doi:10.1631/FITEE.1400267

题目：基于簇流的细粒度 P2P 流量分类

目的：P2P 流量的不断增长带来网络管理和安全方面的各类问题。因此对 P2P 流量进行精确分类显得尤为重要。本文旨在提出一种能对 P2P 流量实现高效精确且细粒度分类的方法。

创新点：本文方法不依赖于对报文负载内容的检查，也无需借助复杂的统计特征和机器学习方法。仅利用网络流的几个基本属性就能实现对 P2P 流量的精确且细粒度分类。当待检测主机的网络流量组成较为复杂时，其他基于主机的流量分类方法将失效，但本文方法仍然有效。

方法：首先，将 P2P 应用产生的流量中出现最频繁且稳定的相似流簇定义为簇流，并认为一组簇流是由一类 P2P 网络活动所产生（图 2）。本文 P2P 流量分类方法分两步进行（图 3）。在簇流提取阶段，为每一种 P2P 应用采集训练流量集，并从中提取出对应的簇流集合。在流量分类阶段，监测待检测主机在单位时间窗口内所产生的簇流的类型和数量，并根据一个记分函数对流量进行分类。

结论：提出一种能对 P2P 流量实现高效精确且细粒度分类的方法。根据现实流量评价所提方法的性能。实验结果达到高于 97.22%的正确率和低于 2.78%的误报率。

关键词组：流量分类；P2P 网络；细粒度；基于主机