(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 6 月 30 日 (30.06.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/101783 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2015/096509

(22) 国际申请日: 2015 年 12 月 6 日 (06.12.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410810857.X 2014 年 12 月 22 日 (22.12.2014) 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: **余庆华 (YU, Qinghua)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **杨欣华 (YANG, Xinhua)**; 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))

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: ATTACK PACKET PROCESSING METHOD, APPARATUS, AND SYSTEM

(54) **发明名称** : 一种攻击数据包的处理方法、装置及系统

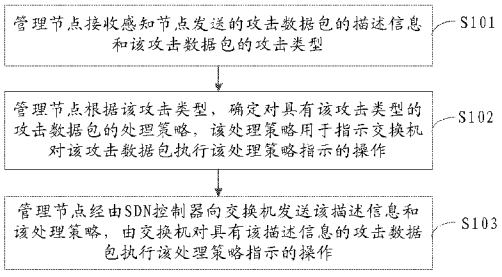

图 2 / Fig.2

S101 A management node receives description information and an attack type of the attack packet sent by a sensing node

S102 According to the attack type, the management node determines a processing policy with respect to the attack packet having the attack type, the processing policy being used to instruct an exchanger to conduct an operation instructed by the processing policy with respect to the attack packet

S103 The management node sends to the exchanger via a software defined network (SDN) controller the description information and the processing policy, and the exchanger conducts the operation instructed by the processing policy on the attack packet having the description information

(57) **Abstract**: An embodiment of the present invention relates to the technical field of communication, and provided are an attack packet processing method, apparatus, and system. The present invention limits a network bandwidth occupied by the attack packet when the same is transmitted in the network, and ensures the transmission of a normal packet. The method comprises: a management node receives description information and an attack type of the attack packet sent by a sensing node; according to the attack type, determining a processing policy with respect to the attack packet having the attack type, the processing policy being used to instruct an exchanger to conduct an operation instructed by the processing policy with respect to the attack packet having the description information; sending to the exchanger via a software defined network (SDN) controller the description information and the processing policy, the exchanger conducts the operation instructed by the processing policy on the attack packet having the description information. The method is applied as a network security maintenance technique.

(57) **摘要**:

[见续页]

WO 2016/101783 A1

本发明实施例提供一种攻击数据包的处理方法、装置及系统，涉及通信技术领域，能够限制攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，该方法包括：管理节点接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型，根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。该方法应用于网络安全维护技术中。

一种攻击数据包的处理方法、装置及系统

技术领域

本发明涉及通信技术领域，尤其涉及一种攻击数据包的处理方法、装置及系统。

背景技术

随着云技术的飞速发展，云技术应用中出现的问题也越来越多。例如，云数据中心的服务器（以下简称云服务器）进行网络协议（英文：Internet Protocol，缩写：IP）通信时会受到各种攻击数据包的攻击，例如受到分布式拒绝服务(英文:distributed denial of service，缩写：DDoS)的攻击，假消息攻击等。因此，处理攻击数据包，保证云服务器进行安全通信成为云技术的核心技术之一。

目前，处理攻击数据包的一种常见方式为通过在云数据中心的入口云服务器上部署物理防火墙，或者在云数据中心的每台云服务器上运行的虚拟机监控器（英文：hypervisor）上部署虚拟防火墙，以保证所有待进入云服务器的数据包均经过物理/虚拟防火墙的过滤与转发，从而过滤掉攻击数据包，防止攻击数据包进入云数据中心的云服务器，进而保证云服务器能够安全通信。具体的，根据工作人员为物理/虚拟防火墙配置的安全策略，物理/虚拟防火墙通过识别待进入 IP 层的数据包中承载的 IP 层的信令，当该 IP 层的信令不符合该安全策略时，物理/虚拟防火墙过滤掉该数据包，从而防止攻击数据包攻击云服务器，进而保证云服务器能够安全通信。

然而，在上述通过防火墙阻止攻击数据包进入云服务器的方法中，由于只能由防火墙阻止攻击数据包进入云服务器，但是负责将数据包转发给防火墙的交换机仍然会将这些攻击数据包转发给防火墙，即攻击数据包仍然会在网络中传输，因此，这些异常的数据包会占用大量的网络带宽，从而影响了正常的数据包的传输。

发明内容

本发明的提供一种攻击数据包的处理方法、装置及系统，能够限制攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输。

为达到上述目的，本发明采用如下技术方案:

第一方面，本发明提供一种攻击数据包的处理方法，包括：

管理节点接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型；

所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作；

所述管理节点经由软件定义网络 SDN 控制器向所述交换机发送所述描述信息和所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第一方面的第一种可能的实现方式中，所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括：

所述管理节点根据所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

结合前述的第一方面，在第一方面的第二种可能的实现方式中，所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括：

所述管理节点根据所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

结合前述的第一方面或第一方面的第一种可能的实现方式至第一方面的第二种可能的实现方式中的任一种实现方式，在第三种可能的实现方式中，

所述处理策略指示的操作包括：

对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

结合前述的第一方面或第一方面的第一种可能的实现方式至第一方面的第三种可能的实现方式中的任一种实现方式，在第四种可能的实现方式中，当所述管理节点接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，

所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括：

所述管理节点根据所述多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型；

所述管理节点根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

结合前述的第一方面或第一方面的第一种可能的实现方式至第一方面的第四种可能的实现方式中的任一种实现方式，在第五种可能的实现方式中，所述管理节点经由 SDN 控制器向所述交换机发送所述描述信息和所述处理策略，包括：

所述管理节点通过预设的通讯接口向所述 SDN 控制器发送所述描述信息和所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

结合前述的第一方面或第一方面的第一种可能的实现方式至第一方面的第五种可能的实现方式中的任一种实现方式，在第六种可能的实现方式中，

所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

第二方面，本发明提供一种攻击数据包的处理方法，包括：

软件定义网络 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略；

所述 SDN 控制器向第一交换机发送所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第二方面的第一种可能的实现方式中，所述 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略，包括：

所述 SDN 控制器通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

结合前述的第二方面或第二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 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略之

后，所述方法还包括：

所述 SDN 控制器向与所述 SDN 控制器连接的主 SDN 控制器发送所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

第三方面，本发明提供一种攻击数据包的处理方法，包括：

感知节点识别所述感知节点接收的数据包为攻击数据包；

所述感知节点确定所述攻击数据包的描述信息和所述攻击数据包的攻击类型；

所述感知节点向管理节点发送所述描述信息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第三方面的第一种可能的实现方式中，

所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

第四方面，本发明提供一种管理节点，包括：

接收单元，用于接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型；

确定单元，用于根据所述接收单元接收的所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作；

发送单元，用于经由软件定义网络 SDN 控制器向所述交换机发送所述接收单元接收的所述描述信息和所述确定单元确定的所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第四方面的第一种可能的实现方式中，

所述确定单元，具体用于根据所述接收单元接收的所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

结合前述的第四方面，在第二种可能的实现方式中，

所述确定单元，具体用于根据所述接收单元接收的所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

结合前述的第四方面或第四方面的第一种可能的实现方式至第四方面的第二种可能的实现方式中的任一种实现方式，在第三种可能的实现方式中，

所述确定单元确定的所述处理策略指示的操作包括:

对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

结合前述的第四方面或第四方面的第一种可能的实现方式至第四方面的第三种可能的实现方式中的任一种实现方式，在第四种可能的实现方式中，

所述确定单元，具体用于当所述接收单元接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，根据所述多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型，以及根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

结合前述的第四方面或第四方面的第一种可能的实现方式至第四方面的第四种可能的实现方式中的任一种实现方式，在第五种可能的实现方式中，

所述发送单元，具体用于通过预设的通讯接口向所述 SDN 控制器发送所述接收单元接收的所述描述信息和所述确定单元确定的所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

结合前述的第四方面或第四方面的第一种可能的实现方式至第四方面的第五种可能的实现方式中的任一种实现方式，在第六种可能的实现方式中，

所述接收单元接收的所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的

IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

第五方面，本发明提供一种软件定义网络 SDN 控制器，包括：

接收单元，用于接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略；

发送单元，用于向第一交换机发送所述接收单元接收的所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第五方面的第一种可能的实现方式中，

所述接收单元，具体用于通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

结合前述的第五方面或第五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，

所述发送单元，还用于向主 SDN 控制器发送所述接收单元接收的所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

第六方面，本发明提供一种感知节点，包括：

识别单元，用于识别接收的数据包为攻击数据包；

确定单元，用于确定所述识别单元识别的所述攻击数据包的描述信息和所述攻击数据包的攻击类型；

发送单元，用于向管理节点发送所述确定单元确定的所述描述信息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

在第六方面的第一种可能的实现方式中，

所述确定单元确定的所述描述信息包括：

所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

第七方面，本发明提供一种通信系统，包括：

如上述第四方面或第四方面的任一种可能的实现方式所述的管理节点，如上述第五方面或第五方面的任一种可能的实现方式所述的软件定义网络 SDN 控制器，如上述第六方面或第六方面的第一种可能的实现方式所述的感知节点，以及交换机。

本发明提供一种攻击数据包的处理方法、装置及系统，具体为管理节点接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型，并根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，以及经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，其中，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。通过本发明提供一种攻击数据包的处理方法、装置及系统，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，管理节点能够根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

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作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例的附图，而不是全部的实施例的附图。

图 1 为本发明实施例提供的一种通信系统框图一；

图 2 为本发明实施例提供的一种攻击数据包的处理方法的流程图一；

图 3 为本发明实施例提供的一种攻击数据包的处理方法的流程图二；

图 4 为本发明实施例提供的第一交换机的流表示意图；

图 5 为本发明实施例提供的一种攻击数据包的处理方法的流程图

三；

图 6 为本发明实施例提供的一种攻击数据包的处理方法的交互图一；

图 7 为本发明实施例提供的一种攻击数据包的处理方法的交互图二；

图 8 为本发明实施例提供的一种攻击数据包的处理方法的交互图三；

图 9 为本发明实施例提供的一种通信系统框图二；

图 10 为本发明实施例提供的一种通信系统框图三。

图 11 为本发明实施例提供的一种管理节点的结构示意图；

图 12 为本发明实施例提供的一种 SDN 控制器的结构示意图；

图 13 为本发明实施例提供的一种感知节点的结构示意图；

图 14 为本发明实施例提供的一种管理节点的硬件结构示意图；

图 15 为本发明实施例提供的一种 SDN 控制器的硬件结构示意图；

图 16 为本发明实施例提供的一种感知节点的硬件结构示意图；

图 17 为本发明实施例提供的一种通信系统框图四；

图 18 为本发明实施例提供的一种通信系统框图五。

具体实施方式

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，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。

在本发明实施例中，感知节点可以为云数据中心中所有能够识别攻击数据包的云服务器，例如，各种处理业务的虚拟机（英文：virtual machine，缩写：VM），虚拟机监控器，防火墙，负载均衡器（英文：load balancer），网关（英文：gateway）等。管理节点可以为云数据中心中的所有业务管理节点或策略管理节点，例如，VM 管理器（英文：manager），虚拟机基础设施管理器（英文：virtualized infrastructure manager，缩写：VIM），策略与计费规则功能单元（英文：policy and charging rules function，缩写：PCRF）等。

本发明实施例提供的攻击数据包的处理方法，可以应用于基于软

件定义网络（英文：software defined network，缩写：SDN）技术的网络架构中。基于 SDN 技术的网络架构是一种将控制与转发分离并直接可编程的网络架构。在基于 SDN 技术的网络架构中，每一个数据包在网络中的具体转发路径以及转发策略均由 SDN 控制器（英文：controller）控制，由 SDN 控制器将数据包的转发路径和转发策略等通过 Open Flow 协议，发送至 SDN 架构中的交换机群，由交换机群中的交换机将数据包转发至云数据中心中的云服务器。其中，基于 SDN 技术的网络架构中的交换机只负责根据数据包的转发策略转发路径对数据包进行转发。

示例性的，如图 1 所示，为本发明实施例提供的一种通信系统框图。如图 1 所示，数据中心中有 3 个 VM 和一个 VM 管理器，数据中心中的 3 个 VM 在基于 SDN 技术的网络架构中，无论是与数据中心外部的服务器进行数据包的传输，还是与 3 个 VM 之间相互进行数据包的传输，均由 SDN 控制器控制数据包的转发路径和转发策略，并由交换机实现对数据包的转发。

本发明实施例提供一种攻击数据包的处理方法，能够通过控制交换机对攻击数据包进行处理，限制交换机对攻击数据包的转发，进而限制攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而保证云数据中心中的云服务器能够进行安全通信。

实施例一

本发明实施例提供一种攻击数据包的处理方法，如图 2 所示，该方法可以包括：

S101、管理节点接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型。

其中，攻击数据包可以理解为对感知节点造成威胁的数据包，例如具有畸形报文的数据包，报文分片异常的数据包，传输控制协议(英文：transmission control protocol，缩写：TCP)无效连接的数据包，数据量过大的数据包等。

可选的，该攻击数据包的描述信息可以为感知节点从该攻击数据包的包头中获取的信息，具体可以为该攻击数据包的源 IP 地址、该攻击数据包的目的 IP 地址、该攻击数据包的源端口号、该攻击数据包的目的端口号，以及该攻击数据包协议号。其中，该攻击数据包的源端

口号具体可以为用户数据包协议（英文：user data protocol，缩写：UDP)源端口号，该攻击数据包的目的端口号具体可以为 UDP 目的端口号；或者该攻击数据包的源端口号具体可以为 TCP 源端口号，该攻击数据包的目的端口号具体可以为 TCP 目的端口号。通过该描述信息，就能够使得交换机对具有该描述信息的攻击数据包进行处理。

其中，攻击数据包的攻击类型可以包括但不限于 DDoS 攻击、基于会话初始协议（英文：session initiation protocol，缩写：SIP）攻击、TCP 无效连接、超大数据量、假消息攻击等。

S102、管理节点根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

其中，处理策略可以包括对攻击数据包的处理动作，例如，丢弃（英文：drop），限流（英文：car），重定向（英文：redirect）等。或者，处理策略也可以包括对攻击数据包的处理动作和执行该处理动作的时间。其中，执行该处理动作的时间具体可以为立即执行（英文：immediately）该处理动作，延时执行（英文：delay）该处理动作，或是持续执行（英文：duration）该处理动作等。

进一步的，在本发明实施例中，管理节点根据攻击类型确定对具有该攻击类型的攻击数据包的处理策略的方式有多种。下面以两种可能的实现方式（方式一和方式二）对管理节点根据攻击类型确定对具有该攻击类型的攻击数据包的处理策略进行示例性的说明。其他管理节点根据攻击类型确定对具有该攻击类型的攻击数据包的处理策略的方式均在本发明的保护范围内，本发明不作限制。

方式一，在本发明实施例中，管理节点可以根据攻击类型，获取预设的对具有该攻击类型的攻击数据包的处理策略。具体的，可以在管理节点中预设一个攻击类型与处理策略之间的映射关系，当管理节点接收到某个攻击类型时，可以根据该攻击类型从该预设的映射关系中，确定出与该攻击类型对应的处理策略，即确定出对具有该攻击类型的攻击数据包的处理策略。

举例来说，假设，在管理节点中预设的攻击类型与处理策略之间的映射关系可以如表 1 所示。表 1 中的处理策略包括攻击数据包的处理动作。其中，“Car+1Mbps”表示对具有超大数据量的攻击数据包执

行限流操作，使得限流以后该数据包使用的最大带宽为 1Mbps；“Redirect+null0”表示对具有基于 SIP 攻击的攻击数据包执行重定向操作，使得该攻击数据包被转发到 null0 接口，其中，null0 接口表示路由黑洞接口，被转发至 null0 接口的数据包都被丢弃，且将攻击数据包转发到 null0 接口对网络负载的影响非常小。具体的，例如，当管理节点接收到的攻击类型为 DDoS 攻击时，可以根据表 1 确定对具有 DDoS 攻击的攻击数据包的处理策略为丢弃“drop”。

表 1

攻击类型	处理策略
DDoS攻击	Drop
超大数据量	Car+1Mbps
基于SIP的攻击	Redirect+null0

可选的，在上述表 1 中的处理策略还可以包括处理动作和执行该处理动作的时间。例如，可以预设与 DDoS 攻击对应的处理策略可以为“Drop+immediately”，表示对具有 DDoS 攻击的攻击数据包立即执行丢弃操作；与基于 SIP 攻击对应的处理策略可以为“Redirect+null0+immediately +duration180”，表示对具有基于 SIP 攻击的攻击数据包立即执行重定向操作，使得该攻击数据包被立即转发到 null0 接口，并持续转发 180 分钟。

需要说明的是，在具体实现过程中，可以根据实际工程需要在管理节点中设置合适的攻击类型与处理策略之间的映射关系，本发明不作限制。

方式二，管理节点根据攻击类型和预设的算法，生成对具有该攻击类型的攻击数据包的处理策略。具体的，可以在管理节点中预设一种算法，当管理节点接收到某个攻击类型时，通过对该攻击类型进行该预设的算法流程，生成对具有该攻击类型的攻击数据包的处理策略。

示例性的，当管理节点接收到攻击类型为 DDoS 攻击时，管理节点将该攻击类型的代码通过该预设的算法进行计算，生成对具有该攻击类型的攻击数据包的处理策略“drop”。当管理节点接收到攻击类型为基于 SIP 攻击时，管理节点将该攻击类型的代码通过该预设的算法进行计算，生成对具有该攻击类型的攻击数据包的处理策略为

“Redirect+null0”。

需要说明的是，在具体实现过程中，可以根据实际工程需要在管理节点中设置合适的算法，本发明不作限制。

S103、管理节点经由 SDN 控制器向交换机发送该描述信息和该处理策略，由该交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

示例性的，假设管理节点接收的攻击数据包的描述信息具体为“【10.11.100.100 10.22.200.200 6 1234 4321】”，其中，10.11.100.100 表示该攻击数据包的源 IP 地址，10.22.200.200 表示该攻击数据包的目的IP地址，1234表示该攻击数据包的源端口号，4321表示该攻击数据包的目的端口号，该攻击数据包的协议号为 6。管理节点接收的该攻击数据包的攻击类型为 DDoS 攻击，根据该攻击类型确定的该攻击数据包的处理策略为“Drop+immediately”。则管理节点可以将该描述信息和该处理策略以“【10.11.100.100 10.22.200.200 6 1234 4321】+Drop+immediately”的格式发送给 SDN 控制器。由 SDN 控制器将接收到的“【10.11.100.100 10.22.200.200 TCP 1234 4321】+ Drop+immediately”按照 Open Flow 协议规定的格式转发给交换机。

交换机接收到该描述信息和该处理策略后，根据该处理策略立即丢弃具有该描述信息的攻击数据。从而该交换机不再对该攻击数据包进行转发，使得攻击数据包不在网络中传输，即使得具有该描述信息的攻击数据包不占用网络带宽，进而保证正常数据包的传输。

可以理解的是，若管理节点根据该攻击类型确定的该攻击数据包的处理策略为“Car+1Mbps”，则当管理节点将该描述信息和该处理策略经由 SDN 控制器发送至交换机后，交换机对具有该描述信息的攻击数据包执行限流操作，使得具有该描述信息的攻击数据包在网络中传输时最多只占用 1Mbps 的带宽。也就是说，即使交换机仍然对该攻击数据包进行转发，但是该攻击数据包在网络中传输时最多只占用 1Mbps 的带宽，因此，限制了具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输。

进一步的，交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作的过程，将在下述实施例中进行详细说明，此处不再赘

述。

本发明实施例提供一种攻击数据包的处理方法，具体为管理节点接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型，并根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，以及经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，其中，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。通过该方法，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，管理节点能够根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

本发明实施例提供一种攻击数据包的处理方法，如图 3 所示，该方法可以包括:

S201、SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略。

其中，攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略具体可参见如图 2 所示的实施例中的相关描述，此处不再赘述。

S202、SDN 控制器向第一交换机发送该描述信息和该处理策略，由第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

其中，第一交换机为由 SDN 控制器控制的交换机群中的任意一个。

具体的，SDN 控制器可以将该描述信息和该处理策略转换成控制器-交换机（英文: Controller-to-Switch）消息发送至第一交换机。其中，控制器-交换机消息是 Open Flow 协议规定的一种消息，由 SDN 控制器向交换机发送，指示交换机修改或丢弃该交换机的流表中记录的信息。

当SDN控制器将该描述信息和该处理策略转换成控制器-交换机消息发送至第一交换机后，第一交换机根据该控制器-交换机消息中包含的该描述信息，在该第一交换机的流表中查找与该描述信息匹配的攻击数据流，然后根据该控制器-交换机消息中包含的该处理策略，对该攻击数据流的攻击数据包执行该处理策略指示的操作，即 SDN 控制器根据该处理策略，对具有该描述信息的攻击数据包执行该处理策略指示的操作。

如图 4 所示，为本发明实施例提供的第一交换机的流表示意图。在图 4 中，第一交换机的流表由包头域（英文: header fields），计数器（英文: counters）和对数据包的实施动作（英文:actions）构成。其中，包头域中具体可以包括该第一交换机接收的数据流的源 IP 地址、目的 IP 地址、源介质访问控制（英文: media access control，缩写: MAC）地址、目的 MAC 地址、协议号，源端口号和目的端口号等；计数器用于统计该第一交换机接收的数据流的数据包的个数，该数据流字节数和该数据流持续传输的时间等；对数据包的实施动作可以包括转发数据包，丢弃数据包和修改流表中数据包的包头中的信息等。

示例性的，假设，SDN 控制器接收的描述信息和处理策略为“【 10.11.100.100 10.22.200.200 6 1234 4321 】+ Drop+immediately”，则 SDN 控制器将“【 10.11.100.100 10.22.200.200 6 1234 4321】+ Drop+immediately”按照 Open Flow 协议规定格式发送至第一交换机后，第一交换机在该第一交换机的流表中查找源 IP 地址为 10.11.100.100，目的 IP 地址为 10.22.200.200，源端口号为 1234，目的端口号为 4321，以及协议号为 6 的攻击数据流。第一交换机查找到该攻击数据流后，根据该处理策略，对该攻击数据流的攻击数据包的实施动作具体为立即丢弃。即第一交换机对具有描述信息为“【10.11.100.100 10.22.200.200 6 1234 4321】”的攻击数据包执行立即丢弃的操作。

需要说明的是，第一交换机的流表中保存的每个数据流，都具有唯一的描述信息，和对每个数据流的数据包的实施动作。当一个数据流的所有数据包传输完成后，流表将删除对该数据流的记录。因此，在本发明实施例提供的攻击数据包的处理方法中，第一交换机能够根据 SDN 控制器发送的描述信息和处理策略，在流表中查找具有该描述

信息的攻击数据流，并将对该攻击数据流的攻击数据包的实施动作更改为该处理策略指示的操作，从而对该攻击数据流的攻击数据包中未传输的攻击数据包执行该处理策略指示的操作，进而避免云服务中心中的感知节点被该攻击数据流的攻击数据包持续攻击。

本发明实施例提供一种攻击数据包的处理方法，具体为 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略，并向第一交换机发送该描述信息和该处理策略，由第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。通过该方法，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的云服务器能够进行安全通信。

本发明实施例提供一种攻击数据包的处理方法，如图 5 所示，该方法可以包括:

S301、感知节点识别该感知节点接收的数据包为攻击数据包。

其中，感知节点识别该感知节点接收的数据包为攻击数据包的方式有多种，下面列举三个例子对感知节点识别攻击数据包的方法进行示例性的说明。

例一，感知节点接收到数据包后，识别该感知节点接收的数据包的报文，若感知节点判断该数据包的源 IP 地址和目的 IP 地址相同，则感知节点确定该数据包的报文为畸形报文，进而确定该数据包为攻击数据包。

例二，感知节点接收到数据包后，在预设时间内，若感知节点判断该感知节点收到的数据包的报文流量超过预设的阈值，则感知节点确定该数据包为攻击数据包。

例三，感知节点接收到数据包后，识别该数据包中的 SIP 信令，

判断该数据包的SIP会话流程与已知的标准中SIP会话流程是否相同，若感知节点判断该数据包的SIP会话流程与已知的标准中SIP会话流程不相同，则感知节点确定该数据包为攻击数据包。

进一步的，感知节点识别该感知节点接收的数据包为攻击数据包的其他方式，与现有技术中感知节点识别该感知节点接收的数据包为攻击数据包的方式相同，此处不再一一列举。

需要说明的是，由于在本发明实施例中，感知节点可以为云数据中心中所有能够识别攻击数据包的业务节点，例如，VM，虚拟机监控器，防火墙，负载均衡器，网关等。因此，与现有技术中通过防火墙识别IP层信令的方式识别攻击数据包相比，在本发明实施例提供的攻击数据包的处理方法，感知节点不止能够通过识别IP层信令识别攻击数据包（例如，通过识别畸形报文识别攻击数据包），也能通过识别业务层信令识别攻击数据包（例如，通过识别SIP信令识别基于SIP攻击的攻击数据包）。从而提高识别攻击数据包的精确度，进而更全面的防止攻击数据包对感知节点的攻击。

S302、感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型。

示例性的，若感知节点识别该感知节点接收的数据包的报文为畸形报文，由于畸形报文攻击数据DDoS攻击的一类，则感知节点可以确定该攻击数据包的攻击类型为DDoS攻击；若感知节点通过识别SIP信息识别该感知节点接收的数据包为攻击数据包，则感知节点可以确定该数据包的攻击类型为基于SIP攻击；若感知节点数据包的报文流量超过预设的阈值，识别该数据包为攻击数据包，则感知节点可以确定该数据包的攻击类型为大数据量攻击。

进一步的，感知节点确定该感知节点接收的数据包为攻击数据包后，感知节点从该攻击数据包中获取该攻击数据包的描述信息。可选的，该攻击数据包的描述信息具体可以为该攻击数据包的源IP地址、该攻击数据包的目的IP地址、该攻击数据包的源端口号、该攻击数据包的目的端口号，以及该攻击数据包的协议号。

S303、感知节点向管理节点发送该描述信息和该攻击类型，该攻击类型用于管理节点确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示转发数据包的交换机对具有该描述信息的攻

击数据包执行该处理策略指示的操作。

其中，管理节点确定对具有该攻击类型的攻击数据包的处理策略的过程，具体可以参见如图 2 所示的实施例中的相关描述，交换机根据该处理策略对具有该描述信息的攻击数据包执行该处理策略指示的操作，具体可参见如图 3 所示的实施例中的相关描述，此处不再赘述。

本发明实施例提供一种攻击数据包的处理方法，具体为感知节点识别该感知节点接收的数据包为攻击数据包，并确定该攻击数据包的描述信息和该攻击数据包的攻击类型，以及向管理节点发送该描述信息和该攻击类型，该攻击类型用于管理节点确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示转发数据包的交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。通过该方法，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和具有该描述信息的攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，解决了现有技术中攻击数据包占用大量的网络带宽，影响正常的数据包的传输的问题，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够进行安全通信。

实施例二

本发明实施例提供一种攻击数据包的处理方法，如图 6 所示，该方法可以包括:

S401、感知节点接收数据包。

S402、感知节点识别该数据包为攻击数据包。

S403、感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型。

S404、感知节点向管理节点发送该描述信息和该攻击类型。

具体的，上述 S401-S404 的具体实现方式，可以参见如图 5 所示

的实施例中的相关描述，此处不再赘述。

S405、管理节点接收感知节点发送的该描述信息和该攻击类型后，根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略。

S406、管理节点将该描述信息和该处理策略发送至 SDN 控制器。

需要说明的是，在本发明实施例中，在管理节点上预设了一个通讯接口，该通讯接口用于管理节点向 SDN 控制器发送该描述信息和该攻击类型。同时，在 SDN 控制器上预设了一个通讯接口，用于 SDN 控制器接收管理节点发送的该描述信息和该攻击类型。

具体的，若管理节点和 SDN 控制器之间是通过 UDP 协议进行信息交互，则管理节点和 SDN 控制器上的通讯接口可以基于 UDP 协议进行设置。当管理节点向 SDN 控制器发送该描述信息和该攻击类型时，无需建立与 SDN 控制器之间的通信链路，可以直接通过管理节点上预设的通讯接口的地址和 SDN 控制器预设的通讯接口的地址，向 SDN 控制器发送该描述信息和该攻击类型。

若管理节点和 SDN 控制器之间是通过 TCP 协议进行信息交互，则管理节点和 SDN 控制器上的通讯接口可以基于 TCP 协议进行设置。当管理节点向 SDN 控制器发送该描述信息和该攻击类型时，管理节点与 SDN 控制器之间需建立 TCP 连接，在两个预设的通讯接口之间建立通信链路，管理节点通过该通信链路将该描述信息和该攻击类型发送至 SDN 控制器。

S407、SDN 控制器向第一交换机发送该描述信息和该处理策略。

S408、第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

具体的，上述 S407-S408 的具体实现方式，可以参见如图 3 所示的实施例中的相关描述，此处不再赘述。

可选的，在上述 S405 中，若管理节点接收到多个感知节点发送的多个攻击数据包的描述信息和该多个攻击数据包的攻击类型时，结合图 6，如图 7 所示，上述 S405 具体可以包括：

S405a、管理节点根据该多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型。

S405b、管理节点根据该至少两个攻击类型中的一个攻击类型，确

定对具有该一个攻击类型的攻击数据包的处理策略。

具体的，若管理节点接收到多个感知节点发送的多个攻击数据包的描述信息和该多个攻击数据包的攻击类型，则管理节点根据多个攻击数据包的攻击类型，判断该多个攻击数据包的攻击类型中是否有至少两个攻击类型相同，若管理节点确定该多个攻击数据包的攻击类型中存在至少两个攻击类型相同，则管理节点根据该至少两个攻击类型中的一个攻击类型，确定对具有该一个攻击类型的攻击数据包的处理策略。即由于该至少两个攻击类型均相同，因此管理节点根据该至少两个攻击类型中的任意一个攻击类型，确定出具有该攻击类型的攻击数据包的处理策略。

进一步的，管理节点将该处理策略分别与该至少两个攻击数据包的描述信息发送至 SDN 控制器，即该至少两个具有该相同攻击类型的攻击数据包的描述信息分别对应的处理策略均为该处理策略。

进一步的，在上述 S406 之后，结合图 6，如图 8 所示，该方法还包括:

S409、SDN 控制器向与该 SDN 控制器连接的主 SDN 控制器发送该描述信息和该处理策略。

S410、主 SDN 控制器向第二交换机发送该描述信息和该处理策略。

S411、第二交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

需要说明的是，上述 S407 和 S409 的先后顺序在本发明实施例中不作限制。

具体的，若一个数据中心的内部网络与该数据中心的外部网络都采用基于 SDN 技术的网络架构，则当该数据中心内部的 SDN 控制器接收到管理节点发送的该描述信息和该处理策略后，SDN 控制器会将该描述信息和该处理策略直接转发至主 SDN 控制器，主 SDN 控制器是该数据中心外与该 SDN 控制器连接的 SDN 控制器，即主 SDN 控制器是与该数据中心连接的骨干网络中的 SDN 控制器。主 SDN 控制器将该描述信息和该处理策略以 Open Flow 协议规定的格式发送至第二交换机。该第二交换机为由主 SDN 控制器控制的交换机群中的任意一个。该第二交换机接收到该描述信息和该处理策略后，对具有该描述信息的数据包执行该处理策略指示的操作，从而达到在全网中限制攻击数据包在

传输时占用个网络带宽，保证正常的数据包的传输。

其中，该第二交换机对该攻击数据包执行该处理策略指示的操作的具体过程可参见如图 3 所示的实施例中，第一交换机对该攻击数据包执行该处理策略指示的操作的具体过程，此处不再赘述。

进一步的，下面列举两种可能的应用场景，对本发明实施例提供的攻击数据包的处理方法进行示例性的说明。如图 9 所示，为本发明实施例提供的一种通信系统框图，当感知节点具体为云数据中心中的客机操作系统(英文: guest operating system)层的 VM 时，例如虚拟交换机（英文: virtual switch，缩写: vSwitch）中的一个 VM，可以为 VM 交换机 2 中的 VM2,管理节点具体为云数据中心中的 VM 管理器时，由于 VM2 能够识别数据包的 IP 层信令,因此当 VM2 接收到 IP 层 DDoS 攻击（如畸形报文攻击）的攻击数据包时，VM2 能够识别该攻击数据包。从而如图 9 所示的通信系统中的 VM2、VM 管理器，SDN 控制器以及交换机能够通过执行上述如图 6 或如图 7 所示的方法，处理攻击数据包。

如图 10 所示，为本发明实施例提供的另一种通信系统框图，当感知节点具体为云数据中心中的虚拟机监控器，例如虚拟机监控器 2，管理节点具体为云数据中心中的 PCRF 时，由于虚拟机监控器 2 能够通过识别数据包的业务层信令识别攻击数据包，例如通过识别 SIP 信令识别基于 SIP 攻击的攻击数据包，因此，当虚拟机监控器 2 接收到基于 SIP 攻击的攻击数据包时，虚拟接监控器 2 能够识别该攻击数包。从而虚拟机监控器 2、PCRF，SDN 控制器以及交换机能够通过执行上述如图 6 或如图 7 所示的方法，处理攻击数据包。

本发明实施例提供一种攻击数据包的处理方法，具体包括: 感知节点识别该感知节点接收的数据包为攻击数据包，确定该攻击数据包的描述信息和对该攻击数据包的处理策略，并将该描述信息和该处理策略发送给管理节点，管理节点根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，其中，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。通过该方法，能够限制该攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，从而解决了现有技术中攻击数据包占用大量的网络带宽，

影响正常的数据包的传输的问题，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的云服务器能够安全通信。

实施例三

如图 11 所示，本发明实施例提供一种管理节点，该管理节点可以包括:

接收单元 10，用于接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型。

确定单元 11，用于根据所述接收单元 10 接收的所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

发送单元 12，用于经由软件定义网络 SDN 控制器向所述交换机发送所述接收单元 10 接收的所述描述信息和所述确定单元 11 确定的所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

可选的，所述确定单元 11，具体用于根据所述接收单元 10 接收的所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

可选的，所述确定单元 11，具体用于根据所述接收单元 10 接收的所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

可选的，所述确定单元 11 确定的所述处理策略指示的操作包括:对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

可选的，所述确定单元 11，具体用于当所述接收单元 10 接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，根据所述多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型，以及根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

可选的，所述发送单元 12，具体用于通过预设的通讯接口向所述

SDN 控制器发送所述接收单元 10 接收的所述描述信息和所述确定单元 11 确定的所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

可选的，所述接收单元 10 接收的所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

需要说明的是，本发明实施例提供的管理节点可以为云数据中心中的所有业务管理节点或策略管理节点，例如，VM 管理器，VIM，PCRF 等。

本发明实施例提供一种管理节点，该管理节点能够接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型，并根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，以及经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，其中，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，本发明实施例提供的管理节点能够根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

如图 12 所示，本发明实施例提供一种 SDN 控制器，该 SDN 控制器可以包括:

接收单元 20，用于接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略。

发送单元 21，用于向第一交换机发送所述接收单元 20 接收的所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

可选的，所述接收单元 20，具体用于通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

可选的，所述发送单元 21，还用于向主 SDN 控制器发送所述接收单元 20 接收的所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

本发明实施例提供一种 SDN 控制器，该 SDN 控制器能够接收管理节点发送的攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略，并向第一交换机发送该描述信息和该处理策略，由第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由本发明实施例提供的 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

如图 13 所示，本发明实施例提供一种感知节点，该感知节点可以包括：

识别单元 30，用于识别所述感知节点接收的数据包为攻击数据包。

确定单元 31，用于确定所述识别单元 30 识别的所述攻击数据包的描述信息和所述攻击数据包的攻击类型。

发送单元 32，用于向管理节点发送所述确定单元 31 确定的所述描述信息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

可选的，所述确定单元 31 确定的所述描述信息包括：所述攻击数

据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

需要说明的是，本发明实施例提供的感知节点可以为云数据中心中所有能够识别攻击数据包的云服务器，例如，各种处理业务的 VM，虚拟机监控器，防火墙，负载均衡器，网关等。

本发明实施例提供一种感知节点，该感知节点能够识别该感知节点接收的数据包为攻击数据包，并确定该攻击数据包的描述信息和该攻击数据包的攻击类型，以及向管理节点发送该描述信息和该攻击类型，该攻击类型用于管理节点确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示转发数据包的交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当本发明实施例提供的感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和具有该描述信息的攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

实施利四

如图 14 所示，本发明实施例提供一种管理节点，该管理节点可以包括：处理器 40、通信接口 41、存储器 42，以及系统总线 43。所述处理器 40、通信接口 41，以及存储器 42 之间通过所述系统总线 43 连接并完成相互之间的通信。

所述处理器 40 可以是一个中央处理器（英文：Central Processing Unit，缩写：CPU），或者是特定集成电路（英文：Application Specific Integrated Circuit，缩写：ASIC），或者是被配置成实施本发明实施例的一个或多个集成电路。

所述通信接口 41，用于与其他设备进行交互，例如，与感知节点

进行交互，或者与 SDN 控制器进行交互。

所述存储器 42 可以包括易失性存储器（英文：volatile memory），例如随机存取存储器（英文：random-access memory，缩写：RAM）；所述存储器 42 也可以包括非易失性存储器（英文：non-volatile memory），例如只读存储器（英文：read-only memory，缩写：ROM），快闪存储器（英文：flash memory），硬盘（英文：hard disk drive，缩写：HDD）或固态硬盘（英文：solid-state drive，缩写：SSD）；所述存储器 42 还可以包括上述种类的存储器的组合。

当所述管理节点运行时，所述处理器 40、通信接口 41，以及存储器 42，可以执行图 2、或图 6 至图 8 任意之一所述的方法流程，具体包括：

所述处理器 40，用于通过所述通信接口 41 接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型，并根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，以及经由 SDN 控制器向所述交换机发送所述描述信息和所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作；所述存储器 42，用于存储所述描述信息的代码、所述攻击类型的代码、所述处理策略的代码，以及控制所述处理器 40 完成上述过程的软件程序，从而所述处理器 40 通过执行所述软件程序，并调用所述描述信息的代码、所述攻击类型的代码，以及所述处理策略的代码，完成上述过程。

可选的，所述处理器 40，具体用于根据所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

可选的，所述处理器 40，具体用于根据所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

可选的，所述处理器 40 确定的所述处理策略指示的操作包括：

对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

可选的，所述处理器 41，具体用于当通过所述通信接口 41 接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，根据所述多个攻击数据包的攻击类型，确定攻击

类型相同的至少两个攻击类型，以及根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

可选的，所述处理器 40，具体用于通过预设的通讯接口向所述 SDN 控制器发送所述描述信息和所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

可选的，所述处理器 40 通过所述通信接口 41 接收的所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

本发明实施例提供一种管理节点，该管理节点能够接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型，并根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，以及经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，其中，该处理策略用于指示交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，本发明实施例提供的管理节点能够根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

如图 15 所示，本发明实施例提供一种 SDN 控制器，该 SDN 控制器可以包括：处理器 50、通信接口 51、存储器 52，以及系统总线 53。所述处理器 50、通信接口 51，以及存储器 52 之间通过所述系统总线 53 连接并完成相互之间的通信。

所述处理器 50 可以是一个 CPU，或者是 ASIC，或者是被配置成实施本发明实施例的一个或多个集成电路。

所述通信接口 51，用于与其他设备进行交互，例如，与管理节点

进行交互，或者与交换机进行交互。

所述存储器 52 可以包括易失性存储器，例如，RAM；所述存储器 52 也可以包括非易失性存储器，例如 ROM，快闪存储器，HDD 或 SSD；所述存储器 52 还可以包括上述种类的存储器的组合。

当所述 SDN 控制器运行时，所述处理器 50、通信接口 51，以及存储器 52，可以执行图 3、或图 6 至图 8 任意之一所述的方法流程，具体包括：

所述处理器 50，用于通过所述通信接口 51 接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略，并向第一交换机发送所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作；所述存储器 52，用于存储所述描述信息的代码、所述处理策略的代码，以及控制所述处理器 50 完成上述过程的软件程序，从而所述处理器 50 通过执行所述软件程序，并调用所述描述信息的代码和所述处理策略的代码，完成上述过程。

可选的，所述处理器 50，具体用于通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

可选的，所述处理器 50，还用于通过通讯接口 51 向主 SDN 控制器发送所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

本发明实施例提供一种 SDN 控制器，该 SDN 控制器能够接收管理节点发送的攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略，并向第一交换机发送该描述信息和该处理策略，由第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由本发明实施例提供的 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，

保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

如图 16 所示，本发明实施例提供一种感知节点，该感知节点可以包括：处理器 60、通信接口 61、存储器 62，以及系统总线 63。所述处理器 60，通信接口 61 以及存储器 62 之间通过所述系统总线 63 连接并完成相互之间的通信。

所述处理器 60 可以是一个 CPU，或者是 ASIC，或者是被配置成实施本发明实施例的一个或多个集成电路。

所述通信即可 61，用于与其他设备之间进行交互，例如与其他感知节点的交互，或者与管理节点之间进行交互。

所述存储器 62 可以包括易失性存储器，例如，RAM；所述存储器 62 也可以包括非易失性存储器，例如 ROM，快闪存储器，HDD 或 SSD；所述存储器 62 还可以包括上述种类的存储器的组合。

当所述感知节点运行时，所述处理器 60、通信接口 61，以及存储器 62，可以执行图 5 至图 8 任意之一所述的方法流程，具体包括：

所述处理器 60，用于识别通过所述通信接口 61 接收的数据包为攻击数据包，并确定所述攻击数据包的描述信息和所述攻击数据包的攻击类型，以及向管理节点发送所述描述信息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作；所述存储器 62，用于存储所述攻击数据包的代码、所述描述信息、所述攻击类型，以及控制所述处理器 60 完成上述过程的软件程序，从而所述处理器 60 通过执行所述软件程序，并调用所述攻击数据包的代码、所述描述信息，以及所述攻击类型，完成上述过程。

可选的，所述处理器 60 确定的所述描述信息包括：所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

本发明实施例提供一种感知节点，该感知节点能够识别该感知节点接收的数据包为攻击数据包，并确定该攻击数据包的描述信息和该

攻击数据包的攻击类型，以及向管理节点发送该描述信息和该攻击类型，该攻击类型用于管理节点确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示转发数据包的交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。因此，当本发明实施例提供的感知节点在识别其接收的数据包为攻击数据包，并将该攻击数据包的描述信息和具有该描述信息的攻击数据包的攻击类型发送给管理节点后，由管理节点根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，管理节点将该描述信息和该攻击类型经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

实施例五

如图 17 所示，本发明实施例提供通信系统，该通信系统可以包括：如图 11 所示的管理节点、如图 12 所示的 SDN 控制器、如图 13 所示的感知节点，以及交换机；或者，本发明实施例提供的通信系统也可以包括：如图 14 所示的管理节点、如图 15 所示的 SDN 控制器、如图 16 所示的感知节点，以及交换机。其中，交换机为基于 SDN 技术的网络架构中的由 SDN 控制器控制的交换机。

在本发明实施例提供的通信系统中，感知节点能够识别该感知节点接收的数据包为攻击数据包，并确定该攻击数据包的描述信息和该攻击数据包的攻击类型，以及向管理节点发送该描述信息和该攻击类型。管理节点接收到该描述信息和该攻击类型后，能够根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，并向 SDN 控制器发送该描述信息和该处理策略。SDN 控制器接收到管理节点发送的该处理策略和该描述信息后，向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

可选的，结合图 17，如图 18 所示，本发明实施例还提供的通信系统还可以包括主 SDN 控制器，以及由主 SDN 控制器控制的交换机。所述主 SDN 控制器为数据中心外部与所述 SDN 控制器连接的 SDN 控制器。

在本发明实施例提供的通信系统中，当 SDN 控制器接收到管理节点发送描述信息和处理策略后，SDN 控制器将该描述信息和该处理策略转发给主 SDN 控制器，并由主 SDN 控制将该描述信息盒盖处理策略发送至由主 SDN 控制器控制的交换机，并由该交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作。

通过本发明实施例提供的通信系统，当感知节点在识别该感知节点接收的数据包为攻击数据包，并将该攻击数据包的描述信息和该攻击数据包的攻击类型发送给管理节点后，管理节点能够根据该攻击类型确定对具有该攻击类型的攻击数据包的处理策略，并经由 SDN 控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作，从而限制具有该描述信息的攻击数据包在网络中传输时占用的网络带宽，保证正常的数据包的传输，进而避免云数据中心中的感知节点被具有该描述信息的攻击数据包持续攻击，保证云数据中心中的感知节点能够安全通信。

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，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。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。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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）或处理器执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（英文全称：Read-Only Memory，英文缩写：ROM）、随机存取存储器（英文全称：Random Access Memory ，英文缩写： RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

权 利 要 求

1、一种攻击数据包的处理方法，其特征在于，包括:

管理节点接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型;

所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作;

所述管理节点经由软件定义网络 SDN 控制器向所述交换机发送所述描述信息和所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

2、根据权利要求 1 所述的方法，其特征在于，所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括:

所述管理节点根据所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

3、根据权利要求 1 所述的方法，其特征在于，所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括:

所述管理节点根据所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

4、根据权利要求 1-3 任一项所述的方法，其特征在于，

所述处理策略指示的操作包括:

对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，当所述管理节点接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，

所述管理节点根据所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，包括:

所述管理节点根据所述多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型;

所述管理节点根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述管理节点经由 SDN 控制器向所述交换机发送所述描述信息和所述处理策略，包括：

所述管理节点通过预设的通讯接口向所述 SDN 控制器发送所述描述信息和所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，

所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

8、一种攻击数据包的处理方法，其特征在于，包括：

软件定义网络 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略；

所述 SDN 控制器向第一交换机发送所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

9、根据权利要求 8 所述的方法，其特征在于，所述 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略，包括：

所述 SDN 控制器通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

10、根据权利要求 8 或 9 所述的方法，其特征在于，所述 SDN 控制器接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略之后，所述方法还包括：

所述 SDN 控制器向与所述 SDN 控制器连接的主 SDN 控制器发送所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

11、一种攻击数据包的处理方法，其特征在于，包括：

感知节点识别所述感知节点接收的数据包为攻击数据包；

所述感知节点确定所述攻击数据包的描述信息和所述攻击数据包

的攻击类型;

所述感知节点向管理节点发送所述描述信息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

12、根据权利要求 11 所述方法，其特征在于，

所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

13、一种管理节点，其特征在于，包括:

接收单元，用于接收感知节点发送的攻击数据包的描述信息和所述攻击数据包的攻击类型;

确定单元，用于根据所述接收单元接收的所述攻击类型，确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作;

发送单元，用于经由软件定义网络 SDN 控制器向所述交换机发送所述接收单元接收的所述描述信息和所述确定单元确定的所述处理策略，由所述交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

14、根据权利要求 13 所述的管理节点，其特征在于，

所述确定单元，具体用于根据所述接收单元接收的所述攻击类型，获取预设的对所述具有所述攻击类型的攻击数据包的处理策略。

15、根据权利要求 13 所述的管理节点，其特征在于，

所述确定单元，具体用于根据所述接收单元接收的所述攻击类型和预设的算法，生成对所述具有所述攻击类型的攻击数据包的处理策略。

16、根据权利要求 13-15 任一项所述的管理节点，其特征在于，

所述确定单元确定的所述处理策略指示的操作包括:

对所述具有所述描述信息的攻击数据包的处理动作，或对所述具有所述描述信息的攻击数据包的处理动作和执行所述处理动作的时间。

17、根据权利要求 13-16 任一项所述的管理节点，其特征在于，

所述确定单元，具体用于当所述接收单元接收多个所述感知节点发送的多个攻击数据包的描述信息和所述多个攻击数据包的攻击类型时，根据所述多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型，以及根据所述至少两个攻击类型中的一个攻击类型，确定对具有所述一个攻击类型的攻击数据包的处理策略。

18、根据权利要求 13-17 任一项所述的管理节点，其特征在于，

所述发送单元，具体用于通过预设的通讯接口向所述 SDN 控制器发送所述接收单元接收的所述描述信息和所述确定单元确定的所述处理策略，由所述 SDN 控制器向所述交换机转发所述描述信息和所述处理策略。

19、根据权利要求 13-18 任一项所述的管理节点，其特征在于，

所述接收单元接收的所述描述信息包括所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

20、一种软件定义网络 SDN 控制器，其特征在于，包括:

接收单元，用于接收管理节点发送的攻击数据包的描述信息和对具有所述描述信息的攻击数据包的处理策略;

发送单元，用于向第一交换机发送所述接收单元接收的所述描述信息和所述处理策略，由所述第一交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

21、根据权利要求 20 所述的 SDN 控制器，其特征在于，

所述接收单元，具体用于通过预设的通讯接口接收所述管理节点发送的所述描述信息和所述处理策略。

22、根据权利要求 20 或 21 所述的 SDN 控制器，其特征在于，

所述发送单元，还用于向主 SDN 控制器发送所述接收单元接收的所述描述信息和所述处理策略，由所述主 SDN 控制器向第二交换机转发所述描述信息和所述处理策略，并由所述第二交换机对所述具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

23、一种感知节点，其特征在于，包括:

识别单元，用于识别接收的数据包为攻击数据包;

确定单元，用于确定所述识别单元识别的所述攻击数据包的描述信息和所述攻击数据包的攻击类型;

发送单元，用于向管理节点发送所述确定单元确定的所述描述信

息和所述攻击类型，所述攻击类型用于所述管理节点确定对具有所述攻击类型的攻击数据包的处理策略，所述处理策略用于指示转发数据包的交换机对具有所述描述信息的攻击数据包执行所述处理策略指示的操作。

24、根据权利要求 23 所述感知节点，其特征在于，

所述确定单元确定的所述描述信息包括:

所述攻击数据包的源互联网协议 IP 地址、所述攻击数据包的源端口号、所述攻击数据包的目的 IP 地址、所述攻击数据包的目的端口号以及所述攻击数据包的协议号。

25、一种通信系统，其特征在于，包括:

如权利要求 13-19 任一项所述的管理节点，如权利要求 20-22 任一项所述的软件定义网络 SDN 控制器，如权利要求 23 或 24 所述的感知节点，以及交换机。

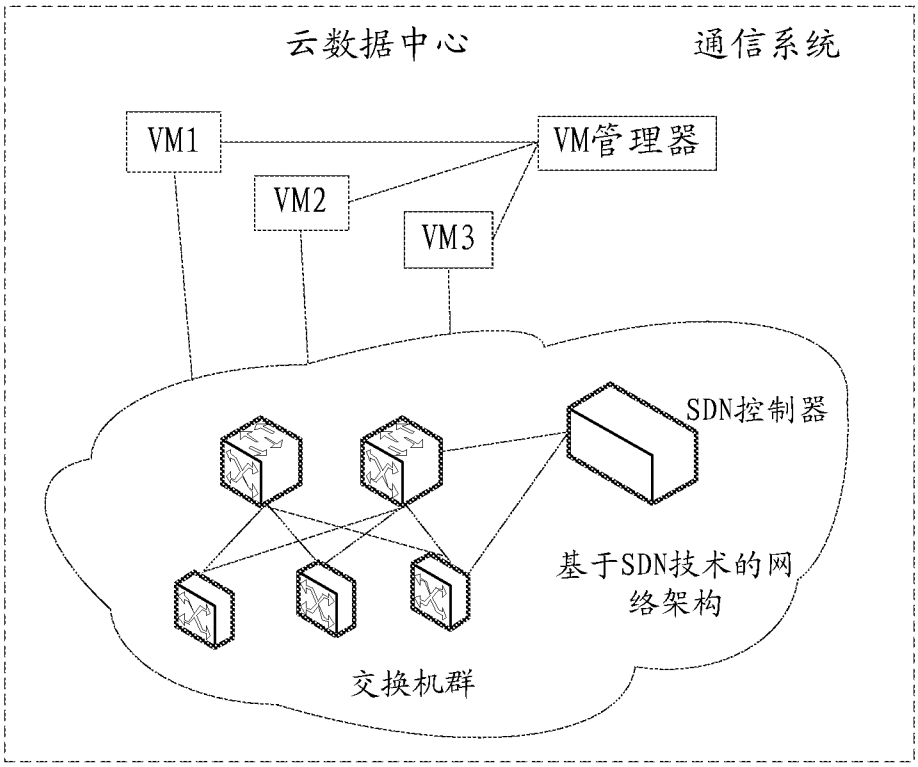
云数据中心
通信系统
VM1
VM2
VM3
VM管理器
SDN控制器
基于SDN技术的网络架构
交换机群

图 1

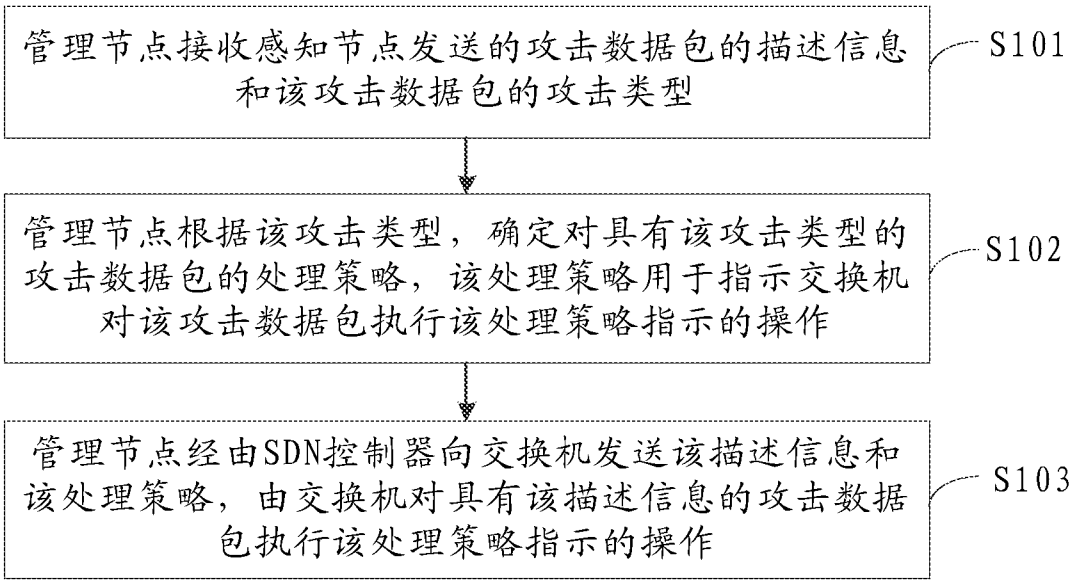
管理节点接收感知节点发送的攻击数据包的描述信息和该攻击数据包的攻击类型
S101
管理节点根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示交换机对该攻击数据包执行该处理策略指示的操作
S102
管理节点经由SDN控制器向交换机发送该描述信息和该处理策略，由交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作
S103

图 2

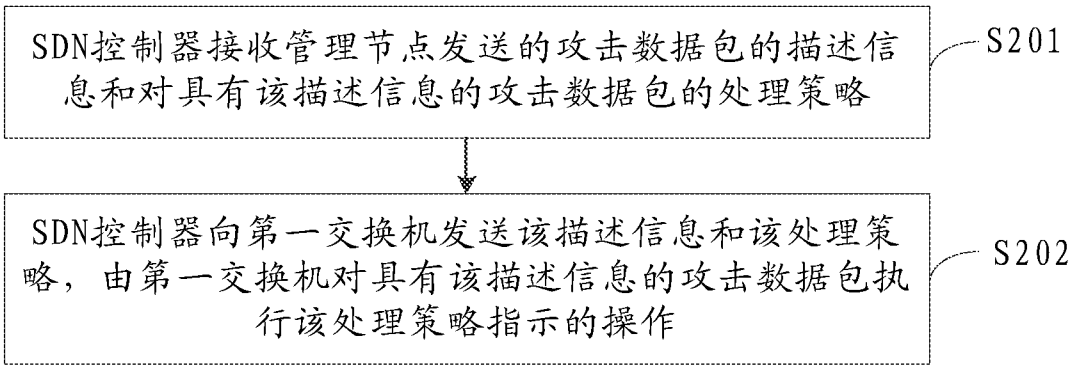
SDN控制器接收管理节点发送的攻击数据包的描述信息和对具有该描述信息的攻击数据包的处理策略
S201
SDN控制器向第一交换机发送该描述信息和该处理策略，由第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作
S202

图 3

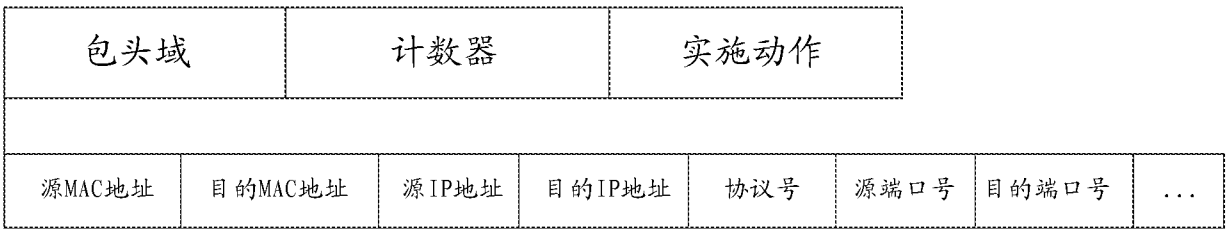
包头域
计数器
实施动作
源MAC地址
目的MAC地址
源IP地址
目的IP地址
协议号
源端口号
目的端口号
...

图 4

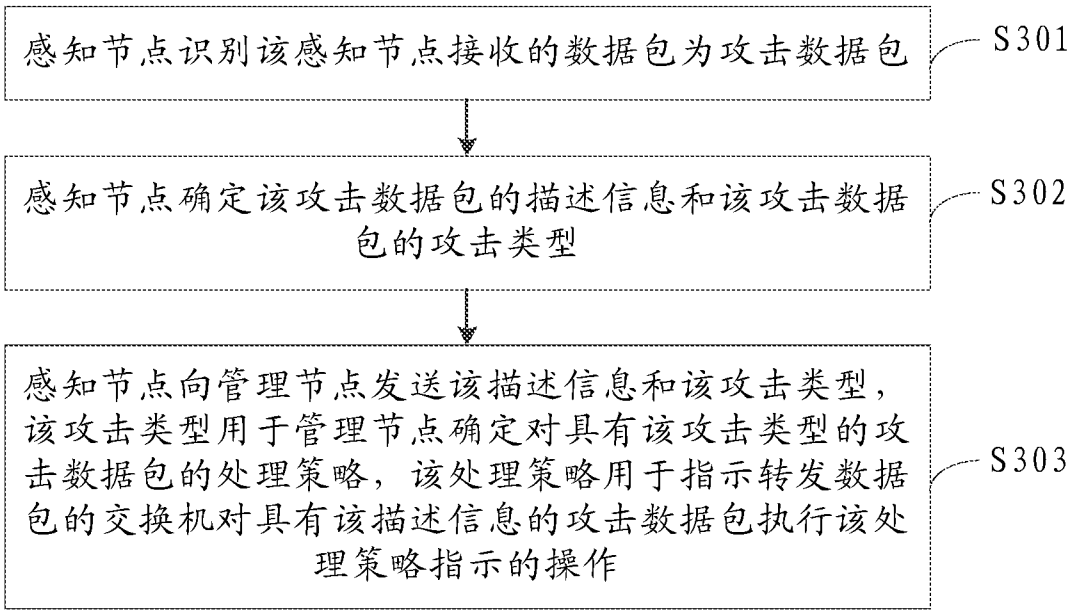
感知节点识别该感知节点接收的数据包为攻击数据包
S301
感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型
S302
感知节点向管理节点发送该描述信息和该攻击类型，该攻击类型用于管理节点确定对具有该攻击类型的攻击数据包的处理策略，该处理策略用于指示转发数据包的交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作
S303

图 5

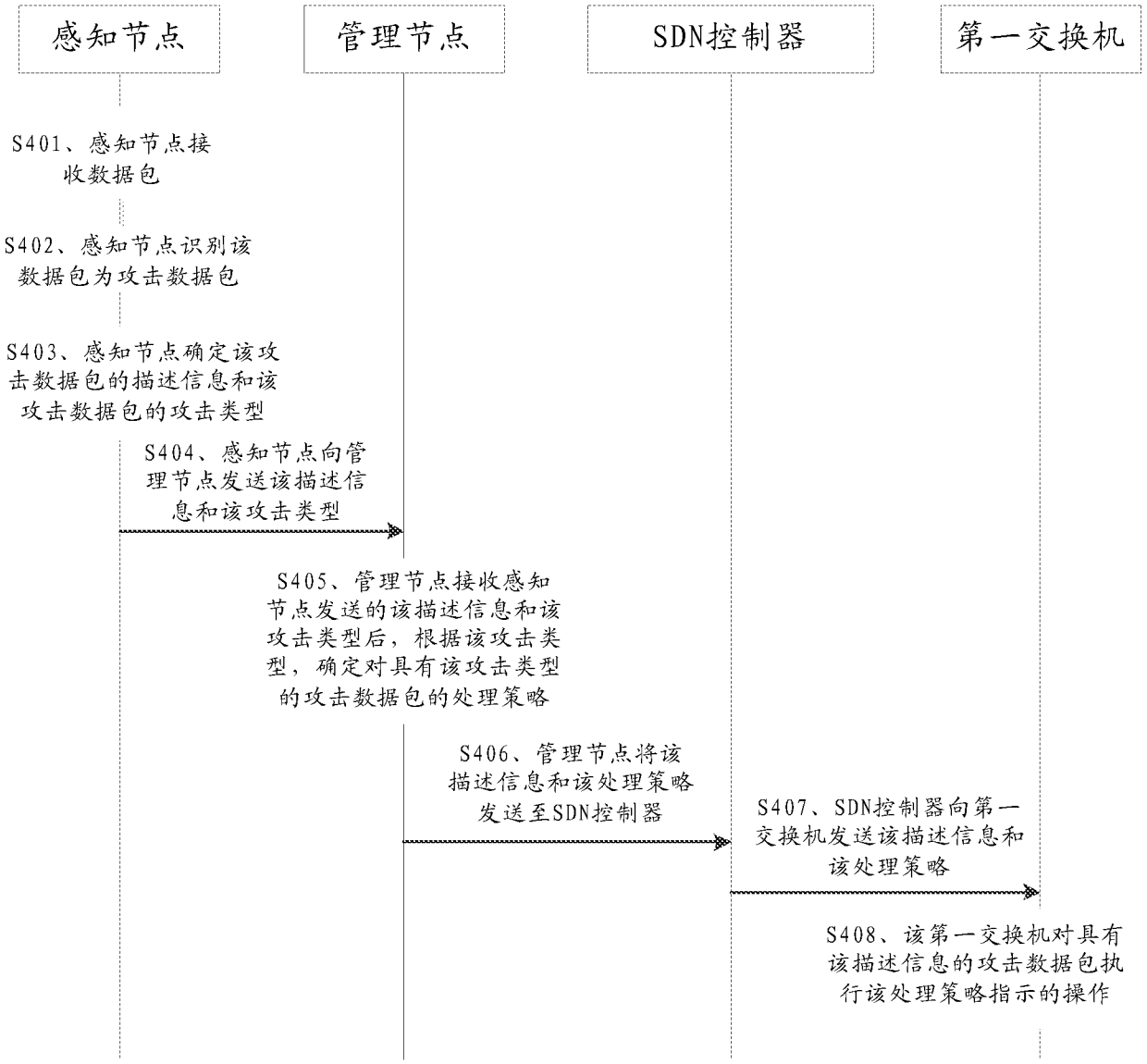
感知节点
管理节点
SDN控制器
第一交换机
S401、感知节点接收数据包
S402、感知节点识别该数据包为攻击数据包
S403、感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型
S404、感知节点向管理节点发送该描述信息和该攻击类型
S405、管理节点接收感知节点发送的该描述信息和该攻击类型后，根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略
S406、管理节点将该描述信息和该处理策略发送至SDN控制器
S407、SDN控制器向第一交换机发送该描述信息和该处理策略
S408、该第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作

图 6

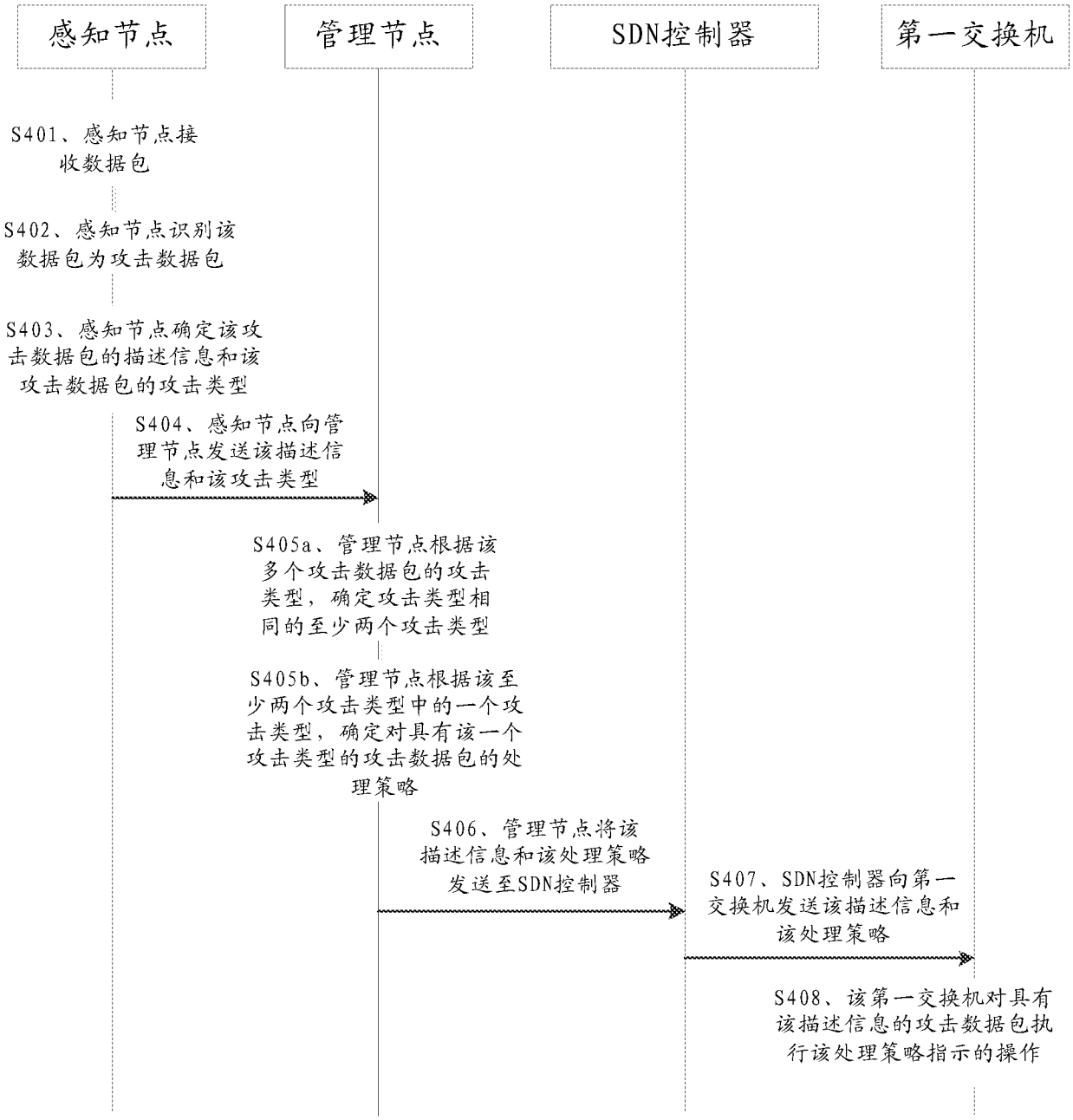
感知节点
管理节点
SDN控制器
第一交换机
S401、感知节点接收数据包
S402、感知节点识别该数据包为攻击数据包
S403、感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型
S404、感知节点向管理节点发送该描述信息和该攻击类型
S405a、管理节点根据该多个攻击数据包的攻击类型，确定攻击类型相同的至少两个攻击类型
S405b、管理节点根据该至少两个攻击类型中的一个攻击类型，确定对具有该一个攻击类型的攻击数据包的处理策略
S406、管理节点将该描述信息和该处理策略发送至SDN控制器
S407、SDN控制器向第一交换机发送该描述信息和该处理策略
S408、该第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作

图 7

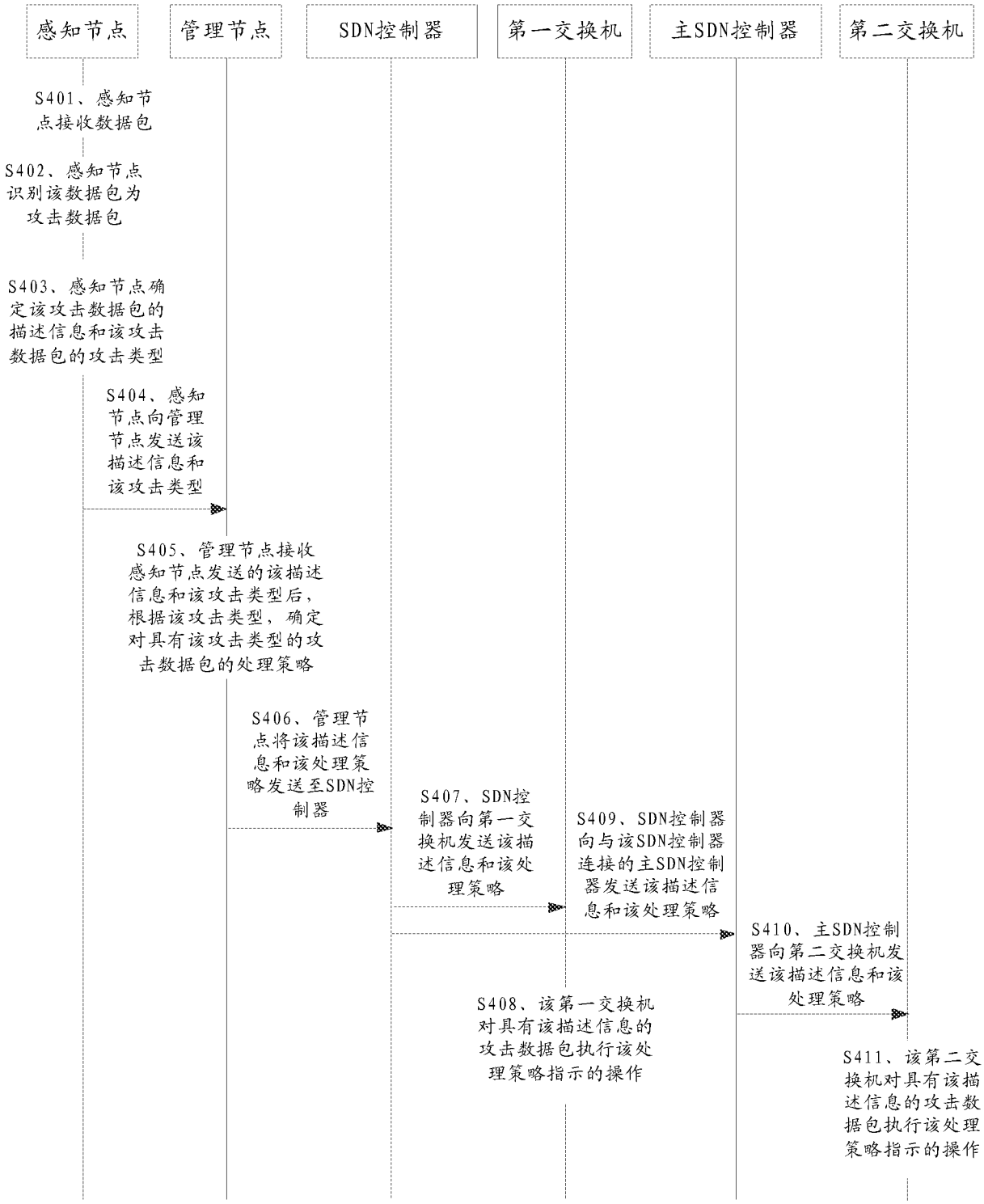
感知节点
管理节点
SDN控制器
第一交换机
主SDN控制器
第二交换机
S401、感知节点接收数据包
S402、感知节点识别该数据包为攻击数据包
S403、感知节点确定该攻击数据包的描述信息和该攻击数据包的攻击类型
S404、感知节点向管理节点发送该描述信息和该攻击类型
S405、管理节点接收感知节点发送的该描述信息和该攻击类型后，根据该攻击类型，确定对具有该攻击类型的攻击数据包的处理策略
S406、管理节点将该描述信息和该处理策略发送至SDN控制器
S407、SDN控制器向第一交换机发送该描述信息和该处理策略
S408、该第一交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作
S409、SDN控制器向与该SDN控制器连接的主SDN控制器发送该描述信息和该处理策略
S410、主SDN控制器向第二交换机发送该描述信息和该处理策略
S411、该第二交换机对具有该描述信息的攻击数据包执行该处理策略指示的操作

图 8

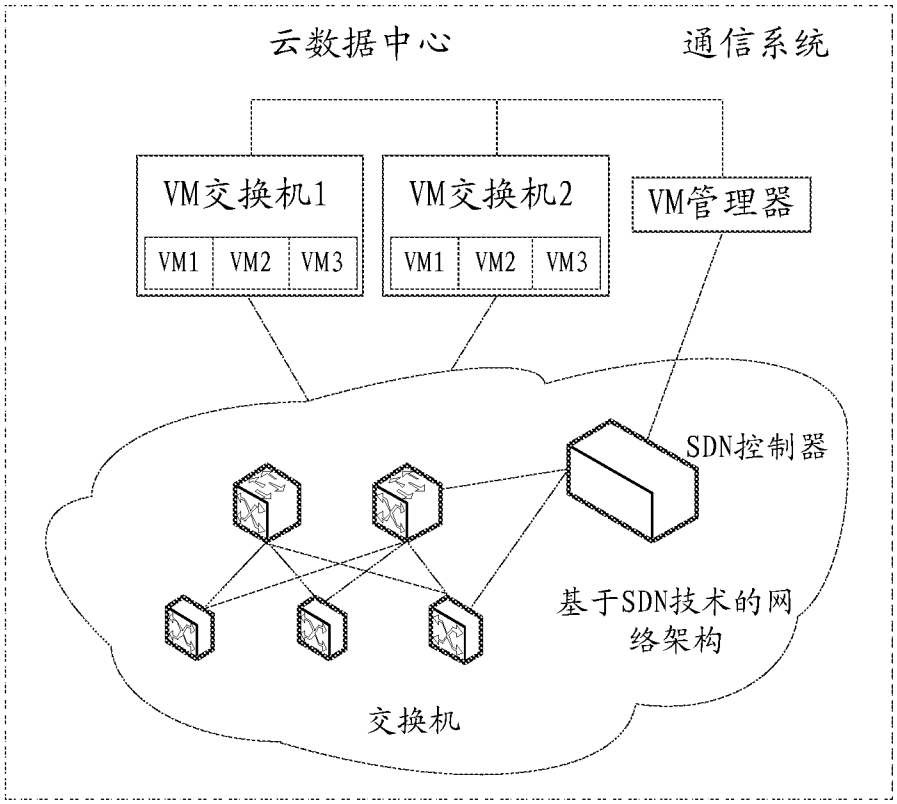
云数据中心
通信系统
VM交换机1
VM1
VM2
VM3
VM交换机2
VM1
VM2
VM3
VM管理器
SDN控制器
基于SDN技术的网络架构
交换机

图 9

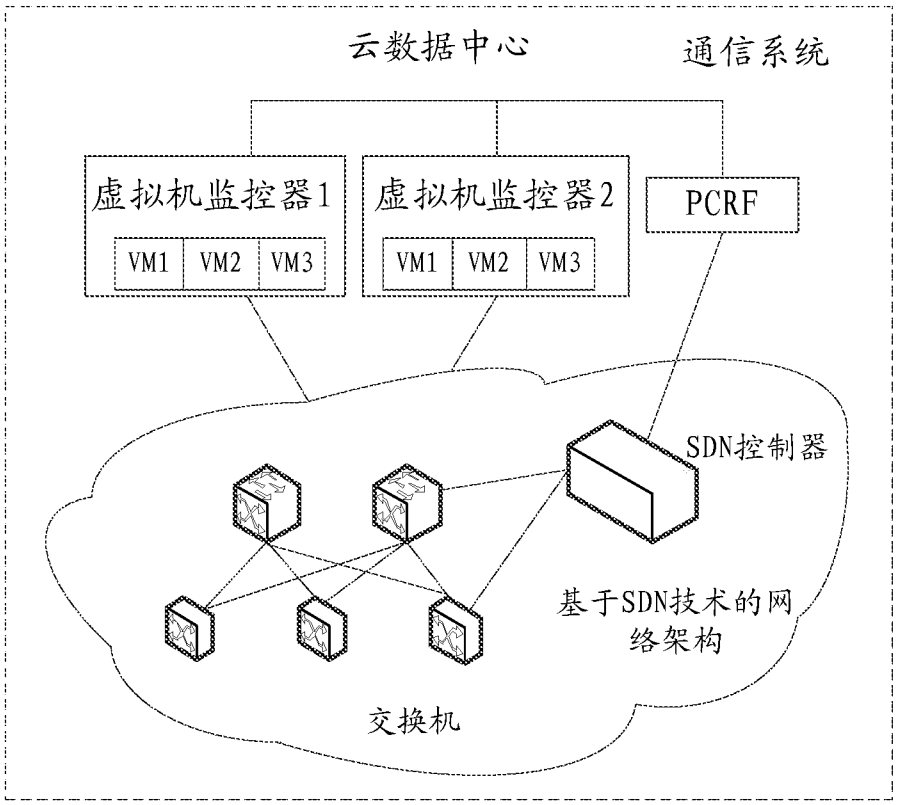
云数据中心
通信系统
虚拟机监控器1
VM1
VM2
VM3
虚拟机监控器2
VM1
VM2
VM3
PCRF
SDN控制器
基于SDN技术的网络架构
交换机

图 10

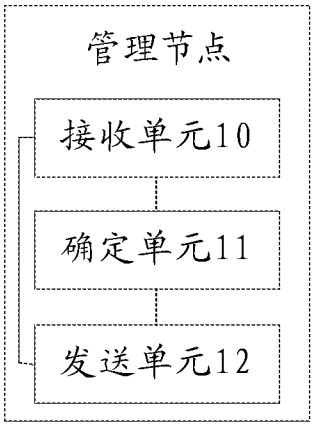
管理节点
接收单元10
确定单元11
发送单元12

图 11

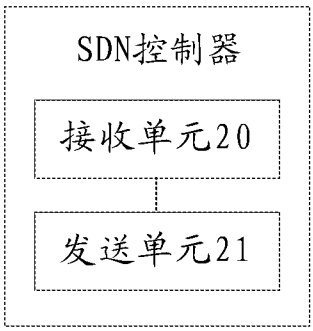
SDN控制器
接收单元20
发送单元21

图 12

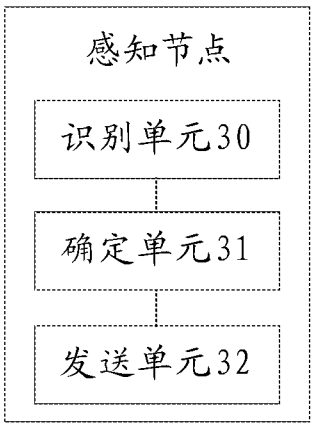
感知节点
识别单元30
确定单元31
发送单元32

图 13

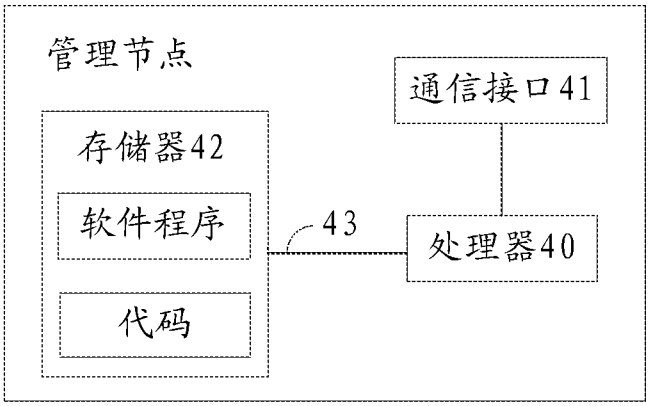
管理节点
通信接口41
存储器42
软件程序
代码
43
处理器40

图 14

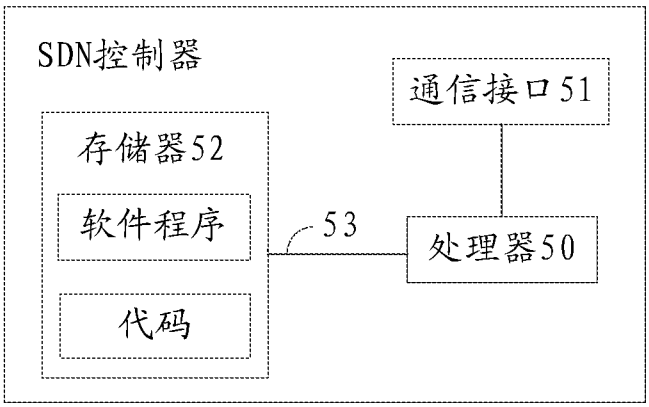
SDN控制器
通信接口51
存储器52
软件程序
代码
53
处理器50

图 15

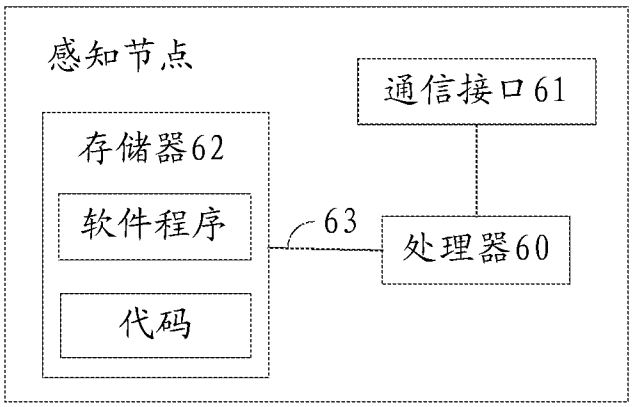
感知节点
通信接口61
存储器62
软件程序
代码
63
处理器60

图 16

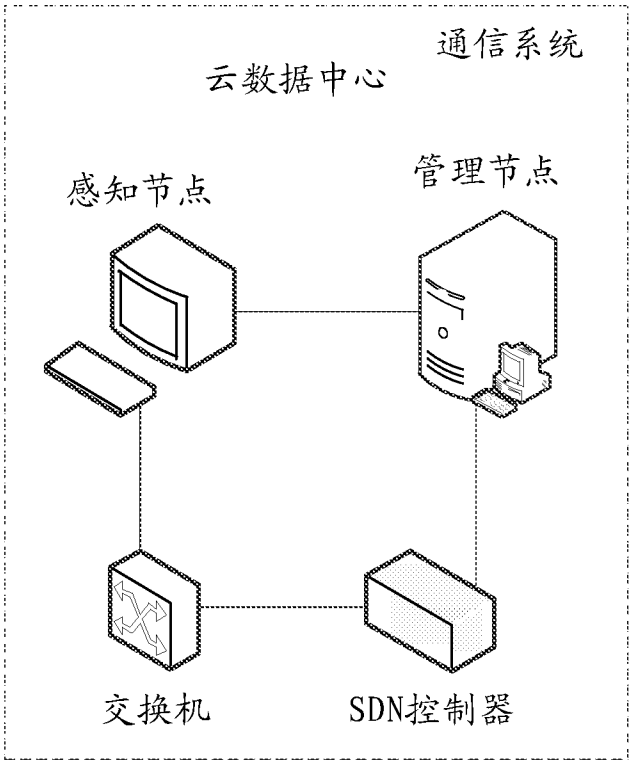
通信系统
云数据中心
感知节点
管理节点
交换机
SDN控制器

图 17

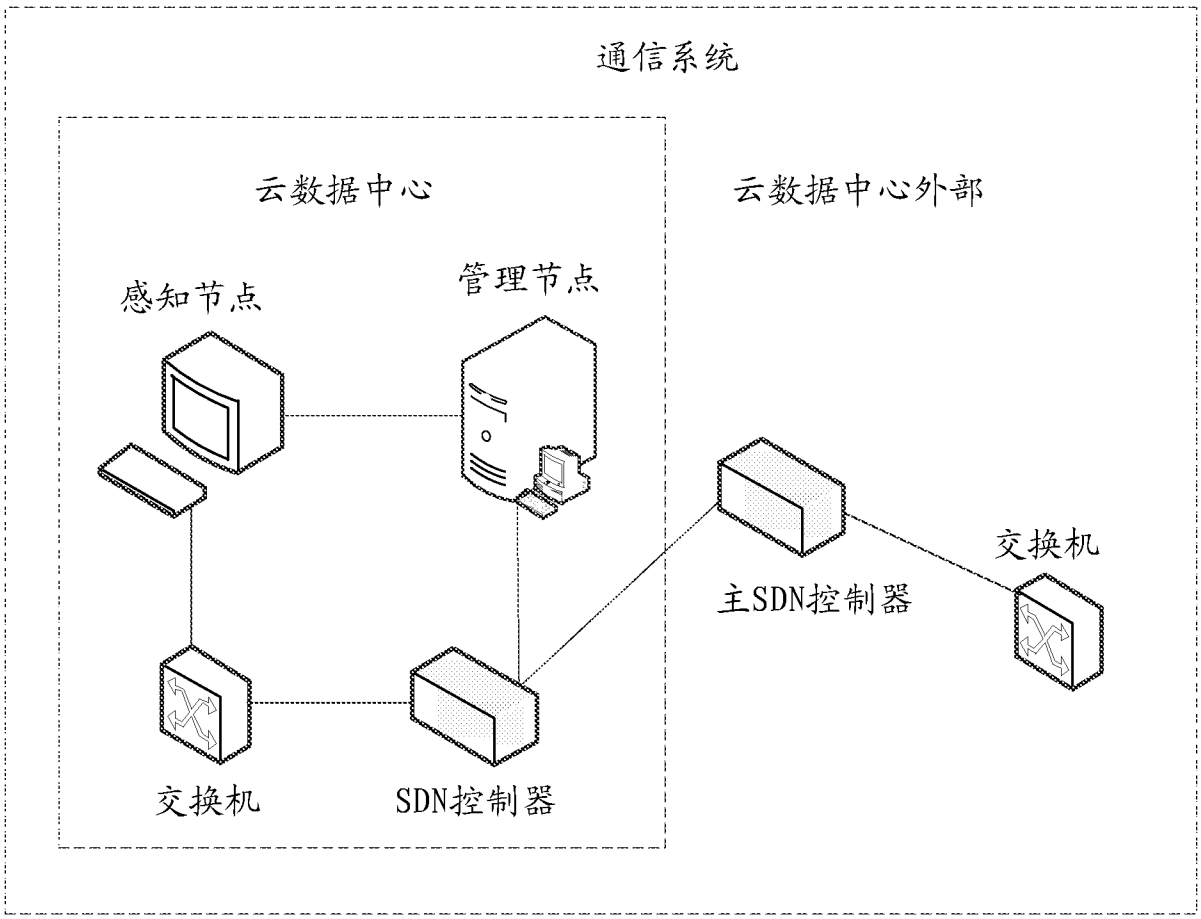
通信系统
云数据中心
云数据中心外部
感知节点
管理节点
交换机
SDN控制器
主SDN控制器
交换机

图 18

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/096509

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)

CNKI, CNPAT, WPI, EPODOC, IEEE, GOOGLE: attack, packet, processing, strategy, method, management node, perception node, description, information, attack, type, switch, SDN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104580168 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 April 2015 (29.04.2015) claims	1-25
A	CN 103051605 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER et al.) 17 April 2013 (17.04.2013) description, paragraphs [0098] to [0125]	1-25
A	CN 1588880 A (HUAZHONG UNIVERSITY OF SCIENCE & TECHNOLOGY) 02 March 2005 (02.03.2005) the whole document	1-25
A	US 2006075093 A1 (ENTERASYS NETWORKS, INC.) 06 April 2006 (06.04.2006) the whole document	1-25

☐ 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
25 February 2016	02 March 2016

Name and mailing address of the ISA
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
XING, Yunfeng
Telephone No. (86-10) 62413374

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/096509

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104580168 A	29 April 2015	None	
CN 103051605 A	17 April 2013	None	
CN 1588880 A	02 March 2005	None	
US 2006075093 A1	06 April 2006	EP 1817684 A2	15 August 2007
		WO 2006041818 A2	20 April 2006

国际检索报告

国际申请号 PCT/CN2015/096509

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）)

CNKI;CNPAT;WPI;EPODOC;IEEE;GOOGLE:攻击，数据包，处理，策略，方法，管理节点，感知节点，描述信息，攻击类型，类型，交换机，软件定义网络，attack, packet, strategy, method, management node, description, type, switch, SDN

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
PX	CN 104580168 A (华为技术有限公司) 2015年 4月 29日 (2015-04-29) 权利要求书	1-25
A	CN 103051605 A (国家计算机网络与信息安全管理中心等) 2013年 4月 17日 (2013-04-17) 说明书第[0098]-[0125]段	1-25
A	CN 1588880 A (华中科技大学) 2005年 3月 2日 (2005-03-02) 全文	1-25
A	US 2006075093 A1 (ENTERASYS NETWORKS, INC.) 2006年 4月 6日 (2006-04-06) 全文	1-25

☐ 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
2016年 2月 25日	2016年 3月 2日

ISA/CN的名称和邮寄地址	受权官员
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	邢雲峰
传真号 (86-10)62019451	电话号码 (86-10)62413374

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/096509

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	104580168	A	2015年 4月 29日	无			
CN	103051605	A	2013年 4月 17日	无			
CN	1588880	A	2005年 3月 2日	无			
US	2006075093	A1	2006年 4月 6日	EP	1817684	A2	2007年 8月 15日
				WO	2006041818	A2	2006年 4月 20日