(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 103003790 A
(43)申请公布日 2013.03.27

(21)申请号 201180024678.8
(22)申请日 2011.04.11
(30)优先权数据
12/781,432 2010.05.17 US
(85)PCT申请进入国家阶段日
2012.11.19
(86)PCT申请的申请数据
PCT/US2011/031937 2011.04.11
(87)PCT申请的公布数据
WO2011/146172 EN 2011.11.24
(71)申请人 国际索拉温兹公司
地址 美国德克萨斯州
(72)发明人 D·R·莫尔特比 J·道里斯
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民
(51)Int.Cl.
G06F 7/00(2006.01)

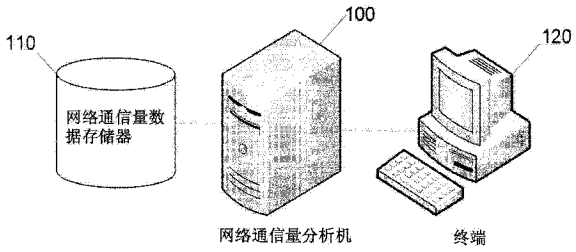
权利要求书 2 页 说明书 5 页 附图 5 页

(54)发明名称

渐进的制图

(57)摘要

本发明实施例包括用于逐步绘制网络通信流数据的图的装置、方法和计算机程序。在一个实施例中，所述方法包括，在网络通信量分析机接收对于某时期内的网络通信流数据的查询。所述方法还包括修改该查询，从而产生多于一个子查询，每个子查询基于所述某时期内的不同时段；执行至少一个子查询；以及随着完成每个子查询而递增地输出每个执行过的所述子查询的结果。



CN 103003790 A

1. 一种方法，其包括：

在网络通信量分析机接收对于某时期内的网络通信流数据的查询；

修改所述查询以产生多于一个子查询，其中每个所述子查询基于所述某时期内的不同时段；

执行至少一个所述子查询；以及

随着完成每个所述子查询，递增地输出每个所述执行过的子查询的结果。

2. 根据权利要求 1 所述的方法，其中递增地输出所述结果包括当完成一个子查询时立即输出所述子查询的所述结果。

3. 根据权利要求 1 所述的方法，其中递增地输出所述结果包括生成示出所述子查询的增量结果的图形图。

4. 根据权利要求 1 所述的方法，还包括迭代地进行递增输出直至完成所有的所述子查询。

5. 根据权利要求 1 所述的方法，其中所述查询涉及来自至少一个网络实体的通信流数据。

6. 根据权利要求 1 所述的方法，还包括扫描用于报告的多个网络实体，并且在所述多个网络实体中选择进行报告的至少一个传送最大数据量的网络实体。

7. 一种装置，其包括：

接收器，所述接收器被配置用于接收对于某时期内的网络通信流数据的查询；以及

处理器，所述处理器被配置用于控制所述装置用以

修改所述查询以产生多于一个子查询，其中每个所述子查询基于所述某时期内的不同时段；

执行至少一个所述子查询；以及

随着完成所述子查询而递增地输出所述子查询的结果。

8. 根据权利要求 7 所述的装置，其中所述处理器还被配置用于控制所述装置在当完成一个子查询时立即输出所述子查询的所述结果。

9. 根据权利要求 7 所述的装置，其中所述处理器还被配置用于控制所述装置去生成示出所述子查询的增量结果的图形图。

10. 根据权利要求 7 所述的装置，其中所述处理器还被配置用于控制所述装置去迭代地执行递增输出直至所有的所述子查询被完成。

11. 根据权利要求 7 所述的装置，其中所述查询涉及来自至少一个网络实体的通信流数据。

12. 根据权利要求 7 所述的装置，其中所述处理器还被配置用于控制所述装置用以

扫描要报告的多个网络实体，以及

在所述多个网络实体中选择至少一个传送最大数据量的网络实体进行报告。

13. 一种计算机程序，其被包含在计算机可读介质上，所述计算机程序被配置用于控制处理器去执行操作，所述操作包括：

在网络通信量分析机接收对于某时期内的网络通信流数据的查询；

修改所述查询用以产生多于一个子查询，每个所述子查询基于所述某时期内的不同时段；

执行至少一个所述子查询；以及

随着完成每个所述子查询，递增地输出每个执行过的所述子查询的结果。

14. 根据权利要求 13 所述的计算机程序，其中递增地输出所述结果包括当一个子查询被完成时立即输出所述子查询的所述结果。

15. 根据权利要求 13 所述的计算机程序，其中递增地输出所述结果包括生成示出所述子查询的增量结果的图形图。

16. 根据权利要求 13 所述的计算机程序，还包括迭代地进行递增输出直至完成所有的所述子查询。

17. 根据权利要求 13 所述的计算机程序，其中所述查询涉及来自至少一个网络实体的通信流数据。

18. 根据权利要求 13 所述的计算机程序，还包括扫描要报告的多个网络实体，并且在所述多个所述网络实体中选择至少一个传送最大数据量的网络实体进行报告。

19. 一种装置，其包括：

接收构件，用于在网络通信量分析机接收对于某时期内的网络通信流数据的查询；

修改构件，用于修改所述查询用以产生多于一个子查询，每个所述子查询具有基于所述某时期内的不同时段；

执行构件，用于执行至少一个所述子查询；以及

输出构件，用于随着每个所述子查询被完成，递增地输出每个所述执行过的子查询的结果。

渐进的制图

技术领域

[0001] 本发明实施例一般涉及网络通信量分析和报告。具体来说，本发明的示例涉及用于报告网络通信流数据的方法、系统和计算机程序。

背景技术

[0002] 由于一些原因，其中包括分析网络上新应用的影响，对网络缺陷点进行故障检测，探测大流量用户的带宽以及保护网络，网络管理员关注网络通信流数据。思科公司(Cisco Systems®)开发的 NetFlow 是有关通信流数据的主要协议。还有一些其他种类的流协议，例如，sFlow、IPFIX、Jflow、NetStream 和 Cflowd。所有这些协议支持与 NetFlow 相似的流，并且这些流包括相似的信息类型，例如，源网际协议(IP)地址、目的地 IP 地址、源端口、目的地端口、IP 协议、进路接口、IP 服务类型、开始和结束时间、字节数和下一跳。

[0003] 由于网络变得更加庞大和复杂，分析和报告通信流数据的系统必须更加有效地处理关于网络通信生成的越来越多的信息量。从许多的网络设备聚集数据会造成包含数亿条目或数亿流量的数据集。此外，运行并报告对于大规模的数据集的查询会使存储系统或者数据库负担加重。解决这种数据过量问题的传统方法是提高作为存储系统的主机的硬件的数量或质量。

发明内容

[0004] 本发明的一个实施例涉及方法。所述方法包括在网络通信量分析机接收对于某时期内的网络通信流数据的查询，并且修改该查询从而产生多于一个子查询，其中每个子查询基于所述某时期内的不同时段。所述方法还包括执行至少一个子查询，并且随着完成每个子查询而递增(或渐进地)输出每个所述执行过的子查询的结果。

[0005] 另一个实施例涉及装置。所述装置包括接收器和处理器，接收器被配置用于接收对于某时期内的网络通信流数据的查询。处理器被配置用于控制该装置以修改该查询从而产生多于一个子查询，其中每个子查询基于所述某时期内的不同时段；执行至少一个子查询；以及随着完成子查询而递增地输出所述子查询的结果。

[0006] 另一个实施例涉及包含在计算机可读介质上的计算机程序。所述计算机程序被配置用于控制处理器去执行操作，所述操作包括在网络通信量分析机接收对于某时期内的网络通信流数据的查询；以及修改该查询从而产生多于一个子查询，其中每个子查询基于该某时期内的不同时段。所述操作进一步包括执行至少一个子查询，以及随着完成每个子查询而递增输出每个所述执行过的子查询的结果。

[0007] 另一个实施例涉及装置。所述装置包括接收构件和修改构件；接收构件用于在网络通信量分析机接收对于某时期内的网络通信流数据的查询，修改构件用于修改该查询从而产生多于一个子查询，其中每个子查询基于该某时期内的不同时段。所述装置还包括执行构件和输出构件；执行构件用于执行至少一个子查询，输出构件用于随着完成每个子查询而递增输出所述每个执行过的子查询的结果。

附图说明

[0008] 为了正确的理解本发明，应参考附图，其中：

[0009] 图 1 根据一个实施例示出系统；

[0010] 图 2 示出由本发明例示性的实施例产生的初始图；

[0011] 图 3 根据本发明实施例示出另一图；

[0012] 图 4 根据一个实施例还示出另一图；

[0013] 图 5 依据实施例示出完整图；

[0014] 图 6 根据一个实施例示出系统；以及

[0015] 图 7 根据一个实施例示出例示性的方法。

具体实施方式

[0016] 本发明实施例包括用于报告网络通信流数据的方法、装置、系统和 / 或计算机程序。响应性是报告网络通信量的重要方面。需要报告的用户通常在请求这些报告时有紧迫的目地。在网络管理领域尤其如此。网络管理员需要快速评估网络状态从而对可能存在的任何问题进行故障诊断。网络管理员监控的一个重要的方面是网络通信量。网络通信量数据经常被封装在流中。复杂的网络产生大量流。当有巨大量的流时，生成关于网络通信量的报告是困难的。完成单个查询要耗费数分钟或者甚至数小时。如果商业关键业务没有正常执行，那么对于组织来说这种时间损失的代价昂贵。本发明实施例通过快速地向管理员(用户)返回最重要的数据解决这些问题。根据一个实施例，最重要的数据可理解为业务、协议或者消耗最多资源数量的实体。

[0017] 因此，本发明的实施例包括系统，该系统通过随着执行已分段的查询并且返回结果而逐步地发送图，从而提高网络通信流报告的响应性。在一个实施例里，网络通信量分析机扫描要报告的适合网络实体。在一些实施例中，网络通信量分析机将选择消耗网络带宽量最多的网络实体进行报告。然后，网络通信量分析机可以从每个实体选择最近时期的数据。网络通信量分析机可以生成并且发送表示第一时期的图。然后，网络通信量分析机对每个下一最近的时期重复该过程。结果，网络通信流报告的初始响应时间被显著提高。

[0018] 图 1 根据一个实施例示出例示性的系统。所述系统包括网络通信量分析机 100、网络通信量数据存储器 110 和终端 120。网络通信量数据存储器 110 存储网络通信流数据。网络通信量数据存储器 110 可以是数据库或者任何其他适当的存储设备。用户，例如网络管理员，可以利用终端 120 向网络通信量分析机 100 发送请求或者查询。例如，该请求可以是对关于涉及网络中一个或者更多个网络实体的网络通信流数据的报告的请求。在一些实施例中，该请求可以指示网络管理员关注的若干网络实体和某个时期。

[0019] 网络通信量分析机 100 从终端 120 接收请求并且扫描要报告的适合网络实体。例如，如果用户请求关于在昨天一天内在网络上产生的通信量为前五名的网络实体的报告，则网络通信量分析机 100 将创建查询去获取前五个的结果，该结果根据传送的数据总量排序。然后，网络通信量分析机 100 向终端 120 发送初始响应，该初始响应指示出网络上正在产生最大通信量的网络实体。这是向关注于发现网络上的问题的用户发送及时反馈的最快速的方式。

[0020] 接下来，网络通信量分析机 100 递增地生成表示请求的时期的图。例如，继续上面的例子，网络通信量分析机 100 可以通过创建查询开始，以获取之前标识的前五名通信量产生者在最近的时间段传送的数据总量，该查询被发送到网络通信量数据存储器 110。该时间段可以是一小时、两小时或者任何其他有用的时间段。在一个实施例中，该时间段为用户请求里包含的时期的某个部分。因此，在一些实施例中，网络通信量分析机 100 可以修改请求从而产生部分请求或者子请求，该部分请求或者子请求覆盖的时间段在请求的时期之内。以这种方式，网络通信量分析机 100 可以更快更有效地产生针对请求的增量结果，下面将对此进行进一步的详细讨论。

[0021] 响应从网络通信量分析机 100 接收到的查询，网络通信量数据存储器 110 依据该查询提供的参数来获取数据总量，并且向网络通信量分析机 100 返回获取到的信息。当网络通信量数据存储器 110 返回查询结果时，网络通信量分析机 100 生成图的图像或者数据表示并且向用户发送初步结果，该图示出查询结果。图 2 示出初始的增量时间段的例示性增量图。图更新可以被绘制或生成在终端 120（客户端）或网络通信量分析机 100（服务器端）。在一个实施例中，传递初始增量图或结果的速度是传递完整图的两倍或者更快。

[0022] 网络通信量分析机将继续查询网络通信量数据存储器 110 并且产生附加的增量结果，如图 3 和 4 所示，这些增量结果被合并在图中。具体地，根据一个实施例，对每个之后的时间段重复该过程，迭代地向用户返回更完整的图，直到完成如图 5 中所示的图。

[0023] 图 6 示出系统 10 的框图，该系统可以实现本发明的一个实施例。系统 10 包括总线 12 或者其他通信机构，用于在系统 10 的组件之间通信信息。系统 10 也包括处理器 22，该处理器连接到总线 12 上用于处理信息和执行指令或者操作。处理器 22 可以是任何类型的通用处理器或者特殊用途的处理器。系统 10 还包括存储器 14，其用以存储信息和要被处理器 22 执行的指令。存储器 14 可以由随机存取存储器（“RAM”）、只读存储器（“ROM”）、诸如磁盘或者光盘的静态存储器或者任何其他类型的机器或计算机可读介质的任意组合构成。系统 10 还包括提供网络接入的通信设备 20，例如，网络接口卡或者其他通信接口。因此，用户可以直接连接到系统 10，或者通过网络或者任何其他的方法远程地连接到系统 10。

[0024] 计算机可读介质可以是处理器 22 可访问的任何可用的介质，并且包括易失性介质和非易失性介质、可移动介质和不可移动介质和通信介质。通信介质可以包括计算机可读的指令、数据结构、程序模块或者调制数据信号（例如，载波或其他传送机制）里的其他数据，并且可以包括任何信息传递介质。

[0025] 为了向用户显示信息，例如网络通信量信息，处理器 22 还可以通过总线 12 连接到显示器 24（例如，终端 120 的液晶显示器）。为了使用户能够与系统 10 交互，键盘 26 和光标控制设备 28（例如，计算机鼠标）还可以连接到总线 12。处理器 22 和存储器 14 也可以通过总线 12 连接到数据库系统 30，因此，其能够访问并且获取存储在数据库系统 30 里的信息。在一个实施例中，数据库系统 30 为图 1 中示出的网络通信量数据存储器 110。虽然在图 6 里仅示出一个数据库，但依据某些实施例可以使用任何数量的数据库。

[0026] 在一个实施例，存储器 14 存储软件模块，这些软件模块在被处理器 22 执行时提供功能。这些软件模块可以包括操作系统 15，其为系统 10 提供操作系统功能。存储器也可以存储网络通信量分析机模块 16，该模块通过提高网络通信流报告的响应性提供增强的网络通信量分析解决方案。系统 10 也可以包括提供附加功能的一个或者更多个其他功能模块

18。

[0027] 数据库系统 30 可以包括数据库服务器和任何类型的数据库，例如，关系数据库或者平面文件数据库。数据库系统 30 可以存储关于网络中每个实体的网络通信流的数据，和 / 或任何与系统 10 相关的或与系统 10 相关联模块以及组件相关的数据。

[0028] 在某些实施例，处理器 22、网络通信量分析机模块 16 和其他功能模块 18 可以被实现为分离的物理单元和逻辑单元或者实现在单个物理单元和逻辑单元里。此外，在一些实施例，处理器 22、网络通信量分析机模块 16 和其他功能模块 18 可以被实现在硬件里，或者实现为硬件和软件的任何合适组合。

[0029] 此外，在一些实施例，系统 10 可以包括接收器，该接收器被配置用于接收对于某时期里的网络通信流数据的查询。一旦接收到此种查询，处理器 22 被配置用于控制系统 10 以将查询分段为子查询，每个子查询基于该某时期内的不同时段，并且，处理器 22 被配置用于控制系统 10 执行至少一个子查询。一旦执行过子查询并返回其结果，处理器 22 控制系统 10 以在完成所述子查询时，立即递增输出所述子查询的结果。根据一个实施例，处理器 22 还被配置用于控制系统 10 生成示出子查询的增量结果的图形图。系统 10 被配置用于迭代地执行子查询，并且迭代地进行递增输出直到完成所有的子查询，这样该图形图示出了查询的完整结果。

[0030] 如上所述，根据一个实施例，系统 10 接收到的查询涉及来自至少一个网络实体的通信流数据。在一些实施例中，处理器 22 还可以被配置用于控制系统 10 去扫描要报告的多个网络实体，并且在多个网络实体中选择至少一个传递最大数据量的网络实体进行报告。根据某些实施例，例如，系统 10 可以在网络里的所有网络实体中选择五个传递最大数据量的网络实体。

[0031] 本发明的实施例也包括逐步地（或渐进地）绘制网络通信流信息图的方法，如图 7 所示。所述方法包括在网络通信量分析机接收 700 对于某时期内的网络通信流数据的查询。在 710，所述方法包括修改该查询，用以产生多于一个子查询，每个子查询基于该某时期内的不同时段。在 720，所述方法包括执行至少一个子查询。在 730，所述方法包括随着完成每个子查询而递增输出每个已执行子查询的结果。在 740，所述方法包括迭代地进行递增输出直到完成所有的子查询。

[0032] 在一个实施例，递增地输出结果包括当完成子查询时立即输出该子查询的结果。此外，在一些实施例中，递增地输出结果包括生成示出子查询的增量结果的图形图。网络通信量分析机接收到的查询可能涉及来自至少一个网络实体的通信流数据。而且，在一个实施例，方法还包括扫描要报告的多个网络实体，并且在多个网络实体中选择至少一个传递最大数据量的网络实体进行报告。在一些实施例中，网络通信量分析机可以选择五个传递最大数据量的网络实体进行报告。

[0033] 上述计算机可读介质可以至少部分由传输线、光盘、数字视频盘、磁带、伯努利驱动、磁盘、全息盘或者全息带、闪速存储器、磁阻存储器、集成电路或者其他数字处理装置存储器设备具体化。

[0034] 在一个或者更多个实施例中可以以任何合适的方式组合本发明的所述特性、优点和特征。本领域的技术人员可以认识到，可以实践本发明，而不具备特定实施例的一个或者更多具体的特性或者优点。在其他情况下，某些实施例中可以识别不是存在于本发明的所

有实施例中的附加特性和优点。

[0035] 因此，本发明的普通技术人员容易认识到，上述发明可以以不同顺序的步骤实施，或者以不同于本发明公开的配置的硬件组件实施。并且本发明的实施例可以以任意合适的方式组合。此外，尽管以优选实施例来描述本发明，但是显而易见的，对本领域的技术人员而言，某些修改、变化和替代构造是明显的，同时保持在本发明的精神和范围内。因此，应参考所附的权利要求来确定本发明的边界。

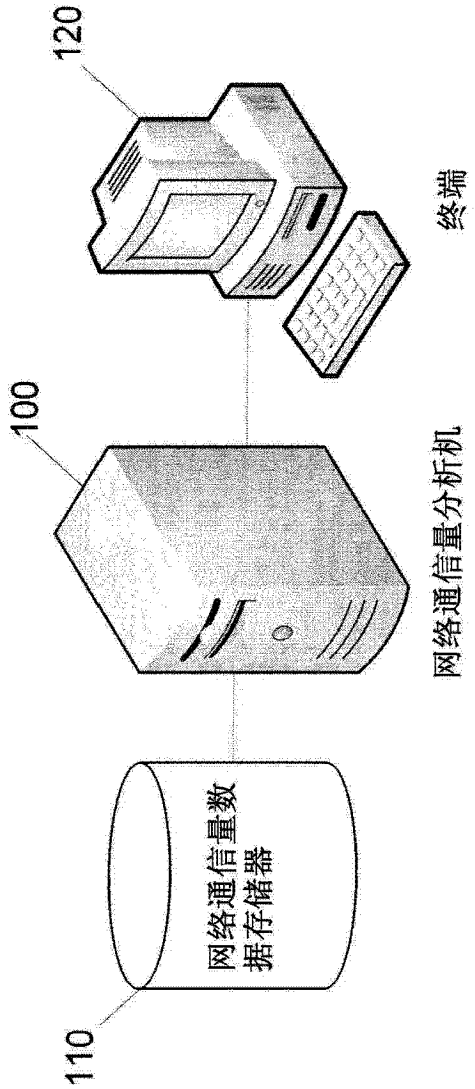


图 1

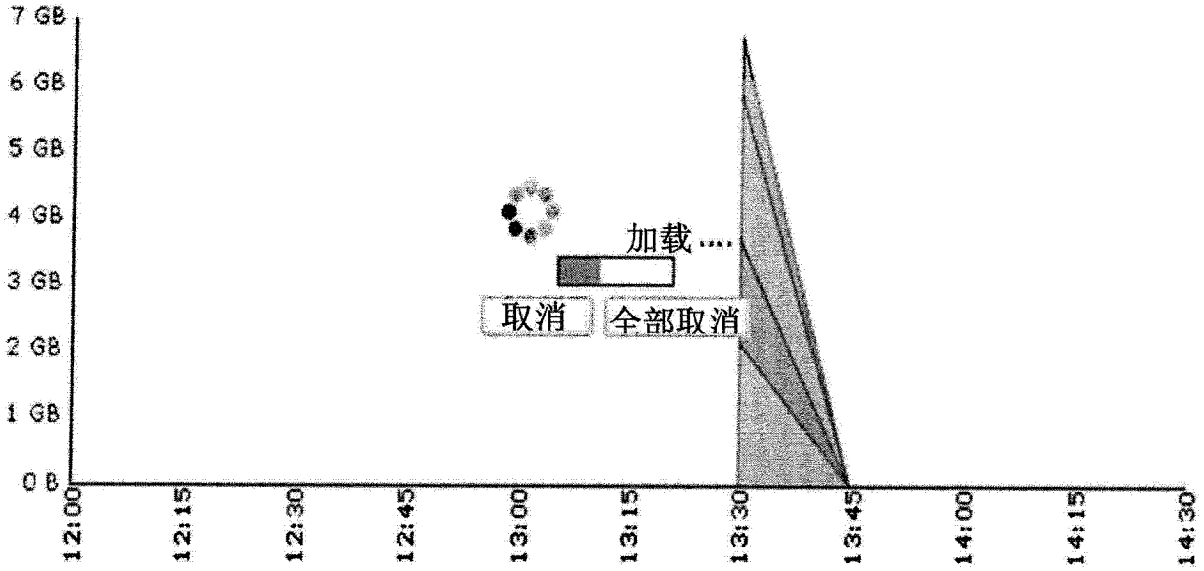

7 GB
6 GB
5 GB
4 GB
3 GB
2 GB
1 GB
0 B
加载....
取消
全部取消
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30

图 2

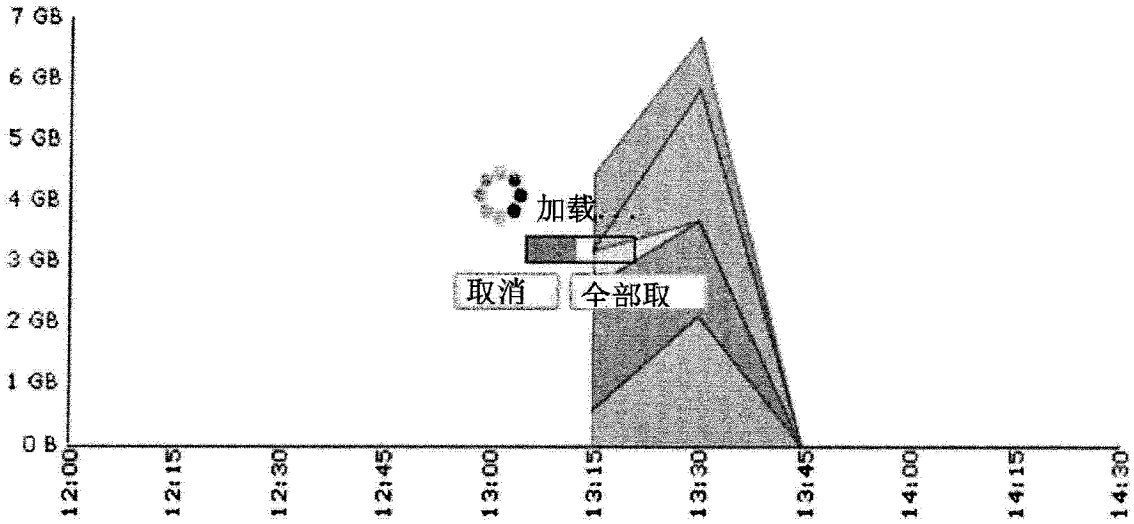

7 GB
6 GB
5 GB
4 GB
3 GB
2 GB
1 GB
0 B
加载...
取消
全部取
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30

图 3

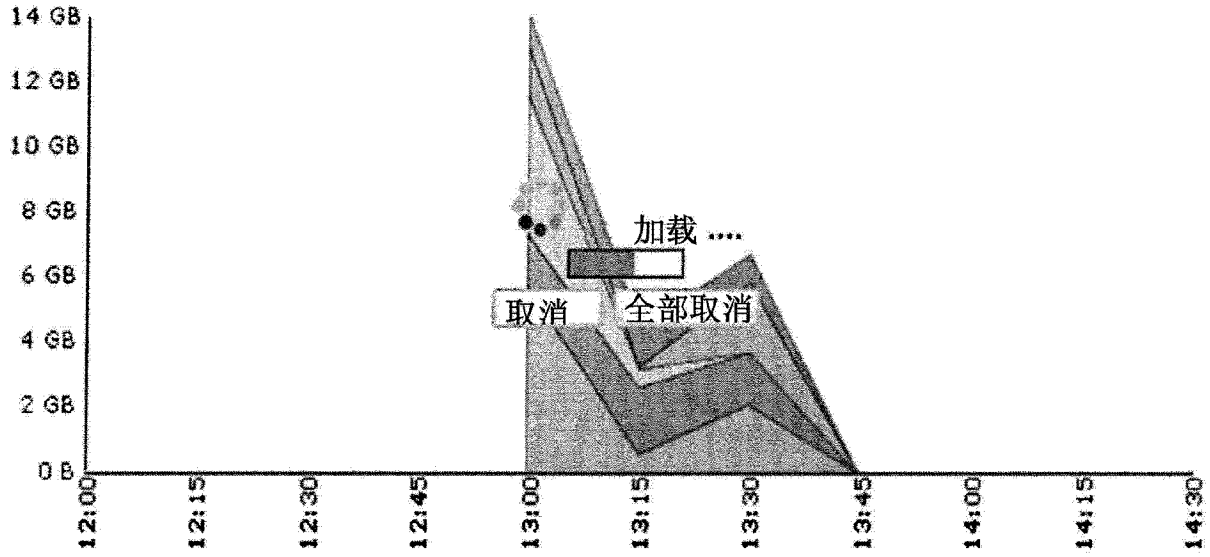

14 GB
12 GB
10 GB
8 GB
6 GB
4 GB
2 GB
0 B
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30
加载 ....
取消
全部取消

图 4

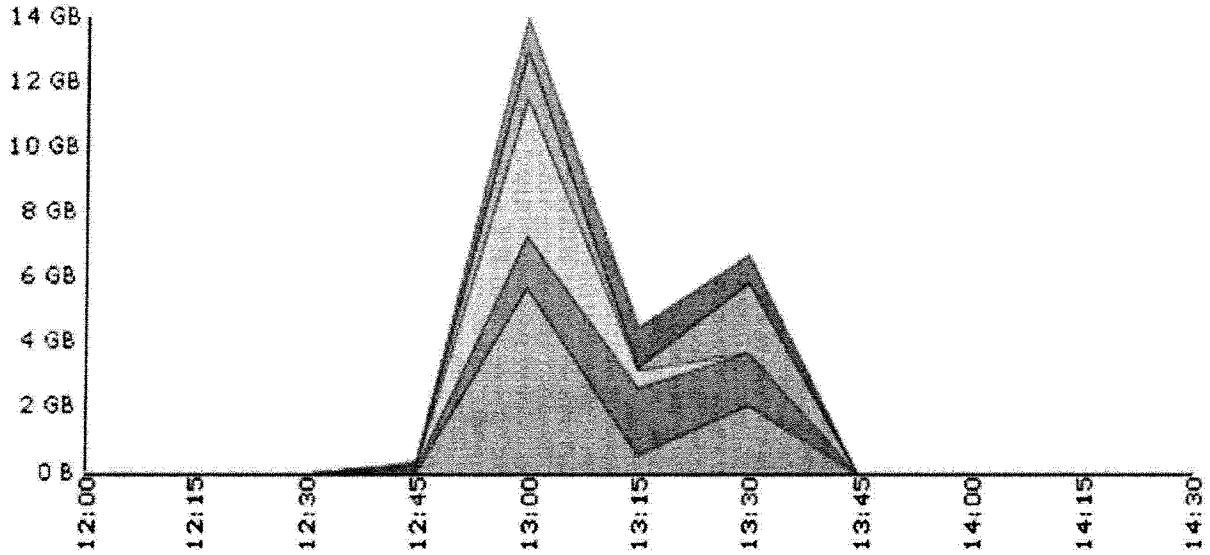

14 GB
12 GB
10 GB
8 GB
6 GB
4 GB
2 GB
0 B
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30

图 5

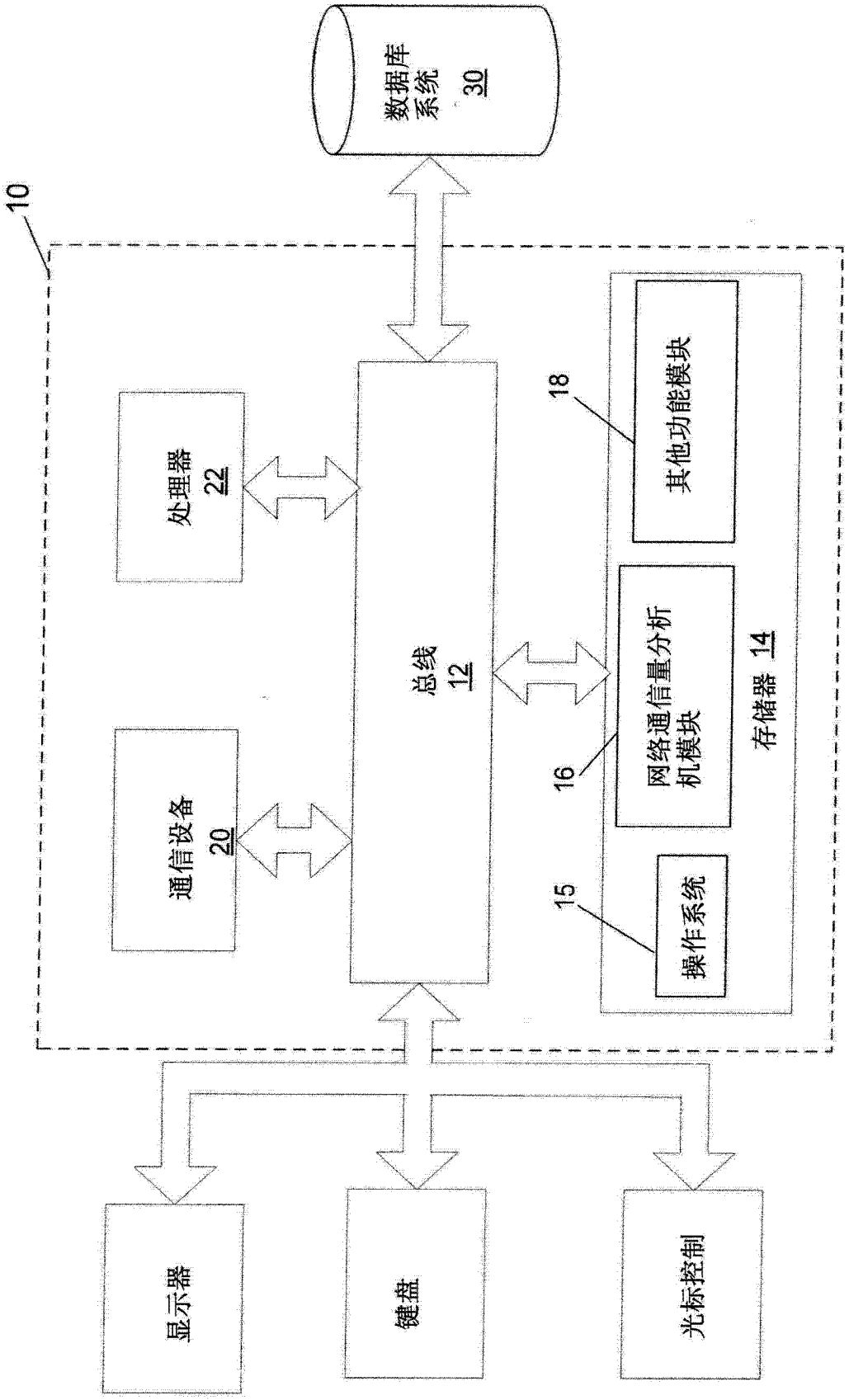

数据库系统 30
10
处理器 22
总线 12
通信设备 20
18
其他功能模块
网络通信量分析机模块
16
存储器 14
15
操作系统
显示器
键盘
光标控制

图 6

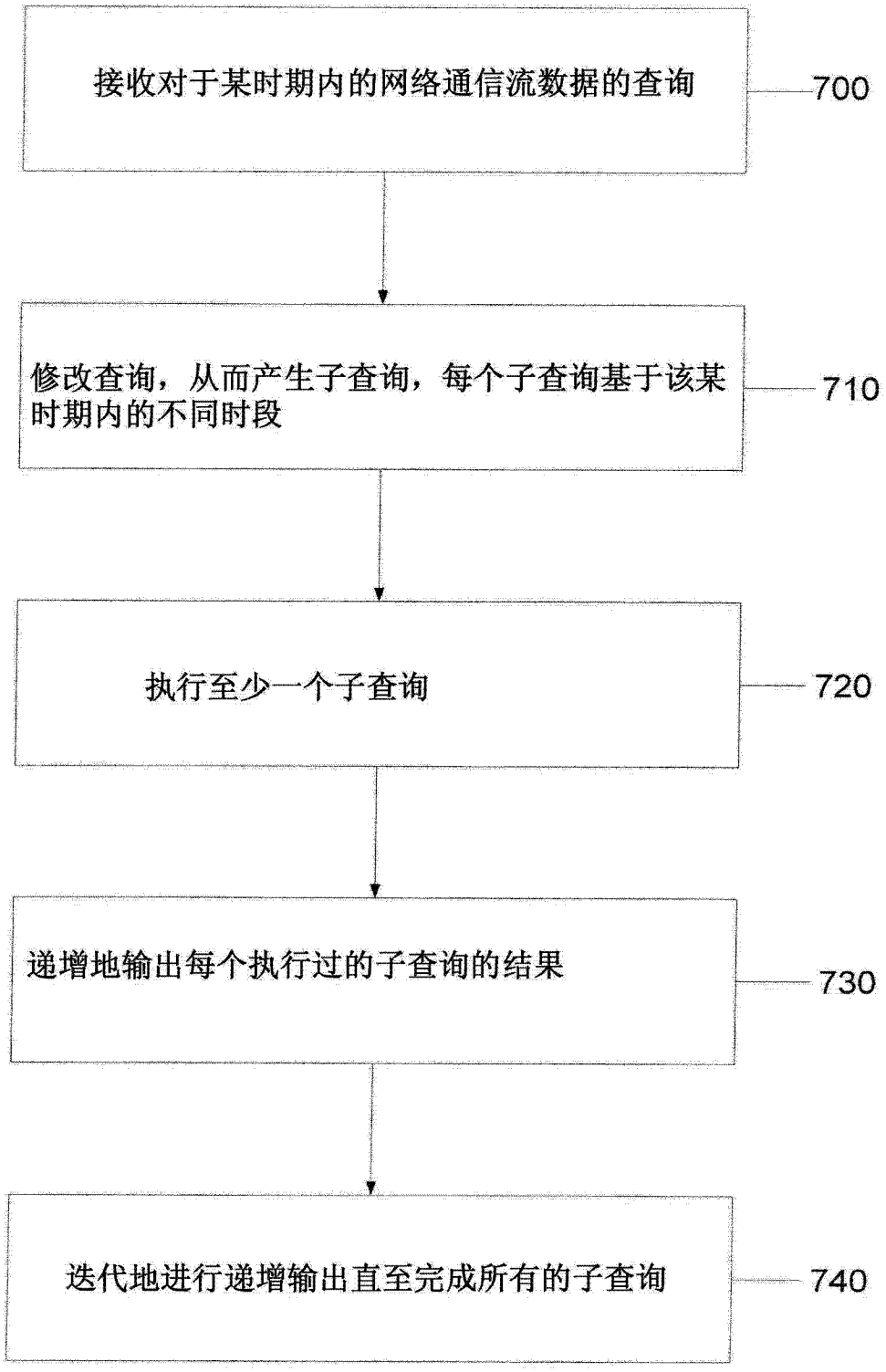

接收对于某时期内的网络通信流数据的查询
700
修改查询，从而产生子查询，每个子查询基于该某时期内的不同时段
710
执行至少一个子查询
720
递增地输出每个执行过的子查询的结果
730
迭代地进行递增输出直至完成所有的子查询
740

图 7