



一种 SDN 中基于熵值计算的异常流量检测方法

王铭鑫,周华春,陈 佳,张宏科

(北京交通大学电子信息工程学院 北京 100044)

摘 要:软件定义网络(software defined networking,SDN)是一种新型网络创新架构,其分离了控制平面与转发平面,使得网络管理更为灵活。借助 SDN 控制与转发分离的思想,在 SDN 基础上引入一个集中式安全中心,在数据平面设备上采集数据,用于对网络流量进行分析,通过熵值计算和分类算法判断异常流量行为。对于检测到的网络异常情况,安全中心通过与 SDN 控制器的接口通告 SDN 控制器上的安全处理模块,进行流表策略的下发,进而缓解网络异常行为。通过本系统可以在不影响 SDN 控制器性能的情况下,快速检测网络中的异常行为,并通过 SDN 下发流表策略对恶意攻击用户进行限制,同时对 SDN 控制器进行保护。

关键词:软件定义网络;安全中心;熵值;分布式拒绝服务攻击

doi: 10.11959/j.issn.1000-0801.2015217

An Entropy Based Anomaly Traffic Detection Approach in SDN

Wang Mingxin, Zhou Huachun, Chen Jia, Zhang Hongke

(School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: SDN (software defined networking) is a novel network infrastructure which separate the control plane from the data plane. Taking advantage of the idea of SDN, a central security center was built which collected traffic from the SDN data plane entity for analyzing. The attacks can be detected based on the entropy variation of the identifier and locate the type of attack with the classification algorithm. As the anomaly patterns were detected, the security center would cooperate with the central controller to install the flow table to alleviate the influence of the attack. The anomaly traffic can be detected early and can't influence the performance of the controller. Besides, the controller can be protected from attack based on our system.

Key words: SDN, security center, entropy, DDoS

1 引言

随着信息网络的发展,互联网用户数量和应用规模不

断扩大,结构和功能日趋复杂,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。但互联网也在使用过程中暴露了越来越多的问题,尤其是网络安全

收稿日期:2014-12-01;修回日期:2015-09-02

基金项目:国家科技重大专项基金资助项目(No. 2013ZX03006002),基本科研业务费资助项目(No. 2015YJS028),国家高技术研究发展计划("863"计划)基金资助项目(No. 2015AA015702)

Foundation Items: The National Science and Technology Major Projects of the Ministry of Science and Technology of China (No. 2013ZX03006002), Fundamental Research Funds for the Central Universities(No. 2015YJS028), The National High-Tech R&D Program(863 Program)(No. 2015AA015702)

论文引用格式:王铭鑫,周华春,陈佳等. 一种 SDN 中基于熵值计算的异常流量检测方法. 电信科学,2015217

Wang M X, Zhou H C, Chen J, *et al.* An entropy based anomaly traffic detection approach in SDN. Telecommunications Science, 2015217

全问题日益严重。DDoS(distributed denial of service, 分布式拒绝服务)攻击已经成为现有互联网的一个主要威胁,其不需要很强的专业知识,并且攻击者采用 IP 地址欺骗的方式,很难定位攻击者。对于 DDoS 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来应对来自不同地点的 DDoS 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^[1]。在 SDN 中,交换机不对数据分组进行过多的处理,仅依照流表匹配进行转发。如果没有匹配,数据分组则会被交到控制器中进行解析处理。SDN 控制器是网络的操作系统,由它处理数据分组,并决策数据分组是否要被转发或者丢弃,并下发规则到数据平面交换机上。通过这种方式,SDN 分离了控制层与数据转发层。通过 SDN 的集中式控制机制,很容易获得网络状态信息,并且能够通过下发流表的方式灵活地控制数据分组的处理方式,转发或者丢弃。OpenFlow^[2]作为 SDN 的一种实现方法,定义了控制平面控制器与数据平面设备之间通信的协议,为研究者提供了一个开放式的研究平台^[3]。

一些研究通过 SDN 控制器获取交换机接收到的数据分组,利用控制器上的应用进行分析处理。Braga 等人利用自组织映射(self-organizing map, SOM)方法来对 DDoS 流量和正常流量进行分类,他们通过对 OpenFlow 交换机上采集的流量信息进行训练,通过神经网络的方式确定 DDoS 攻击行为^[4]。Mousavi S M 利用 SDN 控制器收到的请求分组进行熵值计算,可以快速地检测到网络中的异常行为^[5]。Hu 等人提出一个运行在 SDN 交换机和控制器之上的入侵检测系统,引入一个超级控制器运行在所有控制器之上用来监测网络中的事件^[6]。Giotis K 主要是借助 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,通过控制器上的异常检测模块分析抽样数据分组,生成扩展的 OpenFlow 流表规则下发到数据平面,流表规则主要包含流匹配规则、流超时时间、流表项建立后匹配该流表项的数据分组个数、流表项优先级。其提出的架构包含 3 个部分,分别为:控制器,负责流信息收集;异常检测模块,负责流统计分析、异常监测、确认异常模式;异常缓解模块,负责白名单、异常消除^[7]。

然而,以上很多研究都是直接利用 SDN 控制器本身对数据平面流量进行收集处理,而 SDN 控制器只对不匹配的数据分组头进行分析,不能完整地对流经 SDN 的流

量进行监控,同时全部由控制器进行流量监测也在一定程度上增加了控制器的开销。为了缓解 SDN 控制器处理数据分组的压力,引入了一个集中式网络流量监视与异常行为分析设备,称为安全中心。同时,在连接接入网与核心网的数据平面接入设备上添加安全代理模块,用于对接入核心网的数据流进行预处理,提取网络流量熵值信息,并交由安全中心进行进一步处理和分析。对于异常流量情况,安全中心通过与 SDN 控制器协作的方式为数据平面转发设备安装流表规则,针对不同的攻击行为做出管控。

基于以上分析,本文贡献如下:

- 开发了一种基于 SDN 的异常流量检测系统;
- 提出一种 SDN 架构下,基于熵值计算和 SVM(support vector machine)分类的异常流量分类与检测方法;
- 提出一种安全中心与 SDN 中心控制器的协作机制,对发现的异常行为进行处理;
- 基于本系统,提出一种保护 SDN 中心控制器的方法。

2 SDN 下基于熵值的安全系统设计

本文基于软件定义网络和分离映射机制,提出一种 SDN 下应对 DDoS 攻击的安全性保障方法。把 SDN 分为接入网与核心网,其中,接入网连接用户终端,核心网负责数据的传输与转发。在连接接入网与核心网的接入转发设备处,通过安全代理模块对数据分组进行提取并预处理,以一定格式的流摘要信息提交给安全中心进行分析。安全中心通过流量分析检测是否发生异常行为并定位攻击类型,同时通告中心控制器做进一步的处理。系统中主要涉及的网络功能设备有:接入交换设备(带有安全代理)、中心控制器和安全中心。核心设计思想是通过安全中心与中心控制器的协作机制来对异常行为进行检测并做出相应处理方法。该系统的关键是接入转发设备中安全代理模块的设计和安全中心的设计以及安全中心与控制器之间的协作机制设计。网络拓扑结构如图 1 所示。

2.1 中心控制器设计

SDN 控制器是 SDN 的核心,相当于整个网络的大脑,掌握网络拓扑信息和网络状态信息。本系统中的中心控制器是基于 POX^[8]进行开发的。POX 开发语言是 Python,具有速度快、轻量级的特点,广泛用于实验研究中。修改 POX 之后,在控制器上开发安全解析模块,用于接收来自安全中心的异常信息进行解析,并生成防御流表规则,通过控制器下发到接入转发设备中,指示转发设备如何处理数据流。

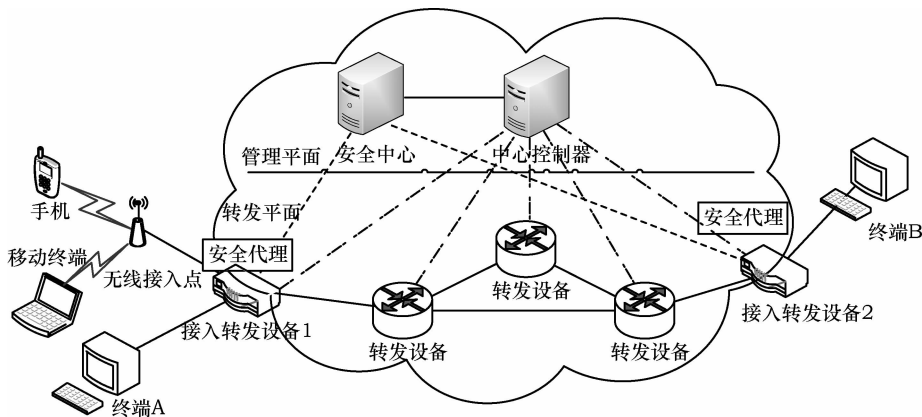


图1 一体化标识网络下控制与转发分离安全系统结构

2.2 接入转发设备设计

接入转发设备作为数据平面转发设备,兼顾数据采集和数据流转发。基于 OpenFlow 1.0.0 源码进行开发,在接入转发设备上安装安全代理模块。安全代理模块是一个网络流量监视器,它负责对所有接入转发设备收到的接入数据分组进行采集、存储等预处理工作。最终按照源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议类型和分片标识信息归类成标准流摘要信息,上报给安全中心。实现这个目的的方式有很多,如 NetFlow、sFlow、IPFIX^[9]等。它们之间的比较见表 1。

NetFlow 是一种基于软件的技术,而 sFlow 则采用内置在硬件中的专用芯片,这种做法消除了路由器或交换机的 CPU 和内存的负担。但是实际开发中,采用同样是软件形式的 IPFIX 进行开发,IPFIX 基于 NetFlow V9 进行开发,已经成为 IETF 的标准规范之一。

此外,修改接入转发设备,添加异常隔离机制,即当接入转发设备短时间内收到没有匹配的数据分组超过一定阈值时,停止向控制器发送请求,而交给安全中心进行流量分析,尽可能地减缓中心控制器的负载。

2.3 安全中心设计

安全中心是一个集中式网络攻击探测器和异常行为分析服务器。它可以通过安全代理上传的流摘要信息分析网络流量,监视网络行为是否出现异常。安全中心通过

SVM 算法^[10]预先训练好不同攻击类型流量的训练集,针对特定类型的安全威胁进行模式匹配,确定攻击行为与威胁程度,然后通过设定好的阈值来判断是否通报控制器以及命令控制器如何处理。对于确定需要处理的异常行为和攻击行为,安全中心通过特定接口发送防御指令给中心控制器的安全解析模块,安全解析模块解析防御指令并生成相应的流表规则,指定动作下发给数据平面设备,对异常流量进行处理。

2.4 系统工作流程

整个系统的工作过程如图 2 所示。

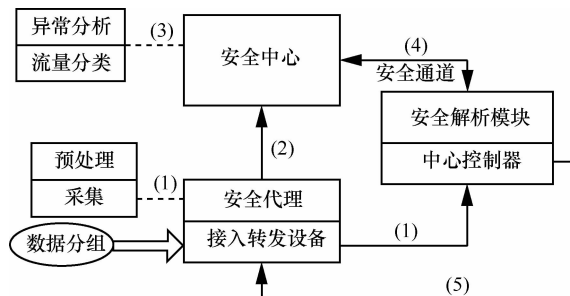


图2 安全系统异常检测与防御流程

当接入转发设备收到一系列数据分组时,将触发以下处理过程。

(1)接入转发设备向中心控制器发送携带接入标识的数据分组头信息,请求去往目的地的转发规则。同时安全代理采集接入转发设备上收到的数据分组,对其进行预处理

表 1 各种网络流量监控方式比较

名称	代表厂商	版本	主要特点
NetFlow	Cisco	V1、V5、V7、V8、V9	应用最广泛,衍生版本最多
sFlow	HP、NEC、Open vSwitch	V4、V5	实时性较强,具备突出的第 2~7 层信息描述能力
CFlowd	Juniper	V5、V8	应用厂商较少
NetStream	华为	V5、V8、V9	与 NetFlow 类似
IPFIX	IETF 标准	RFC3917	以 NetFlow V9 为蓝本衍生,成为 IETF 标准

理,按照五元组进行分类,生成流摘要信息。

(2)安全代理以一定的窗口值将流摘要信息输出给安全中心。

(3)安全中心汇总存储模块数据库中的流量记录,按照设定的窗口值进行样本划分后,进行熵值变换,得到熵值向量组,用熵值数值大小来直观表示网络带宽的波动状况。

(4)安全中心通过流量分析结果,定期通告 SDN 控制器网络状态。若发生异常,则立即根据分析结果确定攻击类型和防御手段,并反馈给中心控制器的安全解析模块。

(5)中心控制器中的安全解析模块解析防御手段并生成流表规则,对接入数据流进行相应处理。

安全中心通过将各个接入转发设备中的安全代理商收集到的流摘要信息按一定数量进行分组,对每一组的流摘要信息中的信息熵值进行计算来分析攻击类型:相同的 IP 地址或端口号出现次数越多,则其中包含的信息量越低,熵值越低;反之,若出现大量不同的 IP 地址或端口号,则其中包含的信息量越高,熵值也越高。安全应用通过分析熵值向量特点,与不同的攻击模型进行匹配,最后得出攻击类型信息,同时生成攻击者与被攻击者的相关信息,通过特定数据结构的数据分组反馈给中心控制器中的安全解析模块。

3 安全系统对网络攻击的检测与处理

系统对网络中异常流量的检测方式主要有两种:基于异常映射请求的攻击检测与基于安全中心流量分析的攻击检测。其中,基于映射请求的异常检测主要针对 DDOS 攻击,能够在攻击发生之前预测到即将发生的攻击行为,但是具有局限性;而基于安全中心对流量进行分析的检测方法能在攻击发生之后很短的时间内检测到异常流量,做出反应,可以应对的攻击方式更为丰富。在系统设计中,采用熵值计算的方式对异常流量进行检测。众多研究表明,网络流量中的 IP 地址、端口号与协议类型等属性在分布特征上表现出较强的自相似特性和重尾特性^[1],正常流量和异常流量的各个属性在分布特征上存在明显的差异。因此,可以将信息熵应用于异常检测,用熵值量化网络流量的不同属性。将网络信息流中某个属性 X 的特征值记为 N (出现了 N 个不同结果), $X=\{n_i, i=1,2,\dots,N\}$ 表示在测量数据中特征值 i 出现了 n_i 次, $S=\sum_{i=1}^N n_i$ 表示特征值出现的总

次数,这样就可以计算这个信息流中属性 X 的信息熵:

$$H(X)=-\sum_{i=1}^N \left(\frac{n_i}{S}\right) \ln\left(\frac{n_i}{S}\right) \quad (1)$$

3.1 基于安全中心的异常行为分析机制

(1)数据流采集过程

首先,接入转发设备上的安全代理模块采集数据分组,将数据分组放置在循环队列中,并对数据分组按照关键字段进行预处理,提取源 IP 地址、目的 IP 地址、源端口、目的端口、协议类型和同一源 IP 地址出现次数信息,整理为数据流的格式,传送到等待队列中。数据流依照 IETF 标准中的 IPFIX 模板。一旦等待队列装满,安全代理立即把整理过的数据流发送给安全中心进行分析处理。

(2)流量的熵值量化方法

安全中心从分布在接入转发设备上的安全代理模块收集数据分组,将捕获到的数据分组按照接收时间顺序以每 m 个数据分组为单位划分为一个子集,并规定其为单位流量,记为 $S_i=\{S_{i1}, S_{i2}, \dots, S_{im}\}, S_i \in D$ 。然后选取源接入标识、目的接入标识、协议类型、源端口和目的端口五元组属性,并统计每个流中数据分组个数,随后安全代理发送这些流摘要信息给安全中心进行处理。

安全中心分别计算单位流量在这些属性上的熵值。以源 IP 地址为例, N 为单位流量 S 中出现的不同的源 IP 地址的个数, $n_i(i=1,\dots,N)$ 代表不同的源 IP 地址分别出现的次数,则 $S=\sum_{i=1}^N n_i=m$,代入信息熵的定义公式即可得到单位流量源 IP 地址的熵值。

(3)流量模型训练

在异常流量检测系统中,需要一定数量的训练样本来建立正常或异常流量模型^[12]。在实际网络环境中,获得所需的数据并不容易,采集得到的数据源往往具有维数高、样本数小等问题^[13]。与其他分类算法相比,SVM 可以更好地解决小样本、非线性、高维数等问题,因此非常适合被应用于异常检测系统中^[10]。基于 SVM 算法,首先模拟正常流量,建立相应的正常流量模型作为参考模型。然后针对一些不同的攻击情况,模拟不同的攻击流量,同样采用 SVM 算法建立对应不同攻击的异常流量模型。

(4)异常流量检测

正常情况下,单位流量的五元组(源接入标识、目的接入标识、源端口、目的端口和协议类型)熵值较为稳定,不同比例和各种类别的异常流量在熵值上变化明显。由于异



常流量改变了网络流量的微观结构和重尾分布特征,必然使得单位流量的平均信息熵值出现大幅度变化,因此对各种流量进行异常检测可以转化为对熵值的分类。

用计算出的信息熵值向量,与安全中心中各种攻击流量模型进行熵值匹配,确定攻击类型。常见的异常流量对应的攻击类型有 DoS、DDoS、端口扫描等。相对于正常流量,端口扫描异常流量的目的 IP 地址更集中,目的端口更分散,因此目的 IP 地址熵值较小,目的端口熵值较大;而 DDoS 攻击者会雇佣大量的僵尸主机,并且采用 IP 地址欺骗机制,使得源 IP 地址会比较分散,因此 DDoS 攻击下异常流量的源 IP 地址熵值较大,而目的 IP 地址熵值较小。

3.2 系统对中心控制器的保护机制

在 SDN 中,控制器作为网络的大脑起着至关重要的作用。当网络状态产生异常时,攻击者会向交换机发送大量没有匹配的数据分组。此时,如果控制器响应来自交换机的流表请求,则很容易造成控制器负载过高,甚至瘫痪。系统提出一种针对接入转发设备的流量隔离机制,即当接入转发设备短时间内收到大量没有匹配的数据分组时,中断向控制器发起不匹配请求,而是先把流量通过安全代理转发给安全中心进行流量分析。如果判断产生攻击,安全中心就把关键参数通过安全通道发送给中心控制器,实现对异常流量的限制,从而达到保护中心控制器的目的。

3.3 安全防御流表的生成机制

利用 SDN 集中控制的特性,可以方便地由控制器下发流匹配策略,从而实现对异常主机发生数据分组进行丢弃的效果。在整个系统正常工作时,安全中心的数据库对流量样本进行存储,当通过熵值计算检测到异常行为时,安全中心需要查询数据库中相应样本,提取攻击关键信息通告给中心控制器。定义并设计了一个用于安全中心与中心控制器通信的安全通道,安全通道采用类似 OpenFlow 中安全通道的 TLS 加密机制。安全中心以定义好格式的数据分组通知中心控制器中安全解析模块。数据分组中主要包含攻击类型、协议类型、攻击者的 IP 地址(列表)及端口、被攻击者 IP 地址及端口等信息。

中心控制器中的安全解析模块收到该数据分组后,首先匹配攻击类型,然后根据数据分组中的信息生成流表规则,规定匹配项和动作来对异常流量进行处理,从而可以定向地为相应的接入转发设备配置流表。根据目前 OpenFlow 协议规定的动作类型,把规则设置为简单的丢弃数据分组。

在系统实际开发中,对每个样本进行熵值计算,如果连续 5 个样本出现熵值异常,安全中心就判断发生攻击(在实际测试中发现,当样本容量为 100 时,选取 4~5 个连续样本会大大降低误报率)。随后,安全中心提取这 5 个样本中的关键信息,针对 DDoS 攻击,设置样本容量为 100,从数据库中选取连续 5 个样本的数据。把发送给同一目的 IP 地址超过 3 次的源 IP 地址条目认定为攻击者,发送给中心控制器。中心控制器根据这些信息生成流规则,匹配攻击者 IP 地址,设定动作为丢弃数据分组,实现在一定时间范围内,限制攻击 IP 地址的接入的目的。

4 实验验证

4.1 实验拓扑

测试拓扑包含一台中心控制器、一台接入转发设备、一台安全中心和用户网络。连接情况如图 3 所示,其中,安全中心与中心控制器直连,安全代理安装在接入转发设备上与安全中心连接。

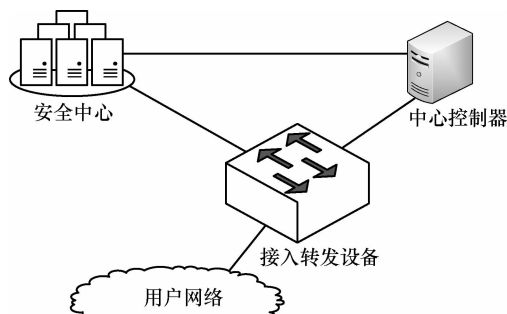


图 3 实验拓扑

4.2 流量生成

实验中,通过实验室网络出口链路数据分组的方式获取正常流量;使用 Scapy^[14]来模拟端口扫描、网络扫描、DoS 和 DDoS 等几种常见的攻击流量。Scapy 是用 Python 语言编写的一个功能强大的交互式数据分组处理程序,可用来发送、嗅探、解析和伪造网络数据分组,常常被用到网络攻击和测试中。在实验中,使用 Scapy 生成 UDP 分组并伪造其源或目的地址。采用一对其余 SVM 多分类器对正常和异常流量进行训练。

4.3 阈值设定

实际测试中,针对正常流量和 DDoS 攻击流量分别进行训练,选取 100 作为样本窗口大小,分别测试 100 个样本算出平均训练集。窗口大小应该根据实际网络状况进行设置,窗口值越大测得的熵值范围越大,精确度也就越高,

但是同时,窗口越大,所用时间就会更长,CPU 使用率就会更高。由于采用独立的安全中心进行流量分析,因此很大程度上降低了中心控制器的开销。考虑到测试网络的规模,以 100 作为窗口值,兼顾速度与准确度。将捕获到的数据分组按照时间顺序划分为不同的样本。针对 DDoS 攻击下目的接入标识熵值进行计算,并与正常流量进行比较,见表 2。

表 2 25% DDoS 攻击流量时,目的接入标识熵值计算

目的接入标识	正常流量	25% DDoS 攻击流量
平均熵值	1.523	1.322
标准差	0.010	0.016
置信区间	[-0.003 2, +0.003 2] [-0.005 4, +0.005 4]	
正常流量最小值与异常流量最大值之间差值	1.519 8-1.327 4=0.192 4	
阈值	1.33	

4.4 性能分析

由表 2 可知,在 DDoS 攻击流量占全部流量 25%时,异常流量目的接入标识熵值最大值为 1.327 4,设置阈值为 1.33 稍大于这个值,这样会有最低的误报率。当有连续 5 个样本的目的 IP 地址熵值低于这个阈值,即产生攻击检测警报。接下来又测试了 DDoS 攻击流量占全部流量 50%和 75%的情况,随着 DDoS 攻击流量占比的增加,异常流量熵值与正常流量熵值差别越来越明显,这样检测率会提升,精度会越来越高,误报率越来越低。

另外需要关注的一个性能指标就是检测时间。检测时间取决于多个参数,如分类算法的选取、样本容量大小、CPU 处理能力等。采用 SVM 分类算法,在保证检测率的前提下,考虑样本值为 100,连续 5 个样本均低于设定阈值才触发流量异常的情境,通过 10 次测试测得,检测时间主要在 5~7 s 的范围。因此基于此方法,在攻击发生时系统可以很快地检测出异常。

最后分析了 SDN 中心控制器的开销,在处理正常流量的情况下,测得 SDN 控制器的 CPU 使用率在 30%左右。基于流量隔离机制,在大量没有匹配数据分组到达接入转发设备的时候,接入转发设备不会把数据分组转发给控制器,因此中心控制器不会突然变成高负载状态。仅在安全中心通知中心控制器攻击事件时,由于控制器上安全解析模块需要工作,解析消息并生产防御流表规则,这时的 CPU 使用率会达到 40%。整体来看,中心控制器的开销并没有很大的变化。

5 结束语

本文提出一种在 SDN 中异常流量检测方法。为了提高检测效率,引入了安全中心的概念,对接入网络用户进行行为监测与流量分析。安全中心上面利用 SVM 算法对不同的攻击行为的流量进行分类,对流入网络的流量进行模型匹配,定位攻击类型。随后安全中心通过对数据库中攻击流量样本进行分析,提取攻击关键信息,并反馈给 SDN 控制器进行处理。中心控制器中的安全分析模块根据安全中心通报的消息中的参数生成流表规则,下发给数据平面转发设备,对数据流进行处理。通过这种手段可以动态灵活地对攻击行为进行限制。在接下来的工作中,将重点研究中心控制器流表规则下发机制,使中心控制器通过接收到的攻击参数能够更准确、更有效地遏制攻击者的行为。

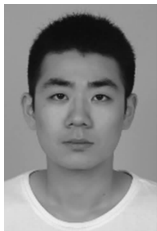
参考文献

- 1 Open Networking Foundation. Software-Defined Networking: the New Norm for Networks, 2012
- 2 McKeown N, Anderson T, Balakrishnan H, *et al.* OpenFlow: enabling innovation in campus networks. *Computer Communication Review*, 2008, 38(2): 69~74
- 3 ONF. OpenFlow Switch Specification 1.3.4, 2014
- 4 Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. *Proceedings of IEEE 35th Conference on Local Computer Networks (LCN)*, Denver, Colorado, USA, 2010: 408~415
- 5 Mousavi S M, St-Hilaire M. Early detection of DDoS attacks against SDN controllers. *Proceedings of 2015 International Conference on Computing, Networking and Communications (ICNC)*, Ottawa, Canada, 2015: 77~81
- 6 Su W, Wu L, Huang Y, *et al.* Design of event-based intrusion detection system on OpenFlow network. *Proceedings of IEEE International Conference on Dependable Systems and Networks (SDN)*, Budapest, Hungary, 2013: 1~2
- 7 Giotis K, Argyropoulos C, Androulidakis G, *et al.* Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Computer Networks*, 2014(62): 122~136
- 8 POX . <http://www.noxrepo.org/pox/about-pox/>, 2015
- 9 Hofstede R, Celeda P, Trammell B, *et al.* Flow monitoring explained: from packet capture to data analysis with NetFlow and IPFIX. *IEEE Communications Surveys and Tutorials*, 2014, 16(4): 2037~2064



- 10 Denning D E. An intrusion-detection model. IEEE Transactions on Software Engineering, 1987, 13(2): 222~232
- 11 Lakhina A, Crovella M, Diot C. Mining anomalies using traffic feature distributions. Proceedings of ACM SIGCOMM, Philadelphia, PA, USA, 2005: 217~228
- 12 陈小辉. 基于数据挖掘算法的入侵检测方法. 计算机工程, 2010, 36(17): 72~76
Chen X H. Intrusion detection method based on data mining algorithm. Computer Engineering, 2010, 36(17): 72~76
- 13 杜强, 孙敏. 基于改进聚类分析算法的入侵检测系统研究. 计算机工程与应用, 2011, 47(11): 106~108
Du Q, Sun M. Intrusion detection system based on improved clustering algorithm. Computer Engineering and Applications, 2011, 47(11): 106~108
- 14 Scapy. <http://www.secdev.org/projects/scapy>, 2014

[作者简介]



王铭鑫,男,北京交通大学电子信息工程学院博士生,主要研究方向为互联网体系结构、移动互联网、网络安全。



周华春,男,博士,北京交通大学电子信息工程学院教授、博士生导师,主要研究方向为互联网结构、移动互联网、移动和安全计算、路由协议、网络管理技术和数据库应用,主持国家“863”计划课题、“新一代宽带无线移动通信网”国家科技重大专项课题、国家自然科学基金项目多项,发表论文 50 余篇,授权发明专利共 18 项。



陈佳,女,博士,北京交通大学电子信息工程学院副教授,主要研究方向为互联网体系架构研究、路由技术、移动互联网。



张宏科,男,博士,北京交通大学电子信息工程学院教授、博士生导师,作为首席科学家主持国家“973”计划项目“智慧协同网络理论基础研究”的研究工作,主要研究方向为下一代信息网络关键理论与技术。