抓包进展汇报

目前进度

- Ipv4 抓包程序的开发（保存为pcap文件格式）
- 包特征的提取（包头的所有基本信息）
- 地址匿名化处理（暂定Crypto-PAn.1.0）
- 机器学习算法选取（K-means、DBSCAN、Auto-Class）

一些问题

- 抓包的数量
- 程序的性能
- 抓包环境（交换机？）
- online && offline?

短期目标

- 尽快与公司联系，开始实际环境的抓包
- 数据的处理、解析、更多的有用信息（包间隔）
- 实现多种机器学习算法并对比（Python Scikit-learn）

THANKS