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

(21) **PI 0721542-8 A2**

BRPI0721542A2

(22) Data de Depósito: 30/04/2007
(43) Data da Publicação: 22/01/2013
(RPI 2194)

(51) Int.Cl.:
H04L 12/24
H04L 9/08
H04L 29/06
H04L 29/12

(54) Título: SISTEMA PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO, MÉTODO PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMAPLURALIDADE DE NÓS EM UM EVENTO E MEIO LEGÍVEL POR MÁQUINA

(73) Titular(es): HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.

(72) Inventor(es): DIRK JOHN HOGAN, EVAN L. SCHEESSELE, KEITH M. TAYLOR, TED BEERS

(74) Procurador(es): ANTONIO MAURICIO PEDRAS ARNAUD

(86) Pedido Internacional: PCT US2007067827 de 30/04/2007

(87) Publicação Internacional: WO 2008/133692de 06/11/2008

(57) Resumo: SISTEMA PARA DISTRIBUIR INFORMAÇOES DE CONFIGURAÇAO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO, MÉTODO PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇAO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO E MEIO LEGÍVEL POR MÁQUINA. Um sistema para distribuir informações de configuração de nó para uma pluralidade de nós em um evento é provido. O sistema inclui um primeiro nó, um segundo nó conectado operativamente ao primeiro nó, e um gerenciador de eventos conectado operativamente ao primeiro nó e ao segundo nó. O gerenciador de eventos transmite as informações de configuração de nó para o primeiro nó e o segundo nó, e transmite indicação para o primeiro nó e o segundo nó para iniciar comunicação entre o primeiro nó e o segundo nó usando as informações de configuração de nó.

"SISTEMA PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO, MÉTODO PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO E MEIO LEGÍVEL POR MÁQUINA".

Antecedentes

Conteúdo multimídia é comumente transmitido entre usuários através de redes, tais como redes de área local (LANs) e a Internet. Exemplos de conteúdo multimídia incluem texto, conteúdo de áudio, conteúdo de visual, e qualquer combinação dos mesmos. Medidas de segurança são algumas vezes necessárias para garantir que um bisbilhoteiro não possa acessar conteúdo multimídia confidencial transmitido através da rede.

Como um modo para garantir segurança, um remetente pode criptografar conteúdo multimídia antes de enviar o conteúdo multimídia criptografado, e um receptor pode descriptografar o conteúdo multimídia criptografado após receber o conteúdo multimídia criptografado. Tipos comuns de sistemas de criptografia incluem criptografia assimétrica e criptografia simétrica. A criptografia assimétrica é implementada usando criptografia de chave pública, na qual uma mensagem criptografada com uma chave pública do sujeito pode ser descriptografada somente por um receptor possuindo a correspondente chave privada. Entretanto, a criptografia assimétrica é geralmente muito lenta para aplicações em tempo real, tais como aplicações de fluxo contínuo ["streaming"] ou reuniões virtuais, onde as operações de criptografia e descriptografia necessitam ser executadas com pouca latência ou latência não percebível.

A criptografia simétrica é implementada usando uma única chave secreta compartilhada entre usuários para criptografia e descriptografia. A criptografia simétrica é geralmente mais rápida do que a criptografia assimétrica o que torna a criptografia simétrica mais bem adequada para aplicações em tempo real e outras

aplicações onde latência mínima é desejada. Entretanto, dificuldades podem surgir com a distribuição e redistribuição segura da chave secreta para os usuários. Devido às chaves secretas serem usadas tanto para criptografia quanto descriptografia, as chaves secretas são geralmente distribuídas antes de iniciar as comunicações entre dois ou mais usuários. As chaves secretas também podem necessitar ser geradas e distribuídas novamente por um número de razões. Em um exemplo, uma falha de hardware em um ou mais nós (p.ex., resultando em uma substituição por outro hardware em stand-by ["failover"] para um sistema redundante) pode requerer redistribuir a chave secreta. Em outro exemplo, quando um usuário é removido de um evento, a chave secreta pode necessitar ser gerada e distribuída novamente para os usuários remanescentes para impedir o usuário que saiu de acessos adicionais. A distribuição e redistribuição segura de chaves secretas pode ser difícil quando os usuários estão geograficamente dispersos. Adicionalmente, para certas aplicações, a distribuição e redistribuição segura de chaves secretas pode necessitar ser sem emendas, provocando interrupção mínima para as comunicações e requerendo intervenção mínima a partir dos usuários finais.

Por estas e outras razões, existe uma necessidade da presente invenção.

Sumário

Uma configuração provê um sistema para distribuir informações de configuração de nó para uma pluralidade de nós em um evento. O sistema inclui um primeiro nó, um segundo nó conectado operativamente ao primeiro nó, e um gerenciador de eventos conectado operativamente ao primeiro nó e ao segundo nó. O gerenciador de eventos transmite as informações de configuração de nó para o primeiro nó e o segundo nó e transmite uma indicação para o primeiro nó e o segundo nó para iniciar comunicação entre o primeiro nó e o segundo nó usando as informações

de configuração de nó.

Descrição resumida dos desenhos

Os desenhos anexos são incluídos para fornecer uma compreensão adicional da presente invenção e são incorporados em e constituem uma parte de esta especificação. Os desenhos ilustram as configurações da presente invenção e juntos com a descrição servem para explicar os princípios da invenção. Outras configurações da presente invenção e muitas das vantagens pretendidas da presente invenção serão prontamente apreciadas à medida que elas se tornem mais bem entendidas por referência à descrição detalhada seguinte. Os elementos dos desenhos não estão necessariamente em escala entre si. Numerais de referência iguais designam partes similares correspondentes.

A figura 1 ilustra um diagrama de blocos de um sistema de gerenciamento de chave, baseado em nó;

A figura 2 ilustra um diagrama de blocos de um sistema de distribuição de chave simétrica, baseado em extração utilizando um servidor central;

As figuras 3A e 3B ilustram diagramas de blocos de um sistema de distribuição de chave simétrica baseado em forçamento utilizando um gerenciador de eventos, de acordo com uma configuração;

A figura 4 ilustra um diagrama de uma sequência exemplar de operações nas quais um gerenciador de eventos distribui uma chave simétrica para um primeiro nó e um segundo nó, de acordo com uma configuração; e

A figura 5 ilustra um diagrama de fluxo de um método para distribuir uma chave simétrica para um primeiro nó e um segundo nó, de acordo com uma configuração.

Descrição detalhada

Na Descrição Detalhada seguinte, referência é feita aos desenhos anexos os quais formam uma parte desta, e nos quais são mostradas por meio de ilustração configurações específicas nas quais a invenção pode ser praticada. A este respeito, terminologia direcional, tal como

"superior", "inferior", "frente", "traseira", "guia", "seguidora", etc. é usada com referência à orientação da(s) figura(s) sendo descrita(s). Devido a componentes de configurações da presente invenção poderem ser posicionados em um número de orientações diferentes, a terminologia direcional é usada com propósitos de ilustração e não de modo limitante. Deve ser entendido que outras configurações podem ser utilizadas e mudanças estruturais ou lógicas podem ser feitas sem se desviar do escopo da presente invenção. A descrição detalhada seguinte, portanto, não deve ser tomada em um sentido limitante, e o escopo da presente invenção é definido pelas reivindicações anexas.

Como usado aqui, o termo "mídia" inclui texto, áudio, vídeo, sons, imagens, ou outros dados digitais adequados capazes de serem transmitidos através de uma rede.

Como usado aqui, o termo "dispositivo de nó" inclui dispositivos baseados em processador, dispositivos de entrada/saída, ou outros dispositivos adequados para facilitar comunicações entre usuários remotos. Exemplos de dispositivos de nós incluem máquinas de fax, câmeras de vídeo, telefones, impressoras, scanners, displays, computadores pessoais, microfones, e alto-falantes.

Como usado aqui, o termo "nó" inclui qualquer ambiente ou sistema adequado configurado para transmitir e/ou receber mídia através de um ou mais dispositivos de nós. Em uma configuração, o ambiente é um ambiente colaborativo, o qual permite usuários remotos compartilharem mídia através de um ou mais dispositivos de nós. Um ambiente colaborativo permitirá, por exemplo, um apresentador proporcionar simultaneamente uma apresentação multimídia para uma audiência não somente no local do apresentador, mas também em um ou mais locais remotos. O ambiente colaborativo pode permitir adicionalmente a audiência nos locais remotos participar da apresentação como a audiência no local do apresentador participaria (p.ex., fazer perguntas ao apresentador).

Como usado aqui, o termo "evento" se refere a uma conexão de uma pluralidade de nós tal que um ou mais dispositivos de nós de um nó sejam configurados para transmitir mídia para e/ou receber mídia de um ou mais dispositivos de nós de um outro nó.

Como usado aqui, o termo "topologia" se refere a um evento e sua respectiva configuração, estado, e relacionamento com outros sistemas associados com o evento. Uma topologia exemplar de evento pode incluir um gerenciador de eventos, uma pluralidade de nós, e um ou mais relacionamentos entre o gerenciador de eventos e a pluralidade de nós. Para o bem da simplicidade, a topologia de evento descrita aqui inclui geralmente somente dois nós. Deve ser apreciado que um evento pode incluir qualquer número de nós como contemplado por aqueles experientes na técnica.

Como usado aqui, o termo "informações de configuração de nó" se refere a qualquer informação adequada utilizada para configurar um nó antes do nó transmitir e receber mídia. Em uma configuração, as informações de configuração de nó são uma chave simétrica distribuída para um nó para criptografar mídia antes da transmissão e descriptografar mídia com a recepção. Em um exemplo, a informação de topologia pode ser um ou mais endereços de rede distribuídos para um nó estabelecendo um ou mais fluxos de comunicação para transmitir mídia. Em um outro exemplo, a informação de topologia pode indicar que o ambiente em um nó durante um evento necessita ser ajustado (p.ex., esmaecer a iluminação dentro do nó) de acordo com uma política do nó.

As configurações de um sistema e método para distribuir informações de configuração de nó são descritas aqui. As configurações incluem um processo atômico de duas etapas para distribuir informações de configuração de nó. Como um processo atômico, múltiplas operações são executadas ainda que operando como uma operação. Para fins de simplicidade, as configurações descritas aqui se referem

à distribuição de uma chave simétrica. Será apreciado, entretanto, que alguém de experiência ordinária na técnica reconhecerá que outras informações de configuração de nó podem ser distribuídas em vista das configurações descritas aqui.

A figura 1 ilustra um diagrama de blocos e um sistema de gerenciamento de chave baseado em nós 100 incluindo um primeiro nó 102a conectado operativamente a um segundo nó 102b (coletivamente referidos como nós 102). Sob o sistema baseado em nós 100, cada um de o primeiro nó 102a e o segundo nó 102b mantém e negocia uma chave simétrica via a rede 104. Comunicações seguras (p.ex., compartilhamento de mídia) através dos nós 102 só são iniciadas após os nós 102 terem negociado uma chave simétrica. Um exemplo de um sistema baseado em nós é Segurança IP (isto é, IPsec ou RFC 2401).

A figura 2 ilustra um diagrama de blocos de um sistema de distribuição de chave simétrica baseado em extração 110 utilizando um servidor central 112. O servidor central 112 está conectado operativamente a um primeiro nó 114a e um segundo nó 114b (referidos coletivamente como nós 114). O primeiro nó 114a e o segundo nó 114b também estão conectados operativamente.

Sob o sistema baseado em extração 110, o primeiro nó 114a e o segundo nó 114b obtêm ativamente uma chave simétrica a partir do servidor central 112 via as redes 116a e 116b, respectivamente. Em outras palavras, o servidor central 112 não envia a chave simétrica para o primeiro nó 114a ou segundo nó 114b até que solicitado pelo primeiro nó 114a e segundo nó 114b, respectivamente. O primeiro nó 114a e o segundo nó 114b se comunicam (p.ex., compartilham mídia) entre si via a rede 116c após obterem a chave simétrica do servidor central 112. Um exemplo de um sistema baseado em extração é a Arquitetura de Segurança de Grupo de Multidifusão (isto é, RFC 3740).

O sistema baseado em nós 100 e o sistema baseado em extração 110 requer que cada um dos nós 102 e 104

gerencie suas necessidades individuais para negociar ou adquirir a chave simétrica, o que pode resultar em um número de problemas potenciais. Em um exemplo, um nó pode não estar ciente de certas falhas de hardware, sejam do próprio nó ou de um outro nó, que requerem a regeração e/ou redistribuição de chaves. O nó com falha se tornaria efetivamente não operante uma vez que ele pode não saber solicitar uma nova chave.

Em um outro exemplo, se uma política controlando quando solicitar uma nova chave muda (p.ex., quando mudar a chave quando um nó sai de um evento), a política teria que ser alterada para cada nó envolvido. Dependendo do número de nós, a mudança de política para cada nó pode ser indevidamente demorada. Em adição, requerer que cada nó gerencie políticas pode ser computacionalmente intensivo. Adicionalmente, um número de protocolos de segurança, tais como IPsec e Protocolo de Transporte em Tempo Real Seguro (SRTP), provêem pouca ou nenhuma flexibilidade com políticas, especificando, por exemplo, que chaves simétricas podem ser regeradas somente após um número específico de pacotes de rede terem sido enviados.

Configurações de um sistema e método para distribuir uma chave simétrica para uma pluralidade de nós serão agora descritas. Em uma configuração, o sistema e método utiliza um sistema de distribuição de chave simétrica baseado em extração no qual um gerenciador de chave, central, como uma configuração de um gerenciador de eventos, distribui a chave simétrica para os nós sem solicitação dos nós. O sistema baseado em extração permite o gerenciador de chaves monitorar globalmente as falhas e outras ocorrências de cada e todo nó que requeira a regeração e redistribuição de chaves. Adicionalmente, o sistema baseado em extração permite a implementação de políticas flexíveis governando as chaves provendo um ponto central no qual implementa políticas.

A figura 3A ilustra um diagrama de blocos de um sistema de distribuição de chave simétrica baseado em extração

120 utilizando um gerenciador de eventos 122, de acordo com uma configuração. O gerenciador de eventos 122 está operativamente conectado a um primeiro nó 124a e um segundo nó 124b (coletivamente referidos como nós 124). O primeiro nó 124a e o segundo nó 124b também estão conectados operativamente.

Sob o sistema baseado em extração 120, o gerenciador de eventos 122 administra a distribuição de chaves para os nós 124 via as redes 126a e 126b. Os nós 124 não são requeridos a solicitar as chaves simétricas e, em uma configuração, os nós 124 preferivelmente não estão envolvidos com a distribuição de chave. Assim, o sistema baseado em extração 120 libera os nós de responsabilidades administrativas com relação à distribuição de chave. O gerenciador de eventos 122 é responsável por monitorar a topologia global do evento e por gerenciar a distribuição de chave consequentemente. Adicionalmente, o sistema baseado em extração 120 permite o uso de políticas flexíveis com relação à geração, regeneração, distribuição, e redistribuição de chaves simétricas.

O sistema baseado em extração 120 reforça um processo atômico de duas etapas relacionado com a distribuição de chave. Na primeira etapa, uma chave simétrica é distribuída para cada um de o primeiro nó 124a e o segundo nó 124b. Na segunda etapa, comunicações (p.ex., compartilhamento de mídia) entre o primeiro nó 124a e o segundo nó 124b via a rede 126c são inicializadas. A atomicidade do processo de duas etapas significa que ambas as etapas são efetivamente vistas e observadas como uma operação única embora duas etapas separadas estejam envolvidas. Em uma configuração, o processo em duas etapas é modelado baseado em um protocolo de comprometimento de duas fases, como aplicado a sistemas distribuídos transativos.

Em uma configuração, o gerenciador de eventos 122 recebe do primeiro nó 124a e segundo nó 124b dados relacionados

com a participação pelo primeiro nó 124a e segundo nó 124b, respectivamente, em um evento. Em resposta ao recebimento dos dados do primeiro nó 124a e do segundo nó 124b, o gerenciador de eventos 122 gera e distribui a chave simétrica correta baseado em uma política. Exemplos de dados enviados a partir dos nós 124 para o gerenciador de eventos podem incluir a notificação para participar em um evento e a maneira na qual os nós 124 desejam participar no evento. Em uma configuração, o gerenciador de eventos 122 envia informações adicionais relacionadas com a execução do evento entre os nós 124. Tais informações podem incluir qualquer informação de comunicação adequada, tal como o protocolo de rede (p.ex., protocolo de transferência em tempo real), endereços da rede de dispositivos de nós, e portas.

Em uma configuração, como ilustrado na figura 3B, cada um de o primeiro nó 124a e o segundo nó 124b envia notificação para o gerenciador de eventos 122 para enviar e receber mídia para e de um terceiro nó 124c. O gerenciador de eventos 122 determina as chaves simétricas a serem enviadas para o primeiro nó 124a, segundo nó 124b, e terceiro nó 124c baseado em uma política. A política pode indicar, por exemplo, que as comunicações entre o primeiro nó 124a e terceiro nó 124c utilizem uma chave simétrica diferente do que entre o segundo nó 124b e terceiro nó 124c. Sob esta política, uma primeira chave simétrica é enviada para o primeiro nó 124a e terceiro nó 124c junto com informações indicando que a primeira chave simétrica é para comunicações entre o primeiro nó 124a e o terceiro nó 124c. Uma segunda chave simétrica, a qual é diferente da primeira chave simétrica, é enviada para o segundo nó 124b e terceiro nó 124c junto com informações indicando que a segunda chave simétrica é para comunicações entre o segundo nó 124b e o terceiro nó 124c. O primeiro nó 124a, segundo nó 124b, e terceiro nó 124c não estão relacionados com a política, a qual é mantida pelo gerenciador de eventos 122.

Em outra configuração, a política especifica que uma primeira chave simétrica seja usada para um primeiro fluxo de comunicação entre o primeiro nó 124a e segundo nó 124b, e uma segunda chave simétrica seja usada para um segundo fluxo de comunicação entre o primeiro nó 124a e o segundo nó 124b. Em uma outra configuração, a política especifica que uma primeira chave simétrica seja usada para comunicação do primeiro nó 124a com o segundo nó 124b, e uma segunda chave simétrica seja usada para comunicação do segundo nó 124b com o primeiro nó 124a. Em outra configuração, a política especifica a geração de uma nova chave simétrica e transmissão da nova chave simétrica para um ou mais dos nós 124 em resposta a uma dada duração de tempo decorrer. Em uma outra configuração, a política especifica a geração de uma nova chave simétrica e transmissão da nova chave simétrica para um ou mais dos nós 124 em resposta a informações atualizadas de nó a partir de um ou mais dos nós 124. Um exemplo de informações atualizadas de nó são informações com relação à falha de hardware em um ou mais dos nós 124.

Em outra configuração, a política especifica a geração de uma nova chave simétrica e transmissão da nova chave simétrica para um ou mais dos nós 124 em resposta a um novo nó se juntar ao evento. Em uma outra configuração, a política especifica a geração de uma nova chave simétrica e a transmissão da nova chave simétrica para um ou mais dos nós 124 em resposta a um nó existente sair do evento. Portanto, a chave simétrica é regerada e redistribuída em resposta a um novo nó se juntar ao evento ou a um nó existente sair do evento. Uma solicitação para se juntar ao evento e/ou deixar o evento pode ser recebida de ou originada de um ou mais dos nós 124, bem como, a partir de uma aplicação de programador (p.ex., quando um disparo programado para "atualizar a segurança" chegar) ou uma aplicação suporte usada por um Conselheiro (p.ex., quando uma pessoa chama para solicitar um alívio de segurança).

Em outras configurações, a política especifica quaisquer regras adequadas para gerar, regerar, distribuir, e redistribuir chaves simétricas.

De acordo com o processo atômico de duas etapas descrito anteriormente, após o gerenciador de eventos 122 enviar as chaves simétricas apropriadas para os nós 124 baseado na política e informações de nós, o gerenciador de eventos 122 instrui cada um dos nós 124 para começar comunicações usando as chaves simétricas. Assim, as chaves simétricas permitem os nós 124 se comunicarem seguramente entre si.

A figura 4 ilustra um diagrama de uma sequência exemplar 140 de operações nas quais o gerenciador de eventos 122 distribui uma chave simétrica para um primeiro nó 124a e um segundo nó 124b, de acordo com uma configuração. A figura 5 ilustra um diagrama de fluxo de um método 160 para distribuir uma chave simétrica para um primeiro nó 124a e um segundo nó 124b, de acordo com uma configuração. Referência será feita agora às figuras 4 e 5.

Em uma configuração, o primeiro nó 124a experimenta uma falha (em 142) em um pipeline de comunicações com o segundo nó 124b. Em uma configuração, quando um pipeline de comunicações falha no primeiro nó 124a, o primeiro nó 124a executa uma substituição por outro hardware em stand-by para um sistema redundante. Em uma configuração, uma política imposta pelo gerenciador de eventos 122 requer que o gerenciador de eventos 122 regere e redistribua uma chave simétrica para o primeiro nó 124a e segundo nó 124b quando o primeiro nó 124a executar substituição por outro hardware em stand-by para um sistema redundante.

Em uma configuração, o gerenciador de eventos 122 recebe (em 144) informações de falha a partir do primeiro nó 124a. As informações de falha incluem uma notificação de que o primeiro nó 124a experimenta uma falha. As informações de falha podem incluir adicionalmente

qualquer informação adequada relacionada com o primeiro nó 124a, tal como as capacidades correntes do primeiro nó 124a (isto é, as capacidades do primeiro nó 124a após a falha) para participar em um evento.

Em uma configuração, o gerenciador de eventos 122 envia (em 146) as primeiras informações de topologia para o primeiro nó 124a. As primeiras informações de topologia incluem uma chave simétrica para comunicações com um segundo nó 124b. Em uma configuração, a chave simétrica é determinada baseada nas informações de falha. As primeiras informações de topologia podem incluir adicionalmente qualquer informação de comunicação adequada para comunicações entre o primeiro nó 124a e um segundo nó 124b, tal como o protocolo de rede, endereços da rede de dispositivos de nós, e portas.

Em uma configuração, o gerenciador de eventos 122 recebe (em 148) do primeiro nó 124a uma confirmação (ACK) indicando que o primeiro nó 124a recebeu as primeiras informações de topologia.

Em uma configuração, o gerenciador de eventos 122 envia (em 150) segundas informações de topologia para o segundo nó 124b. As segundas informações de topologia podem ou não ser as mesmas que as primeiras informações de topologia. As segundas informações de topologia incluem a chave simétrica também enviada para o primeiro nó 124 através das primeiras informações de topologia. As segundas informações de topologia podem incluir adicionalmente qualquer informação adequada relacionada com comunicações entre o primeiro nó 124a e o segundo nó 124b, tal como o protocolo de rede, endereços da rede de dispositivos de nós, e portas.

Em uma configuração, o gerenciador de eventos 122 recebe (em 152) do segundo nó 124b uma confirmação (ACK) indicando que o segundo nó 124b recebeu as segundas informações de topologia.

Em uma configuração, o gerenciador de eventos 122 envia (em 154) notificação para o primeiro nó 124a para iniciar

comunicações com o segundo nó 124b. O gerenciador de eventos 122 também envia (em 156) notificação para o segundo nó 124b iniciar comunicações com o primeiro nó 124a. Depois disto, um evento começa, e mídia é transferida seguramente (em 158) entre o primeiro nó 124a e o segundo nó 124b usando a chave simétrica para criptografar e descriptografar comunicações. Em uma configuração, mídia não é transferida entre o primeiro nó 124a e o segundo nó 124b até que o processo atômico de duas etapas para distribuir a chave simétrica (isto é, etapas 146 a 152) e iniciar as comunicações (isto é, etapas 154 a 156) esteja completado.

Para garantir o processo atômico de duas etapas como descrito anteriormente, uma ou mais políticas podem ser implementadas para levar em conta uma falha em qualquer das etapas 146 a 156. Em uma configuração, a falha de qualquer das etapas 146 a 156 resulta em uma sequência de "retrocesso" na qual quaisquer etapas antes da etapa que falhou são desfeitas para um estado anterior ou inicial. Em uma configuração, as etapas 146 a 156 são re-executadas até que a chave simétrica seja distribuída com sucesso. Em outra configuração, o evento ou a comunicação pretendida entre os nós 124 é terminado. Em uma outra configuração, a comunicação pretendida entre os nós 124 continua não criptografada.

Em uma configuração, as informações de falha são incluídas em uma intenção priorizada, como divulgado no pedido de patente referenciado acima de série n° 11/497886 intitulado "System and Method for Managing Virtual Collaboration Systems" [Sistema e método para gerenciar sistemas virtuais de colaboração]. Em uma configuração as primeiras informações de topologia e as segundas informações de topologia são incluídas em uma intenção selecionada, como divulgado no pedido de patente referenciado acima de série n° 11/497886 intitulado "System and Method for Managing Virtual Collaboration Systems". Em uma configuração, a funcionalidade do

gerenciador de eventos 122 é dividida em um gerenciador de eventos e um foco de evento, como divulgado no pedido de patente referenciado acima de série nº 11/497886 intitulado "System and Method for Managing Virtual Collaboration Systems".

As configurações descritas e ilustradas com referência às figuras provêem sistemas e métodos para distribuir informações de configuração de nó. Também deve ser entendido que nem todos os componentes e/ou etapas descritos e ilustrados com referência às figuras são requeridos para todas as configurações. Em uma configuração, um ou mais dos métodos ilustrativos são implementados preferivelmente como uma aplicação compreendendo instruções de programa que são tangivelmente configuradas em um ou mais dispositivos de armazenagem de programa (p.ex., disco rígido, disco flexível magnético, RAM, ROM, CD ROM, etc.) e executáveis por qualquer dispositivo ou máquina compreendendo arquitetura adequada, tal como um computador digital para propósitos gerais tendo um processador, memória, e interfaces de entrada/saída.

Embora configurações específicas tenham sido ilustradas e descritas aqui, será apreciado por aqueles experientes na técnica que uma variedade de implementações alternativas e/ou equivalentes podem ser substitutas para as configurações específicas mostradas e descritas sem se desviar do escopo da presente invenção. Este pedido de patente é intencionado a cobrir quaisquer adaptações ou variações das configurações específicas discutidas aqui. Portanto, é intencionado que esta invenção seja limitada somente pelas reivindicações e equivalentes das mesmas.

REIVINDICAÇÕES

1. Sistema para distribuir informações de configuração de nó para uma pluralidade de nós em um evento, caracterizado pelo fato de compreender:

um primeiro nó;

um segundo nó conectado operativamente ao primeiro nó; e

um gerenciador de eventos conectado operativamente ao primeiro nó e ao segundo nó, sendo que o gerenciador de eventos transmite as informações de configuração de nó para o primeiro nó e o segundo nó, e transmite uma indicação para o primeiro nó e o segundo nó para iniciar comunicações entre o primeiro nó e o segundo nó usando as informações de configuração de nó.

2. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de as comunicações entre o primeiro nó e o segundo nó serem iniciadas somente após o gerenciador de eventos transmitir com sucesso as informações de configuração de nó e a indicação para o primeiro nó e o segundo nó.

3. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de o gerenciador de eventos gerar as informações de configuração de nó.

4. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de as informações de configuração de nó incluírem uma chave simétrica.

5. Sistema, de acordo com a reivindicação 4, caracterizado pelo fato de a comunicação entre o primeiro nó e o segundo nó ser iniciada somente após o gerenciador de eventos transmitir com sucesso tanto a chave simétrica quanto a indicação para o primeiro nó e o segundo nó.

6. Sistema, de acordo com a reivindicação 4, caracterizado pelo fato de o gerenciador de eventos gerar a chave simétrica e transmitir a chave simétrica para o primeiro nó e o segundo nó de acordo com uma política.

7. Sistema, de acordo com a reivindicação 6, caracterizado pelo fato de a política especificar que uma primeira chave simétrica seja usada para comunicação

entre o primeiro nó e o segundo nó, e uma segunda chave simétrica seja usada para comunicação entre o segundo nó e o terceiro nó.

8. Sistema, de acordo com a reivindicação 6, caracterizado pelo fato de a política especificar que uma primeira chave simétrica seja usada para um primeiro fluxo de comunicação entre o primeiro nó e o segundo nó, e uma segunda chave simétrica seja usada para um segundo fluxo de comunicação entre o primeiro nó e o segundo nó.

9. Sistema, de acordo com a reivindicação 6, caracterizado pelo fato de a política especificar que uma primeira chave simétrica seja usada para comunicação do primeiro nó com o segundo nó, e uma segunda chave simétrica seja usada para comunicação do segundo nó com o primeiro nó.

10. Sistema, de acordo com a reivindicação 6, caracterizado pelo fato de a política especificar que uma nova chave simétrica seja gerada e transmitida para o primeiro nó e o segundo nó em resposta a pelo menos um de uma dada duração de tempo passar e receber informações de nó atualizadas de um de o primeiro nó e o segundo nó.

11. Sistema, de acordo com a reivindicação 10, caracterizado pelo fato de as informações de nó atualizadas serem informações com relação à falha de hardware.

12. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de compreender adicionalmente:
um terceiro nó,
sendo que o gerenciador de eventos gera uma nova chave simétrica e transmite a nova chave simétrica para pelo menos dois de o primeiro nó, o segundo nó, e o terceiro nó em resposta a receber pelo menos uma de uma solicitação para se juntar ao evento e uma solicitação para deixar o evento.

13. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de as informações de configuração de nó incluírem informações de topologia.

14. Sistema, de acordo com a reivindicação 13, caracterizado pelo fato de as informações de topologia compreenderem pelo menos um de um protocolo de rede, um endereço de rede de um dispositivo de nó, e uma porta associada com a comunicação entre o primeiro nó e o segundo nó.

15. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de o primeiro nó e o segundo nó estarem geograficamente dispersos.

16. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de a comunicação entre o primeiro nó e o segundo nó compreender compartilhar mídia.

17. Sistema, de acordo com a reivindicação 1, caracterizado pelo fato de o gerenciador de eventos gerar as informações de configuração de nó sem solicitação a partir de um de o primeiro nó e o segundo nó, transmitir as informações de configuração de nó para o primeiro nó e o segundo nó sem solicitação a partir de um de o primeiro nó e o segundo nó, e transmitir a indicação para o primeiro nó e o segundo nó sem solicitação a partir de um de o primeiro nó e o segundo nó.

18. Método para distribuir informações de configuração de nó para uma pluralidade de nós em um evento, caracterizado pelo fato de compreender:

transmitir as informações de configuração de nó para um primeiro nó;

receber confirmação do primeiro nó de que o primeiro nó recebeu as informações de configuração de nó;

transmitir as informações de configuração de nó para um segundo nó;

receber uma confirmação do segundo nó de que o segundo nó recebeu as informações de configuração de nó; e

transmitir uma indicação para o primeiro nó e o segundo nó para iniciar comunicações entre o primeiro nó e o segundo nó usando as informações de configuração de nó.

19. Método, de acordo com a reivindicação 18, caracterizado pelo fato de compreender adicionalmente:

transmitir as informações de configuração de nó para o primeiro nó e o segundo nó em resposta a receber informações de falha a partir do primeiro nó.

20. Método, de acordo com a reivindicação 19, caracterizado pelo fato de as informações de falha compreenderem notificação de que pelo menos uma porção do primeiro nó falhou, e uma capacidade corrente do primeiro nó.

21. Método, de acordo com a reivindicação 18, caracterizado pelo fato de compreender adicionalmente: transmitir as informações de configuração de nó para o primeiro nó e o segundo nó em resposta a receber pelo menos uma de uma solicitação para se juntar ao evento e uma solicitação para sair do evento.

22. Método, de acordo com a reivindicação 18, caracterizado pelo fato de as informações de configuração de nó incluírem informações de topologia.

23. Método, de acordo com a reivindicação 22, caracterizado pelo fato de as informações de topologia compreenderem pelo menos um de um protocolo de rede, um endereço de rede de um dispositivo de nó, e uma porta associada com a comunicação entre o primeiro nó e o segundo nó.

24. Método, de acordo com a reivindicação 18, caracterizado pelo fato de as informações de configuração de nó incluírem uma chave simétrica.

25. Método, de acordo com a reivindicação 24, caracterizado pelo fato de compreender adicionalmente: iniciar a comunicação entre o primeiro nó e o segundo nó somente após transmitir com sucesso tanto a chave simétrica quanto a indicação para o primeiro nó e o segundo nó.

26. Método, de acordo com a reivindicação 24, caracterizado pelo fato de compreender adicionalmente: gerar a chave simétrica baseado em uma política.

27. Método, de acordo com a reivindicação 26, caracterizado pelo fato de a política especificar usar

uma primeira chave simétrica para a comunicação entre o primeiro nó e o segundo nó e usar uma segunda chave simétrica para comunicação entre o segundo nó e um terceiro nó.

28. Método, de acordo com a reivindicação 26, caracterizado pelo fato de a política especificar usar uma primeira chave simétrica para um primeiro fluxo de comunicação entre o primeiro nó e o segundo nó, e usar uma segunda chave simétrica para um segundo fluxo de comunicação entre o primeiro nó e o segundo nó.

29. Método, de acordo com a reivindicação 26, caracterizado pelo fato de a política especificar usar uma primeira chave simétrica para comunicação do primeiro nó com o segundo nó, e usar uma segunda chave simétrica para comunicação entre o segundo nó com o primeiro nó.

30. Método, de acordo com a reivindicação 26, caracterizado pelo fato de a política especificar uma nova chave simétrica e transmitir a nova chave simétrica para o primeiro nó e o segundo nó em resposta a pelo menos um de uma dada duração de tempo passar e receber informações de nó atualizadas de um de o primeiro nó e o segundo nó.

31. Método, de acordo com a reivindicação 30, caracterizado pelo fato de as informações de nó serem informações com relação a uma falha de hardware.

32. Método, de acordo com a reivindicação 26, caracterizado pelo fato de a política especificar gerar uma nova chave simétrica e transmitir a nova chave simétrica para pelo menos dois de o primeiro nó, o segundo nó, e um terceiro nó em resposta a receber pelo menos uma de uma solicitação para se juntar ao evento e uma solicitação para sair do evento.

33. Método, de acordo com a reivindicação 18, caracterizado pelo fato de a comunicação entre o primeiro nó e o segundo nó compreender compartilhar mídia.

34. Método, de acordo com a reivindicação 18, caracterizado pelo fato de o primeiro nó e o segundo nó

estarem geograficamente dispersos.

35. Método, de acordo com a reivindicação 18, caracterizado pelo fato de compreender adicionalmente:

gerar as informações de configuração de nó sem solicitação a partir de um de o primeiro nó e o segundo nó; e

transmitir as informações de configuração de nó sem solicitação a partir de um de o primeiro nó e o segundo nó.

36. Meio legível por máquina, tendo instruções armazenadas nele para execução por um processador para executar um método para distribuir informações de configuração de nó para uma pluralidade de nós em um evento, caracterizado pelo fato de o método compreender:

transmitir as informações de configuração de nó para um primeiro nó no evento;

receber confirmação do primeiro nó de que o primeiro nó recebeu as informações de configuração de nó;

transmitir as informações de configuração de nó para um segundo nó no evento;

receber confirmação do segundo nó de que o segundo nó recebeu as informações de configuração de nó; e

transmitir uma indicação para o primeiro nó e o segundo nó para iniciar comunicação entre o primeiro nó e o segundo nó usando as informações de configuração de nó, sendo que a comunicação entre o primeiro nó e o segundo nó é iniciada somente após transmitir com sucesso tanto as informações de configuração de nó quanto a indicação para o primeiro nó e o segundo nó.

37. Meio legível por máquina, de acordo com a reivindicação 36, caracterizado pelo fato de as informações de configuração de nó compreenderem pelo menos um de um protocolo de rede, um endereço de rede de um dispositivo de nó, e uma porta associada com a comunicação entre o primeiro nó e o segundo nó.

38. Meio legível por máquina, de acordo com a reivindicação 36, caracterizado pelo fato de as

informações de configuração de nó compreenderem uma chave simétrica.

39. Meio legível por máquina, de acordo com a reivindicação 38, caracterizado pelo fato de compreender adicionalmente:

gerar a chave simétrica e transmitir a chave simétrica para pelo menos dois de o primeiro nó, o segundo nó, e um terceiro nó em resposta a receber pelo menos uma de uma solicitação para se juntar ao evento e uma solicitação para sair do evento.

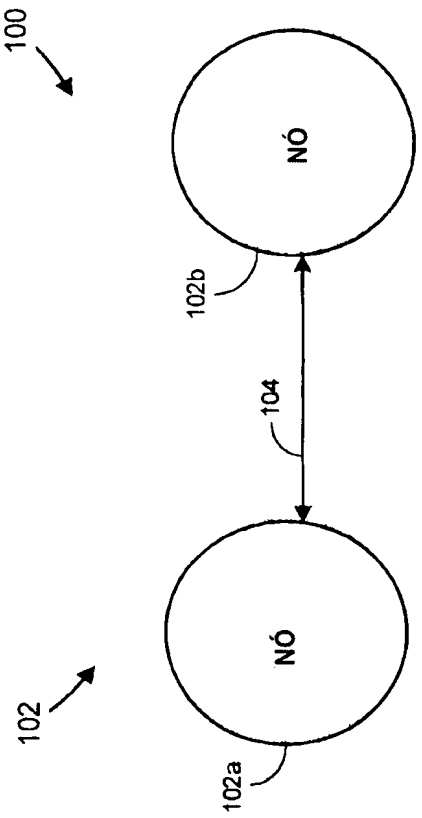

FIG.1
Técnica anterior

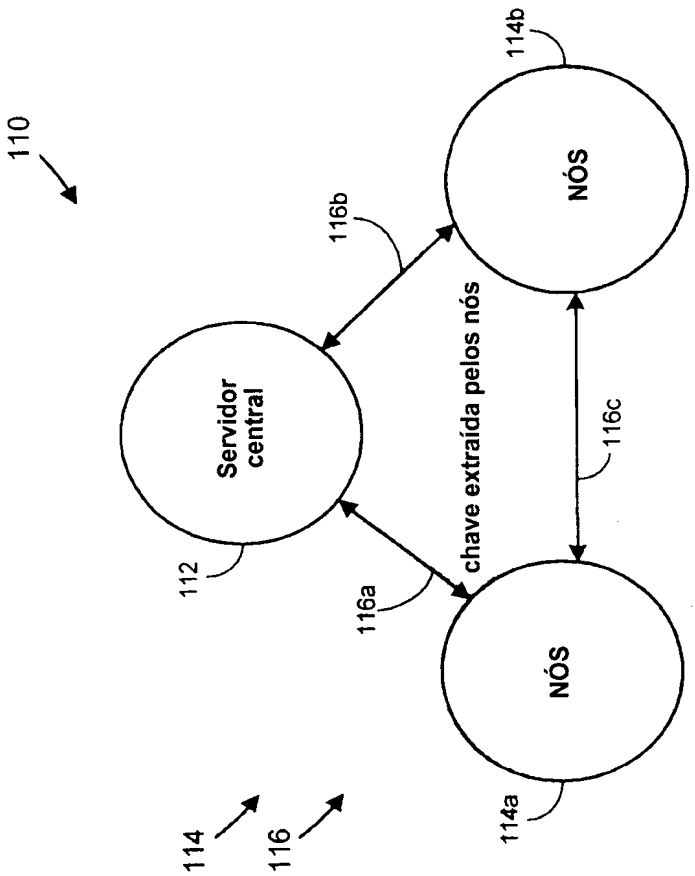

FIG.2
Técnica anterior

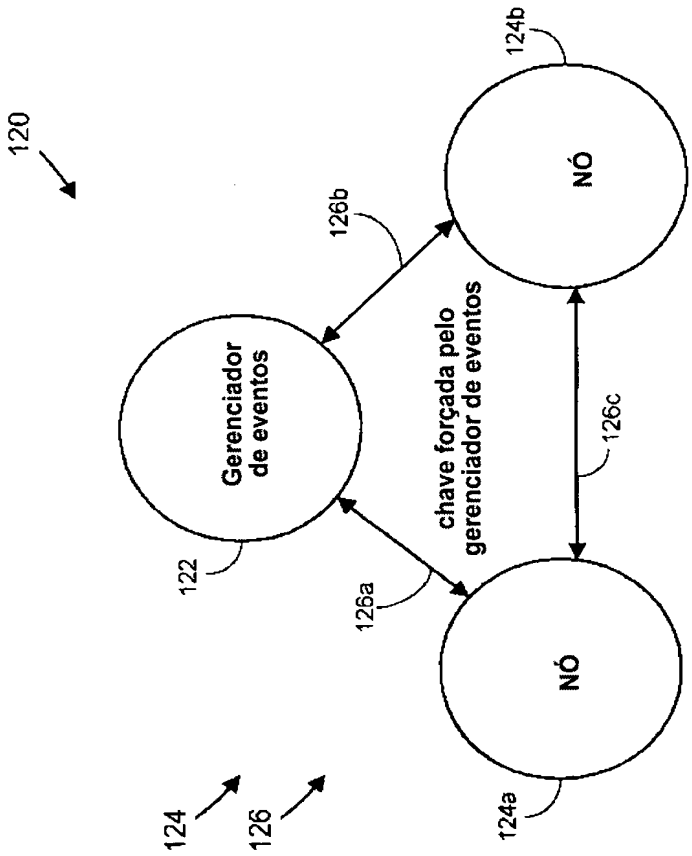
120
Gerenciador de eventos
122
NÓ
124a
NÓ
124b
126a
126b
126c
chave forçada pelo gerenciador de eventos
124
126

FIG.3A

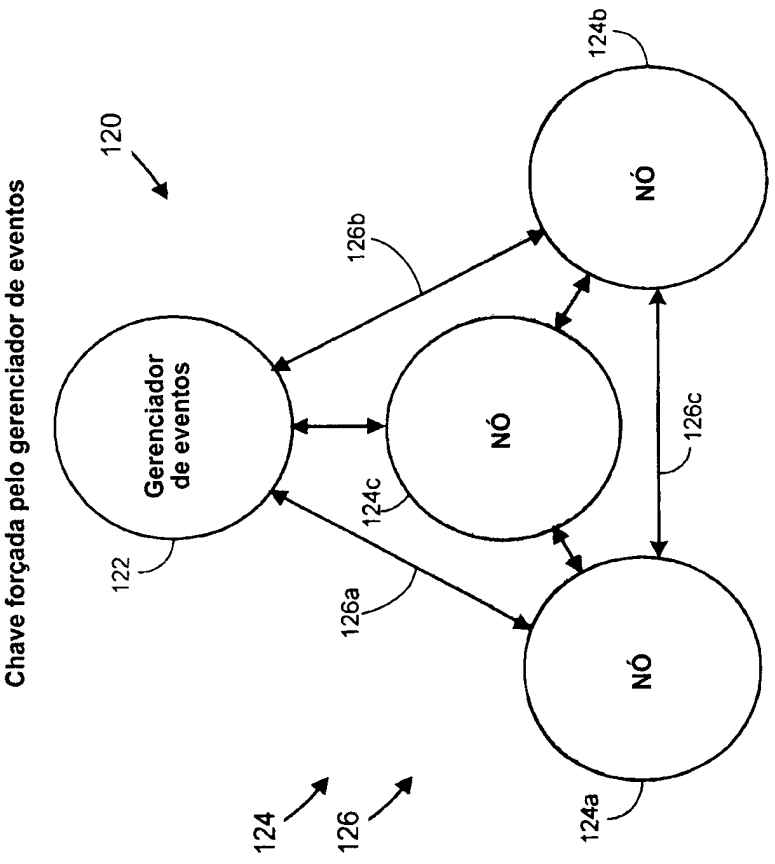
Chave forçada pelo gerenciador de eventos
120
Gerenciador de eventos
122
NÓ
124c
NÓ
124b
NÓ
124a
126a
126b
126c
124
126

FIG.3

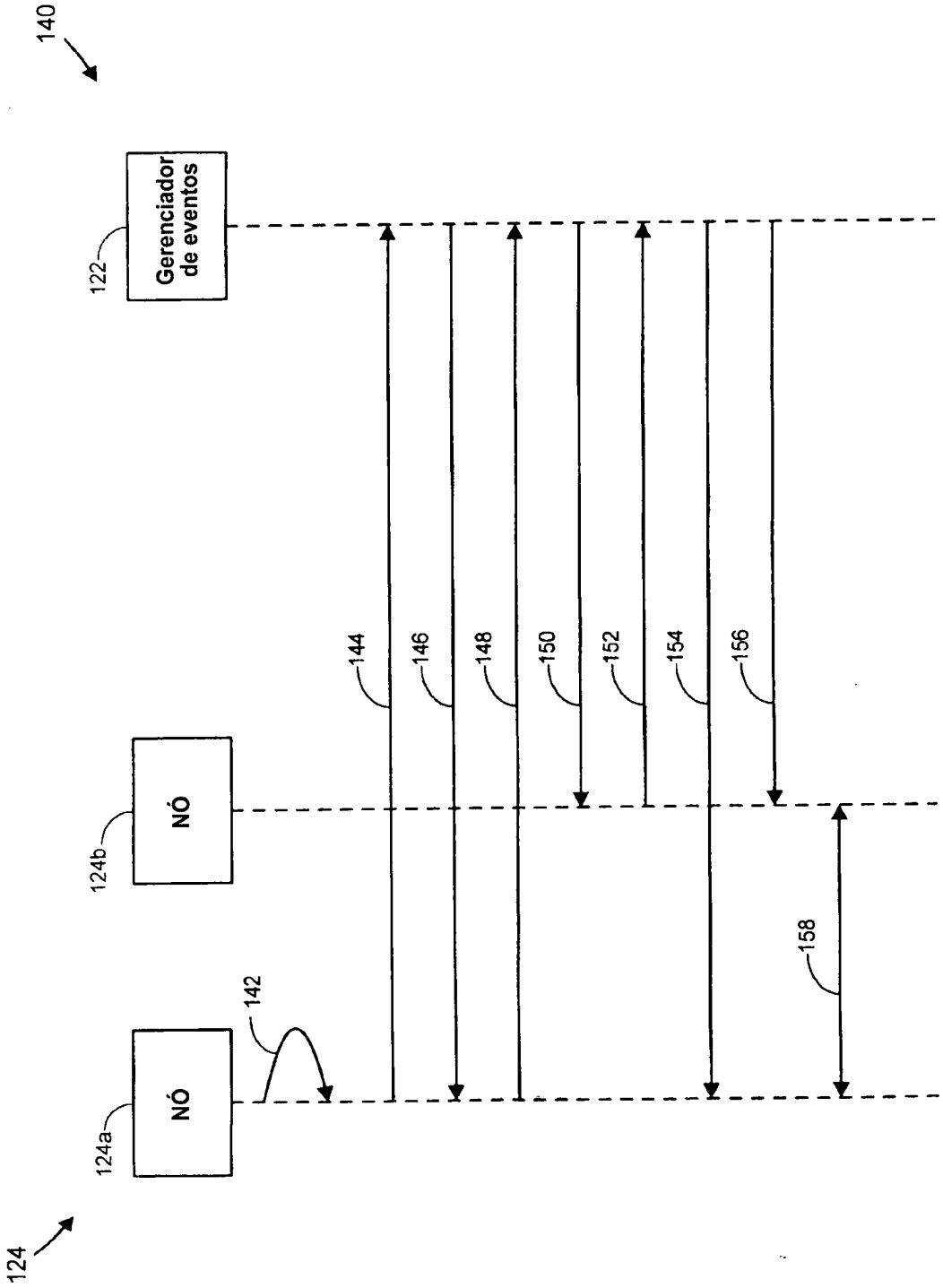
140
Gerenciador de eventos
122
NÓ
124b
NÓ
124a
124
142
144
146
148
150
152
154
156
158

FIG.4

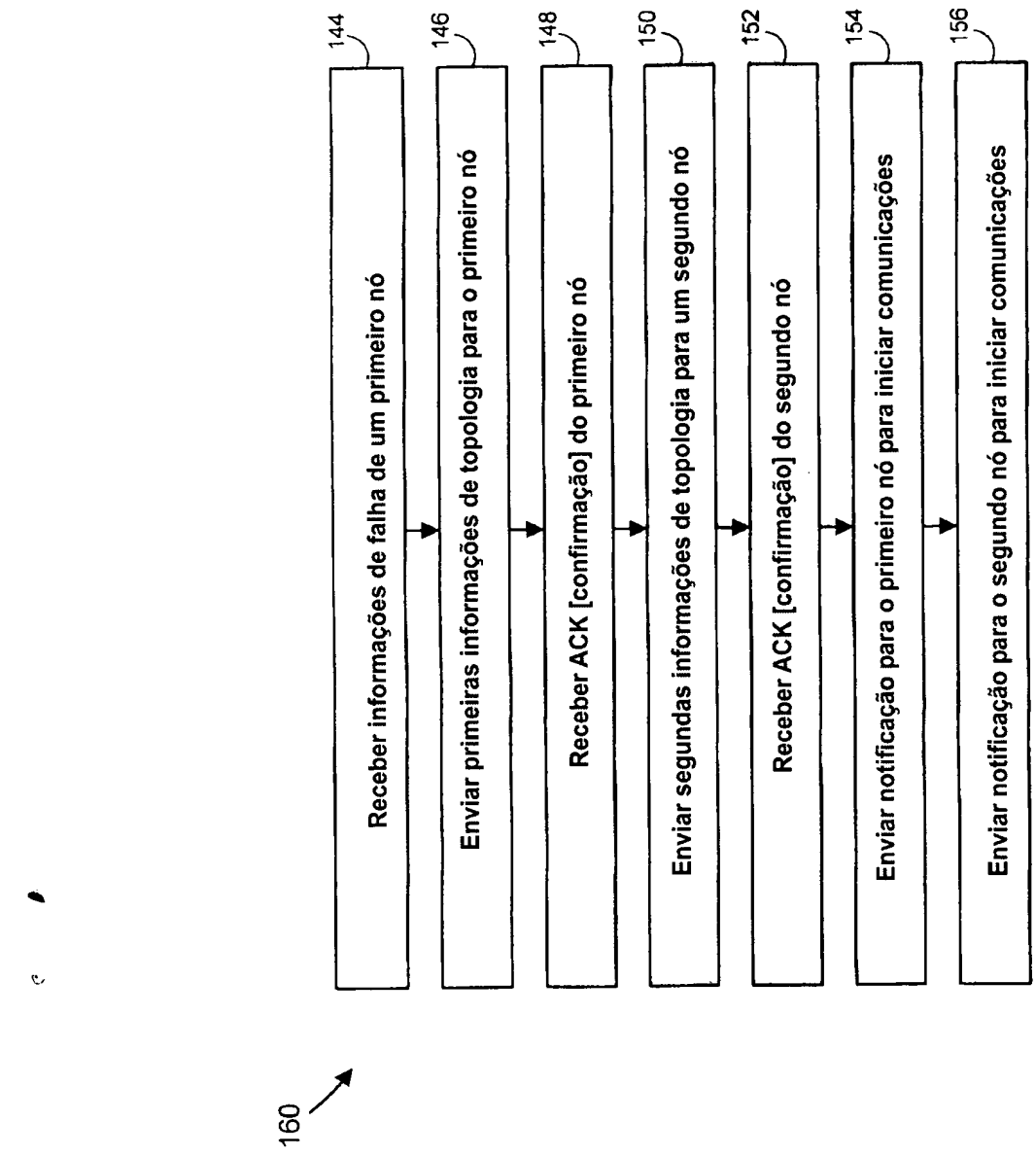
160
144
Receber informações de falha de um primeiro nó
146
Enviar primeiras informações de topologia para o primeiro nó
148
Receber ACK [confirmação] do primeiro nó
150
Enviar segundas informações de topologia para um segundo nó
152
Receber ACK [confirmação] do segundo nó
154
Enviar notificação para o primeiro nó para iniciar comunicações
156
Enviar notificação para o segundo nó para iniciar comunicações

FIG.5

RESUMO

"SISTEMA PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO, MÉTODO PARA DISTRIBUIR INFORMAÇÕES DE CONFIGURAÇÃO DE NÓ PARA UMA PLURALIDADE DE NÓS EM UM EVENTO E MEIO LEGÍVEL POR MÁQUINA".

Um sistema para distribuir informações de configuração de nó para uma pluralidade de nós em um evento é provido. O sistema inclui um primeiro nó, um segundo nó conectado operativamente ao primeiro nó, e um gerenciador de eventos conectado operativamente ao primeiro nó e ao segundo nó. O gerenciador de eventos transmite as informações de configuração de nó para o primeiro nó e o segundo nó, e transmite indicação para o primeiro nó e o segundo nó para iniciar comunicação entre o primeiro nó e o segundo nó usando as informações de configuração de nó.