(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101743530 B
(45)授权公告日 2013.04.24

(21)申请号 200880017269.3

(22)申请日 2008.05.16

(30)优先权数据
11/753,439 2007.05.24 US

(85)PCT申请进入国家阶段日
2009.11.24

(86)PCT申请的申请数据
PCT/US2008/063995 2008.05.16

(87)PCT申请的公布数据
WO2008/147737 EN 2008.12.04

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 V·霍洛斯托弗 Y·埃德瑞

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 蔡悦 钱静芳

(51)Int.Cl.
G06F 3/12(2006.01)
G06F 3/14(2006.01)
G06F 17/00(2006.01)

(56)对比文件
US 6088803 A,2000.07.11, 附图3,说明书第3-4栏.

审查员 王可

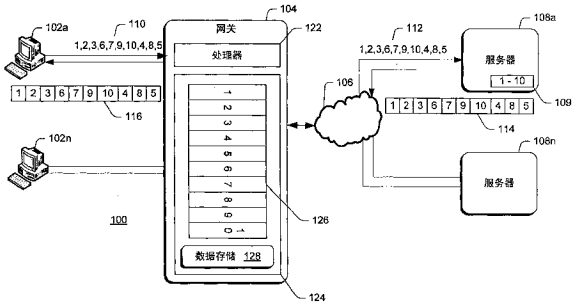
权利要求书2页 说明书6页 附图4页

(54)发明名称

用于部分可用内容的防病毒扫描的方法和系统

(57)摘要

在网络环境中,客户机设备经由网关向服务器传送请求。该请求指示服务器上的文件的要作为下载过程的一部分来传送的特定部分。该网关在其存储器中接收文件的所请求部分并将所接收到的部分组装成组装文件。在将接收到的部分馈送到客户机计算机之前,在文件的所请求部分正被接收并变得可用时,该网关持续地扫描组装文件中的各部分的最大连续序列中的病毒。通过在新部分变得可用的同时扫描最大连续序列,能减少完成扫描的时间,进而增加网关的吞吐量。



CN 101743530 B

1. 一种用于传送包括按原始顺序次序排列的各部分的内容文件的方法，包括：

向服务器传送指示要传送的内容文件的特定部分的请求；

周期性地从所述服务器接收所述内容文件的所请求部分；

将所接收到的部分组装到连续接收到的部分的块中；

确定所述连续接收到的部分的块中的最大块；

在接收所请求的部分的同时，持续地仅仅扫描所述最大块中的所接收到的部分中的病毒；以及

将经扫描的所接收到的部分馈送到客户机计算机。

2. 如权利要求 1 所述的方法，其特征在于，所述内容文件包括按原始顺序次序排列的部分，其中所接收到的部分按该原始顺序次序来组装，并且其中扫描所述最大块中的所接收到的部分包括按该原始顺序次序扫描所述最大块中的连续接收到的部分。

3. 如权利要求 2 所述的方法，其特征在于，扫描包括将所述最大块中的各部分与病毒签名进行比较。

4. 如权利要求 1 所述的方法，其特征在于，还包括标识所述最大块中的可能包含病毒的所接收到的部分，并且扫描所标识的所接收到的部分同时不扫描未标识的所接收到的部分。

5. 如权利要求 4 所述的方法，其特征在于，还包括提供病毒的指示，并在标识到病毒时清除包含该病毒的所接收到的部分。

6. 如权利要求 1 所述的方法，其特征在于，所述请求指示要以顺序次序和不以顺序次序来发送的所述文件的特定部分。

7. 一种用于传送内容的系统，包括：

将内容文件划分成具有原始顺序次序的多个部分的第一计算机；

经由网络与所述第一计算机和第二计算机相耦合的网关；

经由所述网关请求来自所述第一计算机的多个部分的所述第二计算机；

所述第一计算机传送与所述请求相对应的所述多个部分；

所述网关在存储器中接收所述多个部分，在接收所述多个部分的同时按所述原始顺序次序将所接收到的部分组装成组装文件，确定部分的最大连续序列，以所述顺序次序仅仅扫描所述组装文件内的部分的所述最大连续序列中的病毒，将经扫描的组装文件分解成多个分解部分，以及将所述分解部分馈送到所述第二计算机；

以及

所述第二计算机接收所述分解部分并以所述原始顺序次序 (109) 组装所述分解部分。

8. 如权利要求 7 所述的系统，其特征在于，所述第二计算机请求不按所述顺序次序发送所述多个部分中的一些。

9. 如权利要求 7 所述的系统，其特征在于，在接收其它所请求部分的同时，分解所述经扫描的组装文件并将所述分解部分馈送到所述第二计算机。

10. 如权利要求 7 所述的系统，其特征在于，以所请求的顺序将所述分解部分馈送到所述第二计算机。

11. 如权利要求 7 所述的系统，其特征在于，如果在扫描所述组装文件时检测到病毒，则终止将所述分解部分馈送到所述第二计算机。

12. 如权利要求 7 所述的系统，其特征在于，如果在扫描所述组装文件时检测到病毒，则向所述第二计算机提供指示。

13. 如权利要求 7 所述的系统，其特征在于，所述第一计算机是服务器且所述第二计算机是客户机计算机。

14. 一种用于传送包括按原始顺序次序排列的各部分的内容文件的系统，所述系统包括：

用于向服务器传送请求的装置，所述请求指示要按所述原始顺序次序传送所述内容文件的哪些特定部分以及要不按所述原始顺序次序传送所述文件的哪些特定部分；

用于周期性地以所述原始顺序次序在组装文件中接收和存储所述文件 126 的特定部分的装置；

用于确定所述组装文件的特定部分的最大接收到的连续序列的装置；

用于按所述原始顺序次序持续地仅仅扫描所述组装文件的特定部分的所述最大接收到的连续序列的装置，在接收其它所请求的特定部分的同时扫描所述组装文件；以及

用于将经扫描的文件的各部分馈送到客户机计算机的装置。

15. 如权利要求 14 所述的系统，其特征在于，所接收到的特定部分在所述存储器中是按顺序次序来组织的，并且其中扫描所述组装文件包括以所述顺序次序扫描所存储的特定部分的最大连续序列。

16. 如权利要求 14 所述的系统，其特征在于，经由网络以所请求的顺序将所接收到的部分馈送到所述客户机计算机。

17. 如权利要求 14 所述的系统，其特征在于，如果在持续扫描所述组装文件时检测到病毒，则终止将所接收到的部分馈送到所述客户机计算机。

18. 如权利要求 14 所述的系统，其特征在于，还包括用于如果在持续扫描所述组装文件时检测到病毒，则向所述客户机计算机提供指示的装置。

19. 如权利要求 14 所述的系统，其特征在于，将经扫描的组装文件分解成分解部分，并且在接收其它特定部分的同时将所述分解部分馈送到所述客户机计算机。

20. 如权利要求 14 所述的系统，其特征在于，还包括用于在检测到病毒时存储所请求文件的指示，并且在将来请求所请求文件的该特定部分时拒绝对所述文件的特定部分的请求的装置。

用于部分可用内容的防病毒扫描的方法和系统

[0001] 背景

[0002] 一般有两种已接受的方法供计算机应用程序从远程位置下载文件。在第一种方法中，客户机计算机直接或经由网络网关连接到服务器。该客户机计算机向服务器发出一次发送整个文件的请求。该服务器通过向客户机计算机发送该整个文件（通常以分组形式）来响应该请求。在第二种方法中，客户机计算机向服务器或对等计算机（诸如在对等网络中）发送一系列请求，其中每一请求要求文件的特定部分。

[0003] 请求文件的特定部分相对于一次请求整个文件而言是优选的，因为它允许在连接断开的情况下恢复下载。请求文件的特定部分还允许更有效地利用可用带宽，因为当较多带宽可用时客户机计算机可请求较多部分且当较少带宽可用时客户机计算机可请求较少部分。

[0004] 同一文件的已下载部分可以是不同的大小，可被乱序接收或者可与先前下载的部分重叠。当应用程序对所路由的通信量执行防病毒（AV）扫描和检查时，这对网络网关（或者主机计算机）中布署的防病毒应用程序带来了挑战。该扫描过程涉及包含与从远程位置下载的内容进行比较的病毒参考签名或启发式模式的AV应用程序。在许多情况下，防病毒应用程序必须扫描整个文件以确保该文件中没有嵌入任何病毒。

[0005] 通常，在请求文件的一部分后不可能下载整个文件来进行防病毒扫描。整个文件会非常大，从而需要大量网络带宽和时间来完成下载。现有的AV解决方案或者尝试在扫描前下载整个文件或者将扫描限制于已下载部分的内容。对于检测病毒来说，仅检查已下载的一部分内容是不够的。病毒签名可能散布于文件的两个或更多部分，并可能在分开扫描每一文件部分时是不可标识的。

[0006] 概述

[0007] 提供本概述以便以简化形式介绍将在以下详细描述中进一步描述的概念。本概述并非旨在标识要求保护的主题的关键特征或必要特征，也非旨在用于限制要求保护的主题的范围。

[0008] 此处特别描述了用于在内容的防病毒扫描中使用的各种技术的实施例。根据一个实施例，客户机设备经由网络网关将下载内容的请求传送到服务器。这些请求指示要传送的内容的特定部分以及这些部分应被传送的次序。网关在其存储器中接收所请求的各部分内容。这些部分被组装入各个块中并按与它们存储在服务器上时的相同顺序来排列。该排列可不同于经由网络接收到各部分的顺序。当接收到文件的所请求的各部分时，网关扫描具有最大数量的连续部分的块中的病毒。

[0009] 通过扫描具有最大数量的连续部分的块，可以跨各部分边界来快速地标识病毒，以便能在检测到病毒的情况下中止下载剩余部分。这可以在避免传统的效率较差的技术方案的情况下进行，从而增加网关提供的安全性并同时维持正常的最终用户体验并允许进行这种下载，其中所述传统的技术方案或者完全阻塞以各部分来下载的文件或者不在它们之中扫描病毒。

[0010] 因为网关在整个文件在网关处可用之前检查文件各部分的小型组合，因而一旦接

收到最终部分，则对整个文件执行最终扫描。由于仅需要比较病毒签名的子集，所以该最终扫描将快于网关等待整个文件可用的情况。此外，由于网关会中止下载受感染的文件，因此网关能处理更多请求。

[0011] 附图简述

[0012] 参考附图描述以下的详细描述。附图中，参考标号的最左侧的数字标识该标号首次出现的附图。在不同的附图中使用相同的参考标号来指示相似或相同的项。

[0013] 图 1 示出了其中可实现部分可用内容的防病毒扫描的示例性体系结构。

[0014] 图 2a-c 是示出由图 1 中的网关来接收、组装、以及扫描的内容的示图。

[0015] 图 3 是描绘防病毒扫描系统中的网络网关中的选定模块的框图。

[0016] 图 4 是用于当部分可用内容在网关中正被路由时扫描该内容的示例性过程的流程图。

[0017] 详细描述

[0018] 概览

[0019] 此处描述的特别是用于在内容的防病毒扫描中使用的各种技术的实施例。根据这里描述的一个实施例，响应于来自客户机计算设备的请求，防病毒扫描系统经由网络网关（或者任何主机计算机）将内容的各部分从服务器（或任何对等计算机）传输到该计算设备。这些部分由网关接收并被组装成组装文件。在接收文件的被请求部分的同时，网关扫描该组装文件中的最大数量的连续部分的块中的病毒。

[0020] 示例系统体系结构

[0021] 图 1 示出了包括经由网络网关 104 通过网络 106 与服务器 108a-108n 相耦合的客户机计算设备 102a-102n 的病毒检测系统 100。尽管示出了网关 104，但可以使用能扫描病毒的任何类型的网络处理设备来替换网关 104。这种处理设备的示例包括代理服务器和通用计算机。

[0022] 服务器 108a 中存储了内容文件 109。该内容文件具有按原始顺序次序排列的部分 1-10。在一个实施例中，客户机计算设备 102a 发送指示要下载服务器 108a 上存储的内容文件 109 的哪些部分 110 的请求。特别地，设备 102a 请求按所请求的次序 1、2、3、6、7、9、10、4、8 和 5 来传送各部分 110。然后，网关 104 经由网络 106 将部分请求 112 馈送到服务器 108a。服务器 108a 通过按所请求的次序向网关 104 传送各部分 109（如部分 114）来做出响应。

[0023] 网关 104 包括一个或多个处理器 122 和存储器 124。存储器 124 中存储了组装文件 126 和数据存储 128。部分 114 由网关 104 接收并使用处理器 122 来存储在存储器 124 中。在一示例性实施例中，在接收到部分 114 时，处理器 122 按它们原始的顺序次序将接收到的各部分安排入组装文件 126 内的各个块中。同样，在接收到各部分时，扫描组装文件 126 中的最大的连续部分的块，以确定是否存在病毒。扫描过程的示例在图 2a-2c 中描述。

[0024] 病毒签名存储于数据存储 128 中。数据存储 128 以新的病毒签名来周期性地更新。在一个实施例中，通过将组装文件 126 的各部分与病毒签名进行比较来执行扫描。在另一实施例中，防病毒扫描不限于签名比较。可以用以下方式来执行扫描：首先确定内容的类型，然后执行正则表达式匹配（寻找签名）和行为分析，在隔离环境中执行文件的各部分以观察被执行的部分尝试做什么。

[0025] 在一个实施例中，可以标识组装文件 126 的已知不包含病毒或已知包含病毒的特定部分。在扫描时，可以跳过已知不包含病毒的部分。在一个实施例中，AV 引擎可以确定它需要扫描整个文件以检查内容（例如，当是除非整个文档存在否则不能解包的档案的情况时）。在这些情况下，AV 引擎将仅对文件扫描一次，例如当所有部分都可用时。

[0026] 如果在扫描时未检测到病毒，则网关 104 将为整个所请求（或部分所请求）的内容文件继续按照顺序次序将接收到的部分安排在各块内。病毒签名的大小可大 于多个接收到的部分的组合。因此，在将所有所请求的部分从组装文件 126 中分解出来并作为分解部分 116 被馈送到设备 102a 之前，网关扫描所有所请求的部分。特别地，一旦接收到请求（或部分请求）中的所有部分，则网关 104 按设备 102a 所请求的次序将分解的各部分 116 馈送到设备 102a。

[0027] 在接收、组装了每一部分并扫描了组装文件 126 的最大可用部分后并且如果没有检测到病毒，则将最后接收到的部分馈送到客户机计算设备 102a。这确保了在网关 104 进行组装或取出附加部分时客户机不必等待。

[0028] 在一个实施例中，如果在组装文件 126 中检测到病毒，则该组装文件的受感染部分将被清除且不被馈送到客户机设备 102a。同样，在病毒检测后，可以向客户机提供文件 126 的受感染部分的指示。此外，在另一实施例中，可以通过将发送到客户机设备 102a 的部分 116 嵌入病毒指示来将受感染文件的指示馈送到客户机设备 102a，或者这种指示可被发送到系统管理员（未示出）。

[0029] 图 2a-2c 示出了存储器 104，其包括网关 104 的存储器 104 中的在响应于来自设备 102a 的单个请求接收内容之后顺序时间点处的组装文件 126。在一个实施例中，网关 104 可检测来自设备 102a 的请求，并将来自多个请求的响应组装到单个组装文件 126 内的块中以用于扫描。在另一实施例中，网关 104 可在将经扫描的内容转发到设备 102a 之前检测来自单个请求的响应。图 2a 和 2b 中，组装文件 126 被描绘成包含部分可用的内容。图 2c 中，组装文件 126 被描绘成包括整个内容文件 109。

[0030] 参考图 2a，内容文件 109 的部分 114（图 1）被接收并存储于组装文件 126 中。当接收到部分 114 时，它们按其原始的顺序次序排列（同样参见图 1）。同样，当接收到更多部分 114 时，扫描具有最大数量的连续次序部分的块以确定是否存在病毒。在一个实施例中，在扫描这些部分前，必须接收到具有最小大小的最小阈值数量的部分或者总计数量的部分。可以在接收到每一新部分后扫描组装文件 126。此外，在将整个内容文件存储入组装文件 126 后，可扫描该整个文件以确定是否存在病毒。

[0031] 例如，在图 2a 中，接收到的部分 1-3、6、7、9 和 10 被组装入存储器 124 以创建组装文件 126。在该示例中，可将部分的最小阈值数量设为 4。因此，一旦接收到部分 4，则将部分 4 与部分 1-3、6、7、9 和 10 一起组装入组装文件 126 以形成具有部分 1-4 的块、具有部分 6-7 的块和具有部分 9-10 的块。扫描最大的连续部分的块，例如包含部分 1-4 的块，以确定是否存在病毒。如果不存在病毒，则将接 收另外的各部分。

[0032] 参考图 2b，接收到部分 8。然后，将部分 8 与部分 1-4、6-7、9-10 一起组装入组装文件 126 中，以创建具有部分 1-4 的块和具有部分 6-10 的块。扫描最大的连续部分的块，例如包含部分 6-10 的块，以确定是否存在病毒。如果病毒不存在，则将再次接收另外的各部分。

[0033] 参考图 2c，接收到部分 5，并将该部分与部分 1-4 和 6-10 一起组装入组装文件 126 中，以创建具有部分 1-10 的块。扫描最大的连续部分的块，例如包含部分 1-10 的区块。尽管示出了具有十个部分的示例性内容文件 109，但具有附加部分的更大文件也可按类似的方式被组装和扫描，例如通过扫描组装文件 126 中的最大连续部分的块。

[0034] 图 3 中示出了图 1 所示的病毒检测系统 100 的网关 104 中的选定模块。网关 104 具有适于存储和执行计算机可执行指令的处理能力以及存储器。在一个示例中，网关 104 包括一个或多个处理器 122 和存储器 124。

[0035] 存储器 124 可包括按用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任何方法或技术实现的易失性和非易失性存储器、可移动和不可移动介质。这种存储器包括，但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术，CD-ROM、数字多功能盘 (DVD) 或其它光学存储设备，磁盒、磁带、磁盘存储或其它磁性存储设备，RAID 存储系统，或者可用于存储所需信息并可由计算机系统访问的任何其它介质。

[0036] 网关 104 的存储器 124 中存储了收发机组件 306、组装模块 308、扫描模块 310、分解模块 312 和数据存储 314。这些模块和组件 306-314 可被实现为由一个或多个处理器 122 执行的软件或计算机可执行指令。

[0037] 收发机组件 306 接收来自客户机计算机设备 102(a-n) 的信息和请求，并经由网络 106 将这些请求馈送到服务器 108(a-n)。在一个实施例中，这种请求可符合超文本传输协议 (HTTP) 和传输控制协议 / 因特网协议 (TCP/IP)。收发机组件 306 将网关 104 从服务器 108(a-n) 接收到的内容传送到客户机计算机设备 102(a-n) 并将来自客户机设备 102(a-n) 的内容传送到服务器 108(a-n)。在一个实施例中，这些内容直接从存储器 124 传送。

[0038] 组装模块 308 将从服务器 108(a-n) 接收到的各部分积累并存储在存储器 124 中。各部分被顺序地存储入组装文件内的数据块。可以扫描最大连续部分中的病毒。当各部分正由网关 104 接收时，扫描模块 310 扫描组装文件中的具有最大数量的连 续部分的块。扫描该块以检测病毒，包括具有跨各部分边界延伸的签名的病毒。通过扫描最大连续部分，可以在检测到病毒的情况下快速地终止下载过程，并且增加了在部分内容中检测到该病毒的可能性。

[0039] 分解模块 312 将组装文件分解成各分解部分，以便传送到客户机计算机设备 102(a-n)。在分解组装文件后，各分解部分 116 被排列成以请求 110 所指示的次序传送到客户机计算机设备 102(a-n)。在一个较简单的实施例中，当接收到每一部分时，在扫描了最大连续部分后立刻将其发送到客户机 102。

[0040] 数据存储 314 包含了可不时更新的病毒签名。在另一实施例中，AV 引擎中包含检查逻辑，且 AV 引擎被频繁地更新以检测新的恶意软件。同样，数据存储 314 中可以存储来自服务器 108(a-n) 的先前被检测到病毒的内容文件的名称或网络地址 (诸如统一资源定位符 URL)。在一个实施例中，组装文件可被存储在数据存储 314 中。

[0041] 示例性过程

[0042] 图 4 中的示例性过程被示为逻辑流程图中的框的集合，其表示可以用硬件、软件或它们的组合来实现的一系列操作。在软件上下文中，各框表示在由一个或多个处理器执行时执行所述操作的计算机可执行指令。一般而言，计算机可执行指令包括执行特定功能或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。描述各操作的次序并不旨

在被解释为限制，且任何数量的所述框可按任何次序和 / 或并行地组合以实现该过程。出于讨论的目的，参考图 1 的系统 100 来描述该过程，但该过程也可在其它系统体系结构中实现。

[0043] 图 4 示出了病毒检测系统 100 的网关 104（参见图 1）用于扫描部分可用内容中的病毒的示例性过程 400 的流程图。尽管该流程图按所示各框的次序进行描述，但框 402-424 不必以任何特定的次序来实现。

[0044] 在框 402 处，网关 104 与客户机设备 102(a-n) 之一以及服务器 108(a-n) 之一连接。网关 104 还从客户机计算机设备 102(a-n) 中的一个或多个接收对内容文件 109 的部分 110 的请求。在一个实施例中，客户机计算机设备 102(a-n) 实际上指定了从服务器 108(a-n) 传送各部分的次序。在另一实施例中，客户机计算机设备 102(a-n) 可传送文件名或文件地址来作为请求。作为示例，在过程 400 中，网关 104 从客户机 102a 接收请求以传输到服务器 108a。

[0045] 在框 404 处，通过将数据存储 214 中的信息与客户机计算机设备 102a 的请求进行比较，网关 104 确定先前是否已做出接收到的对内容文件的该部分的请求。该 确定可通过检查该请求以标识所请求文件的地址或名称来进行。如果该标识先前已做出（对于框 404 的“是”），则在框 420 中，就先前请求的文件是否包含病毒做出判定。如果该文件先前未被请求（对于框 404 的“否”），则在框 406 中将客户机设备的对内容文件 109 的该部分的请求 110 传送到服务器 108a。

[0046] 接着，在框 408 中，网关 104 从服务器 108a 接收内容文件 109 的下一部分。在框 410 中，网关 104 将接收到的部分存储到存储器 124 中并按顺序的次序将该部分组装到组装文件中的块中。随后，在框 412 中，通过将一个或多个部分与从数据存储 214 检索到的病毒签名进行比较，网关 104 扫描组装文件中具有最大数量的连续部分的块。该扫描可在内容文件的其它部分正由网关 104 接收时跨各部分边界连续进行。如果病毒签名与组装文件相匹配，则检测到病毒。在一个实施例中，可在网关 104 中配置要扫描的块的最小大小以及将扫描组装文件的最大次数。如果不存在最小块大小，则可以不扫描该组装文件。

[0047] 在另一实施例中，网关 104 标识组装文件的文件格式（通过组合由传递协议所传达的关于对象名称或类型的信息，或者通过查看已被组装的连续部分并基于实际内容来确定文件格式）。也可标识组装文件的已知不包含病毒的特定部分，并因此不扫描这些部分。例如，如果被质疑的组装文件被标识为 JPEG 文件，则网关 104 将假定可能在 EXIF 部分中找到恶意代码并使其它文件部分（非 EXIF 部分）通过而不扫描它们。

[0048] 在框 414 中，网关 104 确定是否检测到病毒。如果检测到（对于框 414 的“是”），则在框 422 中网关 104 将病毒指示提供给管理员设备（未示出）或客户机计算机。如果未检测到病毒（对于框 414 的“否”），则在框 415 中从组装文件中分解出各部分，并将它们作为分解部分 116（图 1）以请求 110 中请求这些部分的次序来馈送到客户机计算机设备 102a。在网关 104 接收到所有部分之前，将当前部分（或各部分）发送到客户机计算机设备 102a。然后，在框 416 中，确定网关 104 是否已接收到所请求文件的所有部分（例如，网关 104 是否已接收到整个组装文件）。如果未接收到所有部分（对于框 416 的“否”），则在来自客户机计算机的请求之后，在框 408 中接收内容文件的下一部分。如果已接收到内容文件的所有部分（对于框 414 的“是”），则在框 418 中将来自服务器 108a 的最后接收的部

分发送到客户机计算机设备 102a。

[0049] 在框 422 中指示病毒后，在一个实施例中，在框 424 中，组装文件的该病毒性部分被清除并终止含该病毒的该部分文件的向客户机计算机设备 102a 的传输。 在另一实施例中，在框 424 中，可在将该部分馈送到客户机计算机设备 102a 之前标记含病毒的该部分文件。

[0050] 如果已确定先前请求的文件包含病毒（对于框 420 的“是”），则在框 422 中提供病毒指示。如果确定该文件不含病毒（对于框 420 的“否”），则在框 406 中将部分请求 112 馈送给服务器 108a。

[0051] 结论

[0052] 最后，尽管已经以结构特征和 / 或方法动作专用的语言描述了本发明，但可以理解，所附的权利要求书中限定的发明不必限于所述的具体特征或动作。相反，这些具体特征和动作仅作为实施本发明的示例性形式而被公开。

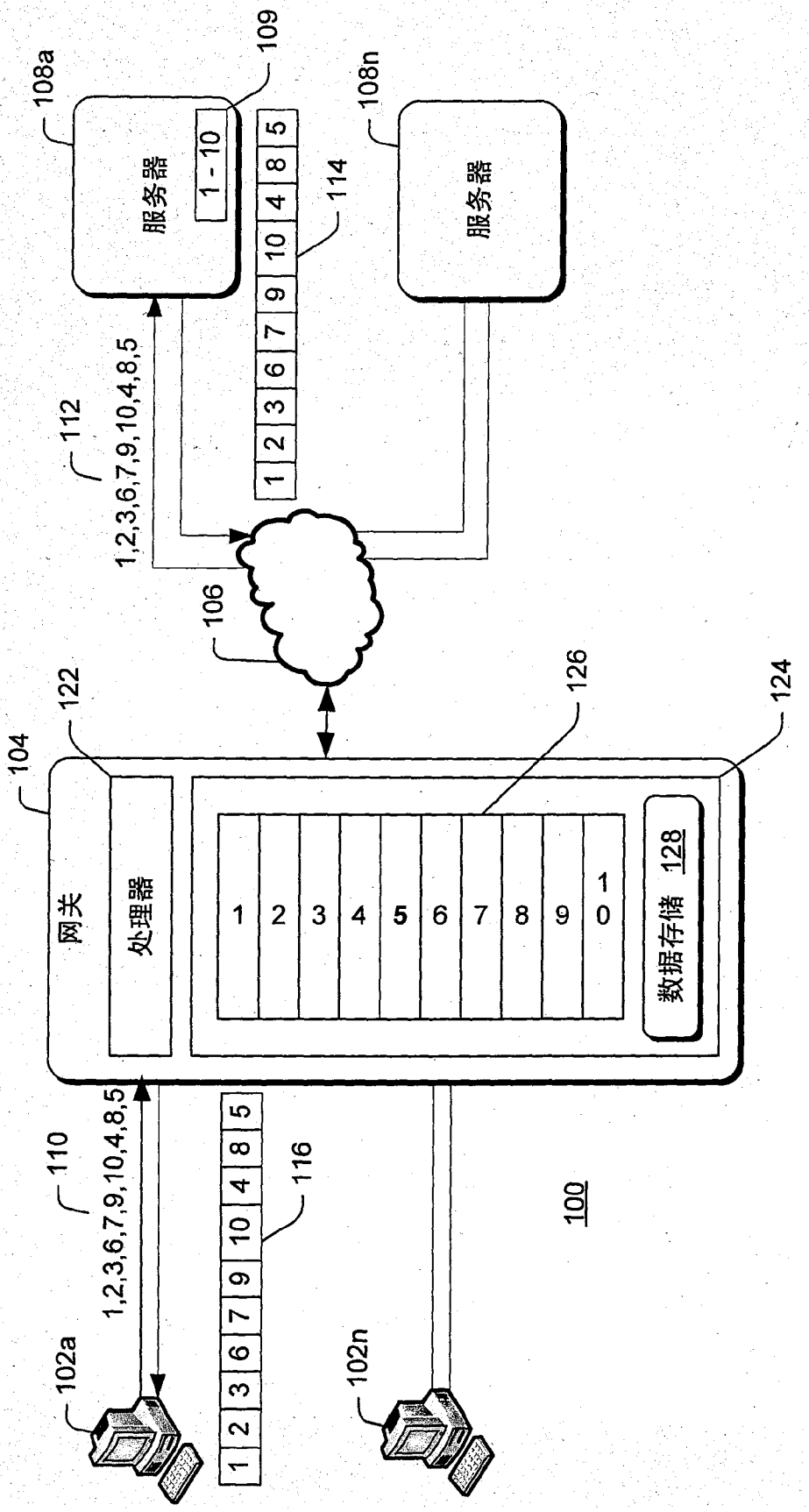

108a
109
服务器
1 - 10
108n
服务器
114
1 2 3 4 5 6 7 8 9 10
112
1,2,3,6,7,9,10,4,8,5
106
104
网关
122
处理器
126
124
1 2 3 4 5 6 7 8 9 10
数据存储 128
110
1,2,3,6,7,9,10,4,8,5
116
1 2 3 6 7 9 10 4 8 5
100
102a
102n

图 1

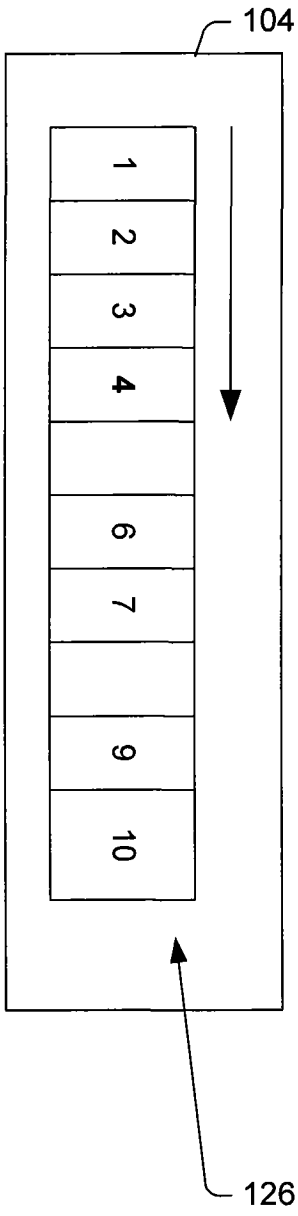


图 2a

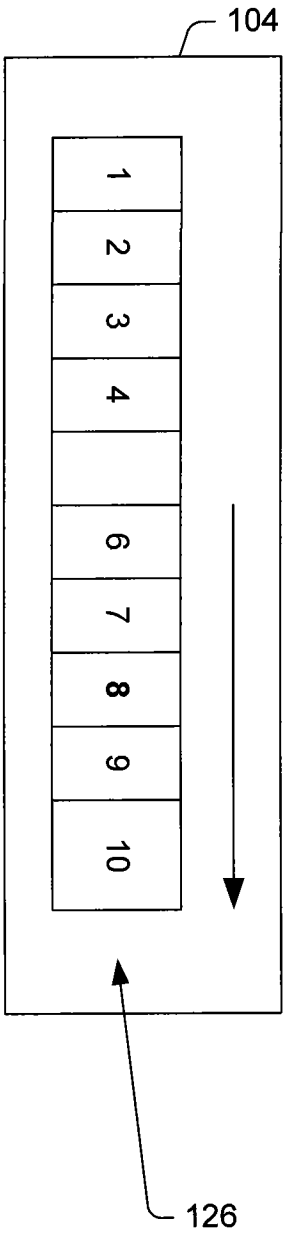


图 2b

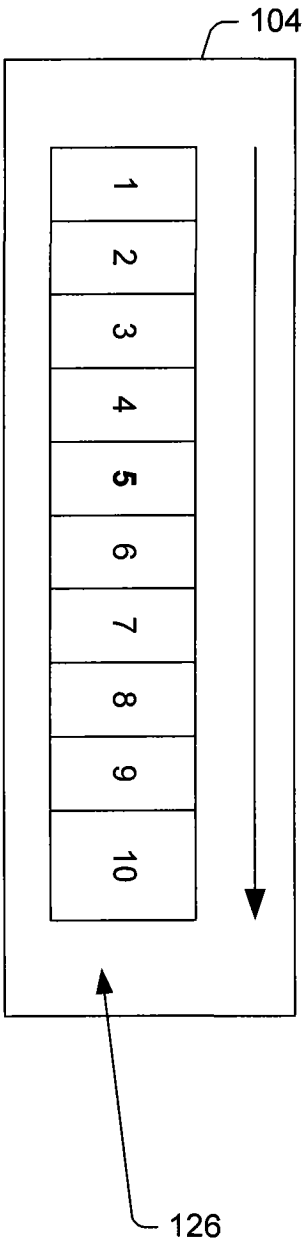


图 2c

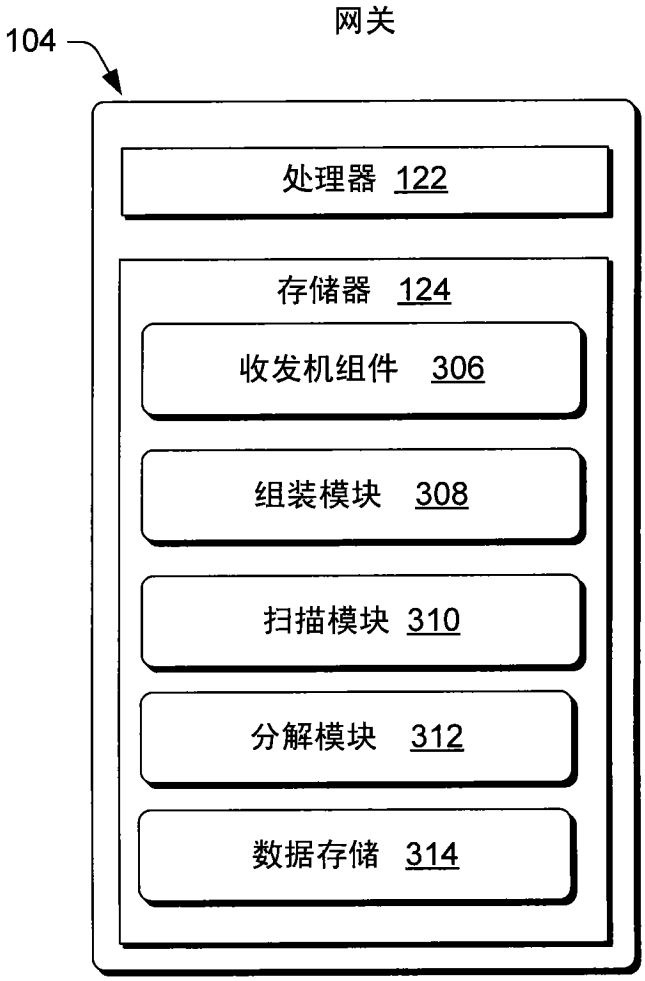

网关
104
处理器 122
存储器 124
收发机组件 306
组装模块 308
扫描模块 310
分解模块 312
数据存储 314

图 3

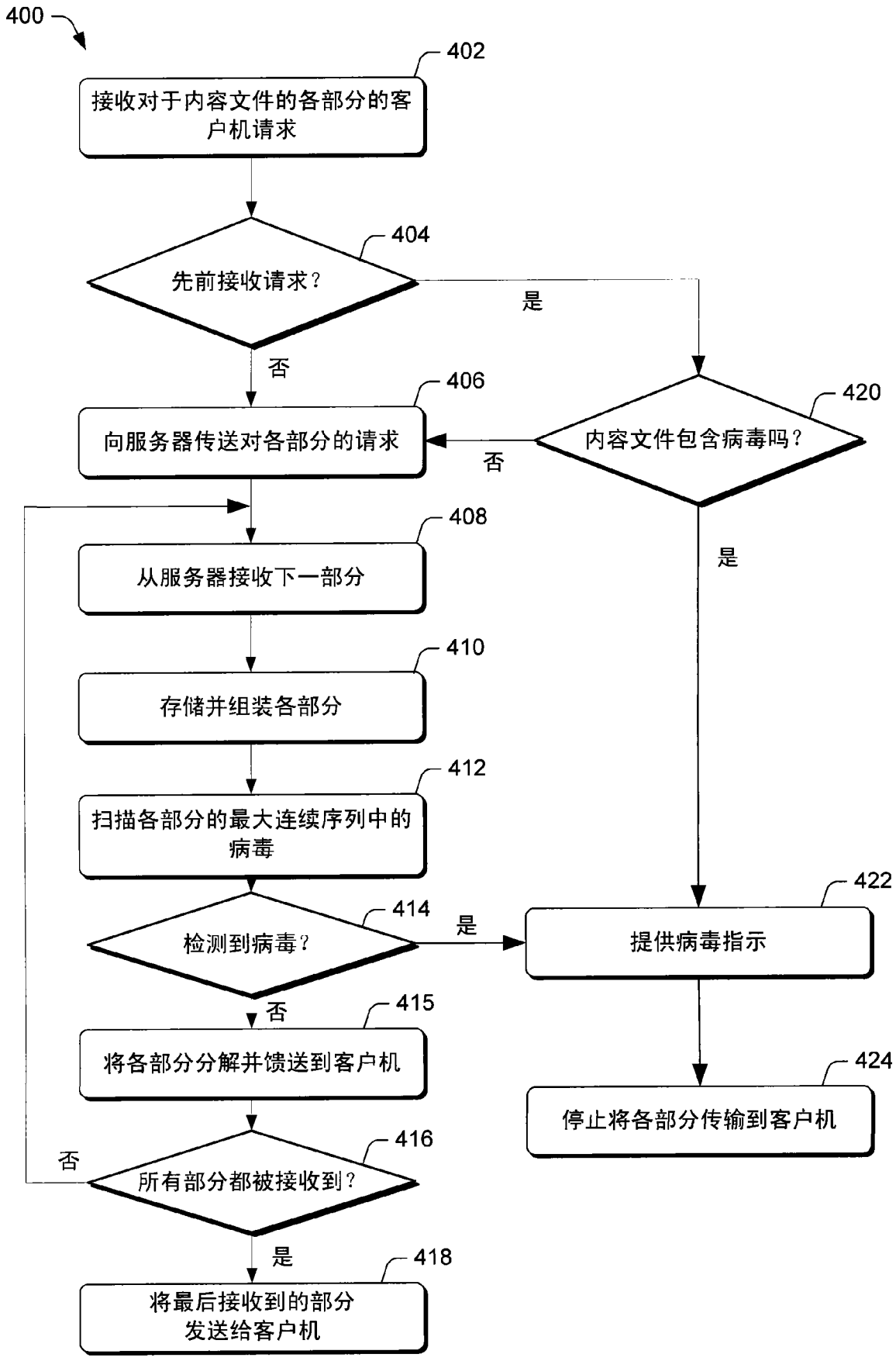

400
402
接收对于内容文件的各部分的客户机请求
404
先前接收请求？
是
否
406
向服务器传送对各部分的请求
420
内容文件包含病毒吗？
否
是
408
从服务器接收下一部分
410
存储并组装各部分
412
扫描各部分的最大连续序列中的病毒
414
检测到病毒？
是
422
提供病毒指示
否
415
将各部分分解并馈送到客户机
424
停止将各部分传输到客户机
416
所有部分都被接收到？
否
是
418
将最后接收到的部分发送给客户机

图 4