一种优化的神经网络树异常入侵检测方法

徐琴珍[1,2] 杨绿溪[1,2]
(1. 东南大学信息科学与工程学院，江苏南京 210096；2. 东南大学水声信号处理教育部重点实验室，江苏南京 210096)

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
中图分类号：TP391 **文献标识码**：A **文章编号**：1003-0530(2010)11-1663-07

An Optimized Neural Network Tree Based Anomaly Intrusion Detection Method

XU Qin-zhen[1,2] YANG Lu-xi[1,2]
(1. School of Information Science and Engineering, Southeast University, Nanjing, 210096;2. Key Lab of Underwater Acoustic Signal Processing of Ministry of Education,Southeast University, Nanjing, 210096)

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.

Key words: Anomaly intrusion detection; understandability and interpretability; Optimized neural network tree; Hybrid learning model

---

收稿日期：2010 年 4 月 23 日；修回日期：2010 年 7 月 3 日
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

1 引言

入侵检测问题的研究始于20世纪80年代,随着Internet的普及和计算机系统本身的迅猛发展,入侵检测已成为信息安全领域的重要课题,并受到越来越广泛的关注。按入侵检测的分析方法区分,网络入侵检测技术可分为滥用检测和异常检测两类。目前绝大多数商用网络入侵检测系统都采用滥用检测技术,对已知的攻击模式能实现高效检测,而对未知的攻击模式无法做出预测。异常检测技术通过建立主体的正常行为模型,发现异常行为,从而能对未知攻击作出预测。

机器学习理论的发展在很大程度上带动了异常检测技术的提高。基于机器学习的异常检测可广义地划分为两类。一类是基于符号式学习模型的异常检测方法。例如:(1)基于RIPPER的异常检测方法:Lee等提出了一种基于数据挖掘技术的RIPPER规则算法,运用关联规则算法得出特征间的关联性,运用频繁序列规则算法表达系统和网络行为的记录序列[1];Helmer等通过简单的遗传算法(GA)实现有效特征子集的选择,在此基础上结合RIPPER算法抽取检测规则集,实现异常检测,提高了检测的精确率[2]。(2)基于决策树的异常检测方法:Chebrolu等采用CART算法构建的决策树及决策树集成实现了入侵检测的特征抽取和分类[3];Cheng等提出了一种有监督决策树分类器与无监督贝叶斯聚类法相结合的入侵检测方法实现检测率的提高和误检率的下降[4];Sheen等在入侵检测训练集上抽取特征信息,构建决策树,得到入侵检测的规则集,并以规则集的检测结果衡量不同的特征抽取方法的有效性[5];Ortiz等应用决策树实现入侵检测数据挖掘,并将决策树的学习规则用于防火墙的构建[6]。

这类基于符号式学习模型的异常检测方法,在很大程度上提高了入侵检测的精确率,并且由于其每一步局部决策都有明确的易于理解的推理过程,由这些局部决策规则构建成的入侵检测规则集,在学习结果上具有较好的可理解性,但这些符号式学习模型在一定程度上难以适应在线学习的需求。

另一类是基于非符号式学习模型的异常检测方法。例如:(1)基于神经网络的入侵检测方法:Tong等提出了一种基于混合神经网络学习模型的入侵检测方法,通过RBF网络实现实时检测,由Elman网络实现知识的存储,从而实现了滥用检测技术和异常检测技术的结合[7];Thomas等从一种独特的角度将神经网络应用于入侵检测,在他们提出的算法中,通过多种检测方法的组合实现入侵检测精确率的整体优化,有监督学习的神经网络用于确定检测某种特定入侵方式的学习方法的权重,即用于衡量该方法的有效性[8];Hernández-Pereira等将符号特征数值化后,采用单层或多层的神经网络对入侵检测的特征抽取结果和检测结果进行分析[9];Herrero等提出了一种自联想反向传播神经网络和合作极大似然Hebbian模型,通过无监督学习实现入侵检测数据降维的方法,对在线流量分析实现早期异常检测,对离线流量进行模式分析实现批处理[10]。(2)基于聚类的方法:Zhong等学者研究并提出了一系列基于无监督学习的异常检测方法,例如,基于增量聚类算法的入侵检测方法,在原始聚类的基础上,通过克隆选择算法优化聚类结果[11];通过核聚类将非线性可分的检测特征空间隐式地映射到核空间,在核聚类的基础上划分出大簇小簇,而后进行不同攻击模式的分离[12];用信息熵度量整体相似度,并以此作为聚类质量的评价标准,通过凝聚层次聚类方法对已划分的簇进行合并[13]。这一系列无监督异常检测算法得到了较好的检测效果,在一定程度上降低了误警率。(3)此外,魏等学者提出了一种在线自适应网络异常检测系统模型与算法,在数据预处理阶段,采用基于网格的方法将源数据粒度化,在学习阶段构建以四元组模式为元素的模式库,在测试阶段,通过特定的距离准则计算未知访问模式与模式库中模式的距离,判定访问模式的类别,系统达到了较高的检测率和满意的误警率[14]。

以上基于非符号式学习模型的异常检测方法往往能够通过修改自由参数等途径实现在线学习,从而有利于实现异常检测策略的实时调整。然而,检测模型学习获得的知识往往是以权值或数值序列的方式记忆的,人们难以据此形成直观的推理过程,通常将此类异常检测模型视为“黑箱”。

作者在前期工作中研究了结合符号式学习模型和非符号式学习模型的优势的混合学习模型,并将之应用于异常检测,能够从学习的结果实现规则的抽取,同时可实现变化环境中的学习[15][16]。本文在此研究基础上,进一步优化嵌入中间节点的神经网络的结构,使基于该混合学习模型的异常检测方法的检测结果可解释;同时,优化神经网络树的整体结构,降低解释结果的复杂度,提高学习结果的可理解性。

2 神经网络树混合学习模型结构

Zhao等对NNT进行了早期的研究[15][16][17],学习模型的整体结构与二分叉的决策树类似(如图1所示),不同的是混合学习模型的每个中间结点上嵌入了全连接的三层前向神经网络,如图2所示。该网络的隐层和输出层神经元均采用Sigmoid输出函数。

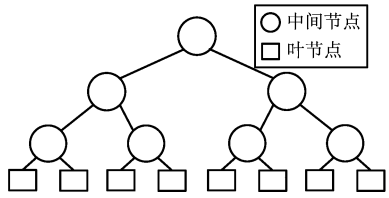

图 1　NNT 混合学习模型示例

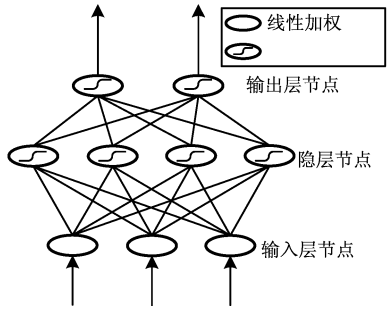

图 2　中间节点上的全连接三层感知器示例

该混合学习模型以二叉树的结构实现了复杂分类问题的分而治之,在每个中间结点上,选择合适的特征,通过嵌入的神经网络抽取特征信息,对当前样本子集实现局部决策,局部决策的有效性由信息增益率准则衡量。信息增益率准则是 C4.5 算法构建决策树过程中,各中间节点上属性(特征)选择的核心准则[18]。在 NNT 中,各中间节点上将选择 1 至多个特征构成特征子集[17],即若各维特征构成的特征集为 $F=\{x_1,x_2,\cdots,x_n\}$,n 为特征总数,则从中抽取 m 个特征构成的特征子集为 $F^*=\{x_{i_1},x_{i_2},\cdots,x_{i_m}\}$,$1\le m\le n$,$i_m\in\{1,\cdots,n\}$。给定当前节点上的样本集为 X,由 k 类模式组成:$c_1,\cdots,c_k$,则该样本集的信息熵为:

$$entro(X)=-\sum_{j=1}^{k}|c_j|/|X|\times\log_2(|c_j|/|X|) \quad (1)$$

其中 $|X|$ 表示样本集 X 中的样本总数,$|c_j|$ 表示 X 中包含的 c_j 类样本数。二叉树结构下,特征子集 F^* 将 X 划分为两个子样本集 X_1 和 X_2,则该节点上的期望信息要求为:

$$entro_{F^*}(X)=\sum_{i=1}^{2}|X_i|/|X|\times entro(X_i) \quad (2)$$

产生的信息增益为

$$gain_{F^*}(X)=entro(X)-entro_{F^*}(X) \quad (3)$$

由 F^* 将 X 划分后产生的势信息为

$$poten_{F^*}(X)=-\sum_{i=1}^{2}|X_i|/|X|\times\log_2(|X_i|/|X|) \quad (4)$$

当样本被过度细分时,信息增益会增大,而此时势信息也会随之增加,因而采用下式的信息增益率准则:

$$ratio_{F^*}(X)=gain_{F^*}(X)/poten_{F^*}(X) \quad (5)$$

可以在避免过度细分样本的同时,优化各中间节点上特征子集的选择。

3　优化的神经网络树异常入侵检测方法

二叉树本身是可解释的,要解决的的问题是:1)如何提高混合学习模型的每个中间节点的可解释性;2)如何使得解释的结果尽量简单,从而易于为人们所理解和接受。为此,我们在 Zhao 等学者的研究基础上作了进一步的优化。

3.1　中间节点的优化

纯粹的决策树学习模型是可解释的,因此在混合学习模型中,若中间节点嵌入的神经网络可解释,则混合学习模型的整体结构也能实现可解释。研究表明,从结构过于复杂的神经网络的学习结果中抽取规则是一个 NP 完全问题[19],而结构简单的神经网络可通过较小的计算代价表示成低复杂度的布尔函数或规则集,因此需要优化 NNT 的中间节点。

中间节点的优化目标为:1)优化中间节点的局部决策性能。需要优化的内容包括特征子集的选择及神经网络权值的优化。2)神经网络结构的精简。在控制神经网络输入特征子集大小的情况下,需要优化的内容为隐层节点数的控制。这是一个多目标优化问题,可以采用多目标优化遗传算法实现。染色体编码的内容为:构成特征子集的特征序号,隐节点数,输入层到隐层的权值,隐层到输出层的权值。适应度函数为 $fit(ratio_{F^*},n_{hid})$,其中 $ratio_{F^*}$ 为当前中间节点上进化群体中某个个体的信息增益率,n_{hid} 为该个体的隐层节点数,依据这两个参数对局部决策的重要性,以 Pareto 排序的方式最终产生最优个体($ratio_{F^*}$ 占排序的优先位),即选择同时具有最高信息增益率和最精简结构的神经网络作为最优个体,嵌入到当前中间节点上。

3.2　整体结构的优化

若二叉树的整体结构比较复杂(即存在冗余的子树),将导致从 NNT 中抽取的规则前件或布尔函数的复杂度过高,超出人们可接受的理解范围,从而影响入侵检测结果的可理解性;此外,过于复杂的整体结构容易对训练样本过拟合,从而影响其泛化性。因而,除了优化中间节点外,还需要优化混合学习模型的整体结构。修剪冗余子树是降低树型结构学习模型的整体复杂度、泛化学习结果的一种直接有效的途径。

在决策树学习过程中,可以通过两类途径避免训练数据的过度拟合,即及早停止树的增长和后修剪法(post-prune)[20]。前者尽管看似更直接,但往往由于很难精确判断何时停止树的增长而难以实现;后者允许树过度拟合,之后对生成的树进行后修剪,可分为规则后修剪和错误率降低修剪两种修剪方式。其中,规

则后修剪需要将学习结果转化为等价的规则集合后修剪,而将结构过于复杂的混合学习模型转化为等价的规则集合往往需要付出很高的计算代价;错误率降低修剪法是考虑将树上的每一个节点作为修剪的候选对象,选取那些删除后可以最大程度提高决策树在验证集上的精度的节点,反复修剪直至修剪有害为止。根据以上分析,混合学习模型的整体结构优化采用了错误率降低修剪法。

3.3 基于优化的神经网络树(ONNT)异常检测算法

给定异常检测训练样本集 X_{tr},验证集 X_{val},每个节点的输入特征数(即特征子集大小)n_{F^*},遗传算法的最大遗传代数 n_{gen},遗传群体的人口数 n_{pop}, 基于 ONNT 的异常检测算法的步骤如下:

1) 初始化当前节点 $initial(X_{tr}, n_{F^*}, n_{pop})$:若当前节点上的样本同属一类,则将当前节点标记为叶节点,结束当前子树的构建;否则,随机产生 n_{pop} 组数据编码(个体),每组编码内容包含随机产生的输入特征子集序号(n_{F^*} 个输入特征的序号),隐节点数 n_{hid},输入层到隐层的权值 $W_{n_{F^*}\times n_{hid}}$,隐层到输出层的权值 $V_{n_{hid}\times 2}$ 的编码。

2) 在当前节点上计算个体的适应度 $fit(ratio_{F^*}, n_{hid})$:计算个体在当前节点上的信息增益率 $ratio_{F^*}$,将所有个体的 $ratio_{F^*}$ 与对应的隐节点数 n_{hid} 进行 Pareto 排序;若排序最前的个体已经满足要求则停止进化,执行 3);否则按照一定的选择率 $ratio_{sel}$ 对排序在前的部分个体的基因进行复制(交叉、变异操作),得到新的群体,若遗传代数已达到 n_{gen},则选择群体中适应度排序最前的个体作为当前节点上嵌入的神经网络;否则,对新的群体执行步骤 2)。

3) 递归构建树型结构:运用当前节点上嵌入的神经网络将当前训练样本集划分为左右两个子集 X_{tr_l}, X_{tr_r},分别在这两个样本子集的基础上执行步骤 1)、步骤 2),递归地构建混合学习模型的左右子树,最终完成神经网络树 *NNT* 的构建。

4) 测试原始 *NNT* 在验证集上的精确率:将 *NNT* 用于测试异常检测验证集中的数据,得到未修剪情况下的原始异常检测精确率 Acc_{or}。

5) 在当前节点上修剪:若当前节点为叶节点,则修剪结束;否则,将当前节点设为叶节点,将当前节点上训练样例中占多数的一类的类别作为该叶节点的类别标签。测试修剪过的 *NNT* 在异常检测验证集上的精确率 Acc_{pr}。

6) 递归修剪当前节点的左右子树:若 $Acc_{or}<Acc_{pr}$,则保留当前节点修剪后的结构,将当前节点设为叶节点;否则,将当前节点恢复为中间节点,并对当前节点的左右子树执行步骤 5)。

4 实验结果及分析

为验证本文提出的异常检测方法,实验选择入侵检测研究广泛使用的 KDD Cup 1999 入侵检测数据库中的 *corrected* 观测数据集,该入侵检测数据库中的样本包含 41 维特征,通过对 *corrected* 标准入侵检测数据库(含 311029 例样本)中各维特征值的分布情况分析,我们剔除了第 20 维特征(*num_outbound_cmds*),该特征在 *corrected* 库中的值始终为 0,对检测结果不产生影响。实验从中随机抽取 5000 例样本,1/4 作为训练样本,1/2作为验证样本,其余作为测试样本。遗传算法参数设置为:最大遗传代数 $n_{gen}=450$,人口数为 $n_{pop}=120$,输入特征数 $n_{F^*}=3$,选择率 $ratio_{sel}=0.4$。实验给出的数值结果为 264 次实验结果的平均值。

本文实验所用的配置是四核(双核×2)CPU,工作频率为 2.4 GHz,内存为 3.48GB,Windows XP 操作系统的 PC 微机,在 visiual studio 2008 编程环境下使用 C++与 matlab 语言混合编实现。

图 3 为归一化后的特征选择频率(各维特征被选择的频率和为 1),图中标示了整体结构未优化情况下异常检测特征的归一化选择频率以及整体结构优化后异常检测特征的归一化选择频率。由于错误率降低修剪法删去了冗余的神经网络子树,降低了检测超曲面的复杂程度,剔除了一些对训练样本产生过拟合的特征信息,因此一些特征的选择频率在修剪前后有了一定程度的调整。

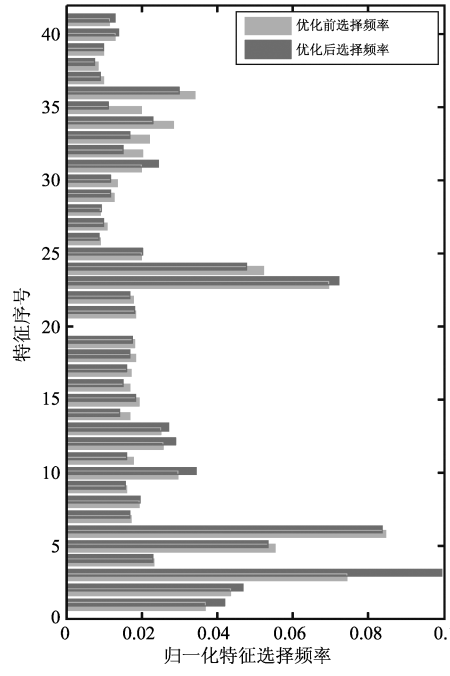

图 3 整体结构优化前后归一化特征选择频率直方图

我们以第 3 维特征和第 38 维为例,说明 ONNT 学习结果所反映的特征信息。这两维特征均具有复杂的属性值分布,如图 4(a)(b)所示。其中,第 3 维特征为具有 66 个离散值的 *service* 属性,在修剪前后,其选择频率均较高,这在一定程度上说明其多个离散值与分类规则的构建均有密切的关系;而第 38 维特征为连续特征 *dst_host_serror_rate*,尽管其取值情况对方差也有较大的贡献,但其选择频率并不高,这在一定程度上反映了该连续属性的一个或少数几个阈值与分类密切相关(具体选择的离散属性值和连续属性的阈值将在课题后期的规则抽取研究中得出结果),这说明混合模型的特征选择频率结果可以在一定程度上给出对异常检测具有重大影响的一些特征信息。

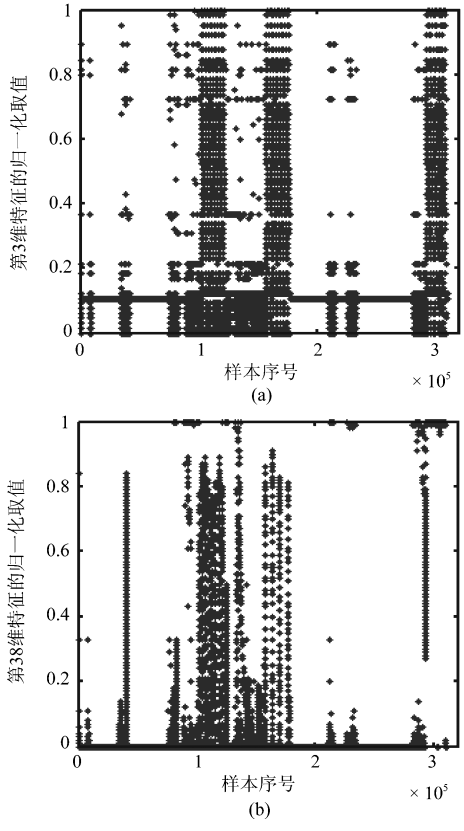

图 4　*corrected* 入侵检测数据库部分特征取值情况

实验将基于 ONNT 的异常入侵检测方法与整体结构未优化前的 NNT 的检测结果做了对比。其数值结果如表 1 所示,其中 n_{int},n_{hid},n_{in},err,far,t_{trn}和 t_{tst}分别表示每种学习模型的中间节点数,嵌入的神经网络的隐节点平均数,输入总数,测试集上的异常检测误差,虚警率,训练时间和测试时间的平均数值结果。数值对比结果说明,优化后的学习模型在整体结构上有了较大的精简(中间节点数 n_{int}降低),若学习模型能够实现规则抽取,则规则前件的析取表达式的复杂度相对于优化前将有大幅的降低,从而提高了学习结果的可理解性;中间节点的优化使得学习模型上嵌入的神经网络结构简单(平均中间节点数<4),这为每个中间节点上以可接受的计算量实现规则抽取提供了可能,为实现学习结果的可解释性提供了基础;此外,冗余子树的修剪也降低了特征输入的总数,改变了一些特征的选择频率,从另一个方面说明了规则集的简化;从检测误差和虚警率上看,与基于 NNT 的异常检测方法相比,基于 ONNT 的异常检测方法能够以更加精简的结构获得与之相当甚至更高的检测精确率和与之相当的低虚警率;从训练时间和测试的时间看,ONNT 与 NNT 的训练时间比为 1.0007,这表明 ONNT 算法的复杂度增加在可接受的范围之内;从测试时间看,ONNT 与 NNT 的测试时间比为 0.75,在一定程度上说明了 ONNT 经优化后提高了异常检测的效率。

表 1　ONNT 与 NNT 数值结果对比

方法	n_{int}	n_{hid}	n_{in}	err(%)	far(%)	t_{trn}(sec)	t_{tst}(sec)
NNT	23.37	3.63	69.17	3.67	2.75	613.52	0.04
ONNT	15.26	3.59	45.18	3.59	2.72	613.97	0.03

实验还将基于 ONNT 的异常检测结果与其他常用的经典学习算法的检测结果作了对比,包括(1)K 近邻法(KNN)异常检测,实验中近邻数设为 3。KNN 算法是一种存储样本后,等待查询的消极学习(lazy learning)方法,其泛化决策在查询时实现。(2)对输入特征进行主分量分析(PCA)降维后(实验中 PCA 的累积量和为 0.999),再进行 K 近邻异常检测。在特征信息抽取方面,已经被广泛应用的主分量分析(PCA)算法主要关注数据集中对方差贡献最大的特征,通过保留低阶主成分,忽略高阶主成分实现新的特征集的构建,是一种行之有效的无监督特征信息抽取方法,而对有监督学习经验数据提供的类别信息往往会忽略。本文提出的学习算法与 PCA 算法对特征有效性的衡量有所不同,在每个中间节点上的学习都是有监督的,包括通过信息增益率准则衡量特征子集的有效性时都考虑到当前节点上的访问类别分布(攻击访问或正常访问),充分利用了原有的监督信息(类别)。(3)用径向基神经

网络(RBNN)进行异常检测,RBNN 能够自适应调整隐层节点的个数,该方法与 ONNT 都属于积极学习(eager learning)方法,在对新样例做出预测前,已经形成泛化决策。(4)支持向量机(SVM)异常检测方法,其核函数采用高斯核,通过构造最优超平面,在保持经验风险值最低的情况下最小化置信范围,降低结构风险,提高泛化性。

ONNT 与以上四类方法的264次实验的平均数值结果对比如表2所示。KNN 与 PCA-KNN 并未形成泛化决策,其覆盖的知识域由其存储的样本决定;而 RBNN,SVM 和 ONNT 均为积极学习方式,形成了泛化决策,在训练结束后,可以不必存储训练样本,独立进行预测。而单个 RBNN 的隐节点数较大,对于学习后的规则抽取而言是个 NP 完全问题;SVM 的学习过程包含了低维空间到高维空间的隐性映射(由核函数实现),决策曲面由其众多的支持向量表示,学习的结果不能明确地反映各维特征信息,难以形成推理规则。从异常检测误差和虚警率的数值对比结果看,ONNT 异常检测方法比其他四种对比算法具有相对较低的误差和虚警率,并且在检测的时间消耗上也相对较低。

表2 ONNT 异常检测方法与其他方法的对比

方法	*err*(%)	*far*(%)	t_{tst}(sec)
KNN	4.59	2.96	0.43
PCA-KNN	4.67	2.99	0.20
RBNN	4.90	4.04	0.48
SVM	4.46	3.89	0.53
ONNT	3.59	2.72	0.03

5 结束语

本文针对异常入侵检测问题,提出了一种基于 ONNT 的异常检测方法,提高检测的精确率,增强检测结果的可理解性、可解释性。ONNT 为一种具有二叉树结构的混合学习模型,在二叉树的中间节点上嵌入了专家神经网络。二叉树本身是可解释的,要解决的的问题是:1)如何提高混合学习模型的每个中间节点的可解释性;2)如何使得解释的结果尽量简单,从而易于为人们所理解和接受。对于前者,结构简单的神经网络也可以表示成低复杂度的布尔函数或规则集,本文通过优化神经网络的结构,提高了基于原始 NNT 的入侵检测方法的检测结果可解释性。对于后者,二叉树的整体结构有可能比较复杂,即存在冗余的子树,这将导致从 NNT 中抽取的规则前件的复杂度过高,超出人们可接受的理解范围,从而影响入侵检测结果的可理解性。本文通过修剪 NNT,优化 NNT 的整体结构,降低了解释结果的复杂度。实验结果表明,优化的神经网络树(ONNT)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,同时保证检测结果的高精确率。课题的后期研究将着重于异常检测规则集的抽取和可在线学习性的进一步提高。

参考文献

[1] Lee W, Stolfo S J, Mok K W. A data mining framework for building intrusion detection models [C]. Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 1999, 120-132.

[2] Helmer G, Wong J S K, Honavar V G, Miller L. Automated discovery of concise predictive rules for intrusion detection [J]. Journal of Systems and Software, 2002, 60(3):165-175.

[3] Chebrolu S, Abraham A, Thomas J P. Feature deduction and ensemble design of intrusion detection systems [J]. Computers and Security, 2005, 24(4): 295-307.

[4] Cheng X, Png C Y, Lim S M. Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees [J]. Pattern Recognition Letters 2008, 29(7):918-924.

[5] Sheen S, Rajesh R. Network intrusion detection using feature selection and Decision tree classifier [C]. TENCON 2008 IEEE Region 10 Conference, Hyderabad, India, Nov. 2008,1-4.

[6] Ortiz J, Tomelden J, Beheshti M, Kowalski K, Han J C. Component Based Information Network for Computer Security [C]. Sixth International Conference on Information Technology: New Generations, Las Vegas, Nevada, USA, 27-29, Apr. 2009, 467-469.

[7] Tong X J, Wang Z, Yu H N. A research using hybrid RBF/Elman neural networks for intrusion detection system secure model [J]. Computer Physics Communications, 2009, 180(10):1795-1801.

[8] Thomas C, Balakrishnan N. Improvement in Intrusion Detection With Advances in Sensor Fusion [J]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 542-551.

[9] Hernández-Pereira E, Suárez-Romero J A, Fontenla-Romero O, Alonso-Betanzos A. Conversion methods for symbolic features: A comparison applied to an intrusion detection problem [J]. Expert Systems with Applications, 2009, 36(7): 10612-10617.

[10] Herrero Á, Corchado E, Gastaldo P, Zunino R. Neural projection techniques for the visual inspection of network traffic [J]. Neuro computing, 2009, 72(16-18): 3649-3658.

[11] Zhong C, Li N. Incremental Clustering Algorithm for Instrusion Detection Using Clonal Selection[C]. Proceedings of 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, California, US, Dec. 2008, 1:326-331.

[12] 钟诚,罗程. 无监督异常检测的核聚类和序列分析方法[J]. 计算机研究与发展,2008,45(s1):326-331.

[13] 李娜,钟诚. 基于划分和凝聚层次聚类的无监督异常检测[J]. 计算机工程, 2008, 34(2):120-123.

[14] 魏小涛. 黄厚宽. 田盛丰. 在线自适应网络异常检测系统模型与算法. 计算机研究与发展, 2010, 47(3): 485-492.

[15] Xu Q Z, Zhao Q F, Pei W J, Yang L X, He Z Y. Design interpretable neural network trees through self-organized learning of features [C]. IEEE International Joint Conference on Neural Networks, Hungary, 2004, 1433-1438.

[16] Xu Q Z, Yang L X, Zhao Q F, He Z Y. A Novel Intrusion Detection Mode Based On Understandable Neural Network Trees [J]. Journal of Electronics (China), 2006, 23(4):574-579.

[17] Zhao Q F. Training and retraining of neural network trees [C]. International Joint Conference on Neural Networks, Washington DC, 2001, 126-731.

[18] Quinlan J R. C4.5:Programs For Machine Learning [M]. San Mateo, California: Morgan Kaufmann publishers, 1993:17-26.

[19] Tsukimoto H. Extracting Rules from trained neural networks [J]. IEEE Trans. on Neural Networks, 2000, 11(2):377-389.

[20] Mitchell T. Machine Learning [M]. USA:The McGraw-Hill Companies, Inc., 1997:52-78.

作者简介

徐琴珍(1977-),女,江苏吴江人,博士,东南大学信息科学与工程学院讲师。主要研究方向:智能信息处理、混合学习模型、入侵检测。
E-mail: summer@seu.edu.cn

杨绿溪(1964-),男,安徽桐城人,博士,东南大学信息科学与工程学院,教授,博士生导师。主要研究方向:通信信号处理、移动通信中的 MIMO 空时信号处理、中继协作通信与网络编码、盲信号处理与阵列信号处理。
E-mail: lxyang@seu.edu.cn