

202301 学期《软件定义网络》大作业

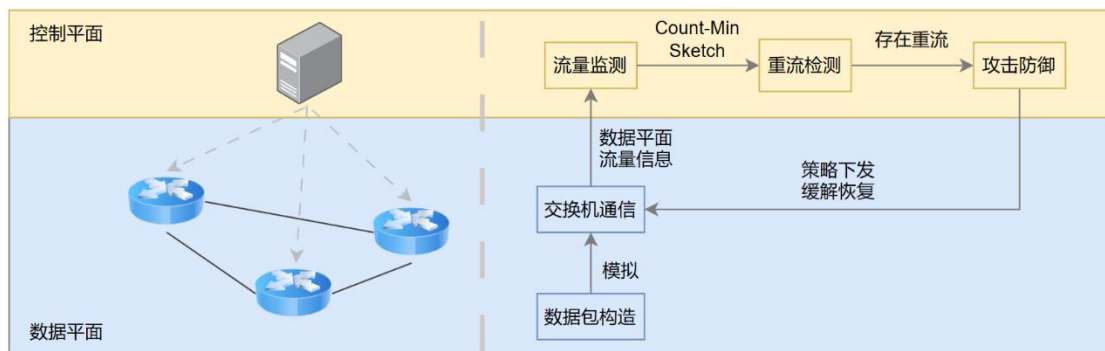
一、作业内容

1. 背景

你是一名校园网络管理员，你所在的校园网数据中心机房刚刚完成 SDN 的架构改造，但是时常收到师生反馈关于网络速度不稳定的问题。学校领导高度重视这个问题，要求你排查出影响网络速度的根本问题。

请以小组为单位，基于 SDN 的全局控制，利用开源控制器(推荐 ODL 或 Ryu)，实现一个校园 SDN 网络的管理和测量分析。

2. 内容



任务总览

2.1 拓扑搭建（必做）

初始拓扑结构见附件，从拓扑1到拓扑3实现难度逐渐增加，任选一个拓扑，在这个拓扑的基础上完成本次大作业的所有功能。

2.2 网络测量（1、2 必做，3、4 选做）

- 1) 数据包构造：自学 Scapy 工具实现自定义数据包构造，并根据选定的拓扑构造相应的数据包，形成如附件 **traces** 的网络流量包（至少构造三台交换机间通信的数据包，数据包的源目的地址、端口等信息在拓扑中有对应）。
- 2) 流量统计：自学 Count-Min Sketch，实现 Count-Min Sketch 并估计 1) 中所构造的网络流量包中每个流的出现次数（以相同五元组标记一条流，即若数据包 A 和 B 具有相同的源 IP、目的 IP、源端口、目的端口、传输层协议，则它们属于同一条流）。在完成流频率的估计后，请将估计结果与你构造的数据集内流频率的精确值进行比较并分析：用 Count-Min Sketch 估计流量是否准确？在什么情况下用 Count-Min Sketch 估计流量准确？（可构造多个不同特征（可以从 **Count-Min Sketch** 解决的问题出发考虑）的数据包进行测试，以得出全面的结论）

（注：可用精确率(Precision)、准确率(Accuracy)、召回率(Recall)、F1-Score 等数据评估预测结果）

- 3) 真实流量的测量分析：基于真实流量（附件中的 traces 文件），测量判断是否存在 Heavy Hitter（重流，即网络中占用大量带宽或资源的特定数据流或数据包，本作业中指出出现次数最多的数据流），并找到出现次数最多的 k 条流（Top-k 问题），k 的具体数值可自行选择。
- 4) 若检测到重流，实现相应的防御策略（如拦截端口，修改流表等）。

2.3 系统集成（根据 2.2 中的完成情况实现）

实现基于 web 的前端界面，展示网络情况，并向用户提供网络监测功能，要求：

- 1) 拓扑查看：获取现有拓扑的完整视图；
- 2) 流量统计：运用 Count-Min Sketch 或其他网络测量算法，粗略估计网络中各条流的出现次数（网络流量包由 2.2（1）生成，要求与实际拓扑相对应）；
- 3) 安全预警：运用 Count-Min Sketch 或其他网络测量算法，实现 Heavy Hitter（重流）检测，检测后的预警信息展示在 Web 前端（要求生成的流量包存在 Heavy Hitter）；
- 4) 流量分析：展示出现次数最多的 k 条流量（Top-k），k 的具体值由用户输入指定；
- 5) 安全防御：实现 Heavy Hitter 攻击防御，防御措施实施后，相关预警信息消失，前端呈现正常的网络状态。

二、作业要求

1. 5~6 人/组，分工完成，每个人都要有实际的工作量，不得只是资料收集、整理文档、视频制作；
2. 课程结束时必须提交设计文档（模板见参考资料）、完整源代码和部署方法、作品视频（要求 mp4 格式，10 分钟以内），可选提交在线演示链接；
3. 作业应充分体现 SDN 架构思想、技术选型、编程框架及业务流程；
4. 文档提供模板，内容必须规范，以 PDF 格式提交。
5. 截止时间：详见课程中心作业
6. 提交方式：按“2023FZUSDN_第 x 小组_题目_组长姓名”压缩打包命名(x=01, 02, 03, ..., 10, 11, ...), 上传课程中心, 文件命名不规范将扣分。