通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

王一鹏1,2,3,云晓春1,3,张永铮3,李书豪3.基于主动学习和SVM方法的网络协议识别技术[J].通信学报,2013,(10):135~142

基于主动学习和SVM方法的网络协议识别技术

Network protocol identification based on activelearning and SVM algorithm

投稿时间： 2013-04-29

DOI：10.3969/j.issn.1000-436x.2013.10.016

中文关键词：网络安全 网络协议识别 主动学习 网络数据流 支持向量机

英文关键词:network security protocol identification active learning network traces support vector machine

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(2012AA012803, 2013AA014703)；国家科技支撑计划基金资助项目(2012BAH46B02)；国家自然科学基金资助项目(61303261, 61303170)

作者	单位
王一鹏1,2,3，云晓春1,3，张永铮3，李书豪3	1. 中国科学院 计算技术研究所，北京 100190；2. 中国科学院大学，北京 100049；3. 中国科学院 信息工程研究所，北京 100093

中文摘要:

针对未知网络协议数据流的获取与标记工作主要依赖于领域专家。然而，样本数据量的增加会导致人工成本超过实际负荷。提出了一种新颖的未知网络协议识别方法。该方法基于主动学习算法，仅依靠原始网络数据流的载荷部分实现对未知网络协议的有效识别。实验结果表明，采用该方法设计的识别系统在保证识别准确率和召回率的前提下，能够有效地降低学习过程中标记的样本数目，更适用于实际的网络应用环境。

英文摘要:

Obtaining qualified training data for protocol identification generally requires domain experts to be involved, which is time-consuming and laborious. A novel approach for network protocol identification based on active learning and SVM algorithm was proposed. The experimental evaluations on real-world network traces show this approach can accurately and efficiently classify the target network protocol from mixed Internet traffic, and meanwhile display a significant reduction in the number of labeled samples. Therefore, this approach can be employed as an auxiliary tool for analyzing unknown protocols in real-world environment.

查看全文 查看/发表评论 下载PDF阅读器

关闭