doi:10.11959/j.issn.1000-436x.2015252

基于单分类支持向量机和主动学习的网络异常检测研究

刘敬[1,2]，谷利泽[1]，钮心忻[1]，杨义先[1]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 解放军 61741 部队，北京 100094)

摘 要：对基于支持向量机和主动学习的异常检测方法进行了研究，首先利用原始数据采用无监督方式建立单分类支持向量机模型，然后结合主动学习找出对提高异常检测性能最有价值的样本进行人工标记，利用标记数据和无标记数据以半监督方式对基于单分类支持向量机的异常检测模型进行扩展。实验结果表明，所提方法能够利用少量标记数据获取性能提升，并能够通过主动学习减小人工标记代价，更适用于实际网络环境。

关键词：网络安全；异常检测；单分类支持向量机；主动学习
中图分类号：TP309 **文献标识码**：A

Research on network anomaly detection based on one-class SVM and active learning

LIU Jing[1,2], GU Li-ze[1], NIU Xin-xin[1], YANG Yi-xian[1]
(1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. Troops 61741 of PLA, Beijing 100094, China)

Abstract: A network anomaly detection method based on one-class SVM and active learning was presented. Firstly, the original instances were used to trained an one-class SVM model in unsupervised manner. Then the instances which can improve the performance mostly were found by active learning strategy. Finally, the classify model was retrained in semi-supervised manner with both labeled and unlabeled data. The experiment results demonstrate that the presented method can improve performance with a small amount of labeled data and reduce the cost of labeling through active learning. It is more feasible to be used in real network environment.

Key words: network security; anomaly detection; one-class SVM; active learning

1 引言

在日益复杂的网络环境中，网络攻击越来越多样化和复杂化，新的攻击手段层出不穷。异常检测通过训练集为网络行为建立特征轮廓模型，通过计算新数据与正常行为模型的偏离程度来判断是否存在异常行为，与基于特征规则库的误用检测方式相比，异常检测能够检测出未知类型的攻击，是保障网络安全的重要环节，近年来受到越来越多关注，成为网络安全领域的研究热点。

然而异常检测方法误报率较高，并且通常需要大量标记数据完成正常行为模型的训练，在实际的网络环境中，区分和标记数据通常需要专家知识，费时费力且代价高昂，因此能够获取的高质量标记数据的数量非常有限，容易得到的通常是大量正常数据和少量异常数据混杂在一起的不纯净数据集，因此如何在数据集不纯净的条件下提升异常检测性能成为该领域亟需解决的问题。针对该问题，本文对基于单分类支持向量机和主动学习的网络异常检测方法进行了研究，首先利用不纯净的原始数据集以无监督方式训练一个单分类支持向量机模型，在此基础上以主动学习方式选取少量高价值数据请求标记，然后利用这些标记数据的类型信息以半监督方式重新训练模型，提高模型的检测性能。

收稿日期：2015-01-14；修回日期：2015-06-03
基金项目：国家自然科学基金资助项目 (61202082,61370194)
Foundation Item: The National Natural Science Foundation of China (61202082,61370194)

2　相关工作

网络异常检测是网络安全领域研究的重点和难点问题，国内外学者在该领域进行了大量研究，给出了很多异常检测方法，主要包括基于数据挖掘的方法[1]、基于分形时间序列的方法[2]、基于信息融合的方法[3]、基于主成分分析的方法[4]、基于小波分析的方法[5]、基于分形特征参数的方法[6]和基于时间序列分析的方法[7]等。这些方法从不同角度进行特征分析并建立异常检测模型，在实际中得到了较好应用，然而上述方法侧重于研究如何提取网络数据特征和训练模型，属于有监督学习的方法，需要大量有标记样本作为训练数据集，该类方法检测准确率较高，但在实际网络环境中获取大量标记数据非常困难。无监督学习方法无需标记数据即可完成聚类，由于在实际环境中得到的海量无标记网络数据是一种不平衡类，其中绝大多数是正常数据，因此可将异常检测看作单分类问题以无监督方式来解决，单分类支持向量机作为无监督学习领域的常用方法，在网络异常检测领域的应用得到了研究者的关注[8~11]。单分类支持向量机的理论基础是由 Vapnik 等[12]提出的统计学习理论，支持向量机是统计学习理论的具体实现，单分类支持向量机是其在无监督学习领域的扩展；Wang 等[8]将单分类支持向量机引入网络安全领域，通过在传统的核方法中使用单分类支持向量机，获得较好的检测性能；Ma 等[9]提出一种基于相异度的单分类支持向量机用于网络异常检测，根据数据与目标类集合的相异度表示将原始数据转换到新的空间，在该空间建立单分类支持向量机，并结合 KPCA 方法对数据特征进行约简；Barani 等[10]提出了一种适合于自组织网络中异常检测的单分类支持向量机模型，该方法利用正常数据集训练单分类支持向量机模型，并且随网络拓扑变化进行模型更新，利用该模型进行异常检测可适应网络动态性；Chen 等[11]提出了一种结合统计密度信息的单分类支持向量机，该方法首先使用正常数据点构建一个无向图，通过计算数据样例的平均 KNN 距离来获取样例排序，通过将成对样例的排序比较结果反馈给单分类支持向量机完成模型的训练，在检测阶段通过数据样本的排序门限来确定是否异常。单分类支持向量机无需任何先验知识即可建立异常检测模型，并能够通过特征空间变换、引入松弛变量等方法应对数据集不纯净的问题，改善模型的检测性能。

单分类支持向量机方法采用无监督方式完成异常检测模型的训练，在实际的网络异常检测中，合理使用高质量的标记数据有助于提高模型性能，但标记数据的获取通常依赖专家知识，费时费力、代价高昂，因此如何利用有限的标记代价选取更有价值的数据也是一个值得研究的问题，Angluin[13]提出的主动学习算法能够主动选择最有利于提升机器学习算法性能的样本交由专家进行标注，并用来训练分类模型，以较小的标记代价获得模型性能的提升，该方法在网络安全领域的应用受到研究者的关注[14~18]。Almgren 等[14]将主动学习方法引入入侵检测系统，可利用较小的标记代价获取较好的检测性能，同时减少在检测模型建立过程中对安全专家知识的依赖；李洋等[15]提出一种将主动学习和 KNN 算法引入直推信度机的入侵检测方法，由于 TCM-KNN 属于有监督分类方法，为达到较好的训练效果需要用大量标记样本进行训练，通过引入主动学习可精简标记样本，降低算法开销；龙军等[16]提出一种针对入侵检测的代价敏感主动学习算法，通过使用主流代价敏感学习算法产生版本空间并选择能够产生最大误分类代价的样例进行标注，使版本空间缩减更快，从而减少分类器的标注开销，使误分类代价最小；Seliya 等[17]将主动学习引入神经网络，提出了一种入侵检测方法，该方法首先使用初始抽样的训练数据建立一个神经网络模型对剩余数据的相关变量进行预测，然后采用主动学习的方法将选中的实例加入训练集，该过程循环进行直到满足终止条件，从而能够以较小的标记代价获得较好的检测性能。然而上述研究主要是基于有监督训练模型展开的，而且主动学习的选择策略主要考虑了样本的置信度指标。Gu 等[18]对入侵检测中主动学习方法的应用研究现状进行了综述，并指出该领域仍有很多值得改进的空间，如何在网络安全领域利用好主动学习技术仍然是一个值得研究的开放性课题。

综上所述，单分类支持向量机和主动学习在网络异常检测领域的应用日益受到重视，本文对基于单分类支持向量机和主动学习的网络异常检测方法进行了研究，在单分类支持向量机模型的训练过程中引入半监督学习的思想，对模型进行扩展和优化，标记数据通过主动学习方法获得，以用较小的标记代价获取较大的性能提升。

3　基于单分类支持向量机和主动学习的网络异常检测方法

本方法思路如下：首先用无监督方式训练单分

类支持向量机模型；然后利用主动学习方法选取少量样本请求标记；接下来结合这些标记数据以半监督方式重新训练模型，其中同时包含了标记数据的引导作用和无标记数据的约束作用；随后再次进行样本选择和模型训练，重复进行直到满足终止条件。

3.1 基于单分类支持向量机的异常检测模型

给定待检测数据序列 $X=\{x_1,x_2,\mathrm{L}\ ,x_n\}$，其中绝大多数为正常数据，下面首先给出传统的以无监督方式训练的单分类支持向量机模型，然后在此基础上扩展为结合标记数据的半监督学习方式的检测模型，并对其求解方法进行了研究。

3.1.1 无监督模型

异常检测的方法通常是通过建立描述正常数据的模型来检测异常，目标是寻找定义正常数据的最优评价函数 $f:X\to Y$，对于给定的 $x_i\in X$，都能得到相应的输出 $y_i\in Y$。根据经验风险最小化原则，最优化问题可用式(1)进行描述。

$$f^*=\arg\min_f \Omega(f)+\frac{\eta}{n}\sum_{i=1}^{n}L(f(x_i)) \tag{1}$$

其中，L 为损失函数，Ω 为函数 f 的正则化项，η 是调和参数。原始数据经过特征变换后映射到新的特征空间并得到基于 SVDD 的模型，即以 c 为中心 R 为半径的包含所有正常数据的超球面，数据样本的异常程度通过计算其与球心在特征空间的距离来获取，如式(2)所示。

$$f(x)=\|\phi(x)-c\|^2-R^2 \tag{2}$$

若实例落入超球面内，对应的评价函数值 $f(x)<0$，则被判定为正常点；若实例落在超球面外则评价函数值 $f(x)>0$，则被判为异常点。考虑到数据集中可能存在噪声，同时为了防止模型过拟合，引入松弛变量 $\xi_i>0$，要求样本满足约束条件

$$\|\phi(x_i)-c\|^2\le R^2+\xi_i,\ \xi_i\ge 0 \tag{3}$$

此时目标函数为式(4)，且需满足式(3)的约束条件

$$\min_{R,c,\xi_i} R^2+C\sum_{i=1}^{n}\xi_i \tag{4}$$

其中，C 为平衡超球面半径和松弛变量的参数，其物理意义可看作是对数据集的不纯净度估计。上述问题为凸优化问题，可通过拉格朗日乘子方法求解，被约束的优化问题的拉格朗日函数为

$$L_{\mathrm{P}}=R^2-\sum_{i=1}^{n}\beta_i\xi_i+C\sum_{i=1}^{n}\xi_i-\sum_{i=1}^{n}\alpha_i(R^2+\xi_i-\|\phi(x_i)-c\|^2) \tag{5}$$

其中，$\alpha_i\ge 0,\beta_i\ge 0$，对 R、c 和 ξ_i 分别求偏导可得

$$\sum_{i=1}^{n}\alpha_i=1,\ c=\sum_{i=1}^{n}\alpha_i\phi(x_i),\ \alpha_i=C-\beta_i \tag{6}$$

将式(6)代入式(5)，可得

$$\max L_{\mathrm{D}}=\sum_{i=1}^{n}\alpha_iK(x_i,x_i)-\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_jK(x_i,x_j)$$

$$\text{s.t. } 0\le\alpha_i\le C,\ \sum_{i=1}^{n}\alpha_i=1 \tag{7}$$

根据 α_i 的取值可将样本分为以下 3 类：$\alpha_i=0$ 对应的样本点位于球体内部，为正常数据样例；$0<\alpha_i<C$ 的样本点落在球面上，为支持向量数据；$\alpha_i=C$ 的点落在球体外，可看作是数据集中包含的异常点。对以上对偶问题求解可通过计算拉格朗日乘子和超球体参数，得到无监督检测模型。

3.1.2 半监督模型

在模型获取标记数据后可用半监督学习方式完成模型的扩展和优化，标记数据采用主动学习的方式获取，选择策略将在 3.2 节介绍。半监督学习方式下对应的数据模型如下：给定数据集 $X=\{x_1,x_2,\mathrm{L}\ ,x_n,x_{n+1},\mathrm{L}\ ,x_{n+m}\}$，前面 n 个为未标记数据，后面 m 个为标记数据，标记类别为 $Y=\{+1,-1\}$，其中+1 表示正常数据(正例)，−1 表示异常数据(负例)，假设其中包含 m_1 个正例及 m_2 个负例，满足 $m_1+m_2=m=\ n$，则优化目标函数为

$$\min_{R,c,\xi} R^2-k\gamma+C_1\sum_{i=1}^{n}\xi_i+C_2\sum_{j=n+1}^{n+m_1}\xi_j+C_3\sum_{k=n+m_1+1}^{n+m}\xi_k,$$

$$\text{s.t. }\forall_{i=1}^{n},\|\phi(x_i)-\mathrm{c}\|^2\le R^2+\xi_i,\xi_i\ge 0$$

$$\forall_{j=n+1}^{n+m_1},\|\phi(x_j)-\mathrm{c}\|^2\le R^2+\xi_j-\gamma,\xi_j\ge 0$$

$$\forall_{k=n+m_1+1}^{n+m},\|\phi(x_k)-\mathrm{c}\|^2\ge R^2+\xi_k-\gamma,\xi_k\ge 0 \tag{8}$$

其中，$\gamma\ge 0$ 为 2 类标记数据边缘之间的距离，C_1、C_2 和 C_3 分别是未标记数据、正例数据和负例数据的权衡参数，ξ_i、ξ_j 和 ξ_k 分别是为优化问题约束引入的松弛变量，其取值与样本和球体中心在特征空间的距离成反比，即距离球心较近的样本被错误分类的代价较大，距离球心较远的样本被错误分类的代价较小。权衡参数 C_1、C_2 和 C_3 的选择也将对模型产生影响，其中 C_1 反映了无标记数据的约束作用，C_2 和 C_3 反映了标记数据的类型引导作用，若 C_1 取值过大，则模型中标记数据的作用会减弱，直至退化为无监督模型，反之若 C_1 取值过小，则模型中无标记数据作用会减弱，直至退化为只包含少量标记数据的有监督模型。对于 C_2 和 C_3，根据具体情况，对误报率和漏报率的要求进行选择，由于在

异常检测中使异常数据误判的代价高于正常数据，因此通常选择 $C_2<C_3$，对标记数据误判的代价高于无标记数据，因此取值通常满足 $C_1<C_2<C_3$，实际应用中通过实验获取具体数值。由于标记数据中可能存在负样本数据，上述问题为非凸优化问题，拉格朗日乘子方法无法找到全局最优解。为解决上述问题，将包含松弛变量的约束条件以风险函数的形式表示，从而将式(8)表示的问题转化为无约束最优化问题，如式(9)所示。

$$\begin{aligned}\xi_i &= \mathrm{l}(R^2-\|\phi(x_i)-c\|^2)\\ \xi_j &= \mathrm{l}(R^2-\|\phi(x_j)-c\|^2-\gamma)\\ \xi_k &= \mathrm{l}(\|\phi(x_k)-c\|^2-R^2-\gamma)\end{aligned} \tag{9}$$

若风险函数取值为 $\mathrm{l}(t)=\max\{-t,0\}$，则与式(8)等价，因此式(8)所示优化问题是式(9)的一种特殊情况。将式(9)代入式(8)并令 $T=R^2-c^2$，可得

$$\begin{aligned}J(T,\gamma,c) = c^2+T-k\gamma+C_1\sum_{i=1}^{n}\mathrm{l}(T-\|\phi(x_i)\|^2+2\phi(x_i)'c)+\\ C_2\sum_{j=n+1}^{n+m_1}\mathrm{l}(T-\|\phi(x_j)\|^2+2\phi(x_j)'c-\gamma)+\\ C_3\sum_{k=n+m_1+1}^{n+m}\mathrm{l}(\|\phi(x_k)\|^2-T-2\phi(x_k)'c-\gamma)\end{aligned} \tag{10}$$

根据式(10)以及文献[19]中的表示定理，并考虑到样本类型取值为+1 或者−1，可得

$$c=\sum_{i=1}^{n}\lambda_i\phi(x_i)+\sum_{j=n+1}^{n+m}\lambda_j y_j\phi(x_j) \tag{11}$$

由式(11)可以看出，通过加入已标记数据，球心 c 的取值由未标记数据和标记数据共同确定，得到一个更为精确的单分类模型。然而当采用风险函数 $\mathrm{l}(t)=\max\{-t,0\}$ 时，函数二阶导数不存在从而无法应用梯度法求解，为此引入如下损失函数

$$\mathrm{l}_{V,\varepsilon}(t)=\begin{cases}(t-\varepsilon)^2, & |t|<\varepsilon\\ \max(-t,0), & |t|>\varepsilon\end{cases} \tag{12}$$

其中参数取值为 $\Delta=0$，$\varepsilon=0.5$。结合式(12)并将式(9)、式(11)代入式(8)可得

$$\begin{aligned}\min_{R,\gamma,\alpha} R^2-k\gamma+C_1\sum_{i=1}^{n}\mathrm{l}_{\varepsilon}(R^2-k(x_i,x_i)+(2e_i-\lambda)'\boldsymbol{K}\lambda)+\\ C_2\sum_{j=n+1}^{n+m_1}\mathrm{l}_{\varepsilon}(R^2-k(x_j,x_j)+(2e_j-\lambda)'\boldsymbol{K}\lambda-\gamma)+\\ C_3\sum_{k=n+m_1+1}^{n+m}\mathrm{l}_{\varepsilon}(k(x_k,x_k)-R^2-(2e_k-\lambda)'\boldsymbol{K}\lambda-\gamma)\end{aligned} \tag{13}$$

其中，矩阵 $\boldsymbol{K}$ 的元素 $k_{ij}=k(x_i,x_j)=<\phi(x_i),\phi(x_j)>$，$e_i$ 表示矩阵 $\boldsymbol{R}^{n+m}$ 的标准基，向量 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\mathrm{L},\lambda_{n+m})$ 由各样本对应的乘子组成。在式(13)中对各变量求导，可得

$$\begin{aligned}\frac{\partial Eq(12)}{\partial R} &= 2R+C_1\sum_{i=1}^{n}\frac{\partial\xi_i}{\partial R}+C_2\sum_{j=n+1}^{n+m_1}\frac{\partial\xi_j}{\partial R}+C_3\sum_{k=n+m_1+1}^{n+m}\frac{\partial\xi_k}{\partial R}\\ \frac{\partial Eq(12)}{\partial\gamma} &= -k+C_2\sum_{j=n+1}^{n+m_1}\frac{\partial\xi_j}{\partial\gamma}+C_3\sum_{k=n+m_1+1}^{n+m}\frac{\partial\xi_k}{\partial\gamma}\\ \frac{\partial Eq(12)}{\partial c} &= C_1\sum_{i=1}^{n}\frac{\partial\xi_i}{\partial c}+C_2\sum_{j=n+1}^{n+m_1}\frac{\partial\xi_j}{\partial c}+C_3\sum_{k=n+m_1+1}^{n+m}\frac{\partial\xi_k}{\partial c}\end{aligned} \tag{14}$$

其中，风险函数关于各参数的求导可通过将胡贝尔函数代入式(9)得

$$\begin{aligned}\frac{\partial\xi_i}{\partial R} &= 2R\mathrm{l}'_{\varepsilon}(R^2-\|\phi(x_i)-c\|^2)\\ \frac{\partial\xi_i}{\partial c} &= 2(\phi(x_i)-c)\mathrm{l}'_{\varepsilon}(R^2-\|\phi(x_i)-c\|^2)\\ \frac{\partial\xi_{\frac{j}{k}}}{\partial R} &= 2y_{\frac{j}{k}}R\mathrm{l}'_{\varepsilon}(R^2-\|\phi(x_{\frac{j}{k}})-c\|^2-\gamma)\\ \frac{\partial\xi_{\frac{j}{k}}}{\partial\gamma} &= -\mathrm{l}'_{\varepsilon}(R^2-\|\phi(x_{\frac{j}{k}})-c\|^2-\gamma)\\ \frac{\partial\xi_{\frac{j}{k}}}{\partial c} &= 2y_{\frac{j}{k}}(\phi(x_{\frac{j}{k}})-c)\mathrm{l}'_{\varepsilon}(R^2-\|\phi(x_{\frac{j}{k}})-c\|^2-\gamma)\end{aligned} \tag{15}$$

根据求导链式法则，结合式(11)可得关于 λ_i 和 λ_j 的偏微分

$$\begin{aligned}\frac{\partial Eq(8)}{\partial\lambda_i} &= \frac{\partial Eq(8)}{\partial c}\frac{\partial c}{\partial\lambda_i}=\frac{\partial Eq(8)}{\partial c}\phi(x_i)\\ \frac{\partial Eq(8)}{\partial\lambda_j} &= \frac{\partial Eq(8)}{\partial c}\frac{\partial c}{\partial\lambda_j}=\frac{\partial Eq(8)}{\partial c}\phi(x_i)y_j\end{aligned} \tag{16}$$

从而得到式(13)的最优解。

3.2　基于主动学习的样本选择

上面标记数据将基于单分类支持向量机的模型扩展为半监督方式，然而由于获取标记数据的过程繁琐、代价高昂，因此应尽量减少标记代价。本文采用主动学习方法请求数据标记，以期望用较小的代价获取模型性能改善，其关键步骤在于选择策略和终止条件的确定上。

3.2.1　选择策略

根据主动学习获取样本的方式不同，选择策略可分为 3 种类型：成员关系查询综合方法、基于流的选择性抽样方法和基于池的选择性抽样方法[20]，其中基于池的研究方法是当前研究最为充分的方法，该类方法首先将无标记样本组成一个分布和特性相对固定的“样本池”，然后按照一定的策略进

行样本评估和选择。根据选择策略的不同，该类方法又可以分为基于不确定度缩减的方法、基于版本空间缩减的方法和基于泛化误差缩减的方法。基于不确定性缩减的样例选择算法对当前分类信息最模糊的样本进行请求标注，基于版本空间缩减的方法选择能够最大限度缩减版本空间的样本请求标记，基于误差约简的方法通过减少分类器误差直接提高算法的分类能力，其核心思想都是选择低置信度的样本进行标记。经分析可知，异常检测方法误报率高的原因有 2 个方面：其一是训练数据集的纯净程度，若训练数据集包含异常数据，则会影响到模型的训练效果，可能导致漏报；其二是训练数据集的完整程度，若训练数据集中包含的正常数据不足以完整地描述正常数据的特征，则可能导致误报。因此在进行样本选择时，一方面需要选择低置信度的样本，确定其类型，提高数据集的纯净程度和模型的检测精确度；另一方面需要选择有代表性的样本，使样本尽可能覆盖所有数据区域，提高模型的完整性。在异常检测中，通常选择距离决策边界最近的样例进行标记，这些样本的不确定度通常最大，能够为模型的优化提供的信息最多，该方法称为最近边界策略，当最初数据集中无标记数据时，采用该策略选择部分样本，如式(17)所示。

$$x^* = \arg\min_{x\in\{x_1,\mathrm{L},x_n\}} \| R^2 - \| \phi(x) - c \|^2 \| \tag{17}$$

然而单独使用最近边界策略会存在如下问题：当样本边界经过稀疏区域时，有可能选到离群点，离群点无法代表样本的特性，无益于提高模型性能；当模型边界经过样例密集区域时，该区域内的大量样本将被请求标记，而这类样例通常具有相同的标记，会对标记代价造成浪费，因而使用有限的标记代价可能无法完整地描述数据特征。为解决这些问题，根据样本之间的类型关系引入邻接矩阵 $\boldsymbol{A} = (a_{ij})_{i,\,j=1,\mathrm{L},n+m}$，其中元素 a_{ij} 表示样本 x_i 和 x_j 之间的关系，当 2 个样本属于同一类型时，$a_{ij}=1$，否则，$a_{ij}=0$。由于数据集中多数样本为未标记样本，因此引入样本扩展标记 $\bar{y}_1, \bar{y}_2, \mathrm{L}, \bar{y}_{n+m}$，对于未标记样本 $\bar{y}_i = 0$，对于已标记样本 $\bar{y}_i = y_i$，即为该样本的标记类型。使用 K 最近邻(KNN, K-nearest neighbors)方法对样本进行分类，若其中包含已标记数据，则按照已标记数据类型对样本进行分类，若其中不包含已标记数据，则将样本标记为 0。在此基础上，选择策略如式(18)所示。

$$x^* = \mathrm{argmin}_{x_i\in\{x_1,\mathrm{L},x_n\}} \sum_{j=1}^{n+m} (\bar{y}_j + 1) a_{ij} \tag{18}$$

利用式(18)倾向于选择可能是异常数据点的样本进行标注，因此能够较快发现新的异常类型，而当边界穿过正常数据或未标记数据密集的区域时，由于 $(\bar{y}_j+1)a_{ij}$ 取值较大，该区域的点不会被大量选择，因此可避免标记代价重复浪费的问题。然而由于球心附近的点通常不会被标记，相应的 $(\bar{y}_j+1)a_{ij}$ 值较小，因此按照式(18)可能会选择到距离实际球心较近的点，这些点虽不会对模型的更新产生误导，但是也无法对模型更新做出贡献，为避免这种情况，可结合最近边界策略得到如式(19)所示的主动学习策略。

$$x^* = \arg\min_{x_i\in\{x_1,\mathrm{L},x_n\}} \alpha \| R^2 - \| \phi(x) - c \|^2 \| + (1-\alpha) \sum_{j=1}^{n+m} (\bar{y}_j + 1) a_{ij} \tag{19}$$

其中，参数 $\alpha \in (0,1)$ 为平衡参数。因不同数据集的样本数量以及训练得到的单分类支持向量机模型球体半径值各不相同，为便于研究，将初始数据集训练得到的无监督单分类支持向量机模型的半径归一化，并以此为标准对式(19)的前一项进行标准化处理，后一项用样本数量归一化。当样本对应值小于门限值时，表示该样本是靠近超平面边界的点或者是可能的簇代表样本点，这些点对于优化模型最为有利，因此被选择出来请求标记。本文根据多次实验尝试设定该门限值为经验值 0.2。特别地，当样本点都是未标记数据时，式(19)的后半部分为定值，样本的选取主要依赖于前半部分，则策略退化为与式(17)等价，因此在初始无监督方式训练的模型条件下，采用的样本选择方法仍是传统的最近边界策略。

3.2.2 终止条件

主动学习需要设定终止条件来限定算法运行时间，通常是达到一定标记代价或者性能指标达到一定标准。标记代价通常为根据实际情况预先给定的值，较为简单，在此不予讨论。对于性能指标，通常有检测性能和变化程度 2 种，由于本方法采用半监督方式，因此终止条件采用 2 种指标相结合的方式，如式(20)所示。

$$con = b_1 MSE(f(x, y^*) + b_2 var(f(x, y^*)) \tag{20}$$

其中，前半部分表示模型对标记样本的预测值与真实值的误差，取值为所有标记样本的预测分类和实际分

类之间差异的比率；后半部分取值为所有无标记样本预测分类差异的比率，反映了模型变化程度。前半部分反映的是标记数据的作用，后半部分表示未标记数据的作用，实际情况下很难保证 2 部分同时最小，需在 2 部分之间折中。设系数 b_1 和 b_2 为 2 部分的权衡系数，若 b_1 取值较大，则强调标记数据的作用，反之若 b_2 取值过大，则强调未标记数据的作用，通过多次实验可得到合适的值。在使用主动学习调优模型的过程中，随着数据集中标记样本的不断增加，上述 *MSE* 值不断下降，*var* 逐渐稳定，当前后 2 次的 *con* 值小于某门限值时，即可认为达到理想的检测率，可终止选择过程，该门限值为经验值，在实验中取 0.1。综上所述，算法步骤如算法 1 所示。

算法 1　基于单分类支持向量机和主动学习的网络异常检测方法

输入：包含少量异常数据的待检测数据 X；

输出：异常检测模型

Step1　利用原始数据集以无监督方式获取异常检测模型；

Step2　按照式(17)的最近边界策略进行主动学习，选择部分数据进行标记；

Step3　利用标记数据和未标记数据按照半监督方式对模型进行扩展；

Step4　按照式(19)的策略进行主动学习，选择数据进行标记；

Step5　利用新的标记数据按照半监督方式进行再次优化；

Step6　若模型性能符合终止条件，算法完成；否则返回 Step4。

4　实验与结果分析

4.1　实验环境和数据集

为验证算法的有效性，本节采用 2 种不同的数据集对算法性能进行了测试，并与其他算法进行了比较，实验的目的是证明通过结合标记数据建立的半监督方式的单分类支持向量机模型能够提升检测性能，而结合主动学习能够以较小的标记代价获取较大性能提升，对比方法包括 SVDD(无标记数据)、$\text{SVDD}_{\text{random}}$(随机选择标记数据方法)、$\text{SVDD}_{\text{neg}}$(仅标记部分异常数据)、$\text{SVDD}_{\text{margin}}$(最近边界策略的选择方法)，本文提出的方法记为 $\text{SVDD}_{\text{hybrid}}$。实验环境为 64 位 Windows7 操作系统，Intel Pentium Dual-Core CPU 3.2 GHz 处理器，4 GB 内存，编程语言使用 Java，单分类支持向量机通过调用 libsvm 实现。

数据集 1 为入侵检测领域常用的 kddcup99 数据集，该数据集由约 500 万条网络连接组成，每条数据由 41 个网络连接特征描述，数据集中包含大量的正常数据和 4 大类异常数据，如表 1 所示。

表 1　　数据类型分布

数据类型	训练数据	百分比	测试数据	百分比
normal(未标记，正例)	10 000	94.51%	4 881	44.54%
DOS(未标记，负例)	368	3.48%	3 293	30.05%
U2R(未标记，负例)	0	0%	707	6.45%
R2L(未标记，负例)	0	0%	911	8.31%
probe(未标记，负例)	213	2.01%	1 167	10.65%
总计	10 581	100%	10 959	100%

其中训练集中绝大多数为正常数据，但同时包含一些“杂质”，测试集中包含的异常数据的类型和数量更多。数据集 2 为某网站(集智百科，http://wiki.swarma.net/)服务器的 Web 访问日志，为便于表示记为 web-access-log 数据集，共包含 112 380 条正常访问数据，异常数据为使用 metasploit 框架产生的 23 种真实的 Web 攻击类型(包括 12 种缓冲区溢出、6 种代码注入、5 种跨站脚本等其他类型)。此外，为进一步验证方法的有效性，将测试集中部分异常连接的 http 头转换为正常数据得到部分新的异常数据集，使这部分异常数据在特征空间中与正常数据更加接近，检测难度更大。从中选取部分数据作为训练集和测试集，同样在测试集中包含部分训练集中不存在的异常类型，如表 2 所示。

表 2　　数据类型分布

数据类型	训练数据	百分比	测试数据	百分比
normal(未标记，正例)	21 000	91.81%	7 835	43.71%
buffer_overflow(未标记，负例)	1 365	5.97%	2 426	13.54%
XSS(未标记，负例)	509	2.22%	1 438	8.02%
code_injection(未标记，负例)	0	0%	2 115	11.8%
other(未标记，负例)	0	0%	4 109	22.93%
总计	22 874	100%	17 923	100%

该数据集在建立模型之前需要首先完成特征转换，要求该特征空间能够很好的描述原数据，进行异常检测。本文利用 1 个字符串集合 S 和 1 个映射函数 ϕ 完成数据载荷 x 到向量空间的映射，对于每个字符串 $s \in S$，若 x 中包含 s，则函数 $\phi_s(x)=1$，

否则 $\phi_s(x)=0$，这样将 $\phi_s(x)$ 应用到 S 中的所有元素，可得映射

$$\phi: X \to \boldsymbol{R}^{|S|}, \phi: x \text{ a } (\phi_s(x))_{s\in S} \tag{21}$$

此处 X 为所有数据载荷组成的集合，S 为所有字符串组成的集合，然而因数据中会出现新的数据类型，因此很难预先定义能够表示所有可能类型的 S。本章采用 n-gram 的方法定义所有可能的长度为 n 的字符串：定义一个长度为 n 的滑动窗口，窗口通过数据上的滑动过程产生不同的 n-grams。一方面，根据扩展的 ASCII 码表，单个字符的可能取值个数为 256，即 n-gram 将数据映射到 256^n 的特征空间，特征空间随 n 值的增大呈现指数级增长，即使在很小的取值映射后，维度依然很高；另一方面，一个长度为 N 的数据块最多包含 $N-n$ 个不同的 n-grams，即特征映射是稀疏的，所以仅需关注其中的非零值即可，实验中取 n=3。在初始情况下，训练数据和测试数据均为未标记数据，其中，正常数据为正例，异常数据均为负例。各方法中的核函数都选择为高斯核函数 $K(x_i,x_j)=\exp\left(-\frac{\| x_i-x_j \|^2}{\delta^2}\right)$，其中 $\delta^2=2$，选择 SVDD 的惩罚系数为 C_1=50，已标记正例数据的惩罚系数设置为 C_2=100，已标记负例数据惩罚系数设置为 C_3=200，主动学习的选择策略中参数 $\alpha=0.6$，终止条件中的参数设置为 b_1=b_2=0.5。

4.2 实验结果分析

在异常检测中数据集通常具有不平衡类分布，大多数为正常数据，同时稀有类的误分类往往会造成更为严重的后果。本实验使用准确率、召回率和检测精度 3 个指标来比较不同方法的性能。表 3 为正确和不正确检测实例数目的混淆矩阵。

表 3 混淆矩阵

实际类型	检测结果	
	正常	异常
正常	TP	FN
异常	FP	TN

准确率定义为被模型正确检测的实例所占的比例，即 $\frac{(TP+TN)}{(TP+FP+FN+TN)}$；召回率定义为 $\frac{TN}{(FP+TN)}$，检测精度定义为 $\frac{TN}{(FN+TN)}$。准确率可反映模型的总体检测性能；而召回率越高反映出模型灵敏度越高，相应的漏报率越低；检测精度越高则说明模型的误报率越低。模型优化过程中的标记数据比例和检测性能如表 4 所示。

表 4 模型扩展和优化过程

数据集	标记数据			相关参数		
	正例	负例	总计	*MSE*	*var*	*con*
kddcup99	1.82%	0.62%	2.44%	0.12	0.32	0.22
	1.61%	0.18%	1.79%	0.09	0.19	0.145
	1.26%	0.33%	1.59%	0.05	0.08	0.06
web-access-log	1.42%	0.37%	1.79%	0.24	0.35	0.295
	1.04%	0.31%	1.35%	0.18	0.21	0.195
	0.86%	0.22%	1.08%	0.13	0.11	0.12
	0.76%	0.26%	1.02%	0.09	0.05	0.07

从实验结果可看出，2 种数据集分别在 3 次和 4 次数据选择之后满足终止条件，前后 2 次的 *con* 值差别小于门限值 0.1，此时继续增加标记样本，性能提升不再明显。

下面比较不同方法在 2 种数据集上的性能，SVDD 为无监督方式的单分类支持向量机，其他为采用不同选择策略的半监督方式模型，实验结果如表 5 和表 6 所示。

表 5 **kddcup99 数据集实验结果比较**

数据集	标记数据			检测结果		
	正例	负例	总计	准确率	召回率	检测精度
SVDD	0	0	0	83.22%	87.46%	78.33%
$\text{SVDD}_{\text{random}}$	9.84%	0.75%	10.59%	85.67%	85.82%	82.27%
SVDD_{neg}	0	5.49%	5.49%	88.54%	91.35%	76.92%
$\text{SVDD}_{\text{margin}}$	5.83%	0.72%	6.55%	93.18%	93.77%	91.81%
$\text{SVDD}_{\text{hybrid}}$	4.69%	1.13%	5.82%	95.35%	97.15%	94.26%

表 6 **web-access-log 数据集实验结果比较**

数据集	标记数据			检测结果		
	正例	负例	总计	准确率	召回率	检测精度
SVDD	0	0	0	70.74%	78.14%	63.75%
$\text{SVDD}_{\text{random}}$	10.19%	1.39%	11.58%	74.08%	76.51%	73.29%
SVDD_{neg}	0	8.19%	8.19%	80.33%	83.36%	76.83%
$\text{SVDD}_{\text{margin}}$	6.04%	1.07%	7.11%	84.67%	91.17%	75.28%
$\text{SVDD}_{\text{hybrid}}$	3.98%	1.26%	5.24%	90.52%	92.67%	88.67%

从实验结果可看出，与 SVDD 相比，在 2 种数据集的实验中，后面几种采用了半监督方式的异常检测

模型的准确率性能获得了不同程度的提升，这说明通过有效利用标记数据中包含的信息，可以提高异常检测模型的检测效果。在这 4 种方法的比较中，$SVDD_{random}$ 通过随机方式选择样本，多数是正常数据且不在分类边界的边缘，在提高模型检测精度的同时灵敏度有所降低，并且会消耗更多的标记代价；$SVDD_{neg}$ 选择异常数据进行标记，可提高模型的召回率性能，但由于训练数据集中异常数据的数量和类型较少，因此准确率性能提升有限，且有可能使误报率升高，但在异常检测的实际应用环境中，保证灵敏度性能通常比降低误报率重要，因此该方法优于随机选择方法；$SVDD_{margin}$ 选择分类边界附近的点进行标记，这些点的置信度较低，从而这些点的标记能够为模型的修正提供更多的信息，因此 $SVDD_{margin}$ 能够获取优于上面 2 种方法的性能；本文提出的选择策略 $SVDD_{nybrid}$ 在选择样本的同时兼顾了样本的置信度和代表性，从而能够更充分地利用标记信息，其获取的性能提升最大。在 web- access-log 数据集中，由于加入了一些人工改动，使部分异常数据与正常数据的特征非常相近，因此各方法的性能指标都有所下降，方法之间的性能差异也更为明显。

上述实验证明了通过利用标记数据信息，半监督模型可以提升异常检测性能，为进一步说明本文提出的主动学习策略对模型性能提升的影响，下面采用受试者工作特征曲线(ROC，receiver operating characteristic curve)对比算法性能， ROC 曲线是显示分类器真正率和假正率之间折中的一种图形化方法，在 ROC 曲线中 x 轴为假正率，即被错误分类为异常的正常样本，y 轴为真正率，即被正确分类的异常样本比例，取值范围均为[0,1]，其中(0,0)表示将每个实例均预测为正常的模型，(1,1)表示将每个实例预测为异常的模型，因此好的分类模型会靠近图的左上角，当标记数据为 5%时，各种算法的 ROC 曲线比较如图 1 所示。

ROC 曲线能较为直观地反映当固定标记数据比例时的算法性能，而为了比较不同标记数据比例下的情形，则需要用一个数值来表示算法性能的好坏，因此引入接受者操作特征曲线下方面积（AUC，area under the ROC curve）作为模型性能评价指标，AUC 的值就是处于 ROC 曲线下方的那部分面积的大小，通常取值为 0.5~1 之间，ROC 性能越好则 AUC 的值越大。在 kddcup 数据集上各种方法的实验结果如图 2 所示。

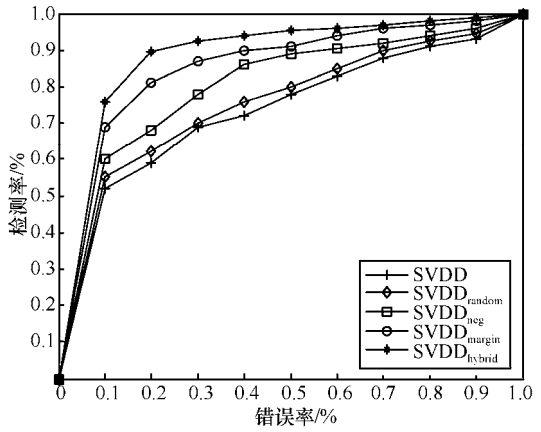


图 1　各方法在 kddcup99 数据集(5%标记数据)上 ROC 性能比较

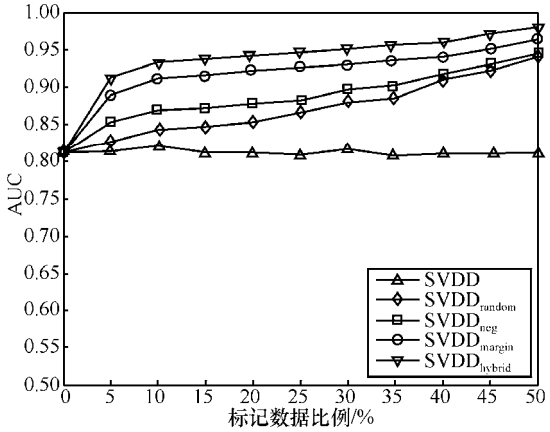


图 2　各方法在 kddcup99 数据集性能比较

由图 2 可看出，由于不使用标记数据信息，SVDD 在不同标记比例时性能都最差，这与上面实验结论一致，当数据集都是标记数据时，SVDD 成为传统的有监督训练方式；$SVDD_{random}$ 利用部分随机标记的信息获得了部分性能的提升，但由于样本选择的随机性，很多样本（如靠近球心位置的明显正常的样本）不能对模型优化起到很大作用，浪费了标记代价，当标记数量达到 30%左右时才有较为明显的性能提升；$SVDD_{neg}$ 利用异常数据的标记信息获取了一定的性能提升，然而由于异常数据数量稀少(本实验中异常数据的比例仅为约 5.5%)，后续标记数据采用随机方式，获取的性能提升有限；$SVDD_{margin}$ 和 $SVDD_{hybrid}$ 都能够充分利用已标记数据，用较少的标记数据获得较大的性能提升，相比之下，$SVDD_{hybrid}$ 在相同的标记代价条件下获取的性能提升更大。在 web-access-log 数据集上的实验结果如图 3 所示。

由图 3 可以看出，当标记数据比例升高时，除 SVDD 外，其他几种利用标记数据的算法性能

均有所提高。由于该数据集中包含有处理过的异常数据样本，在特征空间中与正常数据很接近，因此，无监督方式下训练模型的性能下降到 65%左右；$SVDD_{random}$ 采用随机方式选择样本，性能提升较为缓慢；$SVDD_{neg}$ 方法仅使用数量稀少的异常样本(约 8%)，后续标记的增加为随机方式，性能提升有限；$SVDD_{margin}$ 方法在标记数据为 5%左右时性能开始提升，当达到 15%左右时 AUC 的值达到 0.8 左右；而本文方法在标记数据为 5%左右时即能够获取明显的性能提升，AUC 值达到 0.85 左右。上述实验证明了本文所选用的主动学习选择策略可用较小的标记代价获取较大的性能提升。

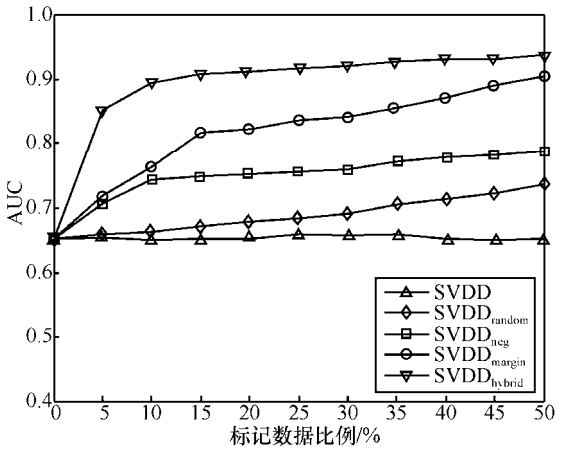


图 3 各方法在 web-access-log 数据集性能比较

最后对方法中部分参数进行实验分析，实验数据集采用 kddcup99。图 4 为半监督模型中权衡参数对模型检测性能的影响，横轴为比值 $k_1=\frac{(C_2+C_3)}{C_1}$，标记数据比例为 10%。由图 4 可以看出，当 k_1 值较小时，性能较差，随着 k_1 值增大性能有所提升，然而随着 k_1 值进一步增大，性能又产生下降。分析原因可知：当 k_1 值较小时，模型主要由无标记数据决定，近似于无监督方式；随着 k_1 值的增加，标记数据的引导和约束作用逐渐显现，因此性能得到提升；然而当 k_1 值过大时，会过度削弱未标记数据的作用，而集中于少量标记数据，此时模型近似于仅包含少量标记数据的有监督方式，性能又会产生下降。在本实验中选取 k_1 值为 6。

图 5 为不同的 $k_2=\frac{C_3}{C_2}$ 比值下的检测性能(k_1=6)。可以看出随着 k_2 值的增加，总准确率变化不大，灵敏度有所提升，同时检测精度随之降低。分析原因可知，随着 k_2 值的增加，异常样本对模型的贡献度逐渐增加，从而异常样本的误报率会减小，因此召回率随之提高，而正常样本对模型的贡献度减小，因此正常样本的误报率增加，检测精度随之降低，在实际的网络异常检测中，漏报付出的代价通常大于误报，所以一般选择 k_2>1。本实验中选取 k_2=2。

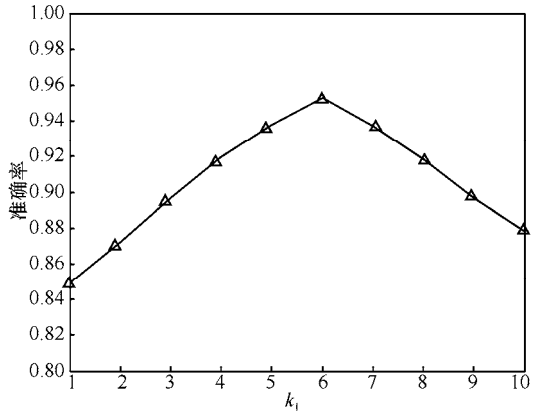


图 4 参数 k_1 对模型性能的影响

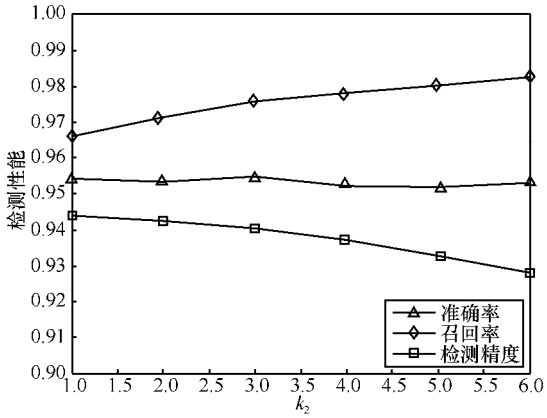


图 5 参数 k_2 对模型性能的影响

图 6 为主动学习的选择策略中参数 α 对算法性能的影响，由图 6 可看出，随着 α 值逐渐增大，算法性能有所提高，在 α 大于 0.6 之后开始出现下降。分析其原因可知：当 $\alpha=0$ 时，样本的选择主要考虑样本的代表性，能较为完整地描述数据特征，但对于决策边界附近的样本误判率仍会较高；随着 α 值的增大，更多低置信度样本被选择，性能得到提升；然而，当 α 值过大时，选择策略会对样本的代表性考虑不足；当 $\alpha=1$ 时退化为最近边界策略。本文实验中选取 α 值为 0.6。

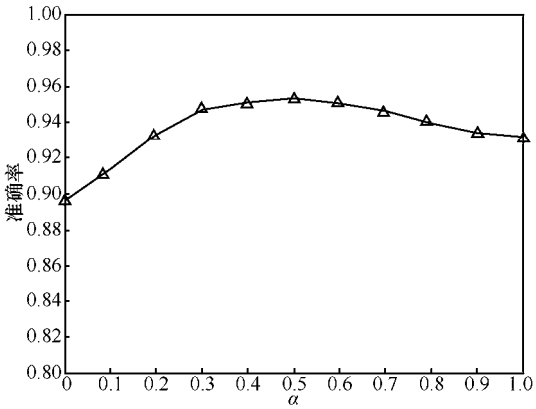


图 6　参数 α 对模型性能影响

图 7 为不同的 $k_3=\frac{b_2}{b_1}$ 比值下算法的检测性能，由图 7 可看出，随着 k_3 值逐渐增大，准确率升高。而当大于门限值（实验中为 1）时性能开始下降。分析其原因，当 k_3 值较小时，*con* 值主要受初次选择的标记样本影响，容易使主动学习方法较早终止，从而影响性能的进一步提升；随着 k_3 值逐渐增大，无标记数据的约束作用产生影响，更多数据被请求标记，提升了性能；然而当 k_3 值过大时，标记数据的引导作用会减弱，造成算法性能的下降。实验中选取 k_3 为 1。

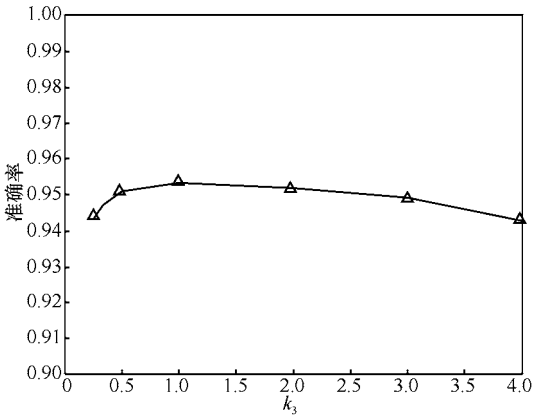


图 7　参数 k_3 对模型性能影响

图 8 为选择策略中不同门限值对检测性能的影响。由图 8 可以看出，随着门限值的增大，检测性能逐渐升高，分析原因可知：门限值越小，每次所选择的样本越少，标记数据信息少，性能提升也会相应较小；而门限值越大相应性能提升也会越大，同时标记代价也会越高。因此应在控制标记代价的同时兼顾性能提升，由图 8 可以看出，当门限值大于 0.2 时性能提升较为缓慢，因此本实验中选取门限值为 0.2。

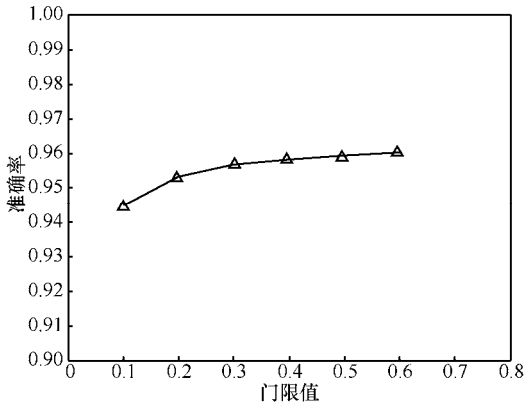


图 8　选择策略门限值对模型性能影响

图 9 为终止条件中不同门限值对检测性能的影响。从图 9 可以看出，随着门限值的增大，检测性能逐渐下降，这较为容易理解：越小的门限值对终止条件要求越严格，从而使更多标记数据参与到模型的优化中以提高模型性能，然而同时需要的标记代价和运算量也相应增加，随着门限值的增大，标记代价和运算量减少，同时性能提升也减少。因此应在对性能影响不明显的前提下选择尽可能高的门限值，本实验中为 0.1。

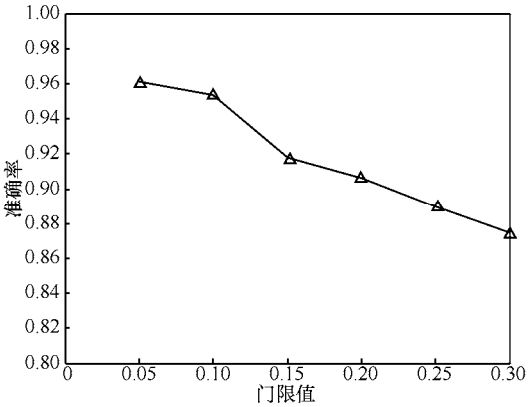


图 9　终止条件门限值对模型性能影响

5　结束语

针对网络异常检测中标记数据获取困难的问题，本文提出了一种基于单分类支持向量机和主动学习的异常检测方法：首先以无监督方式建立单分类支持向量机模型，然后利用主动学习策略找出部分数据请求标记，利用这些标记数据以半监督方式对模型进行扩展和优化，确定新的分类边界；其次对主动学习的选择策略和终止条件进行了研究，在样本选择的同时考虑样本的置信度和代表性，在设定终止条件的同时考虑标记样本和未标记样本的

作用。该方法结合标记数据将单分类支持向量机扩展为半监督方式，并结合主动学习方法利用较小的标记代价完成了模型性能的优化。实验结果表明，与传统方法相比，本文方法能够用较小的标记代价获取较大的性能提升。在下一步工作中，将研究如何寻找更为合适的特征空间表示网络数据以及如何选取更为合适的主动学习策略。

参考文献：

[1] LEE W, STOLFO S J. A framework for constructing features and models for intrusion detection systems[J]. ACM Transactions on Information and System Security, 2000,3(4):227-261.

[2] LI M. An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition[J]. Computers & Security, 2004, 23(7):549-558.

[3] 诸葛建伟,王大为,陈昱. 基于D-S证据理论的网络异常检测方法[J]. 软件学报,2006,17(3):463-471.
ZHUGE J W, WANG D W, CHEN Y. A network anomaly detector based on the D-S evidence theory[J]. Journal of Software, 2006, 17(3): 463-471.

[4] 钱叶魁,陈鸣,叶立新. 基于多尺度主成分分析的全网络异常检测方法[J].软件学报,2012,23(2):361-377.
QIAN Y K, CHEN M, YE L X. Network-wide anomaly detection method based on multiscale principal component analysis[J]. Journal of Software, 2012, 23(2): 361-377.

[5] WEI L, GHORBANI A A. Network anomaly detection based on wavelet analysis[J]. EURASIP Journal on Advances in Signal Processing, 2009,12(5):1234-1249.

[6] LI M. Change trend of averaged Hurst parameter of traffic under DDOS flood attacks[J]. Computers & Security, 2006, 25(3):213-220.

[7] 郑黎明.大规模通信网络流量异常检测与优化关键技术研究[D]. 长沙: 国防科学技术大学, 2012.
ZHENG L M. Key Technologies Research on Traffic Anomaly Detection and Optimization for Large-Scale Networks[D]. National University of Defense Technology, 2012.

[8] WANG Y, WONG J, MINER A. Anomaly intrusion detection using one class SVM[A]. Proceedings of the Fifth Annual IEEE SMC on Information Assurance Workshop[C]. 2004.358-364.

[9] MA J, DAI G Z, XU Z. Network anomaly detection using dissimilarity-based one-class SVM classifier[A]. Proceedings of the International Conference on Parallel Processing[C]. 2009. 409-414.

[10] BARANI F, GERAMI S. ManetSVM: dynamic anomaly detection using one-class support vector machine in MANETs[A]. Proceedings of 10th International ISC Conference on Information Security and Cryptology[C]. 2013.1-6.

[11] CHEN Y T, QIAN J, SALIGRAMA V. A new one-class SVM for anomaly detection[A]. IEEE International Conference on Acoustics, Speech and Signal Processing[C]. 2013.3567-3571.

[12] VAPNIK V N. The Nature of Statistical Learning Theory[M]. New York: Springer-Verlag Inc, 2000.

[13] ANGLUIN D. Queries and concept learning [J]. Machine Learning, 1988, 2(4): 319-342

[14] ALMGREN M, JONSSON E. Using active learning in intrusion detection[A]. Proceedings of 17th IEEE Computer Security Foundations Workshop[C]. 2004.88-98.

[15] 李洋, 方滨兴, 郭莉, 等. 基于主动学习和 TCM-KNN 方法的有指导入侵检测技术[J]. 计算机学报,2007,30(8):1464-1473.
LI Y, FANG B X, GUO L, *et al*. Supervised intrusion detection based on active learning and TCM-KNN algorithm[J]. Chinese Journal of Computers, 2007,30(8):1464-1473.

[16] 龙军, 殷建平, 祝恩, 等. 针对入侵检测的代价敏感主动学习算法[J].南京大学学报(自然科学版),2008,44(5):527-535.
LONG J, YIN J P, ZHU E. Cost-sensitive active learning algorithm for intrusion detection[J].Journal of Nanjing University(Natural Sciences),2008,44(5): 527-535.

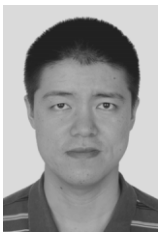
[17] SELIYA N, KHOSHGOFTAAR T M. Active learning with neural networks for intrusion detection[A]. IEEE International Conference on Information Reuse and Integration[C]. 2010.49-54.

[18] GU Y J, ZYDEK D. Active learning for intrusion detection[A]. 2014 National Wireless Research Collaboration Symposium[C]. 2014.117-122.

[19] SMOLA A, SCHÖLKOPF B. Learning with Kernels[M]. Cambridge MITPress, 1998.

[20] SETTLES B. Active learning literature survey[J]. University of Wisconsin, 2010, 52(11):55-66.

作者简介：



刘敬[通信作者]（1981-），男，河北石家庄人，北京邮电大学博士生，主要研究方向为网络安全和数据挖掘。E-mail:liujing81@sohu.com。

谷利泽（1965-），男，辽宁营口人，北京邮电大学教授、硕士生导师，主要研究方向为密码学和网络安全。

钮心忻（1963-），女，浙江湖州人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、数字内容及安全。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为编码理论、密码学、信息安全、信号与信息处理。