计算机工程 2006 32 (16): 127-129 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于One-class SVM的实时入侵检测系统

黄 谦,王 震,韦 韬,陈 昱

北京大学计算机科学技术研究所，北京 100871

收稿日期 修回日期 网络版发布日期 2006-8-14 接受日期

摘要 将One-class支持向量机和Online训练算法应用于入侵检测研究中，把入侵检测看作是一种单值分类问题，能够在有噪声的数据集中进行训练，降低了对训练集的要求，提高了检测准确性。同时解决了基于SVM的入侵检测系统实时训练的问题，在实际运用中可以实时地添加新的训练样本对新出现的攻击手段进行分类。在KDD CUP’99标准入侵检测数据集上进行实验，系统缩短了训练时间并且获得了较高的检测准确率。

关键词 信息安全 入侵检测 支持向量机

分类号

DOI:

通讯作者:

作者个人主页: 黄 谦;王 震;韦 韬;陈 昱