文章编号:1007-5321(2021)02-0033-07 **DOI**:10.13190/j.jbupt.2020-114

基于迁移学习的跨域异常流量检测

彭雨荷, 陈 翔, 陈双武, 杨 坚
(中国科学技术大学 信息科学技术学院, 合肥 230026)

摘要: 基于已知数据的机器学习模型在实际异常流量检测任务中不完全可靠,为此,将不同分布的流量分别作为源域和目标域,建立跨域网络异常流量检测框架,提出了基于联合分布适配的迁移学习方法. 通过寻找最优变换矩阵、适配源域与目标域之间的条件概率和边缘概率,实现源域与目标域间的特征迁移,从而解决由于源域与目标域分布差异大所引起的检测准确率下降等问题. 实验结果表明,所提方法可以显著提升跨域流量的检测准确率.

关 键 词: 异常流量检测; 跨域; 迁移; 联合分布适配; 机器学习
中图分类号: TP393.08 **文献标志码**: A

Cross-Domain Abnormal Traffic Detection Based on Transfer Learning

PENG Yu-he, CHEN Xiang, CHEN Shuang-wu, YANG Jian
(School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China)

Abstract: In order to solve the problem that the machine learning model based on known data is not completely reliable in actual abnormal traffic detection tasks due to the dynamics of the network environment. The different distributed traffic as the source domain and target domain is used to establish a cross-domain framework for abnormal network traffic detection. The transfer learning method based on joint distribution adaptation is proposed by finding the optimal transformation matrix, adapting the conditional probability and edge probability between the source domain and the target domain, the feature transfer between the source domain and the target domain is realized thereby for solving the problem of the large difference in the distribution of the source domain and the target domain causes problems such as decreased detection accuracy. Experiments show that the proposed method can significantly improve the detection accuracy of cross-domain traffic.

Key words: abnormal traffic detection; cross-domain; transformation; joint distribution adaptation; machine learning

随着信息技术的发展,网络安全系统受到的威胁日益严重. 根据思科白皮书[1]的报道,2018 年 9 月共记录到 864 次由于恶意攻击造成的数据泄露,因此带来的损失难以估量. 为了维护网络安全,入侵检测技术[2]一直都备受关注. 误用检测[3]技术通过对已知异常行为规则进行建模与匹配,实现了针对异常流量的检测[4];传统基于签名[5]的检测方法通过在数据包中搜索已知异常行为的特定字节等

收稿日期: 2020-08-04
基金项目: 国家重点研发计划项目(2018YFF01012200); 中央高校基本科研业务费专项资金项目(WK2100000009); 安徽省自然科学基金项目(1908085QF266)
作者简介: 彭雨荷(1996—), 女, 硕士生.
通信作者: 陈双武(1988—), 男, 副研究员, E-mail:chensw@ustc.edu.cn.

判断其是否为异常流量.

1 传统机器学习算法在流量检测领域的局限性

由于异常网络流量的多样性和保密性,基于签名和行为的检测不再可靠,机器学习逐渐流行[6]. 虽然常规机器学习算法在异常流量检测领域具有较高的准确率[7],但这些算法都是建立在假定训练集和测试集中的数据具有相同的特征分布之上的,而实验数据集和实际应用场景中的数据却并非如此.

通常,将1个时期或站点中收集的标记流量视为源域;将另一时期或站点中收集的未标记流量视为目标域. 预先训练的机器学习模型无法描述出不同域之间的动态变化,因此跨域异常流量检测往往不能取得理想中的检测效果. 而造成跨域异常流量检测准确率较低的根本原因在于源域和目标域间特征的条件分布与边缘分布存在差异.

从CICIDS2017[8]和CSE-CIC-IDS2018[9]数据集中选取了部分异常流量进行特征分布评估,并分别选取了传输数据包个数与数据流激活前的平均空闲时间2个特征,分别得出其条件分布的累计分布,如图1所示. 可以看出,2个数据集捕获流量的网络环境差异使得2个特征的取值较为分散. 类似于图1中由于网络环境改变导致的分布差异即被称为域偏移. 正因为域偏移的存在,预先训练好的模型应用于新环境时,检测准确性将会大幅度下降.

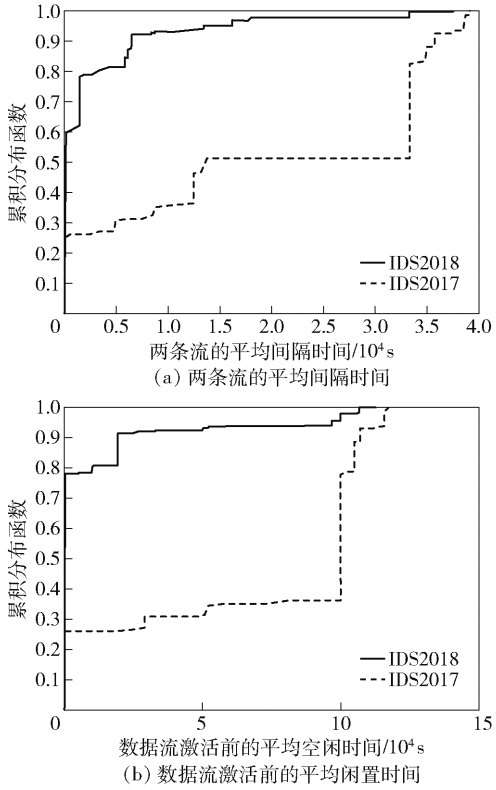

图1 IDS2017与IDS2018数据集间的特征条件分布

为了解决域偏移问题,Pan等[10]提出了一种基于迁移学习的跨域异常流量检测的框架,并且在该框架中引入了一种基于联合分布适配[11]的跨域异常流量检测方法,解决了源域与目标域流量特征分布差异较大的问题. 此外,实验部分基于真实数据集验证了方法的性能. 实验结果表明,该方法在传统机器学习算法的基础上最多可以提高56%左右的检测准确率.

2 基于联合分布适配的异常流量检测

与现有方法相比,基于联合分布适配(JDA, joint distribution adaptation)的方法通过特征适配提高了目标域检测的准确性. 该方法第1次被引入跨域异常流量检测.

2.1 问题描述

训练与实际应用中流量特征分布的差异会导致检测准确性大幅下降. 因此,实际的异常流量检测任务被表述为迁移学习问题,用不同特征分布的网络流量分别作为训练(源域)和测试(目标域)流量,在表征空间中最小化二者间的距离,以实现跨域流量特征条件与边缘分布的联合适配.

在跨域异常检测任务中,给定1个源域 D_s,包含 n_s 个有标签的网络流量特征向量 $\boldsymbol{x}_s$;给定1个目标域 D_t,包含 n_t 个无标签的网络流量特征向量 $\boldsymbol{x}_t$. 设源域和目标域的异常流量检测任务分别为 T_s 和 T_t,异常检测任务中假定源域和目标域特征的条件分布与边缘分布均不相同,有 $Q(\boldsymbol{y}_s|\boldsymbol{x}_s)\neq Q(\boldsymbol{y}_t|\boldsymbol{x}_t)$, $P(\boldsymbol{x}_s)\neq P(\boldsymbol{x}_t)$. 该方法旨在学习合适的映射函数 $f(\boldsymbol{x}_s)$ 和 $f(\boldsymbol{x}_t)$ 来预测异常流量类型. 因此,直接将源域训练出的映射函数 $f(\boldsymbol{x}_s)$ 作为目标域 D_t 的预测函数是不准确的. 此外,源域 D_s 和源任务 $f(\boldsymbol{x}_s)$ 的信息可以提高 D_t 域中目标任务 $f(\boldsymbol{x}_t)$ 的学习能力,即通过不断适配源域与目标域间的条件分布和概率分布,从而实现跨域流量检测.

2.2 基于联合分布适配的流量检测框架

基于联合分布适配的流量检测框架主要由特征迁移模块和分类器模块2部分组成. 如图2所示,特征迁移模块实现边缘分布与条件分布的适配,并通过多次迭代获取最佳特征. 分类器模块则通过主分类器对特征迁移模块获取的最佳特征进

行训练及测试，以达到跨域异常流量检测的目的.

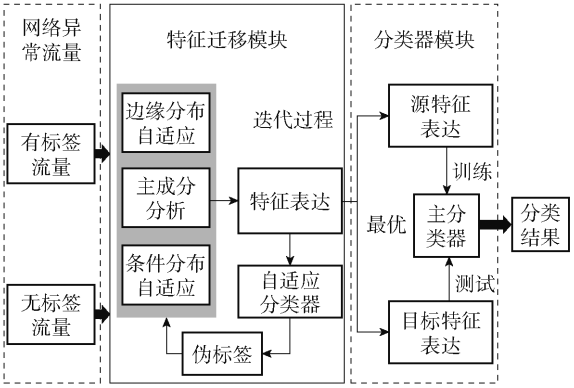

图 2　基于联合分布适配的流量检测框架

首先，将训练流量（源域）和测试流量（目标域）输入至特征迁移模块，通过主成分分析法对输入的流量进行降维. 由于输入的测试数据为无标签流量，特征迁移模块使用自适应分类器生成测试数据的伪目标标签，并在迭代过程中反复调整标记流量、未标记流量的条件分布和概率分布，直至获得源域和目标域间概率分布与条件分布距离相近的最佳特征表达. 分类器模块通过主分类器对最优源特征表达进行训练，并在最优目标特征表达上进行测试. 在获得最佳特征表达之前，分类器模块中的主分类器仅用来预测目标标签，不参与迭代过程；获得最佳特征表达之后，主分类器使用最佳特征表达进行训练和测试，最终得到迁移后网络流量的检测结果.

2.3　基于联合分布适配的具体方法

如前所述，基于 JDA 的方法旨在找到正交变换矩阵，以减少表征空间中 2 个数据集之间边缘分布和条件分布的差异. 最后，由源特征和攻击类型标签训练的预测函数 $f(\boldsymbol{x}_s)$ 即可用于识别目标域中的异常流量类型.

1）特征降维

在进行特征分布适配前，需要重构输入流量特征，在降低计算复杂度并消除冗余特征干扰的同时不丢失重要信息. 这里选择主成分分析法，令 $\boldsymbol{X}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n]\in R^{m\times n}$ 为输入流量矩阵，其中 $n=n_s+n_t$ 为源域和目标域数据特征的数量之和，m 为流量特征向量 $\boldsymbol{x}$ 的特征数. 主成分分析法将 n 维输入优化为正交空间中的 k 维主成分，各主成分之间的信息不重合. 最大化新 k 维正交空间中的方差，有

$$\max_{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{I}}\operatorname{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{H}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}) \tag{1}$$

其中：$\boldsymbol{H}=\boldsymbol{I}_n-\frac{1}{n}\mathbf{1}_n\mathbf{1}_n^{\mathrm{H}}$ 为中心矩阵，$\mathbf{1}_n=[1,\cdots,1]^{\mathrm{H}}\in\mathbb{R}^{n\times 1}$ 为全 1 的列向量，记为 $\mathbf{1}$；$\boldsymbol{A}\in\boldsymbol{\Phi}^{m\times k}(k<m)$ 为正交变换矩阵. 在特征映射之后，可将原始的 m 维异常流量特征 $\boldsymbol{X}$ 转换为 k 维特征表示空间 $\boldsymbol{Z}$，以下工作均在优化后的 k 维特征表示空间上执行.

2）分布自适应

尽管主成分分析法使原本高维的网络流量特征转化为更高效的特征表示，但源域和目标域流量间的特征分布差异仍然很大. 因此，提出了基于 JDA 的方法，通过求出最小分布距离时的正交变换矩阵 $\boldsymbol{A}$，实现条件分布与边缘分布自适应.

将表征空间中边缘分布 $P(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_s)$ 和 $P(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_t)$ 之间的最大均值误差的估计式化为式(2)，可反映来自 2 个域特征的边缘分布差异：

$$\left\|\frac{1}{n_s}\sum_{i=1}^{n_s}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_i-\frac{1}{n_t}\sum_{j=n_s+1}^{n_s+n_t}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_j\right\|^2=\operatorname{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{M}_0\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}) \tag{2}$$

其中：最大均值误差矩阵 $\boldsymbol{M}_0$ 反映了源域与目标域流量间的边缘分布距离，有

$$(\boldsymbol{M}_0)_{ij}=\begin{cases}\dfrac{1}{n_s^2}, & \boldsymbol{x}_i,\boldsymbol{x}_j\in D_s\\ \dfrac{1}{n_t^2}, & \boldsymbol{x}_i,\boldsymbol{x}_j\in D_t\\ -\dfrac{1}{n_sn_t}, & \text{其他}\end{cases} \tag{3}$$

除了边缘分布适配，还考虑了条件分布适配. 通过构造自适应分类器预测出伪标签，然后使用最大均值误差距离来估计 $Q_s(\boldsymbol{y}_s|\boldsymbol{x}_s)$ 和 $Q_t(\boldsymbol{y}_t|\boldsymbol{x}_t)$ 之间的分布差异. 类别标签为 c 时，类条件分布 $Q_s(\boldsymbol{x}_s|\boldsymbol{y}_s=c)$ 和 $Q_t(\boldsymbol{x}_t|\boldsymbol{y}_t=c)$ 之间的最大均值误差距离为

$$\left\|\frac{1}{n_s^{(c)}}\sum_{\boldsymbol{x}_t\in D_s^{(c)}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_i-\frac{1}{n_t^{(c)}}\sum_{\boldsymbol{x}_j\in D_t^{(c)}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x}_j\right\|^2=\sum_{c=0}^{C}\operatorname{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{M}_c\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}) \tag{4}$$

其中：$D_s^{(c)}$ 为源域中属于攻击类型标签为 c 的异常流量的集合，$D_t^{(c)}$ 为目标域中属于伪攻击类型标记为 c 的异常流量的集合，C 为标签类别集合.

最大均值误差矩阵 $\boldsymbol{M}_c$ 反映了源域与目标域中异常流量间的条件分布距离，计算如下：

$$(\boldsymbol{M}_c)_{ij}=\begin{cases}\dfrac{1}{n_{\mathrm{s}}^{(c)}n_{\mathrm{s}}^{(c)}}, & \boldsymbol{x}_i,\boldsymbol{x}_j\in D_{\mathrm{s}}^{(c)}\\ \dfrac{1}{n_{\mathrm{t}}^{(c)}n_{\mathrm{t}}^{(c)}}, & \boldsymbol{x}_i,\boldsymbol{x}_j\in D_{\mathrm{t}}^{(c)}\\ \dfrac{-1}{n_{\mathrm{s}}^{(c)}n_{\mathrm{t}}^{(c)}}, & \begin{cases}\boldsymbol{x}_i\in D_{\mathrm{s}}^{(c)}, & \boldsymbol{x}_j\in D_{\mathrm{t}}^{(c)}\\ \boldsymbol{x}_j\in D_{\mathrm{s}}^{(c)}, & \boldsymbol{x}_i\in D_{\mathrm{t}}^{(c)}\end{cases}\\ 0, & \text{其他}\end{cases}\tag{5}$$

特征迁移模块的作用在于减少源域和目标域间边缘和条件分布的差异. 因此,结合式(2)和式(4),根据广义 Rayleigh 商将反映异常流量的分布距离优化为

$$\min_{\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{H}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{I}}\sum_{c=0}^{C}\operatorname{tr}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{M}_c\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A})+\lambda\|\boldsymbol{A}\|_{\mathrm{F}}^2\tag{6}$$

其中:$\lambda\|\boldsymbol{A}\|_{\mathrm{F}}^2$ 为正则化部分,当流量类别标签 $c=0$ 时式(6)反映了源域与目标域间异常流量边缘分布自适应的情况;当 $c\neq0$ 时则为条件分布自适应的情况.

利用拉格朗日乘数法来解决式(6)中的优化问题,其中 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{H}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{I}$ 为约束条件,其目的是通过求解式(7)找到最佳正交变换矩阵 $\boldsymbol{A}$,有

$$\left(\boldsymbol{X}\sum_{c=0}^{C}\boldsymbol{M}_c\boldsymbol{X}^{\mathrm{T}}+\lambda\boldsymbol{I}\right)\boldsymbol{A}=\boldsymbol{X}\boldsymbol{H}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{\Phi}\tag{7}$$

其中 $\boldsymbol{\Phi}=\operatorname{diag}(\phi_1,\phi_2,\cdots,\phi_k)\in R^{k\times k}$ 为拉格朗日乘数.

为了解决伪标签的准确性问题,通过多次迭代优化了特征迁移模块的最优变换矩阵.

特征迁移算法的复杂度计算如下:最大均值误差矩阵 $\boldsymbol{M}_0$ 和 $\boldsymbol{M}_c$ 的计算复杂度为 $O(TCn^2)$,迁移矩阵 $\boldsymbol{A}$ 以及最佳特征表达 $\boldsymbol{Z}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}$ 的计算复杂度为 $O(Tkm^2)$,其余步骤的计算复杂度为 $O(Tmn)$,因此该算法总计算复杂度为 $O(TCn^2+Tkm^2+Tmn)$. 其中:m 为特征维数,$n=n_{\mathrm{s}}+n_{\mathrm{t}}$ 是源训练集和目标测试集数据特征数量之和,k 为迁移后特征维数,T 为最大迭代周期.

算法1 特征迁移

输入:源和目的流量特征 $\boldsymbol{X}$,源标签 $\boldsymbol{Y}_{\mathrm{s}}$,正则化参数 λ,维度 k 和最大迭代周期 t.

输出:新的特征表示 $\boldsymbol{Z}_{\mathrm{s}}$ 和 $\boldsymbol{Z}_{\mathrm{t}}$,迁移矩阵 $\boldsymbol{A}$.

1 根据式(5)构造最大均值误差矩阵 $\boldsymbol{M}_0$
2 for $t=1$ to t do
3 if 伪标签 $\hat{\boldsymbol{Y}}_{\mathrm{t}}$ 存在 then
4 根据式(6)构造最大均值误差矩 $\boldsymbol{M}_c(c\neq0)$
5 end if
6 通过求解式(7)获得最佳迁移矩阵 $\boldsymbol{A}$
7 通过 $\boldsymbol{Z}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X}$ 获得最佳特征表达 $\boldsymbol{Z}_{\mathrm{s}}$
8 用 $\boldsymbol{Z}_{\mathrm{s}}$ 训练自适应分类器,以预测伪标签 $\hat{\boldsymbol{Y}}_{\mathrm{t}}$
9 $i=i+1$
10 end for
11 返回 $\boldsymbol{Z}_{\mathrm{s}},\boldsymbol{Z}_{\mathrm{t}},\boldsymbol{A}$

3) 基于特征表示的分类器

在特征迁移模块中进行特征映射和分布适配后,属于同一类型的流量特征已足够相似. 此时,便可通过源测试集中的流量检测任务 $f(\boldsymbol{x}_{\mathrm{s}})$ 识别目标训练集中无标签的流量数据. 为了尽快找到最佳转换矩阵 $\boldsymbol{A}$,用特征转换模块训练了1个自适应分类器,并经过多次迭代寻找最优特征表达. 因为使用迭代更新无法保证其稳定性和鲁棒性,分类器模块中训练了1个主分类器,使用转换后的源特征表示 $\boldsymbol{Z}_{\mathrm{s}}$ 训练该主分类器,在获得最佳变换矩阵后,主分类器用其重新训练,并评估最佳变换矩阵的有效性和功能性.

3 跨域流量检测性能实验

在 CICIDS2017 和 CSE-CIC-IDS2018 两个入侵检测数据集上做了5个实验. 第1个实验从特征迁移后的2个数据集中分别选取了2组数据绘制成累计分布图;第2个实验将基于联合分布适配方法的性能与传统机器学习进行了对比;第3个实验将基于联合分布适配的方法与另一种无监督迁移学习方法进行对比;第4个实验对比了使用不同机器学习算法分别训练自适应分类器和主分类器时,2个分类器之间的相互作用效果;第5个实验将5种分类器50次迭代的准确率绘制成折线图.

3.1 实验实施

实验在 Intel Xeon CPU E5-2620 v2 服务器上运行,服务器配置有 2.10 GHz 主频和 64 GB 内存.

3.1.1 数据集

实验要求2个数据集中相同攻击种类较多,且捕获的时间、地点不同,而选择 IDS2017 和 IDS2018 数据集即可达到这个目的. 其中,IDS2017 数据集捕获了 2017-07-03—2017-07-07 内各个时间段的13种攻击数据和正常流量数据. 而 IDS2018 数据集捕获了另一地点在 2018-02-14—2018-03-02 中9 d 的各时间段12种攻击数据和正常流量数据.

因为不同年份数据集中的流量样本分布不均,实验中仅选择了正常流量与数量较多的5种异常流

量. 此外,由于 2 个数据集中的特征并不完全相同,从中选取了 71 个共同特征进行实验. 将 IDS2017 数据集中选取的数据作为训练集(源域), IDS2018 数据集中选取的数据作为测试集(目标域),所选异常流量的类别和其对应的数量如表 1 所示.

表 1　实验流量类别及数量

类别	训练集	测试集
正常流量	1 404	1 916
Botnet ARES 攻击	1 966	833
暴力破解 Web 攻击	1 473	609
DOS Slowloris 攻击	1 278	2 036
DOS Hulk 攻击	3 288	3 507
DOS GoldenEye 攻击	1 016	1 214
总计	10 425	10 115

3.1.2　评估指标

1）检测准确率

$$P=\frac{H+N}{H+Q+F+N} \tag{8}$$

其中:H 为将样本 $\boldsymbol{X}$ 正确检测为 $\boldsymbol{X}$ 的样本数,N 为将不是 $\boldsymbol{X}$ 的样本正确检测为不是 $\boldsymbol{X}$ 的样本数,Q 为将不是 $\boldsymbol{X}$ 的样本错误地检测为 $\boldsymbol{X}$ 的样本数,F 为将样本 $\boldsymbol{X}$ 错误地检测为不是 $\boldsymbol{X}$ 的样本数.

2）单次迭代时间

$$T=\frac{T_{\mathrm{ttl}}}{t_{\mathrm{ttl}}} \tag{9}$$

其中:T_{ttl} 为特征转换模块运行总时间,t_{ttl} 为总迭代次数.

3.2　实验结果

实验采用了 5 种机器学习方法分别构造主分类器与自适应分类器. 这 5 个模型分别为 k 最近邻(KNN, k-nearest neighbor)、决策树(DT, decision tree)、多层感知器(MLP, multilayer perceptron)、朴素贝叶斯(NB, naive Bayesian)和随机森林(RF, random forest).

对表 1 所示的 6 种流量做多分类任务,正则化参数设为 1,最大迭代次数 t 设为 40,新特征维数设为 40,取数据集总检测的准确率为实验结果.

3.2.1　特征映射

特征迁移模块通过主成分分析以及最大均值差异法对输入的流量特征进行迁移,图 3 所示为特征映射后部分源域与目标域流量特征的条件分布,分别取自 IDS2017 数据集和 IDS2018 数据集,x 轴为归一化之后的特征参数值,分布在 -1 ~ 1. 与图 1 中的原始数据相比,源域与目标域特征分布距离明显减小. 这说明特征适配效果明显,对提高实验结果的准确率有积极作用.

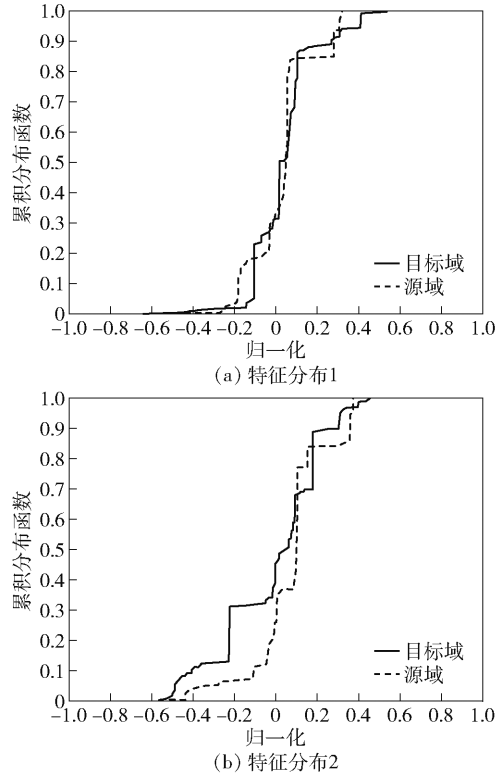

图 3　特征映射后源域与目标域特征的条件分布

3.2.2　基于联合分布适配方法的性能

为分析特征分布适配前后的检测准确性变化,实验中使用传统机器学习模型、JDA 方法分别在源流量域和目标流量域上进行测试. 如图 4 所示,当源域中训练的模型直接应用于目标域流量时,分类器的性能会急剧下降. 而使用 JDA 方法进行分布适配之后,5 种分类器的准确性均得到了较大提高. 其中,NB 算法的准确率提升最大,从 18.62% 提升至 75.47%. 虽然基于不同机器学习算法进行特征迁移之后的检测准确率都得到了部分提升,但提升效果差异较大,可能是因为在特征适配之后各维度特征间的信息互不重合,在 NB 算法上有更好的表现效果. 而该特征在其余机器学习算法上的优势相对较小,实验的目的即利用现有的输入信息,基于实验方法框架找出表现最好的机器学习方法.

3.2.3　基于 JDA 的方法与迁移成分分析算法的对比实验

通过实验对比了另一种常见的无监督迁移学习

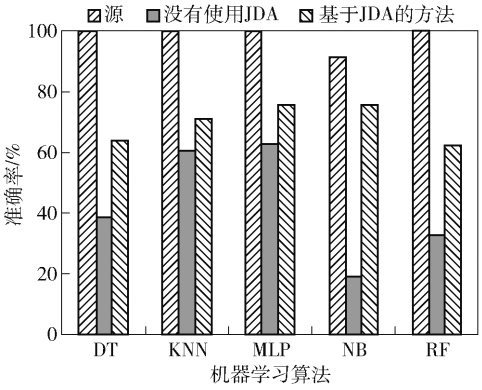

图4 基于JDA方法的性能

方法——迁移成分分析(TCA, transfer componet analysis)算法[12]. TCA算法仅适配了边缘分布. 实验仅考虑不同无监督迁移学习方法的效果差异,2种分类器使用相同的机器学习模型. 图5显示了将以上2种迁移学习方法应用于目标域中的检测准确性. 显然,基于JDA的方法比TCA算法具有更好的性能. 其中,TCA算法对于部分算法相较于迁移之前反而有所下降,而JDA方法在TCA算法准确度的基础上分别提升了43.44%、5.45%、17.59%、5.24%和30.31%. 因此,同时执行边缘和条件分布适配更有利于消除特征差异,仅考虑边缘分布的适配则有可能引入其他误差. 此外,相较于TCA算法,基于JDA的方法在训练中使用了源域流量的标签信息,这对于提高最终迁移后的准确性也起到了关键作用.

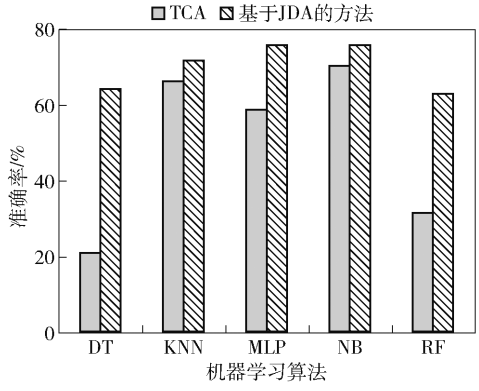

图5 基于不同方法时的性能比较

3.2.4 自适应分类器与主分类器的相互作用实验

使用5种不同的主分类器来评估最佳转换矩阵的有效性和通用性以及2种分类器之间的相互作用效果. 采用机器学习的方法构造2种分类器. 如图6所示,分别获得了25个准确度作为评估的标准. 其中,作为自适应分类器,MLP和NB算法的性能相对而言要优于其他3种算法,而不论选择哪种机器学习模型作为主分类器时,RF和DT算法作为自适应分类器的结果检测都相对较低,说明这2种算法在进行特征迁移时得到的新的特征表示不足以主分类器进行学习和检测. 作为主分类器,MLP和NB算法作为主分类器的性能相对较好,而当NB算法作为主分类器,MLP作为自适应分类器时,检测准确率最高,达到了79.15%.

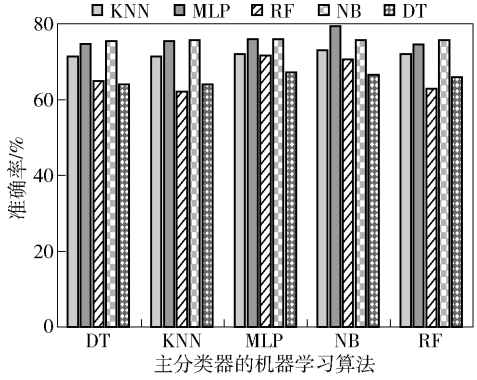

图6 使用不同自适应分类器的主分类器性能

3.2.5 迭代次数选择

实际应用时,最佳迭代次数t较难确定,但该方法中目标域数据不需要标签,因此较易获得数据. 在实际场景中,可先获取部分数据进行预训练,根据真实场景调整参数. 图7所示为5种分类器的机器学习算法50次迭代的准确率. 可以看出,各分类器随着迭代次数增加准确率的变化逐渐趋于平稳,并于40次左右收敛. 在预训练中,可以根据迭代过程中的数据确定大致收敛范围,在该范围内,如果准确率的变化不超过一定误差则可视为最终数据.

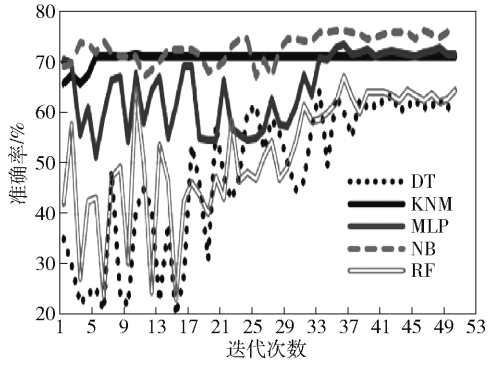

图7 迭代过程的准确率

选择收敛之后的迭代次数作为参数t的值,因

此，了解每种模型的单次迭代时间尤为重要. 表 2 所示为基于不同模型的 1 次迭代的平均时间. 可以看到，NB 算法 1 次迭代的平均时间最短，而 KNN 算法的平均时间最长. 结合上述实验，得出了以下结论：对于自适应分类器的选择，NB 算法在耗时和检测准确度的实验中均表现良好，而 MLP 算法的时间性能相对 NB 较差，但检测准确度高. 因此，在时间要求不高的情况下，NB 与 MLP 算法均为自适应分类器的最佳选项；对时间要求较高时优先选择 NB 算法. 对于主分类器，NB 和 MLP 准确度相对较高，均为最佳选择.

表 2　5 种自适应分类器的平均迭代时间

机器学习算法	花费时间/s
KNN	20.43
DT	18.62
MLP	19.63
RF	19.53
NB	17.88

4　结束语

针对动态网络场景下的跨域异常流量检测问题，基于 JDA 的异常检测方法，解决由外部环境改变而造成的准确率下降问题. 然而，这种算法会产生高维特征迁移矩阵的搜索问题，受限于当前服务器的计算和存储资源，对训练数据集的规模有一定要求；此外，大规模数据集的模型训练还存在收敛速度较慢的问题，这都是未来工作中的研究重点.

参考文献：

[1] Cisco V. Cisco visual networking index: forecast and trends, 2017—2022[R]. San Jose: [s. n.], 2018: 1-38.

[2] Ahmed M, Mahmood A N, Hu J. A survey of network anomaly detection techniques[J]. Journal of Network and Computer Applications, 2016(1): 19-31.

[3] Li C, Gu Z, Zhou M, et al. API misuse detection in C programs: practice on SSL APIs[J]. International Journal of Software Engineering & Knowledge Engineering, 2019, 29(11): 1761-1779.

[4] 吉星，黄韬，鄂新华，等. 基于日志信息的 DNS 查询异常检测算法[J]. 北京邮电大学学报，2018，41(6)：83-89.
Ji Xing, Huang Tao, E Xinhua, et al. A DNS query anomaly detection algorithm based on log information[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(6): 83-89.

[5] Du Z, Ma L, Li H, et al. Network traffic anomaly detection based on wavelet analysis[C]//2018 IEEE 16th International Conference on Software Engineering Research, Management and Applications (SERA). Kunming: IEEE, 2018: 94-101.

[6] Wang M, Cui Y, Wang X, et al. Machine learning for networking: workflow, advances and opportunities[J]. IEEE Network, 2017, 32(2): 92-99.

[7] Almseidin M, Alzubi M, Kovacs S, et al. Evaluation of machine learning algorithms for intrusion detection system[C]//2017 IEEE 15th International Symposium on Intel-Ligent Systems and Informatics (SISY). Subotica: IEEE, 2017: 277-282.

[8] Sharafaldin I, Lashkari A H, Ghorbani A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]// ICISSp. Portugal: SciTe-Press, 2018: 108-116.

[9] Canadian Institute for Cybersecurity. CSE-CIC-IDS2018 on AWS[DB/OL]. Canadian: University of New Brunswick, 2019: 1-1[2020-04-01]. https://www.unb.ca/cic/datasets/ids-2018.html.

[10] Pan S J, Yang Q. A survey on transfer learning[J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 22(10): 1345-1359.

[11] Long M, Wang J, Ding G, et al. Transfer feature learning with joint distribution adaptation[C]// Proceedings of the IEEE International Conference on Computer Vision. Sydney: IEEE, 2013: 2200-2207.

[12] Pan S J, Tsang I W, Kwok J T, et al. Domain adaptation via transfer component analysis[J]. IEEE Transactions on Neural Networks, 2010, 22(2): 199-210.