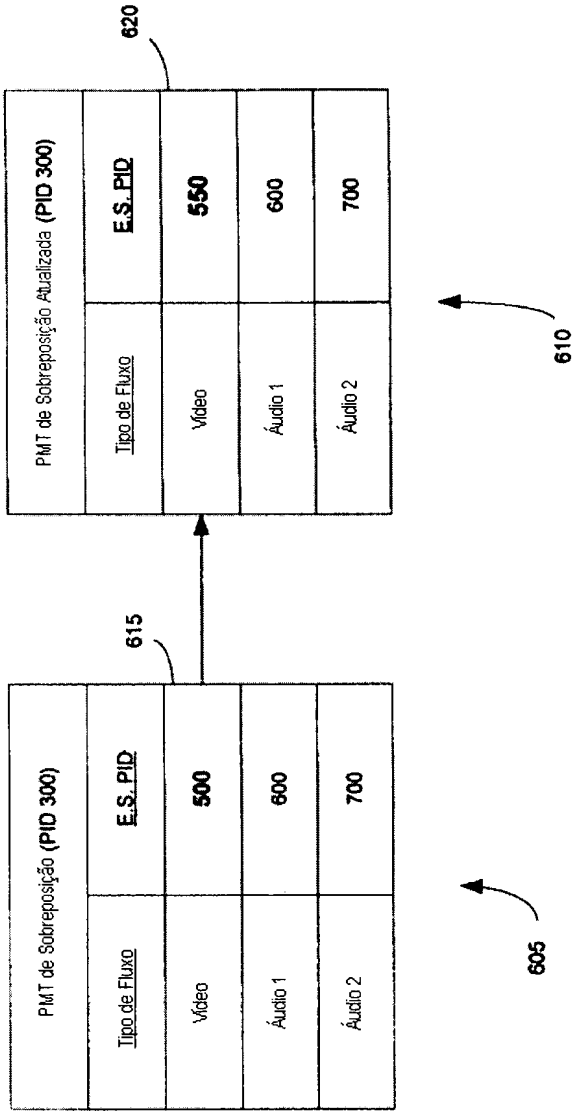

PMT de Sobreposição (PID 300)
Tipo de Fluxo
E.S. PID
Vídeo
500
Áudio 1
600
Áudio 2
700
615
605
PMT de Sobreposição Atualizada (PID 300)
Tipo de Fluxo
E.S. PID
Vídeo
550
Áudio 1
600
Áudio 2
700
620
610

FIG. 6