



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

(11) BR 112013004510-8 B1



(22) Data do Depósito: 22/08/2011

(45) Data de Concessão: 13/10/2020

(54) Título: MÉTODO PARA SELECIONAR ADAPTATIVAMENTE REGRAS USADAS PARA CLASSIFICAR MENSAGENS ELETRÔNICAS E SISTEMA PARA SELECIONAR ADAPTATIVAMENTE REGRAS DE DETECÇÃO DE SPAM

(51) Int.Cl.: G06Q 50/00.

(30) Prioridade Unionista: 31/08/2010 US 12/872,691.

(73) Titular(es): MICROSOFT TECHNOLOGY LICENSING, LLC.

(72) Inventor(es): HANS CHRISTIAN ANDERSEN; ANATOLIY PANASYUK; VENKATA SOMANADHA SARMA REMANY; BART KUS.

(86) Pedido PCT: PCT US2011048664 de 22/08/2011

(87) Publicação PCT: WO 2012/030576 de 08/03/2012

(85) Data do Início da Fase Nacional: 26/02/2013

(57) Resumo: MÉTODO PARA SELECIONAR ADAPTATIVAMENTE REGRAS USADAS PARA CLASSIFICAR MENSAGENS ELETRÔNICAS E SISTEMA PARA SELECIONAR ADAPTATIVAMENTE REGRAS DE DETECÇÃO DE SPAM. A presente invenção refere-se a métodos (400), sistemas e produtos de programa de computador para selecionar adaptativamente regras de verredura de mensagem eletrônica. As modalidades da invenção se referem à variação dinâmica (potencial e não previsível) da profundidade/perfeição de classificação de mensagens eletrônicas para proteger contra conteúdo de mensagem indesejável (por exemplo, SPAM, vírus, vazamento digital, etc). Uma eficácia mínima é mantida e, quando os recursos disponíveis permitem, pode ser excedida para fornecer proteção aumentada. Um subconjunto ideal de regras de classificação de mensagem (121) disponíveis pode ser selecionado em um base por mensagem. A seleção de regras é baseada em recursos de sistema disponíveis, na eficácia desejada mínima (por exemplo, definida em um Acordo de Nível de Serviço ("SLA")) e em características de regra. Os enlases de realimentação podem ser usados para otimizar subconjuntos de regra de classificação selecionados.

Relatório Descritivo da Patente de Invenção para **"MÉTODO PARA SELECIONAR ADAPTATIVAMENTE REGRAS USADAS PARA CLASSIFICAR MENSAGENS ELETRÔNICAS E SISTEMA PARA SELECIONAR ADAPTATIVAMENTE REGRAS DE DETECÇÃO DE SPAM"**.

Antecedentes

[0001] Os sistemas de computador e tecnologia relacionada afetam muitos aspectos da sociedade. Na realidade, a capacidade do sistema de computador em processar informação tem transformado a maneira de viver e de trabalhar. Os sistemas de computador agora executam comumente uma hospedagem de tarefas (por exemplo, processamento de palavra, programação, contabilidade, etc.) que antes do advento do sistema de computador eram executados manualmente. Mais recentemente, os sistemas de computador foram acoplados um ao outro e a outros dispositivos eletrônicos para formar tanto redes de computador sem fio quanto com fio pelas quais os sistemas de computador e outros dispositivos eletrônicos podem transferir dados eletrônicos. Consequentemente, o desempenho de muitas tarefas de computação é distribuído por inúmeros sistemas de computador diferentes e/ou inúmeros ambientes computacionais diferentes.

[0002] Em muitos ambientes computacionais, as mensagens eletrônicas, tais como, por exemplo, mensagens de correio eletrônico, são usadas para validar informação de troca entre usuários de sistema de computador. Entretanto, esses ambientes computacionais também submetem os usuários a mensagens eletrônicas não solicitadas e/ou indesejadas, frequentemente chamadas de SPAM. Muitas tecnologias diferentes foram desenvolvidas para varrer e bloquear SPAM.

[0003] As tecnologias de varredura de SPAM precisam tipicamente negociar um conjunto de métricas, que inclui: eficácia, precisão, eficiência e latência. A eficácia se refere a qual ponto o SPAM pode ser

identificado e parado. A precisão se refere a qual ponto as mensagens válidas são incorretamente identificadas como SPAM (por exemplo, taxa de falsos positivos). A eficiência se refere ao consumo de recurso associado à identificação de uma mensagem como SPAM ou válida. A latência se refere a quanto tempo cada mensagem individual está atrasada em trânsito como um resultado da varredura.

[0004] O equilíbrio entre essas métricas pode ser uma tarefa relativamente complexa posto que o aprimoramento em uma área tipicamente significa a degradação em uma ou mais outras áreas. Por exemplo, a detecção de anti-SPAM mais agressiva (eficácia aumentada) pode levar a falsos positivos superiores (precisão reduzida), e/ou carga de CPU superior devido aos algoritmos de processamento mais complexos (consumo de recurso aumentado).

[0005] Adicionalmente, alguma combinação dessas métricas é frequentemente mapeada para Acordos de Nível de Serviço ("SLAs") que um provedor de serviço está suportando. Por exemplo, um provedor de serviço anti-SPAM pode concordar em suportar eficácia não inferior a X, precisão não inferior a Y, etc. Comprometendo os termos de um SLA, por exemplo, que tem eficácia menor que X para alguma quantidade de tempo, pode submeter o provedor de serviço anti-SPAM a algum reembolso financeiro para o cliente.

[0006] Entretanto, ao mesmo tempo, os serviços anti-SPAM experimentam tipicamente alta variabilidade da carga de sistema. Por exemplo, durante qualquer dia, em finais de semana e por temporada, o volume de SPAM e/ou o volume de mensagens eletrônicas pode oscilar. Desafortunadamente, isso pode levar ao sobreposicionamento de provedores de serviço. Por exemplo, um padrão de projeto comum é construir um serviço de varredura com potência suficiente para garantir um SLA em tempo de carga pico, que pode ser três a cinco vezes maior que a carga média.

[0007] Na prática, o projeto para resultados de carga pico em recursos é (potencial e severamente) subutilizou uma porção significativa do tempo. A varredura tipicamente inclui um número fixo de estágios e/ou o uso de um número fixo de regras de varredura com consideração limitada, se houver, para recursos disponíveis. Dessa forma, em tempos não pico, o número fixo de estágios e/ou regras é usado para varrer uma mensagem, mesmo se os recursos estiverem disponíveis para varredura adicional. Como tal, o projeto para carga pico forma indesejavelmente um custo de perspectiva de venda de produtos, mas é, todavia requerido para SLAs

[0008] As complicações adicionais podem ocorrer quando se suporta vários níveis diferentes de serviço, tais como, por exemplo, clientes regulares, clientes especiais, clientes de baixo custo, etc., tipicamente com diferentes métricas definidas em seu SLA. Frequentemente, as ofertas de serviço especial vêm com SLAs que garantem um nível superior de serviço (por exemplo, precisão aumentada, menos latência, etc.) que requer mais recursos de computação/processador na parte do provedor de serviço.

[0009] Um padrão de projeto para manipular diferentes níveis de serviço é um serviço anti-SPAM comum para todos os níveis de serviço. Cada nível de serviço é limitado a um número de regras e/ou estágios de processamento pelo qual uma mensagem passa com base em um SLA requerido. Por exemplo, um correio eletrônico cliente especial pode percorrer dez estágios de processamento, enquanto o correio eletrônico de cliente básico pode percorrer apenas cinco estágios de processamento. O custo de serviço de clientes básicos é reduzido no gasto de qualidade inferior de varredura (por exemplo, eficácia reduzida), mesmo quando os recursos para varredura adicional podem estar disponíveis. Além da qualidade inferior de varredura, os clientes básicos também são mais vulneráveis a ataque alvejado através da explo-

ração das fraquezas no nível de proteção fornecido para clientes básicos (previsibilidade do sistema).

[00010] Um outro padrão comum é configurar dois sistemas separados, um para clientes especiais e um outro um para os clientes básicos. Cada sistema é projetado para equilibrar a qualidade de serviço e o custo de serviço de acordo com o tipo de cliente. Desafortunadamente, esse tipo de sistema requer infraestrutura duplicada, levando custos gerais superiores, bem como o problema geral de sobreprovisão a fim de satisfazer o SLA na carga pico.

Breve Sumário

[00011] A presente invenção se estende a métodos, sistemas e produtos de programa de computador para selecionar adaptativamente regras de varredura de mensagem eletrônica. Em algumas modalidades, as regras usadas para classificar mensagens eletrônicas são adaptativamente selecionadas. Uma ou mais mensagens eletrônicas são recebidas. Para cada uma das uma ou mais mensagens eletrônicas, cada regra de classificação de mensagem em um subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica é aplicada à mensagem eletrônica. O subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica é um subconjunto de uma pluralidade de regras de classificação de mensagem eletrônica disponíveis.

[00012] Para cada regra de classificação de mensagem eletrônica no subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica, um resultado que indica uma probabilidade da mensagem eletrônica que tem uma característica de mensagem especificada é calculado. Um custo de recurso, que indica uma quantidade de recursos consumidos para aplicar a regra de classificação de mensagem eletrônica à mensagem eletrônica, é calculado. O resultado calculado e o custo de recurso medido associado à aplicação de cada

regra de classificação de correio eletrônico a cada mensagem eletrônica são retidos.

[00013] Para cada regra de classificação de mensagem no subconjunto anteriormente selecionado de regras de classificação de mensagem, uma métrica de eficiência é sintetizada a partir dos resultados calculados e dos custos de recurso medidos retidos para a regra de classificação de mensagem. As métricas de eficiência sintetizadas são comparadas com as métricas de eficiência existentes para regras de classificação de mensagem eletrônica incluídas na pluralidade de regras de classificação de mensagem eletrônica disponíveis. Um novo subconjunto de regras de classificação de mensagem eletrônica é selecionado, dentre a pluralidade de regras de classificação de mensagem eletrônica disponíveis, com base pelo menos em parte nos resultados de comparação das métricas de eficiência sintetizadas com as métricas de eficiência existentes. O novo subconjunto de regras de classificação de mensagem eletrônica é para uso na classificação de mensagens eletrônicas subsequentemente recebidas. Consequentemente, as regras de classificação de mensagem podem ser giradas para dentro e para fora para adaptar à troca de padrões de conteúdo de mensagem.

[00014] Esse sumário é fornecido para introduzir uma seleção de conceitos de uma forma simplificada que são adicionalmente descritos abaixo na Descrição Detalhada. Esse Sumário não pretende identificar recursos-chave ou recursos essenciais do assunto reivindicado, nem pretende ser usado como um auxílio na determinação do escopo do assunto reivindicado.

[00015] Os recursos e vantagens adicionais da invenção serão apresentados na seguinte descrição, e em parte serão óbvios a partir da descrição ou podem ser aprendidos pela prática da invenção. Os recursos e vantagens da invenção podem ser realizados e obtidos por

meio dos instrumentos e combinações particularmente apontados nas reivindicações anexas. Esses e outros recursos da presente invenção se tornarão mais completamente evidentes a partir da seguinte descrição e das reivindicações anexas, ou podem ser aprendidos pela prática da invenção conforme apresentado doravante no presente documento.

Breve Descrição dos Desenhos

[00016] A fim de descrever a maneira na qual os recursos e vantagens mencionados acima além de outro da invenção podem ser obtidos, uma descrição mais particular da invenção brevemente descrita acima será produzida por referência às modalidades específicas da mesma que são ilustradas nos desenhos anexos. Com a compreensão de que esses desenhos revelam apenas modalidades típicas da invenção e não devem, portanto, ser considerados como limitantes de seu escopo, a invenção será descrita e explicada com especificidade e detalhe adicional através do uso dos desenhos anexos, nos quais:

[00017] A Figura 1 ilustra uma arquitetura de computador exemplificativa que facilita a classificação adaptativa de uma mensagem eletrônica.

[00018] A Figura 2 ilustra uma arquitetura de computador exemplificativa que facilita a seleção adaptativa de regras usadas para classificar mensagens eletrônicas.

[00019] A Figura 3 ilustra um fluxograma de um método exemplificativo para classificar adaptativamente uma mensagem eletrônica.

[00020] A Figura 4 ilustra um fluxograma de um método exemplificativo para selecionar adaptativamente regras usadas para classificar mensagens eletrônicas.

[00021] A Figura 5 ilustra uma outra arquitetura de computador exemplificativa que facilita a varredura adaptativa de mensagem eletrônica varredura e a seleção adaptativa de regras usadas para classi-

ficar mensagens eletrônicas.

Descrição Detalhada

[00022] A presente invenção se estende a métodos, sistemas e produtos de programa de computador para selecionar adaptativamente regras de varredura de mensagem eletrônica. Em algumas modalidades, as regras usadas para classificar mensagens eletrônicas são adaptativamente selecionadas. Uma ou mais mensagens eletrônicas são recebidas. Para cada uma das uma ou mais mensagens eletrônicas, cada regra de classificação de mensagem em um subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica é aplicada à mensagem eletrônica. O subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica é um subconjunto de uma pluralidade de regras de classificação de mensagem eletrônica disponíveis.

[00023] Para cada regra de classificação de mensagem eletrônica no subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica, um resultado que indica uma probabilidade da mensagem eletrônica que tem uma característica de mensagem especificada é calculado. Um custo de recurso, que indica uma quantidade de recursos consumida para aplicar a regra de classificação de mensagem eletrônica à mensagem eletrônica, é calculado. O resultado calculado e o custo de recurso medido associados à aplicação de cada regra de classificação de correio eletrônico a cada mensagem eletrônica são retidos.

[00024] Para cada regra de classificação de mensagem no subconjunto anteriormente selecionado de regras de classificação de mensagem, uma métrica de eficiência é sintetizada a partir dos resultados calculados e dos custos de recurso medidos retidos para a regra de classificação de mensagem. As métricas de eficiência sintetizadas são comparadas com as métricas de eficiência existentes para regras de

classificação de mensagem eletrônica incluídas na pluralidade de regras de classificação de mensagem eletrônica disponíveis. Um novo subconjunto de regras de classificação de mensagem eletrônica é selecionado, dentre a pluralidade de regras de classificação de mensagem eletrônica disponíveis, com base pelo menos em parte nos resultados da comparação das métricas de eficiência sintetizadas com as métricas de eficiência existentes. O novo subconjunto de regras de classificação de mensagem eletrônica é para uso na classificação de mensagens eletrônicas subsequentemente recebidas. Consequentemente, a regra de classificação de mensagem pode ser inserida e retirada do serviço para adaptar à alteração de padrão de conteúdo de mensagem.

[00025] Em outras modalidades, as mensagens eletrônicas são adaptativamente classificadas. Uma mensagem eletrônica, enviada de um remetente para um recipiente, é recebida em um tempo específico. Um nível de serviço aplicável à mensagem eletrônica recebida é identificado com base em um ou mais I: o remetente e o recipiente.

[00026] O nível de serviço define pelo menos um valor mínimo de eficácia e um conjunto de valores de custo máximo para varredura de mensagens eletrônicas. O mínimo de eficácia representa a eficácia total máxima acumulativa em que uma combinação de regras de classificação de mensagem tem que satisfazer o nível de serviço. Cada valor de custo máximo no conjunto de valores de custo máximo corresponde a um período de tempo projetado diferente e representa uma quantidade total de recursos que podem ser usados para aplicar regras de classificação de mensagem a uma mensagem eletrônica. Um valor de custo máximo, dentre o conjunto de valores de custo máximo, é selecionado para uso quando se varre a mensagem eletrônica recebida com base no tempo específico que está dentro período de tempo designado para o valor de custo máximo selecionado.

[00027] Uma ou mais regras de classificação de mensagem são aplicadas à mensagem eletrônica recebida. Cada regra de classificação de mensagem tem uma eficácia medida, um custo de recurso medido e uma eficiência calculada com base na eficácia medida em vista do custo de recurso medido. A eficácia medida representa uma probabilidade de identificar apropriadamente uma mensagem eletrônica como tendo uma característica de mensagem especificada. As uma ou mais regras de classificação de mensagem são aplicada em ordem de eficiência até que a eficácia total máxima acumulativa definida no nível de serviço seja alcançada.

[00028] Cada regra de classificação de mensagem é aplicada à mensagem eletrônica para gerar um resultado que indica uma probabilidade da mensagem eletrônica que tem a característica de mensagem especificada. O custo de recurso medido para a regra de classificação de mensagem aplicada é adicionado a uma quantidade acumulativa de recursos consumidos. A quantidade acumulativa de recurso consumido é calculada pela soma dos custos de recurso medidos de regras de classificação de mensagem aplicadas anteriormente nas uma ou mais regras de classificação de mensagem.

[00029] Isso é determinado se a quantidade acumulativa de recursos consumidos for menor que o valor de custo máximo selecionado. As regras de classificação de mensagem adicionais são aplicadas às mensagens eletrônicas com base na determinação. Quando a quantidade de recursos consumidos é menor que o valor de custo máximo selecionado, mais regras de mensagem eletrônica são aplicadas à mensagem eletrônica recebida resultando em eficácia acima daquela definida no nível de serviço. Quando a quantidade de recursos consumidos é pelo menos igual ao valor de custo máximo selecionado, as regras de mensagem eletrônica são aplicadas a uma outra mensagem eletrônica diferente.

[00030] As modalidades da presente invenção podem compreender ou utilizar um computador de propósito geral ou de propósito especial que inclui hardware de computador, tais como, por exemplo, um ou mais processadores e memória de sistema, conforme discutido em maiores detalhes abaixo. As modalidades dentro do escopo da presente invenção também incluem meios físicos e outros meios legíveis por computador para portar ou armazenar instruções executáveis por computador e/ou estruturas de dados. Tais meios legíveis por computador podem ser quaisquer meios disponíveis que podem ser acessados por um sistema de computador de propósito geral ou propósito especial. Os meios legíveis por computador que armazenam instruções executáveis por computador são meios de armazenamento físico. Os meios legíveis por computador que portam instruções executáveis por computador são meios de transmissão. Dessa forma, por meio de exemplo, e sem limitação, as modalidades da invenção podem compreender pelo menos dois tipos distintamente diferentes de meios legíveis por computador: meios de armazenamento em computador (dispositivos) e meios de transmissão.

[00031] Os meios de armazenamento em computador (dispositivos) incluem RAM, ROM, EEPROM, CD-ROM ou outro armazenamento em disco óptico, armazenamento em disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que pode ser usado para armazenar os meios de código de programa desejados na forma de instruções executáveis por computador ou estruturas de dados e que podem ser acessados por um computador de propósito geral ou propósito especial.

[00032] Uma "rede" é definida como um ou mais enlaces de dados que permitem o transporte de dados eletrônicos entre os sistemas de computador e/ou módulos e/ou outros dispositivos eletrônicos. Quando a informação é transferida ou fornecida por uma rede ou uma outra co-

nexão de comunicações (com fio rígido, sem fio ou uma combinação de com fio ou sem fio) a um computador, em que o computador visualiza apropriadamente a conexão como um meio de transmissão. Os meios de transmissão podem incluir uma rede e/ou enlaces de dados que podem ser usados para transporte ou meios de código de programa desenhados na forma de instruções executáveis por computador ou estruturas de dados e que podem ser acessados por um computador de propósito geral ou propósito especial. As combinações acima também devem estar incluídas no escopo de meios legíveis por computador.

[00033] Adicionalmente, mediante o alcance de vários componentes de sistema de computador, os meios de código de programa na forma de instruções executáveis por computador ou estruturas de dados podem ser transferidos automaticamente a partir dos meios de transmissão para os meios de armazenamento em computador (dispositivos) (ou vice versa). Por exemplo, as instruções executáveis por computador ou estruturas de dados recebidas por uma rede ou enlace de dados pode ser armazenadas temporariamente em RAM dentro de um módulo de interface de rede (por exemplo, um "NIC") e, então, eventualmente transferidas para RAM do sistema de computador e/ou para meios de armazenamento em computador menos voláteis em um sistema de computador. Dessa forma, deve ficar entendido que os meios de armazenamento em computador (dispositivos) podem ser incluídos em componentes de sistema de computador que também (ou ainda principalmente) utilizam os meios de transmissão.

[00034] As instruções executáveis por computador compreendem, por exemplo, instruções e dados que, quando executados em um processador, fazem com que um computador de propósito geral, computador de propósito especial ou dispositivo de processamento de propósito especial execute uma certa função ou grupo de funções. As instruções executáveis por computador podem ser, por exemplo, binárias,

instruções de formato intermediário tal como linguagem de montagem ou ainda código-fonte. Embora o assunto tenha sido descrito em linguagem específica para recursos estruturais e/ou atos metodológicos, deve ficar entendido que o assunto definido nas reivindicações anexas não é necessariamente limitado aos recursos descritos ou atos descritos acima. De preferência, os recursos e os atos descritos são revelados como formas exemplificativas de implantação das reivindicações.

[00035] Aqueles elementos versados na técnica irão observar que a invenção pode ser colocada em prática em ambientes computacionais de rede com muitos tipos de configurações de sistema de computador, que incluem, computadores pessoais, computadores do tipo desktop, computadores do tipo laptop, processadores de mensagem, dispositivos portáteis, sistemas de múltiplos processadores, eletrônicos à base de microprocessador ou programáveis pelo consumidor, PCs em rede, minicomputadores, computadores terminais, telefones móveis, PDAs, pagers, roteadores, comutadores e similares. A invenção também pode ser colocada em prática em ambientes de sistema distribuídos onde sistemas de computador locais e remotos, que são ligados (por enlaces de dados com fio, enlaces de dados sem fio ou por uma combinação de enlaces de dados com e sem fio) através de uma rede, executam tarefas. Em um ambiente de sistema distribuído, os módulos de programa podem ser localizados tanto em dispositivos de armazenamento de memória remotos quanto locais.

[00036] Em geral, as modalidades da invenção se referem à variação dinâmica (e potencial e não previsível) da profundidade/perfeição de classificação de mensagens eletrônicas para proteger contra conteúdo de mensagem indesejável (por exemplo, SPAM, vírus, vazamento digital, etc.). Uma eficácia mínima é mantida e, quando os recursos disponíveis permitem, pode ser excedida para fornecer proteção aumentada. Um subconjunto ideal de regras de classificação de mensa-

gem disponíveis pode ser selecionado em uma base por mensagem. A seleção de regras é baseada em recursos de sistema disponíveis, eficácia desejada mínima (por exemplo, definido em um Acordo de Nível de Serviço ("SLA")), e características de regra. Os enlaces de retroalimentação podem ser usados para otimizar os subconjuntos de regra de classificação.

[00037] Como tal, dentro do relatório descritivo e das seguintes reivindicações, "classificação de mensagem" inclui classificação de mensagens eletrônicas (por exemplo, mensagens de correio eletrônico, mensagens de Serviço de Mensagem Curta ("SMS"), arquivos, etc.) em diferentes "classes" com base em características de mensagem (ou arquivo), tais como, por exemplo, conteúdo, tamanho de mensagem, anexos, domínios de negócios vs. consumidor, região de origem, remetente, recipiente, tempo, data, etc.

[00038] Em algumas modalidades, uma mensagem eletrônica é classificada para determinar um nível de serviço (por exemplo, de acordo com um SLA) correspondente à mensagem eletrônica. O nível de serviço define a aplicação adicional de regras de classificação de mensagem à mensagem eletrônica. Um nível de serviço pode definir quais tipos e quantas outras regras de classificação de mensagem devem ser aplicadas à mensagem eletrônica. Por exemplo, as regras de classificação que são muito eficazes para classificar as mensagens em um país podem ser menos eficazes para classificar as mensagens em outro país e vice-versa.

[00039] Em algumas modalidades, a classificação adicional se refere à determinação se ou não uma mensagem eletrônica é uma mensagem eletrônica indesejada e/ou não solicitada (por exemplo, SPAM), se uma mensagem eletrônica contém malware ou está, de outro modo, infectada e/ou é perigosa (por exemplo, vírus, spyware, cavalos de Troia, etc.), se a informação confidencial está sendo vazada em uma

mensagem eletrônica, etc. Por exemplo, um sistema de prevenção de vazamento digital prevenção ("DLP") pode usar regras para determinar se ou não uma mensagem eletrônica inclui informação confidencial.

[00040] A Figura 1 ilustra uma arquitetura de computador exemplificativa 100 que facilita a classificação adaptativa de uma mensagem eletrônica. Em referência à Figura 1, a arquitetura de computador 100 inclui classificador de mensagem 102, identificador de nível de serviço 107, relógio 108, porcentagem de neutralização 118, regras de classificação de mensagem 121, e Acordos de Nível de Serviço 131. Cada um dos componentes revelados é conectado a um outro (ou é parte de) por uma rede, tais como, por exemplo, uma Rede de Área Local ("LAN"), uma Rede de Área Ampla ("WAN") e até mesmo a Internet. Consequentemente, cada um dos componentes revelados bem como quaisquer outros sistemas de computador conectados e seus componentes, podem criar dados relacionados à mensagem e troca dados relacionados à mensagem (por exemplo, dados de Protocolo de Internet ("IP") e outros protocolos de camada superior que utilizam dados de IP, tais como, Protocolo de Controle de Transmissão ("TCP"), Protocolo de Transferência de Hipertexto ("HTTP"), Protocolo de Transferência de Correio Simples ("SMTP"), etc.) pela rede.

[00041] As regras 121 contêm uma pluralidade de regras de classificação de mensagem, tais como, por exemplo, regras 121A a 121N, que podem ser usadas para classificar mensagens eletrônicas. Cada regra pode indicar eficácia, custo, eficiência, e pode incluir instruções. A eficácia indica a probabilidade de a regra identificar precisamente uma mensagem como algo indesejável com base no tipo de varredura que está sendo utilizado. Por exemplo, a eficácia de uma regra para detectar SPAM, pode indicar o quanto é provável que regra detecte SPAM sem falsos positivos. O custo indica uma quantidade de recursos de sistema (por exemplo, estimada) que são consumidos mediante

a operação do módulo que opera as instruções da regra. A eficiência indica quão eficiente uma regra é com base na eficácia em vista de consumo de recurso. Em algumas modalidades, a eficiência é o cociente de eficácia dividido pelo custo. As instruções são executadas para gerar um resultado relacionado à classificação de uma mensagem eletrônica (por exemplo, para determinar se ou não uma mensagem eletrônica é SPAM, contém malware, contém informação confidencial, etc.).

[00042] Em geral, o classificador de mensagem 102 é configurado para classificar mensagens eletrônicas com base em características de mensagem eletrônica. Conforme revelado, o classificador de mensagem 102 inclui módulo de operação 103, monitor de custo 104 e monitor de eficácia 106. O módulo de operação 103 é configurado para operar instruções (por exemplo, scripts ou outro código executável) incluídas em uma regra recebida. As instruções produzem um resultado individual que pode ser usado como um ponto de dados para classificar uma mensagem eletrônica. Por exemplo, um resultado individual pode indicar se ou não uma mensagem eletrônica é uma mensagem eletrônica indesejada e/ou não solicitada (por exemplo, SPAM), é infectada ou perigosa, contém informação confidencial, etc. O módulo de operação 103 pode acumular resultados individuais da operação de inúmeras regras diferentes. O classificador de mensagem 102 pode, então, usar resultados individuais acumulados para classificar uma mensagem.

[00043] O monitor de custo 104 é configurado para rastrear o custo de recurso em andamento associado à varredura de uma mensagem eletrônica. Conforme as regras são operadas, o monitor de custo 104 mantém um custo de recurso total para quaisquer regras operadas contra uma mensagem eletrônica. Em algumas modalidades, conforme cada regra é operada, o custo para a regra é adicionado ao custo

de recurso para quaisquer regras operadas anteriormente.

[00044] O monitor de eficácia 106 é configurado para rastrear a eficácia em andamento de varredura de uma mensagem eletrônica. Conforme as regras são operadas, o monitor de eficácia 106 mantém uma eficácia total para quaisquer regras operadas contra uma mensagem eletrônica. Em algumas modalidades, conforme cada regra é operada, a eficácia para a regra é adicionada à eficácia para quaisquer regras operadas anteriormente.

[00045] Os Acordos de Nível de Serviço 129 contêm uma pluralidade de SLAs que incluem SLA 131. Cada SLA inclui uma eficácia mínima e um ou mais custos. Cada custo é aplicável a uma faixa de data/tempo especificada. A eficácia mínima representa a eficácia acumulativa (isto é, a soma de eficácia para uma pluralidade de regras de classificação) que devem ser alcançadas mediante a varredura de uma mensagem (mesmo que o consumo de recurso seja excedido). A Tabela 1 é um exemplo de eficácia por SLA com base em tipo de cliente.

Tabela 1

Tipo de cliente	Eficácia
Cliente Básico	75
Cliente Especial	100

[00046] A Tabela 1 indica que a eficácia mínima (isto é, a eficácia acumulativa resultante da aplicação de uma pluralidade de regras de classificação) é 75 para um cliente básico e 100 para um cliente especial. Outros fatores também podem ser considerados quando se atribui uma eficácia mínima em um SLA.

[00047] Os um ou mais custos incluem uma faixa de tempo e um custo máximo. Cada par de faixa de tempo/custo máximo representa que um custo máximo de recurso para aplicar regras deve ser considerado para uma mensagem quando a mensagem é recebida dentro da

faixa de tempo. Os pares de faixa de tempo/custo máximo podem variar ou ser iguais para diferentes níveis de serviço. Em algumas modalidades, os pares de faixa de tempo/custo máximo são atribuídos em uma tabela comumente acessível em que os pares de faixa de tempo/custo máximo são iguais para muitos SLAs. Em outras modalidades, os pares de faixa de tempo/custo máximo podem ser atribuídos em uma base por SLA, tal como, por exemplo, através da inclusão em um SLA. A Tabela 2 é um exemplo de pares de faixa de tempo/custo máximo.

Tabela 2

Tempo do dia	Custo máximo
Horas pico	50
Horas normais	75
Horas fora do pico	100

[00048] A Tabela 2 indica que o custo máximo de recurso para aplicação de regras de classificação durante as horas pico é 50, durante as horas normais é 75 e durante as horas fora do pico é 100. Outros fatores também podem ser considerados.

[00049] Os custos máximos podem trocar ao longo do tempo. Se um servidor de classificação de mensagem adicionar hardware adicional e, dessa forma, tiver mais capacidade computacional, figuras de custo máximo podem surgir. Por outro lado, se o serviço adicionar clientes adicionais ou se a carga aumentar repentinamente, a figura do custo máximo pode diminuir.

[00050] Em algumas modalidades, a eficácia mínima é considerada com mais importância em relação ao custo máximo. Nessas modalidades, os recursos em excesso de custo máximo podem ser consumidos para assegurar que a eficácia mínima é alcançada. Se a eficácia mínima for alcançada com o uso de menos recursos que o custo máximo, regras de classificação adicionais podem ser aplicadas para au-

mentar a eficácia até que o custo máximo seja alcançado ou excedido.

[00051] O identificador de nível de serviço 107 é configurado para identificar um nível de serviço correspondente a uma mensagem eletrônica recebida. Com base em características e tempo/data da mensagem, o identificador de nível de serviço 107 pode identificar um SLA apropriado dos Acordos de Nível de Serviço 131. O relógio 108 pode manter uma data e tempo do dia e enviar essa informação para o identificador de nível de serviço 107 quando uma mensagem eletrônica é recebida. O identificador de nível de serviço pode enviar eficácia mínima e custo máximo para a mensagem para o classificador de mensagem 102. Por regra de classificação de mensagem, o classificador de mensagem 102 pode comparar uma eficácia acumulativa com os efetivos máximos e um custo acumulativo com o custo máximo para determinar quais e quantas regras de classificação aplicar à mensagem recebida.

[00052] A porcentagem de neutralização 118 define alguma porcentagem que as regras de classificação adicionais devem ser aplicadas a uma mensagem eletrônica mesmo quando a eficácia mínima já é alcançada e o custo máximo já é alcançado ou excedido. A porcentagem de neutralização 118 permite que as regras de classificação que podem, de outro modo, ser puladas (por exemplo, devido a sua eficiência) sejam executadas de tempos em tempos. Em algumas modalidades, a porcentagem de neutralização 118 indica uma porcentagem em que cada regra em regras de classificação de mensagem 121 deve ser aplicada a uma mensagem eletrônica.

[00053] A Figura 3 ilustra um fluxograma de um método exemplificativo 300 para classificar adaptativamente uma mensagem eletrônica. O método 300 será descrito em relação aos componentes e aos dados de arquitetura de computador 100.

[00054] O método 300 inclui um ato que recebe uma mensagem

eletrônica em um tempo específico, em que a mensagem eletrônica é enviada de um remetente para um recipiente (ato 301). Por exemplo, o classificador de mensagem 102 pode receber a mensagem 101U no tempo 114 (conforme indicado pelo relógio 108). A mensagem 101U pode incluir características de mensagem 111 que incluem um endereço de remetente e um endereço de recipiente.

[00055] O método 300 inclui um ato de identificação de um nível de serviço aplicável à mensagem eletrônica recebida com base em um ou mais dentre: o remetente e o recipiente, o nível de serviço que define pelo menos um valor mínimo de eficácia e um conjunto de valores de custo máximo, em que o valor mínimo de eficácia representa a eficácia total máxima acumulativa que uma combinação de regras de classificação de mensagem tem que satisfazer o nível de serviço, cada valor de custo máximo no conjunto de valores de custo máximo correspondente a um período de tempo designado diferente, cada valor de custo máximo que representa uma quantidade total de recursos que podem ser usados para aplicar regras de classificação de mensagem a uma mensagem eletrônica (ato 302). Por exemplo, o identificador de nível de serviço 107 pode receber características de mensagem 111 e tempo 114. Com base em características de mensagem 111, (por exemplo, os endereços de remetente e/ou recipiente) o identificador de nível de serviço 107 pode identificar um SLA 131 como aplicável para classificação de mensagem 101U.

[00056] Conforme revelado, o SLA 131 define a eficácia mínima 132 e os custos 133. Os custos 133 incluem pares de faixa de tempo/custo máximo, que incluem faixa de tempo 134A/custo máximo 136A, faixa de tempo 134B/custo máximo 136B, faixa de tempo 134C/custo máximo 136C, etc.

[00057] O método 300 inclui um ato de seleção de um valor de custo máximo, dentre o conjunto de valores de custo máximo, a ser usado

mediante a varredura da mensagem eletrônica recebida com base no tempo específico que está dentro do período de tempo designado para o valor de custo máximo selecionado (ato 303). Por exemplo, o identificador de nível de serviço 107 pode determinar se esse tempo 114 está dentro da faixa de tempo 134A. Em resposta, o identificador de nível de serviço 107 pode selecionar o custo máximo 136A a ser usado mediante a varredura de uma mensagem não classificada 101U.

[00058] O identificador de nível de serviço 107 pode enviar a eficácia mínima 132 e o custo máximo 136A para o classificador de mensagem 102. O classificador de mensagem 102 pode usar a eficácia mínima 132 e o custo máximo 136A para determinar quando a aplicação das regras de classificação de mensagem à mensagem não classificada 101U deve parar.

[00059] O método 300 inclui um ato de aplicação de uma ou mais regras de classificação de mensagem à mensagem eletrônica recebida, cada regra de classificação de mensagem tem uma eficácia medida, um custo de recurso medido e uma eficiência calculada com base na eficácia medida em vista do custo de recurso medido, em que a eficácia medida representa uma probabilidade de classificação apropriada de mensagens eletrônicas como tendo uma característica de mensagem especificada, as uma ou mais regras de classificação de mensagem aplicadas em ordem de eficiência até que a eficácia total máxima acumulativa definida no nível de serviço seja alcançada (ato 304). Por exemplo, o classificador de mensagem pode aplicar as regras a partir das regras 121 em ordem de eficiência até que a eficácia mínima 132 (isto é, 60) seja alcançada.

[00060] Das regras reveladas, pode ser que a eficiência 124A (isto é, 4) seja a mais alta para as regras nas regras 121. Dessa forma, a regra 121A é a primeira regra aplicada à mensagem não classificada 101U. Mediante a aplicação da regra 121A, a eficácia acumulativa 162

é 8 igual à eficácia 122A. O classificador de mensagem 102 determina que 8 é menor que 60, então, as regras de classificação adicionais devem ser aplicadas para alcançar a eficácia mínima 132A.

[00061] Pode ser que a eficiência 124B (isto é, 3) seja a próxima mais alta para as regras em regras 121. Dessa forma, a regra 121B é a próxima regra aplicada à mensagem não classificada 101U. Mediante a aplicação da regra 121B, a eficácia acumulativa 162 é 11 igualando à soma da eficácia 122A mais a eficácia 122B. O Classificador de mensagem 102 determina que 11 é menor que 60, então, as regras de classificação adicionais devem ser aplicadas para alcançar eficácia mínima 132A.

[00062] Pode ser que a eficiência 124C (isto é, 2,8) seja a mais alta para as regras nas regras 121. Dessa forma, a regra 121C é a próxima regra aplicada à mensagem não classificada 101U. Mediante a aplicação da regra 121C, a eficácia acumulativa 162 é 65 igualando à soma da eficácia 122A mais a eficácia 122B mais a eficácia 122C. O classificador de mensagem 102 determina que 65 é maior que 60, então, não se requer que as regras de classificação satisfaçam o SLA 131.

[00063] Para cada uma das uma ou mais regras de classificação de mensagem aplicadas, o método 300 inclui um ato de aplicação da regra de classificação de mensagem à mensagem eletrônica para gerar um resultado que indica uma probabilidade de a mensagem eletrônica ter a característica de mensagem especificada (ato 305). Por exemplo, o módulo de operação 103 pode executar instruções 126A contra mensagem não classificada 101U para gerar resultado 112. O resultado 112 indica uma probabilidade de que a mensagem não classificada 101U seja uma mensagem eletrônica indesejada e/ou não solicitada, uma mensagem infectada ou perigosa, contenha informação confidencial, etc. O módulo de operação 103 pode armazenar os resultados 112 em resultados acumulativos 113. As instruções 126B e 126C po-

dem ser executadas de modo similar contra mensagem não classificada 101U para gerar resultados. Esses resultados também podem ser armazenados em resultados acumulativos 113.

[00064] Para cada uma das uma ou mais regras de classificação de mensagem aplicadas, o método 300 inclui um ato de adição do custo de recurso medido para a regra de classificação de mensagem aplicada para uma quantidade acumulativa de recursos consumidos, em que a quantidade acumulativa de recurso calculado consumido através da soma dos custos de recurso medidos das regras de classificação de mensagem aplicadas anteriormente nas uma ou mais regras de classificação de mensagem (ato 306). Por exemplo, mediante a aplicação de regras 121 A, 121B, e 121C, o custo acumulativo 161 é 21 igual ao custo 123A mais o custo 123B mais o custo 123C.

[00065] O método 300 inclui um ato de determinação de se a quantidade acumulativa de recursos consumidos é menor que o valor de custo máximo selecionado (ato 307). Por exemplo, o monitor de custo 104 pode determinar se o custo acumulativo 104 é menor que o custo máximo 136A. O método 300 inclui um ato de aplicação de regras de classificação de mensagem adicionais a mensagens eletrônicas com base na determinação (ato 308). Por exemplo, o classificador de mensagem 102 pode aplicar regras de classificação de mensagem adicionais a mensagens eletrônicas com base em se ou não o custo acumulativo 161 é menor que o custo máximo 136A.

[00066] Conforme revelado na arquitetura de computador 100, mediante o alcance da eficácia mínima 132A, o custo acumulativo 161 (isto é, 21) é menor que o custo máximo 136A (isto é, 25). Dessa forma, regras de classificação adicionais podem ser aplicadas à mensagem não classificada 101U para aumentar a eficácia de classificação de mensagem não classificada 101U.

[00067] Por exemplo, pode ser que a eficiência 124D (1,75) seja a

próxima mais para as regras nas regras 121. Dessa forma, a regra 121D é a próxima regra aplicada à mensagem não classificada 101U. Como tal, o módulo de operação 103 pode executar instruções 126D contra mensagem não classificada 101U para gerar um resultado e armazenar os resultados em resultados acumulativos 113. Mediante a aplicação da regra 121D, o custo acumulativo 161 é transitado para 29 igualando ao custo 123A mais o custo 123B mais o custo 123C mais o custo 123D. (A eficácia 122D é essencialmente ignorada uma vez que a eficácia mínima 132A já foi alcançada). Uma vez que o custo acumulativo 161 (isto é, 29) excede o custo máximo 136A (isto é, 25), nenhuma regra adicional é aplicada à mensagem não classificada 101U.

[00068] Alternativamente, se mediante o alcance da eficácia mínima 132A após a aplicação de regra 121C, o custo acumulativo 161 tiver igualado ou for maior que o custo máximo 136A (isto é, 25), nenhuma regra adicional é aplicada à mensagem não classificada 101U. Entretanto, a eficácia mínima 132A ainda é alcançada.

[00069] Quando a eficácia mínima 132A é alcançada e o custo máximo 136A é alcançado ou excedido, o classificador de mensagens 102 pode se referir à porcentagem de neutralização 118. O classificador de mensagem 102 pode usar a porcentagem de neutralização 118 para determinar se regras de classificação adicionais devem ser aplicadas à mensagem não classificada 101U. Se sim, o classificador de mensagem 102 aplica uma ou mais (ou todas as restantes) regras das regras de classificação de mensagem 121, como tal, por exemplo, a regra 121E, à mensagem não classificada 101U. O uso da porcentagem de neutralização 118 permite que o desempenho (por exemplo, eficácia e custo) de regras de classificação de mensagem de uso limitado ou, de outro modo, não usado seja avaliado e apropriadamente alterado. Com base nas alterações, a frequência de uso dessas regras de classificação pode ser aumentada. Por exemplo, a avaliação do de-

sempenho de uma regra mais antiga pode revelar que a regra mais antiga é agora mais eficaz devido à alteração dos padrões de SPAM.

[00070] Quando nenhuma regra adicional deve ser aplicada à mensagem não classificada 101U, o classificador de mensagem 102 pode usar resultados acumulativos 113 para classificar a mensagem não classificada 101U. Por exemplo, a partir dos resultados acumulativos 113, o classificador de mensagem 102 pode classificar a mensagem não classificada 101U como uma mensagem válida ou como uma mensagem indesejada e/ou não solicitada (por exemplo, SPAM), como incluindo ou não incluindo malware, como incluindo ou não incluindo informação confidencial, etc. O classificador de mensagem 102 pode emitir a mensagem classificada 101C para indicar a classificação.

[00071] Mediante a emissão da mensagem classificada 101C, o classificador de mensagem 102 pode transitar para classificar uma próxima mensagem eletrônica.

[00072] A Figura 2 ilustra uma arquitetura de computador exemplificativa 200 que facilita selecionar adaptativamente regras usadas para classificar mensagens eletrônicas. Em referência à Figura 2, a arquitetura de computador 200 inclui classificador de mensagem 202, regras de classificação de mensagem 221, e módulo de reordenação e seleção de regra 216. Cada um dos componentes revelados é conectado um ao outro por uma rede (ou é parte de), tais como, por exemplo, uma Rede de Área Local ("LAN"), uma Rede de Área Ampla ("WAN") e até mesmo a Internet. Consequentemente, cada um dos componentes revelados bem como quaisquer outros sistemas de computador e seus componentes conectados, pode criar dados relacionados à mensagem e trocar os dados relacionados à mensagem (por exemplo, dados de Protocolo de Internet ("IP") e outros protocolos de camada superior que utilizam dados de IP, tais como, Protocolo de Controle de Transmissão ("TCP"), Protocolo de Transferência de Hipertexto ("HTTP"),

Protocolo de Transferência de Correio Simples ("SMTP"), etc.) pela rede.

[00073] As regras 221 contêm uma pluralidade de regras de classificação de mensagem, tais como, por exemplo, as regras 221A a 221N, que podem ser usadas para classificar mensagens eletrônicas. De modo similar às regras 121, cada regra nas regras 221 pode indicar uma eficácia, custo, eficiência e pode incluir instruções.

[00074] Em geral, o classificador de mensagem 202 é configurado para classificar mensagens eletrônicas com base em características de mensagem eletrônica. Por exemplo, o classificador de mensagem pode receber mensagens não classificadas 201U como entrada e gerar mensagens classificadas 201C como saída. Cada mensagem nas mensagens classificadas 201C pode ser classificada, por exemplo, para indicar se ou não a mensagem é SPAM, contém malware, contém informação confidencial, etc.

[00075] Conforme revelado, o classificador de mensagem 202 inclui módulo de operação 203, que inclui adicionalmente monitor de recurso 213, e sintetizador de eficiência 214. O módulo de operação 203 é configurado para operar instruções (por exemplo, scripts ou outro código executável) incluídas em uma regra recebida. As instruções produzem um resultado individual (potencialmente submetido à retroalimentação externa de usuário) que pode ser usado como um ponto de dados para classificar uma mensagem eletrônica. O monitor de recurso 213 pode monitorar (por exemplo, em tempo essencialmente real) uma quantidade de vários recursos consumidos (por exemplo, memória de sistema, processador, largura de banda de rede, etc.) durante a execução da regra.

[00076] O sintetizador de eficiência 214 pode receber um resultado e uma indicação de recursos consumidos e sintetizar uma eficiência atualizada para uma regra aplicada. Os resultados e recursos consu-

midos para uma regra aplicada podem também ser usados para atualizar a eficácia e/ou custo para a regra para consistência com uma eficiência sintetizada.

[00077] Como tal, o custo e a eficácia de cada regra de classificação podem ser valores medidos, medidos em um ponto no tempo particular (por exemplo, quando aplicados), e podem alterar ao longo do tempo. Conforme os padrões e o conteúdo de spam evoluem, uma regra de classificação pode se tornar mais ou menos eficaz. Se uma campanha de SPAM histórica particular experimentar um ressurgimento em volume, uma regra mais antiga pode repentinamente se tornar mais eficaz. Adicionalmente, conforme o software é atualizado e otimizado, um custo de regra pode diminuir.

[00078] O módulo de reordenação e seleção de regra 216 pode selecionar regras, a partir de regras de classificação de mensagem 221, para aplicação a uma mensagem eletrônica (por exemplo, com base em eficiência). O módulo de reordenação e seleção de regra 216 também pode classificar as regras de classificação de mensagem 221 (por exemplo, com base em eficiência).

[00079] A Figura 4 ilustra um fluxograma de um método exemplificativo 400 para selecionar adaptativamente regras usadas para classificar mensagens eletrônicas. O método 400 será descrito em relação aos componentes e dados de arquitetura de computador 200.

[00080] O método 400 inclui um ato de recepção de uma ou mais mensagens eletrônicas (ato 401). Por exemplo, o classificador de mensagem 202 pode receber mensagens não classificadas 201U.

[00081] Para cada uma das uma ou mais mensagens eletrônicas, o método 400 inclui um ato de aplicação de cada regra de classificação de mensagem em um subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica à mensagem eletrônica, em que o subconjunto anteriormente selecionado de regras de classifi-

cação de mensagem eletrônica é um subconjunto da pluralidade de regras de classificação de mensagem eletrônica (ato 402). Por exemplo, o classificador de mensagem 202 pode aplicar regras 221A a 221C a cada mensagem em mensagens não classificadas 201U (por exemplo, com base em eficácia mínima e custo máximo em um SLA e possivelmente também uma porcentagem de neutralização).

[00082] Para cada regra de classificação de mensagem eletrônica no subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica, o método 400 inclui um ato da regra de mensagem eletrônica que calcula um resultado que indica uma probabilidade da mensagem eletrônica que tem uma característica de mensagem especificada (ato 403). Por exemplo, o módulo de operação 203 pode executar instruções 226A contra uma mensagem não classificada em 201U para gerar o resultado 212. O resultado 212 pode indicar uma probabilidade da mensagem em 201U que é uma mensagem eletrônica indesejada, uma mensagem eletrônica infectada ou perigosa, que contém informação confidencial, etc. (por exemplo, com base no recipiente designado da mensagem). Os resultados para as regras 221B e 221C também podem ser calculados.

[00083] A retroalimentação externa (por exemplo, de um usuário) pode ser incorporada em um resultado calculado. Por exemplo, a retroalimentação externa 261 pode ser incorporada no resultado 212. A retroalimentação externa pode elevar ou abaixar uma eficácia calculada com base na percepção de eficácia do usuário. Quando apropriado, a retroalimentação externa também pode ser incorporada em resultados calculados para as regras 221B e 221C.

[00084] Em algumas modalidades, as mensagens eletrônicas que contêm SPAM não capturado, malware ou informação confidencial (falsos negativos) bem como as mensagens classificadas válidas que incluem SPAM, malware, ou informação confidencial (falsos positivos)

são submetidas à análise adicional. Esse tipo de retroalimentação também pode ser usado para sintonizar os placares de eficiência.

[00085] Para cada regra de classificação de mensagem eletrônica no subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica, o método 400 inclui um ato de medição de um custo de recurso que indica uma quantidade de recursos consumidos para aplicar a regra de classificação de mensagem eletrônica à mensagem eletrônica (ato 404). Por exemplo, o monitor de recurso 213 pode medir um custo de recurso que indica uma quantidade de recursos consumidos 231 consumidos pela execução das instruções 226A contra a mensagem de 201U. Os custos de consumo de recurso para as regras 221B e 221C também podem ser medidos.

[00086] O método 400 inclui um ato de retenção do resultado calculado e do custo de recurso medido associado à aplicação de cada regra de classificação de correio eletrônico a cada mensagem eletrônica (ato 405). Por exemplo, o classificador de mensagem 202 pode reter o resultado 212 e os recursos consumidos 231 junto com os custos de recurso para executar a regra 221A contra outras mensagens em mensagens não classificadas 201U. Os resultados e os custos de recurso para execução das regras 221B e 221C contra as mensagens de mensagens não classificadas 201U também podem ser retidos.

[00087] Para cada regra de classificação de mensagem no subconjunto anteriormente selecionado de regras de classificação de mensagem, o método 400 inclui um ato de sintetização de uma métrica de eficiência dos resultados calculados e dos custos de recurso medidos retidos para a regra de classificação de mensagem (ato 406). Dessa forma, para cada uma das regras 221A, 221B, e 221C, o sintetizador de eficiência 214 pode sintetizar uma métrica de eficiência dos resultados calculados e dos custos de recurso medidos retidos. Por exemplo, para a regra 221A, o sintetizador de eficiência 214 pode sintetizar

a eficiência sintetizada 232 do resultado 212 e dos recursos de consumidor 231 bem como de resultados calculados e custos de recurso medidos da aplicação da regra 221A a outras mensagens em mensagens não classificadas 201U. As eficiências também podem ser sintetizadas para as regras 221B e 221C.

[00088] O classificador de mensagem 202 pode, então, substituir 224A pela eficiência sintetizada com 232. A eficácia 222A e o custo 223A também podem ser atualizados conforme apropriado para consistência com a eficiência sintetizada 232. As eficiências, as eficácias e os custos para as regras 221B e 221C também podem ser atualizadas conforme apropriado.

[00089] O método 400 inclui um ato de comparação das métricas de eficiência sintetizadas com as métricas de eficiência existentes para as regras de classificação de mensagem eletrônica incluídas na pluralidade de regras de classificação de mensagem eletrônica (ato 407). Por exemplo, a eficiência sintetizada 232 pode ser comparada com as eficiências contidas em outras regras de classificação de mensagem 221. As eficiências sintetizadas para as regras 221B e 221C também podem ser as eficiências contidas em outras regras de classificação de mensagem 221.

[00090] O método 400 inclui um ato de seleção de um novo subconjunto de regras de classificação de mensagem eletrônica, dentre a pluralidade de regras de classificação de mensagem eletrônica, para uso na classificação de mensagens eletrônicas subsequentemente recebidas com base pelo menos em parte em resultados da comparação das métricas de eficiência sintetizadas com as métricas de eficiência existentes (ato 408). Por exemplo, com base em eficiências sintetizadas, as regras 221A, 221B, e 221C podem se tornar mais ou menos eficientes em relação a uma outra bem como em relação a outras regras de classificação de mensagem 221. Como tal, uma ou mais regras 221,

221B, e 221C podem cair quando um novo subconjunto de regras (por exemplo, com base em um SLA) é selecionado para classificação de mensagens eletrônicas.

[00091] Em algumas modalidades, o custo e a eficácia para as regras de classificação de mensagem são continuamente remeidos (por exemplo, por um dia), posto que medições ativas são retiradas sobre a eficácia relativa de cada regra na classificação de mensagens (por exemplo, captura de SPAM, malware, informação confidencial, etc.) e os custos reais observados de operação das regras. Para regras mais eficientes, existem mais dados sobre a eficácia e o custo da regra conforme é operada contra mais mensagens. Para regras menos eficientes, o percentual de neutralização (ou escolha aleatória), tal como, por exemplo, 1%, desde que pelo menos uma quantidade de linha de base informação de atualização de custo e eficácia seja coletada. Conforme o custo e a eficácia são recalculados, então, o placar de eficiência que é usado para ordenar as regras. As mensagens eletrônicas subsequentes são classificadas com o uso de regras de classificação de mensagem que são selecionadas com base nos placares atualizados.

[00092] Conforme novas regras são gravadas (por exemplo, para capturar novos tipos de spam ou malware), o tamanho da regra cresce. As regras recém-introduzidas podem ser introduzidas com um placar de eficiência de 0 e um placar de 1, o que leva a um placar de eficiência de 0 e coloca a regra no final da lista. Ao longo do tempo, conforme a regra é aplicada às mensagens de acordo com uma porcentagem de neutralização, os dados reais suficientes podem ser eventualmente acumulados para calcular valores mais realistas para custo e eficácia para a nova regra, e dessa forma placares de eficiência mais apropriados. Conforme os placares de eficiência são recalculados, as novas regras migrarão automaticamente para sua ordem ideal na lista.

[00093] Ao longo do tempo, um corpo da regra pode crescer muito para operar plausivelmente com base em uma porcentagem de neutralização atual (por exemplo, 1%). Como tal, uma outra fileira pode ser adicionada, onde as regras com um placar de eficiência que é menor que, talvez, 0,1 são operadas com base em uma porcentagem de neutralização reduzida, tal como, por exemplo, 0,1%. Os resultados de tais regras de eficiência baixa podem não ainda ser usados para classificar mensagens, mas, em vez disso, apenas usados para gerar informação de custo e eficácia atualizada.

[00094] A Figura 5 ilustra a arquitetura de computador exemplificativa 500 que facilita a varredura de mensagem eletrônica adaptativa e a seleção adaptativa de regras usadas para classificar mensagens eletrônicas.

[00095] O correio não classificado 501U é recebido. A informação de remetente/recipientes é enviada para a classe de cliente 531. A classe de cliente 531 identifica uma eficácia mínima para uso mediante a classificação de mensagem não classificada 501U. No estágio 541, a eficácia mínima para classe de cliente 531 é alcançada a partir de regras em operação 511A, 511B e 511C. No estágio 542, uma ou mais regras adicionais, que incluem regra 511D, são operadas de modo oportuno conforme a disponibilidade de recurso 504 permite. No estágio 543, a decisão de não operar uma ou mais outras regras até a regra 511N é neutralizada com base em escolha aleatória 518 e essas uma ou outras regras suprem a regra 511N que são operadas. Com base nos resultados de regras 511A a 511N, o correio classificado 501C (por exemplo, como SPAM ou válido) é emitido.

[00096] Os dados de desempenho são coletados pelo tempo de operação de cada regra 503 para as regras 511A a 511N. Os placares de custo atualizados são gravados de volta nas regras 511A a 511N. O resultado de cada regra 512 como positivo (por exemplo, é SPAM)

ou negativo (por exemplo, válida) é determinado para as regras 511A a 511N. A retroalimentação externa 561 é incorporada para identificar falsos positivos e falsos negativos nos resultados. Os placares de eficiência atualizados são gravados de volta nas regras 511A a 511N. As eficiências são recalculadas e as regras reordenadas com base nas eficiências recalculadas.

[00097] A presente invenção pode ser incorporada em outras formas específicas sem que se afaste de seu espírito ou características essenciais. As modalidades descritas devem ser consideradas em todos os aspectos apenas como ilustrativas e não restritivas. O escopo da invenção é, portanto, indicado pelas reivindicações anexas de preferência pela descrição supracitada. Todas as alterações que se enquadram no significado e na faixa de equivalência das reivindicações devem ser abrangidas dentro de seu escopo.

REIVINDICAÇÕES

1. Método (400) para selecionar adaptativamente regras usadas para classificar mensagens eletrônicas, **caracterizado pelo fato de que** compreende as etapas de:

receber (401) uma ou mais mensagens eletrônicas;

para cada uma ou mais mensagens eletrônicas, calcular um resultado que indica uma probabilidade da mensagem eletrônica que tem uma característica de mensagem especificada através da aplicação de cada regra de classificação de mensagem em um subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica;

medir (404) um custo de recurso que indica uma quantidade de recursos consumidos para aplicar cada regra de classificação de mensagem eletrônica a cada uma das uma ou mais mensagens eletrônicas;

para cada regra de classificação de mensagem no subconjunto anteriormente selecionado de regras de classificação de mensagem, sintetizar (406) de uma métrica de eficiência dos resultados calculados e custos de recurso medidos para a regra de classificação de mensagem;

comparar (407) das métricas de eficiência sintetizadas para métricas de eficiência existentes para regras de classificação de mensagem eletrônica incluídas na pluralidade de regras de classificação de mensagem eletrônica; e

selecionar (408) de um novo subconjunto de regras de classificação de mensagem eletrônica, dentre a pluralidade de regras de classificação de mensagem eletrônica, para uso na classificação de mensagens eletrônicas subsequentemente recebidas com base pelo menos em parte nos resultados de comparação das métricas de eficiência sintetizadas para métricas de eficiência existentes.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** selecionar um novo subconjunto de regras de classificação de mensagem eletrônica compreende selecionar um novo subconjunto de regras de classificação de mensagem eletrônica de acordo com um Acordo de Nível de Serviço ("SLA").

3. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** selecionar um novo subconjunto de regras de classificação de mensagem eletrônica compreende reordenar a pluralidade da pluralidade de regras de classificação de mensagem eletrônica com base em placares de eficiência.

4. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a recepção de uma ou mais mensagens eletrônicas compreende receber uma ou mais mensagens de correio eletrônico.

5. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** receber uma ou mais mensagens eletrônicas compreende receber uma ou mais mensagens de Serviço de Mensagem Curta ("SMS").

6. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** receber uma ou mais mensagens eletrônicas compreende receber um ou mais arquivos.

7. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a pluralidade de regras de classificação de mensagem eletrônica é usada para classificar mensagens eletrônicas como SPAM ou como válida.

8. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a pluralidade de regras de classificação de mensagem eletrônica é usada para classificar mensagens eletrônicas como contendo malware ou não contendo malware.

9. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a pluralidade de regras de classificação de mensa-

gem eletrônica é usada para classificar mensagens eletrônicas como contendo informação digital confidencial ou não contendo informação digital confidencial.

10. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** ainda compreende, antes de aplicar cada regra de classificação de mensagem em um subconjunto anteriormente selecionado de regras de classificação de mensagem eletrônica, selecionar o subconjunto de regras de classificação de mensagem eletrônica selecionado com base em placares de eficiência calculados.

11. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** ainda compreende:

receber retroalimentação externa relacionada à aplicação de pelo menos uma regra de classificação de mensagem a uma mensagem eletrônica; e

incorporar a retroalimentação externa no resultado calculado a partir da aplicação de pelo menos uma regra de classificação de mensagem à mensagem eletrônica.

12. Método, de acordo com a reivindicação 11, **caracterizado pelo fato de que** a retroalimentação externa recebida indica que o resultado calculado a partir da aplicação de pelo menos uma regra de classificação de mensagem para a mensagem eletrônica é um dentre: um falso negativo ou um falso positivo.

13. Método, de acordo com a reivindicação 11, **caracterizado pelo fato de que** ainda compreende atualizar um placar de eficiência para pelo menos uma regra de classificação de mensagem com base no resultado calculado que incorpora a retroalimentação externa.

14. Sistema para selecionar adaptativamente regras de detecção de SPAM que compreende:

um ou mais processadores;
memória de sistema;

um ou mais meios de armazenamento em computador que têm armazenadas neles uma pluralidade de regras de detecção de SPAM e possuindo um método que representa um classificador de mensagem e uma seleção de regra e um módulo de reordenação, **caracterizado pelo fato de que** o classificador de mensagem é configurado para:

receber uma ou mais mensagens de correio eletrônico;

para cada uma das uma ou mais mensagens de correio eletrônico, aplicar cada regra de detecção de SPAM em um subconjunto anteriormente selecionado de regras de detecção de SPAM à mensagem de correio eletrônico, em que o subconjunto anteriormente selecionado de regras de detecção de SPAM é um subconjunto da pluralidade de regras de detecção de SPAM; e

para cada regra de detecção de SPAM no subconjunto anteriormente selecionado de regras de detecção de SPAM:

calcular um resultado que indica uma probabilidade da mensagem de correio eletrônico ser SPAM;

medir um custo de recurso que indica uma quantidade de recursos consumido para aplicar a regra de detecção de SPAM a cada uma das uma ou mais mensagens de correio eletrônico; e

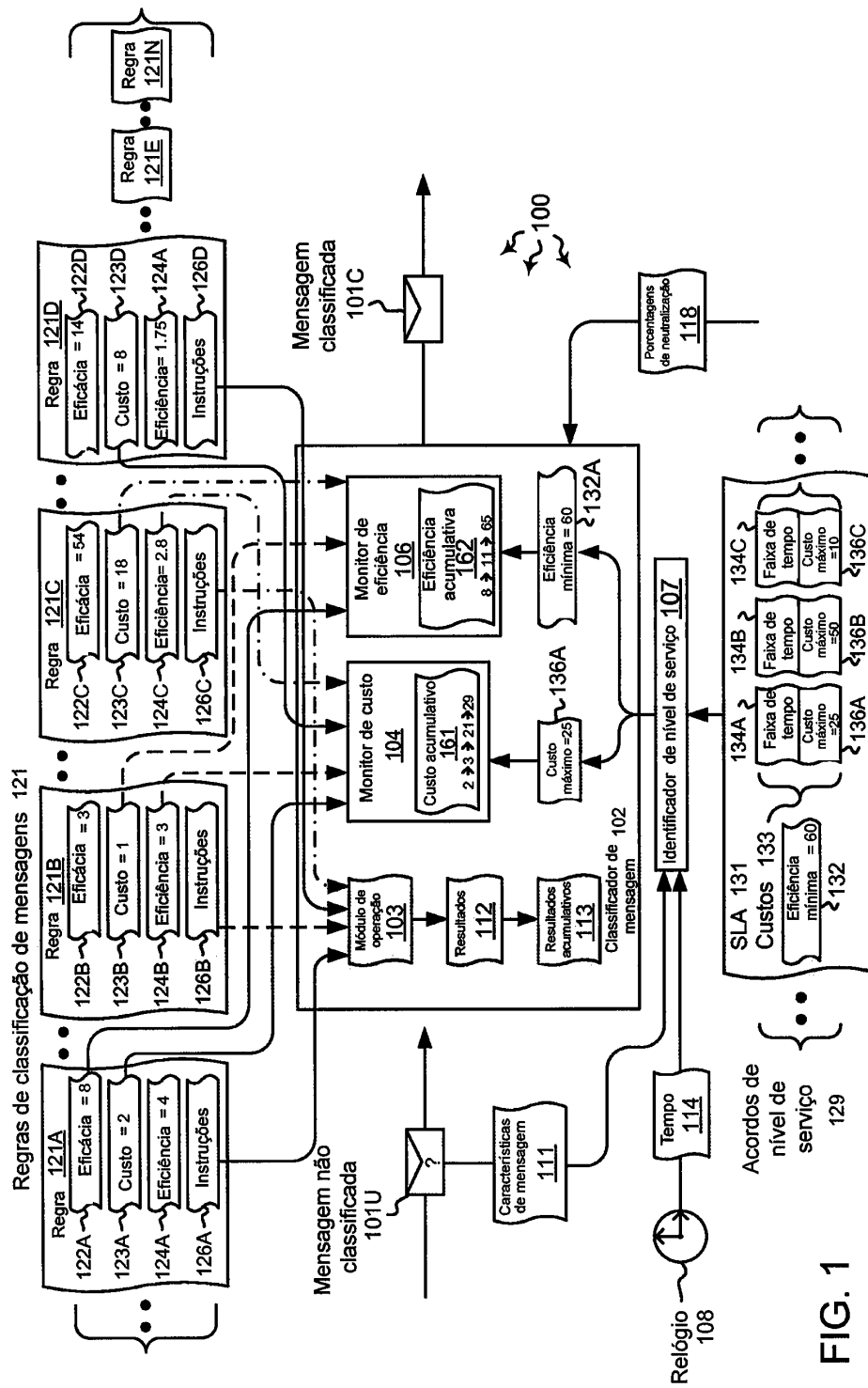
sintetizar uma métrica de eficiência a partir dos resultados calculados e custos de recurso medidos para a regra de detecção de SPAM; e

em que a seleção de regra e o módulo de reordenação é configurado para:

comparar as métricas de eficiência sintetizadas com as métricas de eficiência existentes para regras de detecção de SPAM incluídas na pluralidade de regras de detecção de SPAM; e

selecionar um novo subconjunto de regras de detecção de SPAM para uso na classificação de mensagens de correio eletrônico

subsequentemente recebidas com base pelo menos em parte em resultados da comparação das métricas de eficiência sintetizadas com as métricas de eficiência existentes.



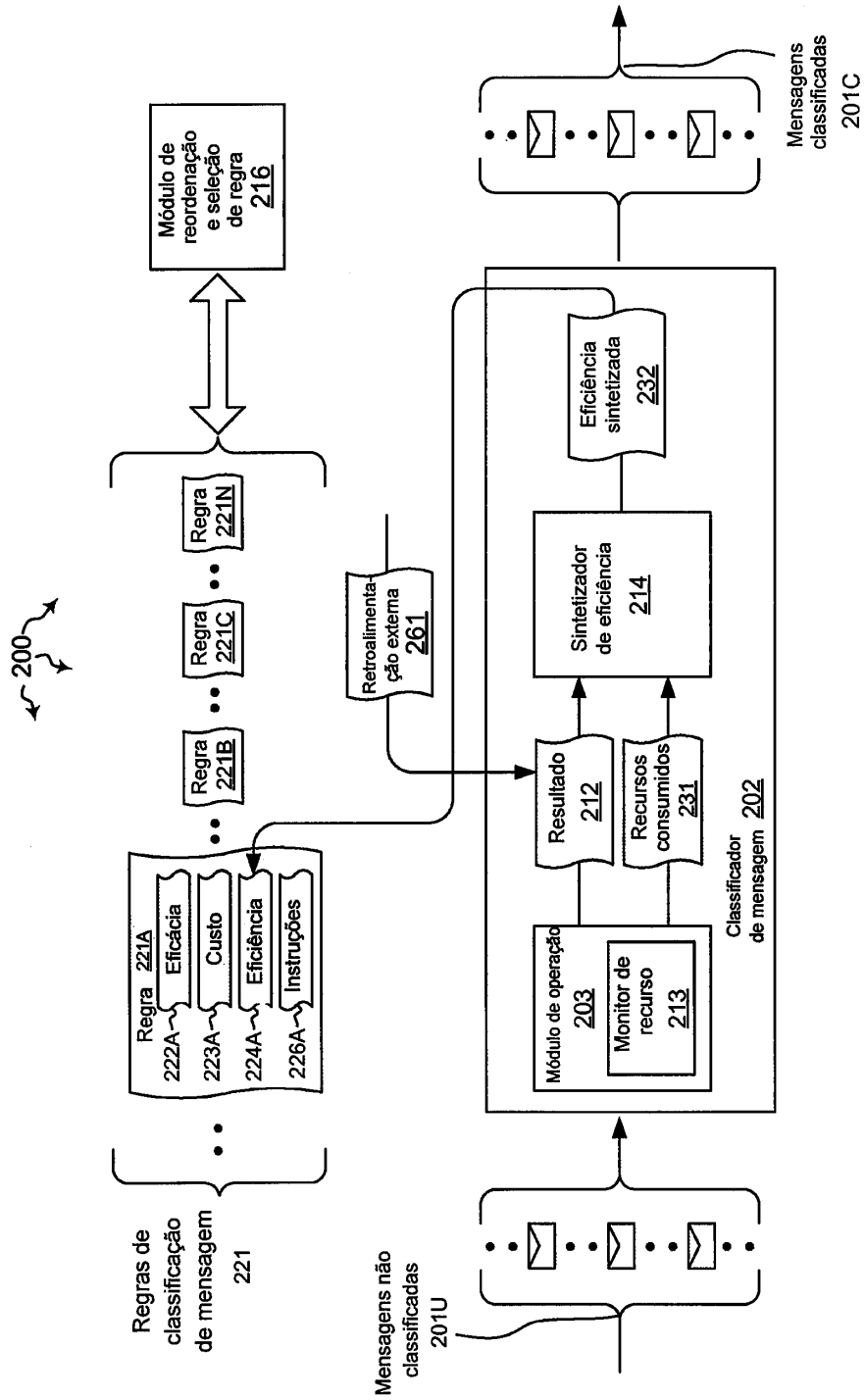


FIG. 2

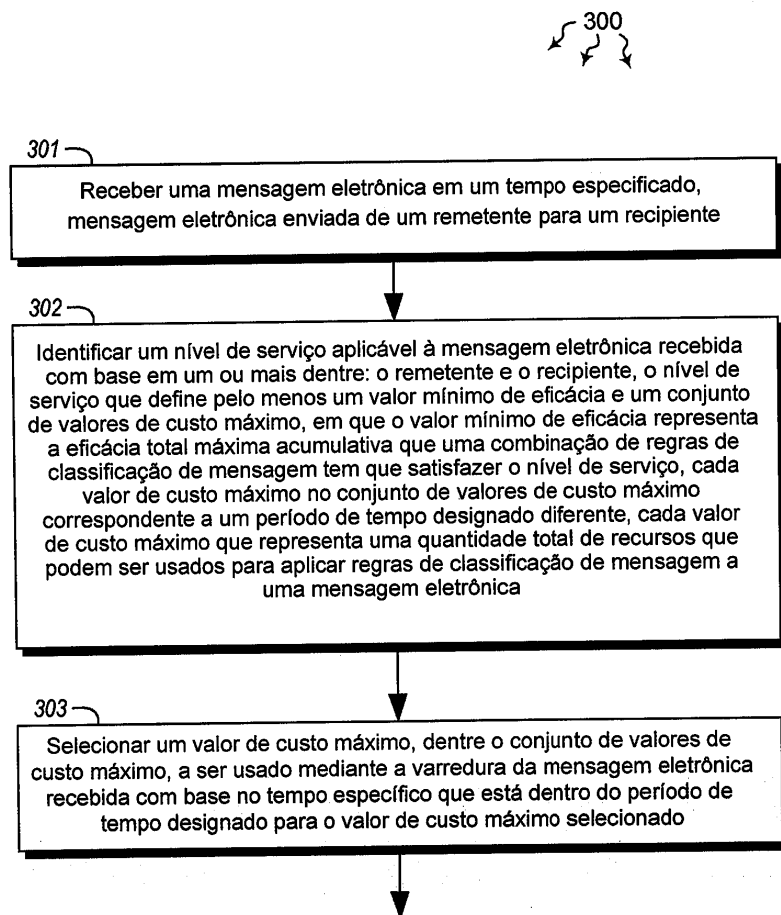


FIG. 3

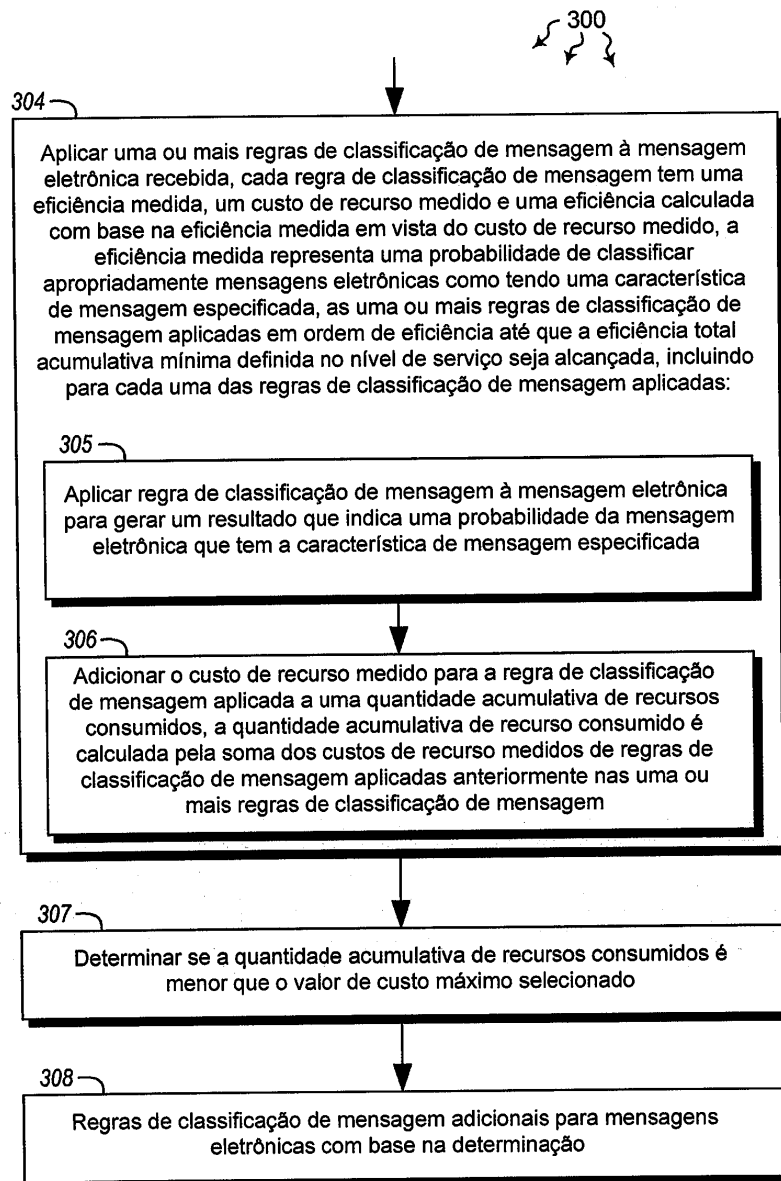


FIG. 3
(Continuação)

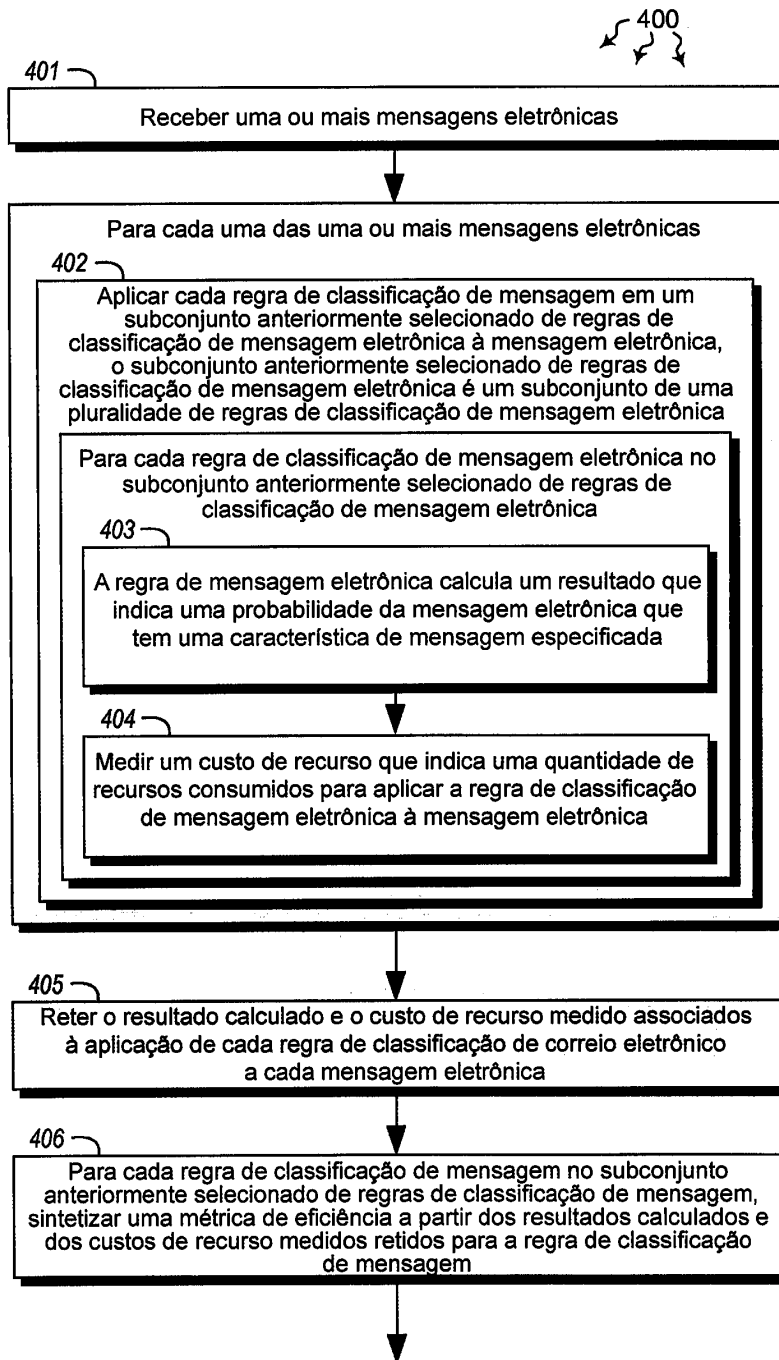


FIG. 4

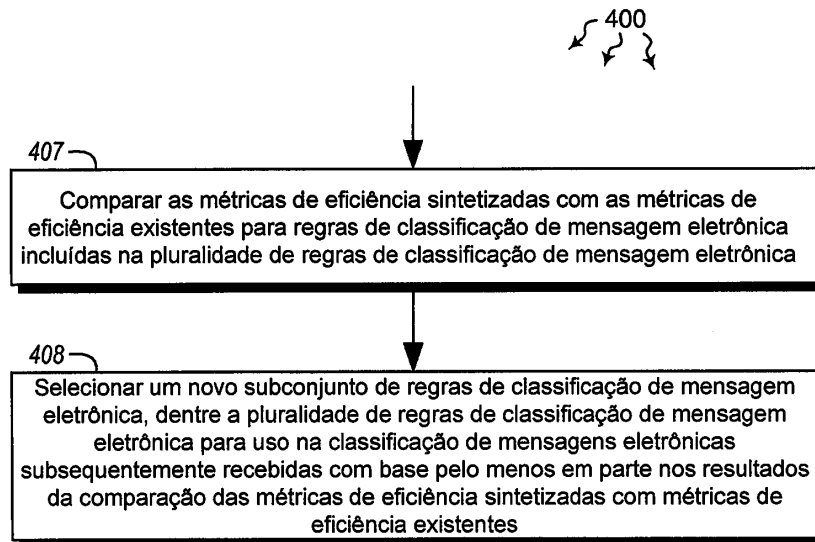


FIG. 4
(Continuação)

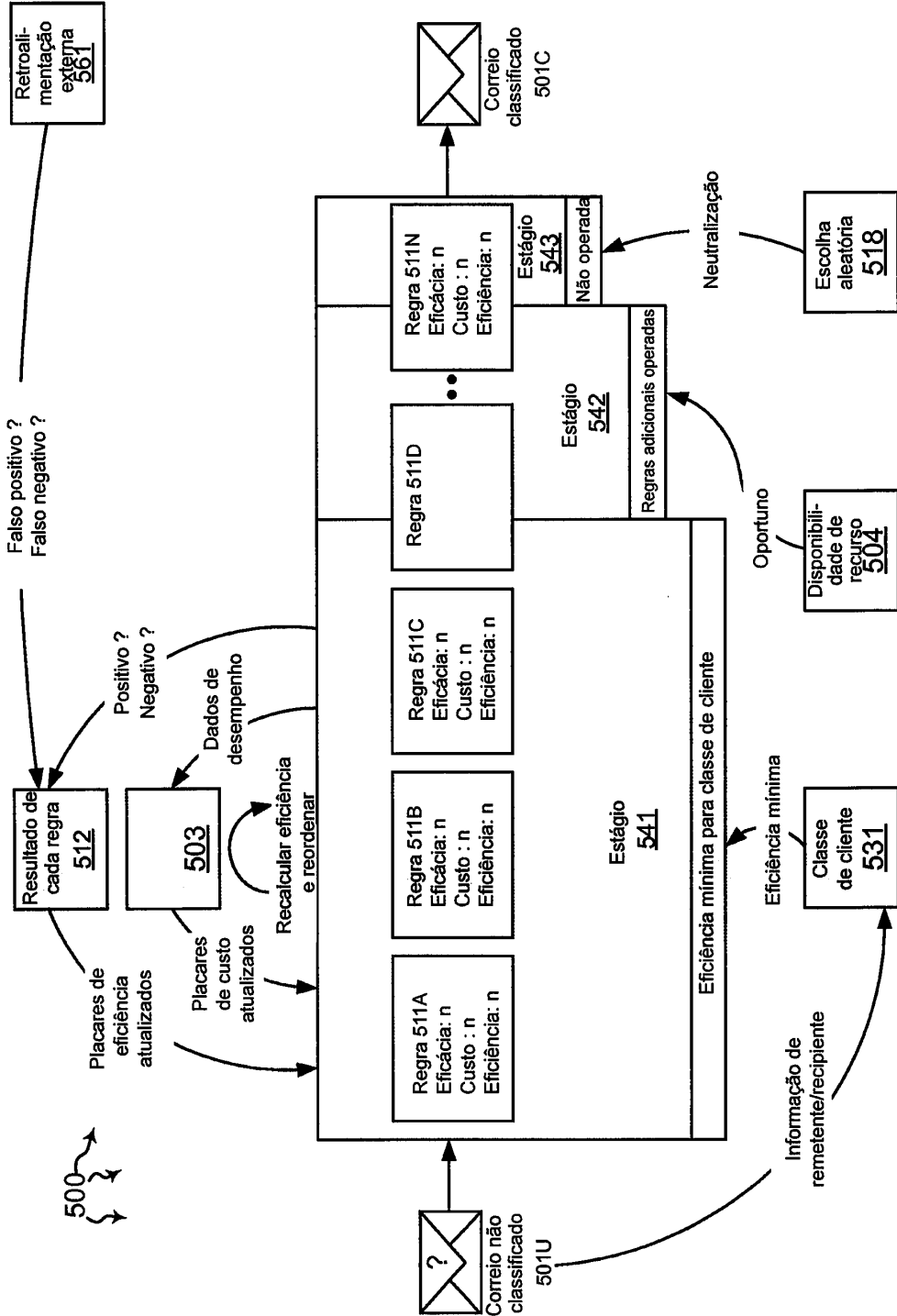


FIG. 5