计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200600025

基于 Borderline-SMOTE 和双 Attention 的入侵检测方法

刘全明　李尹楠　郭　婷　李岩纬
山西大学计算机与信息技术学院　太原 030006

摘　要　随着互联网的发展,网络环境愈加复杂,由此导致的网络安全问题不断出现,因此网络安全的防护成为一项重要研究课题。针对真实网络环境中采集到的流量数据非平衡以及传统机器学习方法提取特征表示不准确等问题,文中提出一种基于 Borderline-SMOTE 和双 Attention 的入侵检测方法。首先对入侵数据进行 Borderline-SMOTE 过采样处理,解决了数据非平衡问题,并且利用卷积网络在图像特征提取方面的优势,将一维流量数据转化为灰度图像;然后通过双注意力网络分别从通道维度和空间维度对低维特征进行维度更新,得到更精准的特征表示;最后利用 Softmax 分类器对流量数据进行分类预测。所提方法的仿真实验均已在 NSL-KDD 数据集上得到验证,其准确率达到 99.24%,相比其他常用方法准确率更高。

关键词:网络安全;Borderline-SMOTE;双 Attention;入侵检测;非平衡问题
中图法分类号　TP181

Intrusion Detection Method Based on Borderline-SMOTE and Double Attention

LIU Quan-ming,LI Yin-nan,GUO Ting and LI Yan-wei
School of Computer and Information Technology,Shanxi University,Taiyuan 030006,China

Abstract　With the development of Internet,the network environment is becoming more complex,and the resulting network security problems continue to emerge,so the protection of network security becomes an important research topic. Aiming at the problems of unbalanced traffic data collected in real network environment and inaccurate feature representation extracted by traditional machine learning methods,this paper proposes an intrusion detection method based on Borderline-SMOTE and dual attention. Firstly,this method performs Borderline-SMOTE oversampling on the intrusion data to solve the problem of data imbalance,and uses the advantages of convolutional networks for image feature extraction to convert 1D flow data into grayscale images. Then it updates the low-dimensional features from the channel dimension and the spatial dimension to obtain a more accurate feature representation respectively. Finally,it uses the Softmax classifier to classify and predict traffic data. The simulation experiments of the proposed method have been verified on the NSL-KDD data set,and the accuracy reaches 99.24%. Compared with other commonly used methods,it has a higher accuracy.

Keywords　Network security,Borderline-SMOTE,Double Attention,Intrusion detection,Unbalanced problems

1　引言

近年来,随着互联网的高速发展和网络技术的日趋成熟,互联网的接入变得更加简单,但却形成了更加复杂的网络环境,人们在享受网络带来的便利的同时也遭受着网络攻击,因此网络安全问题亟待解决。《2019 年我国互联网网络安全态势综述》显示,高危漏洞数量上升,新型攻击不断出现,因此对于安全防护技术的研究引起了广泛关注。

入侵检测系统(Intrusion Detection System,IDS)是监视网络流量并尝试监测可疑活动的系统,作为一种主动防御技术,在安全防护领域发挥着重要作用。目前,根据观察对象的不同,入侵检测系统可分为两种。第一种是基于签名的入侵检测,称为误用检测[1]。误用入侵检测通过将攻击特征库中的流量特征与新的流量特征进行匹配来达到检测入侵行为的目的,其缺点是难以检测未知入侵攻击行为,并且特征库的维护工作量巨大。第二种是基于行为的入侵检测,称为异常检测[2]。异常检测通过对正常行为的学习,建立起正常行为模式作为先验知识,将新的流量特征与正常行为模式进行比较,如果差异超过阈值,则归类为异常流量,以此来检测入侵,其优点是能够检测新型未知攻击,缺点是行为模型建立困难。

目前已有多种异常入侵检测方法,许多异常检测与攻击分类都是基于传统机器学习方法完成的。例如,Tan 等[3]利用改进的粒子群算法来确定 SVM 分类器的重要参数,从而进行入侵特征识别,在 DoS 攻击类别和 Probe 攻击类别上分

到稿日期:2020-06-03　返修日期:2020-10-04　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61673295);山西省国际科技合作重点研发计划项目(201903D421050)
This work was supported by the National Natural Science Foundation of China(61673295) and Shanxi Provincial International Science and Technology Cooperation Key R&D Program Project(201903D421050).
通信作者:刘全明(liuqm@sxu.edu.cn)

别具有较高的检测率和较低的误报率，但未考虑该方法对其他攻击类别的识别效果；Zhao[4]提出了一种基于SVM主动学习的入侵检测优化算法，利用最小二乘SVM来改进SVM训练效率，生成一系列加权基学习器，并将其用于入侵检测模型；Ren等[5]根据网络流量的相似性提出一种类别检测划分方法，该方法避免了异常行为在检测过程中的相互干扰，他们结合这种划分方法构建了多层次的随机森林模型来检测网络异常行为，能够有效地检测Probe，U2R和R2L这3种攻击类型，但检测结果仍有很大的提升空间。基于传统机器学习的入侵检测方法面对高维特征时需要人工提取大量特征，存在特征提取困难、提取特征不准确等共性劣势。近年来，伴随着人工智能的热潮，机器学习已被应用于很多领域，深度学习作为机器学习的一个重要分支，由于具有超强的非线性拟合能力，且能够从复杂特征中提取出具有主要意义的特征，已经在文本处理、图像、语音、视频等复杂领域中获得了巨大的成就[6]。基于深度学习的方法很好地解决了基于传统机器学习的检测方法的共性劣势，并且有研究表明，将深度学习方法应用于入侵检测分类的效果优于传统机器学习方法。Raff等[7]将长短期记忆网络(Long Short-Term Memory，LSTM)和注意力机制相结合用于恶意软件的检测，取得了较好的效果。Shi等[8]提出了一种相关信息熵特征选择和混合深度学习算法相结合的工业控制入侵检测方法，并使用Borderline-SMOTE算法对数据进行非平衡处理，同时利用注意力机制为特征重新进行权重分配，达到了较高的准确率和较低的误报率。Wang等[9]提出了一种基于卷积神经网络的入侵检测系统，虽然其总体准确率可达到99%以上，但针对相似性较大的攻击类型其检测率仍有提升空间。Phetlasy等[10]利用SMOTE算法对训练数据集中的少数类进行过采样处理，并提出一种将多个分类器组合的分类方法，该方法可以将未被第一个分类器分类正确的流量数据送入第二个分类器重新分类，将未被第二个分类器分类正确的流量数据送入第三个分类器重新分类，以提高分类的灵敏度和准确率。Ding等[11]通过叠加加入了正则化修正的多个自编码网络来构建深度自编码网络模型，以学习并获取流量数据的低维特征表示，并通过BP算法对这些低维特征进行分类识别.虽然该方法取得了较优效果，但对于U2R和R2L这两种攻击类别的检测率仍有提升空间。

因此，针对真实网络环境中获取到的流量数据存在数据非平衡问题，以及传统机器学习方法中特征提取困难、特征表达不准确的问题，本文提出了一种基于Borderline-SMOTE[12]和双Attention的入侵检测方法。首先，为了解决数据非平衡问题，采用Borderline-SMOTE方法对数据进行过采样处理；然后通过卷积神经网络获取数据的低维特征表示，并剔除无关属性特征；接下来将得到的流量低维特征表示输入到双Attention网络中，分别从通道和空间两个维度为对分类结果影响较大的特征分配更高的权重，进一步更新特征表示；最后通过Softmax分类器对流量进行分类预测。

2 理论基础

2.1 Borderline-SMOTE

Borderline-SMOTE是一种对样本量较少的类别进行过采样处理的合成采样算法。具体地，对于一个少数类样本X_i，使用K近邻方法求出距离X_i最近的K个样本，其距离计算公式如式(1)所示：

$$dist(X,Y)=\sqrt{\sum_{i}^{n}(x_i-y_i)^2} \tag{1}$$

其中，x_i和y_i为n维空间中的两个样本点，$dist(X,Y)$表示两个样本点的欧氏距离。

该算法会将所有的少数类样本分为3类，其中K近邻样本中若有超过一半的样本属于多数类样本，则将该少数类样本称为边界样本，由于边界样本往往更容易被误分类，因此仅对随机选择的边界样本进行新样本的合成处理，如式(2)所示：

$$X_{new}=X_i+\delta\times(\hat{X}_i-X_i) \tag{2}$$

其中，X_i是待处理的少数类别中的一个样本，$\hat{X}_i$是X_i的K邻近点中的一个少数类样本，$\delta\in[0,1]$是一个随机数。

2.2 注意力机制

注意力机制(Attention Mechanism)最早是在视觉图像领域被提出的，而注意力思想是源于人们在观察图像时往往将注意力集中到目标图像的特定部分以达到更加关注重点信息的目的。2014年，Google DeepMind团队发表了“Recurrent Models of Visual Attention”[13]，将注意力的思想应用于图像分类任务并取得较好的效果，之后越来越多的研究者致力于注意力机制的探索。值得一提的是，Woo等[14]提出了一个高效注意力机制模块，并使用增加了该模块的网络模型在ImageNet数据集上进行测试，实验结果证明，增加该模块后的网络模型可以有效提高分类准确度。由于注意力机制在网络模型上可以发挥重要作用，因此，本文将该注意力机制的思想应用于入侵检测方法，以提升分类准确率。

3 基于Borderline-SMOTE和双Attention的入侵检测方法

3.1 问题分析

从入侵数据分析层面和基于传统机器学习的入侵检测方法层面而言，现有的入侵检测方法存在如下问题：

(1)大多数情况下，由于正常行为活动远远多于异常行为活动，并且越复杂的攻击行为越不容易出现，因此入侵数据均存在数据非平衡问题；

(2)基于传统机器学习的入侵检测方法对于入侵流量数据需要人工手动进行特征提取用于向量化，相对于深度学习而言，特征提取困难；

(3)通过传统机器学习的入侵检测方法提取到的特征表示不准确，从而影响分类器的准确率。

3.2 基于Borderline-SMOTE和双Attention的入侵检测设计

本文提出的BS-DAMN(Borderline-SMOTE-Daul Attention Mechanism Network)入侵检测方法主要由3部分组成，分别为数据预处理、双Attention网络的特征提取和特征更

新，以及流量预测分类。方法的总体架构如图 1 所示。其整体训练过程分为 3 个阶段：1）对数据集进行预处理，得到一个新的训练集和测试集；2）使用新的训练集来训练双 Attention 网络，该网络模型可以实现对输入数据的自动特征提取以及特征更新，使得流量特征的表达更准确；3）使用新的测试集对训练好的网络模型进行测试，进而得到检测结果。

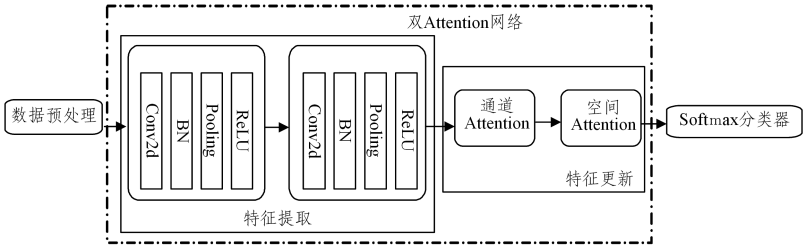

图 1　BS-DAMN 入侵检测方法

Fig. 1　BS-DAMN intrusion detection method

本文实验所使用的数据集为 NSL-KDD 数据集。NSL-KDD 克服了 KDD99 数据集的局限性，使得数据集中的总记录统计合理。NSL-KDD 数据集中包括正常流量 Normal 和四大类攻击流量。四大类攻击类型分别为：拒绝服务攻击(DOS)、普通用户对本地超级用户特权的非法访问(U2R)、来自远程机器的非法访问(R2L)以及端口监视或扫描(Probe)。通过分析可以得出，该数据集的每类数据之间存在数据非平衡问题，这种情况会导致某些攻击类别的检测率偏低。因此，在研究过程中使用 Borderline-SMOTE 过采样技术对类别较少的数据类别进行处理。

3.2.1　基于 Borderline-SMOTE 的数据预处理方法

数据预处理模块包括字符特征数值化、数据归一化、Borderline-SMOTE 数据平衡化以及数据图像化，整体处理流程如图 2 所示。

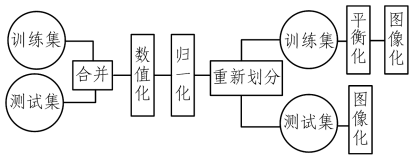

图 2　数据预处理的整体流程

Fig. 2　Overall process of data preprocessing

NLS-KDD 数据集包括 42 维特征，其中前 41 维为特征项，第 42 维为该条流量所属的类别标签。第 2，3，4 维的特征表示为字符型，但深度学习模型的输入只能接收数值型特征表示，因此将 protocol_type，service 和 flag 这 3 维字符型特征进行 one-hot 编码，例如，protocol_type 特征的取值有 3 种，分别为 TCP，UDP 和 ICMP，经过数值化后的取值分别为[0，0，1]，[0，1，0]，[1，0，0]。

由于同一个特征数值间量纲差异较大，为了避免这种差异对分类结果产生影响，对数据进行归一化，本文使用最大-最小归一化处理，其计算式如式(3)所示：

$$x_i' = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{3}$$

其中，x_i'表示经过归一化后的特征值，x_i表示原始特征值，$x_{\min}$表示该特征中最小的特征值，$x_{\max}$表示该特征中最大的特征值。

为了解决 NLS-KDD 数据集中每类样本间的数据非平衡问题，利用 Borderline-SMOTE 方法对样本进行过采样处理。

经上述处理后数据共有 122 维。为了得到有效的图片特征表达，首先，删除名为 num_outbound_cmds 的这列特征，因为在训练集和测试集中该特征的特征值全为零，属于无效特征；然后将 121 维数据转为 11 * 11 的图像。通过观察可以发现同类流量数据间的图片相似度较大(如图 3 所示)，不同类别间的图片相似度较低(如图 4 所示)，因此将一维流量数据转为二维灰度图进行处理再进行分类的思路是可行的。

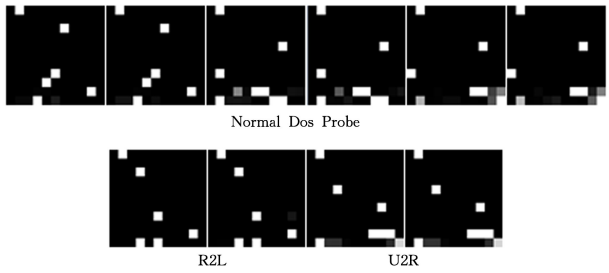

图 3　同类别流量图片相似度对比

Fig. 3　Similarity comparison of traffic pictures in the same category

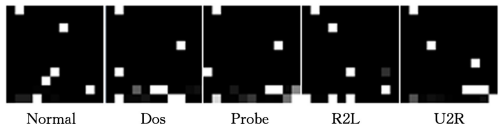

图 4　不同类别流量图片相似度对比

Fig. 4　Similarity comparison of different types of traffic pictures

经上述预处理之后得到的用于仿真实验的训练集和测试集的数据量如表 1 所列。

表 1　重新划分后的数据集分布

Table 1　Data set distribution after re-classification

Type	Normal	Dos	R2L	Porbe	U2R	total
Train	61643	42708	2999	11261	202	649417
Test	15411	10677	750	2816	50	29704

3.2.2　双 Attention 网络模型

双 Attention 网络中特征提取部分的卷积网络有 8 层：第 1 层和第 5 层为卷积层，主要对数据进行卷积操作；第 1 层和第 3 层分别使用 32 个和 64 个滤波器，即使用 32 个和 64 个不同的卷积对其进行操作，卷积核大小均设置为 3 * 3；第 2 层和第 6 层为 BN 层；常用的池化操作是最大池化和平均池化，第 3 层和第 7 层为最大池化层，池化窗口大小均设置为 2 * 2；第 4 层和第 8 层为 ReLU 层。具体的特征提取流程如图 5 所示。

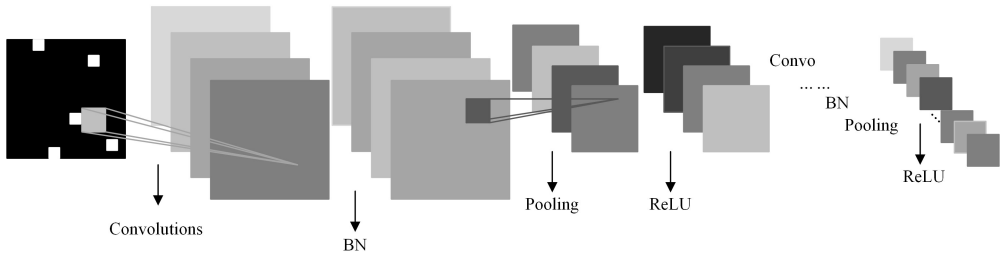

图 5 特征提取流程

Fig. 5 Feature extraction process

对于输入 2 维图像的卷积网络来说，一个维度是图像的尺寸空间，即图像的长和宽，另一个维度是通道。双 Attention 网络中发挥特征更新作用的网络结构包括两部分，分别为通道维注意力和空间维注意力。通道维注意力是根据流量图像在不同通道上的特征对分类结果的影响大小不同，对不同的通道特征表示赋予不同的权重；空间维注意力是对流量图像的尺寸空间进行赋权，在图像的尺寸空间上，并不是所有区域对分类任务的贡献都是相同的，对贡献大的区域赋予更高权重可以增强特征表示，从而提高入侵检测的准确率。假设经过特征提取后得到的流量图像特征表示为 $7*7*64$，通道维注意力就是对 64 个通道分别赋予不同的权重，通过将平均池化操作和最大池化操作相结合的方式在图像尺寸空间维度上对特征进行压缩，如式(4)所示；空间维注意力借助平均池化操作和最大池化操作相结合的方式在通道维度上对特征进行压缩得到 $7*7$ 的特征表示，对 $7*7$ 的不同区域赋予不同的权重，并使用包含一个卷积核的卷积层对其进行卷积操作，如式(5)所示。

$$C(h^k)=\sigma(M\_Conv1(avgpool(h^k))+M\_Conv1(maxpool(h^k))) \tag{4}$$

$$S(h_c^k)\sigma(Conv1_{3*3}[avgpool(h_c^k);maxpool(h_c^k)]) \tag{5}$$

其中，$avgpool$ 和 $maxpool$ 分别表示平均池化操作和最大池化操作，M_Conv1 表示多层一维卷积网络，σ 表示 Sigmoid 激活函数，h_c^k 表示已经过通道注意力机制处理后的低维特征表示，$Conv1_{3*3}$ 代表卷积核大小为 $3*3$ 的卷积层。

最终，对分类结果影响较大的特征可以发挥更大的作用，使得样本的特征表示更加精确，整个处理流程如式(6)所示。

$$X^{TA}=S(C(h^k)\otimes h^k)\otimes h^k \tag{6}$$

其中，$C(h^k)$ 为经过对通道层增加注意力后的中间结果，S 表示进行空间注意力计算，$\otimes$ 运算的目的是在经过双注意力网络后不改变低维特征。特征更新部分的整体处理流程如图 6 所示。

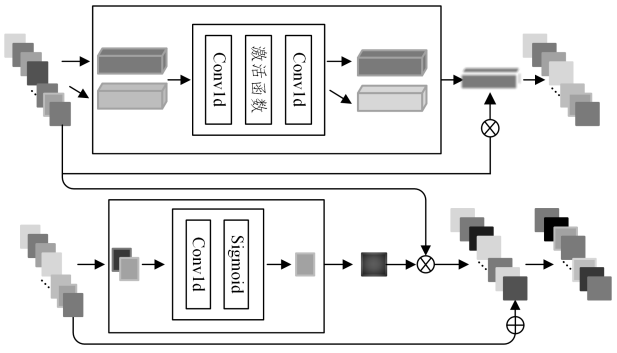

图 6 特征更新流程

Fig. 6 Feature update process

4 实验结果分析

4.1 实验环境

本文全部实验均在硬件环境为 Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.40GHz，20GB RAM，Windows10 操作系统上进行，借助 PyTorch1.5 版本的深度学习框架和 Python3.7 编程语言完成所有的仿真实验代码设计，运用 CUDA10.1 版本的 GPU 运行环境进行仿真实验。

4.2 实验评价指标

评价指标是建立在混淆矩阵上的，混淆矩阵如表 2 所列。

表 2 两类问题的混淆矩阵

Table 2 Confusion matrix for two classes of problems

	实际正类	实际负类
分为正类	*TP*	*FP*
分为负类	*FN*	*TN*

本文入侵检测的相关实验均采用准确率(Accuracy，AC)、漏报率(False Negative Rate，FNR)和精度(Precision，Pre)来评判结果的优劣，计算方式如式(7)—式(9)所示。

$$AC=\frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

$$FNR=\frac{FN}{TP+FN} \tag{8}$$

$$Pre=\frac{TP}{TP+FP} \tag{9}$$

4.3 实验结果分析

本文从 3 个方面进行实验设计。第 1 部分通过对数据进行平衡化处理以及使用双 Attention 网络，证明本文所适配的数据平衡化处理方法和精准特征表示方法提高了分类精确度和准确率；第 2 部分通过对网络结构的选择，训练出最优模型；第 3 部分将本文方法与现有常用的入侵检测方法进行对比，来证明本文方法的可行性。

4.3.1 BS-DAMN 方法分析

第 1 部分的实验是为了证明文中所适配的数据平衡化处理和精准特征表示两种方法的有效性。从表 2 中可以看出，与不经过平衡化处理且仅特征降维的分类结果相比，仅经过平衡化处理的分类结果的准确率提高了 0.64%，其中对于 R2L 攻击类别的检测精确度提高了 5.41%；既经过平衡化处理又进行了特征降维和特征更新的分类结果的准确率提高了 0.73%，其中对于 R2L 攻击类别的检测精确度提高了 5.97%，对于 U2R 攻击类别的检测精确度提高了 1.84%。与仅经过平衡化处理和特征降维的分类结果相比，同时经过具有双注意力机制的特征更新模块的分类结果的准确率提高

了 0.09%，其中正常流量 Normal 和 Dos，R2L，Porbe 以及 U2R4 类攻击流量的检测精度分别提高了 0.04%，0.06%，0.56%，0.35%，1.08%。从以上 3 组实验可以看出，将数据平衡化处理方法和精准特征表示方法相结合可以提高分类精确度和准确率。

表 3 BS-DAMN 方法分析的实验结果

Table 3 Experimental resultsof BS-DAMN method analysis

（单位：%）

Method	*Pre*/%					*AC*/%
	Normal	Dos	R2L	Porbe	U2R	
OriginalData+CNN	99.27	99.38	77.98	97.62	80.49	98.51
BSData+CNN	99.67	99.80	83.39	98.94	81.25	99.15
BSData+CNN+DualAttention	99.71	99.86	83.95	99.29	82.33	99.24

4.3.2 网络结构分析

在深度学习中，模型的网络结构对分类结果影响很大，因此本节通过设置不同大小的低维特征表示和双注意力机制网络中特征更新部分的放置位置，分别从准确率、精确率以及漏报率指标上度量本文入侵检测模型的最佳网络结构设计，实验结果如图 7—图 9 所示。其中，五分类指对正常流量（Normal）和 4 类攻击流量（分别为：Dos、R2L、Probe、U2R）进行的分类。

设置低维特征表示的大小分别为 3 * 3，5 * 5，7 * 7 和 9 * 9，以此进行特征提取实验。从图 7 可以看出，将经过 CNN 后的流量图像特征降维到 7 * 7 时分类准确率最高，模型效果较好。其中 7 * 7 和 9 * 9 大小的特征表示对于前 4 种攻击的分类精确度基本相同，相比之下，5 * 5 大小的特征表示在 R2L 攻击类别上的分类精确度略低，3 * 3 的分类精确度最低。在 U2R 攻击的精确度上，7 * 7 大小的特征表示明显高于其他几种低维特征表示。经过综合分析，选择将经过 CNN 之后的流量空间特征降低到 7 * 7，以使模型达到较好的性能。

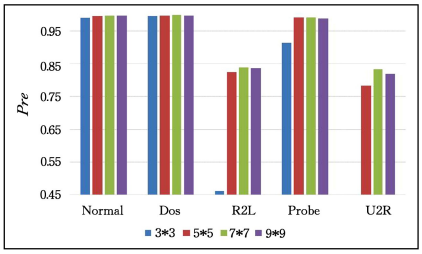

图 7 不同低维特征下五分类的精确度对比

Fig. 7 Precision comparison of five categories with different low-dimensional features

从图 8 中可以看出，虽然将双 Attention 网络中的特征更新部分设置于 CNN 特征提取之后对 Normal 和 Dos 的精确度基本不变，但对于 R2L，Probe 和 U2R 3 种攻击类别来说，特别是对于 U2R 攻击类别，将特征更新部分设置于 CNN 特征提取之后的网络结构的分类结果的精确度更高。从图 9 可以看出，模型对 Normal，Dos 和 Probe 的漏报率基本持平，而将双 Attention 网络的特征更新部分设置于 CNN 特征提取之后，模型对 R2L 和 U2R 两种攻击的漏报率可以达到更低。综上，将具有双注意机制作用的特征更新部分设置于 CNN 特征提取之后，本文模型可以达到更好的性能。

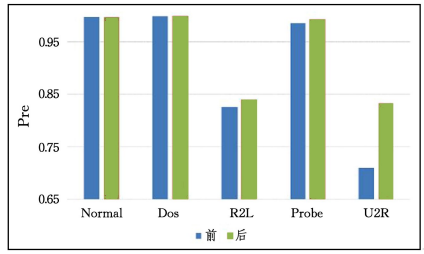

图 8 Attention 设置前后五分类的精确度对比

Fig. 8 Precision comparison of five categories before and after Attention setting

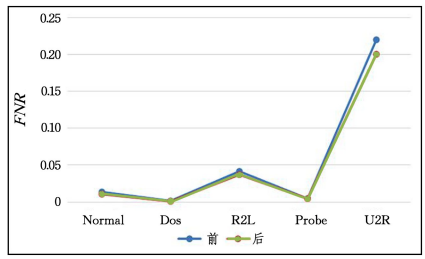

图 9 Attention 设置前后五分类的漏报率对比

Fig. 9 False negative rate comparison of five categories before and after Attention setting

4.3.3 不同算法的对比实验

本节通过对比常用的基于传统机器学习方法的入侵检测方法和基于深度学习的入侵检测方法，从整体准确率和检测精确度层面进行分析。根据不同方法的分类准确率以及在不同攻击类型上的精确度来验证本文方法的有效性，对比结果如表 4、表 5 所列。综合两个评价指标来看，本文方法更加优良。

表 4 所提方法与其他方法的比较

Table 4 Comparison of the proposed method with other methods

Methods	SMOTE+Sequential Classifiers[15]	DCNN[16]	DCNN[17]	SMOTE-ENN+CNN+BiLSTM+Attention[18]	BS+CNN+Dual-Attention (Proposed Method)
AC/%	93.56	94.37	98.00	99.20	99.24

表 5 所提方法与其他方法在精度上的比较

Table 5 Precision comparison of the proposed method with other methods

（单位：%）

Model	Normal	Dos	R2L	Porbe	U2R
传统 RF[19]	88.38	66.08	10.42	60.45	0.50
chi-square+SVM[20]	96.10	98.87	96.37	95.80	76.92
SMOTE+CANN[21]	—	—	92.97	—	55.91
DCNN[16]	75.96	99.91	99.02	77.16	85.71
DCNN[17]	99.47	99.13	83.21	94.35	64.10
GAN-PSO-ELM[22]	97.85	98.11	89.28	97.31	80.53
Proposed Method	99.67	99.81	83.12	98.94	82.61

表 4 列出了 5 种入侵检测方法的准确率比较。第 1 种方法将数据非平衡处理与混合机器学习算法相结合，准确率达到 93.56%，而其他方法都是以卷积神经网络（Convolutional Neural Networks，CNN）为主体网络的入侵检测方法。从表 4 可以看出，两种基于深度卷积神经网络的入侵检测方法（DCNN[15] 和 DCNN[16]）通过加深卷积神经网络的网络层数以及

改变网络超参数的手段来提高准确率，准确率分别达到了94.37%和98%。同时可以看出，文献[17]和本文方法通过加入数据非平衡处理和注意力机制网络模块，分类准确率提高至99%以上，效果优于前3种方法。本文图像化处理了网络流量数据，充分利用卷积神经网络在图像分类上的巨大优势，并分别从通道和空间两个层面进行注意力权重计算，相比之下准确率更高，达到99.24%。上述分析在一定程度上证明了本文方法的独创性和有效性。

本文的入侵检测方法与其他常用的入侵检测方法的分类结果如表5所列。从表5中可以看出，经过非平衡处理和双Attention网络的入侵检测方法提高了分类结果的精确度，特别是在Normal和Probe两种攻击类别的识别上达到了最优的效果，同时对Dos和U2R两种攻击类别的分类精确度也保持在较高的水平。综合比较并分析表5所列的其他入侵检测方法可知，本文方法取得了更优且均衡的分类效果，说明其充分挖掘了网络流量特征，具有较强的入侵特征识别能力。

结束语 本文依据当前入侵检测的研究现状，针对入侵数据存在的非平衡问题，以及特征表示不准确的问题，提出了一种基于Borderline-SMOTE和双Attention的入侵检测方法。该方法利用Borderline-SMOTE方法进行过采样，并利用具有双注意力机制的网络，分别从通道维度和空间维度两个层面对分类结果影响较大的特征赋予更大权重。该方法既解决了数据存在的非平衡问题，又提高了整体网络的特征表示能力。实验结果表明本文提出的入侵检测方法整体分类性能良好，各类攻击的分类准确率度量指标，说明本文方法具有一定的可行性。在今后的工作中我们将致力于小样本攻击类数据的研究，利用生成式对抗网络来提高入侵检测的准确率。

参 考 文 献

[1] KIM J, KIM J, THU H L, et al. Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection[C]// International Conference on Platform Technology and Service. 2016: 1-5.

[2] SHON T, MOON J. A hybrid machine learning approach to network anomaly detection [J]. Information Sciences, 2007, 177(18): 3799-3821.

[3] TAN B, TAN Y, LI Y X, et al. Research on Intrusion Detection System Based on Improved Pso-svm Algorithm [J]. Chemical Engineering Transactions, 2016: 583-588.

[4] ZHAO Y H. Research on intrusion detection Optimization Algorithm based on SVM active learning[J]. Journal of Jingchu University of Technology, 2018, 33(4): 5-9.

[5] REN J D, LIU X Q, WANG Q, et al. An Multi-Level Intrusion Detection Method Based on KNN Outlier Detection and Random Forests[J]. Journal of Computer Research and Development, 2019, 56(3): 566-575.

[6] SCHMIDHUBER J. Deep learning in neural networks: An overview[J]. Neural Networks, 2015, 61: 85-117.

[7] RAFF E, SYLVESTER J, NICHOLAS C, et al. Learning the PE Header, Malware Detection with Minimal Domain Knowledge [J]. Machine Learning, 2017: 121-132.

[8] SHI L Y, ZHU H Q, LIU Y H, et al. Intrusion Detection of Industrial Control System Based on Correlation Information Entropy and CNN-BiLSTM[J]. Journal of Computer Research and Development, 2019, 56(11): 2330-2338.

[9] WANG M, LI J. Network Intrusion Detection Model Based on Convolutional Neural Network[J]. Journal of Information Security Research, 2017, 3(11): 990-994.

[10] PHETLASY S, OHZAHATA S, WU C, et al. Applying SMOTE for a Sequential Classifiers Combination Method to Improve the Performance of Intrusion Detection System[C]// Dependable Autonomic and Secure Computing. 2019: 255-258.

[11] DING H W, WAN L, LONG T Y. Research on the application of deep auto-encoder network in intrusion detection[J]. Journal of Harbin Institute of Technology, 2019, 51(5): 185-194.

[12] HUI H, WANG W Y, MAO B H. Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning[C]// International Conference on Intelligent Computing. Berlin, Heidelberg: Springer, 2005.

[13] MNIH V, HEESS N, GRAVES A, et al. Recurrent Models of Visual Attention[J]. arXiv: 1406.6247v1, 2014.

[14] WOO S, PARK J, LEE J, et al. CBAM: Convolutional Block Attention Module[C]// European Conference on Computer Vision. 2018: 3-19.

[15] PHETLASY S, OHZAHATA S, WU C, et al. Applying SMOTE for a Sequential Classifiers Combination Method to Improve the Performance of Intrusion Detection System[C]// Dependable Autonomic and Secure Computing. 2019: 255-258.

[16] LI Y, ZHANG B. An Intrusion DetectionAlgorithm Based on Deep CNN [J]. Computer Applications and Software, 2020, 37(4): 324-328.

[17] DING H W, WAN L, ZHOU K, et al. Study on Intrusion Detection Based on Deep Convolution Neural Network[J]. Computer Science, 2019, 46(10): 173-179.

[18] LIAN H F, ZHANG H, GUO W Z. Netflow Anomaly Detection Based on Data Enhancement and Hybrid Neural Network [J]. Journal of Chinese Mini-Micro Computer Systems, 2020, 41(4): 786-793.

[19] YANG Y, ZHENG K, WU C, et al. Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks[J]. Applied Sciences, 2019, 9(2): 238.

[20] THASEEN I S, KUMAR C A. Intrusion detection model using fusion of chi-square feature selection and multi class SVM[J]. Journal of King Saud University-Computer and Information Sciences, 2017, 29(4): 462-472.

[21] PARSAEI M R, ROSTAMI S M, JAVIDAN R, et al. A Hybrid Data Mining Approach for Intrusion Detection on Imbalanced NSL-KDD Dataset[J]. International Journal of Advanced Computer Science and Applications, 2016, 7(6): 20-25.

[22] YANG Y R, SONG R J, ZHOU Z Y. Network Intrusion Detection Method Based on GAN-PSO-ELM[J]. Computer Engineering and Applications, 2020, 56(12): 66-72.

LIU Quan-ming, born in 1973, senior engineer, associate professor. His main research interests include network industry analysis and cloud security.