(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
2022 年 9 月 29 日 (29.09.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/199316 A1

(51) 国际专利分类号:
H04L 47/20 (2022.01)

(21) 国际申请号: PCT/CN2022/077740

(22) 国际申请日: 2022 年 2 月 24 日 (24.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110302539.2 2021年3月22日 (22.03.2021) CN

(71) 申请人: 阿里巴巴（中国）有限公司 (**ALIBABA (CHINA) CO., LTD.**) [CN/CN]; 中国浙江省杭州市滨江区长河街道网商路699号4号楼5楼508室, Zhejiang 310052 (CN)。

(72) 发明人: 吕怡龙 (**LYU, Yilong**); 中国浙江省杭州市滨江区长河街道网商路699号4号楼5楼508室, Zhejiang 310052 (CN)。

(74) 代理人: 北京博浩百睿知识产权代理有限责任公司 (**KSK IP AGENCY**); 中国北京市海淀区知春路甲48号盈都大厦C座1单元10E, Beijing 100098 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

WO 2022/199316 A1

(54) **Title:** CONTROL METHOD AND APPARATUS, AND COMPUTING DEVICE

(54) **发明名称:** 控制方法、装置及计算设备

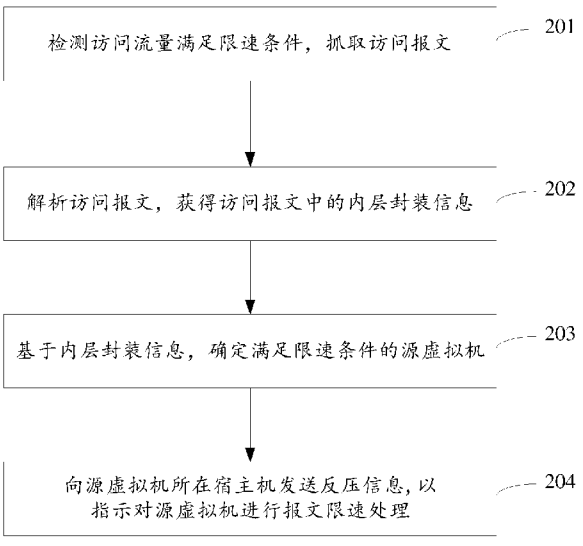


图 2

201 Detect that access traffic satisfies a speed limit condition, and capture an access packet

202 Parse the access packet to obtain inner-layer encapsulation information of the access packet

203 Determine, on the basis of the inner-layer encapsulation information, a source virtual machine that satisfies the speed limit condition

204 Send back pressure information to a host machine of the source virtual machine so as to instruct to perform packet speed limit processing on the source virtual machine

(57) **Abstract:** Embodiments of the present application provide a control method and apparatus, a computing device. The method comprises: detecting that access traffic satisfies a speed limit condition, and capturing an access packet; parsing the access packet to obtain inner-layer encapsulation information of the access packet; determining, on the basis of the inner-layer encapsulation information, a source virtual machine that satisfies the speed limit condition; and sending back pressure information to a source host machine of the source virtual machine, wherein the back pressure information is used for instructing to perform packet speed limit processing on the source virtual machine. According to the technical solution provided by the embodiments of the present application, the access packet is parsed, such that a source virtual machine that launches an attack can be identified, and back pressure can be performed on the source virtual machine to implement packet speed limit processing, and thus the problem of traffic attacks is solved.

[见续页]

SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请实施例提供一种控制方法、装置及计算设备。其中，检测访问流量满足限速条件，抓取访问报文；解析所述访问报文，获得所述访问报文中的内层封装信息；基于所述内层封装信息，确定满足限速条件的源虚拟机；向所述源虚拟机所在源宿主机发送反压信息；其中，所述反压信息用于指示对所述源虚拟机进行报文限速处理。本申请实施例提供的技术方案通过对访问报文进行解析，从而可以识别发起攻击的源虚拟机，并对其进行反压实现报文限速处理，以解决流量攻击问题。

控制方法、装置及计算设备

技术领域

本申请实施例涉及网络技术领域，尤其涉及一种控制方法、装置及计算设备。

背景技术

Overlay 网络（叠加网络或覆盖网络）是一种在现有的物理网络之上构建的虚拟网络，比如 Vxlan（Virtual Extensible Local Area Network，虚拟扩展局域网）即是一种 Overlay 网络。

Overlay 网络采用 many-to-one（多对一）通信模式的情况下，不可避免的会存在流量攻击问题，例如，多个虚拟机访问同一个虚拟机，导致目的虚拟机所在宿主机中的虚拟交换机对应的 CPU（central processing unit，中央处理器）被过多占用，进而会影响同一宿主机中的其它虚拟机的使用；又如，多个虚拟机同时通过一个虚拟网关进行其它网络访问时，导致该虚拟网关所在设备的 CPU 被过多占用，从而影响正常网络访问等。

因此，如何解决流量攻击问题成为在 Overlay 网络中目前迫切需要解决的技术问题。

发明内容

本申请实施例提供一种控制方法、装置及计算设备，用以解决现有技术中的流量攻击问题。

第一方面，本申请实施例中提供了一种控制方法，包括:

检测访问流量满足限速条件，抓取访问报文;

解析所述访问报文，获得所述访问报文中的内层封装信息;

基于所述内层封装信息，确定满足限速条件的源虚拟机;

向所述源虚拟机所在源宿主机发送反压信息；其中，所述反压信息用于指示对所述源虚拟机进行报文限速处理。

第二方面，本申请实施例中提供一种控制方法，包括:

接收反压信息；其中，反压信息由目的端针对满足限速条件的源虚拟机发送；满足限速条件的源虚拟机基于内层封装信息确定；所述内层封装信息由所述目的端检测到访问流量满足限速条件，抓取访问报文，并对所述访问报文解析获得;

按照所述反压信息，对所述源虚拟机进行报文限速处理。

第三方面，本申请实施例中提供了一种控制装置，包括:

报文抓取模块，用于检测访问流量满足限速条件，抓取访问报文;

报文解析模块，用于解析所述访问报文，获得所述访问报文中的内层封装信息;

确定模块，用于基于所述内层封装信息，确定满足限速条件的源虚拟机;

反压触发模块，用于向所述源虚拟机所在源宿主机发送反压信息；其中，所述反压信息用于指示对所述源虚拟机进行报文限速处理。

第四方面，本申请实施例中提供了一种控制装置，包括:

信息接收模块，用于接收反压信息；其中，反压信息由目的端针对满足限速条件的源虚拟机发送；满足限速条件的源虚拟机基于内层封装信息确定；所述内层封装信息由所述目的端检测到访问流量满足限速条件，抓取访问报文，并对所述访问报文解析获得;

处理模块，用于按照所述反压信息，对所述源虚拟机进行报文限速处理。

第五方面，本申请实施例中提供了一种计算设备，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行至少一个虚拟机、以及运行实现如

上述第一方面所述控制方法的虚拟交换机。

第六方面，本申请实施例中提供了一种计算设备，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行实现如上述第一方面所述控制方法的虚拟网关。

第七方面，本申请实施例中提供了一种计算设备，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行至少一个虚拟机、以及实现如上述第二方面所述控制方法的虚拟交换机。

第八方面，本申请实施例中提供了一种计算机存储介质，存储有计算机程序，所述计算机程序被计算机执行时实现如上述第一方面所述控制方法。

第九方面，本申请实施例中提供了一种计算机存储介质，存储有计算机程序，所述计算机程序被计算机执行时实现如上述第二方面所述的控制方法。

本申请实施例中，检测访问流量满足限速条件时，对访问报文进行解析可以获得内层封装信息，进而基于内层封装信息可以确定发起攻击的源虚拟机，从而可以向该源虚拟机所在目的宿主机发送反压信息，以指示对该源虚拟机进行报文限速处理，本实施例通过对访问报文进行解析，从而可以识别发起攻击的源虚拟机，并对其进行反压实现报文限速处理，以解决流量攻击问题。

本申请的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

附图说明

为了更清楚地说明本申请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作一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，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。

图 1a 示出了现有技术中的一种流量攻击场景示意图；

图 1b 示出了现有技术中的另一种流量攻击场景示意图；

图 2 示出了本申请提供的一种控制方法一个实施例的流程图；

图 3 示出了本申请实施例在一个实际应用中的反压报文的报文格式示意图；

图 4 示出了本申请提供的一种控制方法又一个实施例的流程图；

图 5 示出了本申请提供的一种控制方法又一个实施例的流程图；

图 6a 示出了本申请实施例在一个实际应用中控制交互示意图；

图 6b 示出了本申请实施例在又一个实际应用中控制交互示意图；

图 7 示出了本申请提供的一种控制装置一个实施例的结构示意图；

图 8 示出了本申请提供的一种控制装置又一个实施例的结构示意图；

图 9 示出了本申请提供的一种计算设备一个实施例的结构示意图；

图 10 示出了本申请提供的一种计算设备又一个实施例的结构示意图；

图 11 示出了本申请提供的一种计算设备又一个实施例的结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述。

在本申请的说明书和权利要求书及上述附图中的描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的序号如 101、102 等，仅仅是用于区分开各个不同的操作，序号本身不代表任何的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。需要说明的是，本文中的“第一”、“第二”等描述，是用于区分不同的消息、设备、模块等，不代表先后顺序，也不限定“第一”和“第二”是不同的类型。

本申请实施例的技术方案应用于虚拟网络中，用于解决虚拟网络中的流量攻击问题，例如 Overlay 网络（叠加网络或覆盖网络）中的流量攻击问题。

为了便于理解，下面首先对本申请实施例中可能涉及的技术术语进行相应解释:

虚拟机（英文：Virtual Machine，简称：VM）：是指一种通过软件模拟的具有完整硬件系统功能的，并运行在一个完全隔离环境中的完整计算机系统。

宿主机：运行虚拟机的物理主机。

Overlay 网络：一种在现有的物理网络之上构建的虚拟网络。

Vxlan（Virtual Extensible Local Area Network，虚拟扩展局域网）：是在三层网络之上构建的二层网络的一种 Overlay 网络，采取将原始报文封装在 UDP（User Datagram Protoco，用户数据协议）数据包里的封装格式。

五元组信息：包括源 IP（Internet Protocol，网际互连协议）地址，源端口，目的 IP 地址，目的端口和传输层协议，在虚拟网络中，封装在内层的五元组信息中的源 IP 地址为源虚拟机的虚拟 IP 地址，源端口为源虚拟机的虚拟端口，目的 IP 地址为目的端的虚拟 IP 地址，源端口为目的端的虚拟端口。通过内层五元组信息可以唯一标识一个报文流。

报文流：是指一个源 IP 地址和目的 IP 地址之间传输的报文形成的流，一个报文流中的所有报文的五元组信息相同。

虚拟交换机（英文：Virtual Switch，简称 VSwitch）：为运行在本台宿主机中的虚拟机提供二层网络接入和部分三层网络功能，源虚拟机对目的虚拟机的访问需经由虚拟交换机实现，负责转发源虚拟机的访问报文至目的虚拟机。

虚拟网关（中文：Virtual gate，简称：VG）：用以实现虚拟机所在网络与其它网络的互连，

以 Overlay 网络为例，随着云计算技术的发展，目前云数据中心通常是

基于 Overlay 网络实现，在 Overlay 网络中，采用 many-to-one（多对一）通信模式的两种常见访问方式造成的流量攻击场景，分别如图 1a 和如图 1b 所示，图 1a 中示出了多个虚拟机同时访问一个虚拟机的情况，实际应用中，一台宿主机中可能安装有多个虚拟机，如图 1a 中所示，位于源宿主机 10 中的源虚拟机 101，通过源宿主机 10 中的源虚拟交换机 102 向目的宿主机 20 中的某个目的虚拟机 103 请求发送访问报文，由目的宿主机 20 中的目的虚拟交换机 104 负责转发访问报文至该目的虚拟机 103，在 many-to-one 通信模式中，可能会有多个源虚拟机 101 同时向一个目的虚拟机 103 不断请求发送访问报文，其中，多个源虚拟机 101 可能位于同一个源宿主机 10 中，也可能位于多个源宿主机 10 中，那么此时，目的虚拟机交换机 104 会接收到大量访问报文，同时需要进行大量报文转发，就可能导致目的虚拟机交换机 104 对应的转发 CPU 的转发容量过高而被打满，影响转发 CPU 的处理性能，进而就会影响目宿主机 20 中其它虚拟机的正常使用。

图 1b 示出了多个虚拟机同时通过虚拟网关访问公网的情况，如图 1b 中所示，源宿主机 30 中的源虚拟机 105，会通过源宿主机 30 中的源虚拟交换机 106，向虚拟网关 107 发送访问报文，以请求访问向公网 40，由虚拟网关 107 负责进行报文转发，在 many-to-one 通信模式中，可能会有多个源虚拟机 105 同时向虚拟网关 107 发送访问报文，多个源虚拟机 105 可能位于同一个源宿主机 30 中，也可能位于多个源宿主机 30 中，那么此时，虚拟网关 107 会接收到大量访问报文，同时需要进行大量报文转发，就可能导致虚拟网关 107 对应的转发 CPU 的转发容量过高而被打满，影响转发 CPU 的处理性能，进而就会影响其它虚拟机通过该虚拟网关的正常网络访问。

为了解决流量攻击问题，发明人在实现本申请的过程中发现，Overlay 网络中，虚拟机的原始报文会被二次封装，添加网络相关信息如宿主机地址等形成访问报文。也即访问报文中的原始报文封装在内层，外层为网络相关信息。以 Vxlan 为例，Vxlan 报文中是将原始报文封装在 UDP 数据格式中，将

原始报文添加 Vxlan 头部一起封装在 UDP 数据包中，Vxlan 头部信息例如可以包括 Vxaln 标识、IP 头部等，IP 头部主要包括主机之间通信的主机 IP 地址等，Vxlan 头部信息当然还可以包括其它信息，这与现有的相同，本申请不进行过多赘述。而原始报文是虚拟机之间真正传输的报文，其头部信息例如包括了虚拟机之间进行通信的虚拟机 IP 地址、端口、传输层协议等等。

由于原始报文进行了二次封装，无法确定访问报文是由谁来发出的，也就没有办法确定攻击方。而采用本申请实施例的技术方案，结合虚拟交换机或虚拟网关的报文解析能力，可以对访问报文进行解析，以识别产生攻击的源虚拟机，进而可以构造反压信息，实现了对源虚拟机的报文限速处理，从容可以实现解决流量攻击的问题。

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

图 2 为本申请提供的一种控制方法一个实施例的流程图，本实施例的技术方案可以由被攻击方的目的端执行，如虚拟交换机执行或者虚拟网关等，该方法可以包括如下几个步骤:

201：检测访问流量满足限速条件，抓取访问报文。

其中，访问流量是否满足限速条件可以通过检测转发 CPU 的转发容量或者 CPU 水位实现，若转发容量高于一定容易或者 CPU 水位大于一定水位时，可以认为访问流量满足限速条件。

若访问流量满足限速条件，可以从转发 CPU 中抓取访问报文。

实际应用中，虚拟机交换机或者虚拟网关可能会利用一个或多个 CPU 实现其功能，转发 CPU 即是指负责报文转发的 CPU。

可选地，可以按照采样频率及采样数量抓取访问报文，也即在转发 CPU 中进行抓包采样，例如 1 秒种抓取 1000 个访问报文。

需要说明的是，抓取访问报文并非对访问报文进行拦截，而对访问报文进行镜像处理，复制获得的访问报文。目的端仍然会基于访问报文进行正常的访问处理，如转发至目的虚拟机或者外网等。

202：解析访问报文，获得访问报文中的内层封装信息。

对抓取的访问报文可以进行解析，获得其内层封装信息。

该内层封装信息主要是指封装在访问报文中的原始报文中的头部信息，例如内层五元组信息。

203：基于内层封装信息，确定满足限速条件的源虚拟机。

由于内层五元组信息可以唯一标识一条报文流，基于报文流中的报文数量，可以确定是哪条报文流造成攻击，进而可以根据该报文流对应内层五元组信息中的源 IP 地址可以确定对应源虚拟机。

因此，可选地，基于内层封装信息，确定满足限速条件的源虚拟机包括：基于内层封装信息标识的报文流，对访问报文进行汇总以确定不同报文流的报文数量；按照不同报文流的报文数量，选择待限速报文流；确定待限速报文流对应的源虚拟机。

作为一种可选方式，按照不同报文流的报文数量，选择待限速报文流可以是：按照不同报文流的报文数量，选择报文数量大于或等于预设数量的待限速报文流。

作为另一种可选方式，按照不同报文流的报文数量，确定待限速报文流包括：按照报文数量从大到小的顺序，选择前 N 个报文流作为待限速报文流。

其中，满足限速条件的源虚拟机可能包括多个，对于每个满足限速条件的源虚拟机均可以按照如下方式进行报文限速处理。

204：向源虚拟机所在宿主机发送反压信息；其中，反压信息用于指示对源虚拟机进行报文限速处理。

确定出满足限速条件的源虚拟机，即可以发送反压信息，该反压信息具体由源宿主机中的源虚拟交换机接收，并按照反压信息对该源虚拟机进行限

速处理。

其中，可以基于解析访问报文获得的外层封装信息中的宿主机地址来发送该反压信息，宿主机地址可以具体是指宿主机 IP 地址。

本实施例中，检测访问流量满足限速条件时，对访问报文进行解析可以获得内层封装信息，进而基于内层封装信息可以确定发起攻击的源虚拟机，从而可以向该源虚拟机所在目的宿主机发送反压信息，以指示对该源虚拟机进行报文限速处理，本实施例通过对访问报文进行解析，从而可以识别了发起攻击的源虚拟机，并对其进行反压实现报文限速处理，以解决流量攻击问题。

在某些实施例中，该方法还可以包括:

确定源虚拟机中的反压对象；其中，反压对象可以是指源虚拟机发出的全部报文流、源虚拟机发向其发出的待限速报文流对应的目的虚拟机的全部报文流、或者源虚拟机发出的待限速报文流;

至少根据反压对象，生成反压信息；其中，反压信息用于指示对反压对象进行限速处理。

由于源虚拟机可能会发出多条报文流，而产生流量攻击的可能仅是其中一条报文流。对于确定出的该源虚拟机的待限速报文流，可以是将该待限速报文流作为反压对象，或在多个源虚拟机同时访问一个目的虚拟机的场景下，基于该待限速报文流对应内层五元组信息中目的IP地址可以确定目的虚拟机，可以是将发往该目的虚拟机的全部报文流作为反压对象；或者直接将源虚拟机发出的全部报文流均作为反压对象。其中，反压对象可以结合结合实际需求进行预先设定等。

在某些实施例中，该方法还可以包括:

确定源虚拟机对应的限速处理方式及报警处理方式中的至少一种处理方

式;

至少根据至少一种处理方式，生成反压信息；其中，反压信息用于指示按照至少一种处理方式对源虚拟机进行报文限速处理。

可选地，还可以确定源虚拟机中的反压对象；则可以具体是根据该至少一种处理方式及该反压对象，生成反压信息，以指示按照至少一种处理方式对源虚拟机中的反压对象进行报文限速处理。

在某些实施例中，该方法还可以包括:

在至少一种处理方式包括限速处理方式的情况下，确定源虚拟机对应的限速类型;

至少根据至少一种处理方式，生成反压信息包括:

至少根据至少一种处理方式及限速类型，生成反压信息；其中，反压信息可以具体是指示按照该限速流行对应的限速处理方式对源虚拟机进行限速处理。

可选地，还可以是至少根据该至少一种处理方法、该限速类型及反压对象生成反压信息。

实际应用中，限速处理方式可以包括调整发送报文的包转发率（英文: Packet Forwarding Rate，简称: pps）和/或比特率，pps 限速可以是通过限制每秒发包数来实现，比特率可以通过限制 bps（Bit Per Second，每秒比特数）来实现。限速类型即可以包括 pps 限速及 bps 限速中的至少一种。

此外，由于一个宿主机中可能会安装多个虚拟机，且一个虚拟机可能会发送多条报文流，为了方便源虚拟交换机确定反压信息针对的反压对象，可选地，该反压信息中还可以包括该内层封装信息中的内层五元组信息等。

此外，该反压信息中还可以包括虚拟网络标识，例如 Vxlan 网络中的 VNI（Vxlan Network Identifier，Vxlan 标识），只有在同一个虚拟网络上的虚拟

机之间才能相互通信，从而可以基于反压信息中的虚拟网络标识和内层五元组信息可以识别源虚拟机中的反压对象。

结合上文描述可知，反压信息中可以包括至少一种处理方式、限速信息、反压对象、内层封装信息中的内层五元组信息、虚拟网络标识中的至少一个等，此外，还可以包括内层封装信息中的网络协议；此外，在虚拟网关受到流量攻击的场景下，流量攻击可能是来自于内网，也可能是来自于外网，因此该反压信息中还可以包括流量攻击方向等。

其中，报警处理方式可以指示对源虚拟机进行报警处理，例如包括获取源虚拟机的当前发包情况、源虚拟机的虚拟机标识、反压对象标识等作为应答信息反馈给目的端，由目的端据此进行报警等，如输出报警提示信息。

限速处理方式可以指示对源虚拟机进行 pps 限速和/或 bps 限速，并获取源虚拟机的当前发包情况、源虚拟机的虚拟机标识、反压对象标识等反馈给目的端，由目的端据此进行报警等，如输出报警提示信息。

因此，在某些实施例中，该方法还可以包括:

接收按照反压信息对源虚拟机进行报文限速处理之后反馈的应答信息;

基于应答信息，输出报警提示信息。

可选地，该应答信息中可以包括源虚拟机标识、反压对象标识和/或源虚拟机的当前发包情况等。

当前发包情况例如可以包括当前包转发率、最近预设时间范围内的平均包转发率、最近预设时间范围内的最大包转发率，还可以包当前比特率、最近预设时间范围内的平均比特率、最近预设时间范围内的最大比特率等。

可选地，输出报警提示信息可以基于相关人员的通信账号，将发送该报警提示信息，当然也可以发送至相应显示设备显示该报警提示信息等，以方便相关人员发生攻击的源虚拟机、当前攻击情况、和/或限速效果等

实际实现中，反压信息可以封装为反压报文进行发送，因此，在某些实施例中，该方法还可以包括：解析访问报文获得外层封装信息；

则向源虚拟机所在宿主机发送反压信息包括：

基于反压指示信息，及源虚拟机对应的内层封装信息和外层封装信息，构造反压报文；

将反压报文作为反压信息，发送至源虚拟机所在宿主机。

其中，外层封装信息可以具体包括源宿主机地址、此外，还可以目的主机地址等。

在某些实施例中，反压报文可以至少包括反压指示信息对应的至少一个反压字段、宿主机地址字段、网络标识字段、及内层五元组分别对应的字段；

则基于反压指示信息，及源虚拟机对应的内层封装信息和外层封装信息，构造反压报文可以包括：

将反压指示信息填入至少一个反压字段；

将源虚拟机对应外层封装信息中的源宿主机地址，填入宿主机地址字段；

将源虚拟机对应外层封装信息中的虚拟网络标识，填入网络标识字段；

将源虚拟机对应的内层封装信息中的内层五元组信息，填入内层五元组分别对应的字段。

其中，反压指示信息具体用于指示如何进行报文限速处理等；源宿主机地址用以据此发送该反压报文；虚拟网络标识及内层五元组信息用以识别需要进行限速处理的源虚拟机及其反压对象等。

由上文描述可知，反压指示信息例如可以包括至少一种处理方式、反压对象、限速类型等等。

因此，在某些实施例中，该至少一个反压字段可以包括处理方式字段、限速类型字段及反压对象字段；

则将反压指示信息填入至少一个反压字段可以包括：

确定源虚拟机对应的限速处理方式及报警处理方式中的至少一种处理方

式，将标识至少一个处理方式的参数数值写入处理方式字段；例如数值 0 表示限速处理方式，数值 1 报警处理方式；

在至少一种处理方式包括限速处理方式的情况下，确定源虚拟机对应的限速类型，将标识限速类型的参数数值写入限速类型字段；例如，数值 0 表示 pps 限速，数值 1 表示 bps 限速，数值 2 表示同时执行 pps 限速及 bps 限速；

确定源虚拟机中的反压对象，并基于反压对象确定内层五元组信息中的有效信息，以及将标识有效信息的参数数值写入反压对象字段；例如数值 0 表示内层五元组信息中源 IP 地址有效，数值 1 表示内层五元组信息中的三元组即源 IP 地址、目的 IP 地址以及传输层协议有效，数值 2 表示内层五元组全部有效。其中，源 IP 地址有效表示反压对象为源虚拟机发出的全部报文流，三元组有效表示反压对象为源虚拟机发向其发出的待限速报文流对应的目的虚拟机的全部报文流、五元组有效表示的反压对象为源虚拟机发出的待限速报文流。

在某些实施例中，反压报文还可以包括至少一个反馈字段；至少一个反馈字段用于进行报文限速处理之后填入处理结果，以生成应答报文；

该方法还可以包括：接收应答报文；基于应答报文，输出限速提示信息。

可选地，可以是将该应答报文作为限速提示信息。

其中，该至少一个反馈字段例如可以包括用于填入源虚拟机的虚拟机标识的虚拟机标识字段；此外，还可以包括：用于填入反压对象当前包转发率的包转发率字段和/或用于填入反压对象当前比特率的当前比特率字段；此外，还可以包括：用于填入反压对象最近预设时间范围内的平均包转发率的平均包转发率字段、用于填入反压对象最近预设时间范围内的最大包转发率的最大包转发率字段、用于填入反压对象最近预设时间范围内的平均比特率的平均比特率字段、以及用于填入反压对象最近预设时间范围内的最大比特率的最大比特率字段等中的至少一个。该最近预设时间范围例如可以是指最近 10

分钟。

源虚拟交换机可以基于该至少一个反馈字段，获取相应的处理结果并填入相应反馈字段中。

在某些实施例中，该反压报文还可以包括攻击方向字段，该方法还可以包括:

在至少一种处理方式包括报警处理的情况下，确定流量攻击方向;

将标识流量攻击方向的参数数值，填入攻击方向字段。例如，数值 0 表示内网攻击，数值 1 表示外网攻击。

该攻击方向字段中的字段值标识的流量攻击方向用以作为一种报警信息，在反压报文中填入报文限速处理之后的处理结果之后，形成应答报文输出。

在某些实施例中，该反压报文还可以包括网络协议字段，该方法还可以包括:

将标识内层网络协议的参数数值，写入网络协议字段; 例如，数值 0 表示 ipv4(Internet Protocol version 4, 网际协议版本 4), 数值 1 表示 ipv6(Internet Protocol version 6，网际协议版本 6 ）。

该网络协议字段用于按照字段值标识的网络协议从反压报文中解析获得内层五元组信息。

为了便于理解，如图 3 中所示，示出了在一个实际应用中的反压报文的报文格式示意图，结合上文相关描述下面对该反压报文中可能包括的字段进行介绍:

Action: 处理方式字段, 取值可以包括 0 或 1; 数值 0 表示报警处理方式，指示仅报警不限速; 数值 1 表示限速处理方式，执行限速动作。

Limit_type: 限速类型字段，取值可以包括 0、1 或 2; 数值 0 表示进行

pps 限速，数值 1 表示进行 bps 限速，数值 3 表示同时进行 pps 限速和 bps 限速。可选地，Action 取值为 0 时，该 Limit_type 可以为空值。

Direction: 攻击方向字段，取值可以包括 0 或 1，数值 0 表示内网方向，数值 1 表示外网方向；其中，Direction 取值为 1 时，Action 取值为 0。

key_type: 反压对象字段，取值可以包括 0、1 或 2，数值 0 表示内层源 IP 地址有效，数值 1 表示内层三元组（源 IP 地址、目的 IP 地址、传输层协议）有效，数值 2 表示内层五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、传输层协议）有效。

Ncip: 宿主机字段，取值为满足限速条件的源虚拟机所在的宿主机的宿主机 IP 地址;

tunnel id: 网络标识字段，取值为满足限速条件的源虚拟机所在虚拟网络的虚拟网络标识，例如 VNI。

Af: 网络协议字段，取值为内层网络协议。

inner_proto: 内层五元组字段之一，内层协议字段，取值内层传输层协议号。

inner_src ip: 内层五元组字段之一，内层源地址字段，取值为内层源 Ip 地址;

inner_dst ip: 内层五元组字段之一，内层源地址字段，取值为内层目的 IP 地址;

inner src port: 内层五元组字段之一，内层源端口字段，取值为内层源端口号;

inner dst port: 内层五元组字段之一，内层目的端口字段，取值为内层目的端口号。

ecs_id: 虚拟机标识字段，取值为满足限速条件的源虚拟机的虚拟机标识，如虚拟机名称等。

out_pps: 当前包转发率字段，取值为反压对象的当前 pps。

avg_pps: 平均包转发率字段，取值为最近预设时间范围内反压对象的平均 pps，如最近 10 分钟内的平均 pps。

max_pps: 最大包转发率字段，取值为最近预设时间范围内反压对象的最大 pps，如最近 10 分钟内的最大 pps。

其中，构造完成的反压报文即可以基于 Ncip 字段中的宿主机地址进行发送。

图 4 为本申请实施例提供的一种控制方法又一个实施例的流程图，本实施例从反压信息接收端角度对报文限速处理过程进行介绍，接收端具体是指源虚拟交换机。该方法可以包括以下几个步骤:

401: 接收反压信息。

其中，反压信息由目的端针对满足限速条件的源虚拟机发送；满足限速条件的源虚拟机基于内层封装信息确定；内层封装信息由目的端检测到访问流量满足限速条件，抓取访问报文，并对访问报文解析获得，具体实现可以详见图 2 所示实施例，在此不再赘述。

402: 按照反压信息，对请求限速的源虚拟机进行报文限速处理。

其中，请求限速的源虚拟机可以根据反压信息中的内层五元组信息、虚拟网络标识等确定。

在某些实施例中，按照反压信息，对请求限速的源虚拟机进行报文限速处理可以是按照反压信息，对请求限速的源虚拟机中反压信息指示的反压对象进行报文限速处理。

在某些实施例中，按照反压信息，对请求限速的源虚拟机进行报文限速处理可以是按照反压信息指示的至少一种处理方式，对请求限速的源虚拟机进行报文限速处理。

在某些实施例中，按照反压信息指示的至少一种处理方式，对请求限速的源虚拟机进行报文限速处理可以包括:

确定反压信息指示的至少一种处理方式;

在至少一种处理方式包括报警处理方式的情况下，基于请求限速的源虚拟机的虚拟机标识、及该源虚拟机的发包情况信息生成第一反馈结果;

在至少一个处理方式包括限速处理方式的情况下，对请求限速的源虚拟机的报文发送进行限速处理，并基于该源虚拟机的虚拟机标识、及源虚拟机的发包情况信息生成第二反馈结果;

基于第一反馈结果或者第二反馈结果，生成应答信息，并将应答信息反馈给目的端。

其中，对请求限速的源虚拟机的报文发送进行限速处理可以具体是结合反压对象，对请求限速的源虚拟机中的反压对象表示的某个报文流中的报文发送进行限速处理。其中进行限速处理可以包括进行 pps 限速和/或进行 bps 限速等，具体可以是对源虚拟机对应的虚拟网卡进行限速处理，对从该虚拟网卡转发的报文流进行 pps 限速和/或 bps 限速，如将 pps 或 bps 降低一定百分比等。

此外，对报文发送进行限速处理之后，还可以生成限速记录进行保存。

其中，第一反馈结果中的发包情况信息例如可以包括当前包转发率，最近 10 分钟内的平均包转发率、以及最近 10 分钟内的最大包转发率等。

第二反馈结果中的发包情况信息例如可以包括进行限速处理之后的当前包转发率、最近 10 分钟内的平均包转发率、以及最近 10 分钟内的最大包转发率等。

由于前文描述可知，反压信息以反压报文形式发送。因此，在某些实施例中，接收反压信息可以包括：接收反压报文；解析反压报文，获得反压报文中的反压指示信息、虚拟网络标识、及内层五元组信息

则按照反压信息，对请求限速的源虚拟机进行报文限速处理可以包括:

基于虚拟网络标识及内层五元组信息中的源虚拟机地址，确定请求限速的源虚拟机;

按照反压指示信息，对该源虚拟机进行报文限速处理。

可选地，按照反压指示信息，对源虚拟机中进行报文限速处理可以包括：

按照反压指示信息中的反压对象字段值，确定内层五元组信息中的有效信息；

按照反压指示信息中的至少一种处理方式及限速类型，对有效信息标识的反压对象进行报文限速处理。

在某些实施例中，该方法还可以包括：

获取对源虚拟机进行报文限速处理之后的处理结果；

将处理结果填入反压报文中的至少一个反馈字段中，以生成应答报文；

发送应答报文至目的端。

其中，该处理结果即可以包括前文所述的第一反馈结果或者第二反馈结果。

此外，为了保证报文正常发送，在某些实施例中，接收反压信息可以是定时接收反压信息；

该方法还可以包括：

若在定时时间未接收到反压信息，则对已进行限速处理的反压对象执行恢复操作。

可以是基于限速记录，确定已进行限速处理的反压对象并执行恢复操作。例如假设对该反压对象进行 pps 限速，该恢复操作可以是指将该反压对象对应的 pps 升高一定百分比等。

在某些实施例中，对已进行限速处理的反压对象执行恢复操作之后，该方法还可以包括：

若已进行限速处理的反压对象恢复至进行限速处理之前的原始状态，则删除该进行限速处理的反压对象对应的限速记录。

如图 5 中所示，为本申请实施例提供的一种控制方法又一个实施例的流

程图，本实施例由源虚拟交换机执行，可以包括如下几个步骤:

501: 在定时时间，判断是否接收到反压报文，如果是，执行步骤 502，若否，执行步骤 507。

502: 解析反压报文。

解析反压报文，可以获得反压报文中的相关信息，如请求限速的源虚拟机、源虚拟机中的反压对象、处理方式、限速类型等等。

其中，本实施例中以限速类型为 pps 为例进行说明。

503: 确定是否执行限速处理方式，若是执行步骤 504，若否执行步骤 505

504: 将虚拟网卡中该反压对象对应的 pps 调整为原有的 x%，并生成限速记录保存，之后执行步骤 505。

其中，x 小于 100。

505: 确定请求限速的源虚拟机的虚拟机标识和发包情况信息，填入反压报文中的反馈字段中，生成应答报文。

506: 将应答报文发送至目的端。

507: 基于限速记录，判断是否存在已进行限速的反压对象，若是，执行步骤 508。

508: 调整虚拟网卡中，该已进行限速的反压对象对应 pps 为当前的 y%，其中，y 大于 100。

509: 基于限速记录，判断该已进行限速的反压对象对应 pps 是否恢复为原始状态，若是，执行步骤 510。

510: 删除该已进行限速的反压对象对应的限速记录。

下面结合图 1a 和图 1b 分别示出的两种流量攻击场景对本申请技术方案进行介绍，图 6a 为对应图 1a 的流量攻击场景的控制交互示意图，目的虚拟交换机 104 检测访问流量满足限速条件时，抓取访问报文，并通过解析访问报文获得内层封装信息，基于内层封装信息可以确定满足限速条件的源虚拟

机 101，并向该源虚拟机 101 所在源宿主机 10 发送反压报文，由源宿主机 10 中的源虚拟交换机 102 接收该反压报文，并基于反压报文对该源虚拟机 101 进行报文限速处理，并基于处理结果生成应答报文，将应答报文发送至目的虚拟交换机 104，目的虚拟交换机 104 可以基于该应答报文，输出报警提示信息。

图 6b 为对应图 1b 的流量攻击场景的控制交互示意图，虚拟网关 107 检测访问流量满足限速条件时，抓取访问报文，并通过解析访问报文获得内层封装信息，基于内层封装信息可以确定满足限速条件的源虚拟机 105，并向该源虚拟机 105 所在源宿主机 30 发送反压报文，由源宿主机 30 中的源虚拟交换机 106 接收该反压报文，并基于反压报文对该源虚拟机 105 进行报文限速处理，并基于处理结果生成应答报文，将应答报文发送至虚拟网关 107，虚拟网关 107 可以基于该应答报文，输出报警提示信息。

此外，在一个实际应用中，本申请实施例的技术方案可以用于解决 Vxlan 网络中的流量攻击问题。因此，本申请实施例还提供了一种应用于 Vxlan 网络中的控制方法，可以包括:

检测访问流量满足限速条件，抓取 Vxlan 报文;

解析 Vxlan 报文，获得 Vxlan 报文中的内层封装信息;

基于内层封装信息，确定满足限速条件的源虚拟机;

向源虚拟机所在源宿主机发送反压信息；其中，反压信息用于指示对源虚拟机进行报文限速处理。

本实施例与图 2 所示实施例不同之处在于，访问报文具体为 Vxlan 报文，其它相同或相似步骤可以详见前文实施例中所述，在此不再赘述。

本申请实施例还提供了一种应用于 Vxlan 网络中的控制方法，可以包括:

接收反压信息；其中，反压信息由目的端针对满足限速条件的源虚拟机发送；满足限速条件的源虚拟机基于内层封装信息确定；内层封装信息由目

的端检测到访问流量满足限速条件，抓取 Vxlan 报文，并对 VXlan 报文解析获得;

按照反压信息，对源虚拟机进行报文限速处理。

图 7 为本申请实施例提供的一种控制装置一个实施例的结构示意图，该装置可以包括:

报文抓取模块 701，用于检测访问流量满足限速条件，抓取访问报文;

报文解析模块 702，用于解析访问报文，获得访问报文中的内层封装信息;

确定模块 703，用于基于内层封装信息，确定满足限速条件的源虚拟机;

反压触发模块 704，用于向源虚拟机所在源宿主机发送反压信息; 其中，反压信息用于指示对源虚拟机进行报文限速处理。

图 7 所述的控制装置可以执行图 2 所示实施例所述的控制方法，其实现原理和技术效果不再赘述。对于上述实施例中的控制装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

图 8 为本申请实施例提供的一种控制装置又一个实施例的结构示意图，该装置可以包括:

信息接收模块 801，用于接收反压信息; 其中，反压信息由目的端针对满足限速条件的源虚拟机发送; 满足限速条件的源虚拟机基于内层封装信息确定; 内层封装信息由目的端检测到访问流量满足限速条件，抓取访问报文，并对访问报文解析获得;

处理模块 802，用于按照反压信息，对源虚拟机进行报文限速处理。

图 8 所述的控制装置可以执行图 4 所示实施例所述的控制方法，其实现原理和技术效果不再赘述。对于上述实施例中的控制装置其中各个模块、单元执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处

将不做详细阐述说明。

此外，本申请实施例还提供了一种计算设备，如图 9 中所示，该计算设备可以包括处理组件 901 以及存储组件 902，存储组件 902 存储一条或多条计算机指令，该一条或多条计算机指令用以被处理组件 901 调用执行，以使得该处理组件 901 可以运行至少一个虚拟机 903，以及实现图 1 所示的控制方法的虚拟交换机 904。

其中，该处理组件包括一个或多个处理器，处理器可以具体是指 CPU。

此外，计算设备必然还可以包括其他部件，例如输入/输出接口、通信组件等。输入/输出接口为处理组件和外围接口模块之间提供接口，上述外围接口模块可以是输出设备、输入设备等。通信组件被配置为便于计算设备和其他设备之间有线或无线方式的通信等。

实际应用中，该计算设备可以为云计算平台提供的弹性计算主机等，此时计算设备即可以是指云服务器。

本申请实施例还提供了一种计算机可读存储介质，存储有计算机程序，所述计算机程序被计算机执行时可以实现上述图 2 所示实施例的控制方法。

此外，本申请实施例还提供了一种计算设备，如图 10 中所示，该计算设备可以包括处理组件 1001 以及存储组件 1002，处理组件 1001 可以包括一个或多个处理器，存储组件 1002 存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件 1001 调用执行，以运行实现图 1 所示的控制方法的虚拟网关 1003。

其中，处理器可以具体是指 CPU。

此外，计算设备必然还可以包括其他部件，例如输入/输出接口、通信组件等。输入/输出接口为处理组件和外围接口模块之间提供接口，上述外围接口模块可以是输出设备、输入设备等。通信组件被配置为便于计算设备和其他设备之间有线或无线方式的通信等。

实际应用中，该计算设备可以为云计算平台提供的弹性计算主机等，此时计算设备即可以是指云服务器。

本申请实施例还提供了一种计算机可读存储介质，存储有计算机程序，所述计算机程序被计算机执行时可以实现上述图 2 所示实施例的控制方法。

此外，本申请实施例还提供了一种计算设备，如图 11 中所示，该计算设备可以包括处理组件 1101 以及存储组件 1102，处理组件 1101 包括一个或多个处理器，存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行至少一个虚拟机 1103、以及实现如图 4 所示实施例中所述控制方法的虚拟交换机 1104。

其中，处理器可以具体是指 CPU。

此外，计算设备必然还可以包括其他部件，例如输入/输出接口、通信组件等。输入/输出接口为处理组件和外围接口模块之间提供接口，上述外围接口模块可以是输出设备、输入设备等。通信组件被配置为便于计算设备和其他设备之间有线或无线方式的通信等。

实际应用中，该计算设备可以为云计算平台提供的弹性计算主机等，此时计算设备即可以是指云服务器。

本申请实施例还提供了一种计算机可读存储介质，存储有计算机程序，所述计算机程序被计算机执行时可以实现上述图 4 所示实施例的控制方法。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例

方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，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申请各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种控制方法，其特征在于，包括:

检测访问流量满足限速条件，抓取访问报文;

解析所述访问报文，获得所述访问报文中的内层封装信息;

基于所述内层封装信息，确定满足限速条件的源虚拟机;

向所述源虚拟机所在源宿主机发送反压信息；其中，所述反压信息用于指示对所述源虚拟机进行报文限速处理。

2、根据权利要求 1 所述的方法，其特征在于，所述基于所述内层封装信息，确定满足限速条件的源虚拟机包括:

基于所述内层封装信息标识的报文流，对所述访问报文进行汇总以确定不同报文流的报文数量;

按照不同报文流的报文数量，选择待限速报文流;

确定所述待限速报文流对应的源虚拟机。

3、根据权利要求 2 所述的方法，其特征在于，所述按照不同报文流的报文数量，选择待限速报文流包括:

按照不同报文流的报文数量，选择报文数量大于或等于预设数量的待限速报文流。

4、根据权利要求 2 所述的方法，其特征在于，所述按照不同报文流的报文数量，确定待限速报文流包括:

按照报文数量从大到小的顺序，选择前 N 个报文流作为待限速报文流。

5、根据权利要求 2 所述的方法，其特征在于，还包括:

确定所述源虚拟机中的反压对象；其中，所述反压对象包括所述源虚拟机发出的全部报文流、所述源虚拟机发向其发出的待限速报文流对应的目的虚拟机的全部报文流、或者所述源虚拟机发出的待限速报文流;

至少根据所述反压对象，生成所述反压信息；其中，所述反压信息用于指示对所述反压对象进行报文限速处理。

6、根据权利要求 2 所述的方法，其特征在于，还包括:

确定所述源虚拟机对应的限速处理方式及报警处理方式中的至少一种处理方式;

至少根据所述至少一种处理方式，生成所述反压信息；其中，所述反压信息用于指示按照所述至少一种处理方式对所述源虚拟机进行报文限速处理。

7、根据权利要求 6 所述的方法，其特征在于，还包括:

在所述至少一种处理方式包括限速处理方式的情况下，确定所述源虚拟机对应的限速类型;

所述至少根据所述至少一种处理方式，生成反压信息包括:

至少根据所述至少一种处理方式及所述限速类型，生成反压信息。

8、根据权利要求 1 所述的方法，其特征在于，还包括:

接收按照所述反压信息对所述源虚拟机进行报文限速处理之后反馈的应答信息;

基于所述应答信息，输出报警提示信息。

9、根据权利要求 1 所述的方法，其特征在于，还包括:

解析所述访问报文获得外层封装信息;

所述向所述源虚拟机所在宿主机发送反压信息包括:

基于反压指示信息，及所述源虚拟机对应的内层封装信息和外层封装信息，构造反压报文;

将所述反压报文作为反压信息，发送至所述源虚拟机所在宿主机。

10、根据权利要求 9 所述的方法，其特征在于，所述反压报文至少包括反压指示信息对应的至少一个反压字段、宿主机地址字段、网络标识字段、及内层五元组分别对应的字段;

所述基于反压指示信息，及所述源虚拟机对应的内层封装信息和外层封装信息，构造反压报文包括:

将反压指示信息填入所述至少一个反压字段;

将所述源虚拟机对应外层封装信息中的源宿主机地址，填入所述宿主机地址字段；

将所述源虚拟机对应外封装信息中的虚拟网络标识，填入所述网络标识字段；

将所述源虚拟机对应的内层封装信息中的内层五元组信息，填入所述内层五元组分别对应的字段。

11、根据权利要求 10 所述的方法，其特征在于，所述反压报文还包括至少一个反馈字段；所述至少一个反馈字段用于进行报文限速处理之后填入处理结果，以生成应答报文；

所述方法还包括：

接收所述应答报文；

基于所述应答报文，输出限速提示信息。

12、根据权利要求 11 所述的方法，其特征在于，所述至少一个反馈字段包括用于填入所述源虚拟机的虚拟机标识的虚拟机标识字段、用于填入所述反压对象当前包转发率的当前包转发率字段、用以填入所述反压对象最近预设时间范围内的平均包转发率的平均包转发率字段、以及用以填入所述反压对象最近预设时间范围内的最大包转发率的最大包转发率字段。

13、根据权利要求 11 所述的方法，其特征在于，所述反压报文还包括攻击方向字段；

所述方法还包括：

在所述源虚拟机对应报警处理方式的情况下，确定流量攻击方向；

将标识流量攻击方向的参数数值，填入所述攻击方向字段。

14、根据权利要求 10 所述的方法，其特征在于，所述反压报文还包括网络协议字段；所述方法还包括：

将标识内层网络协议的参数数值，填入所述网络协议字段；所述网络协议字段用于按照字段值标识的网络协议解析获得所述内层五元组信息。

15、根据权利要求 10 所述的方法，其特征在于，所述至少一个反压字段包括处理方式字段、限速类型字段及反压对象字段;

所述将反压指示信息填入所述至少一个反压字段包括:

确定所述源虚拟机对应的限速处理方式及报警处理方式中的至少一种处理方式，将标识所述至少一个处理方式的参数数值写入所述处理方式字段;

在所述至少一种处理方式包括限速处理方式的情况下，确定所述源虚拟机对应的限速类型，将标识所述限速类型的参数数值写入所述限速类型字段;

确定所述源虚拟机中的反压对象，并基于所述反压对象确定所述内层五元组信息中的有效信息，及将标识所述有效信息的参数数值写入所述反压对象字段。

16、根据权利要求 1 所述的方法，其特征在于，所述检测访问流量满足限速条件，抓取访问报文包括:

检测访问流量满足限速条件，按照采样频率及采样数量抓取访问报文。

17、一种控制方法，其特征在于，包括:

接收反压信息；其中，反压信息由目的端针对满足限速条件的源虚拟机发送；满足限速条件的源虚拟机基于内层封装信息确定；所述内层封装信息由所述目的端检测到访问流量满足限速条件，抓取访问报文，并对所述访问报文解析获得;

按照所述反压信息，对所述源虚拟机进行报文限速处理。

18、根据权利要求 17 所述的方法，其特征在于，所述按照反压信息，对所述源虚拟机进行报文限速处理包括:

按照所述反压信息，对所述源虚拟机中所述反压信息指示的反压对象进行报文限速处理。

19、根据权利要求 17 所述的方法，其特征在于，所述按照反压信息，对所述源虚拟机进行报文限速处理包括:

按照所述反压信息指示的至少一种处理方式，对所述源虚拟机进行报文

限速处理。

20、根据权利要求 19 所述的方法，其特征在于，按照所述反压信息指示的至少一种处理方式，对所述源虚拟机进行报文限速处理包括:

确定所述反压信息指示的至少一种处理方式;

在所述至少一种处理方式包括报警处理方式的情况下，基于所述源虚拟机的虚拟机标识、及所述源虚拟机的发包情况信息生成第一反馈结果;

在所述至少一种处理方式包括限速处理方式的情况下，对所述源虚拟机的报文发送进行限速处理，并基于所述源虚拟机的虚拟机标识、及所述源虚拟机的发包情况信息生成第二反馈结果;

基于所述第一反馈结果或者所述第二反馈结果，生成应答信息，并将所述应答信息反馈给所述目的端。

21、根据权利要求 17 所述的方法，其特征在于，所述接收反压信息包括:

定时接收反压信息;

所述方法还包括:

若在定时时间未接收到所述反压信息，对已进行限速处理的反压对象执行恢复操作。

22、根据权利要求 17 所述的方法，其特征在于，所述接收反压信息包括:

接收反压报文;

解析所述反压报文，获得所述反压报文中的反压指示信息、虚拟网络标识、及内层五元组信息;

所述按照所述反压信息，对所述源虚拟机进行报文限速处理包括:

基于所述虚拟网络标识及所述内层五元组信息中源虚拟机地址，确定所述源虚拟机;

按照所述反压指示信息，对所述源虚拟机进行报文限速处理。

23、根据权利要求 22 所述的方法，其特征在于，还包括:

获取对所述源虚拟机进行报文限速处理之后的处理结果;

将所述处理结果填入所述反压报文中的至少一个反馈字段中，以生成应答报文;

发送所述应答报文至所述目的端。

24、根据权利要求 23 所述的方法，其特征在于，所述按照所述反压指示信息，对所述源虚拟机中进行报文限速处理包括:

按照所述反压指示信息中的反压对象字段值，确定所述内层五元组信息中的有效信息;

按照所述反压指示信息中的至少一种处理方式及限速类型，对所述有效信息标识的反压对象进行报文限速处理。

25、一种控制装置，其特征在于，包括:

报文抓取模块，用于检测访问流量满足限速条件，抓取访问报文;

报文解析模块，用于解析所述访问报文，获得所述访问报文中的内层封装信息;

确定模块，用于基于所述内层封装信息，确定满足限速条件的源虚拟机;

反压触发模块，用于向所述源虚拟机所在源宿主机发送反压信息;其中，所述反压信息用于指示对所述源虚拟机进行报文限速处理。

26、一种控制装置，其特征在于，包括:

信息接收模块，用于接收反压信息; 其中，反压信息由目的端针对满足限速条件的源虚拟机发送;满足限速条件的源虚拟机基于内层封装信息确定;所述内层封装信息由所述目的端检测到访问流量满足限速条件，抓取访问报文，并对所述访问报文解析获得;

处理模块，用于按照所述反压信息，对所述源虚拟机进行报文限速处理。

27、一种计算设备，其特征在于，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行至少一个虚拟机、以及运行实现如权利要求 1~16 任一项所述控制方法的虚拟交换机。

28、一种计算设备，其特征在于，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行实现如权利要求 1~16 任一项所述控制方法的虚拟网关。

29、一种计算设备，其特征在于，包括处理组件及存储组件，所述存储组件存储一条或多条计算机指令，所述一条或多条计算机指令用以被所述处理组件调用执行，以运行至少一个虚拟机、以及实现如权利要求 17~24 任一项所述控制方法的虚拟交换机。

30、一种计算机存储介质，其特征在于，存储有计算机程序，所述计算机程序被计算机执行时实现如权利要求 1-16 任一项所述控制方法。

31、一种计算机存储介质，其特征在于，存储有计算机程序，所述计算机程序被计算机执行时实现如权利要求 17-24 任一项所述的控制方法。

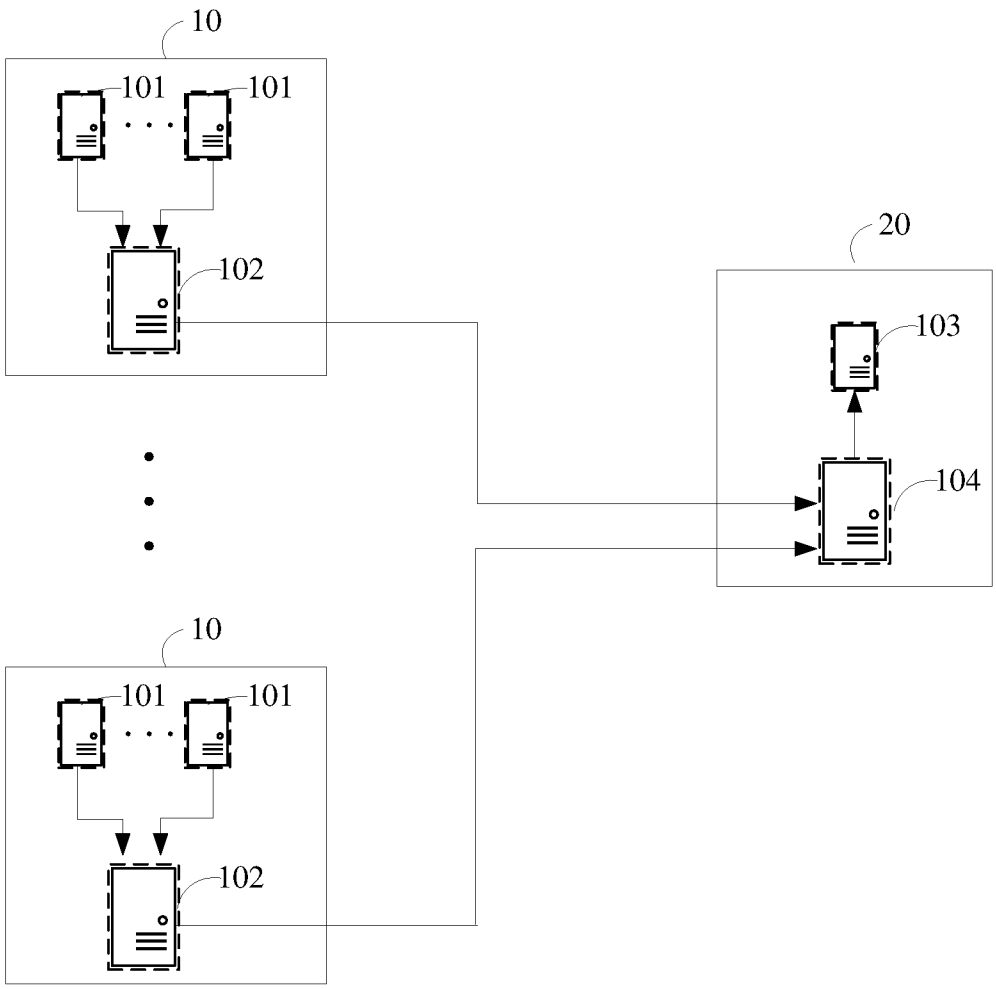


图 1a

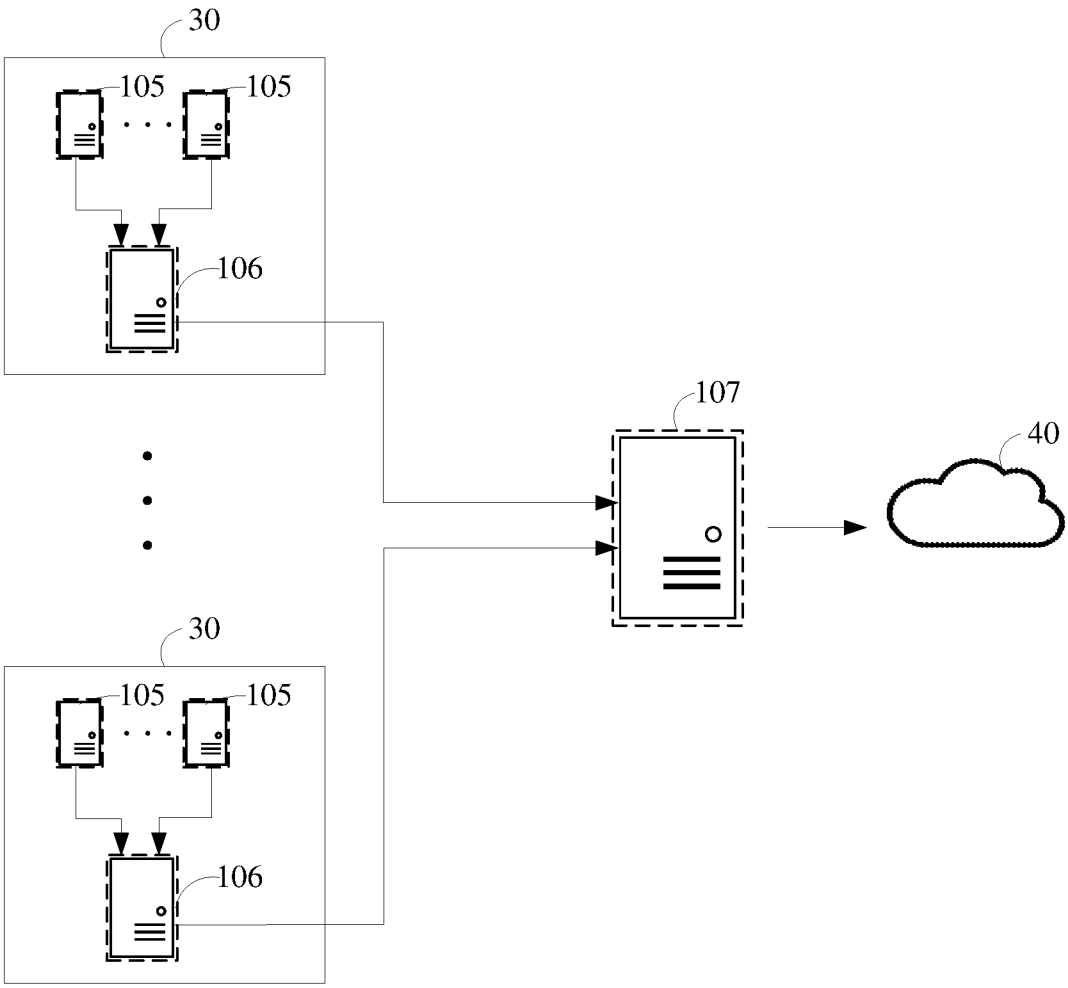


图 1b

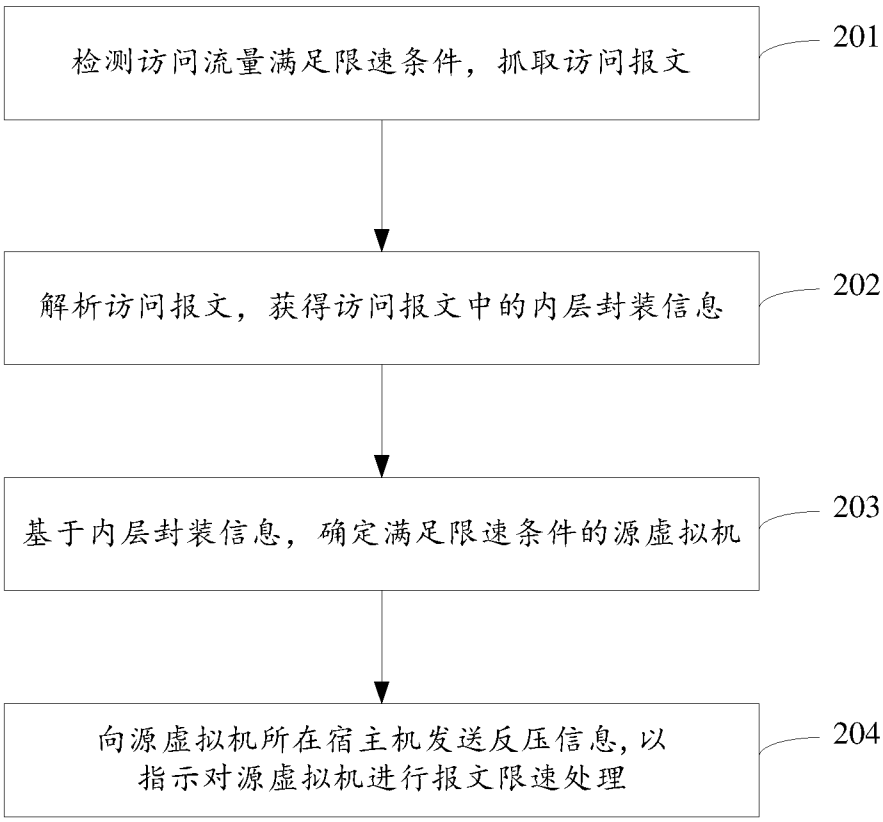


图 2

Action	Limit_type	Direction	key_type	Ncip	tunnel id	Af	inner_proto	inner_src ip	inner_dst ip	inner src port	inner dst port	ecs_id	out_pps	avg_pps	max_pps

图 3

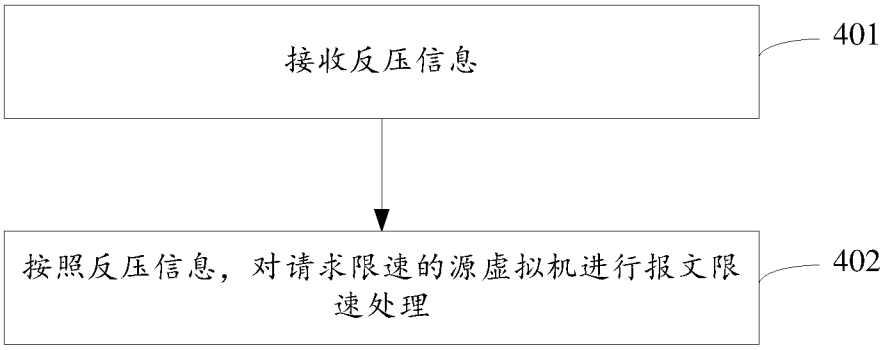


图 4

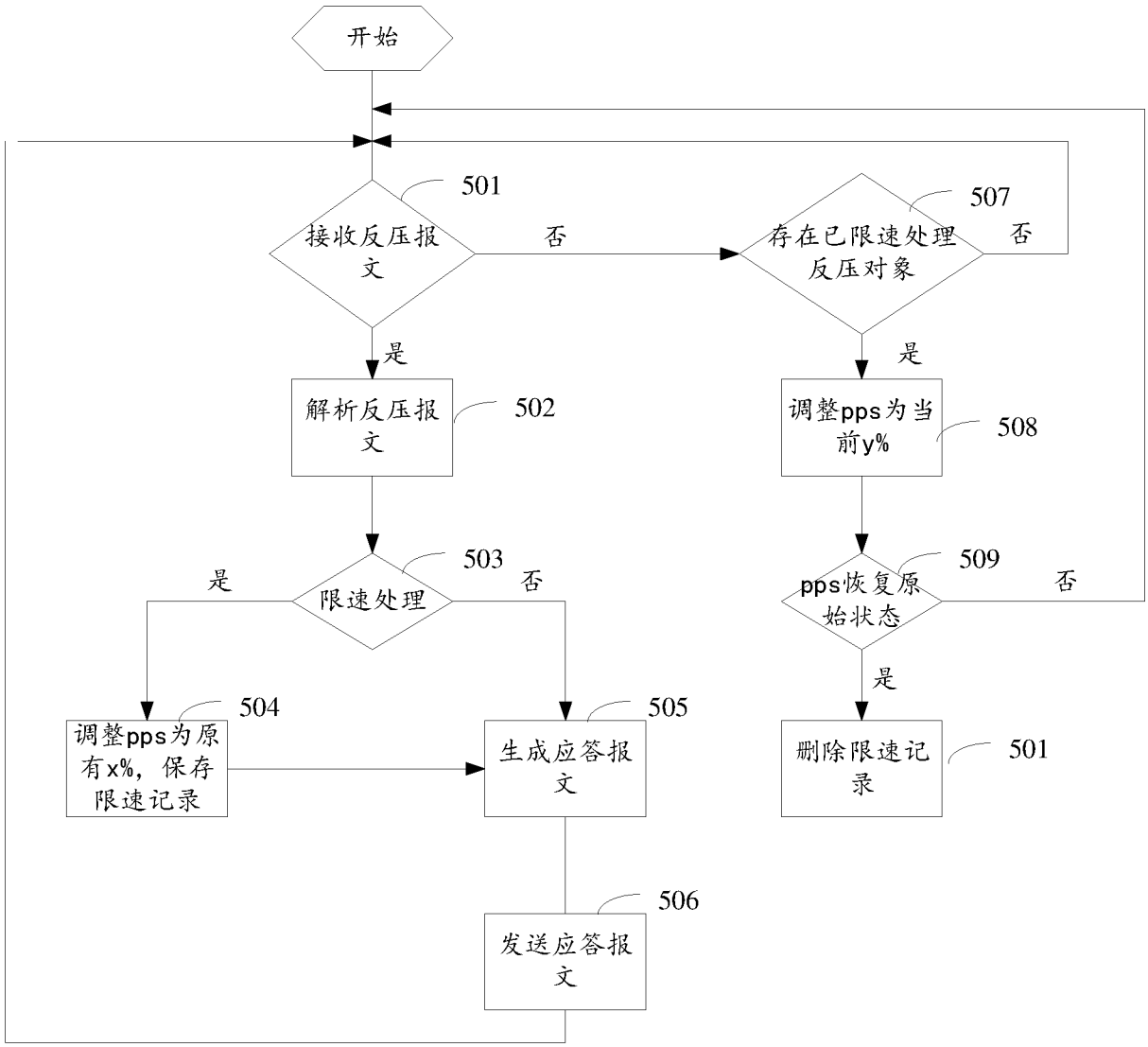

开始
501
接收反压报文
否
是
507
存在已限速处理反压对象
否
是
解析反压报文
502
调整pps为当前y%
508
503
限速处理
是
否
509
pps恢复原始状态
否
是
504
调整pps为原有x%，保存限速记录
505
生成应答报文
删除限速记录
501
506
发送应答报文

图 5

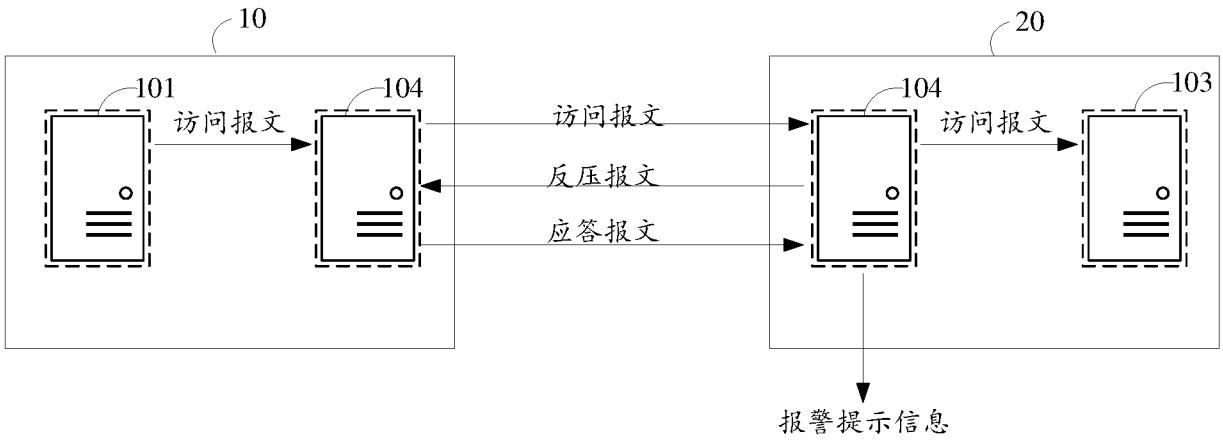

10
20
101
访问报文
104
访问报文
反压报文
应答报文
104
访问报文
103
报警提示信息

图 6a

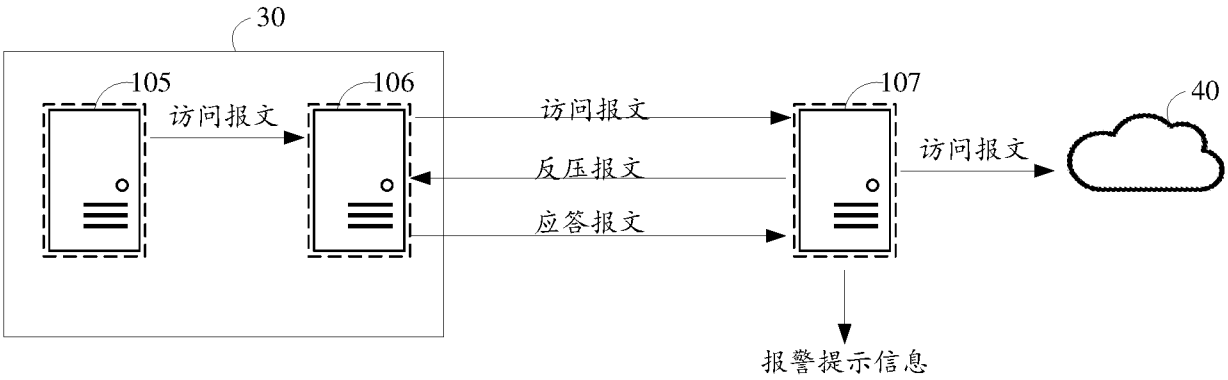

30
105
106
107
40
访问报文
访问报文
反压报文
应答报文
访问报文
报警提示信息

图 6b

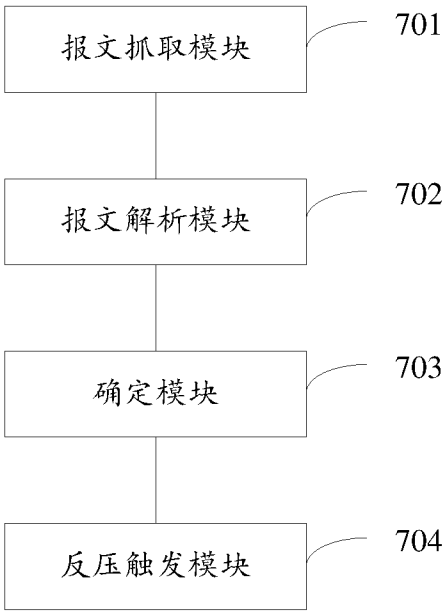

报文抓取模块
701
报文解析模块
702
确定模块
703
反压触发模块
704

图 7

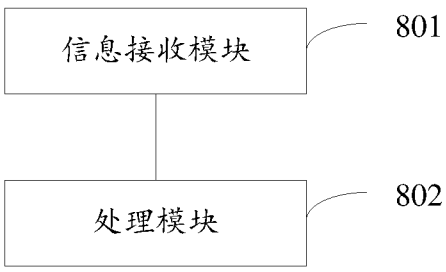

信息接收模块
801
处理模块
802

图 8

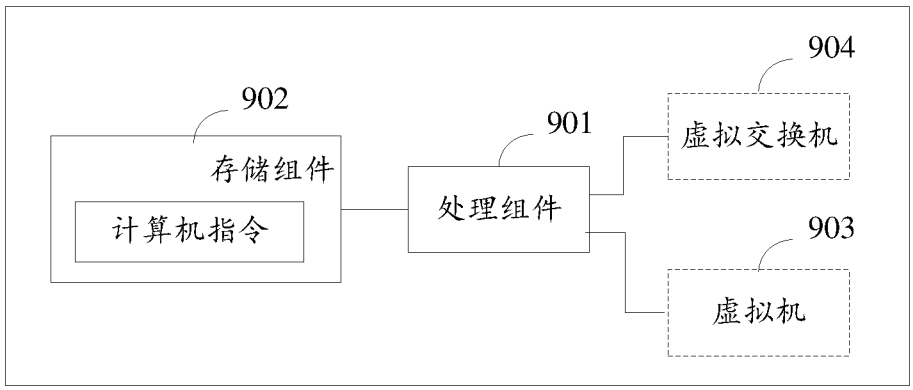

902
存储组件
计算机指令
901
处理组件
904
虚拟交换机
903
虚拟机

图 9

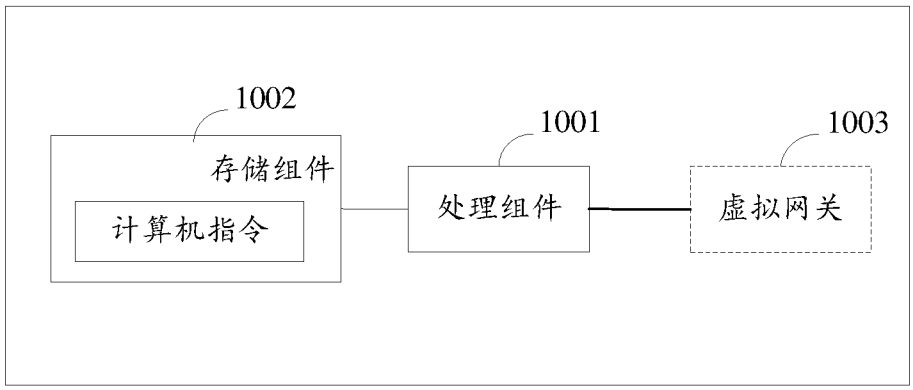

1002
存储组件
计算机指令
1001
处理组件
1003
虚拟网关

图 10

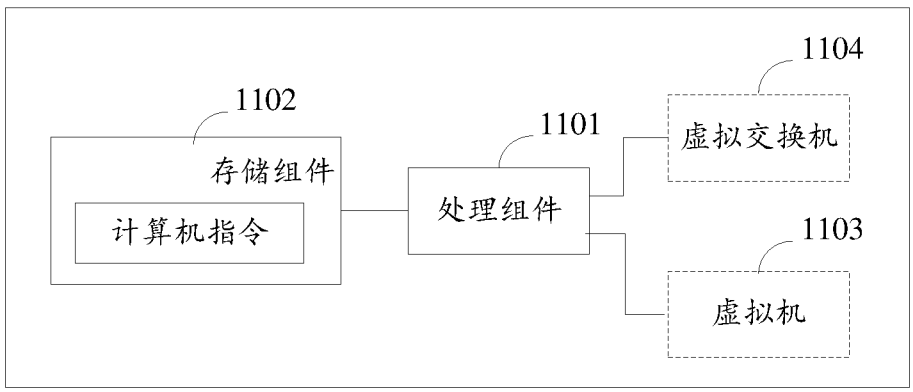

1102
存储组件
计算机指令
1101
处理组件
1104
虚拟交换机
1103
虚拟机

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/077740

A. CLASSIFICATION OF SUBJECT MATTER

H04L 47/20(2022.01)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 H04W

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)

CNTXT, CNKI, VEN, ENTXT: 限速, 流限, 限流, 流量, 控制, 限制, 限定, 减少, 减小, 叠加网络, 覆盖网络, 报文, 源, 虚拟机, 主机, 内层, IP, 封装, 解封装, 确定, 判断, speed 3d limit+, flow 3d limit+, flow, limit+, control+, reduc+, overlay, message, packet, resource, virtual w machine, VM, virtual, host, inner w layer, capsulation, decapsulation, confirm+, judg+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015264077 A1 (IBM) 17 September 2015 (2015-09-17) description, paragraphs 47-142	1-31
Y	US 10764249 B1 (JUNIPER NETWORKS INC.) 01 September 2020 (2020-09-01) claims 1-20	1-31
A	US 2016261624 A1 (IBM) 08 September 2016 (2016-09-08) entire document	1-31
A	CN 106817243 A (QUANTA COMPUTER CO., LTD.) 09 June 2017 (2017-06-09) entire document	1-31

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 2022	**29 April 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/077740

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2015264077 A1	17 September 2015	US 2016261624 A1	08 September 2016
US 10764249 B1	01 September 2020	None	
US 2016261624 A1	08 September 2016	US 2015264077 A1	17 September 2015
CN 106817243 A	09 June 2017	US 2017155560 A1	01 June 2017
		TW 201722109 A	16 June 2017

国际检索报告

国际申请号
PCT/CN2022/077740

A. 主题的分类

H04L 47/20(2022.01)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 H04W

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））

CNTXT, CNKI, VEN, ENTXT:限速，流限，限流，流量，控制，限制，限定，减少，减小，叠加网络，覆盖网络，报文，源，虚拟机，主机，内层，IP，封装，解封装，确定，判断，speed 3d limit+, flow 3d limit+, flow, limit+, control+, reduc+, overlay, message, packet, resource, virtual w machine, VM, virtual, host, inner w layer, capsulation, decapsulation, confirm+, judg+

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
Y	US 2015264077 A1 (IBM) 2015年9月17日 (2015-09-17) 说明书第47-142段	1-31
Y	US 10764249 B1 (JUNIPER NETWORKS INC) 2020年9月1日 (2020-09-01) 权利要求1-20	1-31
A	US 2016261624 A1 (IBM) 2016年9月8日 (2016-09-08) 全文	1-31
A	CN 106817243 A (广达电脑股份有限公司) 2017年6月9日 (2017-06-09) 全文	1-31

☐ 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	国际检索报告邮寄日期
2022年4月24日	2022年4月29日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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	受权官员 亓晓旭 电话号码 86-(010)-62089384

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/077740

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)
US 2015264077 A1	2015年9月17日	US 2016261624 A1	2016年9月8日
US 10764249 B1	2020年9月1日	无	
US 2016261624 A1	2016年9月8日	US 2015264077 A1	2015年9月17日
CN 106817243 A	2017年6月9日	US 2017155560 A1	2017年6月1日
		TW 201722109 A	2017年6月16日