(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103095672 A
(43)申请公布日 2013.05.08

(21)申请号 201210348030.2
(22)申请日 2008.01.24
(30)优先权数据
11/626,603 2007.01.24 US
(62)分案原申请数据
200880009762.0 2008.01.24
(71)申请人 迈可菲公司
地址 美国加利福尼亚州
(72)发明人 D. 阿尔佩罗维奇 T. 富特－伦诺瓦
J. 古尔德 P. 格里夫
A.M. 埃尔南德斯 P. 朱格
S. 克拉泽 T. 朗格 P.A. 施内克
M. 施特赫尔 Y. 唐
A.J.N. 特里维迪 L.L. 维利斯
W. 杨 J.A. 齐齐亚斯基
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 马丽娜 朱海煜
(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/55(2013.01)

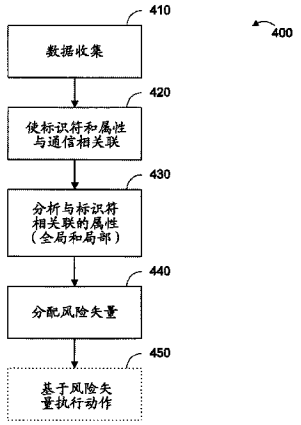
权利要求书2页 说明书15页 附图19页

(54)发明名称

多维声誉评分

(57)摘要

用于给通信实体分配声誉的方法和系统包括从分布的代理收集通信数据，汇聚通信数据，分析通信数据，以及根据通信数据识别通信实体之间的关系。



CN 103095672 A

1. 一种计算机实现的方法，包括以下步骤：

为多个过滤器设置中的每一个识别值的范围，其中过滤器设置值为网络中可能的安全危害的相关分类限定容忍度水平；

使得在显示设备上呈现安全控制界面，该安全控制界面包括多个图形安全控件，每个图形安全控件代表该多个过滤器设置中的相应的一个过滤器设置和该相应的过滤器设置的对应的值范围；

基于与安全控制界面的该多个图形安全控件中的对应的一个图形安全控件的用户交互接收该多个过滤器设置中的特定的一个过滤器设置的值；

基于所接收的值调整该特定过滤器设置；以及

基于所调整的特定过滤器设置使得网络中的通信被过滤。

2. 根据权利要求 1 所述的方法，其中所调整的被过滤的设置是特定用户的被调整的过滤器设置并且适用于涉及该特定用户的通信流。

3. 根据权利要求 2 所述的方法，其中用户交互与该特定用户相关联。

4. 根据权利要求 1 所述的方法，其中图形安全控件包括可操作来被操纵以对应于对应过滤器设置的相应范围内的值的多个交互式安全滑动控件。

5. 根据权利要求 1 所述的方法，其中每个安全过滤器与多个可能的安全危害类别中的一个相关联。

6. 根据权利要求 5 所述的方法，其中该多个可能的安全危害类别包括病毒类别、网络钓鱼类别、蠕虫类别、特洛伊木马类别、垃圾邮件类别、内容类别、间谍软件类别、或群发邮件类别。

7. 根据权利要求 1 所述的方法，其中每个值范围中的每个值指示可能的安全危害的对应分类的相对过滤水平。

8. 根据权利要求 1 所述的方法，其中该特定过滤器设置的值范围是被限定的有限的值范围。

9. 根据权利要求 8 所述的方法，其中代表该特定过滤器设置并使得能够调整该特定过滤器设置的图形安全控件指示该特定过滤器设置的值范围是有限的。

10. 根据权利要求 8 所述的方法，其中对该特定过滤器的值范围的限制被隐藏在安全控制界面的呈现上。

11. 根据权利要求 8 所述的方法，其中该特定过滤器设置的值范围被限制以将值的选择中的至少一个约束在该特定过滤器设置的被限定的最大值之上并且将值的选择约束在该特定过滤器设置的被限定的最小值之下。

12. 根据权利要求 8 所述的方法，其中该多个过滤器设置包括安全设置组和策略设置组，其中安全设置组中的每个过滤器设置的值范围是相应被限定的有限的值范围。

13. 根据权利要求 12 所述的方法，其中策略设置组中的每个过滤器设置的值范围是无约束的。

14. 根据权利要求 1 所述的方法，其中使用在网络中配置的多个安全代理来过滤该网络，并且所调整的特定过滤器设置支配在该多个安全代理中的至少一个特定安全代理的过滤。

15. 根据权利要求 14 所述的方法，其中特定安全代理的调整适用于特定用户并且至少

部分地使用该特定安全代理来过滤涉及该特定用户的通信。

16. 根据权利要求 14 所述的方法，其中安全代理基于通信中涉及的至少一个实体的声誉过滤所述通信。

17. 根据权利要求 16 所述的方法，其中特定实体的声誉基于该特定实体和具有确定的声誉得分的至少一个其它实体之间的被识别的属性相似性。

18. 根据权利要求 16 所述的方法，其中该特定过滤器设置限定将被应用于所述通信中所涉及的实体的声誉的局部偏置。

19. 在非临时性的介质中被编码的逻辑，其包括用于执行的代码并且当被处理器执行时可操作来执行包括下述步骤的操作：

为多个过滤器设置中的每一个识别值的范围，其中过滤器设置值为网络中可能的安全危害的相关分类限定容忍度水平；

使得在显示设备上呈现安全控制界面，该安全控制界面包括多个图形安全控件，每个图形安全控件代表该多个过滤器设置中的相应的一个过滤器设置和该相应的过滤器设置的对应的值范围；

基于与安全控制界面的该多个图形安全控件中的对应的一个图形安全控件的用户交互接收该多个过滤器设置中的特定的一个过滤器设置的值；

基于所接收的值调整该特定过滤器设置；以及

基于所调整的特定过滤器设置使得网络中的通信被过滤。

20. 一种系统，包括：

至少一个处理器设备；

至少一个存储元件；和

安全控制界面，其当被该至少一个处理器设备执行时适于：

呈现安全控制界面，该安全控制界面包括多个图形安全控件，每个图形安全控件代表该多个过滤器设置中的相应的一个过滤器设置和每个相应的过滤器设置的对应的值范围，其中过滤器设置值为可能的安全危害的相关分类限定容忍度水平；以及

接受与图形安全控件的用户交互以识别对应过滤器设置的用户规定的值，其中过滤器设置的用户说明引起对过滤器设置的值的修改；

适于根据该多个过滤器设置过滤网络中的通信的安全代理。

21. 根据权利要求 20 所述的系统，进一步包括适于确定网络中的通信中涉及的多个实体的声誉的声誉引擎，其中安全代理进一步适于基于通信中涉及的实体的所识别的声誉来过滤所述通信。

22. 根据权利要求 20 所述的系统，其中使用安全控制界面调整过滤器设置将过滤器设置的调整应用于不超过整个网络。

23. 根据权利要求 22 所述的系统，其中过滤器的设置的调整适用于涉及与该调整相关联的特定用户的通信。

多维声誉评分

[0001] 本申请是申请号为 200880009762.0、申请日为 2008 年 1 月 24 日、发明名称为“多维声誉评分”的申请的分案申请。

技术领域

[0002] 本文件通常涉及用于处理通信 (communication) 的系统和方法，尤其是涉及用于给与通信相关的实体进行分类的系统和方法。

背景技术

[0003] 在反垃圾邮件行业中，垃圾邮件发送者使用各种创造性的装置来躲避垃圾邮件过滤器进行的检测。这样，通信从其起源的实体可提供是否应允许给定通信进入企业网络环境的另一指示。

[0004] 然而，用于消息发送者进行分析的当前工具包括互联网协议 (IP) 黑名单 (有时称为实时黑名单 (RBL)) 和 IP 白名单 (实时白名单 (RWL))。白名单和黑名单当然对垃圾邮件分类过程增加了益处；然而，白名单和黑名单内在地限于响应于每个查询而提供一个二进制类型 (YES/NO)。而且，黑名单和白名单独立地处理实体，并忽略与实体相关的各种属性所提供的证据。

发明内容

[0005] 提供了分布式声誉体系结构的系统和方法。分布式声誉系统可包括通信接口、数据汇聚引擎、分析器、关联引擎和声誉引擎。通信接口可与布置在全局网络内的多个代理进行通信。数据汇聚引擎可通过通信接口汇聚所收集的数据。分析器可分析数据，以识别分别与发起所接收的通信相关联的属性。关联引擎可关联实体的属性并识别实体之间的关系。声誉引擎可识别实体之间的关系并根据其与一个或更多个其它实体的关系更新与一个或更多个实体相关联的声誉。通信接口也可将更新的声誉信息传递到在全局网络上操作的设备。

[0006] 可操作来获得并分配声誉的其它系统可包括通信接口、数据汇聚引擎、分析器、关联引擎、声誉引擎和业务量控制引擎。通信接口可从全局网络内的代理或中央服务器接收信息。数据汇聚引擎可汇聚来自通信接口的所接收的信息。分析器可分析所接收的信息，以识别分别与发起所接收的通信的实体相关联的属性。关联引擎可关联实体的属性并识别实体之间的关系。声誉引擎可识别实体之间的关系并根据其与一个或更多个其它实体的关系更新与一个或更多个实体相关联的声誉。业务量控制引擎可根据更新的声誉确定与通信相关联的处理。

[0007] 给通信实体分配声誉的方法可包括：将多个代理布置在网络内，所述多个代理与安全设备相关联，所述安全设备可操作来保护相关联的网络免受违反与相关联的网络关联的策略的通信；收集与发起通信的实体相关联的数据，其中收集数据包括使用多个代理来收集与通信相关联的数据；汇聚所收集的数据；分析所汇聚的数据以识别分别与发起通信

的实体相关联的属性；关联属性以识别实体之间的关系；根据通过关联属性而识别的与一个或更多个其它实体的关系来更新与一个或更多个实体相关的声誉；以及将更新的声誉信息传递到所述多个代理中的一个或更多个代理。

[0008] 向通信实体分配声誉的方法可包括：收集与发起通信的实体相关联的数据，其中收集数据包括从多个代理接收数据以收集与通信相关联的数据；汇聚所收集的数据；分析所汇聚的数据以识别分别与发起通信的实体相关联的属性；关联属性以识别实体之间的关系；根据通过关联属性而识别的与一个或更多个其它实体的关系来更新与一个或更多个实体相关联的声誉；以及根据更新的声誉信息处理通信。

附图说明

[0009] 图 1 是描述示例性网络的结构图，本公开的系统和方法可在该网络中进行操作。

[0010] 图 2 是描述本公开的示例性网络体系结构的结构图。

[0011] 图 3 是描述通信和实体的例子的结构图，其包括用于检测实体之间的关系的标识符和属性。

[0012] 图 4 是描述用于检测关系并给实体分配风险的操作方案的流程图。

[0013] 图 5 是示出示例性网络体系结构的结构图，其包括局部安全代理所储存的局部声誉和一个或多个服务器所储存的全局声誉。

[0014] 图 6 是示出基于局部声誉反馈的全局声誉的确定的结构图。

[0015] 图 7 是示出全局声誉和局部声誉之间的示例性转化 (resolution) 的流程图。

[0016] 图 8 是用于调节与声誉服务器相关联的过滤器的设置的示例性图形用户界面。

[0017] 图 9 是示出用于互联网协议语音电话 (VoIP) 或短消息服务 (SMS) 通信的基于声誉的连接抑制 (connection throttling) 的结构图。

[0018] 图 10 是示出基于声誉的负载均衡器的结构图。

[0019] 图 11A 是示出用于基于地理位置的身份验证的示例性操作方案的流程图。

[0020] 图 11B 是示出用于基于地理位置的身份验证的另一示例性操作方案的流程图。

[0021] 图 11C 是示出用于基于地理位置的身份验证的另一示例性操作方案的流程图。

[0022] 图 12 是示出用于基于声誉的动态隔离的示例性操作方案的流程图。

[0023] 图 13 是图像垃圾邮件通信的示例性图形用户界面显示。

[0024] 图 14 是示出用于检测图像垃圾邮件的示例性操作方案的流程图。

[0025] 图 15A 是示出用于分析通信的结构的操作方案的流程图。

[0026] 图 15B 是示出用于分析图像的特征的操作方案的流程图。

[0027] 图 15C 是示出用于标准化图像以用于垃圾邮件处理的操作方案的流程图。

[0028] 图 15D 是示出用于分析图像的指纹以在多个图像中找到共同片段的操作方案的流程图。

具体实施方式

[0029] 图 1 是描述示例性网络环境的结构图，本公开的系统和方法可在该网络中进行操作。安全代理 (security agent)100 一般可存在于在网络 110（例如，企业网）内部的防火墙系统（未示出）和服务器（未示出）之间。如应被理解的，网络 110 可包括很多服务器，

包括例如可由与网络 110 相关的企业使用的电子邮件服务器、网络服务器和各种应用服务器。

[0030] 安全代理 100 监控进入和离开网络 110 的通信。一般通过互联网 120 从连接到互联网 120 的很多实体 130a-f 接收这些通信。实体 130a-f 中的一个或更多个可为通信业务量的合法发起者。然而，实体 130a-f 中的一个或更多个也可为发起不需要的通信的声誉差的实体。因此，安全代理 100 包括声誉引擎。声誉引擎可检查通信并确定与发起通信的实体相关联的声誉。安全代理 100 接着根据发端实体的声誉对通信执行动作。如果声誉指示通信的发起者声誉好，那么例如，安全代理可将通信转发到通信的接收者。然而，如果声誉指示通信的发起者声誉差，那么其中例如，安全代理可隔离通信，对消息执行更多的测试，或要求来自消息发起者的身份验证。在美国专利公布号 2006/0015942 中详细描述了声誉引擎，该申请由此通过引用被并入。

[0031] 图 2 是描述本公开的示例性网络体系结构的结构图。安全代理 100a-n 被示为在逻辑上分别存在于网络 110a-n 与互联网 120 之间。虽然没有在图 2 中示出，但应理解，防火墙可安装在安全代理 100a-n 和互联网 120 之间，以提供防止未授权的通信进入相应的网络 110a-n 的保护。而且，结合防火墙系统可配置侵入检测系统 (IDS)(未示出)，以识别活动的可疑模式并在这样的活动被识别出时用信号通知警报。

[0032] 虽然这样的系统对网络提供了某种保护，但它们一般不处理应用层安全威胁。例如，黑客常常试图使用各种网络类型的应用 (例如，电子邮件、网络、即时消息 (IM)，等等) 来产生与网络 110a-n 的前文本连接，以便利用由使用实体 130a-e 的这些不同的应用所产生的安全漏洞。然而，不是所有的实体 130a-e 都暗示对网络 100a-n 的威胁。一些实体 130a-e 发起合法的业务量，允许公司的雇员与商业伙伴更有效地进行通信。虽然对可能的威胁来说检查通信是有用的，但是维持当前的威胁信息可能很难，因为攻击被不断地改进以解决最近的过滤技术。因此，安全代理 100a-n 可对通信运行多次测试，以确定通信是否是合法的。

[0033] 此外，包括在通信中的发送者信息可用于帮助确定通信是否是合法的。因此，复杂的安全代理 100a-n 可跟踪实体并分析实体的特征，以帮助确定是否允许通信进入网络 110a-n。可接着给实体 110a-n 分配声誉。对通信的决定可考虑发起通信的实体 130a-e 的声誉。而且，一个或更多个中央系统 200 可收集关于实体 130a-e 的信息，并将所收集的数据分发到其它中央系统 200 和 / 或安全代理 100a-n。

[0034] 声誉引擎可帮助识别大量恶意通信，而没有通信的内容的广泛和可能昂贵的局部分析 (local analysis)。声誉引擎也可帮助识别合法通信，并优先考虑其传输，且减小了对合法通信进行错误分类的风险。而且，声誉引擎可在物理世界或虚拟世界中对识别恶意以及合法事务的问题提供动态和预言性的方法。例子包括在电子邮件、即时消息、VoIP、SMS 或利用发送者声誉和内容的分析的其它通信协议系统中过滤恶意通信的过程。安全代理 100a-n 可接着应用全局或局部策略，以确定关于通信对声誉结果执行什么动作 (例如拒绝、隔离、负载均衡、以所分配的优先级传输、以额外的细查局部地进行分析)。

[0035] 然而，实体 130a-e 可用各种方法连接到互联网。如应理解的，实体 130a-e 可同时或在一段时间内具有多个标识符 (例如，电子邮件地址、IP 地址、标识符文件，等等)。例如，具有变化的 IP 地址的邮件服务器可随着时间的过去具有多个身份。而且，一个标识符

可与多个实体相关，例如，当 IP 地址被很多用户支持的组织共享时。而且，用于连接到互联网的特定方法可能使实体 130a-e 的识别模糊不清。例如，实体 130b 可利用互联网服务提供商 (ISP)200 连接到互联网。很多 ISP 200 使用动态主机配置协议 (DHCP) 来将 IP 地址动态地分配给请求连接的实体 130b。实体 130a-e 也可通过欺骗合法实体来伪装其身份。因此，收集关于每个实体 130a-e 的特征的数据可帮助对实体 130a-e 加以分类，并确定如何处理通信。

[0036] 在虚拟世界和物理世界中创建和欺骗身份的容易性可能产生用户恶意动作的动机，而不承担该动作的后果。例如，在互联网上被罪犯盗取的合法实体的 IP 地址（或在物理世界中的被盗的护照）可能使该罪犯能够通过假装被盗的身份而相对容易地参与恶意行动。然而，通过给物理实体和虚拟实体分配声誉并识别它们可能使用的多个身份，声誉系统可能影响声誉好的实体和声誉差的实体来负责任地操作，以免变得声誉差且不能与其它网络实体交流或交互。

[0037] 图 3 是描述通信和实体的例子的结构图，其包括利用用于检测实体之间的关系的标识符和属性。安全代理 100a-b 可通过检查被送往相关网络的通信来收集数据。安全代理 100a-b 也可通过检查由相关网络分程传递的通信来收集数据。通信的检查和分析可允许安全代理 100a-b 收集关于发送和接收消息的实体 300a-c 的信息，其中包括传输模式、数量 (volume)、或实体是否有发送某些类型的消息（例如，合法消息、垃圾邮件、病毒、群发邮件，等等）的倾向。

[0038] 如图 3 所示，每个实体 300a-c 分别与一个或更多个标识符 310a-c 相关联。标识符 310a-c 可例如包括 IP 地址、统一资源定位器 (URL)、电话号码、IM 用户名、消息内容、域，或可描述实体的任何其它标识符。而且，标识符 310a-c 与一个或更多个属性 320a-c 相关联。如应理解的，属性 320a-c 符合所描述的特定标识符 310a-c。例如，消息内容标识符可包括属性，例如恶意软件 (malware)、数量、内容类型、运行状态，等等。类似地，与标识符例如 IP 地址相关联的属性 320a-c 可包括与实体 300a-c 相关联的一个或更多个 IP 地址。

[0039] 此外，应理解，可从通信 330a-c（例如，电子邮件）收集的该数据一般包括发起通信的实体的一些标识符和属性。因此，通信 330a-c 提供用于将关于实体的信息传递到安全代理 100a、100b 的传送。通过检查包括在消息中的标题信息、分析消息的内容，以及通过汇聚安全代理 100a、100b 以前收集的信息（例如，合计从实体接收的通信的数量），安全代理 100a、100b 可检测这些属性。

[0040] 可汇聚并利用来自多个安全代理 100a、100b 的数据。例如，数据可由中央系统汇聚和利用，中央系统接收与所有实体 300a-c 相关联的标识符和属性，安全代理 100a、100b 为实体 300a-c 接收了通信。可选地，彼此传递关于实体 300a-c 的标识符和属性信息的安全代理 100a、100b 可作为分布式系统进行操作。利用数据的过程可使实体 300a-c 的属性彼此关联，从而确定实体 300a-c 之间的关系（例如，事件出现、数量，和 / 或其它确定因素之间的关联）。

[0041] 这些关系可接着用于根据与每个标识符相关的属性的关联为所有标识符建立多维声誉“矢量”。例如，如果具有声誉差的已知声誉的声誉差的实体 300a 发送具有第一组属性 350a 的消息 330a，且接着未知实体 300b 发送具有第二组属性 350b 的消息 330b，则安全代理 100a 可确定第一组属性 350a 的全部或一部分是否匹配第二组属性 350b 的全部或一

部分。当第一组属性 350a 的某个部分匹配第二组属性 350b 的某个部分时，可根据包括匹配的属性 330a、33b 的特定标识符 320a、320b 来建立关系。被发现具有匹配的属性的特定标识符 340a、340b 可用于确定与实体 300a、300b 之间的关系相关联的强度。关系的强度可帮助确定声誉差的实体 300a 的声誉差的性质中有多少被归于未知实体 300b 的声誉。

[0042] 然而，还应认识到，未知实体 300b 可发起包括属性 350c 的通信 330c，属性 350c 与发源于已知的声誉好的实体 300c 的通信 330d 的一些属性 350d 匹配。被发现具有匹配的属性的特定标识符 340c、340d 可用于确定与实体 300b、300c 之间的关系相关联的强度。关系的强度可帮助确定声誉好的实体 300c 的声誉好的性质中有多少被归于未知实体 300b 的声誉。

[0043] 分布式声誉引擎还允许关于最近的威胁前景的全球情报的实时协作共享，对可由过滤或风险分析系统执行的局部分析提供即时保护的益处，以及甚至在可能的新威胁出现之前就识别这种新威胁的恶意来源。使用位于很多不同地理位置处的传感器，可与中央系统 200 或与分布式安全代理 100a、100b 一起快速共享关于新威胁的信息。如应理解的，这样的分布式传感器可包括局部安全代理 100a、100b，以及局部声誉好的客户机、业务量监控器，或适合于收集通信数据的任何其它设备（例如，开关、路由器、服务器，等等）。

[0044] 例如，安全代理 100a、100b 可与中央系统 200 进行通信，以提供威胁和声誉信息的共享。可选地，安全代理 100a、100b 可在彼此之间传递威胁和声誉信息，以提供最新的和准确的威胁信息。在图 3 的例子中，第一安全代理 300a 拥有关于未知实体 300b 和声誉差的实体 300a 之间的关系的信息，而第二安全代理 300b 拥有关于未知实体 300b 和声誉好的实体 300c 之间的关系的信息。在没有共享信息的情况下，第一安全代理 300a 可根据所检测的关系对通信采取特定的动作。然而，知道未知实体 300b 和声誉好的实体 300c 之间的关系，第一安全代理 300a 可利用来自未知实体 300b 的收到的通信来采取不同的动作。安全代理之间的关系信息的共享因而提供更完整的一组关系信息，将针对该关系信息作出确定。

[0045] 系统试图将声誉（反映一般倾向和 / 或分类）分配给物理实体，例如执行事务的个人或自动化系统。在虚拟世界中，实体由在实体正执行的特定事务（例如，发送消息或从银行帐号转移资金）中联系到这些实体的标识符（例如 IP、URL、内容）表示。因此根据那些标识符的总体行为和历史模式以及那些标识符与其它标识符的关系，例如发送消息的 IP 与包括在那些消息中的 URL 的关系，声誉可被分配到那些标识符。如果在标识符之间存在强关联，则单个标识符的“差”声誉可能使其它邻近的标识符的声誉恶化。例如，发送具有差声誉的 URL 的 IP 将由于 URL 的声誉而使其自己的声誉恶化。最后，单独的标识符声誉可被汇聚成与那些标识符相关联的实体的单个声誉（风险评分）。

[0046] 应注意，属性可分成很多类别。例如，证据属性可表示关于实体的物理、数字或数字化的物理数据。该数据可归于单个已知或未知的实体，或在多个实体之间共享（形成实体关系）。与消息安全有关的证据属性的例子包括 IP（互联网协议）地址、已知的域名、URL、实体所使用的数字指纹或签名、TCP 签名，等等。

[0047] 作为另一例子，行为属性可表示关于实体或证据属性的人或机器分配的观测结果。这样的属性可包括来自一个或多个行为参数文件 (behavioral profile) 的一个、很多或所有属性。例如，通常与垃圾邮件发送者相关联的行为属性可依据从该实体发送的大量通信。

[0048] 用于特定类型的行为的很多行为属性可被合并以得出行为参数文件。行为参数文件可包括一组预定义的行为属性。分配给这些参数文件的属性特征包括与限定匹配参数文件的实体的倾向有关的行为事件。与消息安全有关的行为参数文件的例子可包括“垃圾邮件发送者”、“诈骗者”和“合法发送者”。与每个参数文件相关的事件和 / 或证据属性限定参数文件应被分配到的适当实体。这可包括特定的一组发送模式、黑名单事件或证据数据的特定属性。一些例子包括 :发送者 / 接收者身份识别 ;时间间隔和发送模式 ;有效载荷的严重度 (severity) 和配置 ;消息结构 ;消息质量 ;协议和相关的签名 ;通信介质。

[0049] 应理解,共享相同的证据属性中的一些或全部的实体具有证据关系。类似地,共享行为属性的实体具有行为关系。这些关系帮助形成相关参数文件的逻辑组,该关系接着被适应性地应用,以增强参数文件或略微差不多符合所分配的参数文件地来识别实体。

[0050] 图 4 是描述用于检测关系并给实体分配风险的操作方案 400 的流程图。操作方案在步骤 410 通过收集网络数据开始。数据收集可例如由安全代理 100、客户设备、交换机、路由器或任何其它设备完成,所述其它设备可操作来从网络实体 (例如,电子邮件服务器、网络服务器、IM 服务器、ISP、文件传输协议 (FTP) 服务器、gopher 服务器、VoIP 设备等) 接收通信。

[0051] 在步骤 420,标识符与所收集的数据 (例如通信数据) 相关联。步骤 420 可由可操作来从很多传感器设备汇聚数据的安全代理 100 或中央系统 200 执行,包括例如一个或更多个安全代理 100。可选地,步骤 420 可由安全代理 100 本身执行。标识符可基于所接收的通信的类型。例如,电子邮件可包括一组信息 (例如,发起者和收信方的 IP 地址、文本内容、附件等),而 VoIP 通信可包括一组不同的信息 (例如,主叫电话号码 (或如果从 VoIP 客户发起则为 IP 地址)、接收的电话号码 (或如果指定 VoIP 电话则为 IP 地址)、语音内容,等等)。步骤 420 也可包括分配具有相关标识符的通信的属性。

[0052] 在步骤 430,分析与实体相关联的属性,以确定在实体之间是否存在任何关系,为这些实体收集通信信息。步骤 430 可例如由中央系统 200 或一个或更多个分布式安全代理 100 执行。分析可包括比较与不同实体有关的属性以找到实体之间的关系。而且,根据作为关系的基础的特定属性,强度可与关系相关联。

[0053] 在步骤 440,风险矢量被分配给实体。作为例子,风险矢量可由中央系统 200 或一个或更多个安全代理 100 分配。分配给实体 130(图 1-2)、300(图 3) 的风险矢量可基于在实体之间存在的关系,并基于形成关系的基础的标识符。

[0054] 在步骤 450,可根据风险矢量执行动作。该动作可例如由安全代理 100 执行。可对与实体相关联的收到的通信执行动作,风险矢量被分配给该实体。其中,所述动作可包括允许、拒绝、隔离、负载均衡、以所分配的优先级传输、以额外的细查局部地进行分析。然而,应理解,可单独地得到声誉矢量。

[0055] 图 5 是示出示例性网络体系结构的结构图,其包括由局部声誉引擎 510a-e 得到的局部声誉 500a-e 和一个或更多个服务器 530 所储存的全局声誉 520。局部声誉引擎 510a-e 例如可与局部安全代理,例如安全代理 100 相关联。可选地,局部声誉引擎 510a-e 可例如与本地客户机相关联。声誉引擎 510a-e 中的每个包括一个或更多个实体的列表,声誉引擎 510a-e 为这些实体储存所得到的声誉 500a-e。

[0056] 然而,这些储存的得到的声誉在声誉引擎之间可能是不一致的,因为每个声誉引

擎可观察到不同类型的业务量。例如，声誉引擎 1510a 可包括指示特定实体是声誉好的声誉，而声誉引擎 2510b 可包括指示同一实体是声誉差的声誉。这些局部的声誉不一致性可基于从实体接收的不同业务量。可选地，不一致性可基于来自局部声誉引擎 1510a 的用户的、指示通信是合法的反馈，而局部声誉引擎 2510b 提供指示同一通信是不合法的反馈。

[0057] 服务器 530 从局部声誉引擎 510a-e 接收声誉信息。然而，如上所述，一些局部声誉信息可能与其它局部声誉信息不一致。服务器 530 可在局部声誉 500a-e 之间进行仲裁，以根据局部声誉信息 500a-e 确定全局声誉 520。在一些例子中，全局声誉信息 520 可接着被提供回局部声誉引擎 510a-e，以给这些引擎 510a-e 提供最新的声誉信息。可选地，局部声誉引擎 510a-e 可操作来查询服务器 530 以得到声誉信息。在一些例子中，服务器 530 使用全局声誉信息 520 响应于查询。

[0058] 在其它例子中，服务器 530 将局部声誉偏置 (bias) 应用到全局声誉 520。局部声誉偏置可对全局声誉执行变换，以给局部声誉引擎 510a-e 提供全局声誉矢量，其根据发起查询的特定局部声誉引擎 510a-e 的偏好而进行偏置。因此，管理员或用户对垃圾邮件消息指示高容忍度 (tolerance) 的局部声誉引擎 510a 可接收解释所指示的容忍度的全局声誉矢量。返回到声誉引擎 510a 的声誉矢量的特定分量可能包括由于与声誉矢量的其余部分的关系而降低重要性的声誉矢量的部分。同样，局部声誉引擎 510b 可接收放大与病毒声誉有关的声誉矢量的分量的声誉矢量，局部声誉引擎 510b 指示例如来自具有发起病毒的声誉的实体的低容忍度通信。

[0059] 图 6 是示出基于局部声誉反馈的全局声誉的确定的结构图。局部声誉引擎 600 可操作来通过网络 610 向服务器 620 发送查询。在一些例子中，局部声誉引擎 600 响应于从未知实体接收通信而发起查询。可选地，局部声誉引擎 600 可响应于接收任何通信而发起查询，从而促进更加新的声誉信息的使用。

[0060] 服务器 620 可操作来使用全局声誉确定响应于查询。中央服务器 620 可使用全局声誉汇聚引擎 630 得到全局声誉。全局声誉汇聚引擎 630 可操作来从相应的多个局部声誉引擎接收多个局部声誉 640。在一些例子中，多个局部声誉 640 可由声誉引擎周期性地发送到服务器 620。可选地，多个局部声誉 640 可由服务器在从局部声誉引擎 600 中之一接收到查询时取回。

[0061] 使用与每个局部声誉引擎有关的置信值 (confidence value) 并接着积累结果，可合并局部声誉。置信值可指示与相关声誉引擎所产生的局部声誉相关联的置信度。与个人相关联的声誉引擎例如可接收在全局声誉确定中较低的权重。相反，与在大型网络上操作的声誉引擎相关联的局部声誉可根据与该声誉引擎相关联的置信值接收全局声誉确定中较大的权重。

[0062] 在一些例子中，置信值 650 可基于从用户接收的反馈。例如，可给接收很多反馈的声誉引擎分配与该声誉引擎相关的局部声誉 640 的低置信值 650，这些反馈指示通信未被正确地处理，因为与通信相关的局部声誉信息 640 指示错误的动作。类似地，可给接收反馈的声誉引擎分配与该声誉引擎相关的局部声誉 640 的高置信值 650，该反馈根据局部声誉信息 640 指示通信被正确地处理，局部声誉信息 640 与指示正确的动作的通信相关联。与不同声誉引擎相关联的置信值的调整可使用调节器 660 来完成，调节器 660 可操作来接收输入信息并根据所接收的输入调节置信值。在一些例子中，根据被储存的用于被错误地分

类的实体的统计资料，置信值 650 可由声誉引擎本身提供到服务器 620。在其它例子中，用于对局部声誉信息加权的信息可被传递到服务器 620。

[0063] 在一些例子中，偏置 670 可应用于最终形成的全局声誉矢量。偏置 670 可标准化声誉矢量，以向声誉引擎 600 提供标准化的全局声誉矢量。可选地，可应用偏置 670 以解释与发起声誉查询的声誉引擎 600 相关的局部偏好。因此，声誉引擎 600 可接收与查询的声誉引擎 600 的确定的偏好匹配的全局声誉矢量。声誉引擎 600 可根据从服务器 620 接收的全局声誉矢量对通信采取动作。

[0064] 图 7 是示出全局声誉和局部声誉之间的示例性转化的结构图。局部安全代理 700 与服务器 720 进行通信，以从服务器 720 取回全局声誉信息。局部安全代理 700 可在 702 接收通信。局部安全代理可在 704 关联通信以识别消息的属性。消息的属性可包括例如发端实体、消息内容的指纹、消息大小，等等。局部安全代理 700 在对服务器 720 的查询中包括该信息。在其它例子中，局部安全代理 700 可将整个消息转发到服务器 720，且服务器可执行消息的关联和分析。

[0065] 服务器 720 使用从查询接收的信息，来根据服务器 720 的配置 725 确定全局声誉。配置 725 可包括多个声誉信息，包括指示被查询的实体是声誉差的信息 (730) 和指示被查询的实体是声誉好的信息 (735)。配置 725 也可将权重 740 应用于每个汇聚的声誉 730、735。声誉得分确定器 745 可提供用于给汇聚的声誉信息 730、735 加权 (740) 并产生全局声誉矢量的引擎。

[0066] 局部安全代理 700 接着在 706 向局部声誉引擎发送查询。局部声誉引擎 708 执行局部声誉的确定并在 710 返回局部声誉矢量。局部安全代理 700 也接收以全局声誉矢量形式的、对发送到服务器 720 的声誉查询的响应。局部安全代理 700 接着在 712 将局部声誉矢量和全局声誉矢量混合在一起。接着在 714 关于所接收的消息采取动作。

[0067] 图 8 是用于调整与声誉服务器相关联的过滤器的设置的示例性图形用户界面 800。图形用户界面 800 可允许局部安全代理的用户在一些不同的类别 810，例如“病毒”、“蠕虫”、“特洛伊木马”、“网络钓鱼”、“间谍软件”、“垃圾邮件”、“内容”和“群发”中调整局部过滤器的配置。然而，应理解，所述类别 810 只是例子，且本公开不限于在这里被选为例子的类别 810。

[0068] 在一些例子中，类别 810 可分成两种或更多类型的类别。例如，图 8 的类别 810 分成类别 810 的“安全设置”类型 820 以及类别的“策略设置”类型 830。在每个类别 810 和类型 820、830 中，混合器条形表示 840 可允许用户调整与通信或实体声誉的相应类别 810 相关联的特定过滤器设置。

[0069] 而且，虽然“策略设置”类型 830 的类别 810 可根据用户自己的判断被自由调节，但是“安全设置”类型 820 的类别可被限制到在一范围内调整。可产生该差别，以便阻止用户更改安全代理的安全设置超过可接受的范围。例如，不满意的雇员可能试图降低安全设置，从而允许企业网易受攻击。因此，在“安全设置”类型 820 中置于类别 810 上的范围 850 可操作来在将安全保持在最低水平，以防止网络被危害。然而，如应注意的，“策略设置”类型 830 的类别 810 是不危害网络安全的那些类型的类别 810，而是如果设置降低可能只是使用户或企业不方便。

[0070] 此外，应认识到，在各种例子中，范围限制 850 可置于全部类别 810 上。因此，局部

安全代理将阻止用户将混合器条形表示 840 设置在所提供的范围 850 之外。还应注意，在一些例子中，范围可不显示在图形用户界面 800 上。替代地，范围 850 将被从图形用户界面 800 提取出来，且所有设置将为相关的设置。因此，类别 800 可显示并看起来似乎允许设置的满范围，同时将设置变换成在所提供的范围内的设置。例如，“病毒”类别 810 的范围 850 在本例中被设置在水平标记 8 和 13 之间。如果图形用户界面 800 设置成从图形用户界面 800 提取出可允许的范围 850，则“病毒”类别 810 将允许混合器条形表示 840 设置在 0 和 14 之间的任何位置。然而，图形用户界面 800 可将 0-14 设置变换成在 8 到 13 的范围 850 内的设置。因此，如果用户请求在 0 和 14 之间中间的设置，则图形用户界面可将该设置变换成在 8 和 13 中间的设置。

[0071] 图 9 是示出用于互联网协议语音电话 (VoIP) 或短消息服务 (SMS) 通信的基于声誉的连接抑制的结构图。如应理解的，主叫 IP 电话 900 可向接收的 IP 电话 910 安排 VoIP 呼叫。这些 IP 电话 900、910 可以是例如计算机执行的软电话软件、网络支持的电话，等等。主叫 IP 电话 900 可通过网络 920（例如互联网）安排 VoIP 呼叫。接收的 IP 电话 910 可通过局域网 930（例如企业网）接收 VoIP 呼叫。

[0072] 当建立 VoIP 呼叫时，主叫 IP 电话已建立与局域网 930 的连接。该连接可与电子邮件、网络、即时消息或其它互联网应用可被用于提供与网络的未调节 (unregulated) 的连接的方式类似被使用。因此，可使用与接收的 IP 电话的连接，从而根据所建立的连接使在局域网 930 上操作的计算机 940、950 处于入侵、病毒、特洛伊木马、蠕虫和各种其它类型的攻击的危险中。而且，由于 VoIP 通信的时间敏感性质，一般不检查这些通信，以确保没有误用连接。例如，语音会话实时地发生。如果语音会话的一些分组被延迟，则会话变得不自然且难以理解。因此，一旦建立了连接，就一般不能检查分组的内容。

[0073] 然而，局部安全代理 960 可使用从声誉引擎或服务器 970 接收的声誉信息来确定与主叫 IP 电话相关的声誉。局部安全代理 960 可使用发端实体的声誉来确定是否允许与发端实体的连接。因此，安全代理 960 可防止与声誉差的实体的连接，如不遵守局部安全代理 960 的策略的声誉所指示的。

[0074] 在一些例子中，局部安全代理 960 可包括连接抑制引擎，其可操作来使用在主叫 IP 电话 900 和接收的 IP 电话 910 之间建立的连接来控制正被传输的分组的流动速率。因此，可允许具有差声誉的发端实体 900 产生与接收的 IP 电话 910 的连接。然而，分组通过量将被定上限，从而防止发端实体 900 使用连接来攻击局域网 930。可选地，连接抑制可通过执行从声誉差的实体发起的任何分组的详细检查来完成。如上所述，所有 VoIP 分组的详细检查不是有效的。因此，可为与声誉好的实体相关联的连接最大化服务质量 (QoS)，同时减少与声誉差的实体的连接相关联的 QoS。可对与声誉差的实体相关联的连接执行标准通信询问技术，以便发行从发端实体接收的任何被传输的分组是否包括对网络 930 的威胁。在美国专利号 6,941,467、7,089,590、7,096,498 和 7,124,438 中以及在美国专利申请号 2006/0015942、2006/0015563、2003/0172302、2003/0172294、2003/0172291 和 2003/0173166 中描述了各种询问技术和系统，由此以上这些通过引用被并入。

[0075] 图 10 是示出基于声誉的负载均衡器 1000 的操作的结构图。负载均衡器 1000 可操作来通过网络 1030（例如互联网）（分别地）从声誉好的实体 1010 和声誉差的实体 1020 接收通信。负载均衡器 1000 与声誉引擎 1040 进行通信，以确定与进入或传出的通信相关

联的实体 1010、1020 的声誉。

[0076] 声誉引擎 1030 可操作来给负载均衡器提供声誉矢量。声誉矢量可以各种不同的类别指示与通信相关联的实体 1010、1020 的声誉。例如，就发起垃圾邮件的实体 1010、1020 而言，声誉矢量可指示实体 1010、1020 的良好声誉，同时就发起病毒的实体 1010、1020 而言，也指示相同实体 1010、1020 的差声誉。

[0077] 负载均衡器 1000 可使用声誉矢量来确定关于与实体 1010、1020 相关联的通信执行什么动作。在声誉好的实体 1010 与通信相关联的情况下，消息被发送到消息传输代理 (MTA)1050 并被传输给接收者 1060。

[0078] 在声誉差的实体 1020 拥有病毒的声誉但没有其它类型的声誉差的活动的声誉的情况下，通信被转发到多个病毒检测器 1070 中之一。负载均衡器 1000 可操作来根据病毒检测器的当前容量和发端实体的声誉来确定使用多个病毒检测器 1070 中的哪一个。例如，负载均衡器 1000 可将通信发送到被最少利用的病毒检测器。在其它例子中，负载均衡器 1000 可确定与发端实体相关联的差声誉度，并将声誉稍微差的通信发送到被最少利用的病毒检测器，同时将声誉非常差的通信发送到被高度利用的病毒检测器，从而抑制与声誉非常差的实体相关联的连接的 QoS。

[0079] 类似地，在声誉差的实体 1020 有发起垃圾邮件通信的声誉但没有其它类型的声誉差的活动的声誉的情况下，负载均衡器可将通信发送到专门的垃圾邮件检测器 1080 以排除其它类型的测试。应理解，在通信与发起多种类型的声誉差的活动的声誉差的实体 1020 相关联的情况下，可发送通信以测试已知实体 1020 要显示的每种类型的声誉差的活动，同时避免与不知道实体 1020 要显示的声誉差的活动相关联的测试。

[0080] 在一些例子中，每个通信可接收用于多种类型的不合法内容的例行测试。然而，当与通信相关联的实体 1020 显示某些类型的活动的声誉时，通信也可被隔离以用于内容的详细测试隔离，实体显示对于发起该内容的声誉。

[0081] 在又一些例子中，每个通信可接收相同类型的测试。然而，与声誉好的实体 1010 相关联的通信被发送到有最短队列的测试模块或具有空闲的处理容量的测试模块。另一方面，与声誉差的实体 1020 相关联的通信被发送到有最长队列的测试模块 1070、1080。因此，与声誉好的实体 1010 相关联的通信可接受超过与声誉差的实体相关联的通信的传输优先权。因此对于声誉好的实体 1010，服务质量被最大化，同时对于声誉差的实体 1020，服务质量被降低。因此，基于声誉的负载平衡可通过降低声誉差的实体连接到网络 930 的能力来保护网络免于攻击。

[0082] 图 11A 是示出用于收集基于地理位置的数据以进行身份验证分析的示例性操作方案的流程图。在步骤 1100，操作方案从各种登录尝试收集数据。步骤 1100 可例如由局部安全代理，例如图 1 的安全代理 100 执行。其中，所收集的数据可包括与登录尝试相关联的 IP 地址、登录尝试的时间、在成功之前的登陆尝试的次数，或所尝试的任何不成功的口令的详细资料。所收集的数据接着在步骤 1105 被分析，以得出统计信息，例如登录尝试的地理位置。步骤 1105 可例如由声誉引擎执行。接着在步骤 1110 与登录尝试相关联的统计信息被储存。该储存可例如由系统数据存储器执行。

[0083] 图 11B 是示出用于基于地理位置的身份验证的另一示例性操作方案的流程图。在步骤 1115 接收登录尝试。登录尝试可例如由可操作来通过网络提供安全财务数据的安全

网络服务器接收。接着在步骤1120确定登录尝试是否匹配所储存的用户名和口令组合。步骤1120可例如由可操作来验证登录尝试的安全服务器执行。如果用户名和口令不匹配所存储的用户名/口令组合，则在步骤1125宣布登录尝试失败。

[0084] 然而，如果用户名和口令确实匹配合法用户名/口令组合，则在步骤1130确定登录尝试的起源。登录尝试的起源可由如图1所示的局部安全代理100确定。可选地，登录尝试的起源可由声誉引擎确定。登录尝试的起源可接着与在图11A中得出的统计信息比较，如在步骤1135中示出的。步骤1135可例如由局部安全代理100或声誉引擎执行。在步骤1140确定起源是否与统计期望匹配。如果实际起源匹配统计期望，则在步骤1145验证用户。

[0085] 可选地，如果实际起源不匹配对于起源的统计期望，则在步骤1150执行进一步的处理。应理解，进一步的处理可包括从用户请求进一步的信息，以验证他或她的真实性。这样的信息可包括例如家庭地址、母亲的婚前姓、出生地点，或关于用户已知的任何其它部分的信息（例如秘密问题）。额外处理的其它例子可包括搜索以前的登录尝试，以确定当前登录尝试的地点是否确实是异常的或仅仅是巧合的。此外，与发起登录尝试的实体相关联的声誉可被得出并用于确定是否允许登录。

[0086] 图11C是示出用于使用发端实体的声誉进行基于地理位置的验证以确认身份验证的另一示例性操作方案的流程图。在步骤1115接收登录尝试。登录尝试可例如由可操作来通过网络提供安全财务数据的安全网络服务器接收。接着在步骤1160确定登录尝试是否匹配所储存的用户名和口令组合。步骤1160可例如由可操作来验证登录尝试的安全服务器执行。如果用户名和口令不匹配所存储的用户名/口令组合，则在步骤1165宣布登录尝试失败。

[0087] 然而，如果用户名和口令确实匹配合法的用户名/口令组合，则在步骤1170确定登录尝试的起源。登录尝试的起源可由如图1所示的局部安全代理100确定。可选地，登录尝试的起源可由声誉引擎确定。接着可取回与发起登录尝试的实体相关联的声誉，如在步骤1175中示出的。步骤1175可例如由声誉引擎执行。在步骤1180确定发端实体的声誉是否是声誉好的。如果发端实体是声誉好的，则在步骤1185验证用户身份。

[0088] 可选地，如果发端实体是声誉差的，则在步骤1190执行进一步的处理。应理解，进一步的处理可包括从用户请求进一步的信息，以验证他或她的真实性。这样的信息可包括例如家庭地址、母亲的婚前姓、出生地点，或关于用户已知的任何其它部分的信息（例如秘密问题）。额外处理的其它例子可包括搜索以前的登录尝试，以确定当前登录尝试的地点是否确实是异常的或仅仅是巧合的。

[0089] 因此，应理解，可应用声誉系统来识别金融交易中的欺诈行为。声誉系统可根据交易发起者的声誉或实际交易中的数据（来源、目的地、金额，等等）来提高交易的风险评分。在这样的情况下，金融机构可根据发端实体的声誉更好地确定特定交易是欺骗性的概率。

[0090] 图12是示出用于基于声誉的动态隔离的示例性操作方案的流程图。在步骤1200接收通信。接着在步骤1205分析通信，以确定它们是否与未知实体相关联。然而应注意，该操作方案可应用于所接收的任何通信，而不仅仅是从以前的未知实体接收的通信。例如，从声誉差的实体接收的通信可被动态地隔离，直到确定了所接收的通信不对网络造成威胁为止。在通信不与新实体相关联的场合，通信经历对进入的通信的正常处理，如在步骤1210

中示出的。

[0091] 如果通信与新实体相关联，则在步骤 1215 初始化动态隔离计数器。接着在步骤 1220，从新实体接收的通信被发送到动态隔离。接着在步骤 1225 检查计数器以确定计数器的时间是否已经过去了。如果计数器的时间没有过去，则在步骤 1230 递减计数器。在步骤 1235 可分析实体的行为以及被隔离的通信。在步骤 1240 确定实体的行为或被隔离的通信是否是异常的。如果没有发现异常情况，则操作方案返回到步骤 1220，在这里隔离新的通信。

[0092] 然而，如果在步骤 1240 发现实体的行为或通信是异常的，则在步骤 1245 给实体分配声誉差的声誉。通过将通知发送到管理员或发端实体所发送的通信的接收者来结束过程。

[0093] 返回到步骤 1220，隔离和检查通信和实体行为的过程继续进行，直到发现异常行为为止，或直到在步骤 1225 动态的隔离计数器的时间过去为止。如果动态的隔离计数器的时间过去了，则在步骤 1255 给实体分配声誉。可选地，在实体不是未知实体的情况下，在步骤 1245 或 1255 可更新声誉。在步骤 1260 通过释放动态隔离来结束该操作方案，其中动态的隔离计数器的时间已经过去，而在通信中或在发端实体的行为中没有发现异常情况。

[0094] 图 13 是可被分类为不想要的图像或消息的图像垃圾邮件通信的示例性图形用户界面 1300 的显示。如应理解的，图像垃圾邮件对传统垃圾邮件过滤器造成问题。图像垃圾邮件通过将垃圾邮件的文本消息转换成图像格式来绕过垃圾邮件的传统文本分析。图 13 示出图像垃圾邮件的例子。消息显示图像 1310。虽然图像 1300 看起来是文本，但它仅仅是文本消息的图形编码。一般地，图像垃圾邮件也包括文本消息 1320，文本消息 1320 包括被正确地构造的但在消息背景下没有意义的句子。消息 1320 设计成躲避接通通信的垃圾邮件过滤器，在该通信内只包括图像 1310。而且，消息 1320 设计成欺骗滤波器，这些滤波器对包括图像 1310 的通信的文本应用粗略的测试。进一步地，当这些消息确实在头部 1330 中包括关于消息的起源的信息时，用于发出图像垃圾邮件的实体的声誉可能是未知的，直到该实体被发觉发送图像垃圾邮件为止。

[0095] 图 14 是示出用于检测不想要的图像（例如，图像垃圾邮件）的示例性操作方案的流程图。应理解，附图 14 中所示的很多步骤可单独地或结合附图 14 中所示的其它步骤中的任何一个或全部来执行，以提供图像垃圾邮件的某种检测。然而，附图 14 中的每个步骤的使用提供了用于检测图像垃圾邮件的全面的过程。

[0096] 过程在步骤 1400 以通信的分析开始。步骤 1400 一般包括分析通信，以确定通信是否包括受到图像垃圾邮件处理的图像。在步骤 1410，操作方案执行通信的结构分析，以确定图像是否包括垃圾邮件。接着在步骤 1420 分析图像的头部。图像头部的分析允许系统确定关于图像格式本身是否存在异常情况（例如，协议错误、讹误，等等）。在步骤 1430 分析图像的特征。特征分析旨在确定图像的任何特征是否是异常的。

[0097] 可在步骤 1440 标准化图像。图像的标准化一般包括移除可能被垃圾邮件发送者添加以避免图像指纹识别技术的随机噪声。图像标准化旨在将图像转换成在图像中可容易比较的格式。可对被标准化的图像执行指纹分析，以确定图像是否匹配来自以前接收的已知图像垃圾邮件的图像。

[0098] 图 15A 是示出用于分析通信的结构的操作方案的流程图。操作方案在步骤 1500

以消息结构的分析开始。在步骤 1505，分析通信的超文本标记语言 (HTML) 结构，以引入 n- 元文法 (n-gram) 标记作为贝叶斯分析的额外符号 (token)。这样的处理可为异常情况分析包括在图像垃圾邮件通信中的文本 1320。可分析消息的 HTML 结构，以定义元令牌 (meta-token)。元令牌是消息的 HTML 内容，其被处理以丢弃任何不相关的 HTML 标记，并通过移除白空区而被压缩以生成用于贝叶斯分析的“符号”。上述符号中的每个可用作对贝叶斯分析的输入，以与以前接收的通信比较。

[0099] 操作方案接着在步骤 1515 包括图像检测。图像检测可包括将图像分割成多个部分，以及对这些部分执行指纹识别来确定指纹是否匹配以前接收的图像的部分。

[0100] 图 15B 是示出用于下述过程的操作方案的流程图，即分析图像的特征，以提取用于输入到聚类引擎 (clustering engine) 中的消息的特征，以便识别符合已知图像垃圾邮件的图像的组成部分。操作方案在步骤 1520 开始，在这里图像的多个高水平特征被检测，以用在机器学习算法中。这样的特征可包括数值，例如独特的颜色的数量、噪声黑色像素 (noise black pixel) 的数量、水平方向中边缘（形状之间的锐转变）的数量，等等。

[0101] 操作方案所提取的特征之一可包括图像的柱状图模式的数量，如在步骤 1525 示出的。通过检查图像的光谱密度来产生模式的数量。如应理解的，人工图像一般包括比自然图像少的模式，这是因为自然图像颜色一般扩散到广谱 (broad spectrum)。

[0102] 如上所述，从图像提取的特征可用于识别异常情况。在一些例子中，异常情况可包括分析消息的特征以确定多个特征与所储存的不想要的图像的特征的相似性的程度。可选地，在一些例子中，也可分析图像特征，以与已知的声誉好的图像比较，以确定与声誉好的图像的相似性。应理解，单独的所提取的特征都不能决定分类。例如，特定的特征可与 60％的不想要的消息相关联，同时也与 40％的想要的消息相关联。而且，当与特征相关联的数值变化时，消息是想要的或是不想要的概率可能变化。有很多可指示轻微倾向的特征。如果合并这些特征中的每个，则图像垃圾邮件检测系统可进行分类决定。

[0103] 接着在步骤 1530 检查高宽比，以确定关于图像尺寸或高宽比的是否存在任何异常情况。图像尺寸或高宽比与已知图像垃圾邮件所共有的已知尺寸或高宽比的相似性可指示这种在高宽比中的异常情况。例如，图像垃圾邮件能够以特定的尺寸出现，以使图像垃圾邮件看起来更像普通电子邮件。包括下述图像的消息更可能是垃圾邮件本身，即这些图像与已知垃圾邮件图像享有共同的尺寸。可选地，存在不有利于垃圾邮件的图像尺寸（例如，如果垃圾邮件发送者将消息插入图像中，则 1 英寸 x1 英寸的正方形图像可能是难以读取的）。已知不利于垃圾邮件的插入的包括图像的消息较不可能是图像垃圾邮件。因此，消息的高宽比可与在图像垃圾邮件中使用的共同的高宽比进行比较，以确定图像是不想要的图像或图像是声誉好的图像的概率。

[0104] 在步骤 1535，检查图像的频率分布。一般地，自然图像有具有相对少的明显的频率梯度 (gradation) 的均匀频率分布。另一方面，图像垃圾邮件一般包括常变的频率分布，这是因为黑色字母被放置在黑暗背景上。因此，这样的不均匀的频率分布可指示图像垃圾邮件。

[0105] 在步骤 1540，可分析信噪比。高信噪比可指示垃圾邮件发送者可能试图通过将噪声引入图像中来躲避指纹识别技术。由此增加噪声水平可指示图像是不想要的图像的概率增加。

[0106] 应理解，可在整个图像的规模上提取一些特征，而可从图像的子部分提取其它特征。例如，图像可被细分成多个子部分。每个矩形可使用快速付立叶变换 (FFT) 变换到频域中。在被变换的图像中，在多个方向上的频率的优势 (predominance) 可作为特征被提取。也可检查所变换的图像的这些子部分，以确定高频和低频的数量。在被变换的图像中，离原点较远的点表现出较高的频率。类似于其它被提取的特征，这些特征可接着与已知的合法和不想要的图像比较，以确定未知图像与每个类型的已知图像共享哪些特性。而且，被变换的（例如频域）图像也可分成子部分（例如，片段 (slice)、矩形、同心圆，等等），并与来自已知图像（例如，已知的不想要的图像和已知的合法的图像）的数据比较。

[0107] 图 15C 是示出用于标准化图像以用于垃圾邮件处理的的操作方案的流程图。在步骤 1545，从图像除去模糊和噪声。如前所述，这些可能由垃圾邮件发送者引入来躲避指纹识别技术，例如通过改变无用信息的总数的散列法，使得它不与任何以前接收的已知图像垃圾邮件的无用信息的指纹匹配。模糊和噪声的移除可描述用于除去垃圾邮件发送者所引入的人为噪声的几种技术。应理解，人为噪声可包括垃圾邮件发送者所使用的技术，例如条带效应（其中包括在图像中的字体变化，以改变图像的无用信息）。

[0108] 在步骤 1550，边缘检测算法可在标准化的图像上执行。在一些例子中，被进行边缘检测的图像被使用并提供到光学字符识别引擎，以将被进行边缘检测的图像转换成文本。边缘检测可用于从图片除去不必要的细节，该细节可能在相对于其他图像处理该图像中造成低效率。

[0109] 在步骤 1555，可应用中值滤波。应用中值滤波来除去随机的像素噪声。这样的随机像素可对图像的内容分析造成问题。中值滤波可帮助除去垃圾邮件发送者所引入的单像素类型的噪声。应理解，单像素噪声由垃圾邮件发送者使用图像编辑器引入，以改变图像中的一个或多个像素，这可使图像在一些区域中看起来呈颗粒状的，从而使图像更难以检测。

[0110] 在步骤 1560，量化图像。图像的量化除去不必要的颜色信息。这种颜色信息一般需要更多的处理，并与垃圾邮件的试图传播无关。而且，垃圾邮件发送者可稍微改变图像中的颜色方案，并再次改变杂乱信息，以便已知图像垃圾邮件的杂乱信息不匹配从颜色变化的图像垃圾邮件得出的杂乱信息。

[0111] 在步骤 1565，执行对比度扩展。使用对比度扩展，图像中的颜色标度从黑到白被最大化，即使颜色只在灰度阴影中变化也是如此。给图像的最亮的阴影分配白值，而给图像中最暗的阴影分配黑值。与原始图像中最亮和最暗的阴影相比，给所有其它阴影分配他们在光谱 (spectrum) 中的相对位置。对比度扩展帮助限定图像中可能没有充分利用可用光谱的细节，因而可帮助阻止垃圾邮件发送者使用不同部分的光谱来避免指纹识别技术。垃圾邮件发送者有时故意改变图像的密度范围，以使一些类型的特征识别引擎无效。对比度扩展也可帮助标准化图像，以便它可与其它图像比较，以识别包含在图像中的共同特征。

[0112] 图 15D 是示出用于分析图像的指纹以在多个图像中找到共同片段的操作方案的流程图。在步骤 1570，操作方案通过界定图像内的区域开始。接着对所界定的区域执行风选算法 (winnowing algorithm)，以识别图像的相关部分，在步骤 1575 应在该图像上提取指纹。在步骤 1580，操作方案对从风选操作得到的片段进行指纹识别，并确定在所接收的图像和已知垃圾邮件图像的指纹之间是否存在匹配。在每个专利申请公布号 2006/0251068 中描述了类似的风选指纹识别方法，该专利由此通过引用被并入。

[0113] 如这里在说明书中使用的且在接下来的全部权利要求中，“一 (a)”、“一个 (an)”和“所述 (the)”的意思包括复数涵义，除非上下文另外清楚地指出。此外，如这里在说明书中使用的且在接下来的全部权利要求中，“在 ... 中”的意思包括、“在 ... 中”和“在 ... 上”，除非上下文另外清楚地指出。最后，如这里在说明书中使用的且在接下来的全部权利要求中，“和”和“或”的意思包括联合的和分离的涵义，并可互换地使用，除非上下文另外清楚地指出。

[0114] 范围可在这里表示为从“大约”一个特定的值和 / 或到“大约”另一特定的值。当表示这样的范围时，另一实施方式包括从一个特定的值和 / 或到另一特定的值。类似地，当值被表示为近似值时，通过使用前面的“大约”，应理解，特定的值形成另一实施方式。应进一步理解，每个范围的端点相对于另一端点来说是重要的，并独立于另一端点。

[0115] 描述了本发明的很多实施方式。然而，应理解，可进行各种更改，而不偏离本发明的实质和范围。因此，其它实施方式处于下面的权利要求的范围内。

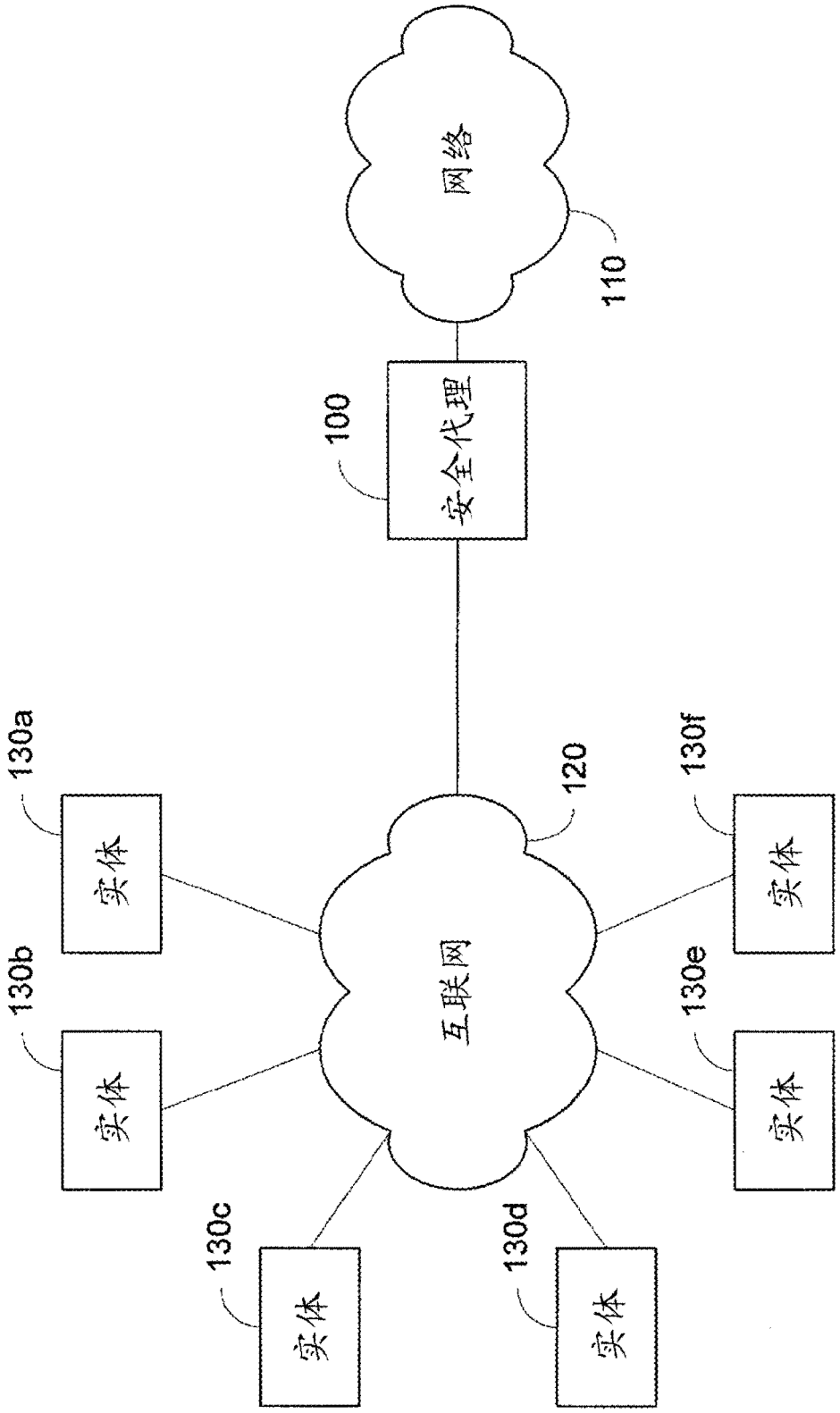

网络
110
100
安全代理
120
互联网
130a
实体
130b
实体
130c
实体
130d
实体
130e
实体
130f
实体

图 1

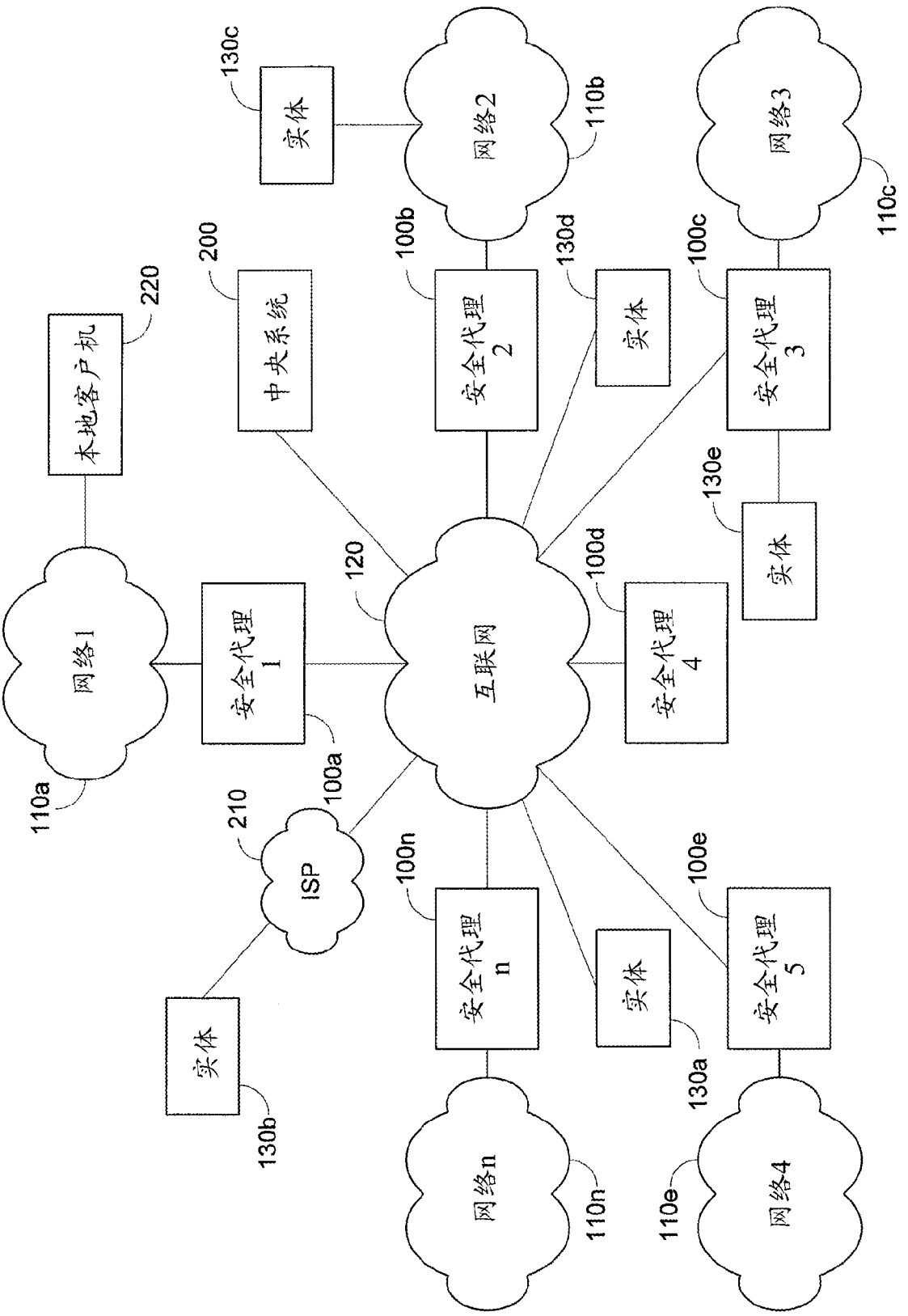

网络1
110a
本地客户机
220
安全代理 1
100a
互联网
120
中央系统
200
ISP
210
实体
130b
网络n
110n
安全代理 n
100n
网络2
110b
实体
130c
安全代理 2
100b
实体
130d
安全代理 4
100d
网络3
110c
安全代理 3
100c
实体
130e
网络4
110e
安全代理 5
100e
实体
130a

图 2

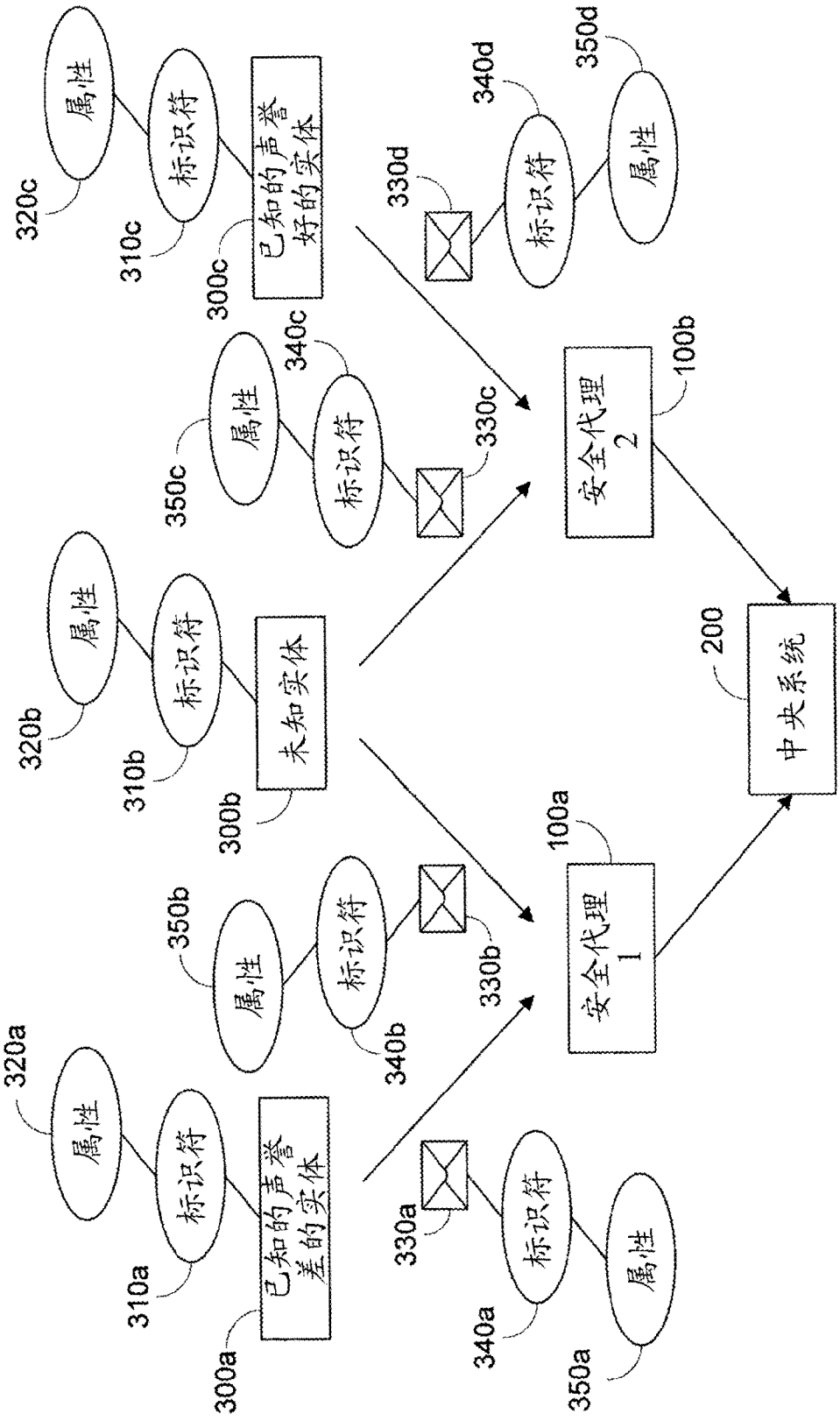

320c
属性
310c
标识符
300c
已知的声誉好的实体
350c
属性
340c
标识符
330c
330d
340d
标识符
350d
属性
320b
属性
310b
标识符
300b
未知实体
320a
属性
310a
标识符
300a
已知的声誉差的实体
350b
属性
340b
标识符
330b
330a
340a
标识符
350a
属性
100a
安全代理 1
100b
安全代理 2
200
中央系统

图 3

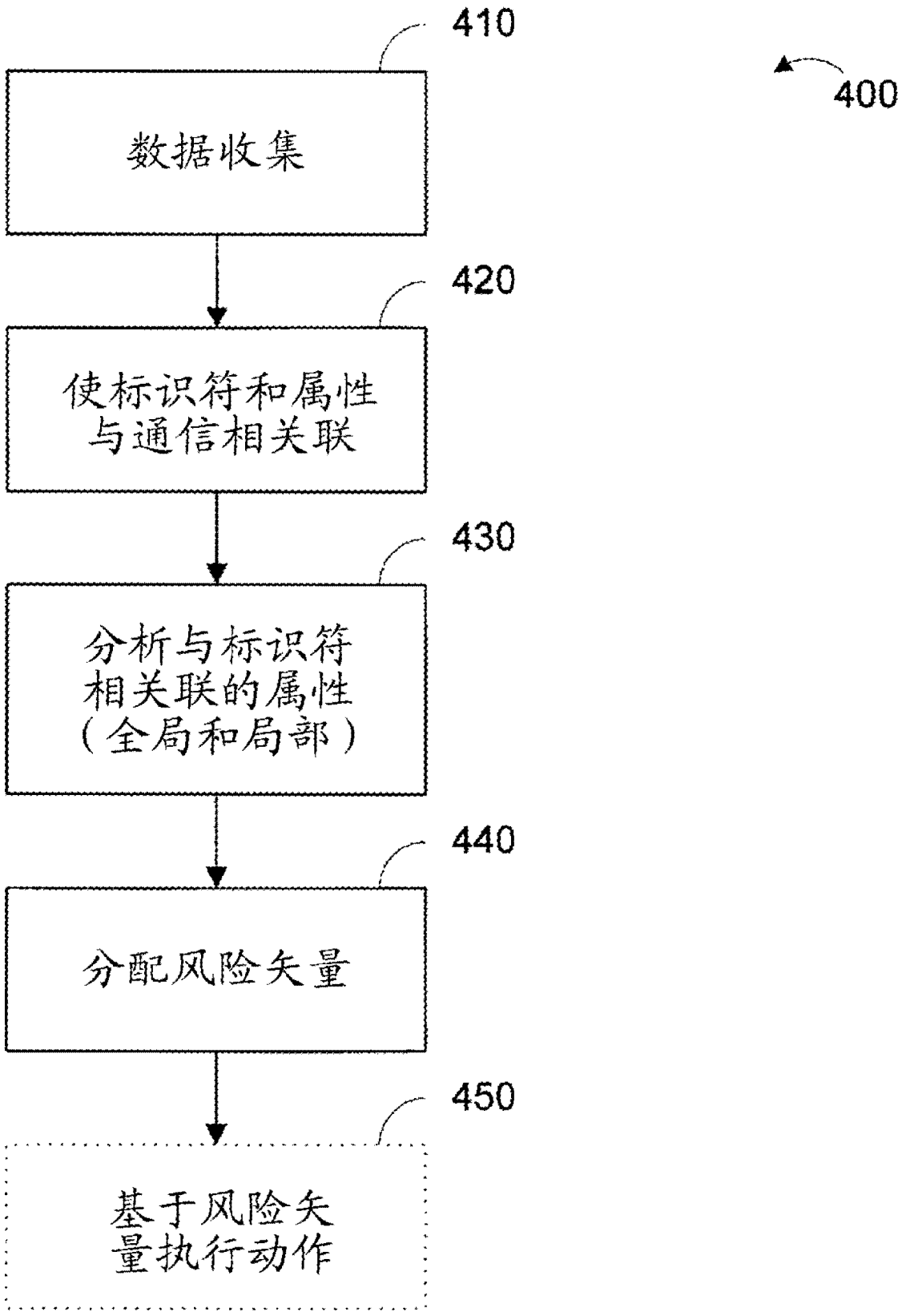

410
400
数据收集
420
使标识符和属性
与通信相关联
430
分析与标识符
相关联的属性
(全局和局部)
440
分配风险矢量
450
基于风险矢
量执行动作

图 4

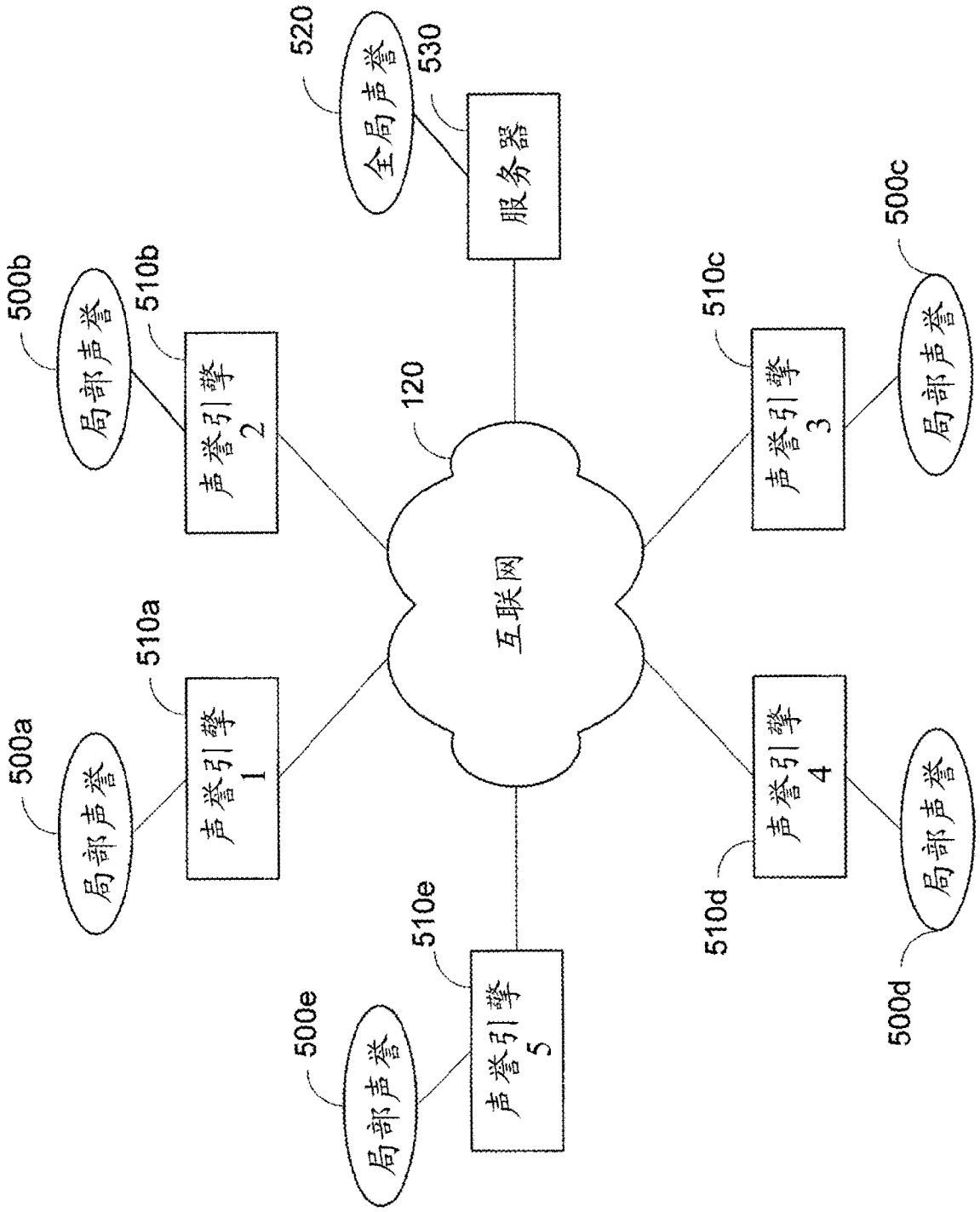

520
全局声誉
530
服务器
500b
局部声誉
510b
声誉引擎
2
120
互联网
510c
声誉引擎
3
500c
局部声誉
500a
局部声誉
510a
声誉引擎
1
510d
声誉引擎
4
500d
局部声誉
510e
声誉引擎
5
500e
局部声誉

图 5

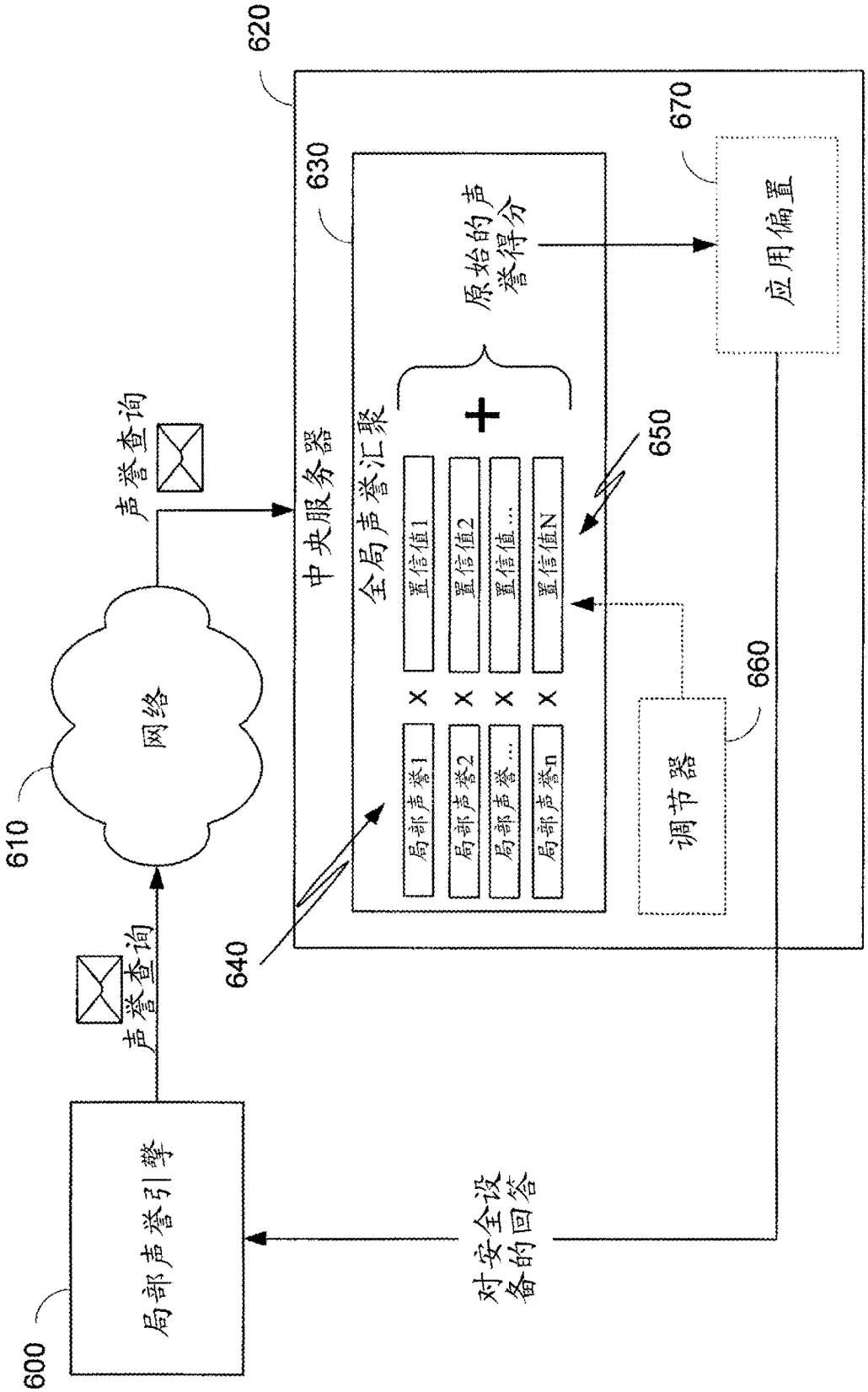

620
630
670
应用偏置
原始的声誉得分
全局声誉汇聚
置信值1
置信值2
置信值...
置信值N
650
660
调节器
中央服务器
声誉查询
网络
610
640
局部声誉1
局部声誉2
局部声誉...
局部声誉n
声誉查询
局部声誉引擎
600
对安全设备的回答

图 6

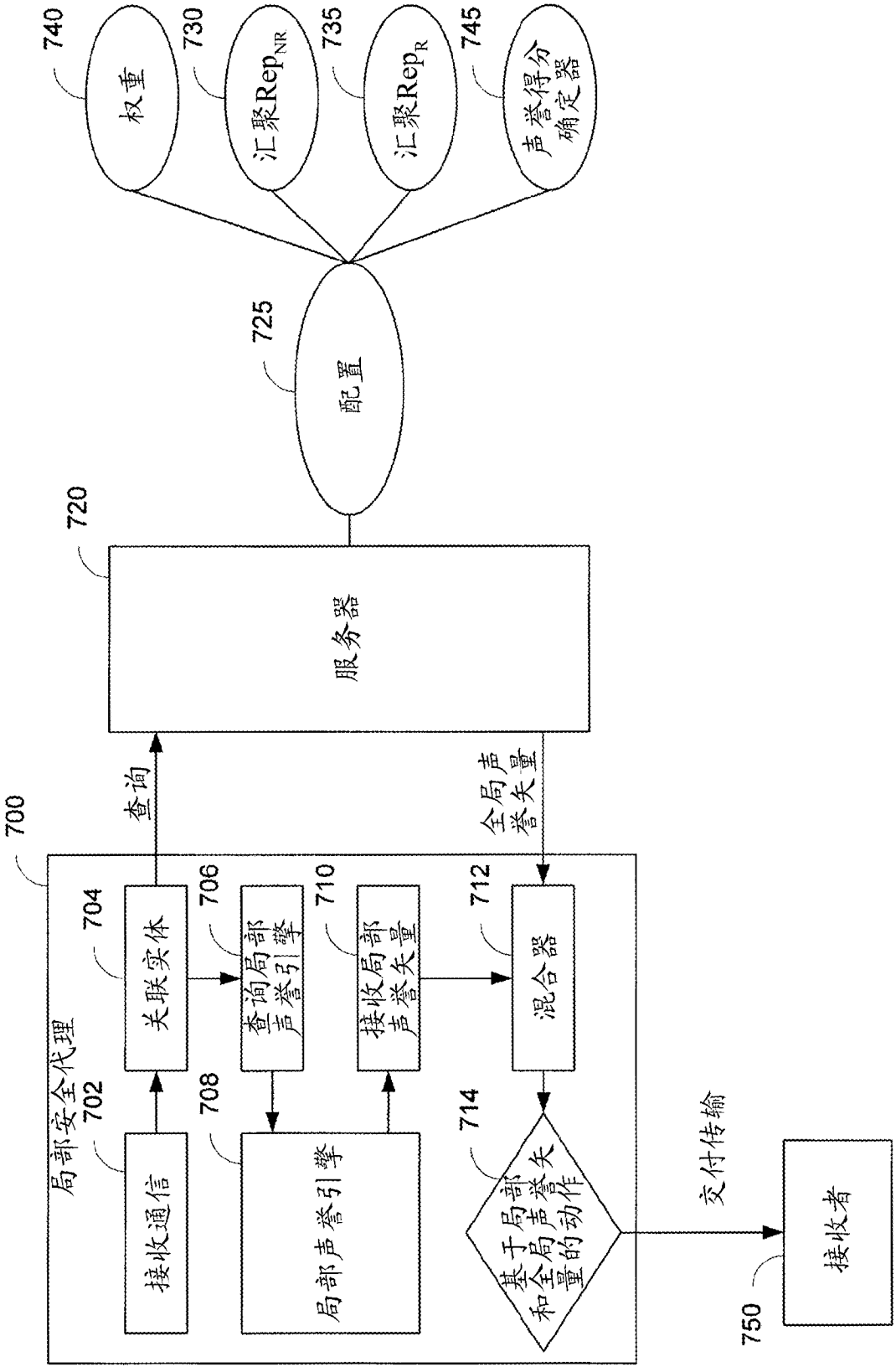

740
权重
730
汇聚Rep_NR
735
汇聚Rep_R
745
声誉得分确定器
725
配置
720
服务器
查询
全局声誉矢量
700
局部安全代理
704
关联实体
706
查询局部声誉引擎
710
接收局部声誉矢量
712
混合器
702
接收通信
708
局部声誉引擎
714
基于局部声誉矢量和全局声誉矢量的动作
交付传输
750
接收者

图 7

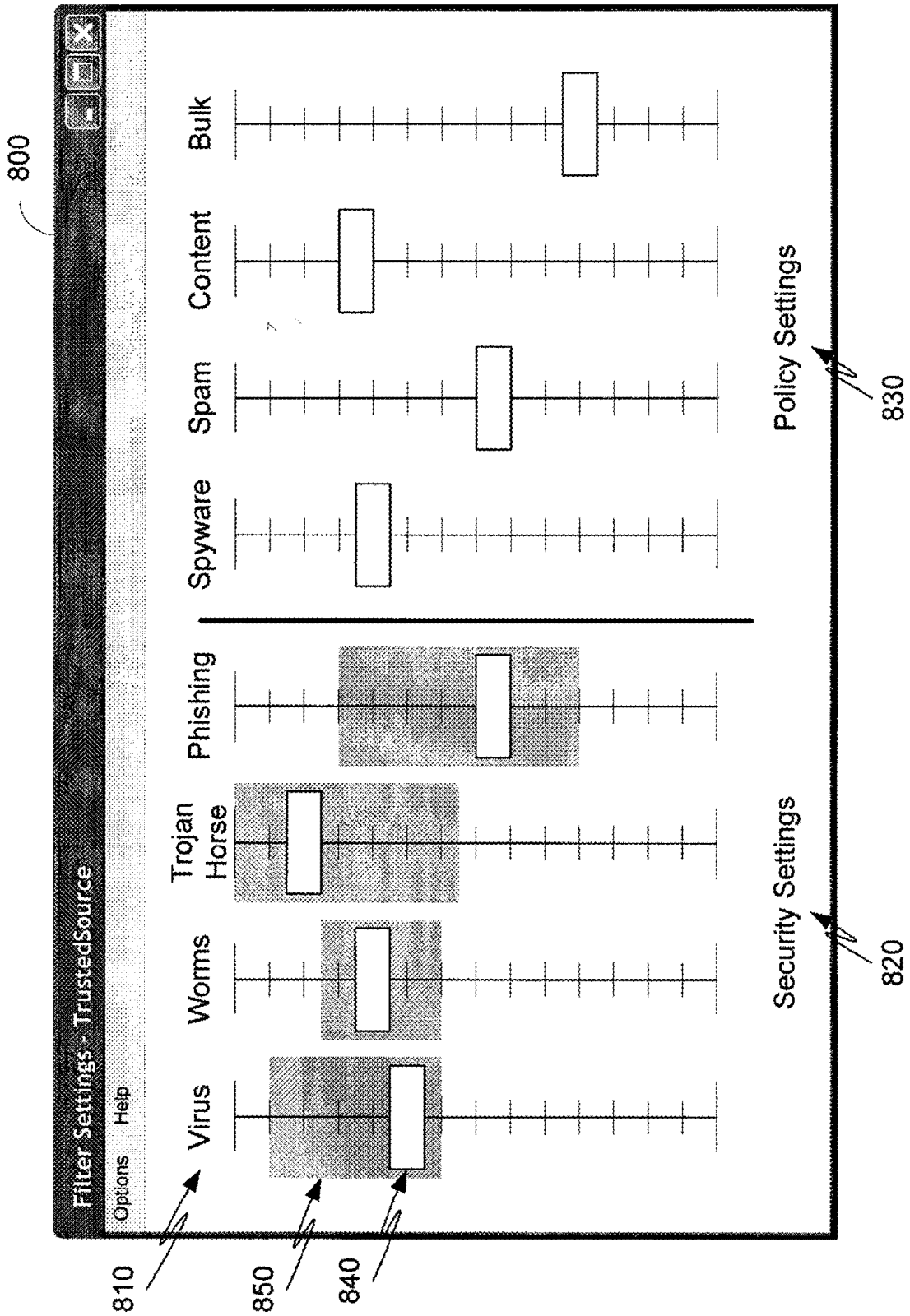

800
Filter Settings - TrustedSource
Options
Help
Virus
Worms
Trojan Horse
Phishing
Spyware
Spam
Content
Bulk
Security Settings
Policy Settings
810
850
840
820
830

图 8

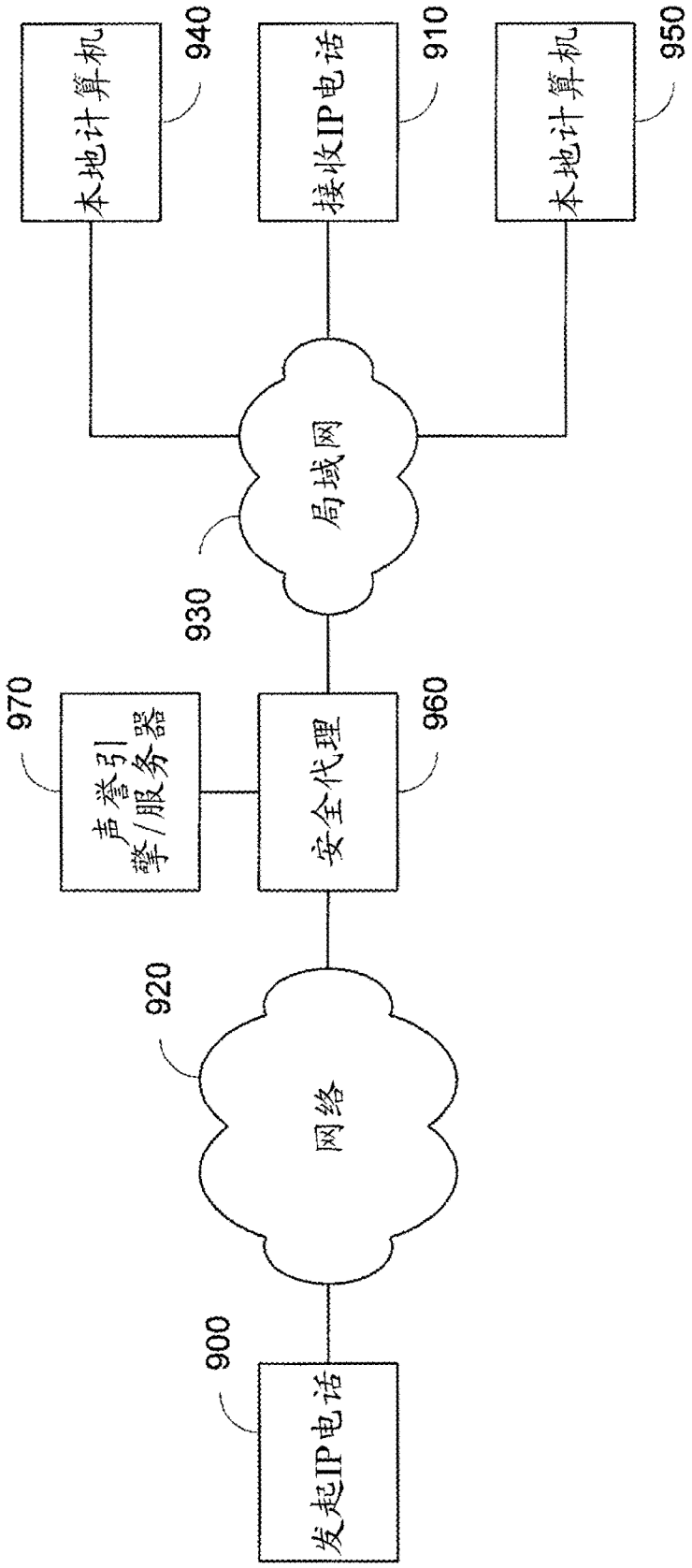

本地计算机
940
接收IP电话
910
本地计算机
950
局域网
930
声誉引擎/服务器
970
安全代理
960
网络
920
发起IP电话
900

图 9

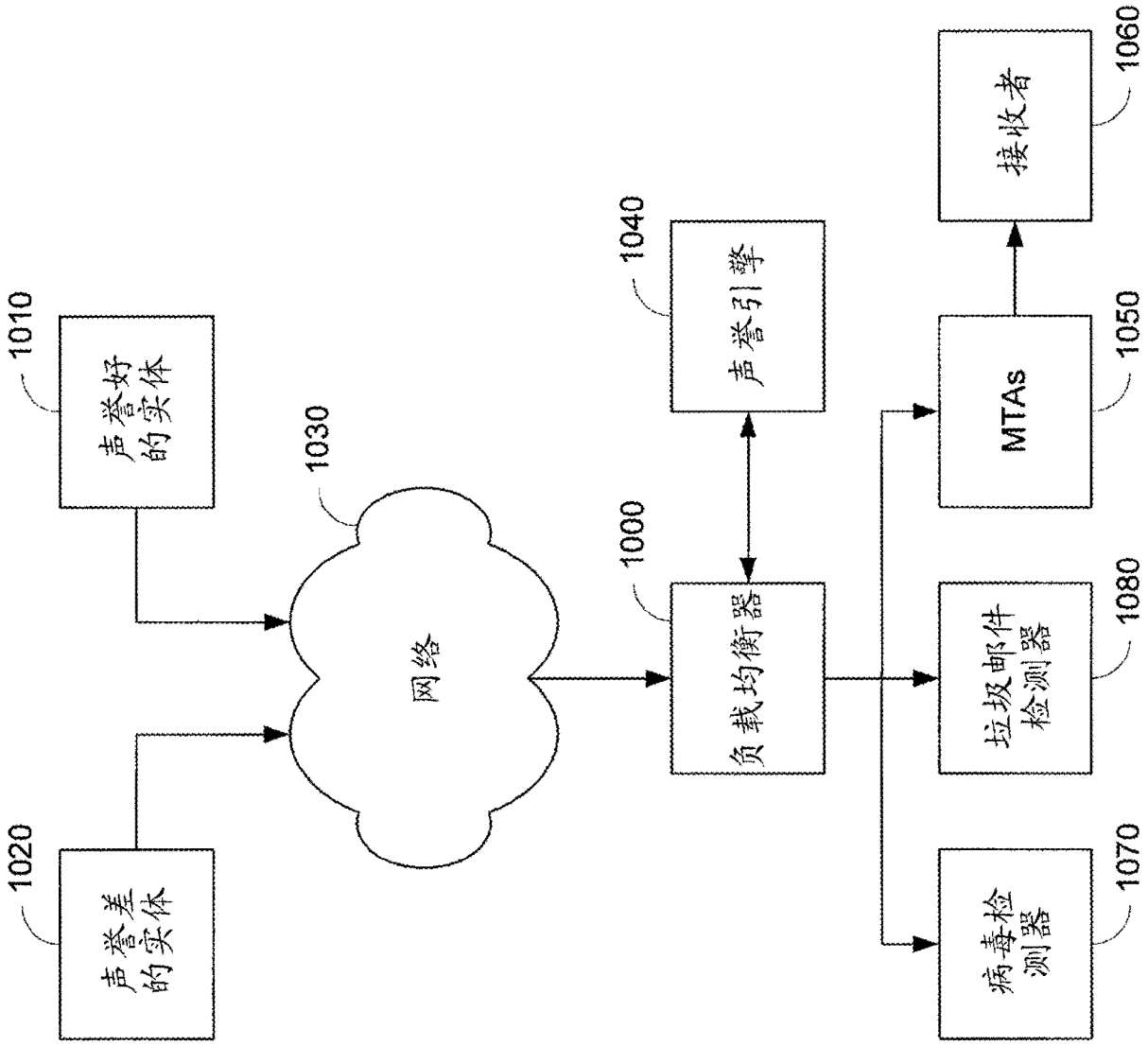

1010
声誉好的实体
1020
声誉差的实体
1030
网络
1000
负载均衡器
1040
声誉引擎
1050
MTAs
1060
接收者
1080
垃圾邮件检测器
1070
病毒检测器

图 10

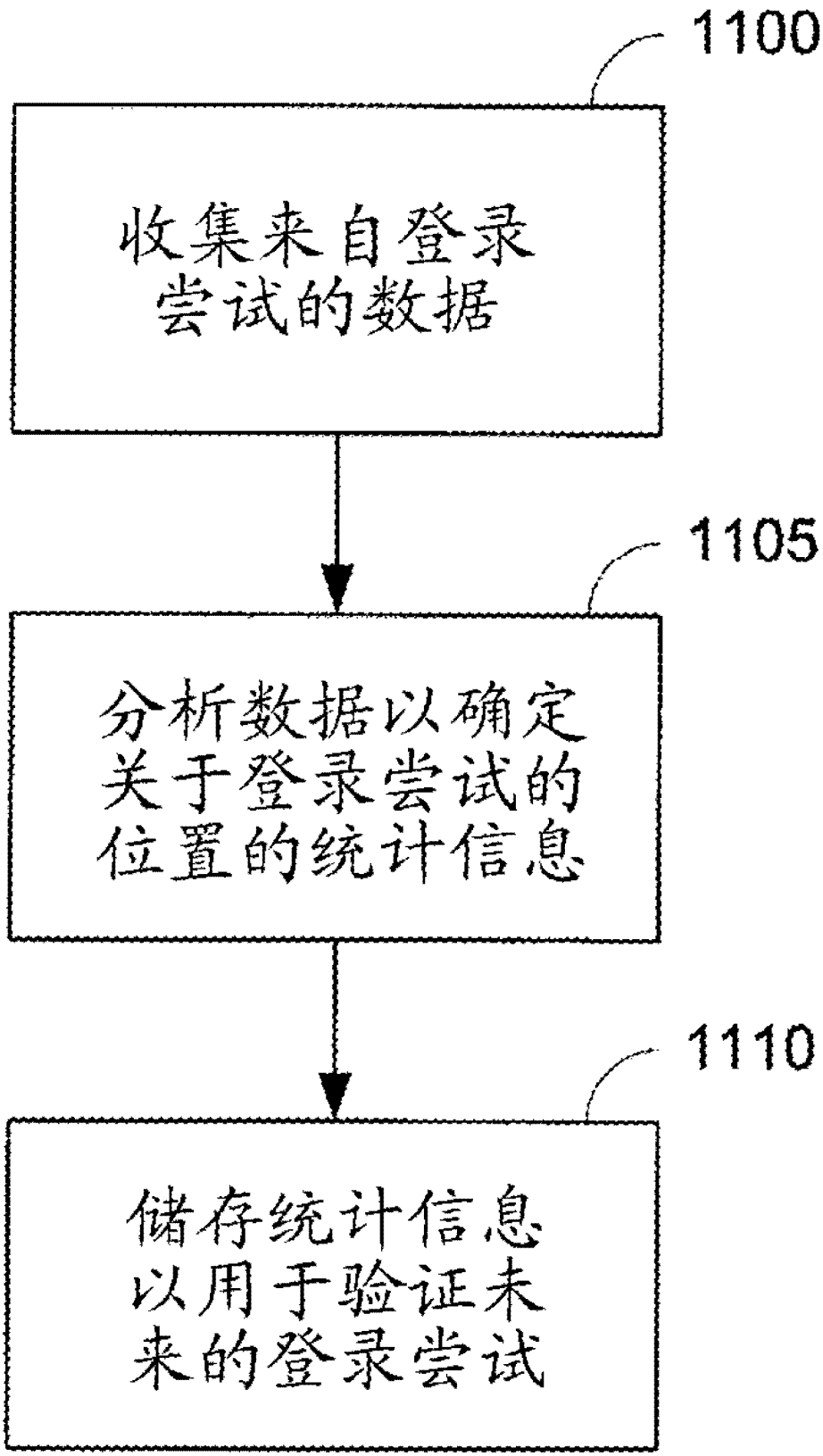

1100
收集来自登录尝试的数据
1105
分析数据以确定关于登录尝试的位置的统计信息
1110
储存统计信息以用于验证未来的登录尝试

图 11A

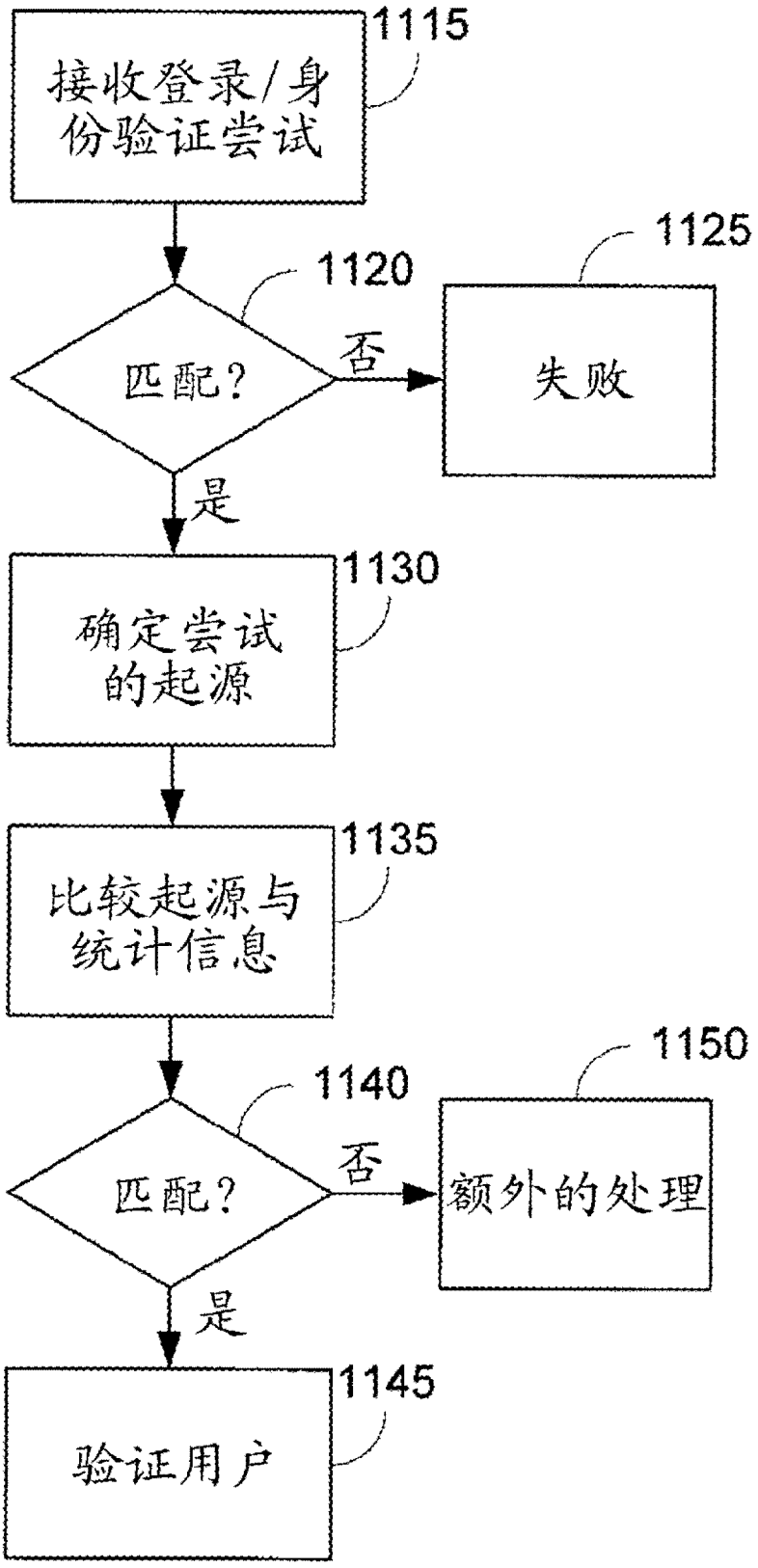

1115
接收登录/身份验证尝试
1120
匹配?
否
1125
失败
是
1130
确定尝试的起源
1135
比较起源与统计信息
1140
匹配?
否
1150
额外的处理
是
1145
验证用户

图 11B

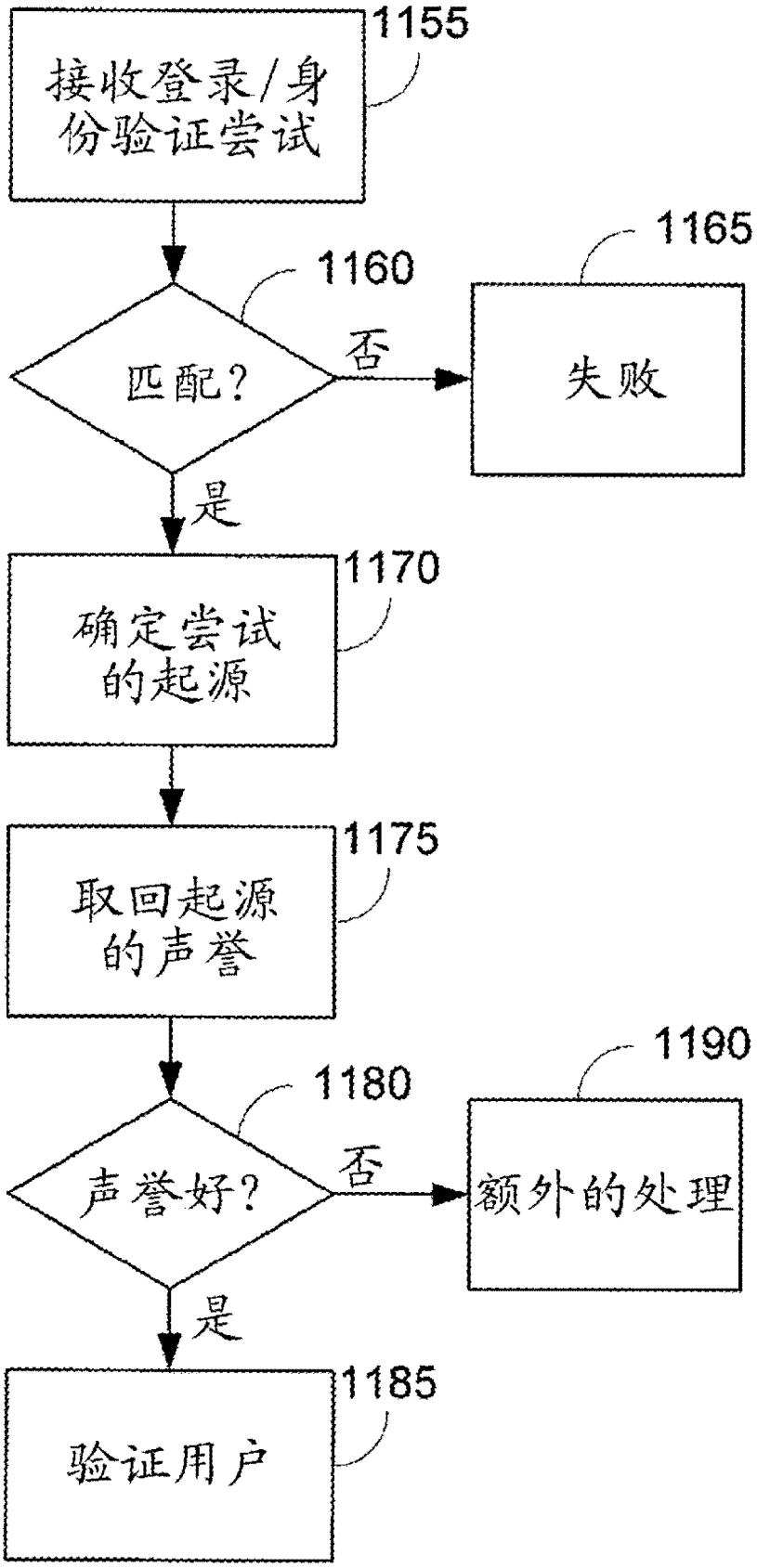

接收登录/身份验证尝试
1155
匹配?
1160
否
失败
1165
是
确定尝试的起源
1170
取回起源的声誉
1175
声誉好?
1180
否
额外的处理
1190
是
验证用户
1185

图 11C

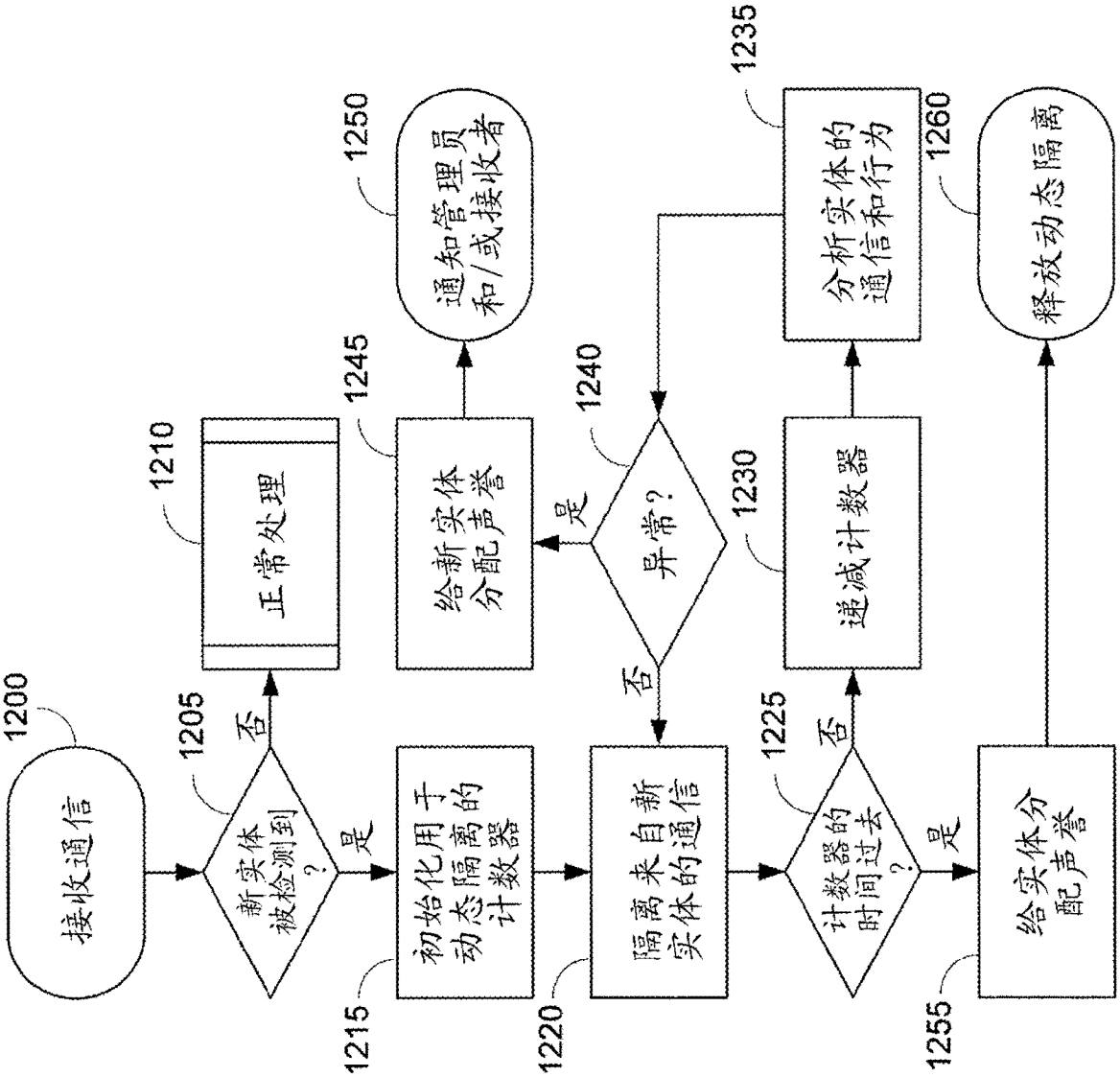

1200
接收通信
1205
新实体被检测到？
否
是
1210
正常处理
1215
初始化用于动态隔离的计数器
1220
隔离来自新实体的通信
1225
计数器的时间过去？
否
是
1230
递减计数器
1235
分析实体的通信和行为
1240
异常？
是
否
1245
给新实体分配声誉
1250
通知管理员和/或接收者
1255
给实体分配声誉
1260
释放动态隔离

图 12

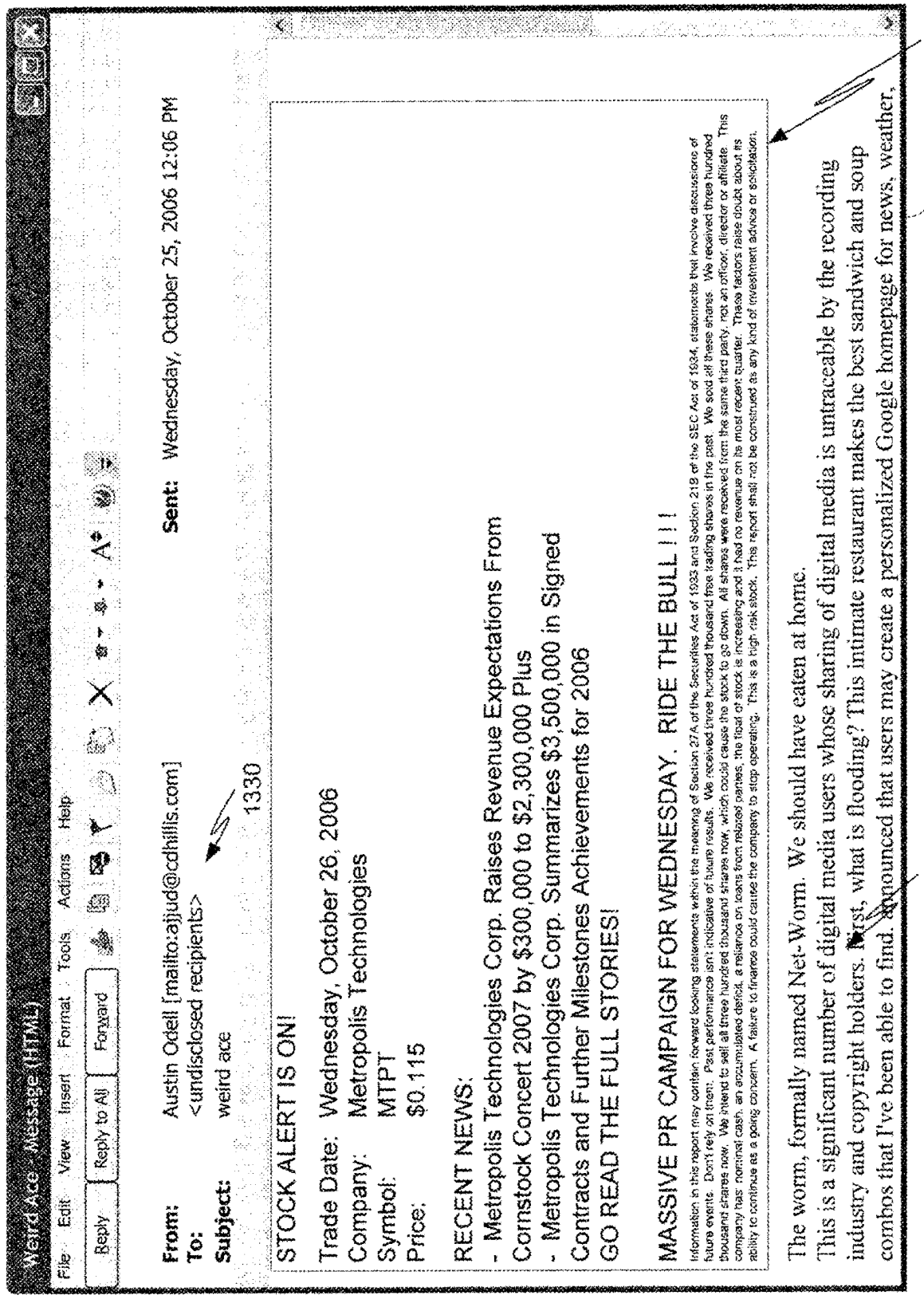

Weird Ace - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: Austin Odell [mailto:ajud@cdhillis.com]
To: <undisclosed recipients>
Subject: weird ace
Sent: Wednesday, October 25, 2006 12:06 PM
1330
STOCK ALERT IS ON!
Trade Date: Wednesday, October 26, 2006
Company: Metropolis Technologies
Symbol: MTPT
Price: $0.115
RECENT NEWS:
- Metropolis Technologies Corp. Raises Revenue Expectations From Cornstock Concert 2007 by $300,000 to $2,300,000 Plus
- Metropolis Technologies Corp. Summarizes $3,500,000 in Signed Contracts and Further Milestones Achievements for 2006
GO READ THE FULL STORIES!
MASSIVE PR CAMPAIGN FOR WEDNESDAY. RIDE THE BULL ! ! !
Information in this report may contain forward looking statements within the meaning of Section 27A of the Securities Act of 1933 and Section 21B of the SEC Act of 1934, statements that involve discussions of future events. Don't rely on them. Past performance isn't indicative of future results. We received three hundred thousand free trading shares in the past. We sold all these shares. We received three hundred thousand shares now. We intend to sell all three hundred thousand shares now, which could cause the stock to go down. All shares were received from the same third party, not an officer, director or affiliate. This company has nominal cash, an accumulated deficit, a reliance on loans from related parties, the float of stock is increasing and it had no revenue on its most recent quarter. These factors raise doubt about its ability to continue as a going concern. A failure to finance could cause the company to stop operating. This is a high risk stock. This report shall not be construed as any kind of investment advice or solicitation.
1320
1300
1310
The worm, formally named Net-Worm. We should have eaten at home.
This is a significant number of digital media users whose sharing of digital media is untraceable by the recording industry and copyright holders. First, what is flooding? This intimate restaurant makes the best sandwich and soup combos that I've been able to find. Announced that users may create a personalized Google homepage for news, weather,

图 13

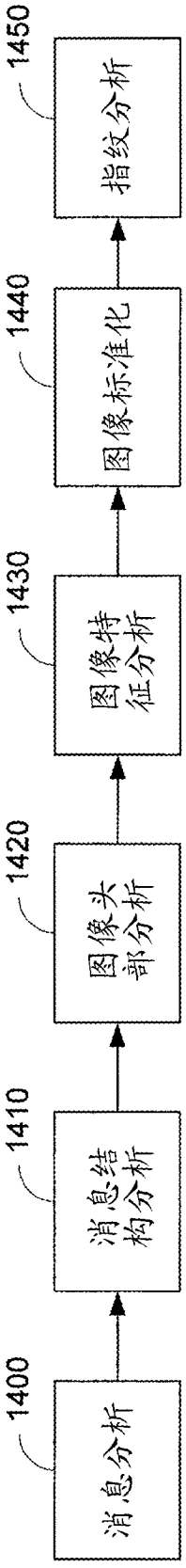

1450
指纹分析
1440
图像标准化
1430
图像特征分析
1420
图像头部分析
1410
消息结构分析
1400
消息分析

图 14

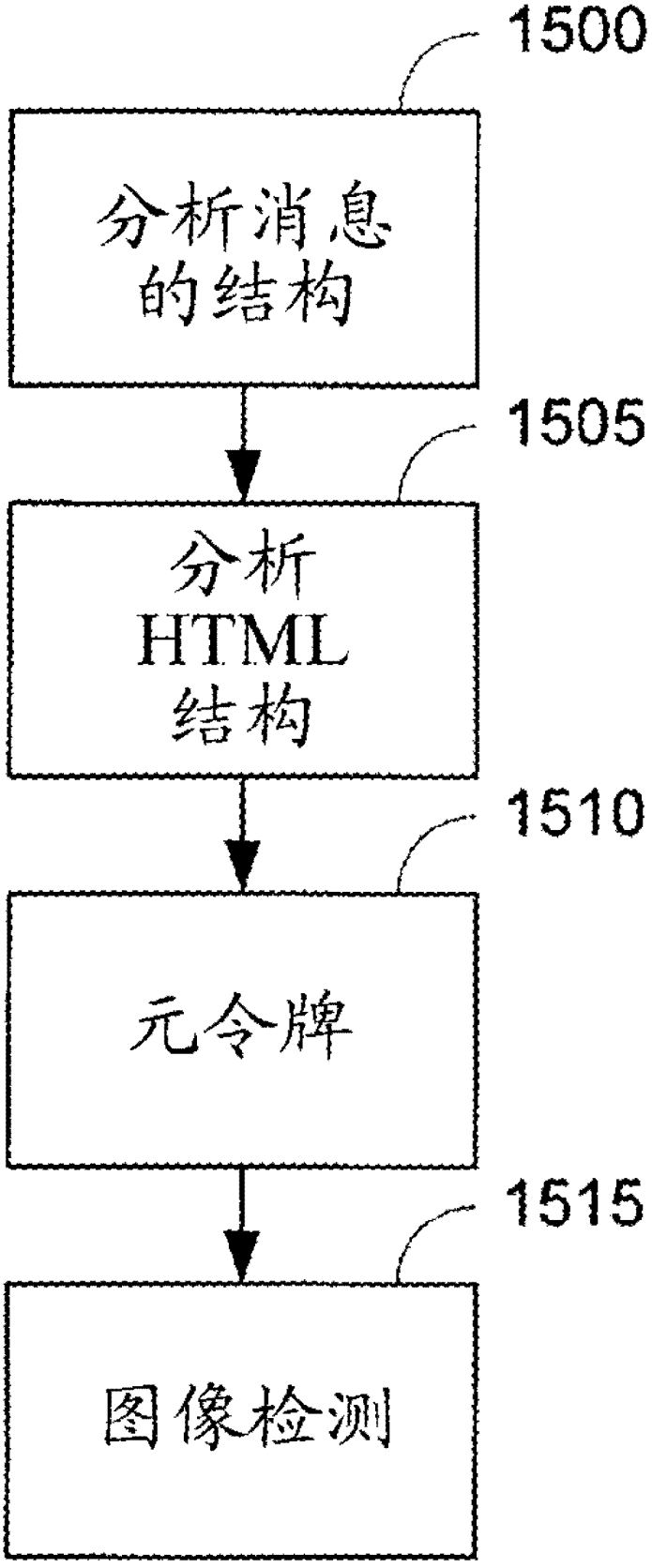

1500
分析消息的结构
1505
分析HTML结构
1510
元令牌
1515
图像检测

图 15A

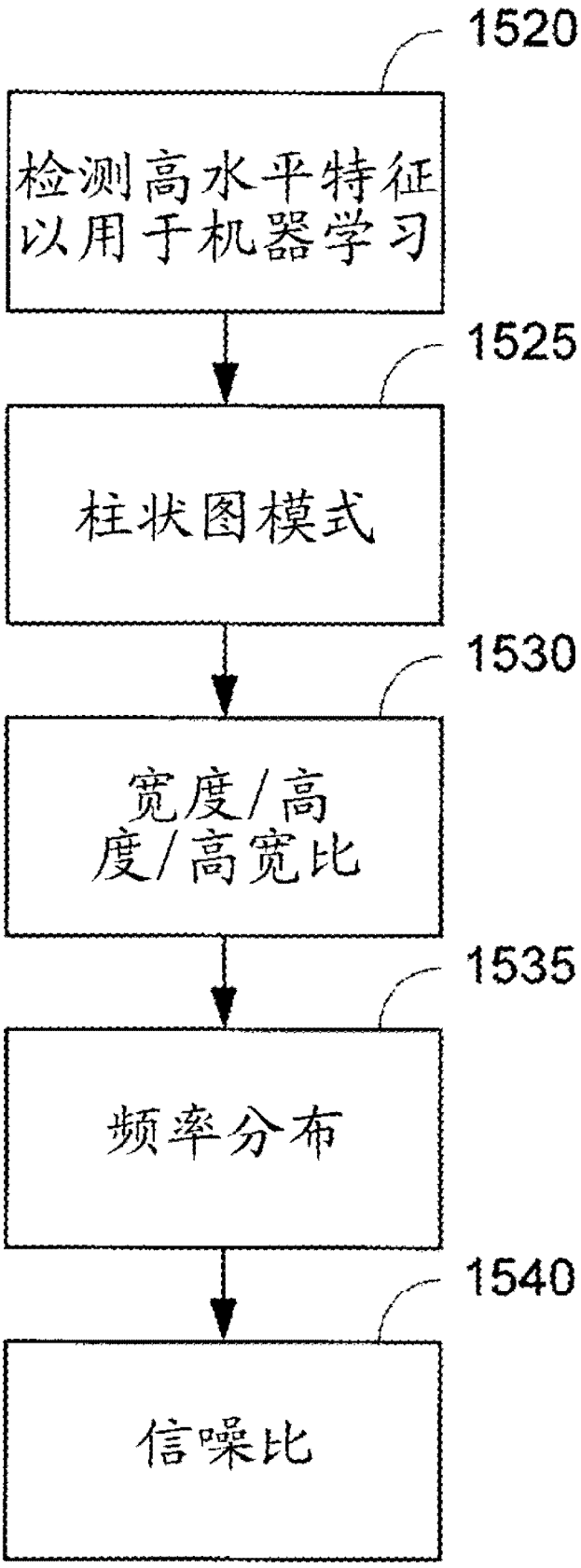

1520
检测高水平特征以用于机器学习
1525
柱状图模式
1530
宽度/高度/高宽比
1535
频率分布
1540
信噪比

图 15B

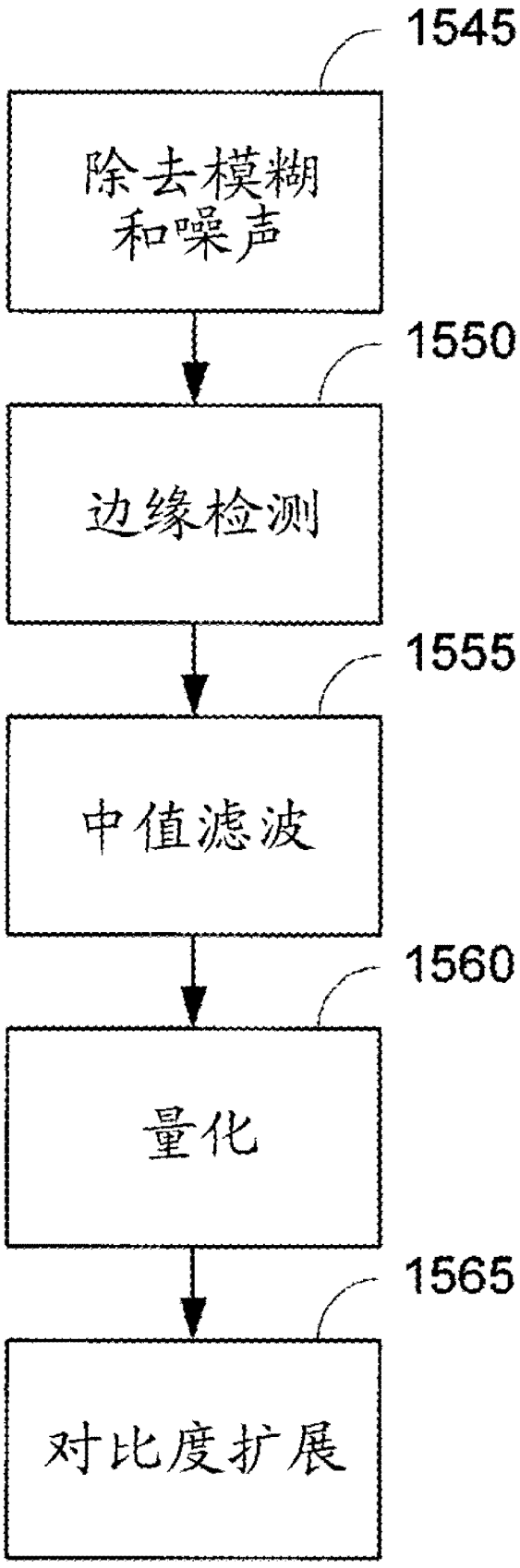


图 15C

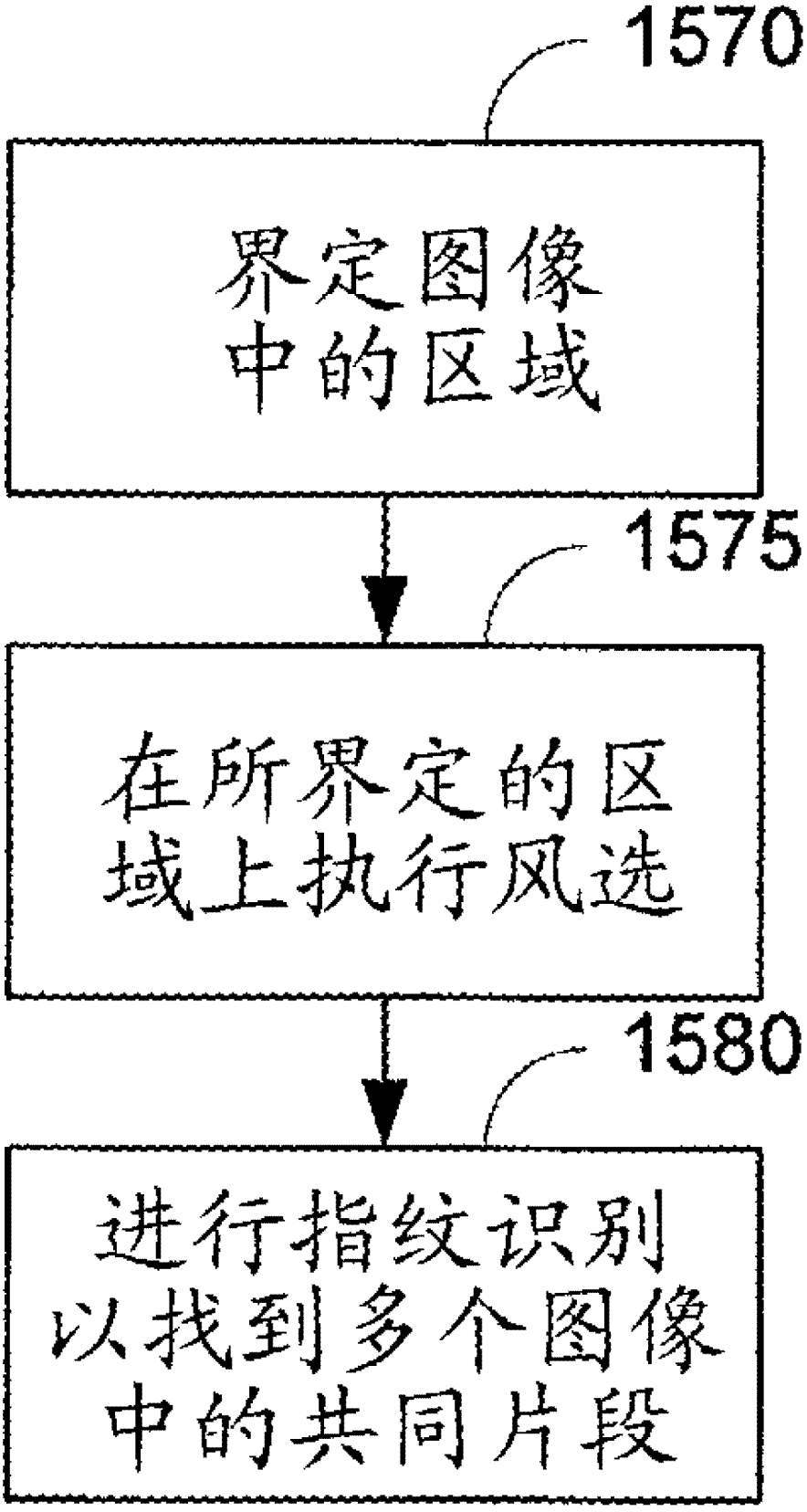

1570
界定图像中的区域
1575
在所界定的区域上执行风选
1580
进行指纹识别以找到多个图像中的共同片段

图 15D