

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 9 月 29 日 (29.09.2016)



(10) 国际公布号
WO 2016/150253 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/072781
- (22) 国际申请日: 2016 年 1 月 29 日 (29.01.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510131608.2 2015 年 3 月 24 日 (24.03.2015) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 蒋武 (JIANG, Wu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

- 关于申请人有权申请并被授予专利(细则 4.17(ii))

[见续页]

(54) Title: SDN-BASED DDOS ATTACK PREVENTION METHOD, DEVICE AND SYSTEM

(54) 发明名称: 基于 SDN 的 DDOS 攻击防护方法、装置及系统

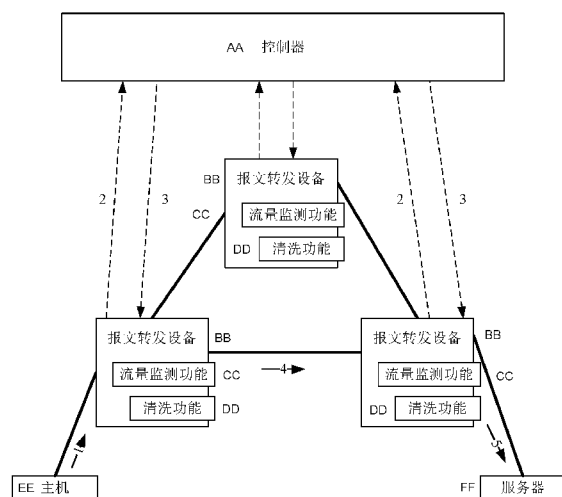


图 9

AA: CONTROLLER
BB: PACKET FORWARDING DEVICE
CC: TRAFFIC MONITORING FUNCTION
DD: CLEANING FUNCTION
EE: HOST
FF: SERVER

(57) Abstract: An SDN-based DDOS attack prevention method, device and system, the method comprising: issuing, via a controller, to a first packet forwarding device a traffic statistic instruction, the traffic statistic instruction instructing the first packet forwarding device to count traffics and carrying a destination IP address; collecting, by the controller, statistic data reported by the first packet forwarding device, the statistic data comprising traffic statistic information flowing to the destination IP address; acquiring, by the controller, and according to the statistic data, a global traffic statistic value flowing to the destination IP address; determining whether the global traffic statistic value exceeds a predetermined threshold, and issuing a DDOS protection policy to a second packet forwarding device based on a determination result indicating that the global traffic statistic value exceeds the predetermined threshold; correspondingly, receiving, by the second packet forwarding device, the DDOS protection policy transmitted by the controller; and protecting, according to the DDOS protection policy, the traffic flowing to the destination IP address, thus reducing a range of an effect of a DDOS attack on a network, and improving network security.

(57) 摘要:

[见续页]

WO 2016/150253 A1

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

一种基于 SDN 的 DDOS 攻击防护方法、装置及系统，通过控制器向第一报文转发设备下发流量统计指令，流量统计指令指示第一报文转发设备进行流量统计，并携带目的地 IP 地址；控制器收集第一报文转发设备上报的统计数据，统计数据包含流向目的地 IP 地址的流量统计信息；控制器根据统计数据，获得流向目的地 IP 地址的全局流量统计值；并判断全局流量统计值是否超过预定阈值，基于全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDOS 防护策略；相应的，第二报文转发设备，接收控制器发送的 DDOS 防护策略；根据 DDOS 防护策略对流向目的地 IP 地址的流量进行防护处理。降低了 DDOS 攻击对网络的影响范围，提高了网络安全性。

基于SDN的DDOS攻击防护方法、装置及系统

本申请要求于 2015 年 3 月 24 日提交中国专利局、申请号为 201510131608.2、发明名称为“基于 SDN 的 DDOS 攻击防护方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术，尤其涉及一种基于软件定义网络 (Software Defined Network, 简称: SDN) 的分布式拒绝服务 (Distributed Denial of Service, 简称: DDOS) 攻击防护方法、装置及系统。

背景技术

图 1 为 DDoS 攻击的示意图。参照图 1，DDoS 的主要实施原理是攻击者利用一级或多级主控主机做跳板，控制大量受感染的受控主机从而组成攻击网络来对受害主机实施大规模的拒绝服务攻击。这种攻击往往能把单个攻击者的攻击效果以级数形式进行放大，从而对受害主机造成重大影响，对网络也会造成严重拥塞。DDoS 利用攻击网络对受害主机发起网间控制报文协议 (Internet Control Messages Protocol, 简称 ICMP) 洪水攻击、同步 (Synchronous, 简称: Syn) 洪水攻击、用户数据报协议 (User Datagram Protocol, 简称: UDP) 洪水攻击等多种攻击形式，使得受害主机消耗大量处理资源来处理这些突增请求而无法响应合法用户请求，从而造成瘫痪。

现有技术中，DDoS 防护方案通常在网络汇聚节点部署清洗设备，通过该清洗设备对汇聚到该节点的 DDoS 攻击流量进行清洗，从而实现 DDoS 防护。其中，网络汇聚节点可以为互联互通网关、国内的城域网出口设备、各类数据中心的出口设备等。但是对于无明显网络汇聚节点的主干网，网络中的节点数量较多，此时，现有技术通常针对特定的 IP 地址部署清洗设备，即在与具有该特定的 IP 地址的主机连接的流量汇聚的节点上部署清洗设备。其中，特定的 IP 地址可以根据客户需求、客户的优先级进行设定的；例如，客户需要保护某个服务器的一个 IP 地址或一段 IP 地址段；则将与该服务器连接的

流量汇聚的节点作为部署清洗设备的节点。

对于上述无明显汇聚节点的主干网场景，虽然采用针对特定 IP 地址部署清洗设备的方式，但是当发生 DDoS 攻击时，无论受害主机的 IP 地址是否为特定 IP 地址，都需要将针对受害主机的 DDoS 攻击流量引流至该清洗设备，导致 IP 地址并非特定 IP 地址的受害主机的流量需要经过网络中的多个路由转发节点才能被引流至该清洗设备。从而占用了这些路由转发节点的网络资源，扩大了 DDoS 攻击对主干网的影响范围，从而降低了网络的安全性。

发明内容

本发明提供一种基于 SDN 的 DDOS 攻击防护方法、装置及系统，用于提高网络安全性。

本发明的第一个方面是提供一种基于软件定义网络 SDN 的分布式拒绝服务 DDoS 攻击防护方法，包括：

控制器向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；

其中，所述流量统计指令携带目的地 IP 地址；

所述控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

所述控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

所述控制器判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略。

结合第一个方面，在第一方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式

持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

结合第一个方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，还包括：

- 5 所述控制器确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值，则所述控制器向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略。

- 10 结合第一个方面或第一个方面的上述任意一种可能的实现方式，在第一方面的第三种可能的实现方式中，在所述控制器向所述第二报文转发设备下发 DDoS 防护策略之前，还包括：

- 15 所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

结合第一个方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，包括：

- 20 所述控制器根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

- 25 所述控制器根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

- 30 结合第一个方面或第一个方面的上述任意一种可能的实现方式，在第五种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗

响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

结合第一个方面的第五种可能的实现方式，在第一个方面的第六种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

在所述控制器向所述第二报文转发设备下发 DDoS 防护策略之前，包括：所述控制器根据所述第一报文转发设备的负载值确定第一引流路径；

其中，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

所述控制器向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第一个方面的第五种可能的实现方式，在第一个方面的第七种可能的实现方式中，在所述控制器向所述第二报文转发设备下发 DDoS 防护策略之前，包括：

所述控制器根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑

关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

所述控制器向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第二个方面是提供一种基于 SDN 的 DDoS 攻击防护方法，所述方法应用于 SDN 系统中，所述 SDN 系统包括控制器和报文转发设备，所述方法由所述报文转发设备执行，包括：

接收所述控制器发送的流量统计指令，所述流量统计指令用于指示所述报文转发设备进行流量统计；

其中，所述流量统计指令携带目的地 IP 地址；

根据所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。

结合第二个方面，在第二个方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述报文转发设备进行所述流量统计的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

结合第二个方面或第二个方面的第一种可能的实现方式，在第二个方面的第二种可能的实现方式中，在所述向所述控制器上报统计数据之后，还包括：

接收所述控制器发送的 DDoS 防护策略；

根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第二个方面的第二种可能的实现方式，在第二个方面的第三种可能的实现方式中，在所述接收所述控制器发送的 DDoS 防护策略之后，还包括：

接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述报文转发设备结束执行所述 DDoS 防护策略；

根据所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第二个方面的第二种可能的实现方式或第二个方面的第三种可能的实现方式，在第二个方面的第四种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述报文转发设备在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

结合第二个方面的第四种可能的实现方式，在第二个方面的第五种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理，具体为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第二个方面的第四种可能的实现方式，在第二个方面的第六种可能的实现方式中，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

则所述根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理，具体为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第三个方面是提供一种控制器，包括：

发送模块，用于向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；其中，所述流量统计指

令携带目的地 IP 地址;

接收模块, 用于收集所述第一报文转发设备根据所述发送模块发送的所述流量统计指令上报的统计数据, 所述统计数据包含流向所述目的地 IP 地址的流量统计信息;

5 处理模块, 用于:

根据所述接收模块接收到的所述统计数据, 获得流向所述目的地 IP 地址的所述全局流量统计值;

其中, 所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后, 获得的用于反
10 映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值;

判断所述全局流量统计值是否超过预定阈值;

所述发送模块, 还用于基于处理模块确定的全局流量统计值超过预定阈值的判断结果, 向第二报文转发设备下发 DDoS 防护策略。

结合第三个方面, 在第三个方面的第一种可能的实现方式中, 所述流量
15 统计指令还携带: 检测起始时刻;

其中, 所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻, 所述流量统计被所述第一报文转发设备以检测周期的方式持续执行, 所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器;

20 所述处理模块, 还用于:

确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值;

所述发送模块, 还用于基于所述处理模块确定的至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值的结果, 向所述第二报文转发
25 设备下发防护消除指示消息;

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略。

结合第三个方面或第三个方面的第一种可能的实现方式, 在第三个方面的第二种可能的实现方式中, 所述处理模块, 在所述发送模块向所述第二报
30 文转发设备下发 DDoS 防护策略之前, 还用于:

根据所述接收模块接收的所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

结合第三个方面的第二种可能的实现方式，在第三个方面的第三种可能的实现方式中，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；

所述处理模块，还用于根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，具体为：

根据所述接收模块接收的所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

结合第三个方面或第三个方面的上述任意一种可能的实现方式，在第三个方面的第四种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述第二报文转发设备将流向所述

目的地 IP 地址的流量发送到清洗设备上进行处理。

结合第三个方面的第四种可能的实现方式，在第三个方面的第五种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

所述处理模块，在所述发送模块向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述第一报文转发设备的负载值确定第一引流路径，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述发送模块根据所述处理模块确定的所述第一引流路径，向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第三个方面的第四种可能的实现方式，在第三个方面的第六种可能的实现方式中，所述处理模块，在所述发送模块向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

则所述发送模块根据所述处理模块确定的所述第二引流路径，向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第四个方面是提供一种报文转发设备，所述报文转发设备应用于 SDN 系统中，所述 SDN 系统包括控制器和所述报文转发设备，所述报文转发设备，包括：

接收模块，用于接收所述控制器发送的流量统计指令，所述流量统计指令用于指示处理模块进行流量统计；其中，所述流量统计指令携带目的地 IP 地址；

所述处理模块，用于根据所述接收模块接收的所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

发送模块，用于根据所述处理模块统计的所述流向所述目的地 IP 地址的流量统计信息，向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。

结合第四个方面，在第四个方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述处理模块进行所述流量统计的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

结合第四个方面或第四个方面的第一种可能的实现方式，在第四个方面的第二种可能的实现方式中，所述接收模块，在所述发送模块向所述控制器上报统计数据之后，还用于：

接收所述控制器发送的 DDoS 防护策略；

所述处理模块，还用于根据所述接收模块接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第四个方面的第二种可能的实现方式，在第四个方面的第三种可能的实现方式中，所述接收模块，在所述接收所述控制器发送的 DDoS 防护策略之后，还用于：

接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述处理模块结束执行所述 DDoS 防护策略；

所述处理模块，还用于根据所述接收模块接收的所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第四个方面的第一种可能的实现方式或第四个方面的第二种可能的实现方式，在第四个方面的第四种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述处理模块通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址

的流量进行防护处理，具体为：根据所述接收模块接收的所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述处理模块对所述流向所述目的地 IP 地址的流量进行限流处理；

- 5 则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块接收的所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述处理模块对所述流向所述目的地 IP 地址的流量进行限速处理；

- 10 则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块接收的所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述处理模块对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

- 15 则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块接收的所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述处理模块在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

- 20 则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块接收的所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述处理模块将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；

- 25 则所述处理模块根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块接收的所述动态引流清洗响应策略指示所述发送模块将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理。

- 30 结合第四个方面的第四种可能的实现方式，在第四个方面的第五种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；所

述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报
5 文转发设备和所述清洗设备；

则所述处理模块根据所述接收模块接收的所述动态引流清洗响应策略指示所述发送模块将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述接收模块接收的所述动态引流清洗响应策略，指示所述发送模
10 块将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第四个方面的第四种可能的实现方式，在第四个方面的第六种可能的实现方式中，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过
15 所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

则所述处理模块根据所述接收模块接收的所述动态引流清洗响应策略指示所述发送模块将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述接收模块接收的所述动态引流清洗响应策略，指示所述发送模
20 块将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第五个方面是提供一种 SDN 系统，包括：控制器、第一报文转发设备和第二报文转发设备；

25 其中，所述控制器，用于：

向所述第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；所述流量统计指令携带目的地 IP 地址；

收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所
30 述统计数据包含流向所述目的地 IP 地址的流量统计信息；

根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

5 判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向所述第二报文转发设备下发 DDoS 防护策略；

所述第一报文转发设备，用于：

接收所述控制器发送的所述流量统计指令；

10 根据所述流量统计指令统计所述流向所述目的地 IP 地址的流量统计信息；

向所述控制器上报所述统计数据；

所述第二报文转发设备，用于：

接收所述控制器发送的所述 DDoS 防护策略；

15 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第五个方面，在第五个方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

20 其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

结合第五个方面的第一种可能的实现方式，在第五个方面的第二种可能的实现方式中，所述控制器，还用于：

25 确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略；

所述第二报文转发设备，还用于：

30 接收所述防护消除指示消息；

结束执行所述 DDoS 防护策略。

结合第五个方面或第五个方面的上述任意一种可能的实现方式，在第五个方面的第三种可能的实现方式中，所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

- 5 根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

结合第五个方面的第三种可能的实现方式，在第五个方面的第四种可能的实现方式中，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；

- 10 所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，具体为：

根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

- 15 所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

- 20 结合第五个方面或第五个方面的上述任意一种可能的实现方式，在第五个方面的第五种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对流向所述目的地 IP 地址的流量进行报文丢弃处理；

- 25 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述黑洞路由响应策略采用黑洞路由对流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限流处理；

- 30 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP

地址的流量进行防护处理，具体为：根据所述限流响应策略对流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限速处理；

5 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限速响应策略对流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行报文丢弃处理；

10 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述丢弃响应策略对流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理；

15 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述本地清洗响应策略对流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述第二报文转发设备将流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；

20 则所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述动态引流清洗响应策略将流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

结合第五个方面的第五种可能的实现方式，在第五个方面的第六种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

25 所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述第一报文转发设备的负载值确定第一引流路径，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

30 向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响

应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；

所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：

将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第五个方面的第五种可能的实现方式，在第五个方面的第七种可能的实现方式中，所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；

所述第二报文转发设备根据所述 DDoS 防护策略对流向所述目的地 IP 地址的流量进行防护处理，具体为：

将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第六个方面是提供一种控制器，包括：处理器、存储器、收发器和总线；

其中，所述收发器，包括：南向接口单元；

所述南向接口单元，用于：

向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；其中，所述流量统计指令携带目的地 IP 地址；

收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

处理器，用于：

根据所述接收模块接收到的所述统计数据，获得流向所述目的地 IP 地址的所述全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

判断所述全局流量统计值是否超过预定阈值；

所述南向接口单元，还用于基于处理器确定的全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略；

所述存储器，用于存储所述统计数据、所述 DDoS 防护策略。

结合第六个方面，在第六个方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器；

所述处理器，还用于：

确定在至少两个检测周期内所述全局流量统计值未超过所述预定阈值；

所述南向接口单元，还用于基于所述处理器确定的至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值的结果，向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述报文转发设备结束执行所述 DDoS 防护策略。

结合第六个方面或第六个方面的第一种可能的实现方式，在第六个方面的第二种可能的实现方式中，所述处理器在所述南向接口单元向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述南向接口单元接收的所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

所述南向接口单元，还用于向所述第二报文转发设备下发 DDoS 防护策

略。

结合第六个方面的第二种可能的实现方式，在第六个方面的第三种可能的实现方式中，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；

- 5 所述处理器，根据所述南向接口单元接收的所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，具体为：

根据所述南向接口单元接收的所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

- 10 所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

- 15 结合第六个方面或第六个方面的上述任意一种可能的实现方式，在第六个方面的第四种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对流向所述目的地 IP 地址的流量进行报文丢弃处理；

- 20 所述限流响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行限速处理；

- 25 所述丢弃响应策略用于指示所述第二报文转发设备对流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述第二报文转发设备将流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

- 30 结合第六个方面的第四种可能的实现方式，在第六个方面的第五种可能

的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

所述处理器，在所述南向接口单元向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述第一报文转发设备的负载值确定第一引流路径；

5 其中，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述南向接口单元根据所述处理器确定的所述第一引流路径，向所述第二报文转发设备下发的 DDoS 防护策略为动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过
10 所述第一引流路径发送到所述清洗设备上进行处理。

结合第六个方面的第四种可能的实现方式，在第六个方面的第六种可能的实现方式中，所述处理器，在所述南向接口单元向所述第二报文转发设备
15 下发 DDoS 防护策略之前，还用于：

根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

则所述南向接口单元根据所述处理器确定的所述第二引流路径，向所述第二报文转发设备下发 DDoS 防护策略为动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过
20 所述第二引流路径发送到所述清洗设备上进行处理。

本发明的第七个方面是提供一种报文转发设备，所述报文转发设备应用于 SDN 系统中，所述 SDN 系统包括控制器和所述报文转发设备，所述报文转发设备，包括：处理器、存储器、收发器和总线；
25

其中，所述收发器，包括：北向接口单元；

所述北向接口单元，用于接收所述控制器发送的流量统计指令，所述流量统计指令用于指示处理模块进行流量统计；其中，所述流量统计指令携带
30 目的地 IP 地址；

所述处理器，用于根据所述北向接口单元接收的所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

所述北向接口单元，还用于根据所述处理器统计的所述流向所述目的地 IP 地址的流量统计信息，向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息；

所述存储器，用于存储所述流量统计指令和所述流向所述目的地 IP 地址的流量统计信息。

结合第七个方面，在第七个方面的第一种可能的实现方式中，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述处理器进行所述流量统计的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

结合第七个方面或第七个方面的第一种可能的实现方式，在第二种可能的实现方式中，所述北向接口单元，在向所述控制器上报统计数据之后，还用于接收所述控制器发送的 DDoS 防护策略；

所述处理器，还用于根据所述北向接口单元接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第七个方面的第二种可能的实现方式，在第七个方面的第三种可能的实现方式中，

所述北向接口单元，在接收所述控制器发送的 DDoS 防护策略之后，还用于：

接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述处理器结束执行所述 DDoS 防护策略；

所述处理器，还用于根据所述北向接口单元接收的所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

结合第七个方面的第一种可能的实现方式或第七个方面的第二种可能的实现方式，在第七个方面的第四种可能的实现方式中，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述处理器通过配置黑洞路由对

所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

所述限流响应策略用于指示所述处理器对所述流向所述目的地 IP 地址的流量进行限流处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理;

所述限速响应策略用于指示所述处理器对所述流向所述目的地 IP 地址的流量进行限速处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理;

所述丢弃响应策略用于指示所述处理器对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

所述本地清洗响应策略用于指示所述处理器在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

所述动态引流清洗响应策略用于指示所述处理器将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理;

则所述处理器根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元接收的所述动态引流清洗响应策略指示所述北向接口单元将所述流向所述目的地 IP 地址的流量发送

到所述清洗设备上进行处理。

结合第七个方面的第四种可能的实现方式，在第七个方面的第五种可能的实现方式中，所述统计数据还包含：所述第一报文转发设备的负载值；

所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流
5 路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述处理器根据所述北向接口单元接收的所述动态引流清洗响应策略
10 指示所述北向接口单元将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述北向接口单元接收的所述动态引流清洗响应策略，指示所述北向接口单元将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

结合第七个方面的第四种可能的实现方式，在第七个方面的第六种可能的实现方式中，所述动态引流清洗响应策略包含第二引流路径指示信息，所述
15 第二引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

则所述处理器根据所述北向接口单元接收的所述动态引流清洗响应策略
20 指示所述北向接口单元将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述北向接口单元接收的所述动态引流清洗响应策略，指示所述北向接口单元将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送
25 到所述清洗设备上进行处理。

本发明实施例提供的基于 SDN 的 DDOS 攻击防护方法、装置及系统，通过控制器向所述第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；所述流量统计指令携带目的地 IP 地址；控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计
30 数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；控制器

根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；并判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向所述第二报文转发设备下发 DDoS 防护策略；相应的，所述第一报文转发设备接收所述控制器发送的所述流量统计指令；并根据所述流量统计指令统计所述流向所述目的地 IP 地址的流量统计信息；最终向所述控制器上报所述统计数据；相应的，所述第二报文转发设备，接收所述控制器发送的所述 DDoS 防护策略；根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

10

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图做一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

15

图 1 为 DDoS 攻击的示意图；

图 2 为本发明实施例提供的一种基于 SDN 网络的 DDoS 攻击防护系统部署示意图；

20

图 3 为本发明实施例提供的一种 SDN 系统的部署示意图；

图 4 为本发明实施例提供的一种控制器的结构示意图；

图 5 为本发明实施例提供的一种报文转发设备的结构示意图；

图 6 为本发明实施例提供的一种独立的调度设备的结构示意图；

图 7 为本发明实施例提供的一种控制器的结构示意图；

25

图 8 为本发明实施例提供的另一种报文转发设备的结构示意图；

图 9 为本发明实施例提供的一种基于 SDN 的 DDOS 攻击防护方法的流程图示意图；

图 10 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图示意图；

30

图 11 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的

流程图;

图 12 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图;

图 13 为攻击路径及最近攻击源头判定示意图;

5 图 14 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图

图 15 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图;

10 图 16 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图;

图 17 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图;

图 18 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图;

15 图 19 为本地清洗处理流程图;

图 20 为本发明实施例提供的一种基于 SDN 的 DDoS 攻击防护方法的交互流程图;

图 21 为本发明实施例提供的另一种基于 SDN 网络的 DDoS 攻击防护方法的交互示意图。

20

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于
25 本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

本发明提供了一种基于 SDN 的 DDoS 攻击防护的技术方案。SDN 中的控制器指示报文转发设备进行基于目的 IP 的流量统计,通过控制器收集报文转发设备的统计数据,并判定是否发生网络攻击;若判断发生攻击,本方案提
30 供多种可能的 DDoS 防护方式。例如,由于 SDN 支持网络拓扑、状态的集中

管理，控制器具有感知全局拓扑的能力，因此控制器能够获知哪些报文转发设备用于与其他网络连接，即获知哪些报文转发设备位于 SDN 的边界；从而指示位于 SDN 边界靠近攻击源的报文转发设备对攻击流量进行限流或丢弃或阻断，或者，控制器指示将疑似攻击流量引流至专业的清洗设备，对该疑似攻击流量进行清洗，从而降低攻击流量在对网络影响。

图 2 为本发明实施例提供的一种基于 SDN 网络的 DDoS 攻击防护系统部署示意图。参照图 2，该系统包括：报文转发设备、控制器、清洗设备。

其中，控制器通过南向接口与报文转发设备及清洗设备进行通信，南向接口可以为 Open Flow 协议、转发件和控制件的分离（Forwarding and Control Element Separation，简称：ForCES）协议、路径计算件（Path Computation Element-Communication Protocol，简称：PCE-P）协议等。

可选的，当 SDN 中只有一个控制器时，该控制器可以具有控制器调度功能，控制器调度功能用于对整个 SDN 中的报文转发设备进行管控与调度，包括链路发现、拓扑管理、策略制定、表项下发等功能。

或者，对于 SDN 中多个控制器组成的集群，可以将控制器调度功能单独设置在一个独立的调度设备上，例如在多个控制器中选举一个控制器作为主控制器，该主控制器既可以作为该独立的调度设备，由该主控制器通过东西向接口与各个控制器进行通信。该主控制器主要负责生成和维护全网范围内副控制器、报文转发设备及清洗设备的状态信息，一旦出现失效，则从集群的其他副控制器中选举一个成为新的主控制器。并且控制器的集群对报文转发设备及清洗设备是透明的，即在 SDN 的运行过程中，报文转发设备及清洗设备无需关心其接收的是哪一台控制器发来的命令，同时在其向控制器发送数据包时，能保持之前单一控制器的操作方式，从而保证控制器在逻辑上的集中。目前，用于多个控制器以及调度设备之间沟通和联系的东西向接口还未具有明确的定义标准，通常可以利用现有成熟的集群技术，例如服务器集群技术，来实现东西向接口的通信。

进一步的，控制器可以装载 DDoS 控制程序，控制器执行 DDoS 控制程序以实现上述 DDoS 防护方案的相关配置，可选的，该 DDoS 控制程序还可以装载在其他用户设备上，用户通过用户设备的应用调用 DDoS 控制程序，用户设备执行 DDoS 控制程序，并与控制器进行交互，以实现上述 DDOS 防

护方案的相关配置。其中，控制器与用户设备通过控制器的北向接口进行通信。需要说明的是，北向接口的协议制定基于不同的需求可以有多种方案。例如应用编程接口 (REST Application Programming Interface, 简称: REST API) 就是一种常用的北向接口形式。部分传统的网络设备厂商在其现有设备上提
5 供了编程接口供业务应用直接调用，也可被视作是北向接口，其目的是在不改变其现有设备架构的条件下提升配置管理灵活性，应对开放协议的竞争。

报文转发设备可以是转发器，也可以为传统网络中的交换机、路由器、防火墙等设备，该报文转发设备具有流量监测功能和清洗功能。

其中，报文转发设备的流量监测功能用于基于控制器下发的流量统计指令对流经该报文转发设备的流量进行监控，该流量统计指令携带目的地 IP 地址，该目的地 IP 地址可以为需要保护的某个服务器的一个 IP 地址或一段 IP 地址段；而报文转发设备的流量监测功能会检测流向所述目的地 IP 地址的流量统计信息，并将统计数据上报给控制器。
10

报文转发设备的清洗功能用于当控制器下发攻击防护策略时，例如 DDoS 防护策略，基于攻击防护策略对疑似攻击流量进行清洗处理，剔除其中可疑的攻击流量。
15

另外，基于不同的攻击防护策略，报文转发设备可以进行流量的限流或丢弃或阻断；或者，将疑似攻击流量引流至清洗设备。

需要说明的是，对于本发明实施例提供的方案，在网络攻击防护过程中，
20 基于不同环节的不同功能，可以将报文转发设备划分成两类：第一报文转发设备和第二报文转发设备。

其中，第一报文转发设备具有流量监测功能，SDN 系统的全部报文转发设备都可以作为第一报文转发设备；第二报文转发设备具有清洗功能。例如，为了有效的对疑似攻击流量进行防护处理，控制器会指示位于 SDN 边界靠近攻击源的报文转发设备对攻击流量进行防护处理，对于这种场景，位于 SDN
25 边界靠近攻击源的报文转发设备即为上述第二报文转发设备；通常情况下，第二报文转发设备也会具有流量监测功能，即第一报文转发设备和第二报文转发设备可以为同一个实体设备，也可以为不同的实体设备。

清洗设备，用于接收报文转发设备引流的疑似攻击流量，并对该疑似攻击流量进行清洗，并将清洗后的流量回注到 SDN 中。
30

需要说明的是，本发明实施例提供的引流方案与现有的引流方案相比，优势在于：由于 SDN 中控制器具有链路发现和拓扑管理的功能，因此，在采用引流方案时，控制器可以根据 SDN 拓扑关系或统计数据配置第二报文转发设备采用对 SDN 网络冲击最小的路径，将疑似攻击流量引流至清洗设备。例如，选择距离清洗设备最近的路径进行引流；或者，选择负载较小的路径进行引流；从而降低了现有技术中由于引流而增加的攻击影响。即，本发明提供的引流方案可以基于 SDN 的链路状况随时进行动态调整，故在下文中将这种方案对应的策略命名为动态引流清洗响应策略。

进一步的，图 3 为本发明实施例提供的一种 SDN 系统的部署示意图，参照图 3，该 SDN 系统，包括：控制器、第一报文转发设备和第二报文转发设备；

其中，所述控制器，用于：

向所述第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；所述流量统计指令携带目的地 IP 地址；

收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向所述第二报文转发设备下发 DDoS 防护策略；

所述第一报文转发设备，用于：

接收所述控制器发送的所述流量统计指令；

根据所述流量统计指令统计所述流向所述目的地 IP 地址的流量统计信息；

向所述控制器上报所述统计数据；

所述第二报文转发设备，用于：

接收所述控制器发送的所述 DDoS 防护策略；

根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

本发明实施例提供的 SDN 系统，通过控制器向所述第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；所述流量统计指令携带目的地 IP 地址；控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；并判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向所述第二报文转发设备下发 DDoS 防护策略；相应的，所述第一报文转发设备接收所述控制器发送的所述流量统计指令；并根据所述流量统计指令统计所述流向所述目的地 IP 地址的流量统计信息；最终向所述控制器上报所述统计数据；相应的，所述第二报文转发设备，接收所述控制器发送的所述 DDoS 防护策略；根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

可选的，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

进一步的，控制器需要一种判断网络攻击是否停止的机制，一种可能的实现方式为：

确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略；

所述第二报文转发设备，还用于：

接收所述防护消除指示消息；

结束执行所述 DDoS 防护策略。

可选的，控制器还可以针对位于 SDN 边界靠近攻击源的报文转发设备下发 DDoS 防护策略，一种可能的实现方式为：

所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

- 5 根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

具体的，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，具体为：

- 10 根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

- 15 所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

- 20 具体的，对上述响应策略进行说明。黑洞（black hole）路由指报文转发设备的访问控制列表（Access Control List，简称：ACL）中的不指向任何下一跳的路由表项。与通常的路由表项类似，黑洞路由也包括匹配项和动作。与黑洞路由的匹配项相匹配的报文将被指报文转发设备丢弃，而不会被转发至下一跳。黑洞路由中的动作可以通过多种方式来实现，例如路由设备将报
25 文转发至以 0.0.0.0 为例的非法 IP 地址、或回环地址，也可以通过 null0 接口来实现。该 null0 为路由设备上的一个逻辑接口，null0 接口总是处于“上（Up）”状态，但不转发任何报文。报文转发设备将报文转发至该报文转发设备的 null0 接口，null0 接口接收到报文后，将报文丢弃。基于黑洞路由的上述特点，当
30 发生网络攻击时，控制器可以配置相应的黑洞路由响应策略，并将黑洞路由响应策略下发给报文转发设备，所述黑洞路由响应策略用于指示所述第二报

文转发设备通过配置黑洞路由对流向所述目的地 IP 地址的流量进行报文丢弃处理，从而实现 DDoS 攻击防护。具体的，黑洞路由响应策略可以包含：目的地 IP 地址、报文支持的协议类型等信息。

则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

由于，第二报文转发设备中设置黑洞路由可以实现对报文丢弃，并且无需指明丢弃的原因，可以化简处理攻击流量的复杂度，提高处理效率。

所述限流响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；具体的：第二报文转发设备基于限流响应策略对单位时间内报文的收发带宽进行限制，比如每秒最多发送多少字节的报文。该限流响应策略可以包含：目的地 IP 地址、报文支持的协议类型、报文的五元组信息等；报文转发设备可以基于报文的五元组信息进行上述限制，例如，针对传输控制协议（Transmission Control Protocol，简称：TCP）报文和/或用户数据报协议（User Datagram Protocol，简称：UDP）报文进行上述限制，针对特定的报文的源端口进行上述限制，针对特定的报文的端口进行上述限制，设置特定的速率上限对报文的传输速率进行限制等。

则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理；例如，第二报文转发设备基于限速响应策略设置收发带宽的大小。

则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；具体的：第二报文转发设备基于丢弃响应策略对接收到的疑似网络攻击流量的报文或准备发送的疑似网络攻击流量的报文进行丢弃。该丢弃响应策略可以包含：目的地 IP 地址、报文支持的协

议类型、报文的五元组信息等；该报文的五元组信息可以包含：报文的 TCP 信息或报文的 UDP 信息，报文的源端口信息，报文的端口信息，坏包(drop packet) 信息等。

5 则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；具体的，所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行
10 清洗处理；第二报文转发设备基于本地清洗响应策略在本地对接收到的疑似网络攻击流量的报文或准备发送的疑似网络攻击流量的报文进行清洗处理，可选的，该本地清洗响应策略可以包括：目的地 IP 地址、报文支持的协议类型、报文的五元组信息等；

则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地
15 地 IP 地址的流量进行防护处理，具体为：根据所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；可选的，动态引流清洗响应策略可以包含目的地 IP 地址和引流路径指示信息；

20 则所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

对于所述动态引流清洗响应策略，在所述南向接口单元下发动态引流清洗响应策略之前，需要控制器确定一条对网络冲击最小的路径来进行流量的
25 引流，下面给出几种可能的实现方式进行说明：

方式一：所述统计数据还包含：所述第一报文转发设备的负载值；

所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述第一报文转发设备的负载值确定第一引流路径，所述第一引流
30 路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第

一引流路径包含所述第二报文转发设备和所述清洗设备；

向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；

所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：

将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

方式二：，所述控制器，在所述向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；

所述第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：

将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

在图 2 和图 3 的基础上，下面分别对基于 SDN 网络的 DDOS 攻击防护系统中的各个节点进行说明。

图 4 为本发明实施例提供的一种控制器的结构示意图，参照图 4，该控制器包括：处理器 10、存储器 11、收发器 12 和总线 13；

其中，收发器 12，包括：北向接口单元 12a、南向接口单元 12b、东西向接口单元 12c；

处理器 10，用于执行 DDoS 控制程序获得 DDoS 防护配置参数，并基于 DDoS 防护配置参数指示南向接口单元 12b 与报文转发设备及清洗设备进行交

互, 以实现上述 DDoS 防护方案的相关配置, 例如, DDoS 防护配置参数为目的
的地 IP 地址, 处理器 10 指示该南向接口单元 12b 向第一报文转发设备下发流
量统计指令, 该流量统计指令携带目的地 IP 地址; 该南向接口单元 12b 接收
所述第一报文转发设备发送的统计数据, 所述统计数据包含流向所述目的地
5 IP 地址的流量统计信息;

需要说明的是, DDoS 防护配置参数可以通过北向接口单元 12a 从用户设
备处获得。

进一步的, 处理器 10 根据所述南向接口单元 12b 接收的所述统计数据,
获得流向所述目的地 IP 地址的所述全局流量统计值; 判断所述全局流量统计
10 值是否超过预定阈值;

其中, 所述全局流量统计值表示所述控制器对包括所述第一报文转发设
备在内的至少两个报文转发设备上报的统计数据进行汇总后, 获得的用于反
映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值;

进一步的, 若发生网络攻击, 则基于所述全局流量统计值超过预定阈值
15 的判断结果, 处理器 10 指示所述南向接口单元 12b 向第二报文转发设备发送
DDoS 防护策略。

可选的, 当控制器具有上文所述控制器调度功能时, 处理器 10 直接指示
南向接口单元 12b 与报文转发设备及清洗设备进行交互, 以实现上述 DDoS
防护方案的相关配置; 若系统中还包含上文所述独立的调度设备, 则处理器
20 10 指示东西向接口单元 12c 与独立的调度设备进行交互, 以实现上文所述控
制器调度功能的相关配置。需要说明的是, 北向接口单元 12a 和东西向接口
单元 12c 为可选单元: 对于能够自行执行 DDoS 控制程序的控制器来说, 可
以不设置北向接口单元 12a; 对于具有上文所述控制器调度功能的控制器来
说, 可以不设置东西向接口单元 12c。

25 存储器 11, 用于存储 DDoS 防护配置参数、DDoS 控制程序和第一报文
转发设备上报的统计数据、DDoS 防护策略等, 以便处理器 10 在进行相应操
作时进行调用。

本发明实施例提供的控制器, 通过处理器指示南向接口单元向第一报文
转发设备下发流量统计指令, 所述流量统计指令用于指示所述第一报文转发
30 设备进行流量统计; 其中, 所述流量统计指令携带目的地 IP 地址; 南向接口

单元接收所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；处理器根据所述南向接口单元接收的所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；处理器判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，处理器指示所述南向接口单元向所述第二报文转发设备下发 DDoS 防护策略。降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

可选的，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

进一步的，控制器需要一种判断网络攻击是否停止的机制，一种可能的实现方式为：

所述处理器 10，还用于确定在至少两个检测周期内所述全局流量统计值未超过所述预定阈值；

所述南向接口单元 12b，还用于基于所述处理器 10 确定的至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值的结果，向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略。

可选的，控制器还可以针对位于 SDN 边界靠近攻击源的报文转发设备下发 DDoS 防护策略，一种可能的实现方式为：

在所述南向接口单元 12b 向所述第二报文转发设备下发 DDoS 防护策略之前，所述处理器 10，还用于根据所述南向接口单元 12b 接收的所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

所述南向接口单元 12b，还用于向所述第二报文转发设备下发 DDoS 防护

策略。

具体的，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；所述处理器 10 根据所述南向接口单元 12b 接收的所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；所述处理器 10 根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；控制器下发响应指令如流向 3 所示。

对于所述动态引流清洗响应策略，在所述南向接口单元 12b 下发动态引流清洗响应策略之前，需要控制器确定一条对网络冲击最小的路径来进行流量的引流，下面给出几种可能的实现方式进行说明：

方式一：所述统计数据还包含：所述第一报文转发设备的负载值；

所述处理器 10，用于根据所述第一报文转发设备的负载值确定第一引流路径；

其中，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述南向接口单元 12b 根据所述处理器 10 确定的所述第一引流路径，向所述第二报文转发设备下发动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

方式二：所述处理器 10，用于根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

所述南向接口单元 12b 根据所述处理器 10 确定的所述第二引流路径，向所述报文转发设备下发动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

进一步的，对于控制器与独立的调度设备之间的交互，下面以副控制器与主控制器作为示例进行说明，其中主控制器与副控制器协作实现攻击防护方案可以有两种可能的实现方式。

方式一：主控制器获得 SDN 中全部的副控制器、报文转发设备及清洗设备的工作情况。各个副控制器周期性地通过南向接口单元与第一报文转发设备进行交互获得统计数据，各个副控制器再将采集回来的统计数据通过各自的东西向接口单元发送给主控制器，再由主控制器汇总处理后获得全局流量统计值，并根据该全局流量统计值判断是否发生网络攻击。主控制器与副控制器进行协商制定一致的网络攻击防护策略，例如 DDoS 防护策略，并由副控制器通过南向接口单元将该网络攻击防护策略统一下发给第二报文转发设备。

方式二：由主控制器选择空闲的副控制器完成攻击防护方案，例如，主控制器通过东西向接口单元与某副控制器进行交互，由主控制器指示该副控制器负责完成攻击防护方案。则该副控制器周期性地通过南向接口单元与第一报文转发设备进行交互获得统计数据，该副控制器再将采集回来的统计数据汇总处理后，获得全局流量统计值，并根据该全局流量统计值判断是否发生网络攻击，并由该副控制器通过南向接口单元将网络攻击防护策略统一下发给第二报文转发设备。

图 5 为本发明实施例提供的一种报文转发设备的结构示意图，该报文转发设备在流量统计过程中为上述第一报文转发设备，在执行 DDoS 防护策略的过程中，为上述第二报文转发设备；参照图 5，该报文转发设备包括：处理器 20、存储器 21、收发器 22 和总线 23；

其中，收发器 22 包括：北向接口单元 22a；

首先，当该报文转发设备作为第一报文转发设备时，其具有如下功能：

该北向接口单元 22a 与控制器的南向接口单元 12b 连接，用于接收控制

器针对 DDoS 攻击配置的相关参数,例如流量统计指令,该流量统计指令携带目的地 IP 地址,用于指示处理器 20 进行流量统计;向控制器上报针对 DDoS 攻击检测的相关数据,例如统计数据,该统计数据包含流向所述目的地 IP 地址的流量统计信息;

- 5 处理器 20,用于根据所述北向接口单元 22a 接收的流量统计指令对流向该目的地 IP 地址的流量进行统计,获得流向所述目的地 IP 地址的流量统计信息。

存储器 21,用于存储控制器针对 DDoS 攻击配置的相关参数、统计数据等。

- 10 本发明实施例提供的第一报文转发设备,通过该北向接口单元接收控制器针对 DDoS 攻击配置的相关参数,例如流量统计指令,该流量统计指令携带目的地 IP 地址,用于指示处理器进行流量统计;进一步的,处理器根据所述北向接口单元接收的流量统计指令对流向该目的地 IP 地址的流量进行统计,获得流向所述目的地 IP 地址的流量统计信息。北向接口单元向控制器上
15 报针对 DDoS 攻击检测的相关数据,例如统计数据,该统计数据包含流向所述目的地 IP 地址的流量统计信息;由于第一报文转发设备针对流向该目的地 IP 地址的流量进行流量统计,并将统计数据上报给控制器,使得控制器能够基于该统计数据判断是否发生 DDoS 攻击,从而触发相应的 DDoS 防护策略;从而降低了 DDoS 攻击对网络的影响范围,提高了网络安全性。

- 20 可选的,所述流量统计指令还携带:检测起始时刻;

其中,所述检测起始时刻用于告知所述处理器 20 进行所述流量统计的起始时刻,以检测周期的方式持续进行所述流量统计,以所述检测周期上报所述统计数据给所述控制器。

- 25 继续参照图 5,当该报文转发设备作为第二报文转发设备时,其具有如下功能:

所述北向接口单元 22a,在向所述控制器上报统计数据之后,还用于:
接收所述控制器发送的 DDoS 防护策略;

所述处理器 20,还用于根据所述北向接口单元 22a 接收的所述 DDoS 防护策略,对所述流向所述目的地 IP 地址的流量进行防护处理。

- 30 本实施例提供的第二报文转发设备,在北向接口单元向所述控制器上报

统计数据之后，通过北向接口单元接收所述控制器发送的 DDoS 防护策略，并由处理器根据所述北向接口单元接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理，实现了对流向所述目的地 IP 地址的流量的 DDoS 防护，从而降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

需要说明的是，对于 SDN 中的报文转发设备，有一些报文转发设备同时具有第一报文转发设备和第二报文转发设备的功能，这些报文转发设备往往为能够将执行 DDoS 防护策略的防护效果最大化的报文转发设备，例如，位于 SDN 边界靠近攻击源的报文转发设备；另一些报文转发设备仅具有第一报文转发设备的功能，例如，并不位于 SDN 边界的报文转发设备；当然，根据 SDN 具体的部署和网络攻击发生时的具体情况，控制器可以根据需求配置 SDN 中的报文转发设备具有第一报文转发设备和/或第二报文转发设备的功能，本发明实施例并不予以限制。

进一步的，对应控制器判断网络攻击是否停止的机制，第二报文转发设备侧相应的功能如下：

所述北向接口单元 22a，在接收所述控制器发送的 DDoS 防护策略之后，还用于：

接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述处理器 20 结束执行所述 DDoS 防护策略；

所述处理器 20，还用于根据所述北向接口单元 22a 接收的所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述处理器 20 通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述北向接口单元 22a 接收的所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述处理器 20 对所述流向所述目的地 IP 地址的流量进行限流处理;

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元 22a 接收的所述限流
5 响应策略对所述流向所述目的地 IP 地址的流量进行限流处理;

所述限速响应策略用于指示所述处理器 20 对所述流向所述目的地 IP 地址的流量进行限速处理;

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元 22a 接收的所述限速
10 响应策略对所述流向所述目的地 IP 地址的流量进行限速处理;

所述丢弃响应策略用于指示所述处理器 20 对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元 22a 接收的所述丢弃
15 响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

所述本地清洗响应策略用于指示所述处理器 20 在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元 22a 接收的所述本地
20 清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

所述动态引流清洗响应策略用于指示所述处理器 20 将所述流向所述目的地 IP 地址的流量发送到清洗设备上清洗处理;

则所述处理器 20 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理, 具体为: 根据所述北向接口单元 22a 接收的所述动态
25 引流清洗响应策略指示所述北向接口单元 22a 将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上清洗处理。

对于所述动态引流清洗响应策略, 在所述控制器下发动态引流清洗响应策略之前, 需要控制器确定一条对网络冲击最小的路径来进行流量的引流, 第二报文转发设备侧相应的功能如下:

30 方式一:

所述统计数据还包含：所述第一报文转发设备的负载值；

所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文
5 转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

其中，报文转发设备为第二报文转发设备。

则所述处理器 20 根据所述北向接口单元 22a 接收的所述动态引流清洗响应策略指示所述北向接口单元 22a 将所述流向所述目的地 IP 地址的流量发送
10 到所述清洗设备上进行处理，具体为：

根据所述北向接口单元 22a 接收的所述动态引流清洗响应策略，指示所述北向接口单元 22a 将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

方式二：

15 所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

其中，报文转发设备为第二报文转发设备。

20 则所述处理器 20 根据所述北向接口单元 22a 接收的所述动态引流清洗响应策略指示所述北向接口单元 22a 将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述北向接口单元 22a 接收的所述动态引流清洗响应策略，指示所述北向接口单元 22a 将所述流向所述目的地 IP 地址的流量通过所述第二引流
25 路径发送到所述清洗设备上进行处理。

图 6 为本发明实施例提供的一种独立的调度设备的结构示意图，参照图 6，该独立的调度设备包括：处理器 30、存储器 31、收发器 32 和总线 33；

其中，收发器 32 包括：东西向接口单元 32a；

进一步的，该独立的调度设备可以具有两种可能的实现方式，下面分别
30 对两种方式进行说明。

方式一:

该独立的调度设备的東西向接口单元 32a 与控制器的東西向接口单元 12c 连接;

处理器 30, 用于指示東西向接口单元 32a 向控制器发送流量统计指令, 5 以使控制器向第一报文转发设备下发该流量统计指令;

可选的, 也可以由控制器自行向第一报文转发设备下发该流量统计指令, 不需要東西向接口单元 32a 向控制器发送流量统计指令。

東西向接口单元 32a, 还用于接收控制器发送的统计数据;

具体的, 控制器收集所述第一报文转发设备根据所述流量统计指令上报 10 的统计数据, 并将所述统计数据发送给独立的调度设备的東西向接口单元 32a。

处理器 30, 用于根据東西向接口单元 32a 接收的统计数据, 获得流向所述目的地 IP 地址的全局流量统计值; 根据该全局流量统计值判断是否发生网 络攻击;

15 其中, 所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后, 获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值;

若发生网络攻击, 则处理器 30 通过東西向接口单元 32a 与控制器协商确定 DDoS 防护策略, 并指示控制器将确定的 DDoS 防护策略下发给第二报文 20 转发设备;

方式二:

该独立的调度设备的東西向接口单元 32a 与控制器的東西向接口单元 12c 连接;

東西向接口单元 32a 接收控制器发送的 DDoS 防护请求消息;

25 处理器 30, 根据 DDoS 防护请求消息和控制器状况信息, 确定用于执行 DDoS 防护功能的控制器。

具体的, 通常多个控制器组成一个集群时, 为了便于管理多个控制器, 会设置独立的调度设备。因此, 处理器 30 需要基于控制器状况信息选择满足 执行 DDoS 防护功能的控制器; 控制器状况信息可以包含集群中每个控制器 30 的处理能力的信息、负载状况、空闲状况等, 确定满足执行 DDoS 防护功能

的控制器后，独立的调度设备向该控制器发送 DDoS 防护响应消息；该 DDoS 防护响应消息包含 DDoS 防护执行指示；该控制器根据该 DDoS 防护执行指示，执行 DDoS 防护功能，具体的功能参照上文图 4 对应实施例的方案。

对于方式一，具体的：独立的调度设备与控制器的协商机制可以有多种，
5 例如，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；独立的调度设备根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备。
10 所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。独立的调度设备指示控制器将所述距离攻击源最近的报文转发设备作为第二报文转发设备，并向该第二报文转发设备下发 DDoS 防护策略；又例如，独立的调度设备在确定使用动态引流清洗响应策略后，根据所述所述第一报文转发设备的负载值确定
15 第一引流路径，所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；独立的调度设备向所述控制器下发所述动态引流清洗响应策略，该策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述
20 所述第一引流路径发送到所述清洗设备上进行处理；又例如，独立的调度设备在确定使用动态引流清洗响应策略后，根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；独立的调度设备向控制器下发动态引流清洗响应策略，该策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指
25 示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。当然，独立的调度设备与控制器之间还可以采用多种可能的协商机制，本发明实施例不予限定。

可选的，上文所述控制器还具有另一种可能的实现方式，具体的，图 7 为本发明实施例提供的一种控制器的结构示意图，参照图 7，该控制器包括：
30 发送模块 40、处理模块 41、接收模块 42；

发送模块 40, 用于向第一报文转发设备下发流量统计指令, 所述流量统计指令用于指示所述第一报文转发设备进行流量统计; 其中, 所述流量统计指令携带目的地 IP 地址;

接收模块 42, 用于收集所述第一报文转发设备根据所述流量统计指令上报的统计数据, 所述统计数据包含流向所述目的地 IP 地址的流量统计信息;

处理模块 41, 用于:

根据所述接收模块 42 接收的所述统计数据, 获得流向所述目的地 IP 地址的所述全局流量统计值;

其中, 所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据汇总后, 获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值;

判断所述全局流量统计值是否超过预定阈值;

所述发送模块 40, 还用于基于处理模块 41 确定的全局流量统计值超过预定阈值的判断结果, 向第二报文转发设备下发 DDoS 防护策略。

本发明实施例提供的控制器, 通过处理模块指示发送模块向第一报文转发设备下发流量统计指令, 所述流量统计指令用于指示所述第一报文转发设备进行流量统计; 其中, 所述流量统计指令携带目的地 IP 地址; 接收模块接收所述第一报文转发设备根据所述流量统计指令上报的统计数据, 所述统计数据包含流向所述目的地 IP 地址的流量统计信息; 处理模块根据所述接收模块接收的所述统计数据, 获得流向所述目的地 IP 地址的全局流量统计值其中, 所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据汇总后, 获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值; 处理模块判断所述全局流量统计值是否超过预定阈值, 所述发送模块基于处理模块确定的全局流量统计值超过预定阈值的判断结果, 向第二报文转发设备下发 DDoS 防护策略。降低了 DDoS 攻击对网络的影响范围, 提高了网络安全性。

可选的, 所述流量统计指令还携带: 上文所述检测起始时刻;

进一步的, 控制器需要一种判断网络攻击是否停止的机制, 一种可能的实现方式为:

所述处理模块 41, 还用于:

确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

所述发送模块 40, 还用于基于所述处理模块 41 确定的至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值的结果, 向所述第二报文
5 转发设备下发上文所述防护消除指示消息；

可选的, 控制器还可以针对位于 SDN 边界靠近攻击源的报文转发设备下发 DDoS 防护策略, 一种可能的实现方式为:

根据所述接收模块 42 接收的所述统计数据, 确定攻击路径上距离攻击源最近的报文转发设备, 将所述距离攻击源最近的报文转发设备作为所述第二
10 报文转发设备。

具体的, 所述流向所述目的地 IP 地址的流量统计信息, 包括: 所述第一报文转发设备上流向所述目的地 IP 地址的流量值;

所述处理模块 41, 还用于根据所述统计数据, 确定攻击路径上距离攻击源最近的报文转发设备, 具体为:

15 根据所述接收模块 42 接收的所述第一报文转发设备上流向所述目的地 IP 地址的流量值, 确定第一攻击路径; 所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径;

根据所述第一攻击路径, 确定所述距离攻击源最近的报文转发设备;

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述
20 流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

可选的, 所述 DDoS 防护策略包含如下任意一种响应策略: 黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略;

具体的, 对于各种响应策略, 上进行了详细说明, 此处不再赘述。

25 对于所述动态引流清洗响应策略, 在所述控制器下发动态引流清洗响应策略之前, 需要控制器确定一条对网络冲击最小的路径来进行流量的引流, 下面给出几种可能的实现方式进行说明:

方式一: 所述统计数据还包含: 所述第一报文转发设备的负载值;

所述处理模块 41, 在所述发送模块 40 向所述第二报文转发设备下发
30 DDoS 防护策略之前, 还用于:

根据所述第一报文转发设备的负载值确定第一引流路径;

所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径; 所述第一引流路径包含所述第二报文转发设备和所述清洗设备;

5 则所述发送模块 40 根据所述处理模块 41 确定的所述第一引流路径, 向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响应策略, 所述动态引流清洗响应策略包含第一引流路径指示信息, 所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

10 方式二: 所述处理模块 41, 在所述发送模块 40 向所述第二报文转发设备下发 DDoS 防护策略之前, 还用于:

根据 SDN 拓扑关系确定第二引流路径, 所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径, 所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系;

15 则所述发送模块 40 根据所述处理模块 41 确定的所述第二引流路径, 向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略, 所述动态引流清洗响应策略包含第二引流路径指示信息, 所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

20 可选的, 上文所述报文转发设备还具有另一种可能的实现方式, 具体的, 图 8 为本发明实施例提供的另一种报文转发设备的结构示意图, 参照图 8, 该控制器包括: 发送模块 50、处理模块 51、接收模块 52;

接收模块 52, 用于接收所述控制器发送的流量统计指令, 所述流量统计指令用于指示处理模块 51 进行流量统计; 其中, 所述流量统计指令携带目的地 IP 地址;

25 所述处理模块 51, 用于根据所述接收模块 52 接收的所述流量统计指令统计流流向所述目的地 IP 地址的流量统计信息;

发送模块 50, 用于根据所述处理模块 51 统计的所述流向所述目的地 IP 地址的流量统计信息, 向所述控制器上报统计数据, 所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。

30 本发明实施例提供的报文转发设备即为上文所述第一报文转发设备, 通

过接收模块接收控制器发送的流量统计指令，该流量统计指令携带目的地 IP 地址，用于指示处理模块进行流量统计；进一步的，处理模块根据所述接收模块接收的流量统计指令对流向该目的地 IP 地址的流量进行统计，获得流向所述目的地 IP 地址的流量统计信息。发送模块向控制器上报统计数据，该统

5 统计数据包含流向所述目的地 IP 地址的流量统计信息；由于第一报文转发设备针对流向该目的地 IP 地址的流量进行流量统计，并将统计数据上报给控制器，使得控制器能够基于该统计数据判断是否发生 DDoS 攻击，从而触发相应的 DDoS 防护策略；从而降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

10 可选的，所述流量统计指令还携带：上文所述检测起始时刻；

进一步的，当图 8 所示报文转发设备作为第二报文转发设备时，其具有如下功能：

所述接收模块 52，在所述发送模块 50 向所述控制器上报统计数据之后，还用于：

15 接收所述控制器发送的 DDoS 防护策略；

所述处理模块 51，还用于根据所述接收模块 52 接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理。

本实施例提供的第二报文转发设备，在发送模块向所述控制器上报统计数据之后，通过接收模块接收所述控制器发送的 DDoS 防护策略，并由处理

20 模块根据所述接收模块接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理，实现了对流向所述目的地 IP 地址的流量的 DDoS 防护，从而降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

进一步的，对应控制器判断网络攻击是否停止的机制，第二报文转发设备侧相应的功能如下：

25 所述接收模块 52，在所述接收所述控制器发送的 DDoS 防护策略之后，还用于：

接收所述控制器发送的防护消除指示消息；

所述处理模块 51，还用于根据所述接收模块 52 接收的所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

30 可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响

应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

其中，所述黑洞路由响应策略用于指示所述处理模块 51 通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

5 则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

10 所述限流响应策略用于指示所述处理模块 51 对所述流向所述目的地 IP 地址的流量进行限流处理；

则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理；

15 所述限速响应策略用于指示所述处理模块 51 对所述流向所述目的地 IP 地址的流量进行限速处理；

则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理；

20 所述丢弃响应策略用于指示所述处理模块 51 对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

25 所述本地清洗响应策略用于指示所述处理模块 51 在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

30 所述动态引流清洗响应策略用于指示所述处理模块 51 将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；

则所述处理模块 51 根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述接收模块 52 接收的所述动态引流清洗响应策略指示所述发送模块 50 将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理。

- 5 对于所述动态引流清洗响应策略，在所述控制器下发动态引流清洗响应策略之前，需要控制器确定一条对网络冲击最小的路径来进行流量的引流，第二报文转发设备侧相应的功能如下：

方式一：

- 10 所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

- 15 则所述处理模块 51 根据所述接收模块 52 接收的所述动态引流清洗响应策略指示所述发送模块 50 将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

根据所述接收模块 52 接收的所述动态引流清洗响应策略，指示所述发送模块 50 将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

- 20 方式二：

所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

- 25 则所述处理模块 51 根据所述接收模块 52 接收的所述动态引流清洗响应策略指示所述发送模块 50 将所述流向所述目的地 IP 地址的流量发送到所述清洗设备上进行处理，具体为：

- 30 根据所述接收模块 52 接收的所述动态引流清洗响应策略，指示所述发送模块 50 将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

在图 2 至 8 的基础上,图 9 为本发明实施例提供的一种基于 SDN 的 DDOS 攻击防护方法的流程示意图,参照图 9,该流程包括:

步骤 1、数据流量正常情况按照 1-→ 4-→ 5 到达服务器。

步骤 2、控制器识别处于 SDN 边界的报文转发设备,当控制器执行 DDoS 控制程序时或用户设备的应用调用 DDoS 控制程序时,控制器向处于 SDN 边界的报文转发设备下发流量统计指令,该流量统计指令用于指示所述报文转发设备进行流量统计,此时,处于 SDN 边界的报文转发设备即为第一报文转发设备;可选的,控制器也可以向 SDN 内全部的报文转发设备下发流量统计指令。

具体的,该流量统计指令携带目的地 IP 地址,该目的地 IP 地址为所述服务器的某个 IP 地址或某段 IP 地址段;第一报文转发设备基于该流量统计指令从某个时间开始对流向该目的地 IP 地址的流量进行统计,获得统计数据,该统计数据包含流向所述目的地 IP 地址的流量统计信息;控制器在统计周期 T 结束的时候可以向第一报文转发设备查询该统计数据。控制器下发策略和查询统计结果例如流向 3 所示;

步骤 3、第一报文转发设备收到该流量统计指令后,建立基于该目的地 IP 地址的目的 IP 监控表,该表采用哈希表形式,包含了该目的地 IP 地址的各种统计项目。第一报文转发设备在每个统计周期内对转发的数据报文目的地址为该目的地 IP 地址的流量进行统计,统计周期结束时,控制器向第一报文转发设备查询该统计数据。第一报文转发设备上报该统计数据例如流向 2 所示;

步骤 4、控制器搜集到所有第一报文转发设备在某检测周期 T 内的统计数据,控制器对该流向所述目的地 IP 地址的流量统计信息进行汇总,获得流向该目的地 IP 地址的全局流量统计值;具体的,控制器可以对统计数据求和等运算处理获得流向该目的地 IP 地址的全局流量统计值。控制器将该全局流量统计值与预定阈值进行比较,如果超过该预定阈值,则认为网络攻击发生;如果持续几个特定周期,该全局流量统计值连续小于该预定阈值,则认为网络攻击消除;

步骤 5、若判断网络攻击发生,则控制器向第二报文转发设备下发网络攻击防护策略,例如 DDoS 防护策略。

进一步的,对于步骤 5,控制器可以确定距离攻击源最近的报文转发设备,

将该距离攻击源最近的报文转发设备作为第二报文转发设备。

步骤 6、第二报文转发设备接收 DDoS 防护策略后，可以基于 DDoS 防护策略进行黑洞路由、限流（限速）、丢弃、本地清洗、动态引流清洗、本地清洗等 DDoS 防护策略。其中，本地清洗指报文转发设备对符合 DDoS 防护策略的流量进行 DDoS 防护清洗处理；动态引流清洗指报文转发设备将符合 DDoS 防护策略的流量引流至专业清洗设备进行清洗，清洗后的流量由该清洗设备回注到 SDN 中。

步骤 7、第二报文转发设备接收控制器发送的防护消除指示消息后，恢复流量正常转发路径，关闭引流，清洗设备停止清洗处理。

需要说明的是，所述第一报文转发设备针对流向所述目的地 IP 地址的流量的所进行的流量统计，在 OpenFlow 协议规定的流程中通过流水线处理实现。具体的：首先，第一报文转发设备定义目的 IP 监控表为流表，当某个流量的目的 IP 地址命中 IP 监控表中的目的地 IP 地址时，则认为命中该流表表项，第一报文转发设备提取该流量数据报文的信息，刷新该表项的统计结果，通常，统计结果的形式为：第一报文转发设备的统计数值=第一报文转发设备的统计原数值+数据包个数；第一报文转发设备同时检查监测周期是否到达，若到达，则把动作项（action）设置为发该第一报文转发设备的统计数据的日志给控制器，并清空该第一报文转发设备缓存的统计结果，进入下一个统计周期。

下面通过具体实施例对上述 SDN 中的控制器和报文转发设备进行说明。

图 10 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，该方法执行主体为上述控制器，该控制器可以采用图 4 或图 7 所示的结构，参照图 10，该方法包括如下流程：

步骤 100、控制器向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；

其中，所述流量统计指令携带目的地 IP 地址。

步骤 101、所述控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

步骤 102、所述控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

步骤 103、所述控制器判断所述全局流量统计值是否超过预定阈值；

5 步骤 104、所述控制器基于所述全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略。

本发明实施例提供的基于 SDN 的 DDoS 攻击防护方法，通过控制器向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；其中，所述流量统计指令携带目的地 IP 地址；所述控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；所述控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；所述控制器判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略。降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

可选的，所述流量统计指令还携带：检测起始时刻；

20 其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

进一步的，控制器需要一种判断网络攻击是否停止的机制，具体的，在图 10 的基础上，图 11 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，参照图 11，在步骤 104 之后，还包括：

步骤 105、所述控制器确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

步骤 106、所述控制器向所述第二报文转发设备下发防护消除指示消息；

30 所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述

DDoS 防护策略。

可选的，控制器还可以针对位于 SDN 边界靠近攻击源的报文转发设备下发 DDoS 防护策略，具体的，具体的，在图 10 的基础上，图 12 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，参照图 12，在步骤 104 之前，还包括：

步骤 107、所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

进一步的，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；步骤 107 的一种可能的实现方式为：

所述控制器根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

所述控制器根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

下面对方式二中“所述控制器根据所述统计数据确定攻击路径上距离攻击源最近的报文转发设备”做进一步说明，图 13 为攻击路径及最近攻击源头判定示意图，参照图 13，其中 SDN 包括：报文转发设备 A 至 G、控制器；其中，报文转发设备 A 与 ISP 网络 1 连接，并且网络攻击的攻击源处于该 ISP 网络 1 中，报文转发设备 B 与 ISP 网络 2 连接，报文转发设备 F 与 ISP 网络 3 连接，报文转发设备 F 与目的地 IP 所处的网络连接，该目的地 IP 为网络攻击的流量的目的地 IP，即受害主机的 IP；由于报文转发设备 A、报文转发设备 B、报文转发设备 E 和报文转发设备 F 分别用于其他网络接入 SDN，因此这些报文转发设备处于 SDN 的边界。

参照图 13，首先，控制器根据 SDN 的拓扑关系，确定距离目的地 IP 最近的报文转发设备 E 和上述几个处于 SDN 边界的报文转发设备，由于在 SDN

中，从攻击源流向目的地 IP 的网络攻击流量可能存在多种路径，例如，该流量路径可以为：报文转发设备 A→报文转发设备 G→报文转发设备 E，下文简称第一攻击路径；报文转发设备 F→报文转发设备 E，下文简称第二攻击路径；报文转发设备 B→报文转发设备 G→报文转发设备 E，下文简称第三攻击路径；

5 控制器统计各个攻击路径上流向目的地 IP 的流量的统计数据，控制器对各个攻击路径上流向目的地 IP 的流量大小进行排序，确定第一攻击路径为流量最大的攻击路径，则控制器确定报文转发设备 A 距离攻击源头最近。

继续参照图 13，对上文所述第一报文转发设备和第一报文转发设备进行说明。当控制器向第一报文转发设备下发流量统计指令后，第一报文转发设备根据该流量统计指令进行流量统计，对于图 13 中的报文转发设备，报文转发设备 A 至 G 均可以进行流量统计，因此报文转发设备 A 至 G 都可以作为第一报文转发设备；进一步的，当控制器确定报文转发设备 A 距离攻击源头最近后，控制器向报文转发设备 A 下发 DDoS 防护策略，则将报文转发设备 A 作为第二报文转发设备；或者，由于流向目的地 IP 的网络攻击流量可能分别

10 经过报文转发设备 A、B 和 F，控制器可以分别向报文转发设备 A、B 和 F 下发 DDoS 防护策略，则将报文转发设备 A、B 和 F 都作为第二报文转发设备。

可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

20 其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；

25 所述限速响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理；

所述丢弃响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理；

30 所述动态引流清洗响应策略用于指示所述第二报文转发设备将所述流向

所述目的地 IP 地址的流量发送到清洗设备上进行处理。

对于所述动态引流清洗响应策略，在所述控制器下发动态引流清洗响应策略之前，需要控制器确定一条对网络冲击最小的路径来进行流量的引流，下面给出几种可能的实现方式进行说明。

5 方式一：在图 10 的基础上，图 14 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，参照图 14，所述统计数据还包含：所述第一报文转发设备的负载值；

进一步的，在步骤 104 之前，还包括：

10 步骤 108、所述控制器根据所述第一报文转发设备的负载值确定第一引流路径；

所述第一引流路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述控制器向所述第二报文转发设备下发的 DDoS 防护策略为所述动态引流清洗响应策略；

15 具体的，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

20 方式二：在图 10 的基础上，图 15 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，参照图 15，在步骤 104 之前，还包括：

步骤 109、所述控制器根据 SDN 拓扑关系确定第二引流路径；

具体的，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

25 则所述控制器向所述第二报文转发设备下发 DDoS 防护策略为所述动态引流清洗响应策略；

30 具体的，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

参照图 13, 对方式一中的“第一引流路径”进行说明: 例如, 假设报文转发设备 F 收到控制器发送的流量统计指令, 该 F 作为第一报文转发设备进行流量统计; 并将统计数据上报给控制器; 若控制器向该 F 下发动态引流清洗响应策略, 则该 F 作为第二报文转发设备执行该动态引流清洗响应策略;

5 该 F 与清洗设备连接; 由于动态引流清洗响应策略包含第一引流路径指示信息, 所述第一引流路径指示信息用于指示该 F 将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。由于该 F 直接与清洗设备连接, 显然 F-清洗设备的引流路径为该 F 至所述清洗设备之间负载最小的路径, 则第一引流路径包含

10 又例如, 假设清洗设备与报文转发设备 D 连接, 若控制器向该 F 下发动态引流清洗响应策略, 则该 F 作为第二报文转发设备执行该动态引流清洗响应策略, 此时从 F 将流量引向清洗设备包含多种可能的引流路径, 如: F-E-G-D-清洗设备; F-A-G-D-清洗设备等; 不同引流路径的负载不一样, 控制器基于上述路径的报文转发设备作为第一报文转发设备时上报的统计数据, 确定第
15 一引流路径, 例如 F-E-G-D-清洗设备的负载最小, 则第一引流路径包含 F、E、G、D 和清洗设备。

需要说明的是, 图 14 和图 15 所示的步骤可以结合图 10 所示的步骤实现, 也可以结合图 11 和图 12 所示的步骤实现。

对于上文所示控制器侧的实施例, 下面对报文转发设备侧的方法流程进行说明。

20 图 16 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程图, 所述方法应用于 SDN 系统中, 所述 SDN 系统包括控制器和报文转发设备, 该方法执行主体为上述报文转发设备, 该报文转发设备可以采用图 5 或图 8 所示的结构, 参照图 16, 该方法包括如下流程:

25 步骤 200、接收所述控制器发送的流量统计指令, 所述流量统计指令用于指示所述报文转发设备进行流量统计;

其中, 所述流量统计指令携带目的地 IP 地址;

步骤 201、根据所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息;

30 步骤 202、向所述控制器上报统计数据, 所述统计数据包含所述流向所述

目的地 IP 地址的流量统计信息。

本发明实施例提供的基于 SDN 的 DDoS 攻击防护方法，通过报文转发设备接收所述控制器发送的流量统计指令，所述流量统计指令用于指示所述报文转发设备进行流量统计；其中，所述流量统计指令携带目的地 IP 地址；报文转发设备根据所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；报文转发设备向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。由于报文转发设备针对流向该目的地 IP 地址的流量进行流量统计，并将统计数据上报给控制器，使得控制器能够基于该统计数据判断是否发生 DDoS 攻击，从而触发相应的 DDoS 防护策略；
10 从而降低了 DDoS 攻击对网络的影响范围，提高了网络安全性。

需要说明的是，执行上述步骤 200 至 202 的报文转发设备，根据其功能可以被定义为上文所述第一报文转发设备；

可选的，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述报文转发设备进行所述流量统计
15 的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

进一步的，当控制器执行判断网络攻击是否停止的机制时，具体的，在图 16 的基础上，图 17 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，在步骤 202 之后，还包括：

20 步骤 203、接收所述控制器发送的 DDoS 防护策略；

步骤 204、根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

在图 17 的基础上，图 18 为本发明实施例提供的另一种基于 SDN 的 DDoS 攻击防护方法的流程示意图，在步骤 204 之后，还包括：

25 步骤 205、接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述报文转发设备结束执行所述 DDoS 防护策略；

步骤 206、根据所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

可选的，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、
30

动态引流清洗响应策略;

其中, 所述黑洞路由响应策略用于指示所述报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

5 则步骤 204 的一种可能的实现方式为: 根据所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

所述限流响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理;

则步骤 204 的一种可能的实现方式为: 根据所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理;

10 所述限速响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理;

则步骤 204 的一种可能的实现方式为: 根据所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理;

15 所述丢弃响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

则步骤 204 的一种可能的实现方式为: 根据所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

所述本地清洗响应策略用于指示所述报文转发设备在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

20 则步骤 204 的一种可能的实现方式为: 根据所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理;

所述动态引流清洗响应策略用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理;

25 则步骤 204 的一种可能的实现方式为: 根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

对于所述动态引流清洗响应策略, 在所述控制器下发动态引流清洗响应策略之前, 需要控制器确定一条对网络冲击最小的路径来进行流量的引流, 为了配合控制器侧实现基于对网络冲击最小的路径进行引流的方案, 下面对报文转发设备需要执行的方法流程进行说明。

30 方式一:

所述统计数据还包含：所述第一报文转发设备的负载值；

所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则步骤 204 的一种可能的实现方式为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

方式二：

所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

则步骤 204 的一种可能的实现方式为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

对于本地清洗指示，下面给出一种可能的处理方式，图 19 为本地清洗处理流程示意图，参照图 19，该流程包括对数据报文分类的处理过程：

步骤 300、判断数据报文是否属于传输控制协议（Transmission Control Protocol，简称：TCP）协议；

若是则执行步骤 301，否则执行步骤 308；

步骤 301、判断所述数据报文是否是超文本传送协议（Hyper Text Transfer Protocol，简称：HTTP）报文；

若是，则采用 HTTP 报文处理函数对数据报文进行清洗处理；否则执行步骤 302；

步骤 302、判断所述数据报文是否是域名系统（Domain Name System，简称：DNS）报文；

若是，则采用 DNS 报文处理函数对数据报文进行清洗处理；否则执行步骤 303；

步骤 303、判断所述数据报文是否是 TCP 分片报文；

若是，则采用 TCP 分片报文处理函数对数据报文进行清洗处理；否则执行步骤 304；

5 步骤 304、判断所述数据报文是否是同步（Synchronous，简称：Syn）报文；

若是，则采用 Syn 报文处理函数对数据报文进行清洗处理；否则执行步骤 305；

步骤 305、判断所述数据报文是否是确认（Acknowledgement，简称：ACK）报文；

10 若是，则采用 ACK 报文处理函数对数据报文进行清洗处理；否则执行步骤 306；

步骤 306、判断所述数据报文是否是 Syn-ACK 报文；

若是，则采用 Syn-ACK 报文处理函数对数据报文进行清洗处理；否则执行步骤 307；

15 步骤 307、判断所述数据报文是否是复位（RST）报文；

若是，则采用复位报文处理函数对数据报文进行清洗处理；否则执行返回步骤；

步骤 308、判断所述数据报文是否属于用户数据包协议（User Datagram Protocol，简称：UDP）协议；

20 若是，则执行步骤 309；否则执行返回步骤；

步骤 309、判断所述数据报文是否是 DNS 询问报文；

若是，则采用询问报文处理函数对数据报文进行清洗处理；否则执行步骤 310；

步骤 310、判断所述数据报文是否是 DNS 响应报文；

25 若是，则采用询问报文处理函数对数据报文进行清洗处理；否则执行步骤 311；

步骤 311、判断所述数据报文是否是会话初始协议（Session Initiation Protocol，简称：SIP）报文；

30 若是，则采用 SIP 报文处理函数对数据报文进行清洗处理；否则执行步骤 312；

步骤 312、判断所述数据报文是否是 UDP 分片报文；

若是，则采用 UDP 分片报文处理函数对数据报文进行清洗处理；否则采用 UDP 报文对所述数据报文进行清洗处理。

需要说明的是，图 19 所示方案仅为一种可能的实现方案，对于其他能够实现本地清理的处理流程，本实施例不予限定。

需要说明的是，执行上述步骤 203 至 206 的报文转发设备，根据其功能可以被定义为上文所述第二报文转发设备。

针对图 10 至图 15 对应实施例所示的控制器执行的流程，和图 16 至图 19 对应实施例所示的报文转发设备执行的流程，下面通过具体实施例对控制器与报文转发设备之间的交互进行说明，图 20 为本发明实施例提供的一种基于 SDN 的 DDoS 攻击防护方法的交互流程示意图，参照图 20，该交互流程包括：

步骤 400、控制器向第一报文转发设备下发流量统计指令；

步骤 401、第一报文转发设备根据所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

步骤 402、控制器接收第一报文转发设备发送的统计数据；

步骤 403、所述控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

步骤 404、所述控制器判断所述全局流量统计值是否超过预定阈值；

步骤 405、所述控制器基于所述全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略；

步骤 406、第二报文转发设备根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

步骤 407、所述控制器确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

步骤 408、所述控制器向所述第二报文转发设备下发防护消除指示消息；

步骤 409、第二报文转发设备根据所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

下面通过具体实施例对控制器与报文转发设备之间的交互进行说明，图 21 为本发明实施例提供的另一种基于 SDN 网络的 DDoS 攻击防护方法的交互示意图，参照图 21，该交互包括如下流程：

步骤 500、控制器向报文转发设备下发流量统计指令;

步骤 501、报文转发设备向报文转发设备发送流量统计指令应答消息;

步骤 502、报文转发设备构建目的 IP 监控表进行流量监控;

步骤 503、控制器周期下发查询消息;

5 需要说明的是, 步骤 503 也可以为报文转发设备周期性主动上报统计数据。

步骤 504、报文转发设备向控制器发送应答消息, 该应答消息包含统计数据;

步骤 505、控制器周期性地基于目的 IP 监控的流量统计信息进行汇总并判断是否超过设定阈值, 若超过则判定进入 DDoS 攻击开始状态; 未超过则继续监测;

步骤 506、进入 DDoS 攻击开始状态, 则控制器根据监测结果, 找到距离攻击最近的报文转发设备, 下发 DDoS 防护策略;

步骤 507、报文转发设备向控制器发送 DDoS 防护策略响应消息;

15 步骤 508、报文转发设备启动防护动作;

步骤 509、进入 DDoS 攻击开始状态, 继续多个周期后, 控制器发现流量恢复正常, 则判定攻击结束状态, 继续监控流量;

步骤 510、进入攻击结束状态, 则控制器向响应的报文转发设备下发防护消除指示消息;

20 步骤 511、报文转发设备向控制器发送防护消除指示响应消息。

下面对于图 20 或 21 中交互的消息、信令及信元给出具体的实现方式:

在报文转发设备构建基于上述目的地 IP 地址的目的 IP 监控表(ddos-group table), 该表采用哈希表形式, 建立算法采用流量数据包的目的地 IP 地址命中指定的目的地 IP 地址, 则认为命中该表, 报文转发设备则可以进行流量统计;

25 流向所述目的地 IP 地址的流量统计信息的一种可能的实现方式中, 其包含的字段可以包括如下信息:

总报文数 (ULONG ulPacketSum)、总字节数 (ULONG ulByteSum)、报文包速率 (ULONG ulICMPPktRate)、ICMP 带宽 (ULONG ulICMPBand)、TCP 报文包速率 (ULONG ulTcpPktRate)、TCP 带宽 (ULONG ulTcpBand)、
30 UDP 报文包速率 (ULONG ulUdpPktRate)、UDP 带宽 (ULONG ulUdpBand);

可选的，对于各类 TCP 报文，流量统计信息包含的字段可以包括如下至少一种信息：SYN 报文包速率（ULONG ulSynPktRate）、SYN 报文的带宽（ULONG ulSynBand）、ACK 报文的包速率（ULONG ulAckPktRate）、ACK 报文的带宽（ULONG ulAckBand）、SYN/ACK 包速率（ULONG
5 ulSynAckPktRate）、SYN/ACK 报文的带宽（ULONG ulSynAckBand）、FIN 报文包速率（ULONG ulFinPktRate）、FIN 报文的带宽（ULONG ulFinBand）、RST 报文包速率（ULONG ulRstPktRate）、RST 报文的带宽（ULONG ulRstBand）、错误报文的包速率（ULONG ulErrPktRate）、错误报文的带宽（ULONG ulErrBand）、分片报文的包速率（ULONG ulFragPktRate）、分片报
10 文的带宽（ULONG ulFragBand）、HTTP GET 报文的包速率（ULONG ulHttpGetPktRate）、HTTP GET 报文的带宽（ULONG ulHttpGetBand）、DNS 报文的包速率（ULONG ulDnsByteNum）、DNS 报文带宽（ULONG ulDnsBand）、流数目（ULONG ulFlowCnt）；

另外，上文统计数据还包含：所述第一报文转发设备的负载值：具体的，
15 该第一报文转发设备的负载值的实现形式可以为：该第一报文转发设备的吞吐量；或者，该第一报文转发设备的带宽占用率等。进一步的，该第一报文转发设备的负载值可以设置在流量统计信息的字段内；也可以设置在统计数据的空闲字段内。

对于控制器与报文转发设备之间交互的消息，下面给出一种可能的实现
20 方式：

控制器向报文转发设备发送流量统计指令，相应的，报文转发设备向控制器发送流量统计指令应答消息，对于这些交互消息，基于 Open Flow 协议其可以具有如下数据结构：

```

struct ofp_ddos_config {
25   struct          ofp_header          header;          /*          Type
OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY. */
   uint32_t dstip[4];    /* 目的地 IP 地址*/
   uint32_t netoff[4];   /* 子网掩码*/
   uint64_t stat_ctrl;   /* 统计使能，启动或者关闭*/
30   uint64_t stat_tics;   /* 统计周期，秒*/

```

```
uint64_t stat_fun;    /* 统计子功能项开关，按位使能*/
};
```

具体的，采用该数据结构的交互消息中携带如下字段：消息类型字段（Type OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY）、目的地 IP 地址、子网掩码、统计使能、统计周期、统计子功能项开关；

其中，目的地 IP 地址的字段为 4 字节；子网掩码的字段为 4 字节；统计使能的字段为 8 字节，其用于指示启动流量统计或关闭流量统计；统计周期的字段为 8 字节，其用于指示流量统计的周期，其时间单位可以为秒或其他符合 SDN 需求的时间单位；统计子功能项开关的字段为 8 字节，其用于指示统计流量的相关功能的开启或关闭，按位使能。

所述控制器收集报文转发设备根据流量统计指令上报的统计数据。具体的，控制器可以采用向报文转发设备发送查询消息，并接收报文转发设备发送的应答消息，该应答消息包含统计数据。基于 Open Flow 协议，查询消息和应答消息可以具有如下数据结构：

```
15 struct ofp_ddos_report {
    struct          ofp_header          header;          /*          Type
OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY. */
    uint32_t dstip[4];    /* 目的地 IP 地址*/
    uint32_t netoff[4];    /* 子网掩码*/
20 uint64_t stat_tics;    /* 统计周期，秒*/
    uint32_t stat_times;    /* 当前已经统计上报的周期次数*/
    struct ofp_ddos_stat statdata; /* 流量统计信息的集合 */
};
```

具体的，采用该数据结构的查询消息和应答消息中携带如下字段：消息类型字段（Type OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY）、目的地 IP 地址、子网掩码、统计周期、当前已经统计上报的周期次数、流量统计信息的集合；

其中，目的地 IP 地址的字段为 4 字节；子网掩码的字段为 4 字节；统计周期的字段为 8 字节，其用于指示流量统计的周期，其时间单位可以为秒或其他符合 SDN 需求的时间单位；当前已经统计上报的周期次数的字段为 4 字

节；流量统计信息的集合包含报文转发设备包含的统计项，各统计项按照统计变量名称和统计变量数值的形式包含在该数据结构中。

在确定网络攻击发生后，控制器会向报文转发设备下发 DDoS 防护策略、报文转发设备会向控制器发送 DDoS 防护策略响应消息，当网络攻击结束后，
5 控制器会向报文转发设备下发防护消除指示消息，报文转发设备会向控制器发送防护消除指示响应消息，对于这些交互消息，基于 Open Flow 协议其可以具有如下数据结构：

```

struct ofp_ddos_action {
    struct      ofp_header      header;          /*      Type
10  OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY. */
    uint32_t dstip[4];          /* 目的地 IP 地址*/
    uint32_t netoff[4];         /* 子网掩码*/
    uint64_t action_flag;       /* 动作使能，启动或关闭*/
    uint64_t action_type;       /* 响应动作的类型*/
15  struct ofp_ddos_action_param actionparam; /* 响应动作参数集合 */

};

```

具体的，采用该数据结构的交互消息中携带如下字段：消息类型字段（Type OFPT_ROLE_REQUEST/OFPT_ROLE_REPLY）、目的地 IP 地址、子
20 网掩码、动作使能、响应动作的类型、响应动作参数集合；

其中，目的地 IP 地址的字段为 4 字节；子网掩码的字段为 4 字节；动作使能的字段为 8 字节，其用于指示动作为“开启”态或“关闭”态；响应动作的类型的字段为 8 字节，其包含黑洞路由、限流（限速）、丢弃、本地清洗、引流清洗；响应动作参数集合包含与具体的响应动作相关的参数。

25 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

30 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对

其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权 利 要 求

1、一种基于软件定义网络 SDN 的分布式拒绝服务 DDoS 攻击防护方法，其特征在于，包括：

5 控制器向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；

其中，所述流量统计指令携带目的地 IP 地址；

所述控制器收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

10 所述控制器根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

15 所述控制器判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略。

2、根据权利要求 1 所述的方法，其特征在于，所述流量统计指令还携带：检测起始时刻；

20 其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器。

3、根据权利要求 2 所述的方法，其特征在于，还包括：

25 所述控制器确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值，则所述控制器向所述第二报文转发设备下发防护消除指示消息；

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略。

4、根据权利要求 1-3 任意一项所述的方法，其特征在于，在所述控制器向所述第二报文转发设备下发 DDoS 防护策略之前，还包括：

5 所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

5、根据权利要求 4 所述的方法，其特征在于，所述流向所述目的地 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；

所述控制器根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，包括：

所述控制器根据所述第一报文转发设备上流向所述目的地 IP 地址的流量值，确定第一攻击路径；

15 所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

所述控制器根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

20 所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

6、根据权利要求 1-5 任意一项所述的方法，其特征在于，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

25 其中，所述黑洞路由响应策略用于指示所述第二报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

所述限流响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；

所述限速响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理;

所述丢弃响应策略用于指示所述第二报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理;

5 所述本地清洗响应策略用于指示所述第二报文转发设备在本地对流向所述目的地 IP 地址的流量进行清洗处理;

所述动态引流清洗响应策略用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

7、根据权利要求 6 所述的方法,其特征在於,所述统计数据还包含:所述
10 所述第一报文转发设备的负载值;

在所述控制器向所述第二报文转发设备下发 DDoS 防护策略之前,包括:
所述控制器根据所述第一报文转发设备的负载值确定第一引流路径;

其中,所述第一引流路径为所述第二报文转发设备至所述清洗设备之间
负载最小的路径;所述第一引流路径包含所述第二报文转发设备和所述清洗
15 设备;

所述控制器向所述第二报文转发设备下发的 DDoS 防护策略为所述动态
引流清洗响应策略,所述动态引流清洗响应策略包含第一引流路径指示信息,
所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述
目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。
20 处理。

8、根据权利要求 6 所述的方法,其特征在於,在所述控制器向所述第二
报文转发设备下发 DDoS 防护策略之前,包括:

所述控制器根据 SDN 拓扑关系确定第二引流路径,所述第二引流路径为
所述第二报文转发设备至所述清洗设备之间距离最近的路径,所述 SDN 拓扑
25 关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系;

所述控制器向所述第二报文转发设备下发 DDoS 防护策略为所述动态引
流清洗响应策略,所述动态引流清洗响应策略包含第二引流路径指示信息,

所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

9、一种基于 SDN 的 DDoS 攻击防护方法，所述方法应用于 SDN 系统中，
5 所述 SDN 系统包括控制器和报文转发设备，所述方法由所述报文转发设备执行，其特征在于，包括：

接收所述控制器发送的流量统计指令，所述流量统计指令用于指示所述报文转发设备进行流量统计；

其中，所述流量统计指令携带目的地 IP 地址；

10 根据所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。

10、根据权利要求 9 所述的方法，其特征在于，所述流量统计指令还携带：检测起始时刻；

15 其中，所述检测起始时刻用于告知所述报文转发设备进行所述流量统计的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

11、根据权利要求 9 或 10 所述的方法，其特征在于，在所述向所述控制器上报统计数据之后，还包括：

20 接收所述控制器发送的 DDoS 防护策略；

根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理。

12、根据权利要求 11 所述的方法，其特征在于，在所述接收所述控制器发送的 DDoS 防护策略之后，还包括：

25 接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述报文转发设备结束执行所述 DDoS 防护策略；

根据所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进

行防护处理。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述 DDoS 防护策略包含如下任意一种响应策略：黑洞路由响应策略、限流响应策略、限速响应策略、丢弃响应策略、本地清洗响应策略、动态引流清洗响应策略；

5 其中，所述黑洞路由响应策略用于指示所述报文转发设备通过配置黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述黑洞路由响应策略采用黑洞路由对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

10 所述限流响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限流处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限流响应策略对所述流向所述目的地 IP 地址的流量进行限流处理；

15 所述限速响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行限速处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述限速响应策略对所述流向所述目的地 IP 地址的流量进行限速处理；

20 所述丢弃响应策略用于指示所述报文转发设备对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述丢弃响应策略对所述流向所述目的地 IP 地址的流量进行报文丢弃处理；

25 所述本地清洗响应策略用于指示所述报文转发设备在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进

行防护处理，具体为：根据所述本地清洗响应策略在本地对所述流向所述目的地 IP 地址的流量进行清洗处理；

所述动态引流清洗响应策略用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理；

5 则所述根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护处理，具体为：根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理。

14、根据权利要求 13 所述的方法，其特征在于，所述统计数据还包含：所述第一报文转发设备的负载值；

10 所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理；所述第一引流路径为所述报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

15 则所述根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理，具体为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

15、根据权利要求 13 所述的方法，其特征在于，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理；所述第二引流路径为所述报文转发设备至所述清洗设备之间距离最近的路径；

25 则所述根据所述动态引流清洗响应策略将所述流向所述目的地 IP 地址的流量发送到清洗设备上进行处理，具体为：

根据所述动态引流清洗响应策略，将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

16、一种控制器，其特征在于，包括：

发送模块，用于向第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；其中，所述流量统计指令携带目的地 IP 地址；

5 接收模块，用于收集所述第一报文转发设备根据所述发送模块发送的所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

处理模块，用于：

10 根据所述接收模块接收到的所述统计数据，获得流向所述目的地 IP 地址的所述全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

判断所述全局流量统计值是否超过预定阈值；

15 所述发送模块，还用于基于处理模块确定的全局流量统计值超过预定阈值的判断结果，向第二报文转发设备下发 DDoS 防护策略。

17、根据权利要求 16 所述的控制器，其特征在于，所述流量统计指令还携带：检测起始时刻；

20 其中，所述检测起始时刻用于告知所述第一报文转发设备进行所述流量统计的起始时刻，所述流量统计被所述第一报文转发设备以检测周期的方式持续执行，所述统计数据被所述第一报文转发设备以所述检测周期上报给所述控制器；

所述处理模块，还用于：

25 确定在至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值；

所述发送模块，还用于基于所述处理模块确定的至少两个连续的检测周期内所述全局流量统计值未超过所述预定阈值的结果，向所述第二报文转发

设备下发防护消除指示消息;

所述防护消除指示消息用于指示所述第二报文转发设备结束执行所述 DDoS 防护策略。

18、根据权利要求 16 或 17 所述的控制器，其特征在于，所述处理模块，
5 在所述发送模块向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述接收模块接收的所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，将所述距离攻击源最近的报文转发设备作为所述第二报文转发设备。

19、根据权利要求 18 所述的控制器，其特征在于，所述流向所述目的地
10 IP 地址的流量统计信息，包括：所述第一报文转发设备上流向所述目的地 IP 地址的流量值；

所述处理模块，还用于根据所述统计数据，确定攻击路径上距离攻击源最近的报文转发设备，具体为：

根据所述接收模块接收的所述第一报文转发设备上流向所述目的地 IP 地
15 址的流量值，确定第一攻击路径；所述第一攻击路径为流向所述目的地 IP 地址的至少一条攻击路径中流量值最大的攻击路径；

根据所述第一攻击路径，确定所述距离攻击源最近的报文转发设备；

所述距离攻击源最近的报文转发设备位于所述第一攻击路径上的、所述
流向所述目的地 IP 地址的流量的源地址侧的 SDN 边界处。

20、根据权利要求 16 或 17 所述的控制器，其特征在于，所述统计数据
还包含：所述第一报文转发设备的负载值；

所述处理模块，在所述发送模块向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据所述第一报文转发设备的负载值确定第一引流路径，所述第一引流
25 路径为所述第二报文转发设备至所述清洗设备之间负载最小的路径；所述第一引流路径包含所述第二报文转发设备和所述清洗设备；

则所述发送模块根据所述处理模块确定的所述第一引流路径，向所述第

二报文转发设备下发的 DDoS 防护策略为动态引流清洗响应策略，所述动态引流清洗响应策略包含第一引流路径指示信息，所述第一引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第一引流路径发送到所述清洗设备上进行处理。

- 5 21、根据权利要求 16 或 17 所述的控制器，其特征在于，所述处理模块，在所述发送模块向所述第二报文转发设备下发 DDoS 防护策略之前，还用于：

根据 SDN 拓扑关系确定第二引流路径，所述第二引流路径为所述第二报文转发设备至所述清洗设备之间距离最近的路径，所述 SDN 拓扑关系包含所述 SDN 中各个报文转发设备以及所述清洗设备的连接关系；

- 10 则所述发送模块根据所述处理模块确定的所述第二引流路径，向所述第二报文转发设备下发 DDoS 防护策略为动态引流清洗响应策略，所述动态引流清洗响应策略包含第二引流路径指示信息，所述第二引流路径指示信息用于指示所述第二报文转发设备将所述流向所述目的地 IP 地址的流量通过所述第二引流路径发送到所述清洗设备上进行处理。

- 15 22、一种报文转发设备，所述报文转发设备应用于 SDN 系统中，所述 SDN 系统包括控制器和所述报文转发设备，其特征在于，所述报文转发设备，包括：

接收模块，用于接收所述控制器发送的流量统计指令，所述流量统计指令用于指示处理模块进行流量统计；其中，所述流量统计指令携带目的地 IP
20 地址；

所述处理模块，用于根据所述接收模块接收的所述流量统计指令统计流向所述目的地 IP 地址的流量统计信息；

- 发送模块，用于根据所述处理模块统计的所述流向所述目的地 IP 地址的流量统计信息，向所述控制器上报统计数据，所述统计数据包含所述流向所述目的地 IP 地址的流量统计信息。
25

23、根据权利要求 22 所述的报文转发设备，其特征在于，所述流量统计指令还携带：检测起始时刻；

其中，所述检测起始时刻用于告知所述处理模块进行所述流量统计的起始时刻，以检测周期的方式持续进行所述流量统计，以所述检测周期上报所述统计数据给所述控制器。

24、根据权利要求 22 或 23 所述的报文转发设备，其特征在于，所述接收模块，在所述发送模块向所述控制器上报统计数据之后，还用于：

接收所述控制器发送的 DDoS 防护策略；

所述处理模块，还用于根据所述接收模块接收的所述 DDoS 防护策略，对所述流向所述目的地 IP 地址的流量进行防护处理。

25、根据权利要求 24 所述的报文转发设备，其特征在于，所述接收模块，在所述接收所述控制器发送的 DDoS 防护策略之后，还用于：

接收所述控制器发送的防护消除指示消息；所述防护消除指示消息用于指示所述处理模块结束执行所述 DDoS 防护策略；

所述处理模块，还用于根据所述接收模块接收的所述防护消除指示消息停止对所述流向所述目的地 IP 地址的流量进行防护处理。

26、一种 SDN 系统，其特征在于，包括：控制器、第一报文转发设备和第二报文转发设备；

其中，所述控制器，用于：

向所述第一报文转发设备下发流量统计指令，所述流量统计指令用于指示所述第一报文转发设备进行流量统计；所述流量统计指令携带目的地 IP 地址；

收集所述第一报文转发设备根据所述流量统计指令上报的统计数据，所述统计数据包含流向所述目的地 IP 地址的流量统计信息；

根据所述统计数据，获得流向所述目的地 IP 地址的全局流量统计值；

其中，所述全局流量统计值表示所述控制器对包括所述第一报文转发设备在内的至少两个报文转发设备上报的统计数据进行汇总后，获得的用于反映所述 SDN 范围内流向所述目的地 IP 地址的流量的统计值；

判断所述全局流量统计值是否超过预定阈值，基于所述全局流量统计值

超过预定阈值的判断结果，向所述第二报文转发设备下发 DDoS 防护策略；

所述第一报文转发设备，用于：

接收所述控制器发送的所述流量统计指令；

根据所述流量统计指令统计所述流向所述目的地 IP 地址的流量统计信

5 息；

向所述控制器上报所述统计数据；

所述第二报文转发设备，用于：

接收所述控制器发送的所述 DDoS 防护策略；

根据所述 DDoS 防护策略对所述流向所述目的地 IP 地址的流量进行防护

10 处理。

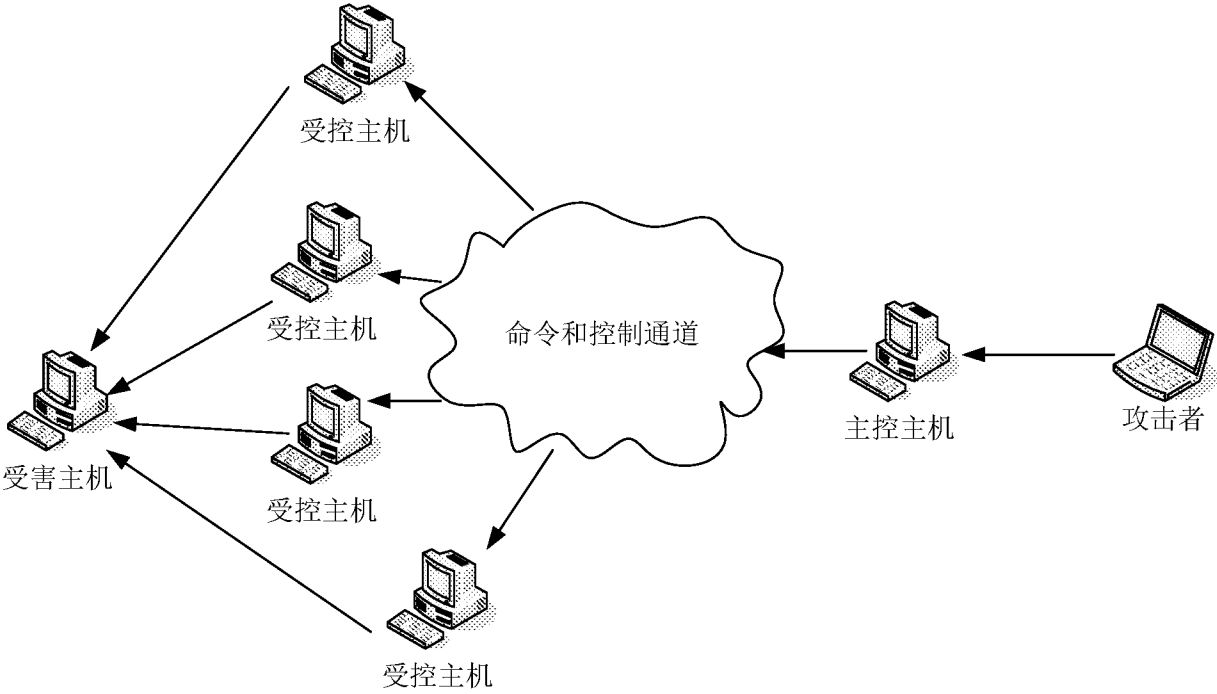


图 1

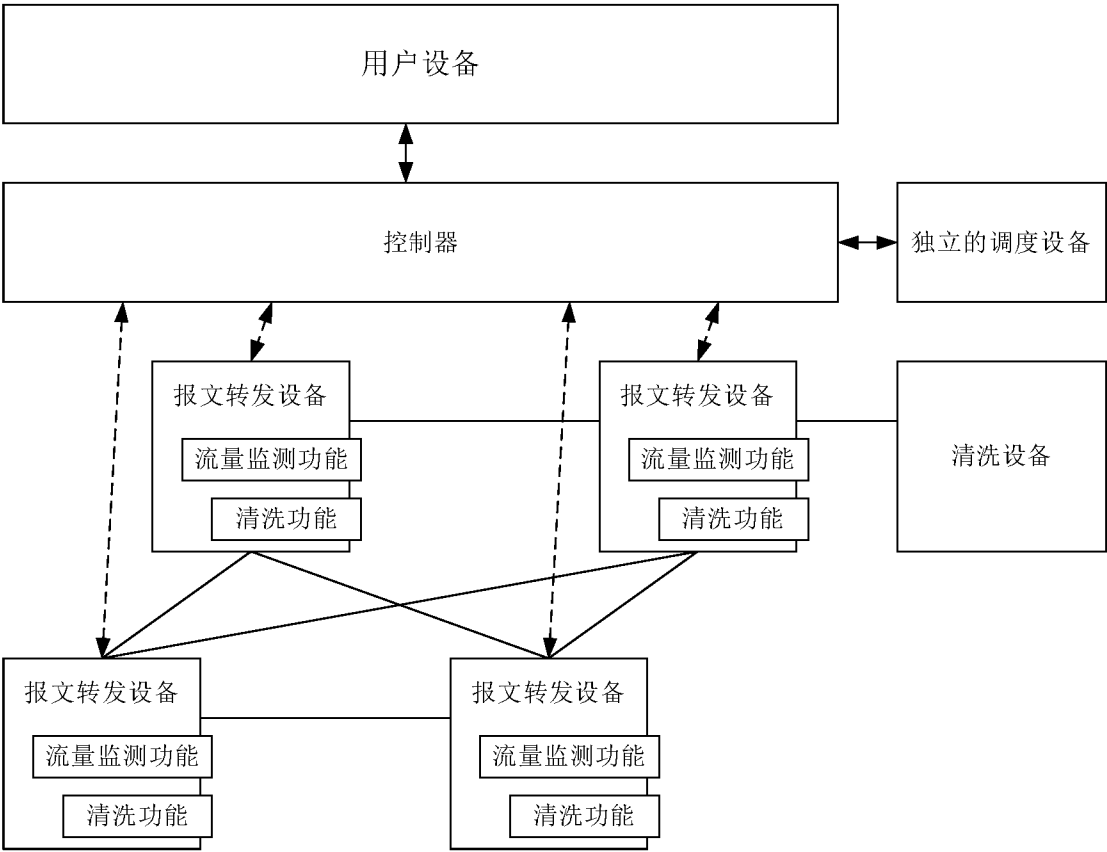


图 2

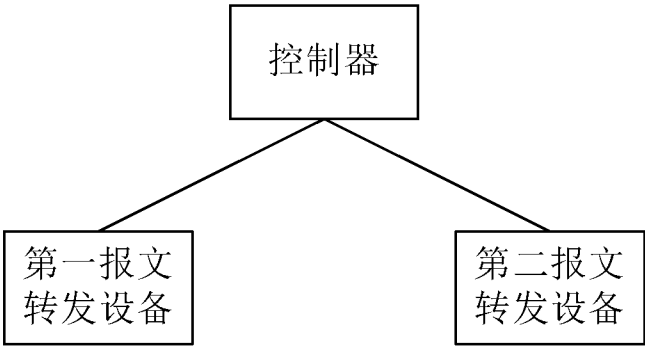


图 3

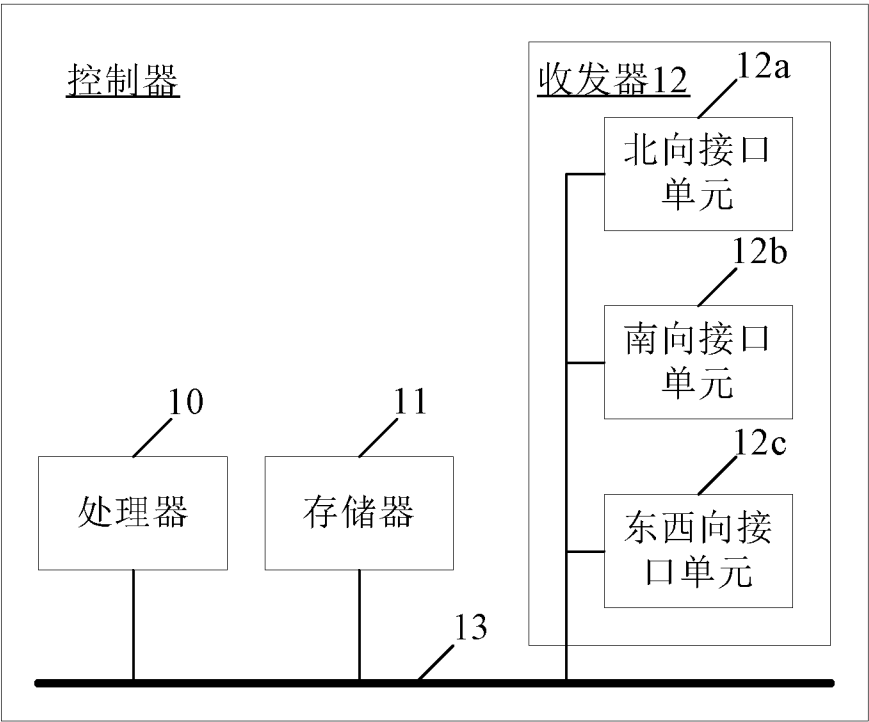


图 4

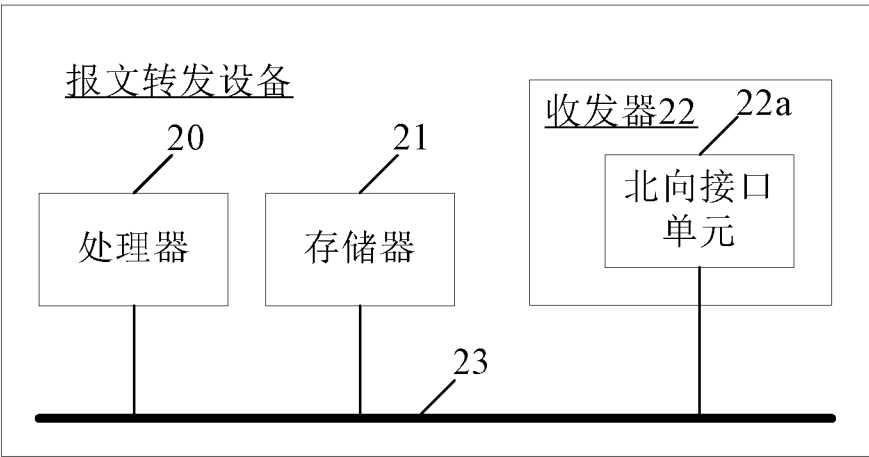


图 5

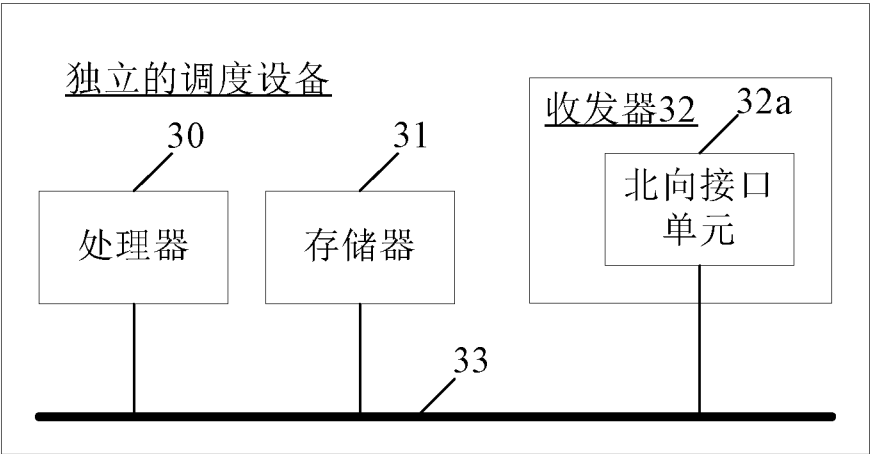


图 6

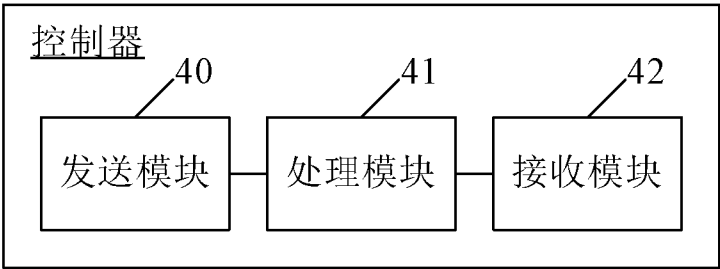


图 7

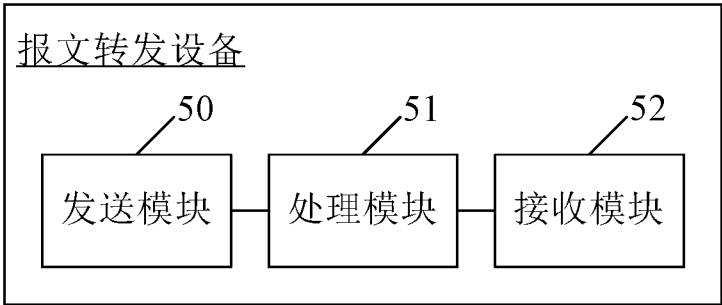


图 8

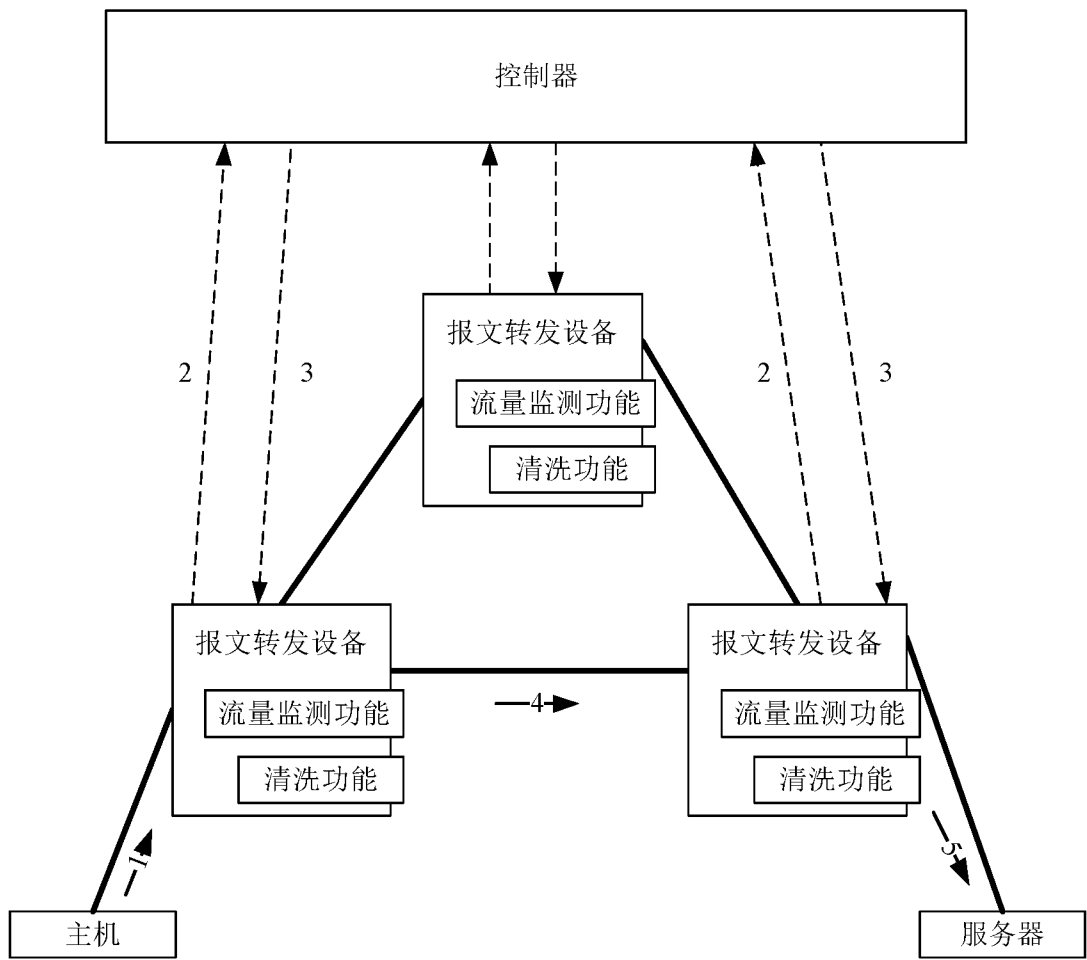


图 9

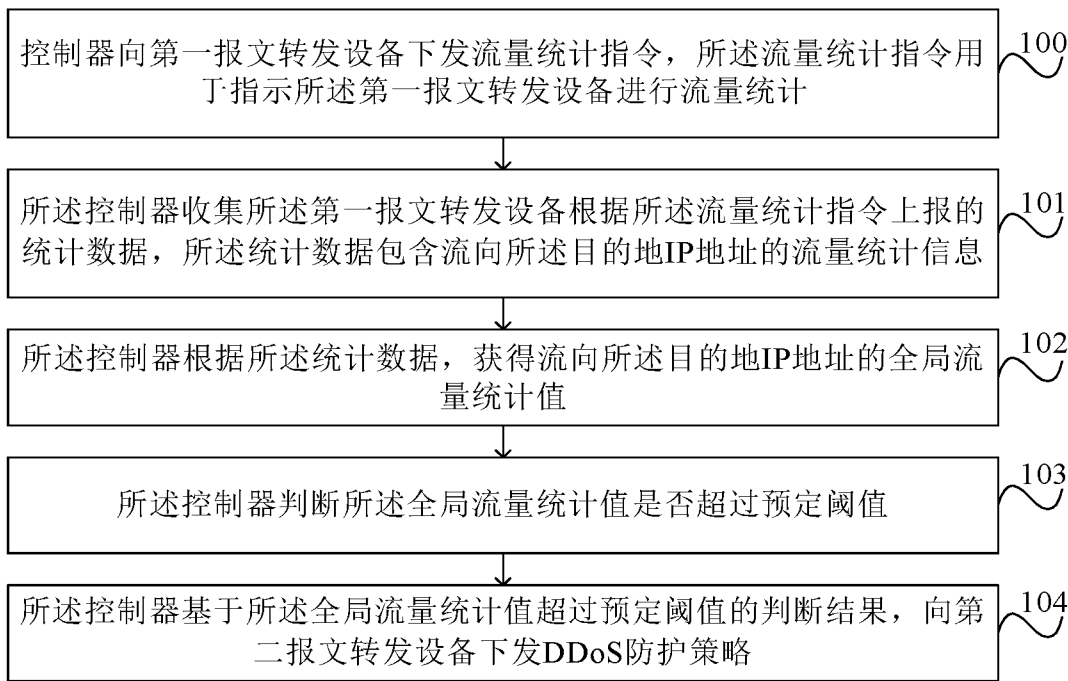


图 10

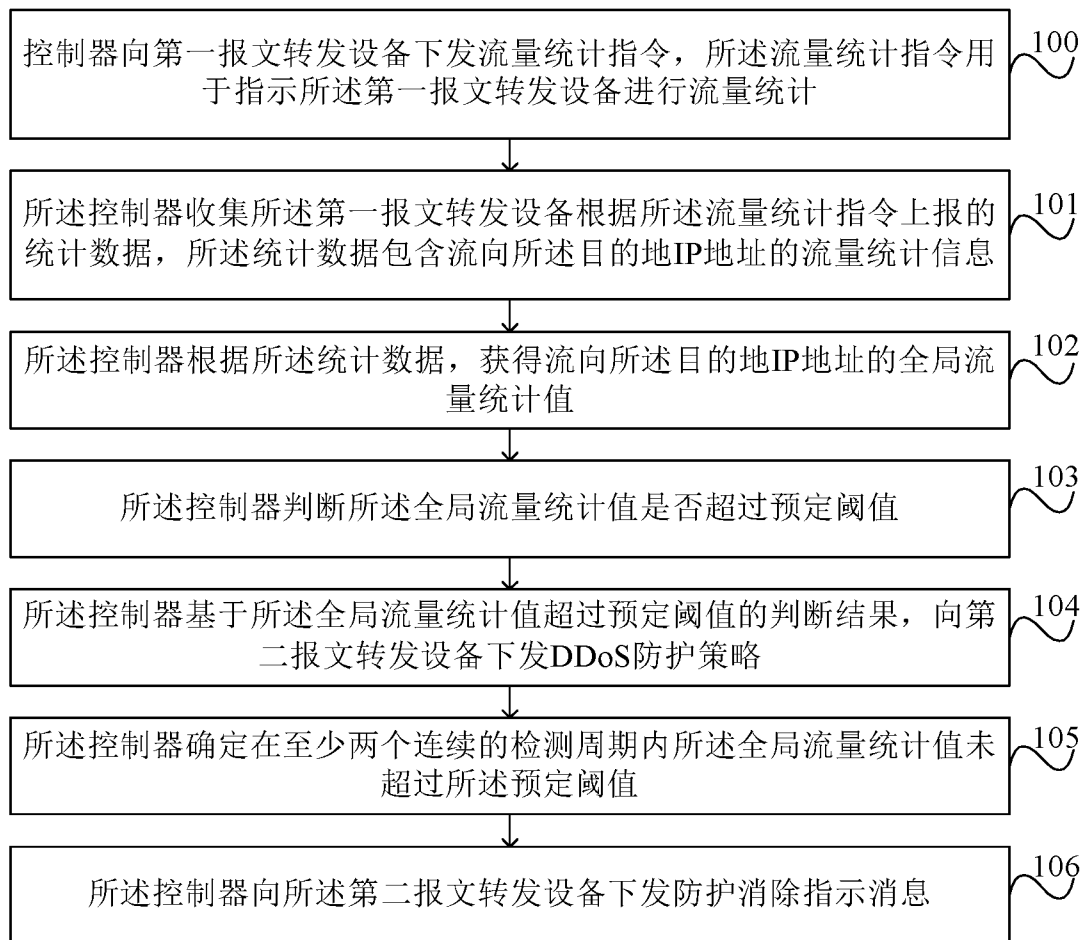


图 11

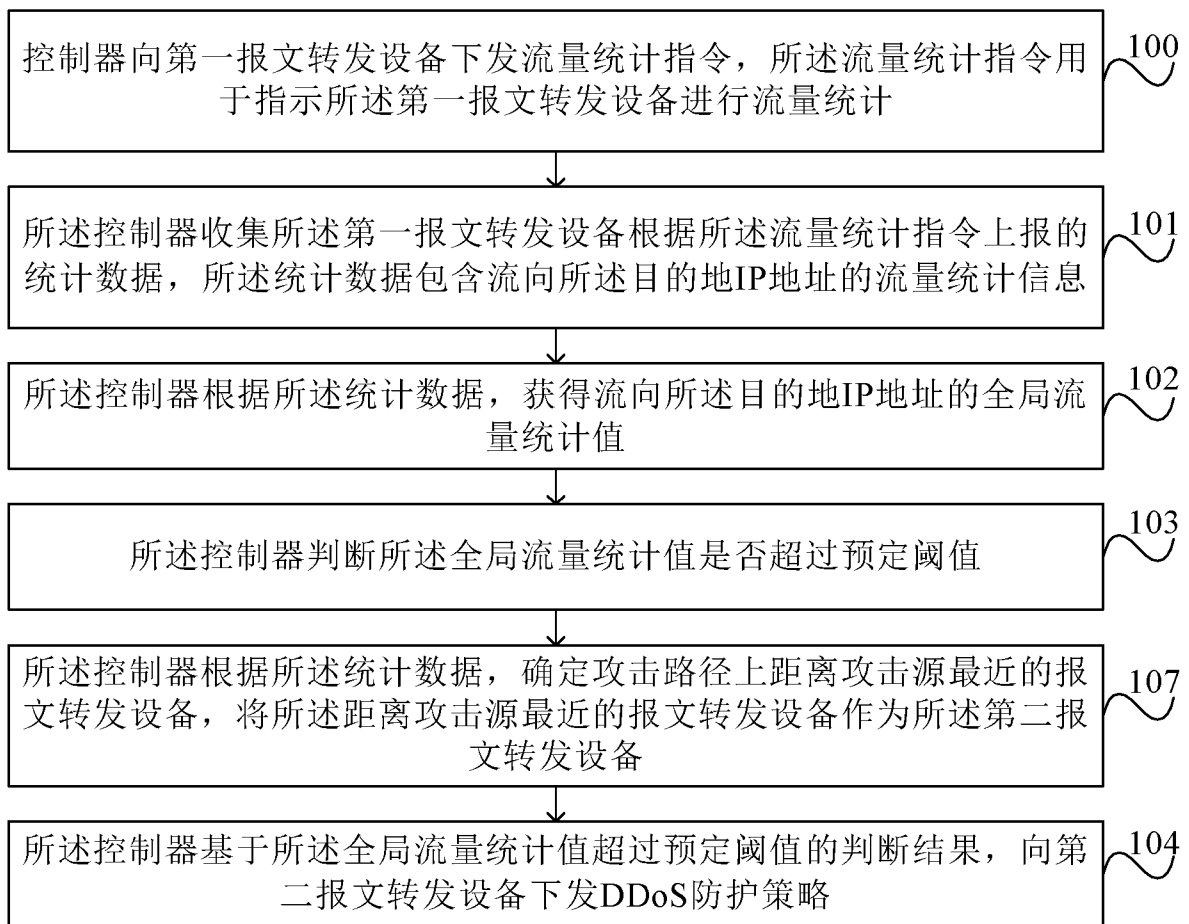


图 12

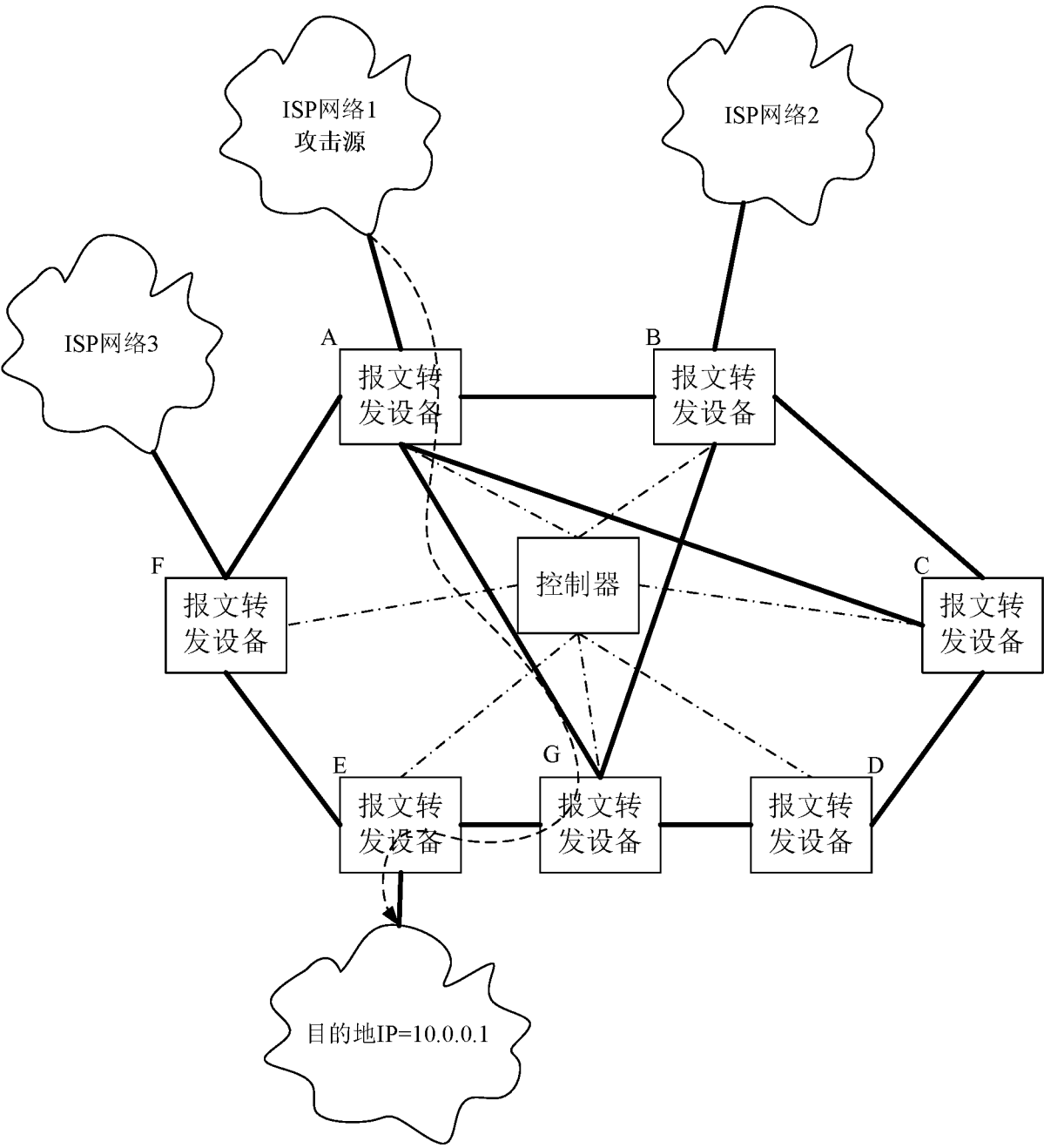


图 13

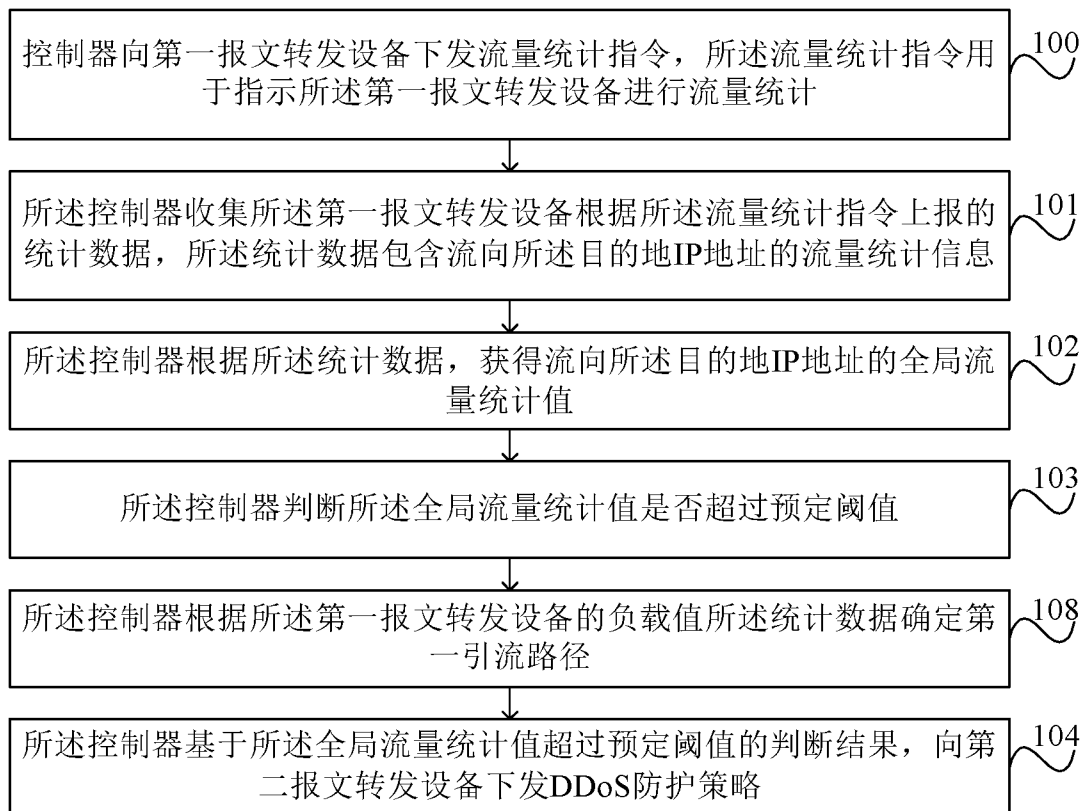


图 14

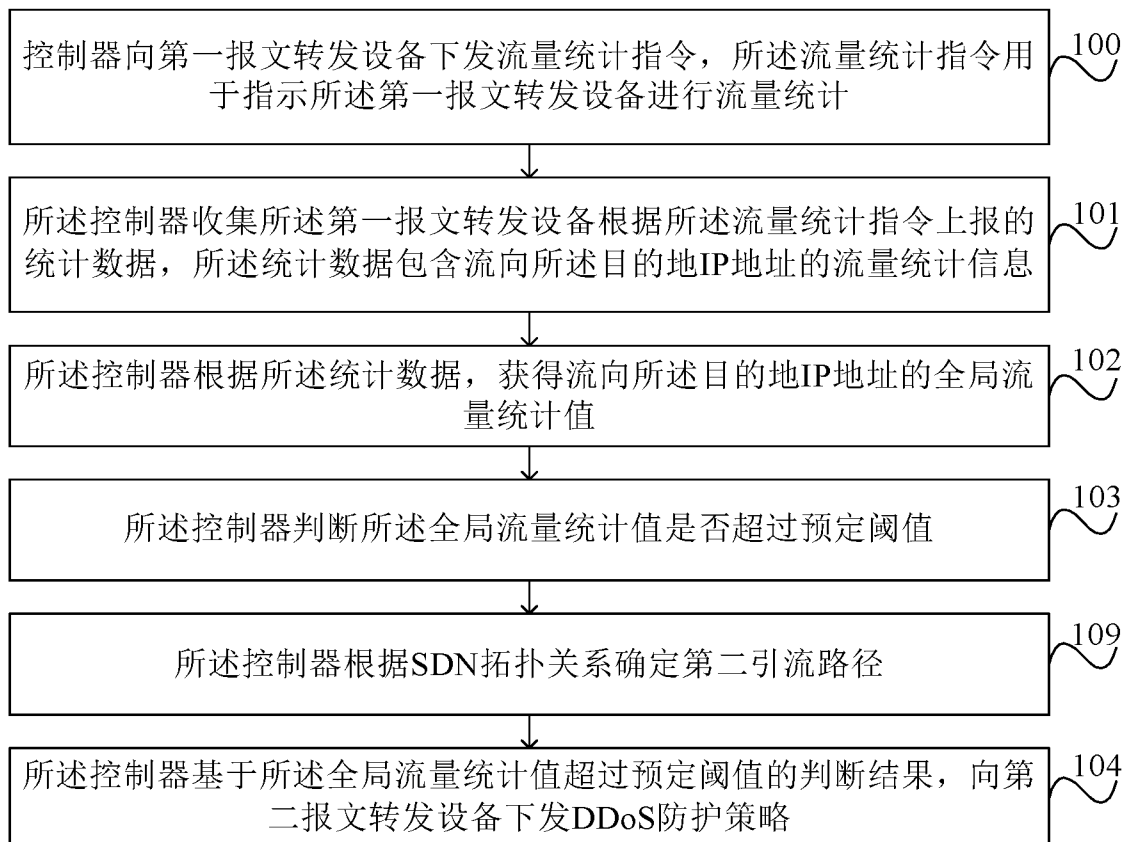


图 15

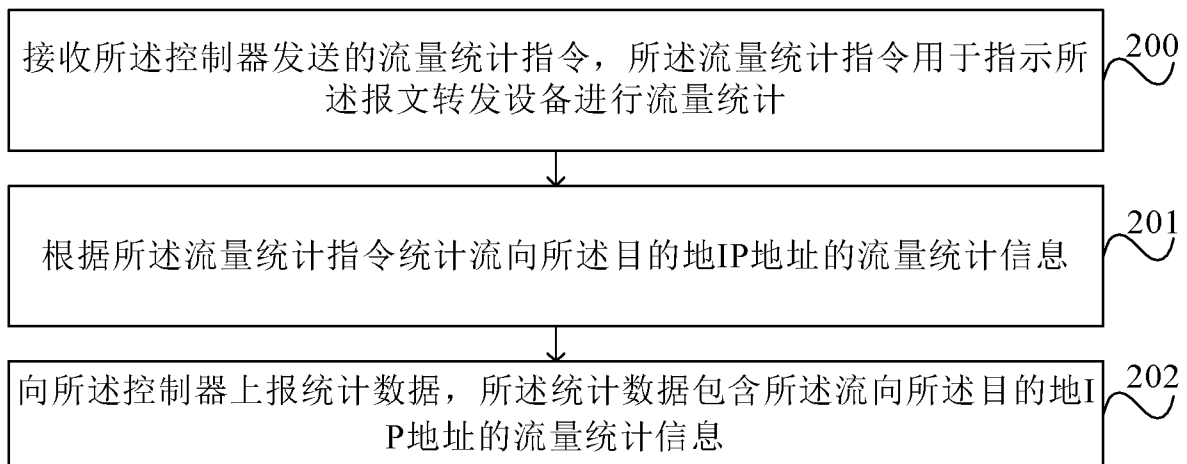


图 16

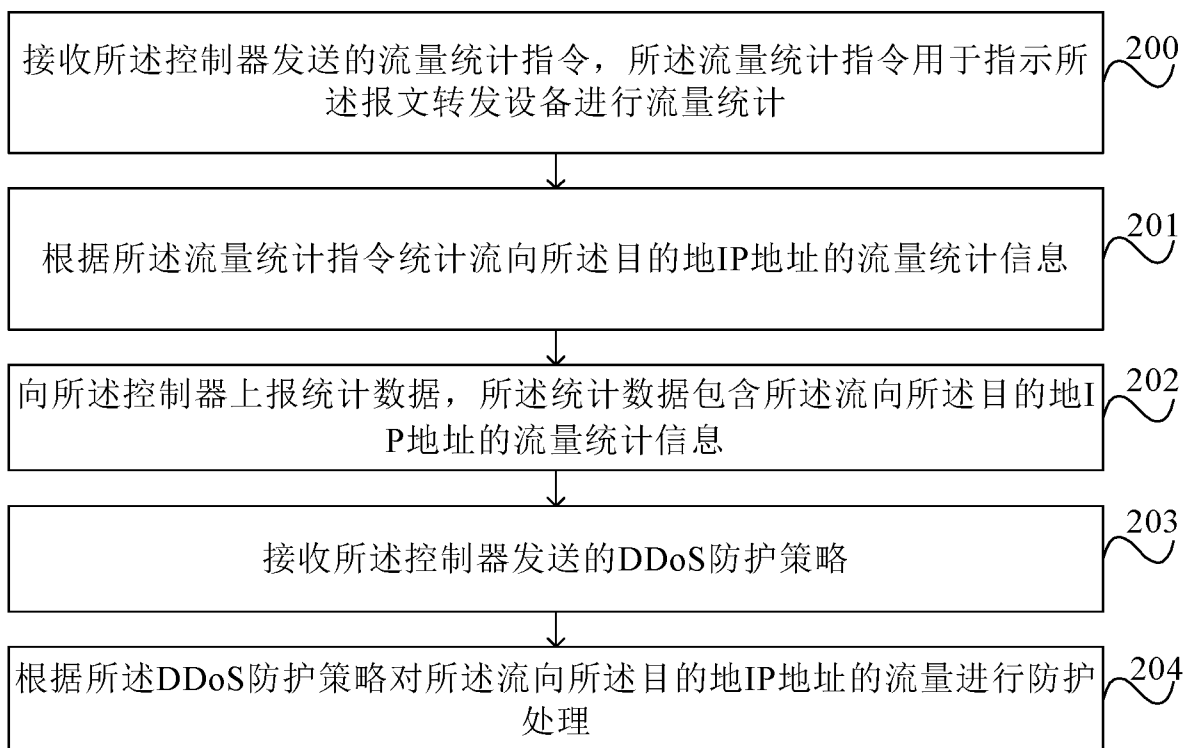


图 17

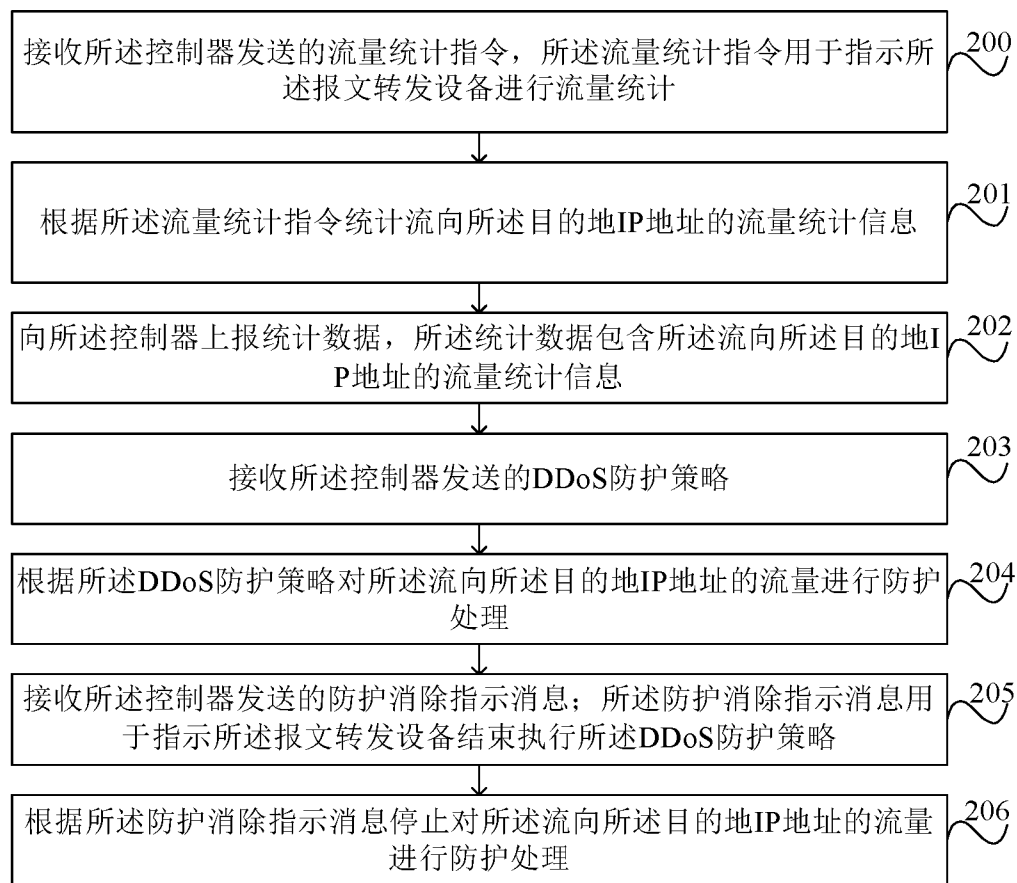


图 18

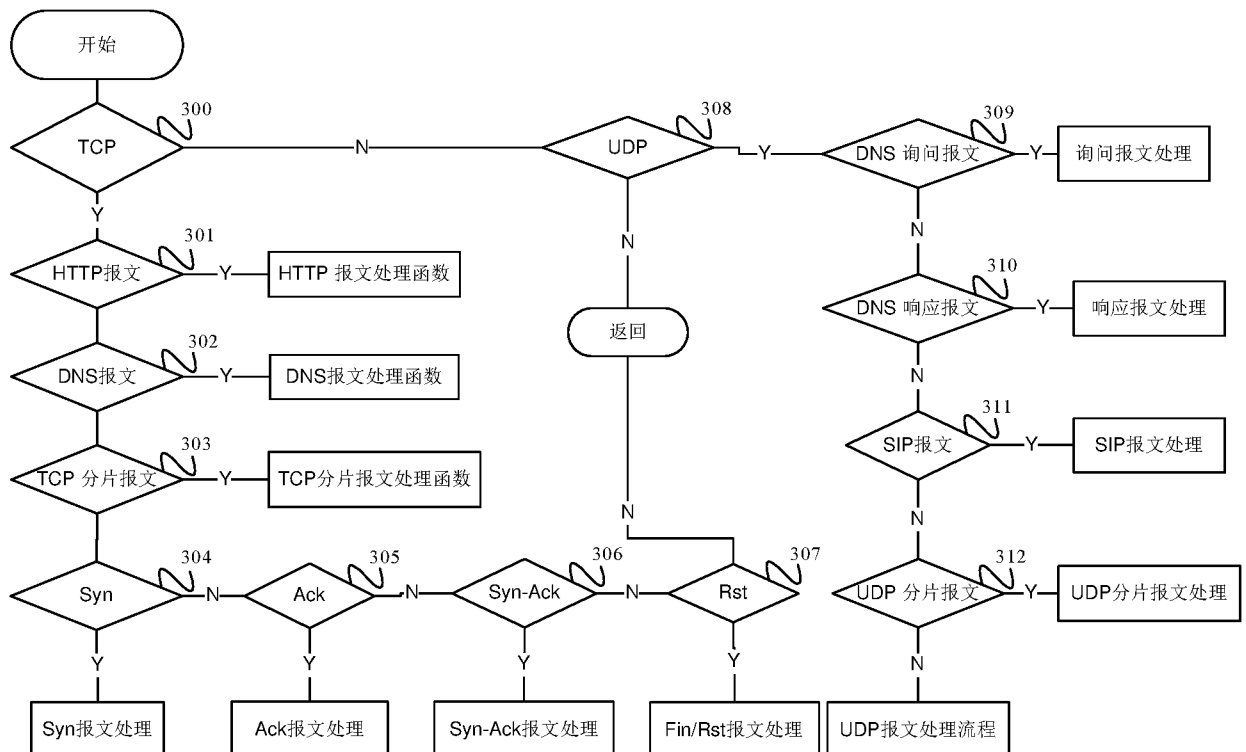


图 19

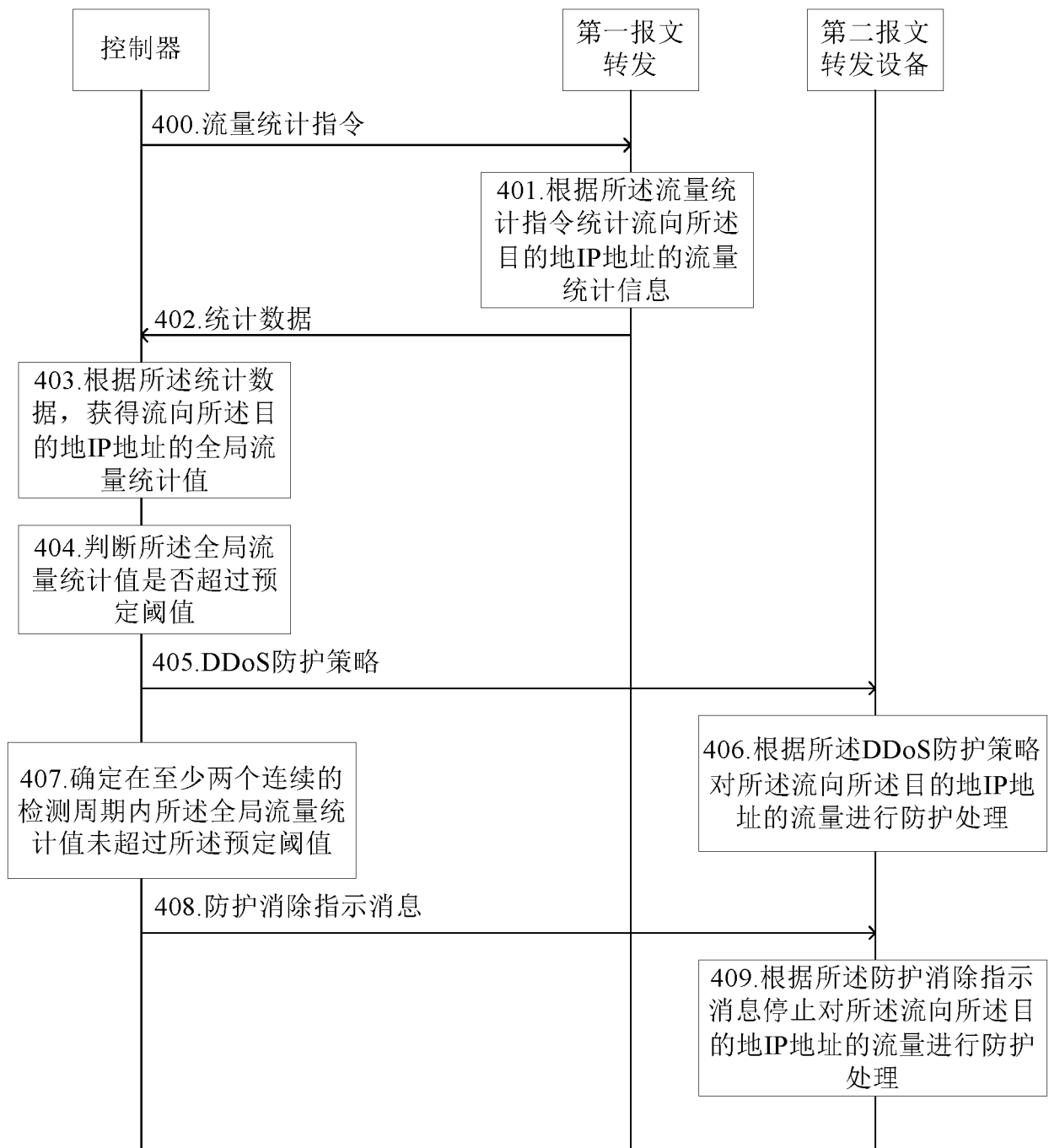


图 20

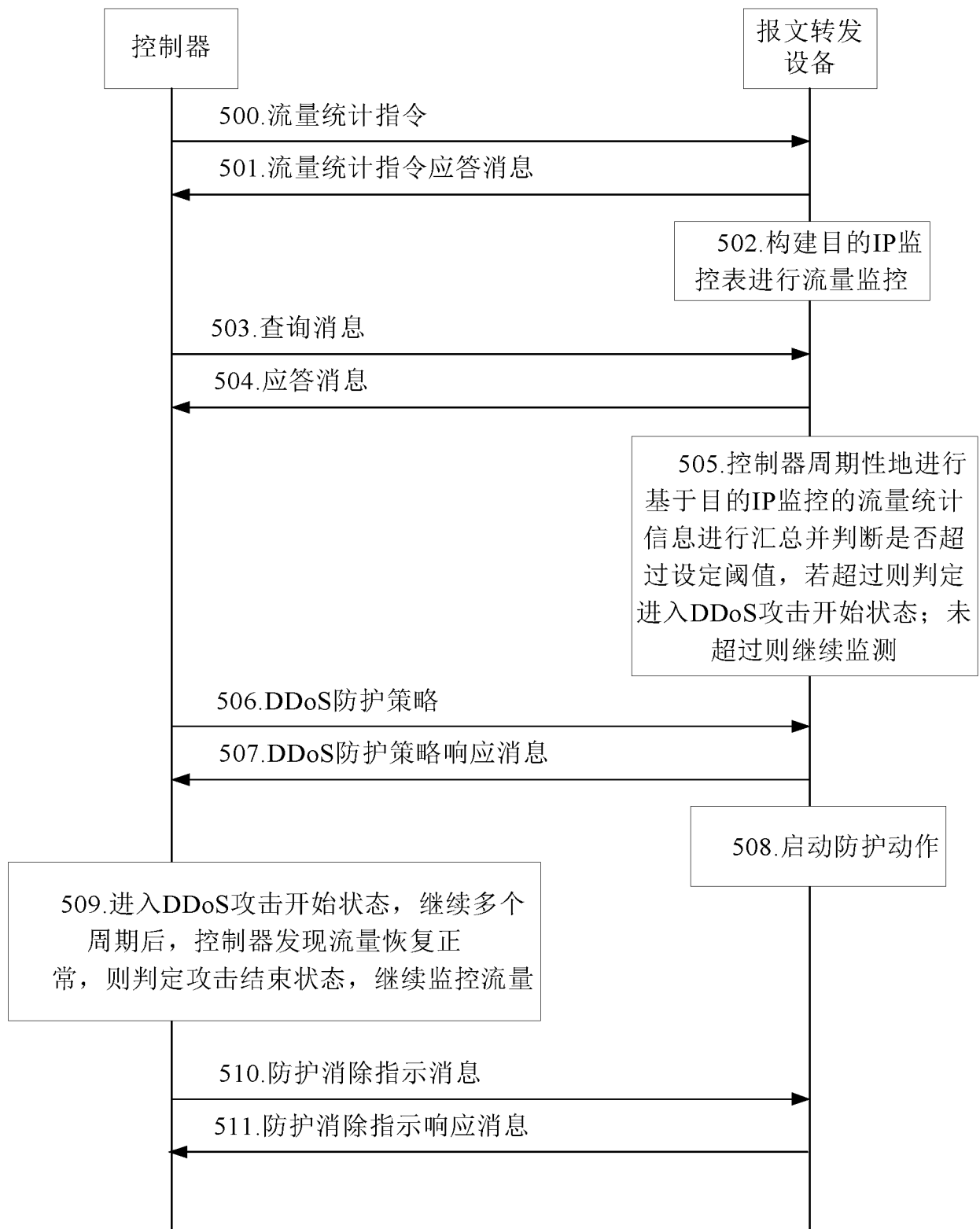


图 21

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/072781

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; CNKI; EPODOC; WPI; GOOGLE: statistics, forwarding, target, IP, DoS, address, special, designate, destination, packet, message, attack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103685057 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 March 2014 (26.03.2014), description, paragraphs [0064]-[0076], and figures 1-4	9-12, 22-25
A	CN 103685057 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 March 2014 (26.03.2014), the whole document	1-8, 13-21, 26
A	US 2014283051 A1 (RADWARE, LTD.), 18 September 2014 (18.09.2014), the whole document	1-26
A	US 2013329734 A1 (RADWARE, LTD.), 12 December 2013 (12.12.2013), the whole document	1-26
A	CN 101883078 A (SHANGHAI CLEARCRANE DIGITAL TECHNOLOGY CO., LTD.), 10 November 2010 (10.11.2010), the whole document	1-26
A	CN 101018156 A (HUAWEI TECHNOLOGIES CO., LTD.), 15 August 2007 (15.08.2007), the whole document	1-26

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 31 March 2016 (31.03.2016)	Date of mailing of the international search report 28 April 2016 (28.04.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer ZHANG, Cuiling Telephone No.: (86-10) 62413373

International application No.
PCT/CN2016/072781

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/072781

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT; CNKI; EPDOC; WPI; GOOGLE:地址, 特定, 报文, 统计, 指定, 转发, 包, 目的, 目标, 攻击, IP, DoS, address, special, designate, destination, packet, message, attack

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 103685057 A (华为技术有限公司) 2014年 3月 26日 (2014 - 03 - 26) 说明书第[0064]-[0076]段, 附图1-4	9-12, 22-25
A	CN 103685057 A (华为技术有限公司) 2014年 3月 26日 (2014 - 03 - 26) 全文	1-8, 13-21, 26
A	US 2014283051 A1 (RADWARE, LTD.) 2014年 9月 18日 (2014 - 09 - 18) 全文	1-26
A	US 2013329734 A1 (RADWARE, LTD.) 2013年 12月 12日 (2013 - 12 - 12) 全文	1-26
A	CN 101883078 A (上海清鹤数码科技有限公司) 2010年 11月 10日 (2010 - 11 - 10) 全文	1-26
A	CN 101018156 A (华为技术有限公司) 2007年 8月 15日 (2007 - 08 - 15) 全文	1-26

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 3月 31日

国际检索报告邮寄日期

2016年 4月 28日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

张翠玲

电话号码 (86-10)62413373

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/072781

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103685057	A	2014年 3月 26日	无			
US	2014283051	A1	2014年 9月 18日	无			
US	2013329734	A1	2013年 12月 12日	US	2013333029	A1	2013年 12月 12日
CN	101883078	A	2010年 11月 10日	无			
CN	101018156	A	2007年 8月 15日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)