(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 112367324 A
(43)申请公布日 2021.02.12

(21)申请号 202011262352.6

(22)申请日 2020.11.12

(71)申请人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼

(72)发明人 张安发

(74)专利代理机构 深圳市隆天联鼎知识产权代理有限公司 44232
代理人 孙强

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/55(2013.01)

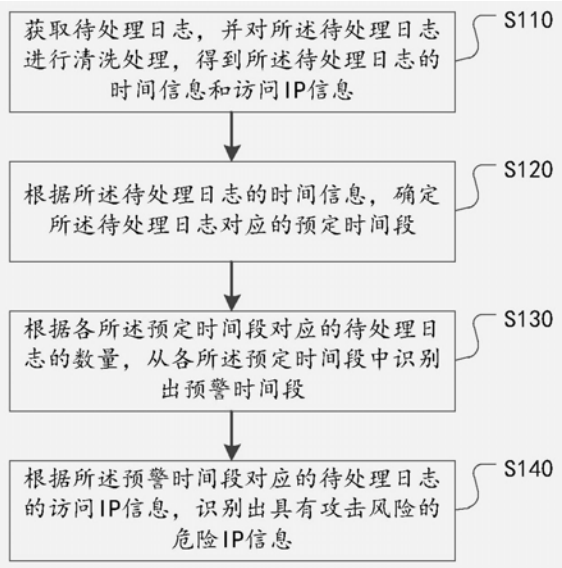
权利要求书2页 说明书11页 附图4页

(54)发明名称

CDN的攻击检测方法、装置、存储介质及电子设备

(57)摘要

本公开提供了一种CDN的攻击检测方法、装置、存储介质及电子设备，属于数据处理技术领域，该方法包括：获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息；根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。该方法能够快速识别异常访问的IP地址，以对异常访问快速响应。



CN 112367324 A

1.一种CDN的攻击检测方法,其特征在于,包括:

获取待处理日志,并对所述待处理日志进行清洗处理,得到所述待处理日志的时间信息和访问IP信息;

根据所述待处理日志的时间信息,确定所述待处理日志对应的预定时间段;

根据各所述预定时间段对应的待处理日志的数量,从各所述预定时间段中识别出预警时间段;

根据所述预警时间段对应的待处理日志的访问IP信息,识别出具有攻击风险的危险IP信息。

2.根据权利要求1所述的攻击检测方法,其特征在于,根据各所述预定时间段对应的待处理日志的数量,从各所述预定时间段中识别出预警时间段,包括:

获取各所述预定时间段对应的历史访问数据;

根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据,确定各所述预定时间段的访问量增长率;

根据所述访问量增长率,从各所述预定时间段中识别出预警时间段。

3.根据权利要求2所述的攻击检测方法,其特征在于,根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据,确定各所述预定时间段的访问量增长率,包括:

根据各所述预定时间段的历史访问数据,计算各所述预定时间段的历史平均访问量;

根据各所述预定时间段的历史平均访问量以及当前各所述预定时间段对应的待处理日志的数量,计算各所述预定时间段的访问量增长率。

4.根据权利要求2所述的攻击检测方法,其特征在于,根据所述访问量增长率,从各所述预定时间段中识别出预警时间段,包括:

获取与各所述预定时间段相邻的上一预定时间段的访问数据;

根据各所述预定时间段对应的上一预定时间段的访问数据和当前所述预定时间段对应的待处理日志的数量,计算各所述预定时间段对应的访问增加量;

根据各所述预定时间段对应的所述访问增加量以及所述访问量增长率,从各所述预定时间段中识别出预警时间段。

5.根据权利要求1所述的攻击检测方法,其特征在于,根据所述预警时间段对应的待处理日志的访问IP信息,识别出具有攻击风险的危险IP信息,包括:

根据所述预警时间段内对应的待处理日志的访问IP信息,获取所述访问IP信息在预定周期内与所述预警时间段对应的同一时间段内的历史访问数据;

根据所述访问IP信息的历史访问数据以及所述访问IP信息在所述预警时间段内的访问数量进行计算,得到所述访问IP信息的访问量增长率;

根据所述访问IP信息的访问量增长率,从所述预警时间段对应的待处理日志的访问IP信息中识别出危险IP信息。

6.根据权利要求1所述的攻击检测方法,其特征在于,所述攻击检测方法还包括:

将所述危险IP访问信息加入至黑名单中,并对所述危险IP信息进行禁止访问处理。

7.一种CDN的攻击检测装置,其特征在于,包括:

获取模块,用于获取待处理日志,并对所述待处理日志进行清洗处理,得到所述待处理

日志的时间信息和访问IP信息；

确定模块，用于根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；

识别模块，用于根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；

处理模块，用于根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

8.根据权利要求7所述的攻击检测装置，其特征在于，所述识别模块包括：

获取单元，用于获取各所述预定时间段对应的历史访问数据；

确定单元，用于根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率；

识别单元，用于根据所述访问量增长率，从各所述预定时间段中识别出预警时间段。

9.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1-6中任一项所述的CDN的攻击检测方法。

10.一种电子设备，其特征在于，包括：

处理器；以及

存储器，其上存储有计算机程序；

其中，所述处理器配置为经由执行所述计算机程序来实现如权利要求1-6中任一项所述的CDN的攻击检测方法。

CDN的攻击检测方法、装置、存储介质及电子设备

技术领域

[0001] 本公开涉及数据处理技术领域，具体而言，涉及一种CDN的攻击检测方法、CDN的攻击检测装置、计算机可读存储介质以及电子设备。

背景技术

[0002] 内容分发网络(CDN)作为现代互联网的基础设施，不仅为用户提供了极致的网络访问体验，也使网站所提供的服务更加安全。然而，CDN服务器也常因为遭受攻击而导致服务器出现瘫痪。在目前的技术方案中，一般的IP防攻击方法都是通过设置单位时间内的访问次数上限，以避免出现访问异常。然而不同IP地址以及不同用户的网站访问特征不同，以致于无法准确表征出是否出现访问异常。因此如何快速识别出异常访问的IP地址，以对异常访问快速响应，保证内容分发网络的安全成为了亟待解决的技术问题。

[0003] 需要说明的是，在上述背景技术部分公开的信息仅用于加强对本公开的背景的理解，因此可以包括不构成对本领域普通技术人员已知的现有技术的信息。

发明内容

[0004] 本公开的实施例提供一种CDN的攻击检测方法、CDN的攻击检测装置、计算机可读存储介质以及电子设备。

[0005] 根据本公开的第一方面，提供一种CDN的攻击检测方法，包括：

[0006] 获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息；

[0007] 根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；

[0008] 根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；

[0009] 根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

[0010] 在本公开的一示例性实施例中，根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段，包括：

[0011] 获取各所述预定时间段对应的历史访问数据；

[0012] 根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率；

[0013] 根据所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0014] 在本公开的一示例性实施例中，根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率，包括：

[0015] 根据各所述预定时间段的历史访问数据，计算各所述预定时间段的历史平均访问量；

[0016] 根据各所述预定时间段的历史平均访问量以及当前各所述预定时间段对应的待

处理日志的数量，计算各所述预定时间段的访问量增长率。

[0017] 在本公开的一示例性实施例中，根据所述访问量增长率，从各所述预定时间段中识别出预警时间段，包括：

[0018] 获取与各所述预定时间段相邻的上一预定时间段的访问数据；

[0019] 根据各所述预定时间段对应的上一预定时间段的访问数据和当前所述预定时间段对应的待处理日志的数量，计算各所述预定时间段对应的访问增加量；

[0020] 根据各所述预定时间段对应的所述访问增加量以及所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0021] 在本公开的一示例性实施例中，根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息，包括：

[0022] 根据所述预警时间段内对应的待处理日志的访问IP信息，获取所述访问IP信息在预定周期内与所述预警时间段对应的同一时间段内的历史访问数据；

[0023] 根据所述访问IP信息的历史访问数据以及所述访问IP信息在所述预警时间段内的访问数量进行计算，得到所述访问IP信息的访问增长率；

[0024] 根据所述IP访问信息的访问增长率，从所述预警时间段对应的待处理日志的访问IP信息中识别出危险IP信息。

[0025] 在本公开的一示例性实施例中，所述攻击检测方法还包括：

[0026] 将所述危险IP访问信息加入至黑名单中，并对所述危险IP信息进行禁止访问处理。

[0027] 根据本公开的第二方面，提供一种CDN的攻击检测装置，包括：

[0028] 获取模块，用于获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息；

[0029] 确定模块，用于根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；

[0030] 识别模块，用于根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；

[0031] 处理模块，用于根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

[0032] 在本公开的一示例性实施例中，所述识别模块包括：

[0033] 获取单元，用于获取各所述预定时间段对应的历史访问数据；

[0034] 确定单元，用于根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率；

[0035] 识别单元，用于根据所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0036] 根据本公开的第三方面，提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如上述任意一项所述的CDN的攻击检测方法。

[0037] 根据本公开的第四方面，提供一种电子设备，包括：

[0038] 处理器；以及

[0039] 存储器，其上存储有计算机程序；

[0040] 其中，所述处理器配置为经由执行所述计算机程序来实现如上述任意一项所述的CDN的攻击检测方法。

[0041] 本公开的实施例提供的技术方案可以具有以下有益效果：

[0042] 基于本公开的各实施例，通过获取待处理日志，并对待处理日志进行清洗处理，得到待处理日志的时间信息和访问IP信息，并根据待处理日志的时间信息，确定待处理日志对应的预定时间段，并根据各预定时间段对应的待处理日志的数量，从各预定时间段中识别出预警时间段，再根据预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。由此，可以快速确定访问存在异常的预警时间段，并针对性的从预警时间段对应的待处理日志的访问IP信息中识别出具有攻击风险的危险IP信息，从而达到快速识别危险IP信息，以对异常访问快速响应的目的。

[0043] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0044] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0045] 图1示出了根据本申请的一个实施例的CDN的攻击检测方法的流程示意图。

[0046] 图2示出了根据本申请的一个实施例的图1的CDN的攻击检测方法中步骤S130的流程示意图。

[0047] 图3示出了根据本申请的一个实施例的图2的CDN的攻击检测方法中步骤S220的流程示意图。

[0048] 图4示出了根据本申请的一个实施例的图2的CDN的攻击检测方法中步骤S230的流程示意图。

[0049] 图5示出了根据本申请的一个实施例的图1的CDN的攻击检测方法中步骤S140的流程示意图。

[0050] 图6示出了根据本申请一个实施例的CDN的攻击检测装置的示意组成框图。

[0051] 图7示出了根据本申请一个实施例的电子设备的示意组成框图。

[0052] 图8示出了根据本申请一个实施例的一种计算机可读存储介质的示意图。

具体实施方式

[0053] 现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本公开将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施方式中。在下面的描述中，提供许多具体细节从而给出对本公开的实施方式的充分理解。然而，本领域技术人员将意识到，可以实践本公开的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知技术方案以避免喧宾夺主而

使得本公开的各方面变得模糊。

[0054] 此外，附图仅为本公开的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。附图中所示的一些方框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0055] 图1示出了根据本申请的一个实施例的CDN的攻击检测方法的流程示意图。参照图1所示，该CDN的攻击检测方法至少包括步骤S110至步骤S140，详细介绍如下：

[0056] 在步骤S110中，获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息。

[0057] 其中，待处理日志可以是分布式网络中各服务节点的服务日志。各服务节点在用户的访问过程中，通过收集用户的操作信息，例如被访问资源、访问时间以及用户的访问IP信息等等，以生成对应的服务日志，并进行存储，以备后续查询。

[0058] 在本申请的一个实施例中，可以实时获取各服务节点的所生成的服务日志以作为待处理日志。在一示例中，当服务节点检测到生成服务日志时，可以将新生成的服务日志发送至处理服务器中，以使处理服务器根据各服务节点所发送的服务日志进行分析，以达到快速检测的目的。

[0059] 在其他示例中，处理服务器可以实时从各服务节点获取新生成的服务日志，具体地，处理服务器可以每隔预定时间向各服务节点发送日志获取请求，若各服务节点存在新生成的服务日志，则可以响应该日志获取请求，将新生成的服务日志向处理服务器进行发送，若未存在新生成的服务日志，则不进行响应。

[0060] 其中，预定时间可以是本领域技术人员预先设定的处理服务器获取服务日志的间隔时间，例如该预定时间可以是2S、10S或者1min等，以上仅为示例性举例，本申请对此不作特殊限定。

[0061] 在本申请的一个实施例中，在处理服务器获取待处理日志以后，处理服务器可以对待处理日志进行清洗处理，以从待处理日志中获取所需的信息，即待处理日志对应的时间信息和访问IP信息。其中，时间信息可以是待处理日志的生成时间，也可以是用户在访问时的开始时间，本申请对此不作特殊限定。

[0062] 在步骤S120中，根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段。

[0063] 在该实施例中，根据每一待处理日志对应的时间信息，可以确定待处理日志对应的预定时间段，其中，预定时间段可以是由本领域技术人员对时间进行预先划分而得到的，例如可以预先设定每两个小时为一个时间段或者每三个小时为一个时间段，等等。

[0064] 由此，可以将每一天划分为多个预定时间段，根据待处理日志的时间信息，则可以确定该待处理日志对应于某一预定时间段，从而可以得到各个预定时间段对应的待处理日志，并统计各预定时间段对应的待处理日志的数量。

[0065] 在步骤S130中，根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段。

[0066] 在该实施例中，待处理日志的数量与分布式网络被访问的次数相对应，可以理解

的，若数量过多，则表示分布式网络在该预定时间段内的被访问次数过多，分布式网络受到攻击的可能性也就较大；若数量较少或正常，则表示分布式网络受到攻击的可能性较小。

[0067] 因此，根据每一预定时间段对应的待处理日志的数量，可以从各预定时间段中识别出预警时间段。在一示例中，可以将每一预定时间段对应的待处理日志的数量与预先设定的阈值进行比较，若某一预定时间段对应的待处理日志的数量达到预定先设定的阈值，则表示该预定时间段对应的被访问次数过多，因此将其识别为预警时间段，需要对预警时间段内的访问情况进行分析；若某一预定时间段对应的待处理日志的数量少于预先设定的阈值，则表示该预定时间段的被访问次数正常，无需进行预警。

[0068] 其中，预先设定的阈值可以是由本领域技术人员根据在先经验进行设定的，也可以结合分布式网络的客户数量情况进行实时修正，以保证预警时间段的识别的准确性。

[0069] 例如，可以根据以下公式确定更新后的阈值Y：

[0070] Y＝y+N*a，其中，y为当前的阈值，N为增加的客户数量，a为每增加一个客户对应增加的预期访问数量，a可以是根据在先经验所得出的。以上仅为示例性举例，本领域技术人员可以根据实际需要，设置对应的阈值计算公式。

[0071] 在步骤S140中，根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

[0072] 在该实施例中，处理服务器可以根据预警时间段对应的待处理日志的访问IP信息，对应获取每一访问IP信息对应的访问情况，例如该访问IP信息在预警时间段内的访问次数以及在其他时间段的访问次数等等，再基于每一访问IP信息对应的访问情况进行分析，从而分析出访问异常的访问IP信息，从而识别出具有攻击风险的危险IP信息，以采取相应的安全措施。

[0073] 由此，在图1所示的实施例中，根据各预定时间段对应的待处理日志的数量，识别出预警时间段，再对预警时间段内对应的待处理日志的访问IP信息进行逐一分析，从而可以快速识别出具有攻击风险的危险IP信息，避免无针对性的全面识别，提高了危险IP信息的识别效率，以能够对分布式网络所受到的攻击进行快速响应。

[0074] 基于图1所示的实施例，图2示出了根据本申请的一个实施例的图1的CDN的攻击检测方法中步骤S130的流程示意图。参照图2所示，步骤S130至少包括步骤S210至步骤S230，详细介绍如下：

[0075] 在步骤S210中，获取各所述预定时间段对应的历史访问数据。

[0076] 其中，历史访问数据可以是历史上对应于该预定时间段的同一时间段的历史访问量。各预定时间段对应的历史访问数据可以是历史上与该预定时间段对应的同一时间段的历史访问数据，例如预定时间段为14:00-16:00，则可以对应获取历史上14:00-16:00时间段内的访问数据，等等。

[0077] 需要说明的，可以获取一组历史访问数据，也可以获取多组历史访问数据，例如可以获取昨天对应于与该预定时间段的历史访问数据，也可以获取前七天内对应于该预定时间段的历史访问数据，等等，本申请对此不作特殊限定。若获取的是多组历史访问量数据，则可以对该多组历史访问数据进行取平均值，以进行后续计算。

[0078] 在步骤S220中，根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率。

[0079] 在该实施例中，根据当前各预定时间段对应的待处理日志的数量，以及历史上对应于各预定时间段的同一时间段的历史访问量，可以计算各预定时间段对应的访问量增长率。具体地，可以将当前各预定时间段对应的待处理日志的数量减去对应的历史访问量，从而得到各预定时间段对应的增长量，再讲各预定时间段对应的增长量除以对应的历史访问量，从而得到各预定时间段对应的访问量增长率。

[0080] 在步骤S230中，根据所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0081] 在该实施例中，根据各预定时间段对应的访问量增长率，可以将其与预先设定的增长率阈值进行比较，若某一预定时间段对应的访问量增长率大于或等于增长率阈值，则表示该预定时间段的访问数据相比于历史访问数据存在异常，可以认为该预定时间段存在风险，进而可以将其识别为预警时间段。若某一预定时间段对应的访问量增长率小于增长率阈值，则表示该预定时间段的访问数据相比于历史访问数据为正常状态。

[0082] 在图2所示的实施例中，基于各预定时间段对应的历史访问数据，计算得到各预定时间段对应的访问量增长率，从而可以根据各访问量增长率分析得到各预定时间段与历史上的访问数据的差异，以保证后续识别的准确性。

[0083] 基于图1和图2所示的实施例，图3示出了根据本申请的一个实施例的图2的CDN的攻击检测方法中步骤S220的流程示意图。参照图3所示，步骤S220至少包括步骤S310至步骤S320，详细介绍如下：

[0084] 在步骤S310中，根据各所述预定时间段的历史访问数据，计算各所述预定时间段的历史平均访问量。

[0085] 在该实施例中，针对每一预定时间段，若获取多组历史访问数据，例如前一周内与该预定时间段对应的同一时间段的历史访问数据，即七组历史访问数据，等等。则可以根据多组历史访问数据进行相加再除以组数，从而得到每一预定时间段对应的历史平均访问量。

[0086] 在步骤S320中，根据各所述预定时间段的历史平均访问量以及当前各所述预定时间段对应的待处理日志的数量，计算各所述预定时间段的访问量增长率。

[0087] 在该实施例中，可以将当前各预定时间段对应的待处理日志的数量减去该预定时间段对应的历史平均访问量，再除以各预定时间段对应的历史平均访问量，从而得到各预定时间段对应的访问量增长率。

[0088] 由此，基于多组历史访问数据进行计算，得到各预定时间段对应的历史平均访问量，可以得到各预定时间段对应的历史访问水平，使得该历史访问量增长率能够基于多组历史访问数据进行计算，避免了因特殊情况而导致的历史访问数据波动，保证了后续识别的准确性。

[0089] 基于图1和图2所示的实施例，图4示出了根据本申请的一个实施例的图2的CDN的攻击检测方法中步骤S230的流程示意图。参照图4所示，步骤S230至少包括步骤S410至步骤S430，详细介绍如下：

[0090] 在步骤S410中，获取与各所述预定时间段相邻的上一预定时间段的访问数据。

[0091] 在该实施例中，相邻的上一预定时间段的访问数据可以是相邻的上一时间段的访问量，例如预定时间段为14:00-16:00，每两个小时为一个时间段，则获取与该预定时间段

相邻的上一预定时间段的访问数据即为获取12:00-14:00时间段内的访问量，等等。

[0092] 在步骤S420中，根据各所述预定时间段对应的上一预定时间段的访问数据和当前所述预定时间段对应的待处理日志的数量，计算各所述预定时间段对应的访问增加量。

[0093] 在该实施例中，将当前各预定时间段对应的待处理日志的数量减去与其相邻的上一预定时间段的访问量，从而可以得到预定时间段对应的访问增加量。

[0094] 在步骤S430中，根据各所述预定时间段对应的所述访问增加量以及所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0095] 在该实施例中，可以预先对访问增加量以及访问量增长率分别设定对应的阈值，并将访问增加量与访问量增长率分别与对应的阈值进行比较，若二者均大于或等于各自对应的阈值，则表示当前预定时间段具有受到攻击的风险，因此可以将该预定时间段识别为预警时间段，若二者中至少一个小于其对应的阈值，则表示该预定时间段不存在风险，为安全时间段。

[0096] 由此，在图4所示的实施例中，通过计算访问增加量以及访问量增长率，结合历史访问数据以及相邻时间段的访问数据进行分析，可以保证预警时间段的识别的准确性。

[0097] 基于图1所示的实施例，图5示出了根据本申请的一个实施例的图1的CDN的攻击检测方法中步骤S140的流程示意图。参照图5所示，步骤S140至少包括步骤S510至步骤S530，详细介绍如下：

[0098] 在步骤S510中，根据所述预警时间段内对应的待处理日志的访问IP信息，获取所述访问IP信息在预定周期内与所述预警时间段对应的同一时间段内的历史访问数据。

[0099] 在该实施例中，根据预警时间段内对应的待处理日志的访问IP信息，获取每一访问IP信息在预定周期内与所述预警时间段对应的同一时间段内的历史访问数据，该历史访问数据可以是该访问IP信息对应的访问量。例如预警时间段为14:00-16:00，则可以获取访问IP信息在预定周期内14:00-16:00时间段的历史访问量。

[0100] 其中，预定周期可以是本领域技术人员预先设定的时间间隔，例如一个预定周期为7天，则对应获取该访问IP信息在前七天内与预警时间段相对应的时间段内的历史访问量，等等。

[0101] 在步骤S520中，根据所述访问IP信息的历史访问数据的平均值以及所述访问IP信息在所述预警时间段内的访问数量进行计算，得到所述访问IP信息的访问量增长率。

[0102] 在该实施例中，将访问IP信息在预警时间段内的访问数量减去对应的历史访问数据的平均值，再除以历史访问数据的平均值，从而得到该访问IP信息对应的访问增长率。例如，某一访问IP信息在预警时间段内的访问数量为15，对应的历史访问数据的平均值为10，则该访问IP信息对应的访问量增长率为(15-10)/10＝50％，等等。

[0103] 在步骤S530中，根据所述访问IP信息的访问量增长率，从所述预警时间段对应的待处理日志的访问IP信息中识别出危险IP信息。

[0104] 在该实施例中，可以将访问IP信息对应的访问量增长率与预先设定的阈值进行比较，若大于或等于阈值，则表示该访问IP信息的访问存在异常，可以将其识别为具有攻击风险的危险IP信息，若小于阈值，则表示该访问IP信息的访问正常，为安全IP信息。其中，该访问IP信息的访问量增长率对应的阈值可以是由本领域技术人员根据在先经验预先设定的。

[0105] 由此，结合访问IP信息的历史访问数据进行分析，可以直观看出该访问IP信息的

访问异常，达到快速识别危险IP信息的目的，提高了分布式网络对攻击的响应速度。

[0106] 基于前述实施例，在本申请的一个实施例中，所述攻击检测方法还包括：

[0107] 将所述危险IP访问信息加入至黑名单中，并对所述危险IP信息进行禁止访问处理。

[0108] 在该实施例中，将识别所得到的的危险IP信息加入至黑名单中，若后续接收到该危险IP信息的访问请求，则可以对该危险IP信息进行禁止访问处理，以防止继续对分布式网络的攻击。

[0109] 若存在误识别情况，则可以由该危险IP信息对应的用户进行申诉，以从黑名单中删除该危险IP信息，从而使该IP信息能够正常访问。

[0110] 本公开还提供了一种CDN的攻击检测装置。参考图6所示，该装置可以包括：

[0111] 获取模块610，用于获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息；

[0112] 确定模块620，用于根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；

[0113] 识别模块630，用于根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；

[0114] 处理模块640，用于根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

[0115] 在本申请的一实施例中，所述识别模块630包括：

[0116] 获取单元，用于获取各所述预定时间段对应的历史访问数据；

[0117] 确定单元，用于根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率；

[0118] 识别单元，用于根据所述访问量增长率，从各所述预定时间段中识别出预警时间段。

[0119] 上述CDN的攻击检测装置中各模块的具体细节已经在对应的CDN的攻击检测方法中进行了详细的描述，因此此处不再赘述。

[0120] 应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本公开的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

[0121] 此外，尽管在附图中以特定顺序描述了本公开中方法的各个步骤，但是，这并非要求或者暗示必须按照该特定顺序来执行这些步骤，或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的，可以省略某些步骤，将多个步骤合并为一个步骤执行，以及/或者将一个步骤分解为多个步骤执行等。

[0122] 通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM，U盘，移动硬盘等)中或网络上，包括若干指令以使得一台计算设备(可以是个人计算机、服务器、移动终端、或者网络设备等)执行根据本公开实施方式的

方法。

[0123] 在本公开的示例性实施例中，还提供了一种能够实现上述方法的电子设备。

[0124] 所属技术领域的技术人员能够理解，本发明的各个方面可以实现为系统、方法或程序产品。因此，本发明的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式(包括固件、微代码等)，或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

[0125] 下面参照图7来描述根据本发明的这种实施方式的电子设备500。图7显示的电子设备500仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0126] 如图7所示，电子设备500以通用计算设备的形式表现。电子设备500的组件可以包括但不限于：上述至少一个处理单元510、上述至少一个存储单元520、连接不同系统组件(包括存储单元520和处理单元510)的总线530。

[0127] 其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元510执行，使得所述处理单元510执行本说明书上述“示例性方法”部分中描述的根据本发明各种示例性实施方式的步骤。例如，所述处理单元510可以执行如图1中所示的步骤110：获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息；步骤S120：根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段；步骤S130，根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段；步骤S140，根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息。

[0128] 存储单元520可以包括易失性存储单元形式的可读介质，例如随机存取存储单元(RAM)5201和/或高速缓存存储单元5202，还可以进一步包括只读存储单元(ROM)5203。

[0129] 存储单元520还可以包括具有一组(至少一个)程序模块5205的程序/实用工具5204，这样的程序模块5205包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0130] 总线530可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

[0131] 电子设备500也可以与一个或多个外部设备700(例如键盘、指向设备、蓝牙设备等)通信，还可与一个或者多个使得用户能与该电子设备500交互的设备通信，和/或与使得该电子设备500能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口550进行。并且，电子设备500还可以通过网络适配器560与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器560通过总线530与电子设备500的其它模块通信。应当明白，尽管图中未示出，可以结合电子设备500使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0132] 通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失

性存储介质(可以是CD-ROM,U盘,移动硬盘等)中或网络上,包括若干指令以使得一台计算设备(可以是个人计算机、服务器、终端装置、或者网络设备等)执行根据本公开实施方式的方法。

[0133] 在本公开的示例性实施例中,还提供了一种计算机可读存储介质,其上存储有能够实现本说明书上述方法的程序产品。在一些可能的实施方式中,本发明的各个方面还可以实现为一种程序产品的形式,其包括程序代码,当所述程序产品在终端设备上运行时,所述程序代码用于使所述终端设备执行本说明书上述"示例性方法"部分中描述的根据本发明各种示例性实施方式的步骤。

[0134] 参考图8所示,描述了根据本发明的实施方式的用于实现上述方法的程序产品600,其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码,并可以在终端设备,例如个人电脑上运行。然而,本发明的程序产品不限于此,在本文件中,可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0135] 所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0136] 计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了可读程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质,该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0137] 可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于无线、有线、光缆、RF等等,或者上述的任意合适的组合。

[0138] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等,还包括常规的过程式程序设计语言—诸如"C"语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中,远程计算设备可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN),连接到用户计算设备,或者,可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0139] 此外,上述附图仅是根据本发明示例性实施例的方法所包括的处理的示意性说明,而不是限制目的。易于理解,上述附图所示的处理并不表明或限制这些处理的时间顺序。另外,也易于理解,这些处理可以是例如在多个模块中同步或异步执行的。

[0140] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本公开的其他实施例。本申请旨在涵盖本公开的任何变型、用途或者适应性变化,这些变型、用途或者

适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由权利要求指出。

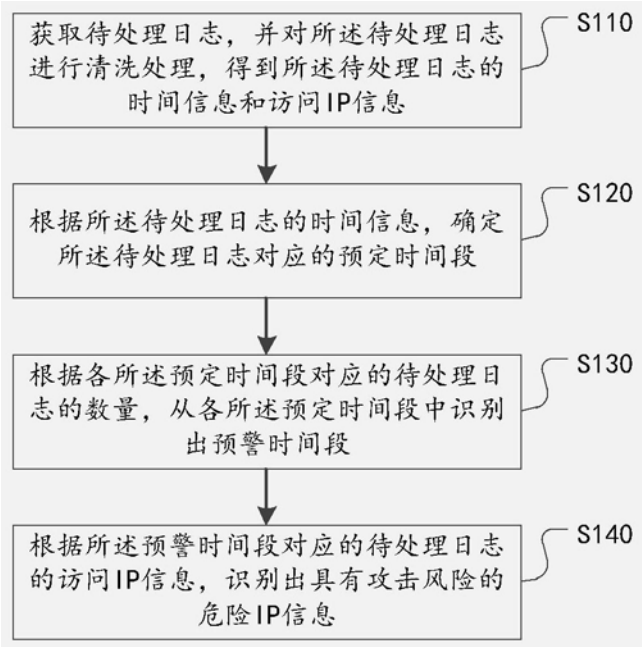

获取待处理日志，并对所述待处理日志进行清洗处理，得到所述待处理日志的时间信息和访问IP信息
S110
根据所述待处理日志的时间信息，确定所述待处理日志对应的预定时间段
S120
根据各所述预定时间段对应的待处理日志的数量，从各所述预定时间段中识别出预警时间段
S130
根据所述预警时间段对应的待处理日志的访问IP信息，识别出具有攻击风险的危险IP信息
S140

图1

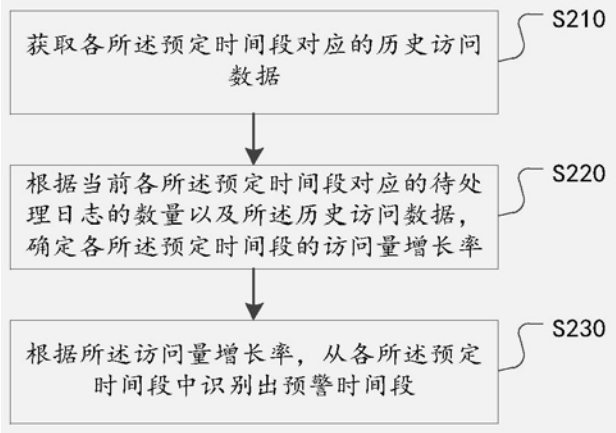

获取各所述预定时间段对应的历史访问数据
S210
根据当前各所述预定时间段对应的待处理日志的数量以及所述历史访问数据，确定各所述预定时间段的访问量增长率
S220
根据所述访问量增长率，从各所述预定时间段中识别出预警时间段
S230

图2

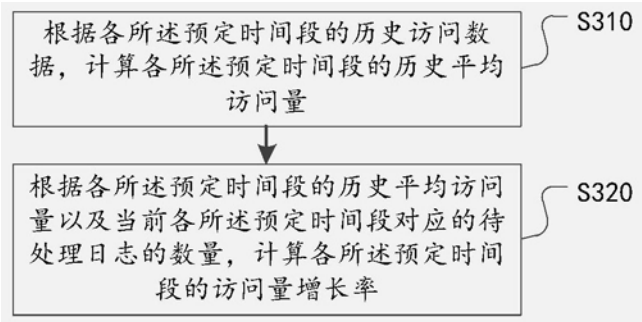

根据各所述预定时间段的历史访问数据，计算各所述预定时间段的历史平均访问量
S310
根据各所述预定时间段的历史平均访问量以及当前各所述预定时间段对应的待处理日志的数量，计算各所述预定时间段的访问量增长率
S320

图3

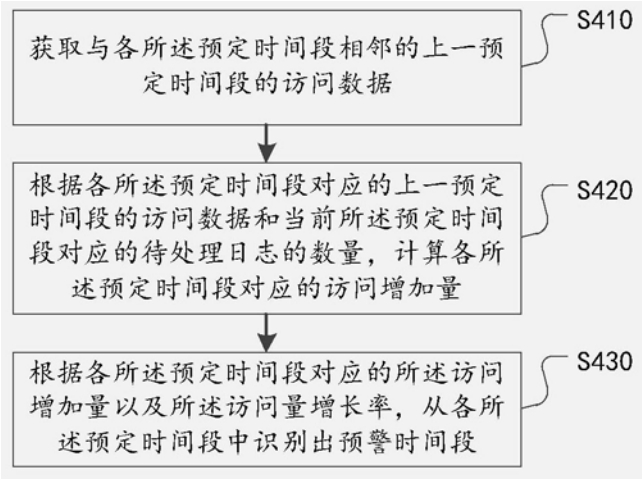

获取与各所述预定时间段相邻的上一预定时间段的访问数据
S410
根据各所述预定时间段对应的上一预定时间段的访问数据和当前所述预定时间段对应的待处理日志的数量，计算各所述预定时间段对应的访问增加量
S420
根据各所述预定时间段对应的所述访问增加量以及所述访问量增长率，从各所述预定时间段中识别出预警时间段
S430

图4

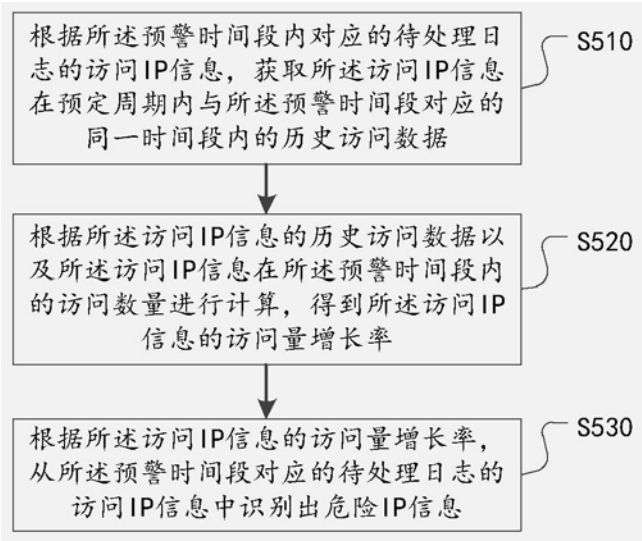

根据所述预警时间段内对应的待处理日志的访问IP信息，获取所述访问IP信息在预定周期内与所述预警时间段对应的同一时间段内的历史访问数据
S510
根据所述访问IP信息的历史访问数据以及所述访问IP信息在所述预警时间段内的访问数量进行计算，得到所述访问IP信息的访问量增长率
S520
根据所述访问IP信息的访问量增长率，从所述预警时间段对应的待处理日志的访问IP信息中识别出危险IP信息
S530

图5

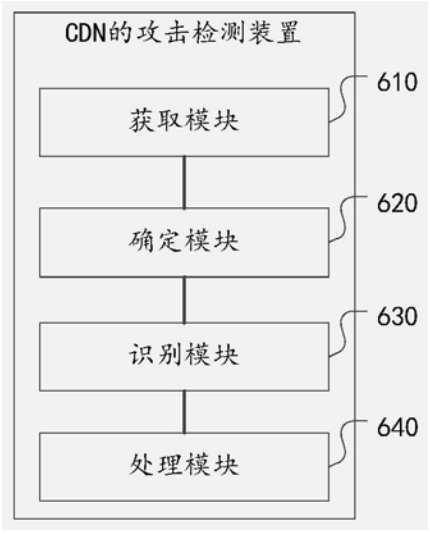

CDN的攻击检测装置
610
获取模块
620
确定模块
630
识别模块
640
处理模块

图6

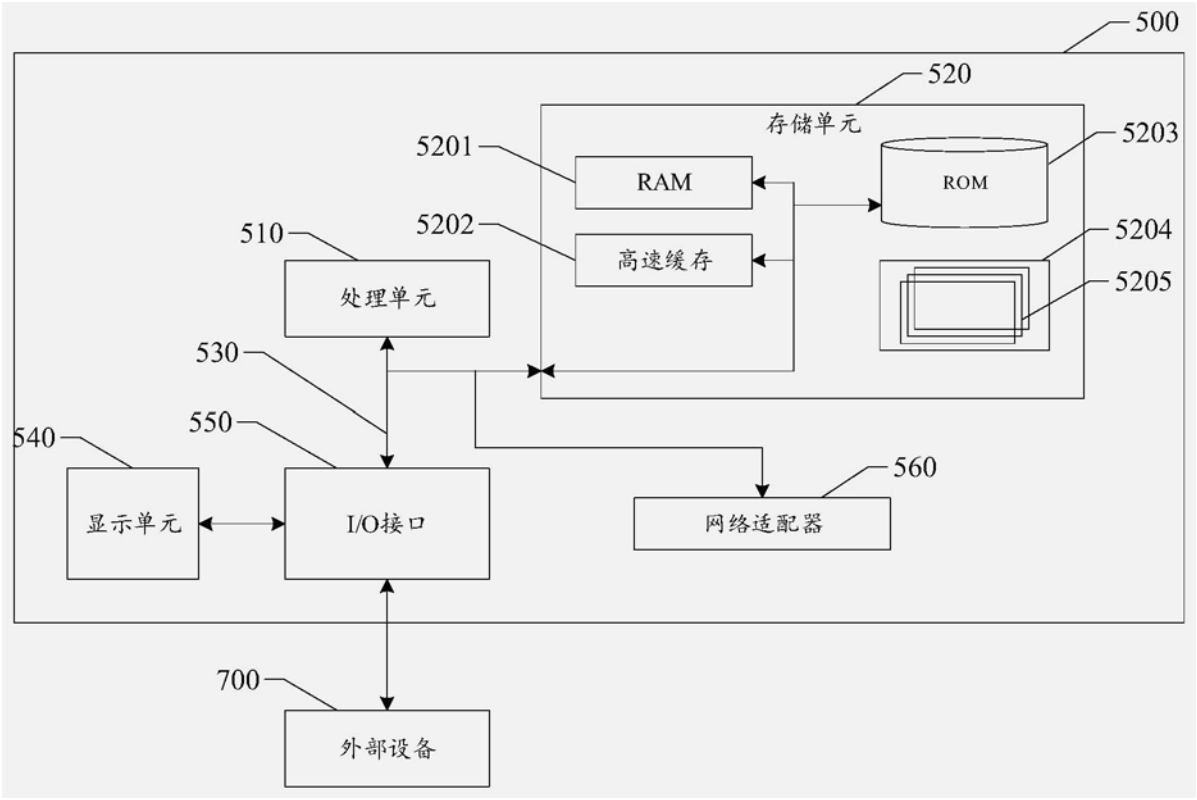

500
520
存储单元
5201
RAM
5203
ROM
5202
高速缓存
5204
5205
510
处理单元
530
550
540
显示单元
I/O接口
560
网络适配器
700
外部设备

图7

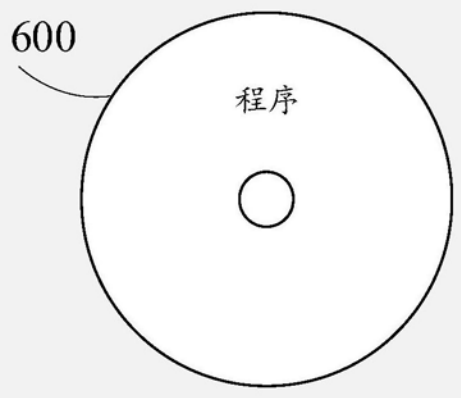


图8