Contribution ID: **144** Type: **分会报告**

基于多特征融合和增量学习的未知流量识别技术

Friday, 28 June 2024 15:00 (15 minutes)

为了进行网络管理、安全监控并确保网络服务的质量，对互联网流量进行准确分类和识别至关重要。然而在现实世界中，许多不同种类的网络应用被定期开发和更新，产生大量在训练集流量类别之外的未知流量，这些未知的流量类型会对当前机器学习模型的准确性造成重大影响，降低流量分类的准确率。现有的未知流量分类算法无法优化流量特征，每次收集到新的流量数据时都需要对整个系统进行重新训练，导致识别效率低下，不适合实时流量检测。为解决上述问题，我们提出了一种基于多特征融合的增量学习方案来检测未知流量。该方法采用了多通道并行架构来提取流量的时间和空间特征。然后引入了 mRMR 算法对从每个通道提取的特征进行排序和融合，以克服加密流量特征冗余的问题。此外，我们结合基于密度比的聚类算法来识别未知的流量特征，并通过增量学习更新模型。分类器通过学习新获得的类知识，实现对已知和未知流量的实时分类。
我们使用公共数据集 ISCX-VPN-Tor 验证在不同场景下该模型对未知的加密隧道流量的检测能力，准确率为 86% 以上。此外，模型在入侵检测数据集 NSL-KDD 上达到了 90％以上的准确率。该工作为识别未知网络流量提供了一种新颖的方法，有助于维护网络环境的安全和稳定。

Summary

Primary authors: 刘, 君怡 (IHEP)；王佳荣, UNKNOWN；YAN, TIAN (IHEP)；齐, 法制 (高能所)；CHEN, Gang (IHEP)

Presenter: 刘, 君怡 (IHEP)

Session Classification: 人工智能与应用