信号处理 2010, 26(11) 1663-1669 DOI: ISSN: 1003-0530 CN: 11-2406/TN

算法研究

一种优化的神经网络树异常入侵检测方法

徐琴珍，杨绿溪

东南大学信息科学与工程学院；东南大学水声信号处理教育部

摘要：

本文提出了一种基于优化神经网络树(ONNT)的异常检测方法，在提高异常检测精确率的同时，增强异常检测模型学习结果的可理解性、可解释性。ONNT是一种具有二叉树结构的混合学习模型，二叉树的节点分裂遵循信息增益率准则；其中间节点嵌入了结构简单的感知器神经网络，能够根据当前节点上给定的子样本集和教师信号，选择较小的特征子集构建相对简单的局部决策曲面。本文提出的异常检测方法包括两个方面的性能优化：1）通过优化神经网络树(NNT)的中间节点，降低局部决策曲面的复杂度，从而使中间节点能在可接受的计算代价内表示成低复杂度的布尔函数或规则集，为实现学习结果的可解释性提供基础；2）通过优化学习模型的整体结构，降低所有中间节点的规则析取式的前件复杂度，从而提高学习结果的可理解性。实验的数值结果表明，与基于NNT的异常检测方法相比，本文提出的方法能够以简单的中间节点和相对精简的整体结构提高检测结果的可解释性和可理解性；与其他同类方法相比，基于ONNT的异常检测方法具有较高的检测精确率，且在一定程度上给出了对异常检测具有重大影响的一些特征信息。

关键词： 异常检测；可理解性和可解释性；优化神经网络树；混合学习模型

An Optimized Neural Network Tree Based Anomaly Intrusion Detection Method

XU Qin-Zhen, YANG Lu-Xi

School of Information Science and Engineesring,Southeast University,Nanjing; Key Lab of Underwater Acoustic Signal Processing of Ministry of Ministry of Education,Southeast University,Nanjing

Abstract:

This paper dedicates to propose an optimized neural network tree (ONNT) based anomaly detection method that is capable to improve the understandability and interpretability on the detection results of the trained learning model as well as the anomaly detection accuracy. ONNT is a binary-tree-structured hybrid learning model whose interior nodes split according to the criterion of information gain ratio. The simple perceptron neural network embedded in each interior node is trained on the current samples. A limited number of input features are selected on current samples in accordance to instruction signal for the perceptron neural network to build a local decision hyper-plane with low complexity. The proposed anomaly detection method involves two optimization items. Firstly, the complexity of local decision hyper-plane is decreased by optimizing each interior node. The trained neural network in an interior node with simple structure enables the learning result to be interpreted into low complexity Boolean functions or rule set followed by acceptable computation cost, and thereby lay a good basis for the interpretability of the learning results. Secondly, the tree structure of the learning model is optimized, i.e., the neural network tree(NNT) is pruned to condense the precondition in disjunctive description of all interior nodes, which makes the extracted rule set as understandable as possible. The experimental results compared with those of NNT based detection method suggest that the ONNT based anomaly intrusion detection method allows better understandability and interpretability on the anomaly detection results as a result of simpler structured neural network in interior nodes and reduced complexity of tree structure. The experimental results compared with those obtained by other parallel methods show that the ONNT based anomaly detection method achieves competitive recognition accuracy as well as lower false alarm rate. And what is more, the proposed anomaly detection method presents the information of those features which make greater contribution to the detection result.

Keywords: Anomaly intrusion detection understandability and interpretability Optimized neural network tree Hybrid learning model

收稿日期 2010-04-23 修回日期 2010-07-03 网络版发布日期 2010-11-25

DOI:

基金项目:

国家自然科学基金（60702029,60902012），国家科技重大专项（2009ZX03003-004），国家973项目

（2007CB310603），东南大学科研启动费(4004001041)资助课题

通讯作者:

作者简介:

作者Email: summer@seu.edu.cn

参考文献：

本刊中的类似文章

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3989