



SDN 环境下网络流量监测与控制系统设计

刘川¹, 娄征², 黄辉¹, 邓辉¹

(1. 国网智能电网研究院, 江苏 南京 210003; 2. 国网南京供电公司, 江苏 南京 210000)

摘要: 由于 SDN 具有可软件定义的特性和控制与转发相分离的特点, SDN 环境下网络流量测控与传统的 IP 网络显著不同。提出了一种基于 sFlow 技术的网络流量监测与控制系统, 借助 sFlow 数据监测的功能, 把数据收集的过程从 SDN 控制平面分离出来。构建了基于 OpenDaylight 控制器与 Mininet 的实验环境, 通过模拟拒绝服务攻击来产生异常流量, 利用网络流量测控的方法实现了异常流量的拦截。

关键词: 软件定义网络; 流量监测; 拒绝服务; 端口

中图分类号: TN914.34

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015398

Design of network traffic monitoring and control system in SDN

LIU Chuan¹, LOU Zheng², HUANG Hui¹, DENG Hui¹

1. State Grid Smart Grid Research Institute, Nanjing 210003, China

2. State Grid Nanjing Power Supply Company, Nanjing 210000, China

Abstract: The core idea of SDN (software defined networking) is that the control plane and data plane are separated, which makes the network traffic can be flexible controlled. Since SDN has these characteristics, the traffic monitoring and control in SDN have significant differences with traditional IP networks. A network traffic monitoring and control system based on sFlow technology was presented. With the application of sFlow, the process of data collection was separated from the control plane of SDN. The experimental environment was constructed based on OpenDaylight controller and Mininet, and the abnormal traffic was simulated by DoS (denial of service) attacks. The experiments show that the proposed network traffic monitoring and control system can effectively intercept the abnormal traffic.

Key words: SDN, traffic monitoring, DoS, port

1 引言

以互联网为代表的信息网络在经济和社会发展中起到了越来越重要的作用。在信息网络不断发展的同时,网

络安全问题日益成为人们关注的焦点。非法访问、恶意攻击等都容易影响网络的正常运行。目前, DoS (denial of service, 拒绝服务) 攻击已经成为现有信息网络的一个主要威胁, 攻击者常采用 IP 地址欺骗的方式, 很难定位攻击

收稿日期: 2015-11-01; 修回日期: 2015-11-15

基金项目: 国家电网公司科技项目“软件定义网络(SDN)体系及其电力应用关键技术研究”; 国网智能电网研究院青年基金项目“支持电力应用 SDN 控制功能的网络流量可视化矩阵关键技术研究”(No.SGRI-HT-81-15-002)

Foundation Items: The Science and Technology Project of State Grid Corporation of China: Research on Software Defined Networking System and Key Technologies of Electric Power Application, Youth Fund Project of Smart Grid Research Institute: Research on the Key Technologies of Network Flow Visualization Matrix Supporting the Software Defined Networking Control Function of Electric Power Application (NO.SGRI-HT-81-15-002)



者^[1]。对于 DoS 攻击的防御主要难点在于区分异常流量和正常流量。同时,传统互联网架构下,网络设备很难通过协作方式应对来自不同地点的 DDos (distributed denial of service, 分布式拒绝服务) 攻击流量。

SDN (software defined networking, 软件定义网络) 提出了一种新型的网络管理模式^[2]。SDN 的核心是控制与数据相分离, 控制器具有全局的拓扑视野, 可以通过下发流表对网络中的数据流进行精细化处理, 交换机根据流表对经过的数据流进行指定的操作。控制层与数据层之间采用开放的统一接口 (如 OpenFlow 等) 进行交互^[3,4]。运营商和科研人员可通过控制器掌握全局网络信息, 便于管理配置网络和部署新协议^[5]。网络流量监控通过实时收集和监视网络数据分组的流量信息, 检查是否有违反安全策略的行为和网络工作异常的迹象, 网络流量监控是一种分析网络状况的有效方法。由于 SDN 具有可软件定义的特性和控制与转发相分离的特点, SDN 环境下的网络流量测控与传统的 IP 网络具有很大的不同。

基于 SDN 的网络流量监控可以先通过 SDN 控制器获取交换机端的数据分组, 然后利用控制器上的应用模块进行分析处理。参考文献[6]通过对 SDN 控制器收到的请求分组进行熵值计算, 检测网络中的异常行为。参考文献[6]的研究是利用 SDN 控制器本身对数据平面流量进行收集和统计, 不能完整地对流经 SDN 的流量进行监控, 并且在一定程度上增加了控制器的开销。

本文提出了一种基于 sFlow 技术的 SDN 流量监测与控制系统。借助 sFlow 数据监测的功能, 把数据监测的过程从 SDN 控制平面分离出来, 从而缓解 SDN 控制器处理数据分组的压力。sFlow 实时地向 SDN 控制器通告交换设备各端口的流量情况, SDN 控制器根据通告修改流表规则并下发新的流表, 从而对攻击行为进行管控。通过构建 OpenDaylight 控制器与 Mininet 交换模拟器相结合的实验环境, 研究了 SDN 环境下网络交换机的转发特性, 并通过模拟拒绝服务攻击验证了流量监控系统的有效性。

2 SDN 下网络流量监测与控制系统设计

本系统基于 SDN 架构, 系统的流量监测与控制功能可以有效拦截 DoS 攻击流量。sFlow 是一种以设备端口为基本单元的流量监控技术, 能够在整个网络中以连续实时的方式完全监视每一个端口。sFlow 组件向 SDN 控制器通告实时的流量情况, 当有攻击行为发生时, 将产生异常流

量通告。SDN 控制器根据通告内容修改流表规则, 并下发新的流表, 从而对 SDN 的流量进行管控。

2.1 系统结构

SDN 环境下网络流量监测与控制系统由流量监控模块、数据转发层和控制层组成。系统结构如图 1 所示。

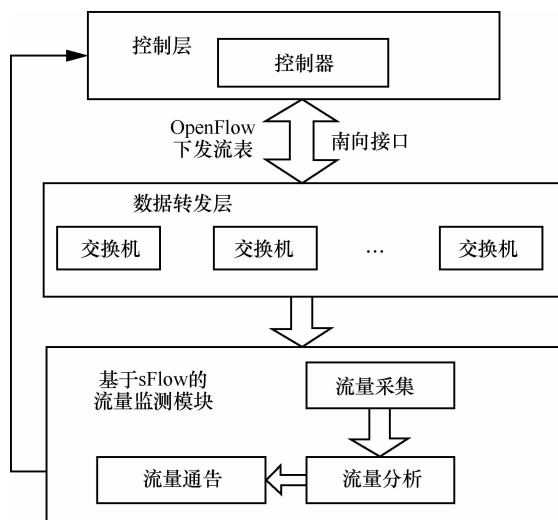


图 1 SDN 环境下网络流量监测与控制系统结构

控制器是整个网络的核心部件, 主要管理数据层的转发。控制器与 OpenFlow 交换机经由控制数据面接口 (南向接口) 交互。控制器与应用层的各种应用软件经由开放 API (北向接口) 交互。控制器通过 OpenFlow 标准协议更新 OpenFlow 交换机中的流表, 从而实现对整个网络流量的集中管控。

数据转发层由支持 OpenFlow 技术的交换机组成。OpenFlow 交换机接收到数据报文后, 首先查找流表, 找到转发报文的匹配表项, 并执行相关动作。若找不到匹配表项, 则把报文转发给控制层, 由控制器决定转发行为。

流量监控模块由流量采集、流量分析和流量通告 3 部分构成。首先通过运行流量监控脚本进行流量采集, 然后通过流量分析工具进行流量分析, 当发现交换机某个端口的流量超过已定义的阈值时, 则通过脚本形成一个异常流量通告, 并通过 OpenFlow 协议向控制器提交流量通告。假如控制器收到异常流量通告, 则将产生并下发新流表, 要求有异常流量的端口丢弃异常流量, 从而防御 DoS 攻击。

2.2 系统工作流程

系统的工作可分为流量监测与流量控制两部分。其中, 流量监测工作从 SDN 的控制层面分离出来, 通过 sFlow 流量监测设备实现, 但流量控制工作的主体仍然是

SDN 控制层面。基于 sFlow 技术的流量监测设备分为两类:一类是 sFlow 代理,负责采集交换设备上每个端口的流量并形成 sFlow 数据分组;另一类是 sFlow 采集器,负责接收 sFlow 数据分组。实际应用中,sFlow 代理可以嵌入网络路由和交换设备 ASIC 中,不需要购买额外的探针和旁路器就能全面监视整个网络。

流量监测是指通过 sFlow 代理和 sFlow 采集器的协作来监测各端口流量,从而及时发现异常流量。流量监测的工作流程如图 2 所示。sFlow 代理采集交换设备上每个端口的流量并形成 sFlow 数据分组,sFlow 采集器通过对 sFlow 数据分组进行分析,获知交换设备上每个端口的实时流量,判断端口流量是否超过阈值,并向控制器发送相应的流量通告。

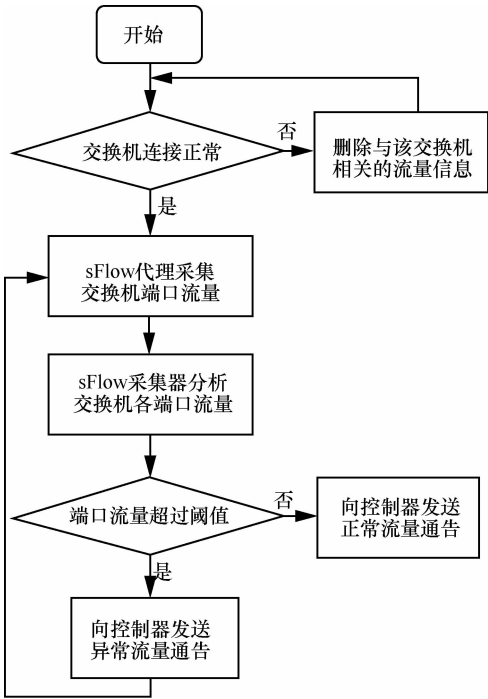


图 2 SDN 环境下网络流量监测工作流程

流量控制是指 SDN 控制器根据流量监测的结果调整流表项,并下发流表,从而实现对整个网络流量的管控。流量控制部分的工作流程如图 3 所示。SDN 控制器收到来自 sFlow 采集器的流量通告后,根据通告内容设置相应动作,生成相应流表项,向 OpenFlow 交换机下发流表。

3 实验验证

3.1 网络拓扑

实验在两台安装 ubuntu 14.04 系统的虚拟机下运行,

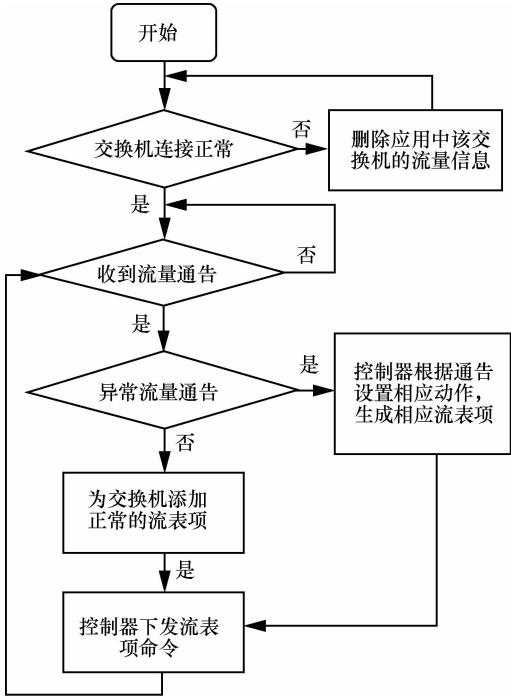


图 3 SDN 环境下网络流量控制工作流程

使用 OpenDaylight 作为控制器。网络拓扑基于 Mininet 平台搭建,通过 Python 在网络拓扑中定义两台 OpenFlow 交换机和 4 台主机。网络拓扑如图 4 所示。Mininet 中的网络流量通过 sFlow 代理传给 sFlow 收集器,sFlow 收集器通过数据分析,将交换机各个端口的流量图形化显示,并且向控制器发送各端口的流量通告。

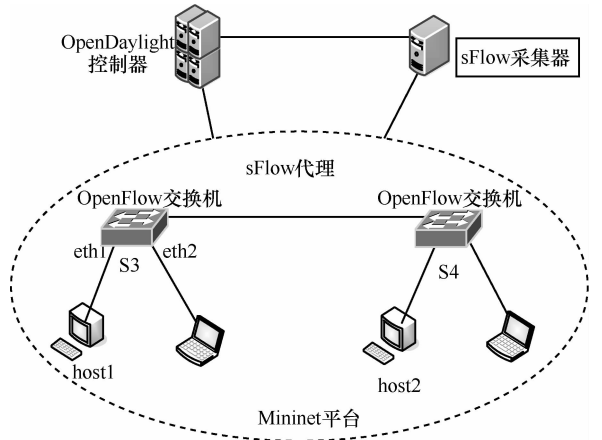


图 4 网络拓扑示意

3.2 关键步骤及结果

(1)部署 sFlow 采集器

下载 sFlow 代码到一台虚拟机,安装并启动 sFlow 采集器。sFlow 采集器默认监听端口为 6343,可以通过虚拟



机内置的浏览器打开监控页面。

(2)部署 sFlow 代理

在 OVS(open vSwitch,开源虚拟交换机)上配置 sFlow 代理,配置后可以看到已配置的代理信息,如图 5 所示。

(3)执行流量监控脚本

流量监控脚本的作用:首先,在 sFlow 采集器设定端口流量的阈值(这里设为 1 500 KB/s)。然后,通过 sFlow 代理获取 Mininet 拓扑里所有交换机端口的每秒流量,若端口每秒流量超过阈值,就认为是异常流量。最后,利用脚本生成向 OpenDaylight 控制器的流量通告。

(4)模拟 DoS 攻击

实验通过 ping flooding 模拟 DoS 攻击流量,采取 host1

向 host2 泛洪的方式,监测交换机 S3 的端口 eth1 的流量变化。结果如图 6 所示。可以看到,未运行流量监控前,host1 向 host2 泛洪的数据分组达到了大约 15 000 个/s。

(5)流量监控

运行脚本,激活流量监测与控制功能。监控系统发现在交换机 S3 的 eth1 端口有流量攻击,将产生异常流量报告,如图 7 所示。

OpenDaylight 控制器将根据异常流量通告,修改与 S3 的 eth1 接口有关的流表项并下发流表,丢弃正在被攻击的端口流量。运行流量监控后,S3 的 eth1 端口的流量如图 8 所示。可以看到,在 10:17 时刻运行脚本后,host1 向 host2 泛洪的分组被迅速地丢弃。

```
root@ubuntu: ~  
root@ubuntu:~# ovs-vsctl list sflow  
_uuid      : c57e0ada-89eb-4381-96ae-7003c4228434  
agent      : "eth0"  
external_ids : {}  
header     : 128  
polling    : 1  
sampling   : 10  
targets    : ["192.168.0.114:6343"]  
root@ubuntu:~#
```

图 5 sFlow 代理的部署信息

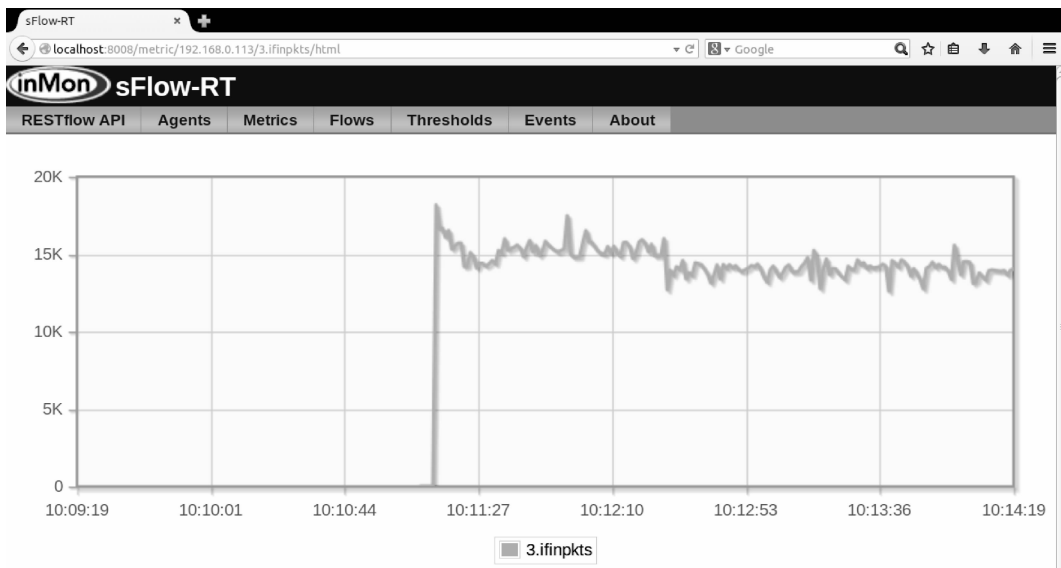


图 6 运行流量监控前被攻击交换机的端口流量

```
root@ubuntu: /home/conan  
root@ubuntu:/home/conan# ./speedtest.sh  
Net s3 Traffic is: 0 k/s  
Net s4 Traffic is: 0 k/s  
Net s3-eth1 Traffic is: 1522 k/s  
s3-eth1 DDOS WARNING !!
```

图 7 流量监控系统发现被攻击交换机的端口有异常流量

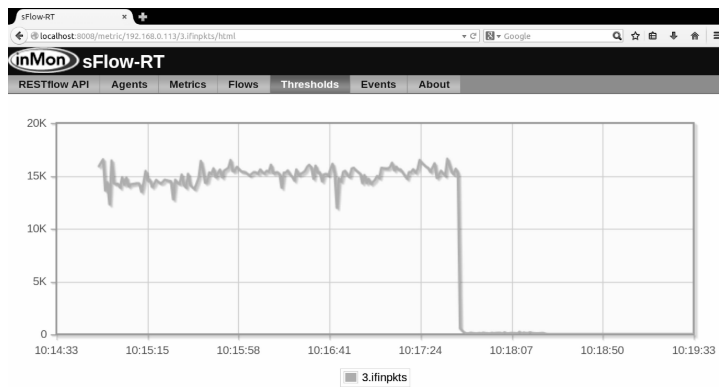


图 8 运行流量监控后被攻击交换机的端口流量

4 结束语

本文针对 SDN 架构,提出了一种基于 sFlow 技术的流量监测与控制系统。该系统可以对网络中每一个端口的实时流量进行监测,并通过控制器实现对整个网络的流量管控。通过构建 OpenDaylight 控制器与 Mininet 交换模拟器相结合的实验环境,验证了该系统在流量监控方面的有效性和准确性。利用该系统还可以实现更多的服务,比如负载均衡、QoS 等。下一步工作是对流量监测结果进行细化,对流入网络的流量进行模型匹配,准确地定位攻击类型,使得控制器可以根据攻击类型生成并下发相应的流表。

参考文献:

- [1] 孙长华, 刘斌. 分布式拒绝服务攻击研究新进展综述 [J]. 电子学报, SUN C H, LIU B. New process review of distributed denial of service attack. [J]. Journal of Electronics, 2009, 37 (7): 1562-1570.
- [2] Stanford University. Clean slate program[EB/OL]. [2015-10-01]. <http://cleanslate.stanford.edu/>.
- [3] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks [J]. ACM Sigcomm CCR, 2008, 38(2): 69-74.
- [4] 张朝昆, 崔勇, 唐嵩伟, 等. 软件定义网络(SDN)研究进展[J]. 软件学报, 2015, 26(1): 62-81. ZHANG C K, CUI Y, TANG H Y, et al. Research progress of software defined networking[J]. Journal of Software, 2015, 26(1): 62-81.
- [5] NUNES B A A, MENDONCA M, NGUYEN X N, et al. A survey of software-defined networking: past, present, and future of programmable networks [J]. IEEE Communications Surveys and Tutorials, 2014, 16(3): 1617-1634.
- [6] MOUSAVI S M, ST-HILAIRE M. Early detection of DDoS

attacks against SDN controllers [C]// 2015 International Conference on Computing, Networking and Communications, Feb 16-19, 2015, Garden Grove, CA, USA. New Jersey: IEEE Press, 2015: 77-81.

[作者简介]



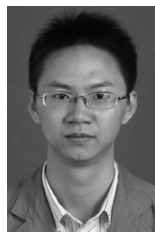
刘川(1986-),男,国网智能电网研究院工程师,主要研究方向为电力通信与未来网络技术。



姜征(1978-),男,国网南京供电公司副高级工程师,主要研究方向为信息、通信安全及计算机体系结构。



黄辉(1978-),男,国网智能电网研究院高级工程师,主要研究方向为电力通信技术与产品开发。



邓辉(1982-),男,国网智能电网研究院高级工程师,主要研究方向为电力通信技术与产品开发。