基于 OpenFlow 校园网异常流量的管理

闫晓洁，于广辉
（大连理工大学 网络与信息化中心，辽宁 大连 116024）

摘 要：随着高校数字化校园的推进，通过网络传输的视频、音频、图像和其他网络应用业务不断增多，从而使网络流量行为日趋复杂，对服务质量和网络安全提出更高的要求。OpenFlow 是近年来支持网络创新研究而提出的基于流分类的新型网络技术，能解决当前网络设备工作负载过重的问题。通过分析 OpenFlow 的体系架构，针对校园网的异常流量进行识别、分类和转发的策略，并通过模拟实验平台 Mininet 验证该策略的有效性，从而有效地改善了网络性能并提高了网络的安全性。

关键词：OpenFlow；异常流量；网络性能；流量管理
中图分类号：TP393 **文献标识码**：A **文章编号**：1674-7720(2013)24-0053-03

Management of anomaly traffic in campus network based on OpenFlow

Yan Xiaojie, Yu Guanghui
(Network and Information Center, Dalian University of Technology, Dalian 116024, China)

Abstract: With the continuous improve of information technology in digital campus, the network transmission of video, audio, images and other network applications business is growing so fast that the network traffic behavior increases the complexity of network services. The quality of service and network security related performance need higher requirements. OpenFlow network is proposed as a new network traffic classification technology to support innovative research in recent years, being able to separate routing control and data transmission, and resolving the current network due to complications resulting work overload network equipment problems. This paper analyzes the OpenFlow architecture for the campus network and designed a strategy to handle with anomaly traffic forwarding data packets. Through verifying the validity of the policy and stability in the simulation platform mininet, the strategy could effectively improve the network performance and network security.

Key words: OpenFlow; anomaly traffic; network performance; traffic management

随着信息化时代计算机网络技术的快速发展，促使高校数字化校园[1]不断地进行信息化建设，上网流量需求和用户的日益增多以及多元化给网络数据流量带来急剧增长，网络设备运转负荷倍增，网络带宽扩容面临巨大压力，成为网络管理的瓶颈。因此网络监控管理已成为不可或缺的部分，尤其是在网络安全以及网络规划方面有非常重要的意义。

网络流量作为网络用户上网记录和活动的一个重要反应，通过监控和分析网络上各种应用的网络带宽的使用情况，剖析用户流量行为，从而合理地分配和规划带宽，尤其是当发现网络流量产生异常时，可以迅速根据流量监控分析的结果采取相应的控制手段，从而达到对攻击源进行有效隔离，防止各类网络攻击，从而保障关键业务应用的正常运行。

1 OpenFlow 技术

1.1 OpenFlow 网络

OpenFlow[2]是斯坦福大学 Clean Slate 计划资助的一个开放式协议标准，主要用于在现有网络上设计新的协议和部署新的业务应用，其最终目标是重新设计互联网，其核心内容是对网络数据流的分类算法来达到对网络进行可编程。

OpenFlow 网络由 OpenFlow 交换机、FlowVisor 和 Controller 三部分组成。OpenFlow 交换机进行数据层的转发；FlowVisor 对网络进行虚拟化；Controller 对网络进行集中控制，实现控制层的功能。OpenFlow 网络组成如图 1 所示。

1.2 OpenFlow 交换机

OpenFlow 交换机由三部分构成：数据流表对应一个转发规则操作，用以指示交换机如何处理该数据流。安

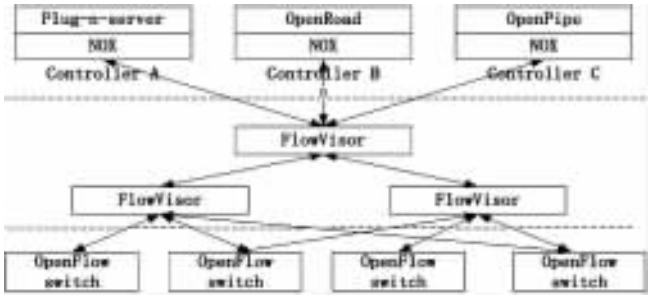

图 1 OpenFlow 网络结构

全通道用于实现 OpenFlow 交换机与控制器之间的指令和数据包的安全传递；OpenFlow 协议用来描述控制器和交换机之间相互所用信息的标准，以及控制器和交换机的接口标准。

OpenFlow 交换机[3]是整个 OpenFlow 网络的核心部件，主要管理数据层的转发。OpenFlow 交换机接收到数据包之后，首先在本地的流表上查找转发目标端口，如果没有匹配，则把数据包转发给 Controller，由控制层决定转发端口。其组成结构如图 2 所示。

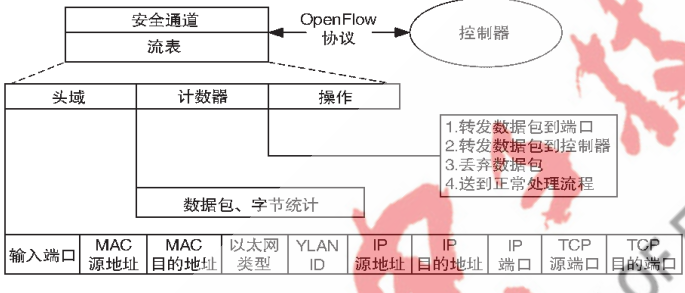

图 2 OpenFlow 交换机结构

2 基于 OpenFlow 的异常流量管理设计

2.1 总体架构图

本系统研究的目的就是减少校园网中的异常流量，利用 OpenFlow 中对流表的管理来控制网络数据包的转向，从而实现网络中控制层面与数据平面相分离，有效地阻止对网络的攻击。本系统设计主要包括异常流量识别模块、异常流量分类模块、流表管理模块和超时处理模块，具体设计管理图如图 3 所示。

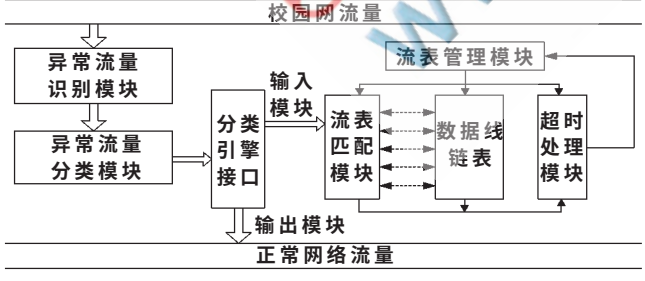

图 3 异常流量管理图

2.2 异常流量识别模块

该模块通过异常流量识别算法[4]进行处理，利用改进的 Adapted-Bloom-Filter 防抖动的地址聚集算法来更好地检测异常流量，对流量进行特征提取和区分过滤。采用 M-CUSUM 算法对网络端口输入输出流量的变化进行监控，及时地检测出流量的异常，从而实现对异常流量攻击采取综合整治。

2.3 异常流量分类模块

该模块主要功能是进一步对异常流量进行聚集分类[5]，缩小异常流量范围。实现的方法是使用基于特征分析的统计方法来识别具有异常流量的聚集。首先要对 IP 流进行分类，依据各协议包使用比例和出现几率，将 IP 包分为 TCP 包、UDP 包和 ICMP 包。其中 TCP 和 UDP 流量是网络中的主要流量，而 TCP 聚集还可以再细分为 TCP 控制包和 TCP 数据包。

2.4 流表管理模块

OpenFlow 交换机拥有一个或多个流表，流表中包含多个流表项，每个流表项都包含规则、操作和计数三部分。当一个分组到达 OpenFlow 交换机时，该分组头部信息被提取出来并被用来与流表项进行匹配，如果交换机的流表中不存在该分组匹配的流表项，则该分组的全部或部分被转发到控制器，并由控制器来决定如何对该分组或此类流进行处理，如果匹配成功，将会按照所匹配的流表项的操作字段的内容对分组进行转发处理。

OpenFlow 主要存在两种类型的流表：线性表和哈希表，当向 OpenFlow 交换机中插入一条流表项时，如果流表项中用来匹配分组的 12 元组信息都含有一个确定值，那么这条流表项将先插入到哈希表中，在哈希表满的情况下才会向线性表插入；如果 12 元组中某些字段是以通配符的方式进行提供，那这条流表项只能插入到线性表中。流量查询算法如下：

```
Input：分组 packet
Output：相应的处理流表项 flow 或 false
Flow_key = extract(packet);          //在分组 packet 中
                                       提取分组头部
Hash_key = hash(flow_key);           //计算首部的哈希值
For i=1 to n do                      //查找 n 个哈希表
    If hash_table[i][hash_key] ! = NULL
        Do return flow = hash_table[i][hash_key];
                                       //返回处理流表项
Linear_flow = linear_list -> next;
While linear_flow ! = NULL           //查询线性表
    If match (linear_flow, flow_key) do
        Return flow = linear_flow;  //返回处理表项 flow
    Else do Linear_flow = linear_flow -> next;
        Return false;//查找不到处理流表项，返回 false
```

2.5 超时处理模块

由于流表项存在超时问题，所以当流表项的存在时间超过最大生存时间时，流表项管理模块需要删除该规则。考虑到流表项具有相同的最大生存时间，删除流表项的顺序与流表项进入的顺序相同，所以采用链表结构存放流表项。当流表项管理模块为新进规则生存链表节

点时，将当前时间置为该链表节点的时间项。管理模块每隔一个虚拟单位时间检查一次超时链表各节点的时间项，如果当前时间与规则进入时间之差大于流表项最大生存时间，则删除超时表项，释放存放表项的链表节点。

3 仿真实验

为了验证本文的设计，决定采用虚拟网络环境 Mininet 仿真平台，它可以在一台机器上创建一张多至数百个节点的大规模虚拟网络，节点类型和拓扑结构可以自行定义，并且支持 OpenFlow 协议，具体的实验拓扑如图 4 所示。

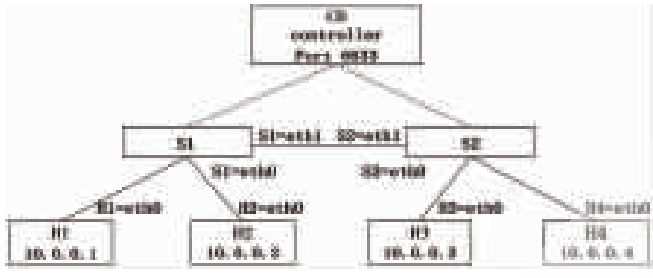

图 4 仿真试验拓扑图

图中 C0 是中心控制器，下面连着两个 OpenFlow 交换机 S1 和 S2，往下分别连着虚拟机 H1、H2、H3 和 H4。由 H1 向系统主动发起正常网络流量 3 370 430 KB 和 TCP flooding 攻击，攻击流量的数据包为固定大小 40 B，Ack 和 Flag 不固定，源端口固定，目的端口随机，大小为 844 297 KB。设置系统把检测到的异常流量全部转发给主机 H4，正常流量随机转到 H2 和 H3 主机上。

经过反复测试 3 次取平均值，对主机 H4 进行流量统计，发现共统计到流量 818 880 KB，H2 和 H3 主机共统计到流量为 3 370 430 KB，说明系统中正常流量都通过了，异常流量基本被捕获拦截，拦截率为 96.99%，基本符合预期的目标。

在复杂的网络环境当中，网络流量的增长不仅仅给路由器交换机等网络设备带来沉重的负载，而且通常会隐藏着异常流量引起的网络安全问题。本文基于 OpenFlow 新型的可编程的网络平台，对网络环境中的流量进行了识别和分类，通过对 OpenFlow 流表进行编程来设计对异常数据包的转发处理，并通过在仿真网络平台上进行测试验证，达到了预计的效果。

参考文献

[1] YMCKEOWN N，ANDERSON T，BALAKRISHNAN H，et al. OpenFlow：enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review，2008，38(2)：69-74.

[2] OpenFlow[EB/OL].[2013-07-20].http://www.OpenFlow.org.

[3] SHERWOOD R，CHAN M，COVINGTON A，et al. Carving research slices out of your production networks with OpenFlow[J]. ACM SIGCOMM Computer Communication Review，2010，40(1)：129-130.

[4] 郑晓霞.校园网异常流量分析系统设计与实现[D].青岛：中国海洋大学，2012.

[5] 杨新存.校园网流量管理及异常监测系统的研究与实现[D].兰州：兰州理工大学，2012.

(收稿日期：2013-09-23)

作者简介：

闫晓洁，女，1984 年生，硕士研究生，主要研究方向：计算机网络、路由与交换技术。