DDoS检测

1、原因：

（1）如果某交换机收到大量不能与规则匹配的数据包，交换机就会默认转发给控制器，造成控制器瘫痪。=》SDN网络特有

（2）交换机收到大量数据包，也会瘫痪。

（3）SYN泛洪、端口扫描、蠕虫传播等

--》了解DDoS种类

2、原理：

（1）攻击者发送的数据包十分相似，即异常流量的熵值小

（2）目的IP和端口一般固定

3、不足：

（1）使用范围有限，只能检测流量异常，很难确定在什么位置

（2）在检测出异常之后，要采用有效、快速的缓解方法

4、检测方法：

4.1基于熵

（1）收集正常流量数据：

利用流表的优势（流表中本身有一个字段为statistic），在正常通信过程中收集

数据集

？如何实现

--》取样

--》特征抽取（五元组）：人工/ PCA

（2）计算正常流量熵值：

不同属性的不同值出现的次数/总数据包（一/多个属性）

总数据包数量：一个时间段/固定数据包数量

【参PacketScore:Statistics-based overload control against distributed denial-of-service attacks】

？如何确定总数包数量（过多/过少均不行）=》实验

--》归一化

（3）收集当前流量数据：

通信过程中收集

（4）计算当前流量熵值：同于上

（5）对比两次熵值：

如果超过一个阈值，则发生了流量异常；否则没有。

？阈值要如何确定

1. 缓解异常：

更新交换机中的规则

管理员手动参与

4.2基于机器学习

1. 利用数据集进行训练

有监督：已知攻击

无监督：新型攻击

（2）特征提取

（3）对当前流量进行分类

（4）缓解异常

4.3两者结合

熵值计算用于检测异常，机器学习用于分类、处理异常。