Atlantic : a framework for anomaly traffic detection, classification, and mitigation in SDN

security

Silva A S D . Atlantic : a framework for anomaly traffic detection, classification, and mitigation in SDN[C]// Network Operations & Management Symposium. IEEE, 2016.

本文提出一个架构用于在SDN中的异常检测与缓解，架构分为两个阶段：检测异常（利用Entropy），分类流（Machine Learning）,并提供了实现的源码。源码下载，这个人的github里只有这一个代码项目....下面详细记录这篇文章。

framework

本架构由lightweighted 和 heavyweight 两部分组成

A. Framework requirements

本段讲解一个架构需要哪些特性、

- 检索网络信息
- 网络管理员可干预该框架
- 可灵活地对网络进行配置

Lightweight and Heavyweight Process

基本架构图如图1

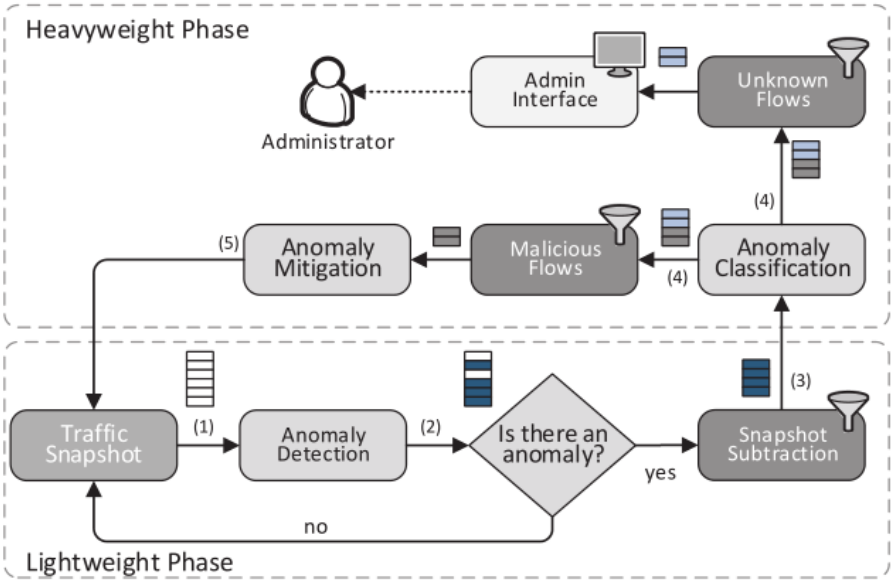


Fig. 1. Framework management process

Lightweight Processing Phase

使用控制平面获得当前流的一个快照（箭头1），并通过计算熵计算得到可疑流（箭头2）移交到下一步（箭头3）。

Heavyweight Processing phase

利用ML方式对流进行分类：benign,malicious,unknow，对malicious:mitigation操作，unknow:收集信息便于以后处理，最后要返回监督阶段。

Anomaly Traffic Classification

分类架构如图2所示

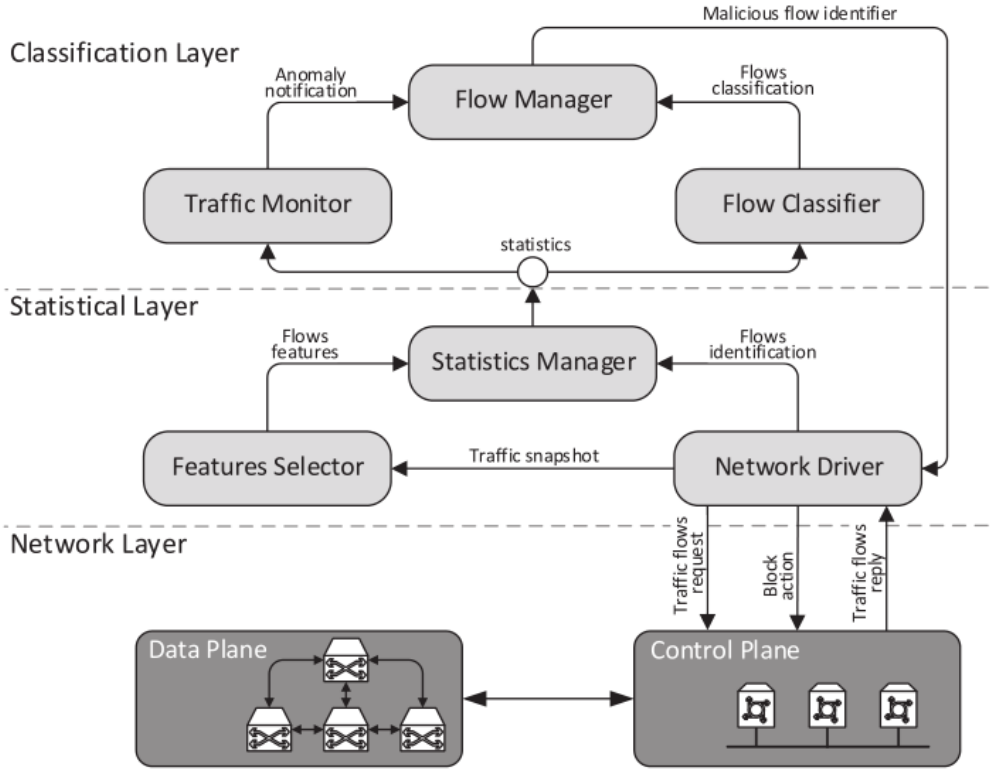


Fig. 2. Overview of the anomaly classification framework

由两层构成：statistical layer和classification Layer
统计层由：statcitics Manager,Features Selector,Network Driver 组成，分类层由:Anomaly Monitor,Flow Classifier,Flow Manager组成。

- Network Driver:获取流信息，并以流ID为标记，flow id 定义为：（ srcip,dstip,srcport,dstport,protocol ）
- Feature Selector：抽取特征：这些特征最好是可以区分流，且计算代价又小的特征
- Statistics Manager:总结由Feature Selector和Network Driver收集到数据的特征，如：mean,standard deviation,coefficient of variance,minimun value,maxmum,value。
- Anomaly Monitor:计算熵(根据IP或端口号，因为这些对找到DDoS攻击很有效)并找到异常流。假设计算的熵是E，平均熵中M，标准差是S，则正常流判定的根据是：[M-S，M+S]
- Flow Classifier:对统计到的流特征进行分类，使用K-means进行聚类分类，再使用SVM对每个类进行类别判别，这两个方法的结果可以互补。
- Flow Manager:对鉴别的恶意流作进一步处理：丢弃或交给其他组件。

Framewrok Evaluation

TABLE I
BACKGROUND TRAFFIC PROFILE USED IN THE EXPERIMENTS

Parameter	Value
Number of hosts	100
Number of switches	11
Number of servers	2 (HTTP and Streaming)
Number of attack flows	3500
Traffic profile	Video: 75 %, Web: 25 %
Host behavior Web Server	Exponential Distribution ($\lambda = 0.033$,mean = 30 s)
Host behavior Video Stream	Lognormal Distribution ($\mu = 11.75$,mean = 324 KB)

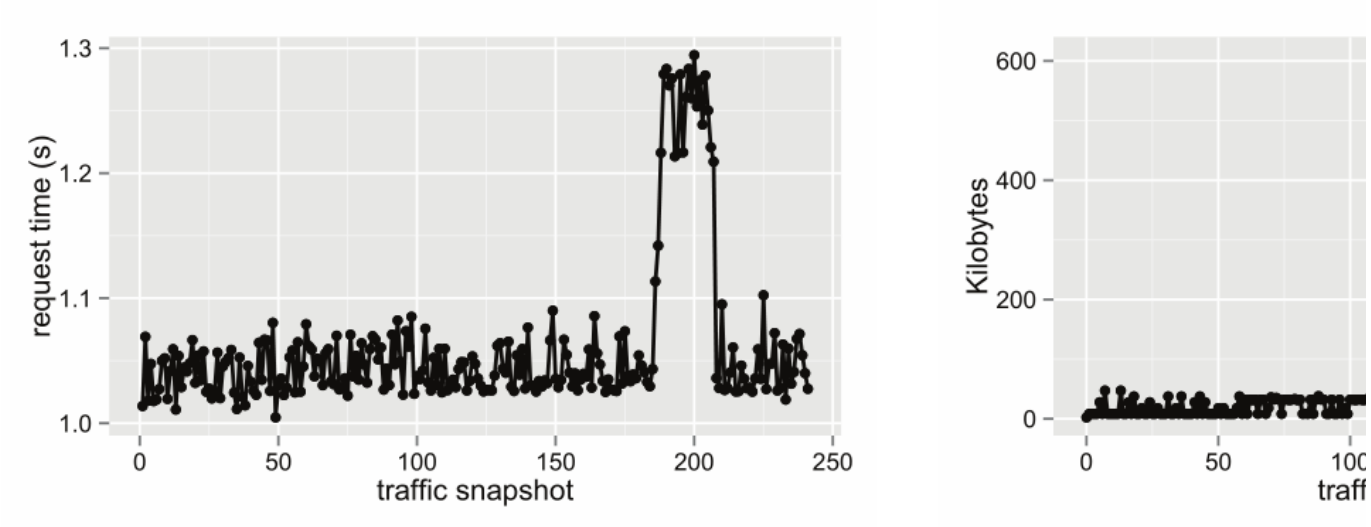
使用校园网络拓扑，基本设备情误解见表1,要评估的问题有：lightweight价段性能，heavyweight 阶段性能，分类准确率。模拟攻击的工具

为scapy tool。模拟的攻击有：

- Port scanning:被打开的端口可以用来传播儒虫。
- DDoS attack。

lightweight Anomaly Detection Evalutation

评估内存和处理时间，启动框架并监控所需要的内存和处理时间，如图3a和3b所示，大概在180间隔时启动DDoS。



(a) Traffic snapshot requesting time (b) Traffic snap

Fig. 3. Resources usage to request and store a traffic snapshot

图4为计算熵所需的时间随流数增加的情况：

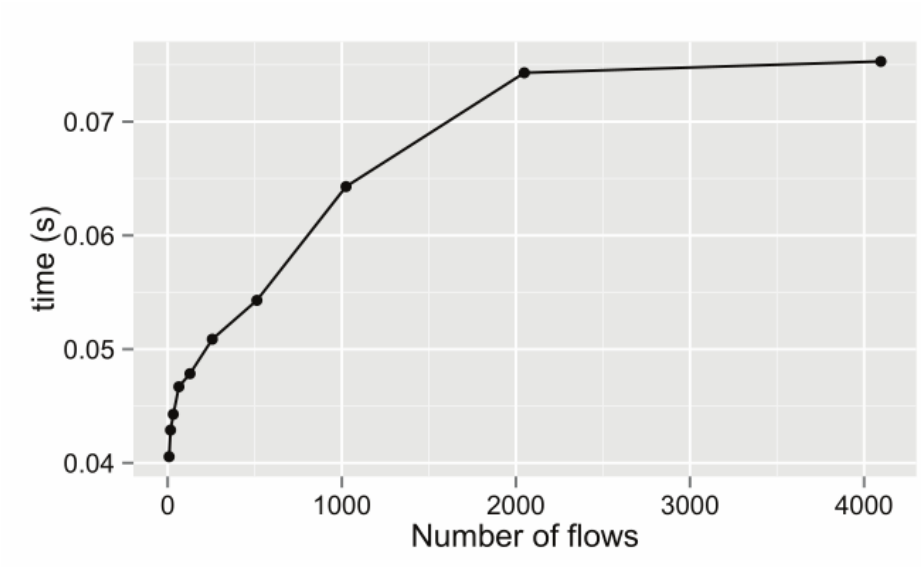
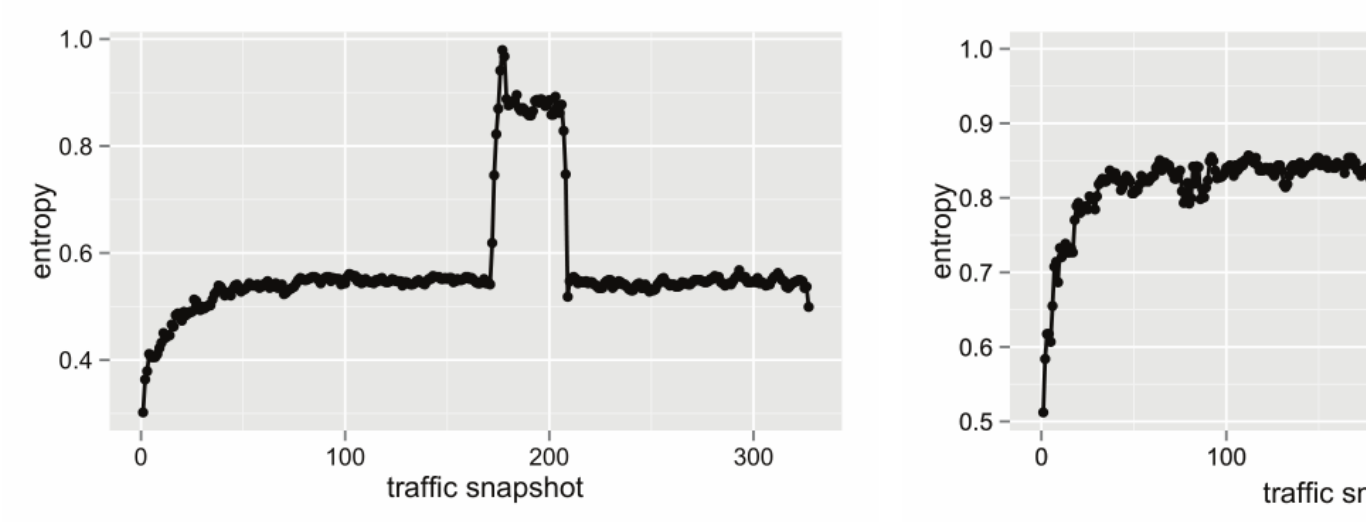


Fig. 4. Processing time of entropy calculation

图5a，5b为异常发生时熵变化情况

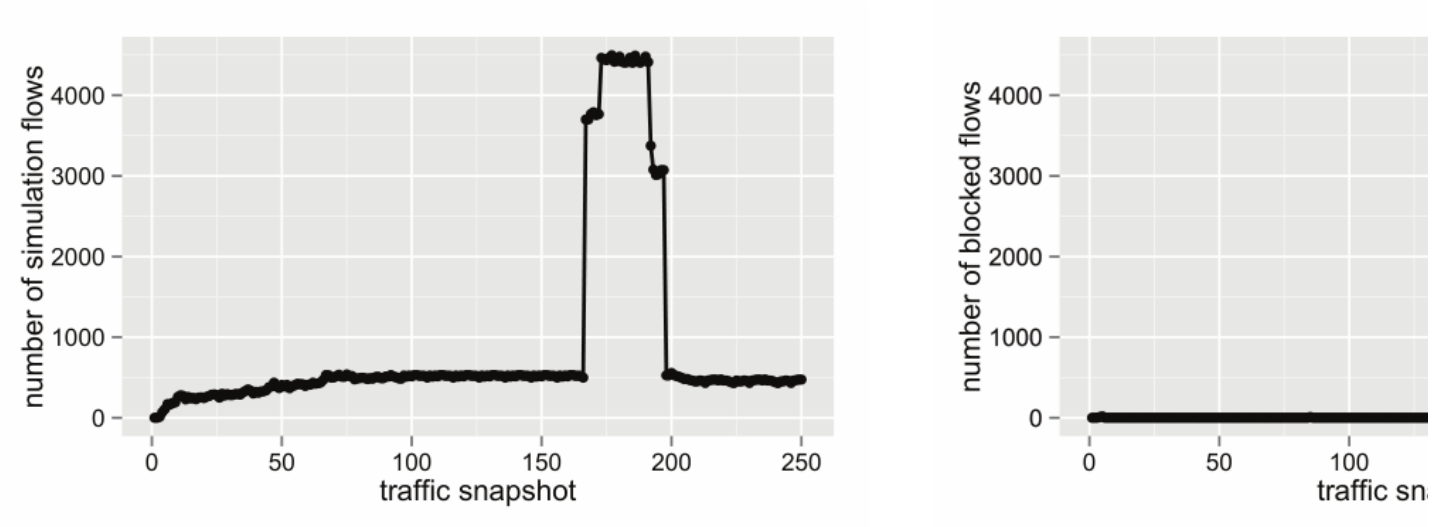


(a) Destination port entropy in the port scanning scenario. (b) Destination IP entropy in

Fig. 5. Entropy observed including benign and malicious flow

heavyweight Anomaly classification evaluation

当熵产生变化超过一定值，即进入本阶段，首先是根据当前流量进行流分类，利用K-means聚类，并使用SVM分类，图6展示在攻击发生时活越流数和被阻塞流数



(a) Overall flows (b) Blocked f

Fig. 6. Number of simulation flows

图7为SVM分类评估指标柱状图

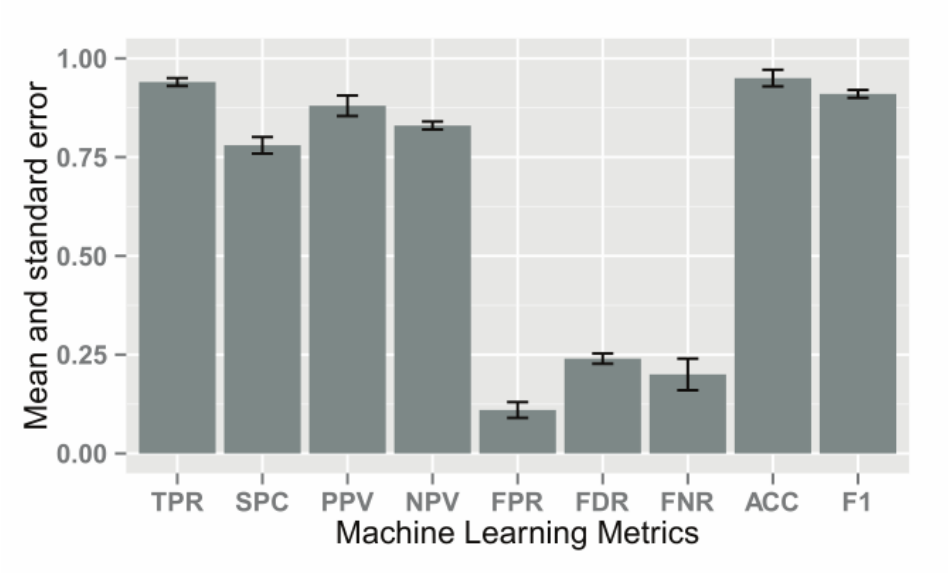


Fig. 7. Machine Learning metrics for SVM

当找到异常流时就得用Flow Manager进行阻断
图8为heavyweight阶段所花时间随流数变化的情况。

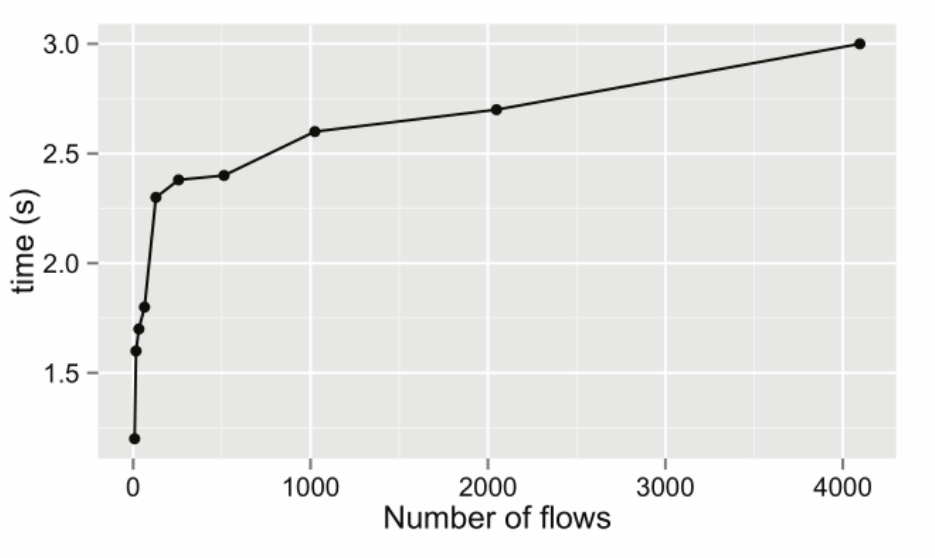


Fig. 8. Processing time of Heavyweight Phase