(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
2014 年 11 月 6 日 (06.11.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/177097 A1

(51) 国际专利分类号:
H04L 12/741 (2013.01)

(21) 国际申请号: PCT/CN2014/078406

(22) 国际申请日: 2014 年 5 月 26 日 (26.05.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310359664.2 2013 年 8 月 16 日 (16.08.2013) CN

(71) 申请人: **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: **梁乾灯 (LIANG, Qiandeng)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **范亮 (FAN, Liang)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **尤建洁 (YOU, Jianjie)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **韩杰 (HAN, Jie)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: **北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (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, LT, 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, 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,

[见续页]

(54) **Title**: FLOW TABLE ENTRY GENERATION METHOD AND CORRESPONDING DEVICE

(54) **发明名称** : 一种流表条目生成方法及相应设备

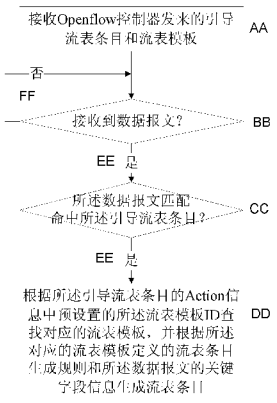

图 3 / Fig.3

AA Receiving a guide flow table entry and a flow table template transmitted by an openflow controller
BB Is a data packet received?
CC Does the data packet match the guide flow table entry?
DD Searching for a corresponding flow table template according to the preset flow table template ID in the action information of the guide flow table entry, and generating a flow table entry according to a flow table entry generation rule defined by the corresponding flow table template and the key field information of the data packet
EE Yes
FF No

(57) **Abstract**: A flow table entry generation method and corresponding device, the method being used for an openflow forwarding device and comprising: receiving a guide flow table entry and a flow table template transmitted by an openflow controller, the action information of the guide flow table entry comprising a preset flow table template ID; after receiving a data packet, if the data packet matches the guide flow table entry, then searching for a corresponding flow table template according to the preset flow table template ID in the action information of the guide flow table entry, and generating a flow table entry according to a flow table entry generation rule defined by the corresponding flow table template and the key field information of the data packet. The technical solution enhances the security of an openflow protocol, and expands the application scenario and usability of an openflow/SDN network.

(57) **摘要**:

[见续页]

WO 2014/177097 A1

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))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

一种流表条目生成方法及相应设备，所述方法应用于开放流（Openflow）转发设备，包括：接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID；在接收到数据报文后，如果该数据报文匹配命中所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。上述技术方案增强了 Openflow 协议的安全性，同时扩展了 Openflow/SDN 网络的应用场景和实用性。

一种流表条目生成方法及相应设备

技术领域

本发明涉及流表条目生成技术领域，具体而言，涉及一种流表条目生成方法及相应设备。

背景技术

基于传输控制协议(TCP, Transmission Control Protocol)/IP 的当今 Internet（互联网）经过四十多年的发展已取得巨大的成功，与人们息息相关，已成为工作、学习和生活必不可少的基础设施之一。TCP/IP 式的互联网，因其设计之初的“网络/网络设备进行简单处理，复杂的处理交给主机端/侧”的分工与组织原则，形成了当今的互联网体系结构现状：主机侧的应用层协议可以很方便、灵活地进行修改和部署，应用层软件因此得到了突飞猛进地发展，应用层的功能因此得到了极大的丰富；与之形成鲜明对比的是网络层，网络层协议的设计虽然简单，但是可扩展性不强并且不易修改，造成：一方面，互联网网络层面暴露出的许多致命的漏洞长期难以得到修补和改进，如网络管理难以部署、网络安全问题日益严重、尽力而为的转发策略不能满足用户的服务质量要求、组播难以部署和应用等；另一方面，新协议、新应用由于对网络层提出变革要求而难以得到实现，如从 IPv4 向 IPv6 过渡困难、接入设备日益呈现泛在移动性与异质性对网络可靠性和区分服务能力提出挑战、大规模网络情况下路由面临可扩展性问题、云计算和内容分发等应用对网络转发效率提出新需求、TCP/IP 之父 Vinton G. Cerf 也指出互联网应该在网络安全和网络可靠性方面做得更好（“安全性与可靠性是迈向未来互联网最基本的两个门槛，否则这个架构将无法存活”）等。因此互联网目前形成了一种“应用层灵活多变、百花齐放，网络层僵硬难变、漏洞百出”的尴尬局面。互联网要解决当前所面临的问题和尴尬局面，需要从网络体系结构、控制等层面深层次的进行探讨、研究和改革，才能全面迎接二十一世纪新的机遇和巨大的挑战。

对于如何解决当前互联网所面临的问题与挑战，国内外研究机构从互联

网体系结构层面进行了大量积极的探索和研究。主要经历了两个阶段的发展，对互联网的改进可分为两类方式：演进式改进和革命性改进。

多年来，针对传统 IP 网络在服务质量保证、移动支持、高效可靠和安全保证等方面暴露出的许多问题，研究领域普遍采用设计针对性的修补方式来分别解决这些问题，一旦发现运行的网络的弱点或错误就立即改进，例如在传统互联网体系结构中添加新的协议和功能组件等。这种“修补->发现问题->再修改”的改进方式是以相关互联网 TCP/IP 体系结构为基础，对相关网络进行逐步演进和发展以添加新的功能和特性来解决目前面临的问题的方式，是一种 Evolution（演进式）的改进方式。这种改进方式的优势在于易于部署和实施，有利于保护相关互联网建设中的已有投入。但是它的缺陷在于：（1）某次修补只是在小范围内解决局部的问题；（2）相关的改进可能引入短期收益，而从长期看则具有破坏性如 NAT（Network Address Translation，网络地址转换），或者局部收益对整体有破坏性；（3）某次修补可能不容易“兼容”未来的继续修改；（4）经过多次修补，互联网变得越来越“厚重”、复杂、不灵活，超出了当初设计 Internet 的简单的体系结构的承受能力；（5）传统互联网体系结构中的一些固有问题难以得到根本性的解决。从 2005 年开始，研究领域逐渐形成了另一种观点，只有重新设计网络体系结构才能从根本上解决 IP 网络所面临的问题，而目前正是互联网体系结构“Clean-Slate”（从零开始）进行全面彻底变革的好时机，完全舍弃相关的互联网体系结构，设计一种全新的、融合多种设计目标的新一代互联网体系结构。这种方案旨在从根本上解决相关互联网体系结构存在的各种问题，是一种 Revolution（革命性）的改进方案。这种方案的优势在于：（1）可以摆脱 TPC/IP 体系结构的束缚，跳出其约束与框架，以解决互联网多年来因体系结构造成的遗留难题；（2）可以对互联网进行重新、全面的设计，统筹解决互联网的诸多问题，统筹安排互联网的诸多新需求的实现。但是这种方案的缺陷在于：（1）由于全新网络可能不能兼容相关互联网，需要完全替换原有网络的基础设施，因此存在着网络部署和平滑过渡的问题；（2）如何建立新的体系结构以及建立了新的体系结构是否能解决当前和未来网络所面临的问题也存在很大风险；（3）需要重新构建适合全新体系结构的试验网络，演进代价高。

为了解决目前互联网存在的问题，实现对新网络协议快速、灵活的部署，开放可编程网络被提出。开放可编程网络是指允许网络研究者而不只是设备厂商，在网络设备上进行编程和管理其网络体系结构或网络协议。开放可编程式思路是革命性改进方案的代表性成果之一，基本可以概括为：将原来多张功能网络并存、整体的、复杂的 MAN（Metropolitan Area Network，城域网）/WAN（Wide Area Network，广域网）网络或网络设备按功能进行划分，例如划分成数据转发部分和逻辑控制部分、或者系统核心部分和用户功能部分等。各部分之间的接口是开放的和标准的。基于这个开放和标准化的接口，每个部分都可以自我演进和改进而不需通知或影响其他部分，这样整个网络或网络设备也将实现独立、平滑演进和改进。开放可编程式思路面临的挑战在于：（1）网络分层需要具备一定的合理性、科学性和可扩展性；（2）定义科学、可扩展的分层间的接口；（3）控制层面如果采取集中管控方式，则需要考虑域间连接、可扩展性（如扩展到全球）等。

在开放可编程网络的研究方面，Berkeley（伯克利）大学的 Scott Shenker 等人提出的软件定义网络（SDN，Software Defined Networking）技术、Stanford（斯坦福）大学的开放流协议（OpenFlow）等技术是网络开放性研究的代表性成果。图 1 是 SDN/OpenFlow 技术的层次模型示意图，包含：基础设施层、网络控制层和应用层三个层次。SDN/OpenFlow 网络中的基础设施层由 1 个以上的转发设备构成，转发设备相对当前网络中的路由器、交换机及各类网关来说结构更加简单、没有复杂的控制面（Control Plane），主要的工作是进行数据流的转发。网络控制层中的主要设备是网络操作系统（或称 SDN/OpenFlow 控制器），网络操作系统通过标准化的接口同时对多台转发设备进行控制，替代了原本独立于各台转发设备中的控制面、甚至当前的网络管理系统，可以实现网络管理和端到端的数据流规则下发（即向转发路径上的多台转发设备下发流规则），同时网络操作系统通过应用程序编程接口（API，Application Programming Interface）与应用层进行交互。应用层由不同应用构成，应用通过 API 接口能够直接调用网络控制层的网络管理和控制功能。

与其它革命性的改进技术的部署一样，运营商网络在向 SDN/OpenFlow

架构演进的过程中势必遇到各方面的问题，如安全性就是其中最重要的问题之一。此外，对各种现网技术的适配性也是衡量一项新技术是否符合网络发展趋势的重要指标。如图 2 所示，在实际的 SDN/OpenFlow 网络中，网络控制层设备（如 SDN/OpenFlow 控制器）和基础设施层设备（即转发设备）之间通过基于 IP 地址的通信协议消息进行交互（如 OpenFlow 协议），网络终端之间、网络终端和应用服务器之间、应用服务器和应用服务器之间的数据流量在转发设备间通过流表进行转发，每条流的流表均由 SDN/OpenFlow 控制器生成并下发给转发设备，转发设备对没有命中本转发设备当前存储的流表的数据报文统一上送给 SDN/OpenFlow 控制器进行流表的查询和生成，转发设备需要等待SDN/OpenFlow控制器下发新的流表才可以转发该数据报文。这种数据报文的转发模式带来了以下几个问题:

一、安全性问题：对于转发面攻击源（如恶意终端）发出的攻击 SDN/OpenFlow 控制器或攻击应用服务器的报文，转发设备在收到流表前会将所有攻击报文发送给 SDN/OpenFlow 控制器，如果攻击报文的发送频率较大，可能导致转发设备和 SDN/OpenFlow 控制器之间的路径拥塞，影响正常的转发设备和控制设备间的其它控制消息（如流表查询、配置下发等）的传递效率，且当前的流表下发机制无法实现在攻击报文抵达应用服务器前对应用服务器进行保护，即在应用服务器发现攻击并通过应用层与 SDN/OpenFlow 控制器之间的接口发送安全策略、SDN/OpenFlow 控制器再形成新的流表下发给转发设备之前，攻击源针对应用服务器的所有攻击报文都将被发送给应用服务器;

二、适配性问题：对于 NAT 等业务场景，当前的流量上送、流表条目生成、流表条目下发模式的控制流程较长，对转发时延和效率影响较大。例如在 NAT 场景下，转发设备收到用户私网终端发出的数据报文后，对于没有命中本转发设备存储的流表条目的报文，需要首先发送给 SDN/OpenFlow 控制器，由 SDN/OpenFlow 控制器完成公网地址和端口号的指定、地址匹配关系及对应流表条目的生成以及流表条目的下发，在当前每个用户同时存在大量会话频繁生成和释放的场景（如 P2P（Peer to Peer，对等网络）应用）而言转发效率较低，在未来 IPv4/IPv6 长期共存、私网 IPv4 地址长期大量存在的网

络中，这种转发模式需要进一步优化。

发明内容

本发明实施例要解决的技术问题是提供一种流表条目生成方法及相应设备，以在提升 SDN/Openflow 网络安全性的前提下提升报文转发模式的时效性和适配性。

为解决上述问题，采用如下技术方案:

一种流表条目生成方法，应用于开放流（Openflow）转发设备，包括:

接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID;

在接收到数据报文后，如果所述数据报文匹配命中所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找与所述流表模板 ID 对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。

可选地，还包括:

将生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

可选地，所述将生成的所述流表条目通过所述流条目添加消息发送给所述 Openflow 控制器的步骤包括:

所述 Openflow 转发设备通过所述流条目添加消息实时或批量发送所述流表条目的信息。

可选地，还包括:

按照生成的所述流表条目对所述数据报文进行处理转发。

可选地，所述引导流表条目的匹配规则包括: 目的地址为受保护设备的 IP 地址;

所述数据报文匹配命中所述引导流表条目的步骤包括:

所述数据报文的目的地址为所述受保护设备的 IP 地址。

可选地，所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速；

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目的步骤包括：

生成所述流表条目；其中，所述流表条目的匹配规则包括：源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址，Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表条目限制发送速率。

可选地，所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段；

所述数据报文匹配命中所述引导流表条目的步骤包括：

所述数据报文的源地址为所述私网地址网段中的一个。

可选地，所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则；

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目的步骤包括：

生成所述流表条目；其中，所述流表条目的匹配规则包括：所述数据报文的私网地址，Actions 包括将所述私网地址转换为分配的公网地址，并通过对应出接口发送转换后的报文。

可选地，还包括：

接收所述 Openflow 控制器发来的第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

可选地，还包括：

根据生成的所述流表条目，结合所述第二流表模板生成所述第二流表条目；

其中，所述第二流表条目的匹配规则包括：所述分配的公网地址，Action

信息为将所述公网地址转换为对应的私网地址，并通过对应出接口发送转换后的报文。

可选地，所述私网地址包括：私网 IP 地址；

所述公网地址包括：公网 IP 地址，或者，公网 IP 地址及端口信息。

可选地，还包括：

将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

一种流表条目生成方法，应用于开放流（Openflow）控制器，包括：

向 Openflow 转发设备发送引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID。

可选地，所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

可选地，还包括：

在接收到所述 Openflow 转发设备通过流条目添加消息发来的流表条目后，

所述 Openflow 控制器不回复所述流条目添加消息，表示接受所述 Openflow 转发设备根据所述流表模板生成的所述本地流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据所述流表模板生成的所述流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送更高优先级的流表条目。

可选地，所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的

地址转换规则。

可选地，所述私网地址网段包括：私网 IP 地址。

可选地，还包括：

向所述 Openflow 转发设备发送第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

一种开放流（Openflow）转发设备，包括接收模块和生成模块，其中：

所述接收模块设置成：接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID； 还用于接收数据报文；

所述生成模块设置成：在所述接收模块接收到所述数据报文后，如果所述数据报文匹配命中所述接收模块接收到的所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找与所述流表模板 ID 对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。

可选地，还包括发送模块，其中：

所述发送模块设置成：将所述生成模块生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

可选地，所述发送模块还设置成：按照所述生成模块生成的所述流表条目对所述数据报文进行处理转发。

可选地，所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；

所述生成模块设置成按照如下方式判断所述数据报文匹配命中所述引导流表条目：

所述数据报文的目的地址为所述受保护设备的 IP 地址。

可选地，所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所

述受保护设备发送的报文进行限速;

所述生成模块设置成按照如下方式根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目:

生成所述流表条目;其中,所述流表条目的匹配规则包括:源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址,Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表条目限制发送速率。

可选地,所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段;

所述生成模块设置成按照如下方式判断所述数据报文匹配命中所述引导流表条目:

所述数据报文的源地址为所述私网地址网段中的一个。

可选地,所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则;

所述生成模块设置成按照如下方式根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目:

生成所述流表条目;其中,所述流表条目的匹配规则包括:所述数据报文的私网地址,Actions 包括将所述私网地址转换为分配的公网地址,并通过对应出接口发送转换后的报文。

可选地,所述接收模块还设置成:接收所述 Openflow 控制器发来的第二流表模板;

其中,所述第二流表模板与所述流表模板级联,所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

可选地,所述生成模块还设置成:根据生成的所述流表条目,结合所述第二流表模板生成所述第二流表条目;

其中,所述第二流表条目的匹配规则包括:所述分配的公网地址,Action 信息为将所述公网地址转换为对应的私网地址,并通过对应出接口发送转换后的报文。

可选地，所述私网地址包括：私网 IP 地址；

所述公网地址包括：公网 IP 地址，或者，公网 IP 地址及端口信息。

可选地，所述发送模块还设置成：将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

一种开放流（Openflow）控制器，包括存储模块和发送模块，其中：

所述存储模块设置成：保存预配置的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID；

所述发送模块设置成：向 Openflow 转发设备发送所述存储模块保存的所述引导流表条目和流表模板。

可选地，所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

可选地，还包括接收模块，其中：

所述接收模块设置成：接收所述 Openflow 转发设备通过流条目添加消息发来的流表条目；

所述发送模块还设置成：在所述接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据所述流表模板生成的所述流表条目；或者，在所述接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送更高优先级的流表条目。

可选地，所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则。

可选地，所述私网地址网段包括：私网 IP 地址。

可选地，所述发送模块还设置成：向所述 Openflow 转发设备发送第二流

表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

上述技术方案实现了在 Openflow 转发设备上根据流表条目模板生成流表条目的功能，增强了 Openflow 协议的安全性，同时扩展了 Openflow/SDN 网络的应用场景和实用性。

附图概述

图 1 是相关技术中 SDN/OpenFlow 网络的拓扑示意图；

图 2 是相关技术中的一种网络拓扑示意图；

图 3 是本发明实施例中流表条目生成方法流程示意图；

图 4 是本发明的第一实施例的拓扑示意图；

图 5 是本发明的第一实施例的流程图；

图 6 是本发明的第二实施例的拓扑示意图；

图 7 是本发明的第二实施例的流程图；

图 8 是本发明的第三实施例的拓扑示意图；

图 9 是本发明的第三实施例的流程图；

图 10 为本发明实施例的 Openflow 转发设备结构示意图；

图 11 为本发明实施例的 Openflow 控制器结构示意图。

本发明的较佳实施方式

下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

在本实施例中，一种流表条目生成方法，应用于 Openflow 转发设备，如图 3 所示，包括:

接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的 Action 信息包括预设置的所述流表模板 ID;

在接收到数据报文后，如果所述数据报文匹配命中所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。

可选地，所述方法还包括:

将生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

可选地，所述将生成的所述流表条目通过所述流条目添加消息发送给所述 Openflow 控制器的步骤包括:

所述 Openflow 转发设备通过所述流条目添加消息实时或批量发送所述流表条目的信息。

可选地，所述方法还包括:

按照生成的所述流表条目对所述数据报文进行处理转发。

可选地，

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址;

所述数据报文匹配命中所述引导流表条目，具体包括:

所述数据报文的目的地址为所述受保护设备的 IP 地址。

可选地，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速;

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目，具体包括:

生成所述流表条目；其中，所述流表条目的匹配规则包括：源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址，Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表

条目限制发送速率。

可选地，

所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段；

所述数据报文匹配命中所述引导流表条目，具体包括：

所述数据报文的源地址为所述私网地址网段中的一个。

可选地，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则；

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目，具体包括：

生成所述流表条目；其中，所述流表条目的匹配规则包括：所述数据报文的私网地址，Actions 包括将所述私网地址转换为分配的公网地址，并通过对应出接口发送转换后的报文。

可选地，所述方法还包括：

接收所述 Openflow 控制器发来的第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

可选地，所述方法还包括：

根据生成的所述流表条目，结合所述第二流表模板生成所述第二流表条目；

其中，所述第二流表条目的匹配规则包括：所述分配的公网地址，Action 信息为将所述公网地址转换为对应的私网地址，并通过对应出接口发送转换后的报文。

可选地，

所述私网地址包括：私网 IP 地址；

所述公网地址包括：公网 IP 地址，或者，公网 IP 地址及端口信息。

可选地，所述方法还包括：

将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

此外，本发明实施例还提供了一种流表条目生成方法，应用于开放流（Openflow）控制器，包括:

向 Openflow 转发设备发送引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID。

可选地，

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

可选地，所述方法还包括:

在接收到所述 Openflow 转发设备通过流条目添加消息发来的流表条目后，

所述 Openflow 控制器不回复所述流条目添加消息，表示接受所述 Openflow 转发设备根据所述流表模板生成的所述本地流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据所述流表模板生成的所述流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送更高优先级的流表条目。

可选地，

所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则。

可选地，

所述私网地址网段包括：私网 IP 地址。

可选地，所述方法还包括：

向所述 Openflow 转发设备发送第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

本实施例所述方法在二层网络设备不支持 IPv6 安全 RA（Random Access，随机接入）特性的情况下，可实现对 IPv6 主机恶意发送 RA 消息造成网关欺骗行为的防范。

下面分别介绍本发明实施例在不同应用场景下的三个实施例。

实施例一

以 Openflow 控制器的攻击防范、Openflow 转发设备的硬件架构以 ASIC 转发平面和 CPU 控制平面的组合为例，组网示意图参见图 4，详细流程如图 5 所示，包括：

步骤 101：Openflow 控制器配置本地安全策略，防范 TCP 半连接攻击；

步骤 102：Openflow 控制器根据本地安全策略向各 Openflow 转发设备发送引导流表条目 X1 和流表模板 Y1。

可选地，引导流表条目 X1 的匹配规则为目的地址为 Openflow 控制器的 IP 地址、报文类型为 TCP 或 TCP SYN（synchronize，同步），引导流表条目的 Action（动作）为查询流表模板 Y1，流表模板 Y1 定义的流表条目生成规则为限制任一源 IP 地址向 Openflow 控制器发送的 TCP 或 TCP SYN 报文的速率。

可选地，所述 Openflow 转发设备收到所述引导流表条目 X1 和流表模板 Y1 后，将引导流表条目 X1 下发到 ASIC 转发平面，将流表模板 Y1 保存在 CPU 控制平面。

步骤 103：攻击源 A1 以一定速率向 Openflow 控制器发送 TCP SYN 报文，形成 TCP 半连接类型的网络攻击；

步骤 104：Openflow 转发设备接收到攻击源 A1 发送的第一个 TCP SYN 报文后，匹配流表命中引导流表条目 X1 后，根据 X1 的 Action 动作查询流表模板 Y1，根据 Y1 定义的流表条目生成规则和所述攻击报文的源 IP 地址生成流表条目 Z1；

可选地，所述 Openflow 转发设备的 ASIC 转发平面命中所述引导流表条目 X1 后，向 CPU 控制平面上送该报文和该流表模板 Y1 的 ID，CPU 控制平面根据上述信息查询流表模板、根据流表模板定义的规则生成流表条目 Z1 并下发给 ASIC 转发平面。

可选地，流表条目 Z1 的匹配规则包括：源 IP 地址为上述 TCP SYN 报文的源 IP 地址、目的 IP 地址为 Openflow 控制器的 IP 地址、报文类型为 TCP 或 TCP SYN，Action 动作为向 Openflow 控制器发送匹配该匹配规则的报文并限制报文的发送速率。

步骤 105：Openflow 转发设备根据流表条目 Z1 将所述攻击源 A1 发出的 TCP SYN 报文发送给 Openflow 控制器并限制该报文的发送速率，并向 Openflow 控制器发送流条目添加消息，将 Z1 定义的流表条目生成规则通知给 Openflow 控制器。

可选地，若攻击源的发送速率高于流表条目 Z1 的限制速率，Openflow 转发设备对超出速率的报文进行缓存或丢弃；

可选地，Openflow 控制器在收到所述 TCP SYN 报文后，若判断其为攻击报文，则向 Openflow 转发设备发送更高优先级的流表条目，该流表条目的匹配规则包括：源 IP 地址为上述 TCP SYN 报文的源 IP 地址、目的 IP 地址为 Openflow 控制器的 IP 地址、报文类型为 TCP，Action 动作为丢弃匹配该匹配规则的报文；Openflow 转发设备在收到该流表条目，对后续收到的报文会优先采用该更高优先级的流表条目进行匹配。

此外，Openflow 控制器在收到上述流条目添加消息后，将其中携带的 Z1 定义的流表条目生成规则进行保存，并可能下发给其他 Openflow 转发设备。

可选地，流表模板的格式根据 Openflow 协议的版本不同略有区别，参考的实例格式如表 1 所示。

表 1 流表模板基本格式

Flow Template Identifier	Flow Template Description	Counters

其中，Flow Template Identifier 表示流表模板的 ID，其取值唯一；Flow Template Description 是流表模板定义的流表条目生成规则；Counters 为计数器，每根据该流表模板生成一个流表条目，可将该计数器的当前计数值加 1。

实施例二

应用服务器的攻击防范，Openflow 转发设备的硬件架构以多核 CPU 架构（控制核和转发核并存）为例。组网示意图参见图 6，详细流程如图 7 所示，包括:

步骤 201: 应用服务器通过 Openflow 控制器的 NBI(North Bound Interface，北向接口）向 Openflow 控制器发送安全需求；其中，该安全需求中可以但不限于包括以下几类信息：一类行为特征的流标识，例如 TCP 建链报文，TTL（Time To Live，生存时间）为 0 的报文；针对这类流需要设置的特性，例如基础限速值等;

步骤 202：Openflow 控制器根据应用服务器发来的安全需求向各 Openflow 转发设备发送引导流表条目 X2 和流表模板 Y2;

可选地，引导流表条目 X2 的匹配规则为目的地址为应用服务器地址、报文类型为 TCP 或 TCP SYN，引导流表条目的 Action 动作为查询流表模板，流表模板 Y2 定义的流表条目生成规则为限制任一源 IP 地址向应用服务器发送的 TCP 或 TCP SYN 报文的速率。

可选地，所述 Openflow 转发设备收到所述引导流表条目 X2 和流表模板 Y2 后，将所述引导流表条目 X2 下发到转发核，将所述流表模板 Y2 保存在控制核。

步骤 203：终端用户 A2 以一定速率向应用服务器发送 TCP 报文;

步骤 204：Openflow 转发设备在接收到 A2 发送的第一个 TCP 报文后，匹配流表命中引导流表条目 X2 后，根据 X2 的 Action 动作查询流表模板 Y2，

根据 Y2 定义的流表条目生成规则和所述 TCP 报文的源 IP 地址生成流表条目 Z2;

可选地，所述 Openflow 转发设备的转发核命中所述引导流表条目 X2 后，向所述控制核发送查询消息并携带所述报文和所述流表模板 Y2 的 ID，所述控制核根据上述信息查询所述流表模板 Y2、据此生成所述流表条目 Z2 并下发给所述转发核。

可选地，所述流表条目 Z2 的匹配规则包括：源 IP 地址为上述 TCP 报文的源 IP 地址、目的 IP 地址为应用服务器的 IP 地址、报文类型为 TCP 或 TCP SYN，Action 动作为通过对应出接口发送匹配所述匹配规则的报文并限制报文的发送速率;

步骤 205：Openflow 转发设备根据流表条目 Z2 将所述终端用户发出的 TCP 报文通过对应的出接口发出并限制该报文的发送速率，并向所述 Openflow 控制器发送流条目添加消息，其中携带所述流表条目 Z2 的信息。

可选地，若攻击源的发送速率高于流表条目 Z2 的限制发送速率，Openflow 转发设备对超出速率的报文进行缓存/或丢弃。

可选地，所述终端用户与所述应用服务器间有多台 Openflow 转发设备，则其他 Openflow 转发设备对所述 TCP 报文的转发过程与步骤 201~205 相同或 Openflow 控制器在预知攻击源的情况下发送优先级更高的精确流表条目来限速。

步骤 206，应用服务器接收到所述终端用户发出的所述 TCP 报文后，判断该终端用户发送的是普通 TCP 报文或攻击报文和/或判断所述终端用户的身份信息。

可选地，在应用服务器和终端用户间进行鉴权的报文交互过程中，应用服务器发向终端用户发送的数据报文根据 Openflow 管道的流表信息转发，由 Openflow 控制器向沿途的 Openflow 转发设备发送对应的流表条目。

步骤 207，应用服务器根据所述 TCP 报文类型和/或对所述终端用户的鉴权结果向所述 Openflow 控制器发送授权信息。若应用服务器判断出所述 TCP 报文是普通 TCP 报文和/或判断出所述终端用户为合法用户，则要求所述

Openflow 控制器取消或放宽对所述 TCP 报文的速率限制; 若判断出所述 TCP 报文为 TCP 半连接攻击报文，则要求所述 Openflow 控制器下发流表条目要求 Openflow 转发设备惩罚性丢弃所述终端用户向所述应用服务器发送的 TCP 报文;

步骤 208，所述 Openflow 控制器根据所述应用服务器的授权信息向所述 Openflow 转发设备发送控制消息，要求所述 Openflow 转发设备删除上述生成的流表条目 Z2 或向所述 Openflow 转发设备发送更高优先级的流表条目;

步骤 209，所述 Openflow 转发设备根据所述 Openflow 控制器发送的控制消息进行流表条目操作和流量转发。

可选地，根据应用服务器的授权信息的不同，所述更高优先级的流表条目包括不限制所述 TCP 报文的发送速率和按需修改对所述 TCP 报文的发送速率的限速参数。

实施例三

网络地址转换会话表的快速生成，Openflow 转发设备的硬件架构以 OF（Openflow 的简称）转发面和 OF-Agent（代理）的组合为例。组网示意图参见图 8，详细流程如图 9 所示，包括:

步骤 301: Openflow 控制器根据本地配置规则或应用需求配置用户的 NAT 公网地址池、端口号段和匹配规则;

可选地，所述应用需求包括: 用户私网主机的公网地址转换需求和/或匹配规则需求，用户可通过特定的 NAT 应用向 Openflow 控制器的北向接口发送所述需求;

步骤 302: Openflow 控制器根据应用服务器的安全需求向对应的 Openflow 转发设备发送引导流表条目 X3 和流表模板 Y3-0 及 Y3-1（其中，Y3-0 和 Y3-1 级联）;

可选地，引导流表条目 X3 的匹配规则包括源地址为用户的私网地址或网段和用户侧接口信息，引导流表条目的 Action 动作为查询流表模板，流表模板 Y3-0 定义的流表条目生成规则包括: 用户的 NAT 公网地址池及为所述

用户的分配一个流表（表示用户发往网络侧地址的报文的地址转换规则），流表模板 Y3-1 定义的流表条目生成规则包括: 为所述用户分配另一个流表条目（表示由网络侧地址向用户发送报文的地址转换规则）；

可选地，所述 Openflow 转发设备收到所述引导流表条目 X3 和流表模板 Y3-0、Y3-1 后，将所述引导流表条目 X3 下发到 OF 转发面，将所述流表模板 Y3-0、Y3-1 保存在 OF-Agent;

步骤 303：私网主机 A3 以一定速率向网络侧设备发送 UDP（User Datagram Protocol，用户数据报协议）报文;

步骤 304：Openflow 转发设备接收到 A3 发送的第一个 UDP 报文后，匹配流表命中引导流表条目 X3 后，根据 X3 的 Action 动作查询流表模板 Y3-0，根据 Y3-0 定义的流表条目生成规则和所述报文信息为该私网主机 A3 分配一个公网 IP 地址、或一个公网 IP 地址及端口号，并生成流表条目 Z31（对应用户发往网络侧地址的报文地址转换规则）。因为 Y3-0 级联了流表模板 Y3-1，Y3-0，在生成 Z31 的同时填充了 Y3-0、Y3-1 约定格式的 metadata（元数据），生成 Z31 后，将报文继续交由 Y3-1 进行处理。根据 Y3-1 定义的流表条目生成规则和所述报文信息以及所述元数据生成 Z32（对应网络侧地址发送用户的报文地址转换规则）。

可选地，所述 Openflow 转发设备的 OF 转发面命中所述引导流表条目 X3 后，向所述 OF-Agent 发送查询消息并携带所述报文和所述流表模板 Y3-0 的 ID，所述 OF-Agent 根据上述信息查询所述流表模板和/或级联的流表模板、分配公网 IP 地址或分配公网 IP 地址及端口号，并生成所述流表条目 Z31 和 Z32 发送给所述 OF 转发面。

可选地，所述流表条目 Z31 的匹配规则包括：源 IP 地址、源端口号、报文类型，Action 动作为将源 IP 地址转换为分配的公网 IP 地址，还有可能将源端口转换为分配的端口号，并通过对应出接口发送转换后的报文。

可选地，所述流表条目 Z32 的匹配规则包括: 目的 IP 地址、目的端口号、报文类型，Action 动作为将目的 IP 地址转换为分配的公网 IP 地址，还有可能就将目的端口转换为分配的端口号，并通过对应出接口发送转换后的报文。

步骤 305：Openflow 转发设备根据流表条目 Z31 和 Z32 将 A3 和网络侧设备间的 TCP/UDP 报文执行 NAT 动作并通过对应的出接口转发，并通过流条目添加消息向所述 Openflow 控制设备发送 Z31 和 Z32 的信息。

可选地，所述流表条目 Z31 和 Z32 老化后，Openflow 转发设备回收对应的公网地址和/或端口号。

可选地，对于同时生成 2 个以上流表条目的情况，可选采用流表模板级联的方式实现，生成流表条目的同时生成级联流表模板间的 meta 数据，主要用于流表模板级联时的处理。

可选地，流表模板的描述方式根据描述手段的不同有区别，以 XML 为例，在本实施例的 NAT 应用场景为例，如果在 OpenFlow 协议中扩展实现，需要转换成对应的数据结构。

```
<flow-template-entry>
<id>1</id>
<table-id>5</table-id>
<cascade-template-id>2</cascade-template-id>
<out-meta>
 <field>
  <id>1</id>
  <size>4</size>
  <desc>public-ip</desc>
 </field>
 <field>
  <id>2</id>
  <size>4</size>
  <desc>"private-ip</desc>
 </field>
```

```
<out-meta>
<match>
 <nw-src>
  <type>packet</type>
  <value>nw-src</value>
  <mask>255.255.255.255</mask>
  <to-meta-field-id>2</to-meta-field-id>
 </nw-src>
</match>
<Instructions>
 <Write-Actions/>
 <Goto-Table>
  <type>fixed</type>
  <value>3</value>
 </Goto-Table>
</Instructions>
<actions>
 <set-nw-src>
  <type>allocated</type>
  <value>100.1.1.1~100.2.1.1,100.2.1.3</value>
  <to-meta-field-id>1</to-meta-field-id>
 </set-nw-src>
</actions>
</flow-template-entry>
```

```
<flow-template-entry>
<id>2</id>
<table-id>7</table-id>
<in-meta>
 <field>
  <id>1</id>
  <size>4</size>
  <desc>public-ip</desc>
 </field>
 <field>
  <id>2</id>
  <size>4</size>
  <desc>"private-ip</desc>
 </field>
<in-meta>
<match>
 <nw-dst>
  <type>metadata</type>
  <from-meta-field-id>1</from-meta-field-id>
 </nw-dst>
</match>
<Instructions>
 <Write-Actions/>
 <Goto-Table>
  <type>fixed</type>
```

```
<value>3</value>
</Goto-Table>
</Instructions>
<actions>
<set-nw-dst>
<type>metadata</type>
<from-meta-field-id>2</from-meta-field-id>
</set-nw-dst>
</actions>
</flow-template-entry>
```

在上述示例中，flow-template-entry 的 id 是流表模板的 ID 标识；table-id 表示该流表模板为该表 ID 标识的流表生成条目；cascade-template-id 表示该流表模板级联一个指定 ID 的流表模板；Out-meta/In-mate 表示级联的两个流表模板传递的中间数据的格式定义

本发明实施例的 Openflow 转发设备的硬件架构和各实施例的应用场景可以根据实际环境的需要自由组合，所述硬件架构保全但不限于上述实施例中的几种类型。

相应地，本发明实施例还公开了一种开放流（Openflow）转发设备，如图 10 所示，包括:

接收模块 1001 设置成：接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID； 还用于接收数据报文；

生成模块 1002 设置成：在所述接收模块接收到所述数据报文后，如果所述数据报文匹配命中所述接收模块接收到的所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的

关键字段信息生成流表条目。

可选地，所述设备还包括发送模块:

发送模块 1003 设置成: 将所述生成模块生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

可选地，所述设备还包括:

发送模块 1003 设置成: 按照所生成模块生成的所述流表条目对所述数据报文进行处理转发。

可选地，

所述引导流表条目的匹配规则包括: 目的地址为受保护设备的 IP 地址;

所述数据报文匹配命中所述引导流表条目，具体包括:

所述数据报文的目的地址为所述受保护设备的 IP 地址。

可选地，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速;

所述生成模块 1002 设置成: 根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目，具体包括:

所述生成模块 1002 设置成: 生成所述流表条目; 其中，所述流表条目的匹配规则包括: 源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址，Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表条目限制发送速率。

可选地，

所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段;

所述数据报文匹配命中所述引导流表条目，具体包括:

所述数据报文的源地址为所述私网地址网段中的一个。

可选地，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的

地址转换规则;

所述生成模块 1002 设置成: 根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目，具体包括:

所述生成模块 1002 设置成: 生成所述流表条目; 其中，所述流表条目的匹配规则包括: 所述数据报文的私网地址，Actions 包括将所述私网地址转换为分配的公网地址，并通过对应出接口发送转换后的报文。

可选地,

所述接收模块 1001 还设置成: 接收所述 Openflow 控制器发来的第二流表模板;

其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

可选地,

所述生成模块 1002 还设置成: 根据生成的所述流表条目，结合所述第二流表模板生成所述第二流表条目;

其中，所述第二流表条目的匹配规则包括: 所述分配的公网地址，Action 信息为将所述公网地址转换为对应的私网地址，并通过对应出接口发送转换后的报文。

可选地,

所述私网地址包括: 私网 IP 地址;

所述公网地址包括: 公网 IP 地址，或者，公网 IP 地址及端口信息。

可选地,

所述发送模块 1003 还设置成: 将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

相应地，一种开放流（Openflow）控制器，如图 11 所示，包括:

存储模块 1101 设置成: 保存预配置的引导流表条目和流表模板; 其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID;

发送模块 1102 设置成：向 Openflow 转发设备发送所述存储模块保存的所述引导流表条目和流表模板。

可选地，

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

可选地，所述控制器还包括：

接收模块 1103 设置成：接收所述 Openflow 转发设备通过流条目添加消息发来的流表条目；

所述发送模块 1102 还设置成：在接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据所述流表模板生成的所述流表条目；或者，还用于在接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送更高优先级的流表条目。

可选地，

所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则。

可选地，

所述私网地址网段包括：私网 IP 地址。

可选地，

所述发送模块 1102 还设置成：向所述 Openflow 转发设备发送第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序

来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

以上所述仅为本发明的优选实施例而已，并非用于限定本发明的保护范围。根据本发明的发明内容，还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

工业实用性

上述技术方案实现了在 Openflow 转发设备上根据流表条目模板生成流表条目的功能，增强了 Openflow 协议的安全性，同时扩展了 Openflow/SDN 网络的应用场景和实用性。因此本发明具有很强的工业实用性。

权 利 要 求 书

1、一种流表条目生成方法，应用于开放流（Openflow）转发设备，包括:

接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID;

在接收到数据报文后，如果所述数据报文匹配命中所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找与所述流表模板 ID 对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。

2、如权利要求 1 所述的流表条目生成方法，还包括:

将生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

3、如权利要求 2 所述的流表条目生成方法，其中，所述将生成的所述流表条目通过所述流条目添加消息发送给所述 Openflow 控制器的步骤包括:

所述 Openflow 转发设备通过所述流条目添加消息实时或批量发送所述流表条目的信息。

4、如权利要求 1~3 中任意一项所述的流表条目生成方法，还包括:

按照生成的所述流表条目对所述数据报文进行处理转发。

5、如权利要求 1~3 中任意一项所述的流表条目生成方法，其中:

所述引导流表条目的匹配规则包括: 目的地址为受保护设备的 IP 地址;

所述数据报文匹配命中所述引导流表条目的步骤包括:

所述数据报文的目的地址为所述受保护设备的 IP 地址。

6、如权利要求 5 所述的流表条目生成方法，其中:

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速;

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目的步骤包括:

生成所述流表条目；其中，所述流表条目的匹配规则包括：源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址，Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表条目限制发送速率。

7、如权利要求 1~3 中任意一项所述的流表条目生成方法，其中：

所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段；

所述数据报文匹配命中所述引导流表条目的步骤包括：

所述数据报文的源地址为所述私网地址网段中的一个。

8、如权利要求 7 所述的流表条目生成方法，其中：

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则；

所述根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目的步骤包括：

生成所述流表条目；其中，所述流表条目的匹配规则包括：所述数据报文的私网地址，Actions 包括将所述私网地址转换为分配的公网地址，并通过对应出接口发送转换后的报文。

9、如权利要求 8 所述的流表条目生成方法，还包括：

接收所述 Openflow 控制器发来的第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

10、如权利要求 9 所述的流表条目生成方法，还包括：

根据生成的所述流表条目，结合所述第二流表模板生成所述第二流表条目；

其中，所述第二流表条目的匹配规则包括：所述分配的公网地址，Action 信息为将所述公网地址转换为对应的私网地址，并通过对应出接口发送转换后的报文。

11、如权利要求 7、8 或 10 所述的流表条目生成方法，其中：

所述私网地址包括：私网 IP 地址；

所述公网地址包括：公网 IP 地址，或者，公网 IP 地址及端口信息。

12、如权利要求 10 所述的流表条目生成方法，还包括：

将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

13、一种流表条目生成方法，应用于开放流（Openflow）控制器，包括：

向 Openflow 转发设备发送引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID。

14、如权利要求 13 所述的流表条目生成方法，其中：

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

15、如权利要求 13 所述的流表条目生成方法，还包括：

在接收到所述 Openflow 转发设备通过流条目添加消息发来的流表条目后，

所述 Openflow 控制器不回复所述流条目添加消息，表示接受所述 Openflow 转发设备根据所述流表模板生成的所述本地流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据所述流表模板生成的所述流表条目；或者，

所述 Openflow 控制器向所述 Openflow 转发设备发送更高优先级的流表条目。

16、如权利要求 13 所述的流表条目生成方法，其中：

所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则。

17、如权利要求 16 所述的流表条目生成方法，其中：

所述私网地址网段包括：私网 IP 地址。

18、如权利要求 16 所述的流表条目生成方法，还包括：

向所述 Openflow 转发设备发送第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

19、一种开放流（Openflow）转发设备，包括接收模块和生成模块，其中：

所述接收模块设置成：接收 Openflow 控制器发来的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID； 还用于接收数据报文；

所述生成模块设置成：在所述接收模块接收到所述数据报文后，如果所述数据报文匹配命中所述接收模块接收到的所述引导流表条目，则根据所述引导流表条目的 Action 信息中预设置的所述流表模板 ID 查找与所述流表模板 ID 对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目。

20、如权利要求 19 所述的转发设备，还包括发送模块，其中：

所述发送模块设置成：将所述生成模块生成的所述流表条目通过扩展的流条目添加消息发送给所述 Openflow 控制器。

21、如权利要求 20 所述的转发设备，其中：

所述发送模块还设置成：按照所述生成模块生成的所述流表条目对所述数据报文进行处理转发。

22、如权利要求 19 或 20 所述的转发设备，其中：

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；

所述生成模块设置成按照如下方式判断所述数据报文匹配命中所述引导流表条目：

所述数据报文的目的地址为所述受保护设备的 IP 地址。

23、如权利要求 22 所述的转发设备，其中：

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速；

所述生成模块设置成按照如下方式根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目：

生成所述流表条目；其中，所述流表条目的匹配规则包括：源 IP 地址为所述数据报文的源 IP 地址、目的 IP 地址为所述受保护设备的 IP 地址，Action 信息为向所述受保护设备发送与本匹配规则相匹配的数据报文并利用测量表条目限制发送速率。

24、如权利要求 19 或 20 所述的转发设备，其中：

所述引导流表条目的匹配规则包括源地址为一类用户的私网地址网段；

所述生成模块设置成按照如下方式判断所述数据报文匹配命中所述引导流表条目：

所述数据报文的源地址为所述私网地址网段中的一个。

25、如权利要求 24 所述的转发设备，其中：

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则；

所述生成模块设置成按照如下方式根据所述流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目：

生成所述流表条目；其中，所述流表条目的匹配规则包括：所述数据报文的私网地址，Actions 包括将所述私网地址转换为分配的公网地址，并通过对应出接口发送转换后的报文。

26、如权利要求 25 所述的转发设备，其中：

所述接收模块还设置成：接收所述 Openflow 控制器发来的第二流表模板；

其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

27、如权利要求 26 所述的转发设备，其中：

所述生成模块还设置成：根据生成的所述流表条目，结合所述第二流表模板生成所述第二流表条目；

其中，所述第二流表条目的匹配规则包括：所述分配的公网地址，Action 信息为将所述公网地址转换为对应的私网地址，并通过对应出接口发送转换后的报文。

28、如权利要求 24、25 或 27 所述的转发设备，其中：

所述私网地址包括：私网 IP 地址；

所述公网地址包括：公网 IP 地址，或者，公网 IP 地址及端口信息。

29、如权利要求 28 所述的转发设备，其中：

所述发送模块还设置成：将生成的所述第二流表条目通过流条目添加消息发送给所述 Openflow 控制器。

30、一种开放流（Openflow）控制器，包括存储模块和发送模块，其中：

所述存储模块设置成：保存预配置的引导流表条目和流表模板；其中，所述引导流表条目的动作（Action）信息包括预设置的所述流表模板 ID；

所述发送模块设置成：向 Openflow 转发设备发送所述存储模块保存的所述引导流表条目和流表模板。

31、如权利要求 30 所述的控制器，其中：

所述引导流表条目的匹配规则包括：目的地址为受保护设备的 IP 地址；和/或，

所述流表模板定义的流表条目生成规则为对任一源 IP 地址向所述受保护设备发送的报文进行限速。

32、如权利要求 30 所述的控制器，其中，还包括接收模块，其中：

所述接收模块设置成：接收所述 Openflow 转发设备通过流条目添加消息发来的流表条目；

所述发送模块还设置成：在所述接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送拒绝消息，要求所述 Openflow 转发设备删除根据

所述流表模板生成的所述流表条目；或者，在所述接收模块接收到所述流表条目后，向所述 Openflow 转发设备发送更高优先级的流表条目。

33、如权利要求 30 所述的控制器，其中：

所述引导流表条目的匹配规则包括源地址为用户的私网地址网段；和/或，

所述流表模板定义的流表条目生成规则为由用户侧发往网络侧的报文的地址转换规则。

34、如权利要求 33 所述的控制器，其中：

所述私网地址网段包括：私网 IP 地址。

35、如权利要求 33 所述的控制器，其中：

所述发送模块还设置成：向所述 Openflow 转发设备发送第二流表模板；其中，所述第二流表模板与所述流表模板级联，所述第二流表模板定义的流表条目生成规则为由网络侧发往所述用户侧的报文的地址转换规则。

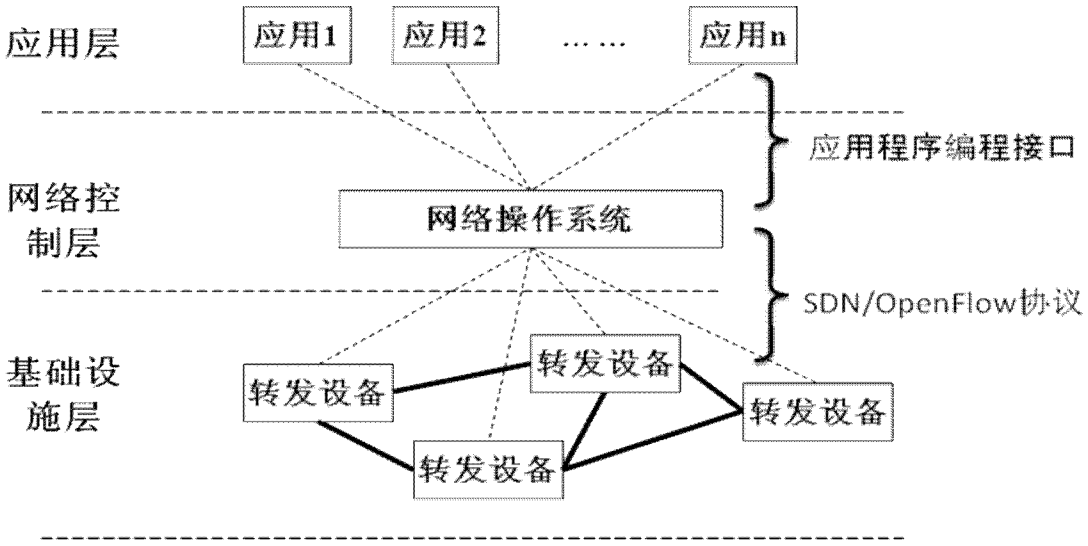
应用层
应用1
应用2
……
应用n
应用程序编程接口
网络控制层
网络操作系统
SDN/OpenFlow协议
基础设施层
转发设备
转发设备
转发设备
转发设备

图 1

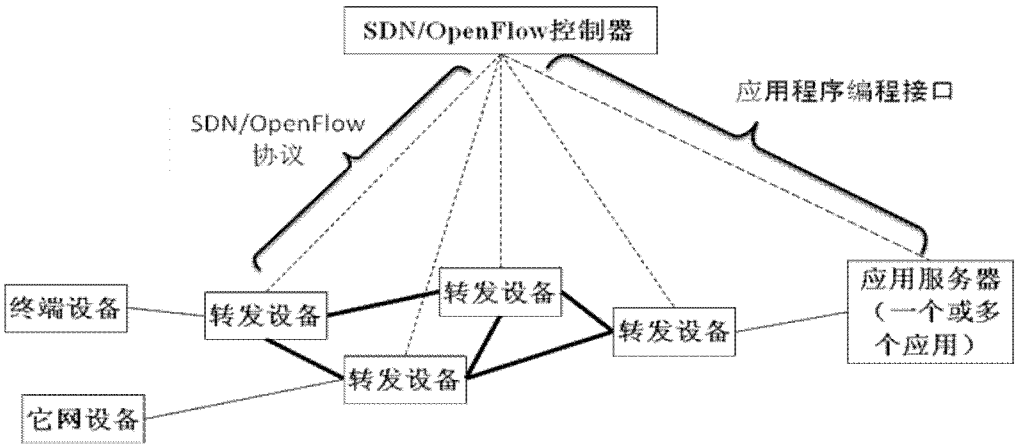
SDN/OpenFlow控制器
SDN/OpenFlow协议
应用程序编程接口
终端设备
转发设备
转发设备
转发设备
转发设备
应用服务器（一个或多个应用）
它网设备

图 2

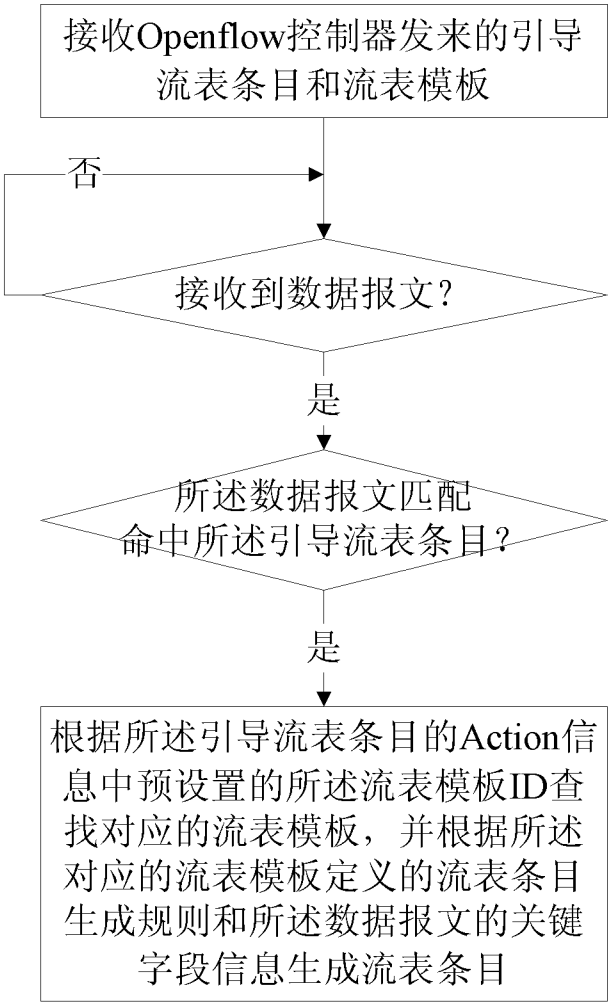
接收Openflow控制器发来的引导流表条目和流表模板
否
接收到数据报文？
是
所述数据报文匹配命中所述引导流表条目？
是
根据所述引导流表条目的Action信息中预设置的所述流表模板ID查找对应的流表模板，并根据所述对应的流表模板定义的流表条目生成规则和所述数据报文的关键字段信息生成流表条目

图 3

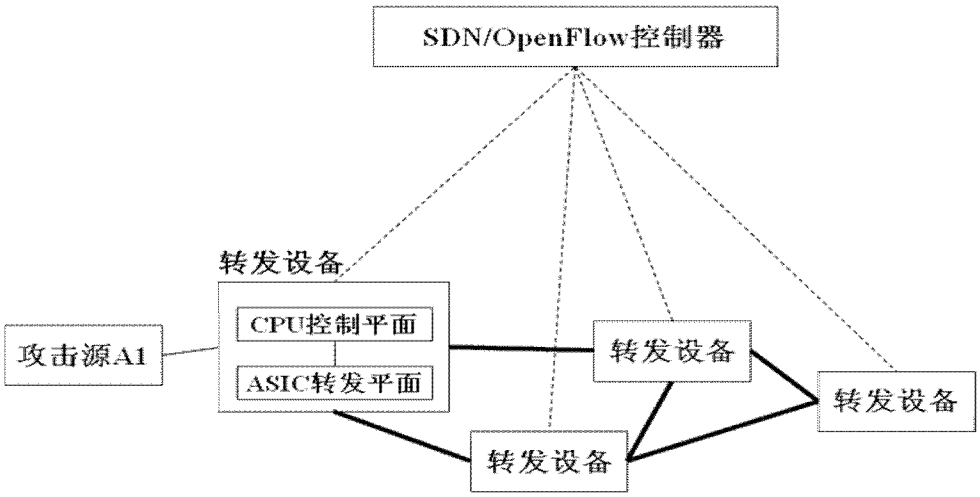
SDN/OpenFlow控制器
转发设备
CPU控制平面
ASIC转发平面
攻击源A1
转发设备
转发设备
转发设备

图 4

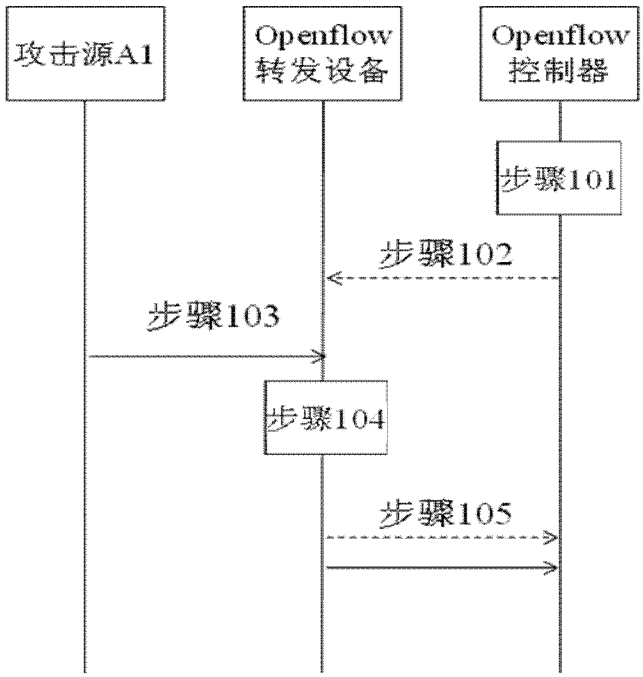
攻击源A1
Openflow
转发设备
Openflow
控制器
步骤101
步骤102
步骤103
步骤104
步骤105

图 5

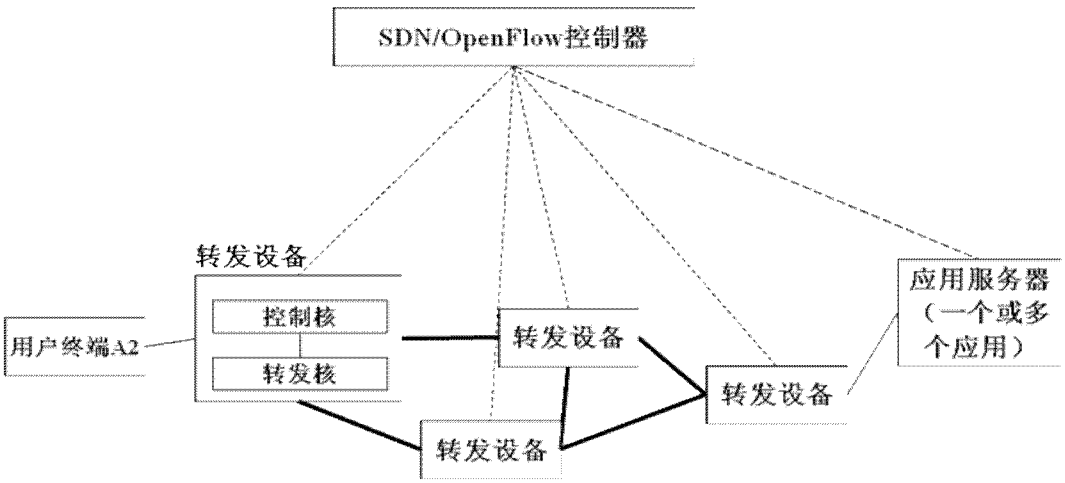
SDN/OpenFlow控制器
转发设备
控制核
转发核
用户终端A2
转发设备
转发设备
转发设备
应用服务器
（一个或多
个应用）

图 6

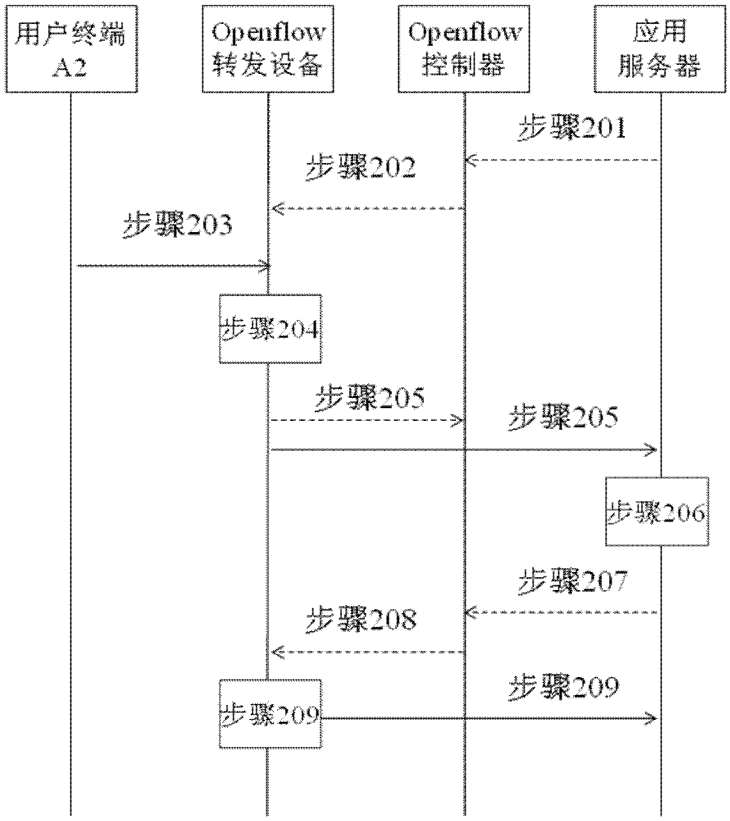
用户终端
A2
Openflow
转发设备
Openflow
控制器
应用
服务器
步骤201
步骤202
步骤203
步骤204
步骤205
步骤205
步骤206
步骤207
步骤208
步骤209
步骤209

图 7

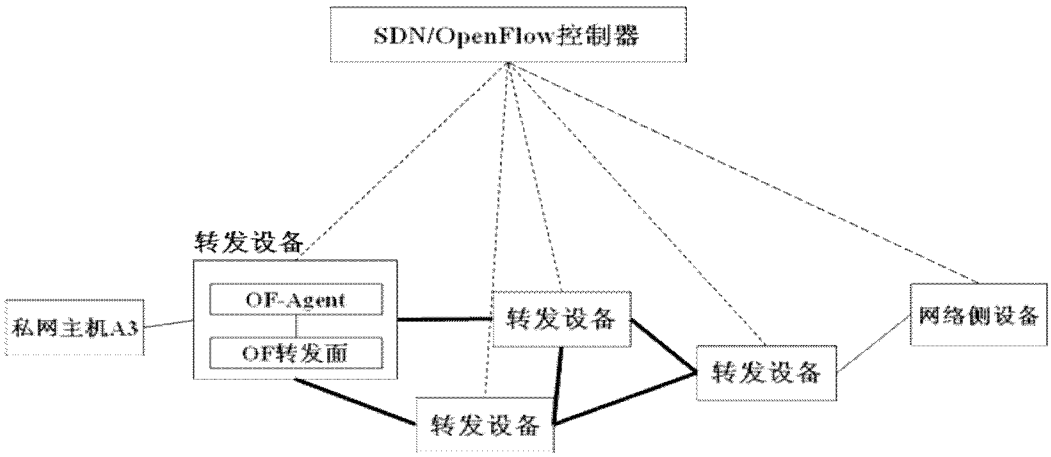
SDN/OpenFlow控制器
转发设备
OF-Agent
OF转发面
私网主机A3
转发设备
转发设备
转发设备
网络侧设备

图 8

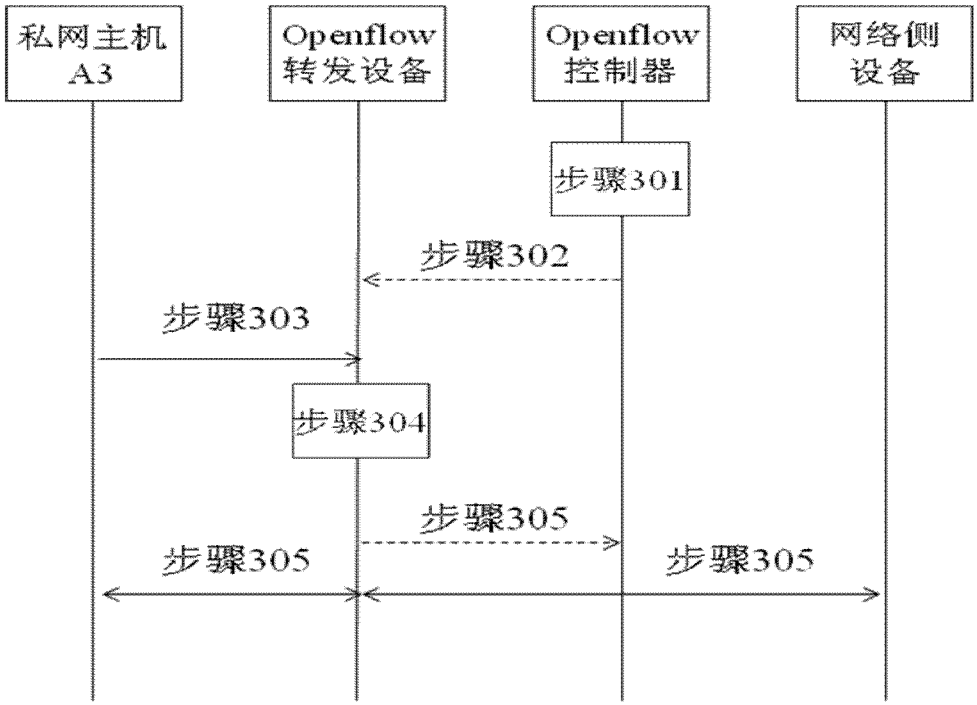
私网主机
A3
Openflow
转发设备
Openflow
控制器
网络侧
设备
步骤301
步骤302
步骤303
步骤304
步骤305
步骤305
步骤305

图 9

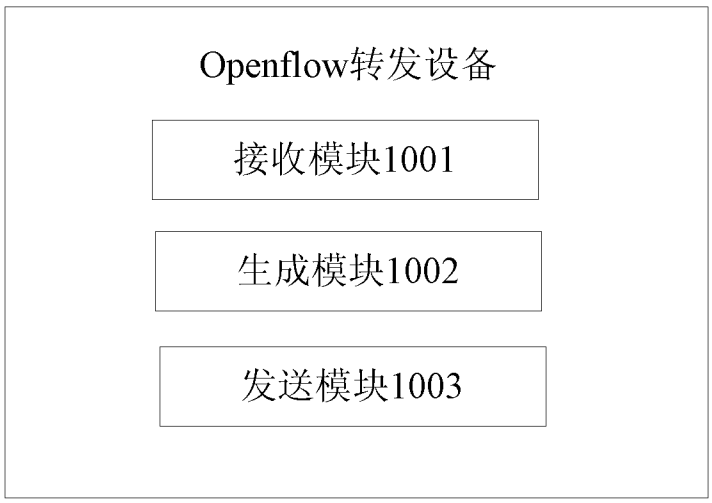
Openflow转发设备
接收模块1001
生成模块1002
发送模块1003

图 10

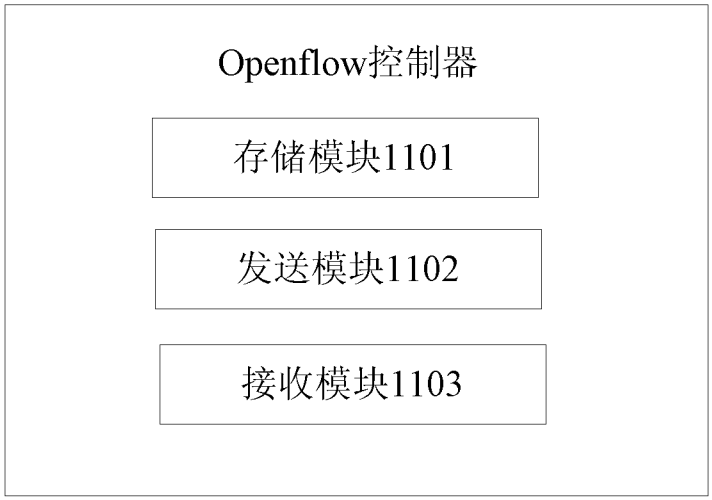
Openflow控制器
存储模块1101
发送模块1102
接收模块1103

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/078406

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/741 (2013.01) 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)

IPC: 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)

CNABS, CNTXT, CNKI, VEN: flow table, development flow, flow, entry, item, open w flow, match, controller

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103428094 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.), 04 December 2013 (04.12.2013), claims 1-2, and description, pages 1-8	1-35
A	CN 102349268 A (NEC CORP.), 08 February 2012 (08.02.2012), the whole document	1-35
A	CN 103166866 A (HUAWEI TECHNOLOGIES CO., LTD.), 19 June 2013 (19.06.2013), the whole document	1-35

☐ 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
04 August 2014 (04.08.2014)	**12 August 2014 (12.08.2014)**
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 **SUN, Zhiling** Telephone No.: (86-10) **62089365**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/078406

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103428094 A	04.12.2013	None	
CN 102349268 A	08.02.2012	US 2011261825 A1	27.10.2011
		EP 2408155 A1	18.01.2012
		JP 5408243 B2	05.02.2014
		WO 2010103909 A1	16.09.2010
		US 8605734 B2	10.12.2013
CN 103166866 A	19.06.2013	WO 2013086897 A1	20.06.2013

国际检索报告

国际申请号
PCT/CN2014/078406

A. 主题的分类

H04L 12/741(2013.01)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））

CNABS,CNTXT,CNKI,VEN:流，流表，条目，开发流，匹配，控制器，flow, entry, item, open w flow, match, controller

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 103428094 A (杭州华三通信技术有限公司) 2013年 12月 04日 (2013-12-04) 权利要求1-2，说明书第1-8页	1-35
A	CN 102349268 A (日本电气株式会社) 2012年 2月 08日 (2012-02-08) 全文	1-35
A	CN 103166866 A (华为技术有限公司) 2013年 6月 19日 (2013-06-19) 全文	1-35

☐ 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
2014年 8月 04日	2014年 8月 12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) 北京市海淀区蓟门桥西土城路6号 100088 中国	孙志玲
传真号 (86-10)62019451	电话号码 (86-10)62089365

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/078406

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	103428094	A	2013年 12月 04日	无			
CN	102349268	A	2012年 2月 08日	US	2011261825	A1	2011年 10月 27日
				EP	2408155	A1	2012年 1月 18日
				JP	5408243	B2	2014年 2月 05日
				WO	2010103909	A1	2010年 9月 16日
				US	8605734	B2	2013年 12月 10日
CN	103166866	A	2013年 6月 19日	WO	2013086897	A1	2013年 6月 20日