(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 106817340 B
(45)授权公告日 2020.05.08

(21)申请号 201510846433.3

(22)申请日 2015.11.27

(65)同一申请的已公布的文献号
申请公布号 CN 106817340 A

(43)申请公布日 2017.06.09

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 屠一凡 乔会来 贾炯

(74)专利代理机构 北京展翅星辰知识产权代理有限公司 11693
代理人 王文生

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 104426906 A,2015.03.18,全文.
CN 102769607 A,2012.11.07,全文.
US 2015106935 A1,2015.04.16,全文.
US 2012324573 A1,2012.12.20,全文.

审查员 陈佳

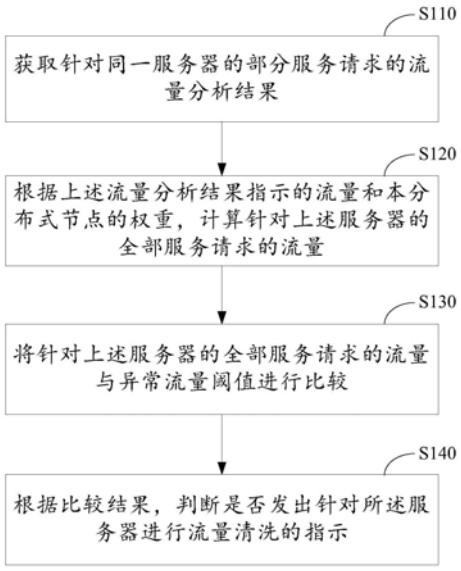
权利要求书4页 说明书10页 附图4页

(54)发明名称

预警决策的方法、节点及子系统

(57)摘要

本申请提供了一种预警决策的方法、节点及系统。该方法包括以下步骤:获取针对同一服务器的部分服务请求的流量分析结果;根据所述流量分析结果指示的流量和本分布式节点的权重,计算针对所述服务器的全部服务请求的流量,所述权重是本分布式节点获取的流量分析结果指示的流量占针对所述服务器的全部服务请求的流量的权重;将针对所述服务器的全部服务请求的流量与异常流量阈值进行比较;根据比较结果,判断是否发出针对所述服务器进行后续处理的指示。根据本申请的方案,有效提高了DDoS预警系统的可靠性和安全性。



CN 106817340 B

1.一种预警决策的方法,其特征在于,应用于进行预警决策的各个分布式节点,该方法包括以下步骤:

获取针对同一服务器的部分服务请求的流量分析结果;

将所述流量分析结果指示的流量与异常流量阈值进行第一次比较;

如果第一次比较结果符合预定条件,发出针对所述服务器的后续处理的指示,所述预定条件为进行比较的流量大于所述异常流量阈值,或者所述预定条件为进行比较的流量不小于所述异常流量阈值;

当所述第一次比较结果不符合所述预定条件时,根据所述流量分析结果指示的流量和本分布式节点的权重,计算针对所述服务器的全部服务请求的流量,所述权重是本分布式节点获取的流量分析结果指示的流量占针对所述服务器的全部服务请求的流量的权重;

将针对所述服务器的全部服务请求的流量与所述异常流量阈值进行第二次比较;

根据第二次比较结果,判断是否发出针对所述服务器进行后续处理的指示。

2.根据权利要求1所述的方法,其特征在于,根据第一次或第二次比较结果,判断是否发出针对所述服务器进行后续处理的指示,包括:

当第一次或第二次比较结果符合所述预定条件,判断发出针对所述服务器进行后续处理的指示;否则,判断不发出针对所述服务器进行后续处理的指示。

3.根据权利要求1～2任一项所述的方法,其特征在于,该方法还包括:

按照预定的权重调整周期,调整本分布式节点的权重。

4.根据权利要求3所述的方法,其特征在于,所述按照预定的权重调整周期,调整本分布式节点的权重的步骤包括:

在每个权重调整周期,确定进行预警决策的其它分布式节点获取的本权重调整周期的部分时间段内的针对所述服务器的部分服务请求的流量分析结果指示的流量;

在每个所述的权重调整周期,根据进行预警决策的全部分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量,计算所述部分时间段内针对所述服务器的全部服务请求的流量;

在每个所述的权重调整周期,至少根据本分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量占所述部分时间段内针对所述服务器的全部服务请求的流量的权重,调整本分布式节点在下一个权重调整周期的权重。

5.根据权利要求1～2任一项所述的方法,其特征在于,所述获取针对同一服务器的部分服务请求的流量分析结果的步骤包括:

从负载均衡设备获取针对同一服务器的部分服务请求的流量分析结果。

6.根据权利要求1～2任一项所述的方法,其特征在于,该方法还包括:

从负载均衡设备获取针对所述服务器的部分服务请求;

所述获取针对同一服务器的部分服务请求的流量分析结果的步骤包括:

对所述部分服务请求进行流量分析,得到针对所述服务器的部分服务请求的流量分析结果。

7.根据权利要求2所述的方法,其特征在于,所述根据所述流量分析结果指示的流量和本分布式节点的权重,计算针对所述服务器的全部服务请求的流量的步骤包括:根据所述流量分析结果指示的流量大小和本分布式节点的权重,计算针对所述服务器的全部服务请

求的流量大小；

所述将针对所述服务器的全部服务请求的流量与异常流量阈值进行第二次比较的步骤包括：将针对所述服务器的全部服务请求的流量大小与异常流量阈值进行比较；

将针对所述服务器的部分服务请求的流量分析结果指示的流量与所述异常流量阈值进行第一次比较的步骤包括：将针对所述服务器的部分服务请求的流量分析结果指示的流量大小与所述异常流量阈值进行比较。

8.根据权利要求2所述的方法，其特征在于，将针对所述服务器的部分服务请求的流量分析结果指示的流量与所述异常流量阈值进行第一次比较的步骤包括：将针对所述服务器的部分服务请求的流量分析结果指示的各流量组成成分对应的流量大小分别与各流量组成成分对应的异常流量阈值进行比较；

所述根据所述流量分析结果指示的流量和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量的步骤包括：根据所述流量分析结果指示的目标流量组成成分对应的流量大小和目标流量组成成分对应的本分布式节点的权重，分别计算针对所述服务器的全部服务请求的目标流量组成成分的流量大小，所述目标流量组成成分为不符合预定条件的流量组成成分；

所述将针对所述服务器的全部服务请求的流量与异常流量阈值进行第二次比较的步骤包括：将针对所述服务器的全部服务请求的目标流量组成成分的流量大小分别与目标流量组成成分对应的异常流量阈值进行比较。

9.根据权利要求8所述的方法，其特征在于，所述当第一次或第二次比较结果符合预定条件，判断发出针对所述服务器进行后续处理的指示的步骤包括：

针对第一次或第二次比较结果符合预定条件的流量组成成分，发出针对所述服务器进行该流量组成成分的后续处理的指示。

10.根据权利要求1～2、9中的任一项所述的方法，其特征在于，所述后续处理包括：流量清洗，流量黑洞，或流量分析。

11.一种预警决策节点，其特征在于，该节点为分布式节点，该节点包括以下模块：

流量分析结果获取模块，用于获取针对同一服务器的部分服务请求的流量分析结果；

完整流量估计模块，用于根据所述流量分析结果指示的流量和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量，所述权重是本分布式节点获取的流量分析结果指示的流量占所述服务器的全部服务请求的流量的权重；

阈值比较模块，用于将针对所述服务器的部分或全部服务请求的流量与异常流量阈值进行比较，包括：

将针对所述服务器的部分服务请求的流量分析结果指示的流量与所述异常流量阈值进行第一次比较；

当所述第一次比较结果不符合预定条件时，将针对所述服务器的全部服务请求的流量与所述异常流量阈值进行第二次比较，所述预定条件为进行比较的流量大于所述异常流量阈值，或者所述预定条件为进行比较的流量不小于所述异常流量阈值；

判断控制模块，用于根据第一次或第二次比较结果，判断是否发出针对所述服务器进行后续处理的指示。

12.根据权利要求11所述的节点，其特征在于，所述判断控制模块具体用于：

当第一次或第二次比较结果符合所述预定条件，判断发出针对所述服务器进行后续处理的指示；否则，判断不发出针对所述服务器进行后续处理的指示。

13.根据权利要求11～12任一项所述的节点，其特征在于，还包括权重调整模块，用于按照预定的权重调整周期，调整本分布式节点的权重。

14.根据权利要求13所述的节点，其特征在于，所述权重调整模块具体用于：

在每个权重调整周期，确定进行预警决策的其它分布式节点获取的本权重调整周期的部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量；

在每个所述的权重调整周期，根据进行预警决策的全部分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量，计算所述部分时间段内针对所述服务器的全部服务请求的流量；

在每个所述的权重调整周期，至少根据本分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量占所述部分时间段内针对所述服务器的全部服务请求的流量的权重，调整本分布式节点在下一个权重调整周期的权重。

15.根据权利要求11～12任一项所述的节点，其特征在于，所述流量分析结果获取模块具体用于：

从负载均衡设备获取针对同一服务器的部分服务请求的流量分析结果。

16.根据权利要求11～12任一项所述的节点，其特征在于，该节点还包括服务请求获取模块，用于：从负载均衡设备获取针对所述服务器的部分服务请求；

所述流量分析结果获取模块具体用于：对所述部分服务请求进行流量分析，得到针对所述服务器的部分服务请求的流量分析结果。

17.根据权利要求11所述的节点，其特征在于，所述完整流量估计模块具体用于：根据所述流量分析结果指示的流量大小和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量大小；

所述阈值比较模块具体用于：将针对所述服务器的部分服务请求的流量分析结果指示的流量大小与所述异常流量阈值进行第一次比较；以及在第一次比较结果不符合所述预定条件时，将针对所述服务器的全部服务请求的流量大小与异常流量阈值进行比较。

18.根据权利要求13所述的节点，其特征在于，所述阈值比较模块具体用于：将针对所述服务器的部分服务请求的流量分析结果指示的各流量组成成分对应的流量大小分别与各流量组成成分对应的异常流量阈值进行比较；以及在流量组成成分对应的流量大小与对应的异常流量阈值的第一次比较结果不符合预定条件时，将针对所述服务器的全部服务请求的目标流量组成成分的流量大小分别与目标流量组成成分对应的异常流量阈值进行第二次比较，所述目标流量组成成分为不符合预定条件的流量组成成分；

所述完整流量估计模块具体用于：根据所述流量分析结果指示的目标流量组成成分对应的流量大小和目标流量组成成分对应的本分布式节点的权重，分别计算针对所述服务器的全部服务请求的目标流量组成成分的流量大小。

19.根据权利要求18所述的节点，其特征在于，所述判断控制模块具体用于：

针对第一次或第二次比较结果符合预定条件的流量组成成分，发出针对所述服务器进行该流量组成成分的后续处理的指示。

20.根据权利要求11～12中的任一项所述的节点，其特征在于，所述后续处理包括：流

量清洗,流量黑洞,或流量分析。

21.一种预警决策系统,其特征在于,包括:

多个如权利要求11～20任一项所述的预警决策节点,多个流量分析节点,第一负载均衡设备和第二负载均衡设备;

所述第一负载均衡设备用于服务请求分流给所述多个流量分析节点;

各个流量分析节点接收服务请求,向第二负载均衡设备上报流量分析结果;

所述第二负载均衡设备将流量分析结果分流给所述多个预警决策节点。

预警决策的方法、节点及子系统

技术领域

[0001] 本申请涉及分布式拒绝服务(Distributed Denial of Service,DDOS)预警技术领域,尤其涉及一种预警决策的方法、节点及子系统。

背景技术

[0002] DDoS攻击通过大量合法的服务请求占用大量网络资源,以达到瘫痪网络的目的。为了应对DDoS攻击,可以通过流量分析识别DDoS攻击,当识别出DDoS攻击时,进行流量清洗,以去掉攻击或异常的服务请求。

[0003] 以图1所示的DDoS预警系统为例。

[0004] 访问机房内服务器的请求数据通过互联网服务提供商(Internet Service Provider,ISP)网络设备到达机房入口网络设备(例如路由器)。并且,从ISP网络设备流入机房入口网络设备的服务请求会通过镜像的方式完整地到达负载均衡设备,再通过负载均衡设备分发给分布式的各个流量分析设备。流量分析设备周期性地对分发到本设备的服务请求进行流量分析,具体是按照IP地址对每个流量分析周期内的服务请求的流量组成成分和流量大小进行统计。然后各个流量分析设备将流量分析结果发送给决策设备,由决策设备根据汇总后的流量分析结果判断各个机房内服务器的流量是否存在异常,如果某个服务器的流量异常,即可能存在DDoS攻击,则通知清洗设备将到达机房入口网络设备的服务请求进行牵引,并在清洗处理完成后再回注到机房入口网络设备,如果服务器不存在流量异常,则不进行处理。

[0005] 基于上述处理过程,在没有DDoS攻击的情况下,服务请求通过机房入口网络设备正常转发给机房内服务器。在有DDoS攻击的情况下,服务请求到达机房入口网络设备后,通过流量牵引将服务请求先转发给流量清洗设备,经过流量清洗设备处理后将服务请求回注给机房入口网络设备,然后再转发给机房内服务器。

[0006] 现有的DDoS预警系统中只有一个决策设备,当这个决策设备由于某种原因(例如出现故障)无法正常工作时,整个机房的网络防御就会失效。因此,现有的DDoS预警系统的可靠性和安全性较差。

发明内容

[0007] 本申请的目的是提供一种预警决策的方法、节点及子系统,以解决现有的DDoS预警系统的可靠性和安全性较差的问题。

[0008] 根据本申请的一个方面,提供一种预警决策的方法,应用于进行预警决策的各个分布式节点中分别实现,该方法包括以下步骤:获取针对同一服务器的部分服务请求的流量分析结果;根据所述流量分析结果指示的流量和本分布式节点的权重,计算针对所述服务器的全部服务请求的流量,所述权重是本分布式节点获取的流量分析结果指示的流量占针对所述服务器的全部服务请求的流量的权重;将针对所述服务器的全部服务请求的流量与异常流量阈值进行比较;根据比较结果,判断是否发出针对所述服务器进行后续处理的

指示。

[0009] 根据本申请的另一方面，还提供了一种预警决策的节点，该节点为分布式节点，该节点包括以下模块：流量分析结果获取模块，用于获取针对同一服务器的部分服务请求的流量分析结果；完整流量估计模块，用于根据所述流量分析结果指示的流量和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量，所述权重是本分布式节点获取的流量分析结果指示的流量占所述服务器的全部服务请求的流量的权重；阈值比较模块，用于将针对所述服务器的全部服务请求的流量与异常流量阈值进行比较；判断控制模块，用于根据比较结果，判断是否发出针对所述服务器进行后续处理的指示。

[0010] 根据本申请的又一方面，还提供了一种预警决策的系统，包括：

[0011] 多个上述预警决策节点，多个流量分析节点，第一负载均衡设备和第二负载均衡设备；

[0012] 所述第一负载均衡设备用于服务请求分流给所述多个流量分析节点；

[0013] 各个流量分析节点接收服务请求，向第二负载均衡设备上报流量分析结果；

[0014] 所述第二负载均衡设备将流量分析结果分流给所述多个预警决策额节点。

[0015] 与现有技术相比，本申请具有以下优点：现有的DDoS预警系统中只有一个决策设备，当这个决策设备由于某种原因无法正常工作时，例如，决策设备出现故障而无法正常工作，或者限于单个决策设备的处理能力，又例如，当需要处理的数据量超出决策设备的处理能力将导致决策设备无法正常工作，整个机房的网络防御就会失效。而本申请实施例提供的技术方案，采用分布式的架构来进行预警决策，即使有进行预警决策的节点无法正常工作，还可以由其他正常工作的节点进行预警决策，从而有效提高了DDoS预警系统的可靠性和安全性。另外，采用分布式的架构进行预警决策，较之单个决策设备的处理能力大大提高。具体地说，每个进行预警决策的分布式节点均有其权重，该权重是本分布式节点获取流量分析结果指示的流量占针对所述服务器的全部服务请求的流量的权重。进一步的，对于每个分布式节点，根据其权重以及针对同一服务器的部分服务请求的流量分析结果指示的流量，就能够估计出针对同一服务器的全部服务请求的流量。进而通过将估计得到的流量与异常流量阈值进行比较，实现预警决策。通过这种方法，使得单个分布式节点在获得的是部分服务请求的流量的前提下，结合其权重即可估计得到全部服务请求的流量，进而实现预警决策。可见，每个上述分布式节点均可以进行预警决策，当有进行预警决策的分布式节点无法正常工作时，仍然可以由其他进行预警决策的分布式节点正常工作，提高了DDoS预警系统的可靠性和安全性，且提高了系统的处理能力。

附图说明

[0016] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0017] 图1为现有的一种DDoS预警系统示意图；

[0018] 图2为本申请一个实施例的方法流程图；

[0019] 图3为本申请另一个实施例的DDoS预警系统示意图；

[0020] 图4为本申请另一个实施例的方法流程图；

[0021] 图5为本申请又一个实施例的节点示意图。

[0022] 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

[0023] 在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作描述成顺序的处理，但是其中的许多操作可以被并行地、并发地或者同时实施。此外，各项操作的顺序可以被重新安排。当其操作完成时所述处理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

[0024] 在上下文中所称“节点”、“负载均衡设备”是一种计算机设备(computing device)，指可以通过运行预定程序或指令来执行数值计算和/或逻辑计算等预定处理过程的智能电子设备，其可以包括处理器与存储器，由处理器执行在存储器中预存的存续指令来执行预定处理过程，或是由ASIC、FPGA、DSP等硬件执行预定处理过程，或是由上述二者组合来实现。

[0025] 需要说明的是，所述计算机设备仅为举例，其他现有的或今后可能出现的计算机设备如可适用于本申请，也应包含在本申请保护范围以内，并以引用方式包含于此。

[0026] 后面所讨论的方法(其中一些通过流程图示出)可以通过硬件、软件、固件、中间件、微代码、硬件描述语言或者其任意组合来实施。当用软件、固件、中间件或微代码来实施时，用以实施必要任务的程序代码或代码段可以被存储在机器或计算机可读介质(比如存储介质)中。(一个或多个)处理器可以实施必要的任务。

[0027] 这里所公开的具体结构和功能细节仅仅是代表性的，并且是用于描述本申请的示例性实施例的目的。但是本申请可以通过许多替换形式来具体实现，并且不应当被解释成仅仅受限于这里所阐述的实施例。

[0028] 应当理解的是，当一个模块被称为“连接”或“耦合”到另一模块时，其可以直接连接或耦合到所述另一模块，或者可以存在中间模块。与此相对，当一个模块被称为“直接连接”或“直接耦合”到另一模块时，则不存在中间单元。应当按照类似的方式来解释被用于描述模块之间的关系的其他词语(例如“处于...之间”相比于“直接处于...之间”，“与...邻近”相比于“与...直接邻近”等等)。

[0029] 这里所使用的术语仅仅是为了描述具体实施例而不意图限制示例性实施例。除非上下文明确地另有所指，否则这里所使用的单数形式“一个”、“一项”还意图包括复数。还应当理解的是，这里所使用的术语“包括”和/或“包含”规定所陈述的特征、整数、步骤、操作、单元和/或组件的存在，而不排除存在或添加一个或更多其他特征、整数、步骤、操作、单元、组件和/或其组合。

[0030] 还应当提到的是，在一些替换实现方式中，所提到的功能/动作可以按照不同于附图中标示的顺序发生。举例来说，取决于所涉及的功能/动作，相继示出的两幅图实际上可以基本上同时执行或者有时可以按照相反的顺序来执行。

[0031] 下面结合附图对本申请作进一步详细描述。

[0032] 图2为本申请一个实施例的预警决策的方法的流程示意图。

[0033] 其中，本实施例的方法主要通过计算机设备来实现，且特别适用于DDoS预警系统中进行预警决策的各个分布式节点。DDoS预警系统中，由流量分析设备根据服务请求中的

IP地址(一个IP地址对应一个服务器),分析每个IP地址的流量组成成分和流量大小。流量分析设备的流量分析结果被分发至进行预警决策的各个分布式节点。即使本领域技术人员能够想到在DDoS预警系统中引入分布式架构进行预警决策,但基于DDoS攻击的特点,需要获知针对一个服务器的全部服务请求的流量,才能够进行预警决策。本申请实施例提供的技术方案,由进行预警决策的各个分布式节点根据其所获得的针对同一服务器的部分服务请求的流量分析结果指示的流量及其权重,计算出针对该服务器的全部服务请求的流量,进而进行预警决策。可见,本申请实施例提供的技术方案,每个分布式节点能够根据碎片化的数据进行预警决策。进而,在有进行预警决策的分布式节点不能正常工作时,仍然可以由其他正常工作的分布式节点进行预警决策,从而提高了DDoS预警系统的可靠性和安全性。另外,多个分布式节点总的处理能力高于单个决策设备的处理能力,因此,本申请实施例提供的技术方案还提高了系统的处理能力。

[0034] 根据本实施例的方法包括步骤S110-S140。

[0035] 在步骤S110中,获取针对同一服务器的部分服务请求的流量分析结果。

[0036] 可选的,步骤S110中,获取当前流量分析周期内针对同一服务器的部分服务请求的流量分析结果。

[0037] 在步骤S120中,根据上述流量分析结果指示的流量和本分布式节点的权重,计算针对上述服务器的全部服务请求的流量。

[0038] 可选的,步骤S120中,根据上述流量分析结果指示的流量和本分布式节点的权重,计算当前流量分析周期内针对上述服务器的全部服务请求的流量。

[0039] 其中,分布式节点的权重是该分布式节点获取的流量分析结果指示的流量占针对服务器的全部服务请求的流量的权重。特别的,分布式节点的权重是至少一个流量分析周期内,该分布式节点获取的流量分析结果指示的流量占针对服务器的全部服务请求的流量的权重。该分布式节点获取的流量分析结果是针对上述服务器的部分服务请求的流量分析结果。

[0040] 在步骤S130中,将针对上述服务器的全部服务请求的流量与异常流量阈值进行比较。

[0041] 可选的,步骤S130中,将当前流量分析周期内针对上述服务器的全部服务请求的流量与异常流量阈值进行比较。

[0042] 本申请实施例中,异常流量阈值是根据实际情况确定的,本申请实施例不对其具体取值进行限定。

[0043] 在步骤S140中,根据比较结果,判断是否发出针对所述服务器进行后续处理的指示。

[0044] 本申请实施例中,不对后续处理进行限定。例如,可以进行流量清洗、流量黑洞、或流量分析等等后续处理。

[0045] 本申请实施例中,步骤S110中获取针对同一服务器的部分服务请求的流量分析结果,是碎片化的数据。为了实现预警决策,在步骤S120中,要根据上述流量分析结果指示的流量和本分布式节点的权重,计算针对上述服务器的全部服务请求的流量。具体的,是在步骤S130中,将估计出的流量与异常流量阈值进行比较,在步骤S140中根据比较结果判断是否发出针对服务器进行后续处理的指示。从而提高了DDoS预警系统的可靠性和安全性,还

提高了系统的处理能力。

[0046] 即使本领域技术人员能够想到在DDoS预警系统中引入分布式架构进行预警决策，但每个分布式节点仅获得部分访问流量的流量分析结果指示的流量，即数据碎片化，如何根据碎片化的数据进行预警决策，是本领域技术人员不付出创造性的劳动而无法获知的

[0047] 本发明实施例中，上述步骤S140具体可以是：当比较结果符合预定条件，判断发出针对所述服务器进行后续处理的指示；否则，判断不发出针对所述服务器进行后续处理的指示；所述预定条件为进行比较的流量大于所述异常流量阈值，或者所述预定条件为进行比较的流量不小于所述异常流量阈值。

[0048] 其中，预定条件为进行比较的流量大于上述异常流量阈值，或者所述预定条件为进行比较的流量不小于上述异常流量阈值。

[0049] 应当指出的是，当比较结果不符合上述预定条件，则表示不存在DDoS攻击，不需要发出针对上述服务器进行后续处理的指示。

[0050] 为了进一步提高处理效率，可选地，在步骤S110之后，将针对上述服务器的部分服务请求的流量分析结果指示的流量与上述异常流量阈值进行比较；如果比较结果符合上述预定条件，发出针对上述服务器的后续处理指示。相应的，上述步骤S120是在针对上述服务器的部分服务请求的流量分析结果指示的流量与上述异常流量阈值进行比较的比较结果不符合上述预定条件时执行的。

[0051] 上述可选的实现方式中，在获取了针对同一服务器的部分服务请求的流量分析结果，首先将该流量分析结果指示的流量与异常流量阈值进行比较，如果比较结果符合预定条件则直接发出针对上述服务器进行后续处理的指示，不再进行后续处理，从而进一步提高了处理效率。

[0052] 例如，异常流量阈值是10MBps，如果获取的当前流量分析周期内针对同一服务器的部分服务请求的流量分析结果指示的流量大小是20MBps，则判断出该流量分析结果指示的流量大于异常流量阈值后，发出针对该服务器进行后续处理的指示；如果获取的当前流量分析周期内针对同一服务器的部分服务请求的流量分析结果指示的流量大小是8MBps，则还进一步需要结合本分布式节点的权重估计出当前流量分析周期内针对该服务器的全部服务请求的流量，进而将估计得到的流量与异常流量阈值进行比较，从而判断是否需要发出针对该服务器进行后续处理的指示。

[0053] 基于上述任意方法实施例，本申请实施例提供的方法可以在流量分析设备中实现，也可以由单独的设备实现。

[0054] 如果由单独的设备实现，由负载均衡设备将流量分析设备得到的流量分析结果分发给进行预警决策的各个分布式节点，相应的，步骤S110中，从负载均衡设备获取针对同一服务器的部分服务请求的流量分析结果。

[0055] 如果由流量分析设备实现，那么，分布式的每个流量分析设备从负载均衡设备获取针对上述服务器的部分服务请求，对这部分服务请求进行流量分析，得到针对上述服务器的部分服务请求的流量分析结果。即步骤S110中，是由本设备进行流量分析从而获取的流量分析结果。

[0056] 基于上述任意方法实施例，可选地，本申请实施例还按照预定的权重调整周期，调整本分布式节点的权重，以保证估计结果的准确性。

[0057] 本申请实施例中，调整本分布式节点的权重的实现方式有多种。

[0058] 可选地，在每个权重调整周期，确定进行预警决策的其它分布式节点获取的当前权重调整周期内的部分时间段(例如一个权重调整周期为60秒，每个流量分析周期为1秒，只取每个权重调整周期内最后两个流量分析周期，即最后2秒)内针对上述服务器的部分服务请求的流量分析结果指示的流量；在每个权重调整周期，根据进行预警决策的全部分布式节点获取的上述部分时间段内针对上述服务器的部分服务请求的流量分析结果指示的流量，计算上述部分时间段内针对所述服务器的全部服务请求的流量；在每个权重调整周期，至少根据本分布式节点获取的上述部分时间段内针对上述服务器的部分服务请求的流量分析结果指示的流量占上述部分时间段内针对上述服务器的全部服务请求的流量的权重，调整本分布式节点在下一个权重调整周期的权重。

[0059] 例如，流量分析周期为1秒，权重调整周期为60秒。则每隔60秒，调整一次权重。

[0060] 其中，既可以与其他分布式节点进行交互，从而确定进行预警决策的其它分布式节点获取的当前权重调整周期内的部分时间段内针对上述服务器的部分服务请求的流量分析结果指示的流量；也可以与负载均衡设备交互，从而确定进行预警决策的其它分布式节点获取的当前权重调整周期内的部分时间段内针对上述服务器的部分服务请求的流量分析结果指示的流量。

[0061] 应当指出的是，为了调整权重，也可以按照预定的权重调整周期，向负载均衡设备请求获取本分布式节点的权重。

[0062] 流量分析结果至少指示了流量大小。可选的，具体指示每个流量组成成分的流量大小。相应的，基于上述任意方法实施例，既可以基于流量的组成成分进行预警决策，也可以仅依据流量大小进行预警决策。

[0063] 如果仅依据流量大小进行预警决策。那么，步骤S120中，具体是根据上述流量分析结果指示的流量大小和本分布式节点的权重，计算针对上述服务器的全部服务请求的流量大小。相应的，上述步骤S130中，具体是将针对所述服务器的全部服务请求的流量大小与异常流量阈值进行比较。如果还将上针对上述服务器的部分服务请求的流量分析结果指示的流量与异常流量阈值进行比较，具体是将针对上述服务器的全部服务请求的流量大小与异常流量阈值进行比较。

[0064] 如果基于流量的组成成分进行预警决策，如果还将上述针对上述服务器的部分服务请求的流量分析结果指示的流量与异常流量阈值进行比较，具体是将上述针对上述服务器的部分服务请求的流量分析结果指示的各流量组成成分对应的流量大小分别与各流量组成成分对应的异常流量阈值进行比较；相应的，上述步骤S110中，具体是根据所述流量分析结果指示的目标流量组成成分对应的流量大小和目标流量组成成分对应的本分布式节点的权重，分别计算针对所述服务器的全部服务请求的目标流量组成成分的流量大小；上述步骤S130中，具体是将针对上述服务器的全部服务请求的目标流量组成成分的流量大小分别与目标流量组成成分对应的异常流量阈值进行比较，目标流量组成成分为不符合预订条件的流量组成成分。如果没有将上述针对上述服务器的部分服务请求的流量分析结果指示的流量与异常流量阈值进行比较的步骤，相应的，上述步骤S110中，具体是根据上述流量分析结果指示的各流量组成成分对应的流量大小和各流量组成成分对应的本分布式节点的权重，分别计算针对上述服务器的全部服务请求的各流量组成成分的流量大小；上述步

骤S130中，具体是将针对上述服务器的全部服务请求的各流量组成成分的流量大小分别与各流量组成成分对应的异常流量阈值进行比较。

[0065] 在此基础上，可选的，无论哪次比较，当比较结果符合预定条件，发出针对所述服务器进行后续处理的指示的步骤包括：针对比较结果符合预定条件的流量组成成分，发出针对所述服务器进行该流量组成成分的后续处理的指示。

[0066] 应当指出的是，也可以是当比较结果符合预定条件，发出针对上述服务器进行后续处理的指示，而不区分具体流量组成成分。

[0067] 下面将结合具体应用场景，对本申请实施例提供的方法进行详细说明。

[0068] 假设在对进行电子商务的服务器进行DDoS预警的系统中，如图3所示，机房内服务器用于处理电子商务的服务请求。具体的，访问机房内服务器的请求数据通过ISP网络设备到达机房入口网络设备，从ISP网络设备流入机房入口网络设备的服务请求会通过镜像的方式完整地到达第一负载均衡设备，该第一负载均衡设备将服务请求分发给分布式的各个流量分析设备。服务请求中会携带目标服务器的IP地址和访问时间，流量分析设备根据IP地址和访问时间，对每秒钟针对同一个服务器的流量组成成分和各流量组成成分的大小进行统计。例如，流量分析设备A对接收到的服务请求进行分析，统计得到访问时间为18时10分20秒的、IP地址为服务器B的访问请求的流量大小可以表示为20MBps，其中，又可以分为三个流量组成成分a、b和c，流量组成成分a对应的流量大小为10MBps，流量组成成分b对应的流量大小为8MBps，流量组成成分c对应的流量大小为2MBps。各个流量分析设备将其流量分析结果发送给第二负载均衡设备，该第二负载均衡设备将接收到的流量分析结果分发给进行预警决策的各个分布式节点，流量分析结果中携带流量组成成分及对应的流量大小，还携带目标服务器的IP地址和访问时间。例如，第二负载均衡设备接收到针对同一个IP地址的、相同访问时间的100条分析结果，进行预警决策的分布式节点共有50个，则将这100条分析结果均分给这50个分布式节点。应当指出的是，当某个分布式节点无法正常工作时，第二负载均衡设备不再向其分发流量分析结果，而是将流量分析结果均分给正常工作的各个分布式节点。

[0069] 如图4所示，进行预警决策的分布式节点执行如下操作：

[0070] 步骤S210、获取1秒内针对同一服务器的部分服务请求的流量分析结果。

[0071] 其中，该流量分析结果中携带该服务器的IP地址，访问时间，以及各流量组成成分的流量大小。

[0072] 例如，18时10分20秒内访问服务器B的流量组成成分共有三个，其中，流量组成成分a的流量大小为10MBps，流量组成成分b的流量大小为8MBps，流量组成成分c的流量大小为2MBps。

[0073] 步骤S220、分别将每个流量组成成分的流量大小与流量组成成分对应的异常流量阈值进行比较，针对比较结果不符合预定条件的流量组成成分，执行步骤S230，针对比较结果符合预定条件的流量组成成分，执行步骤S250。

[0074] 由于流量组成成分的数量是有限的，且能够预先获知。因此，可以预先确定每个流量组成成分对应的异常流量阈值。

[0075] 例如，已知总共有5种流量组成成分，其中，流量组成成分a对应的异常流量阈值为8MBps，流量组成成分b对应的异常流量阈值为20MBps，流量组成成分c对应的异常流量阈值

为2MBps,其他两种流量组成成分由于本申请实施例中未涉及,故不再介绍。

[0076] 步骤S230、根据比较结果不符合预定条件的流量组成成分对应的流量大小和对应的本分布式节点的权重,分别估计上述1秒内针对上述服务器的全部服务请求的比较结果不符合预定条件的流量组成成分的流量大小。

[0077] 例如,预定条件是流量大小不小于异常流量阈值。那么,根据流量组成成分b的流量大小(8MBps)和流量组成成分b对应的本分布式节点的权重0.5,估计上述1秒内针对上述服务器的全部服务请求中、流量组成成分b的流量大小(16MBps)。

[0078] 步骤S240、将估计得到的流量大小与相应的流量组成成分对应的异常流量阈值进行比较,针对比较结果不符合预定条件的流量组成成分,不进行任何处理,针对比较结果符合预定条件的流量组成成分,执行步骤S250。

[0079] 步骤S250、发出针对上述服务器进行比较结果符合预定条件的流量组成成分的流量清洗的指示。

[0080] 即,发出针对上述服务器B进行流量组成成分a和c的流量清洗的指示。

[0081] 清洗设备在接收到上述指示后,对到达机房入口网络设备的服务请求进行清洗,滤除流量组成成分a和c的服务请求,保留流量组成成分b的服务请求(正常电子商务的服务请求),并将清洗后的服务请求回注至机房入口网络设备。

[0082] 机房入口网络设备根据IP地址将服务请求发送给对应的机房内服务器。

[0083] 上述过程中,以1秒作为流量分析周期为例进行说明。应当指出的是,在实际应用中,可以根据实际需要设置流量分析周期的大小。

[0084] 上述过程中,负载均衡设备将流量分析结果均分给正常工作的各个分布式节点。应当指出的是,在实际应用中,可以配置负载均衡设备按照不同的策略进行流量分析结果的分发。

[0085] 图5为本申请一个实施例的预警决策的节点5,该节点5为分布式节点,包括以下模块:

[0086] 流量分析结果获取模块501,用于获取针对同一服务器的部分服务请求的流量分析结果;

[0087] 完整流量估计模块502,用于根据所述流量分析结果指示的流量和本分布式节点的权重,计算针对所述服务器的全部服务请求的流量,所述权重是本分布式节点获取的流量分析结果指示的流量占所述服务器的全部服务请求的流量的权重;

[0088] 阈值比较模块503,用于将针对所述服务器的全部服务请求的流量与异常流量阈值进行比较;

[0089] 判断控制模块504,用于根据比较结果,判断是否发出针对所述服务器进行后续处理的指示。

[0090] 可选地,所述阈值比较模块还用于:

[0091] 当比较结果符合预定条件,判断发出针对所述服务器进行后续处理的指示;否则,判断不发出针对所述服务器进行后续处理的指示;所述预定条件为进行比较的流量大于所述异常流量阈值,或者所述预定条件为进行比较的流量不小于所述异常流量阈值。

[0092] 可选的,所述阈值比较模块还用于:

[0093] 将针对所述服务器的部分服务请求的流量分析结果指示的流量与所述异常流量

阈值进行比较；

[0094] 所述根据所述流量分析结果指示的流量和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量是在比较结果不符合所述预定条件的前提下执行的。

[0095] 可选的，还包括权重调整模块，用于按照预定的权重调整周期，调整本分布式节点的权重。

[0096] 可选的，所述权重调整模块具体用于：

[0097] 在每个权重调整周期，确定进行预警决策的其它分布式节点获取的本权重调整周期的部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量；

[0098] 在每个所述的权重调整周期，根据进行预警决策的全部分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量，计算所述部分时间段内针对所述服务器的全部服务请求的流量；

[0099] 在每个所述的权重调整周期，至少根据本分布式节点获取的所述部分时间段内针对所述服务器的部分服务请求的流量分析结果指示的流量占所述部分时间段内针对所述服务器的全部服务请求的流量的权重，调整本分布式节点在下一个权重调整周期的权重。

[0100] 可选的，所述流量分析结果获取模块具体用于：

[0101] 从负载均衡设备获取针对同一服务器的部分服务请求的流量分析结果。

[0102] 可选的，该节点还包括服务请求获取模块，用于：

[0103] 从负载均衡设备获取针对所述服务器的部分服务请求；

[0104] 所述流量结果获取模块具体用于：对所述部分服务请求进行流量分析，得到针对所述服务器的部分服务请求的流量分析结果。

[0105] 可选的，所述完整流量估计模块具体用于：

[0106] 根据所述流量分析结果指示的流量大小和本分布式节点的权重，计算针对所述服务器的全部服务请求的流量大小；

[0107] 所述阈值比较模块具体用于：将针对所述服务器的部分服务请求的流量分析结果指示的流量大小与所述异常流量阈值进行比较；以及在比较结果不符合所述预定条件时，将针对所述服务器的全部服务请求的流量大小与异常流量阈值进行比较。

[0108] 可选的，所述阈值比较模块具体用于：

[0109] 将针对所述服务器的部分服务请求的流量分析结果指示的各流量组成成分对应的流量大小分别与各流量组成成分对应的异常流量阈值进行比较；以及在有流量组成成分对应的流量大小与对应的异常流量阈值的比较结果不符合预定条件时，将针对所述服务器的全部服务请求的目标流量组成成分的流量大小分别与目标流量组成成分对应的异常流量阈值进行比较，所述目标流量组成成分为不符合预订条件的流量组成成分；

[0110] 所述完整流量估计模块具体用于：根据所述流量分析结果指示的目标流量组成成分对应的流量大小和目标流量组成成分对应的本分布式节点的权重，分别计算针对所述服务器的全部服务请求的目标流量组成成分的流量大小。

[0111] 可选的，所述指示发送模块具体用于：

[0112] 针对比较结果符合预定条件的流量组成成分，发出针对所述服务器进行该流量组成成分的后续处理的指示。

[0113] 基于上述任意节点实施例，可选的，后续处理包括：流量清洗，流量黑洞，或流量分

析。

[0114] 本申请实施例还提供一种预警决策系统，该系统包括多个上述进行预警决策的节点。

[0115] 可选的，还包括多个流量分析节点，第一负载均衡设备和第二负载均衡设备；

[0116] 所述第一负载均衡设备用于服务请求分流给所述多个流量分析节点；

[0117] 各个流量分析节点接收服务请求，向第二负载均衡设备上报流量分析结果；

[0118] 所述第二负载均衡设备将流量分析结果分流给所述多个预警决策额节点。

[0119] 需要注意的是，本申请可在软件和/或软件与硬件的组合体中被实施，例如，本申请的各个装置可采用专用集成电路(ASIC)或任何其他类似硬件设备来实现。在一个实施例中，本申请的软件程序可以通过处理器执行以实现上文所述步骤或功能。同样地，本申请的软件程序(包括相关的数据结构)可以被存储到计算机可读记录介质中，例如，RAM存储器，磁或光驱动器或软磁盘及类似设备。另外，本申请的一些步骤或功能可采用硬件来实现，例如，作为与处理器配合从而执行各个步骤或功能的电路。

[0120] 对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

[0121] 虽然前面特别示出并且描述了示例性实施例，但是本领域技术人员将会理解的是，在不背离权利要求书的精神和范围的情况下，在其形式和细节方面可以有所变化。

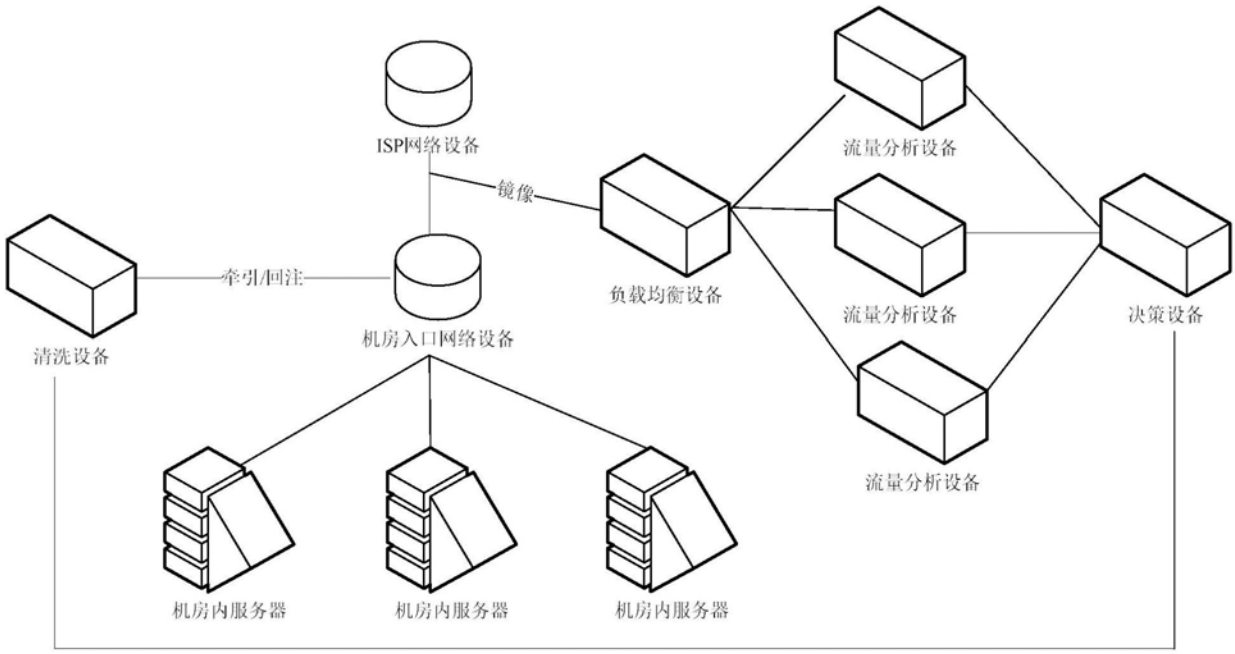

ISP网络设备
镜像
流量分析设备
牵引/回注
负载均衡设备
流量分析设备
决策设备
清洗设备
机房入口网络设备
流量分析设备
机房内服务器
机房内服务器
机房内服务器

图1

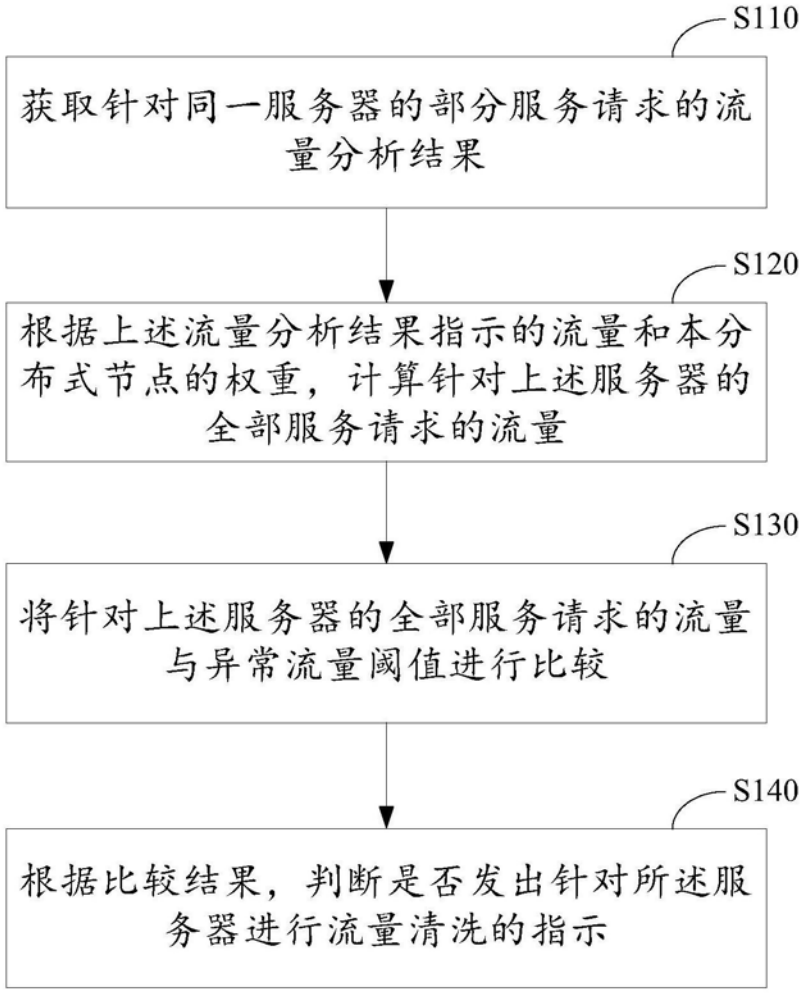

S110
获取针对同一服务器的部分服务请求的流量分析结果
S120
根据上述流量分析结果指示的流量和本分布式节点的权重，计算针对上述服务器的全部服务请求的流量
S130
将针对上述服务器的全部服务请求的流量与异常流量阈值进行比较
S140
根据比较结果，判断是否发出针对所述服务器进行流量清洗的指示

图2

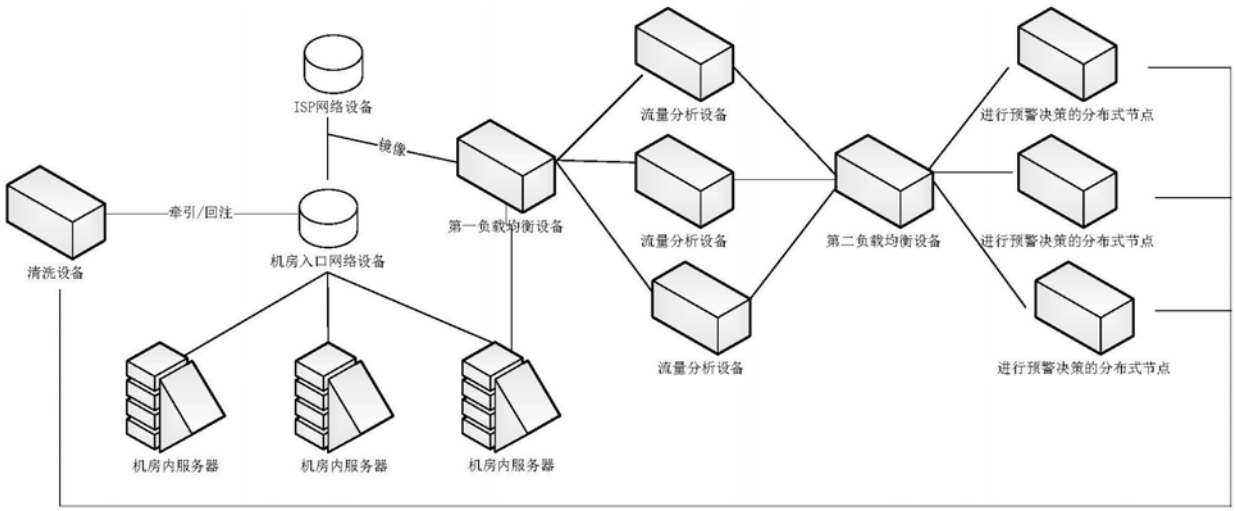

ISP网络设备
镜像
流量分析设备
进行预警决策的分布式节点
牵引/回注
第一负载均衡设备
流量分析设备
第二负载均衡设备
进行预警决策的分布式节点
清洗设备
机房入口网络设备
流量分析设备
进行预警决策的分布式节点
机房内服务器
机房内服务器
机房内服务器

图3

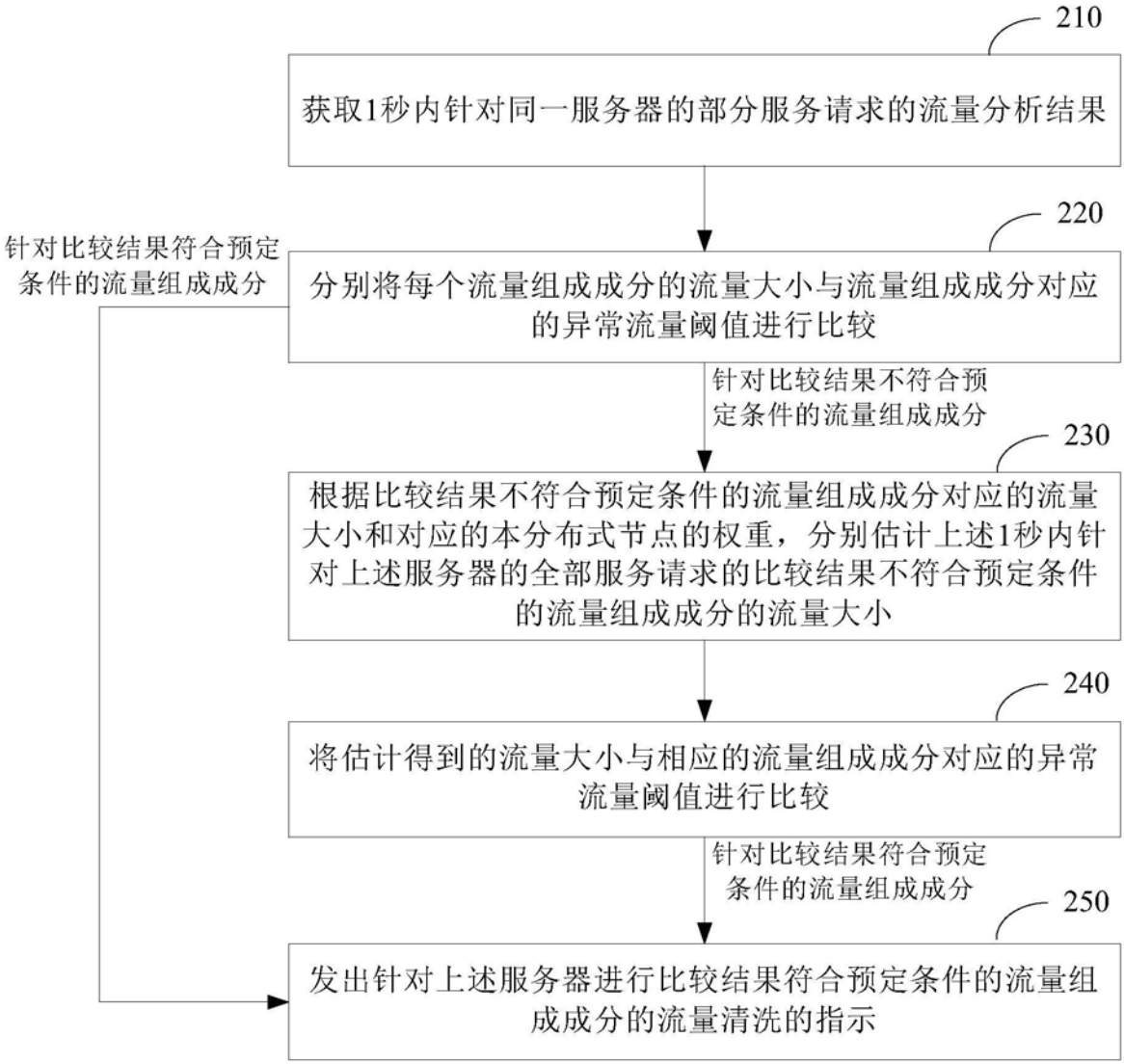

210
获取1秒内针对同一服务器的部分服务请求的流量分析结果
220
针对比较结果符合预定条件的流量组成成分
分别将每个流量组成成分的流量大小与流量组成成分对应的异常流量阈值进行比较
针对比较结果不符合预定条件的流量组成成分
230
根据比较结果不符合预定条件的流量组成成分对应的流量大小和对应的本分布式节点的权重，分别估计上述1秒内针对上述服务器的全部服务请求的比较结果不符合预定条件的流量组成成分的流量大小
240
将估计得到的流量大小与相应的流量组成成分对应的异常流量阈值进行比较
针对比较结果符合预定条件的流量组成成分
250
发出针对上述服务器进行比较结果符合预定条件的流量组成成分的流量清洗的指示

图4

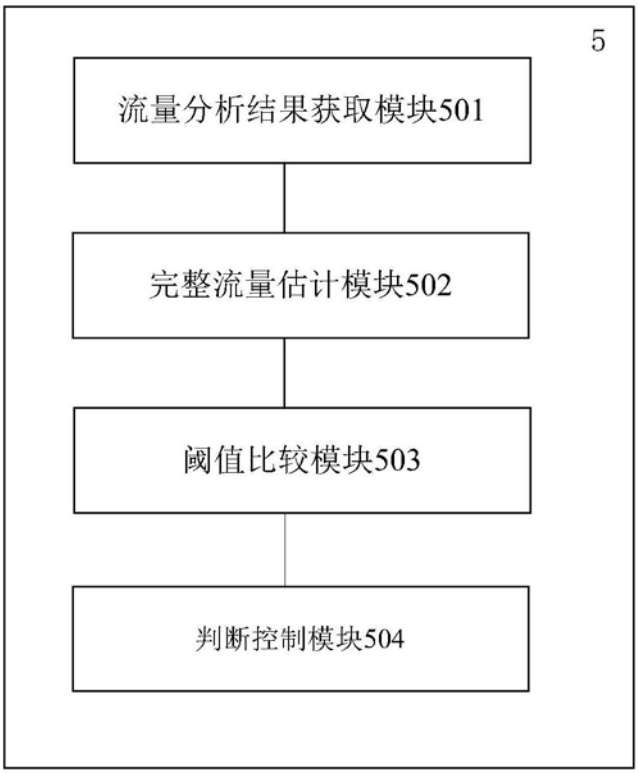


图5