电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (10) :2383-2387 DOI: 10.3724/SP.J.1146.2010.00321

论文

一种基于有监督局部决策分层支持向量机的异常检测方法

徐琴珍 杨绿溪*

东南大学信息科学与工程学院 南京 210096

A Supervised Local Decision Hierachical Support Vector Machine Based Anomaly Intrusion Detection Method

Xu Qin-zhen Yang Lü-xi*

School of Information Science and Engineering, Southeast University, Nanjing 210096, China

摘要 该文针对包含多种攻击模式的高维特征空间中的异常检测问题，提出了一种基于有监督局部决策的分层支持向量机(HSVM)异常检测方法。通过HSVM的二叉树结构实现复杂异常检测问题的分而治之，即在每个中间节点上，通过信息增益准则构建有监督学习所需的训练信号，监督局部决策；在每个嵌入中间节点的二分类支持向量机(SVM)的训练过程中，以局部决策边界对特征的敏感度为依据，选择入侵检测的局部最优特征子集。实验结果表明，该文提出的异常检测方法能够在训练信号的局部决策监督下构建具有良好稳定性的检测学习模型，并能以更精简的特征信息实现检测精确率和检测效率的提高。

关键词： 异常入侵检测 分层支持向量机 特征信用度 有监督局部决策

Abstract： This paper dedicates to propose a supervised local decision Hierachical Support Vector Machine (HSVM) learning model for anomaly intrusion detection in high dimensional feature space. The binary-tree structure of HSVM presents a “divide-and-conquer” algorithm for complex anomaly intrusion detection problem, i.e., the training signal for supervising local decision at each internal node is constructed according to information gain criterion. The embedded SVMs at internal node are trained on local optimized feature subsets standing on the sensitivity degrees of a margin to features. The experimental results suggest that the proposed anomaly intrusion detection method can gain learning model with better stability under the local decision supervisal of training signals. Further, it also achieves competitive detection accuracy and higher detection efficiency with condensed feature information.

Keywords： Anomaly intrusion detection Hierachical Support Vector Machine (HSVM) Feature credit Supervised local decision

Received 2010-03-29;

本文基金:

国家自然科学基金(60702029，60902012)，国家科技重大专项(2009ZX03003-004)，国家973计划项目(2007CB310603)和东南大学科研启动费(4004001041)资助课题

通讯作者: 徐琴珍 Email: summer@seu.edu.cn

引用本文:

徐琴珍, 杨绿溪.一种基于有监督局部决策分层支持向量机的异常检测方法[J] 电子与信息学报, 2010,V32(10): 2383-2387

Xu Qin-Zhen, Yang Lu-Xi.A Supervised Local Decision Hierachical Support Vector Machine Based Anomaly Intrusion Detection Method[J] , 2010,V32(10): 2383-2387

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2010.00321 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I10/2383