基于特征增强的深度学习入侵检测算法

唐群玲,张兴兰
(北京工业大学 信息学部,北京 100124)

摘 要:深度学习技术随着社会的不断发展,逐渐应用到了社会生活的各个领域,其中与入侵检测技术相结合已成为当今的研究热点。在当前不稳定的网络环境下,能够准确识别异常流量是当前入侵检测的主要任务。传统的神经网络面对复杂的数据,无法准确提取到与分类结果有关的特征,过多的冗余特征会导致模型泛化能力差,检测准确率不高,这会导致深度学习技术无法很好地应用在入侵检测的任务中。为了解决这个问题,提出了一种基于特征增强的深度学习入侵检测方法,即在模型训练过程中,通过一个辅助网络,增强对分类结果相关的特征,使模型着重学习对分类有益的特征,同时减轻冗余特征对模型分类的影响。同时,该方法不会修改原有模型的结构,可以轻松地应用在不同的卷积神经网络的模型上。最后在 NSL-KDD 和 CICIDS2017 数据集上的实验结果表明,准确率最高可达 99.73% 和 99.15%。

关键词:特征增强;入侵检测;特征提取;准确率;分类
中图分类号:TP181 **文献标识码**:A **文章编号**:1673-629X(2023)06-0133-06
doi:10.3969/j.issn.1673-629X.2023.06.020

Deep Learning Intrusion Detection Algorithm Based on Feature Enhancement

TANG Qun-ling, ZHANG Xing-lan
(Department of Information Science, Beijing University of Technology, Beijing 100124, China)

Abstract: Deep learning technology has been gradually applied to various fields of social life with the continuous development of society, among which combining with intrusion detection technology has become a hot research topic today. In the current unstable network environment, accurate identification of abnormal traffic is the main task of current intrusion detection. Traditional neural networks cannot accurately extract features related to classification results in the face of complex data, and too many redundant features will lead to poor generalization of the model and low detection accuracy, which will lead to the inability of deep learning techniques to be well applied in the task of intrusion detection. To solve this problem, we propose a deep learning intrusion detection method based on feature enhancement. During the model training process, the features that are relevant to the classification results are enhanced by an auxiliary network, so that the model focuses on learning features that are beneficial to the classification, while mitigating the impact of redundant features on the model classification. At the same time, the proposed method does not modify the structure of the original model and can be easily applied to different models of convolutional neural networks. Finally, experiments on the NSL-KDD and CICIDS2017 datasets show that the accuracy is up to 99.73% and 99.15%.

Key words: feature enhancement; intrusion detection; feature extraction; accuracy; classification

0 引 言

互联网飞速发展的同时也带来了很多安全问题,任何企图危害计算机或网络资源的行为都被定义为入侵。该文主要从入侵检测方面来解决网络安全问题。

传统的入侵检测技术已经暴露出以下弊端:第一,当前入侵的数据量大,传统的入侵检测技术难以处理,比如分布式拒绝攻击,在一分钟内就能产生几十万条攻击数据,对系统的性能要求很高。第二,随着技术的发展,攻击的形式也在不停变化,由于入侵检测属于防御手段,这使得入侵检测面临新型攻击时显得束手无策。第三,在入侵检测数据中存在不平衡现象,例如入侵数据中 Dos 攻击的数量远大于正常流量的数据。

类别不平衡,指的是当信息集中一个类别数据数量大大地超过了另一类别样本数,在实际的分析应用

收稿日期:2022-08-15 **修回日期**:2022-12-15
基金项目:北京市自然科学基金(4212015)
作者简介:唐群玲(1998-),女,硕士研究生,通信作者,研究方向为机器学习;张兴兰(1970-),女,教授,博士,研究方向为密码学、信息安全等。

中,如垃圾邮件分析、电话欺诈分析等过程中都出现了数据不平衡现象。入侵检测中的样本是类别不平衡数据,数据不平衡很容易导致针对少数攻击的高误报检测率。类别不平衡往往导致性能降低,甚至分类失败。对于一般的分类器的训练而言,在非平衡的数据集下很容易训练出一个正确率很高,而召回率很低的分类器。不平衡数据面临的最大问题是过拟合,会因为样本数太少,偏向训练样本,从而造成召回率很低的结果。解决类别不平衡造成的召回率低的问题是一个很有意义的研究课题。

特征对于模型分类的影响可以与梯度信息建立起密切的联系。在卷积神经网络中,不同的卷积层可以学习到不同的特征,将这些特征组合到一起时,就会描述一个特定的对象,这就意味着特征提取的质量,对最后的分类结果有着重要的影响。因此,该文提出了一种基于特征增强的深度学习入侵检测方法,通过一个辅助网络来自适应地学习不同特征对类别预测的重要性,并利用学习到的特征重要性来动态调整分类模型对不同特征的关注度,使模型更加关注对分类结果有积极作用的特征,同时抑制模型对冗余特征的学习,通过这种方式提升模型的准确率。最后在 NSL-KDD 和 CICIDS2017 数据集上进行了实验,并与多个模型进行对比,实验结果表明,该方法在 2 个数据集上都取得了不错的效果。

1 相关工作

1.1 数据增强的发展与研究现状

近年来,异常检测任务中大多数缺乏标记数据,并且数据类别不平衡。为了解决数据不平衡导致性能降低,甚至分类失败的问题,在早期对数据增强产生新样本的方法是围绕原样本进行操作,如移位[1]、旋转[2]、缩放[3-4]、裁剪[3-5]、翻转[5-6]等来扩大数据集。Nitesh V. Chawla 提出了 SMOTE,对小类进行插值产生额外的小类数据[7],以及 ADSYN,根据学习难度的不同,对不同的少数类别的样本使用加权分布。SMOTE 和 ADSYN 都是使用过采样技术进行数据增强。EasyEnsemble 方法使用集成的机制,把大类分割成若干个小集合给不同的学习器使用,对各个学习器都进行了欠采样,且通过全局分析不遗漏重要数据[8]。虽然现在已经开发了几种过采样或数据增强方案来平衡不同类别的数据,但是通常只是合成观察或者复制得到的数据,并不能提高数据的多样性。张志武等人[9]提出 LSTM 深度学习框架下自适应不平衡数据方法。对多数类进行多组欠采样,并分别与少数类样本组合成多组平衡的训练数据集,然后分别对每组训练数据学习一个 LSTM 模型,最后通过集成学习方法获得最终结果,能提高类别不平衡数据的深度学习性能。这些方法都是从数据集入手,解决类别不平衡问题,采用数据增强的方法,使得数据较为均衡,进而提高分类准确率。

1.2 入侵检测

在文献[10]中首次将机器学习引入入侵检测中,目的是对于网络异常进行检测和判断,且进一步识别该攻击行为。文献[11]中提出了 k 最近邻和支持向量机算法,这是常用的数据挖掘算法。文献[12]在入侵检测算法中引入了支持向量机,但是随着数据量的增加,传统的机器学习算法更适合解决小样本问题,对于复杂的入侵检测系统不能更好地进行特征提取,导致误检率升高等问题出现。

入侵检测技术主要是通过特征的提取和特征的分类来达到检测和判断的目的。从大量数据中提取特征从而进行分类,这是非常关键的步骤。文献[13]提出了基于一维卷积神经网络的入侵检测方法,可自动提取原始数据的特征。文献[14]提出了 RNN 进行入侵检测的可能性,它是通过将数据流量建模为状态序列来完成入侵检测行为。文献[15]提出将长短期神经网络(LSTM)应用于入侵检测,长短期神经网络是一种特殊的循环神经网络,也是经典的深度学习方法之一,能够有效地解决数据训练时出现的梯度消失和梯度爆炸问题。文献[16-18]将卷积神经网络(CNN)也应用于入侵检测。文献基于 RNN-SVM 的入侵检测方法研究,该入侵检测系统以 HDFS 作为文件存储平台,以 Spark 作为数据预处理平台,Tensorflow 作为模型训练测试平台,能处理海量数据,利用 RNN 对特征进行提取,同时利用 SVM 分类器,对低维特征具有良好的分类能力,对降维后的特征进行分类,降低漏报率和误报率。

2 方 法

基于特征增强的入侵检测模型的结构如图 1 所示。与传统的卷积神经网络不同,在卷积最后一层添加了一个辅助网络,先对卷积神经网络提取的特征进行增强,再送入全连接层进行分类。

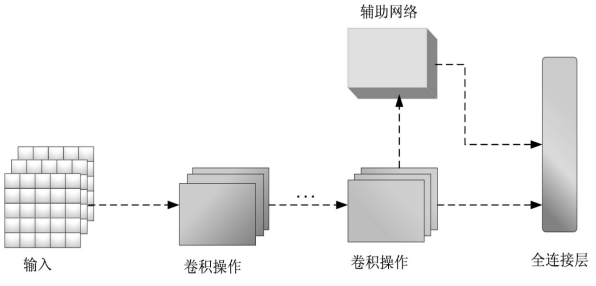

图 1 模型架构

整体任务流程为:设输入的样本数据为 $X=[x_1,x_2,\cdots,x_n]$,其中 $X\in\mathbb{R}^{n\times1}$,$n$ 为输入样本的特征数目,模型的目标是正确对输入流量进行预测。

2.1　特征增强

特征增强本质上是让模型更加关注对分类结果有积极作用的特征。该文设计了两种增强特征方法,首先受到显著图的启发,根据样本的标签类别来计算与其相关的重要通道。计算方法如式(1)所示:

$$g_c^l=\frac{\partial F_c^l(z^l)}{\partial z^l} \tag{1}$$

其中,$F_c^l(z^l)$ 是进入 SoftMax 层之前的 logits 得分;$z^l\in\mathbb{R}^{n\times w\times h}$ 是模型第 l 层的特征图,n、w 和 h 分别代表特征图的通道数、宽度以及高度;$g_c^l\in\mathbb{R}^{n\times w\times h}$ 是特征图 z^l 关于类 c 的重要性得分。需要注意的是,在训练阶段,样本的类别可直接给出;在测试阶段,由模型预测的最高置信度的类别来确定。在训练过程中,为了避免对整个网络进行求导,造成资源的浪费,设计一个辅助网络 $A^l(\cdot)$ 来代替模型的第 l 层 $F^l(\cdot)$,它是由一个全连接层构成,在训练过程中只需对辅助网络进行一层反向求导便可获得相对重要的特征信息。同时,为了让梯度为正的特征得到增强,使用 ReLU 函数进行转化,如式(2)(3)所示。因此,上述公式更改为:

$$\mathrm{ReLU}(x)=\frac{x+\sqrt{x^2+b}}{2},\quad b>0 \tag{2}$$

$$g_c^l=\mathrm{ReLU}\left(\frac{\partial A_c^l(z^l)}{\partial z^l}\right) \tag{3}$$

在得到 g^l 后,对原始特征图 z^l 进行增强,计算方法如式(4)所示:

$$z_1^l=z^l\otimes g_c^l \tag{4}$$

此外,另一种增强的方式是通过辅助网络 $A^l(\cdot)$ 的参数来对其进行增强。对于 C 个类别,辅助网络 $A^l(\cdot)$ 的参数可以写成 $M^l=[M_1^l,M_2^l,\cdots,M_C^l]$,它可以识别每个通道对特定类别的重要性。因此可以使用参数 M 作为特征增强矩阵,以提升重要特征在分类过程中的比重,降低非重要特征产生的影响,在训练和测试过程中,类别的设定与上述一致,即在训练阶段直接给出类别的标签,已进行常规的有监督训练,而在测试阶段,类别由辅助网络的预测结果给出。特征增强的公式如式(5)所示:

$$z_2^l=z^l\otimes m_c^l \tag{5}$$

其中,m_c^l 为辅助网络 $A^l(\cdot)$ 的参数,结合上述两种特征增强的方式,提出的最终增强方法公式如下:

$$\widetilde{z^l}=z^l\otimes(\alpha\cdot m_c^l+g_c^l) \tag{6}$$

其中,$\alpha\in(0,1)$ 是超参数。

2.2　训练方法

在实际操作中,特征增强模块应用于模型的倒数第二层,即全连接层之前的卷积模块。该文提出的是设计一个辅助网络辅助特征增强的方法,因此它有自己的损失函数,需要与原始网络的损失函数一起进行训练。通道增强模块的损失函数如式(7)所示:

$$L(x,y)=L_{\mathrm{CE}}(p,y)+\gamma L_{\mathrm{CE}}(a,y) \tag{7}$$

其中,$L_{\mathrm{CE}}(\cdot)$ 为交叉熵损失函数;p 和 a 分别是原始网络和辅助网络的预测结果;$\gamma\in(0,1)$ 是一个超参数,用来平衡原始网络和辅助网络的预测结果。

3　实验与结果分析

3.1　实验环境与参数设置

该文主要将深度学习模型应用到入侵检测的实验中,并对比了每个模型的结果。实验是在 Linux 系统下进行的;显卡使用的是 GTX 2080Ti;深度学习模型是使用 Pytorch 框架搭建的。

3.2　数据集及预处理

(1)NSL-KDD 数据集。

NSL-KDD 数据集是 KDD 99 数据集的改进,NSL-KDD 数据集的训练集中不包含冗余记录,所以分类器不会偏向更频繁的记录。NSL-KDD 数据集的测试集中没有重复的记录,使得检测率更为准确。训练和测试中的记录数量设置是合理的,这使得在整套实验上运行实验成本低廉而无需随机选择一小部分。因此,不同研究工作的评估结果将是一致的和可比较的。NSL-KDD 数据集解决了 KDD99 数据集中存在的固有问题。NSL-KDD 数据集由于缺少基于入侵检测网络的公共数据集,所以 NSL-KDD 数据集仍然存在一些问题,同时也不是现有真实网络的完美代表。但它仍然可以用作有效的基准数据集,以帮助研究人员比较不同的入侵检测方法。表 1 展示了 NSL-KDD 数据集中的攻击类型。

表 1　NSL-KDD 数据集详细攻击

攻击类型	训练集中攻击	在测试集出现的额外的攻击
Dos	Back,neptune,smurf,teardrop,land,pod	Apache2,mailbomb,processtable
Probe	Satan,portsweep,ipsweep,nmap	Mscan,saint
R2L	Warezmaster,warezclient,ftpwrite,guesspassword,imap,multihop,phf,spy	Sendmail,named,snmpgetattack,snmpguess,xlock,xsnoop,worm
U2R	Rootkit,bufferoverflow,loadmodule,perl	Httptunnel,ps,sqlattack,xterm

(2)CICIDS2017 数据集。

CICIDS2017 数据集包含了大量最新的攻击场景,这个数据集不仅包含了最新的网络攻击,也满足了现

实世界攻击的所有标准。这个数据集其中一个明显的缺点是数据量非常庞大,跨越了八个文件。此外数据集包含冗余记录以及一些缺省值,且数据集本质上是高度不平衡的。

对于分散存在的问题可以通过合并各种数据文件得以解决且删除缺失的值,在实际检测过程开始之前对数据集进行采样,可以克服高容量的缺点。在抽样之前,必须先解决类别不平衡问题,如果是平衡数据集,所有类标签实例的发生概率将增加。解决类别不平衡问题的主要方法之一是重新给类贴标签,包括将多数类分裂形成更多的类,或将少数类合并成一个类,以此减少类别不平衡问题。表 2 展示了 CICIDS2017 数据集标签合并后的结果。

表 2 CICIDS2017 数据集新攻击标签的特征

新标签	旧标签	样本数
Normal	Benign	2 359 087
Botnet ARES	Bot	1 966
Brute Force	FTP-Patator, SSH-Patator	13 835
Dos/DDos	DDoS, DoS GoldenEye, DoS Hulk, DoS Slow-httptest, DoS slowloris, Heartbleed	294 506
Infiltration	Infiltration	36
PortScan	PortScan	158 930
Web Attack	Web Attack - Brute Force, Web Attack - Sql Injection, Web Attack - XSS	2 180

3.2.1 在 NSL-KDD 数据集上的实验

对于 NSL-KDD 数据集的处理主要包括数值化、特征扩充以及归一化三个步骤:

(1)数值化。

在 NSL-KDD 数据集中,含有三种字符类型的特征,然而神经网络并不能很好地处理字符类型的特征,因此在将数据送入神经网络进行学习之前,需要对字符类型的特征进行处理。在数据集中,三种字符类型的特征分别是协议类型、目标主机服务类型以及连接状态。该文将字符类型的特征处理成 one-hot 的形式,例如协议类型的值有 3 种,处理成 one-hot 的形式后,3 种值分别被处理成[0,0,1][0,1,0][1,0,0]。其他特征的处理方式类似,最终,数据集中的每条样本的特征长度为 121 维。

(2)特征扩充。

该文提出的方法主要依托卷积神经网络来提取样本特征,因此在特征提取过程中,需要将样本转化成图片数据的格式。在数值化以后,样本的长度被处理成为 121 维,再通过维度转化,将 121 维的向量转化成 11×11 的矩阵。针对某些卷积神经网络的结构不能很好地处理小维度的样本的问题,将 11×11 维的矩阵扩充成 32×32 的矩阵,扩充的特征用 0 进行填充。值得注意的是,针对 LSTM 等网络,则不需要再进行维度转化和特征扩充的操作。

(3)归一化。

在样本特征中,由于衡量特征的量纲不同,会导致特征之间有很大的数值差异,会影响模型的判断。在对样本进行数值化以后,再进行归一化处理,消除量纲不同带来的数据差异。采用最大-最小归一化的方法,将所有特征的值统一到[0,1]之间,如公式(8)所示:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{8}$$

其中,x 是原始数据,x_{min} 是所有样本中同一特征中的最小值,x_{max} 是所有样本中同一特征中的最大值,x_{norm} 是原始数据归一化后的结果。

将处理后的数据集可视化后可以发现,不同类别的数据样本之间有着明显的不同特征,将标签为 Normal 和 DoS 的部分样本进行了可视化,结果如图 2 所示。

(a)Normal

(b)DoS

图 2 NSL-KDD 数据集中部分样本可视化

3.2.2 在 CICIDS2017 数据集上的实验

在原始 CICIDS2017 数据集中存在特征缺失的现象,因此在处理数据前,先将特征缺失的样本进行删除。并且为了解决类别不平衡的问题,根据文献[19],将特征相似的类别进行合并,生成新的标签。最后将处理后的数据集进行数值化、特征扩展以及归一化的操作,操作过程与 NSL-KDD 一致。同时,将标签为 Normal 和 Attack 的部分样本进行了可视化,结果如图 3 所示。

(a)Normal

(b)Attack

图 3 CICIDS2017 数据集中部分样本可视化

3.3 评价指标

该文使用准确率 AC、精确率 P 、召回率 R 以及 F1

-Score 作为实验结果的评价指标,其公式定义如下:

$$AC = \frac{TN + TP}{TN + TP + FN + FP} \tag{9}$$

$$P = \frac{TP}{TP + FP} \tag{10}$$

$$R = \frac{TP}{TP + FN} \tag{11}$$

$$F1 - Score = \frac{2 \times P \times R}{P + R} \tag{12}$$

其中,TN(True Negative)是预测结果为 Negative,且预测正确的数量;TP(True Positive)是预测结果为 Positive,且预测正确的数量;FN(False Negative)是预测结果为 Negative,且预测错误的数量;FP(False Positive)是预测结果为 Positive,且预测错误的数量。

3.4　结果与分析

3.4.1　在 NSL-KDD 数据集上的实验

在划分测试集上的实验:

在实验过程中,使用了 5 折交叉验证,即将原始训练集平均划分为 5 等份,其中 4 份用来训练模型,1 份用来测试模型,并且训练集与测试集中的样本没有重叠,最终的实验结果去平均值。使用了 ResNet-50、VGG-19 以及 LSTM 进行对照,实验结果如表 3 所示。

表 3　在 NSL-KDD 划分数据集上的结果　%

模型	AC	*P*	*R*	F1
ResNet-50	99.59	99.60	99.57	99.58
VGG-19	99.43	99.38	99.42	99.40
LSTM	99.37	99.21	99.32	99.26
文中	99.73	99.72	99.74	99.73

从实验结果可以看出,在准确率上,ResNet-50 比 LSTM 高 0.22 百分点,VGG-19 要比 LSTM 高 0.06 百分点,这说明卷积神经网络提取特征的能力要优于 LSTM,而该文提出的方法在准确率上要比 ResNet-50 和 VGG-19 分别高 0.14 百分点和 0.3 百分点。显然该文提出的方法要优于传统的神经网络分类模型。

在原始测试集上的实验:

该文也使用了原始的测试集 KDDTest+进行了实验,原始测试集中存在训练集中不存在的样本,并且类别不平衡的影响更加明显,可以检验模型的泛化能力。在实验过程中,依旧使用 ResNet-50、VGG-19 以及 LSTM 进行对照,实验结果如表 4 所示。

表 4　在 NSL-KDD 原始测试集上的结果　%

模型	AC	*P*	*R*	F1
ResNet-50	82.66	84.69	84.61	83.12
VGG-19	81.33	83.33	82.98	82.10
LSTM	79.67	81.55	81.53	79.98
文中	84.85	84.97	84.74	84.85

从结果中可以看出,该文提出的方法与其他方法相比,在每个指标上都取得了最高的分数。其中与 ResNet-50 相比,准确率提升了 2.19 百分点;与 LSTM 相比,准确率提升了 5.18 百分点。这说明传统的卷积神经网络并不能很好地提取相关特征,尤其是在类别不平衡的数据集上。而该文提出的方法可以着重使模型关注与分类密切相关的特征,而削弱噪声特征对分类结果的影响。在类别不平衡的数据集下,模型可以在只有获得少量样本的情况下,提取到更加重要的特征,提升模型在不平衡数据集下的准确率,也进一步提升了模型的泛化能力。

3.4.2　在 CICIDS2017 数据集上的实验

在划分测试集上的实验:

由于 CICIDS2017 数据集并没有提供专门用于模型评估的测试集,因此在实验过程中,需要手动划分训练集和测试集。数据集的划分步骤与 NSL-KDD 一致,同样使用了 5 折交叉验证的方法。对比模型使用了 ResNet-50、VGG-19 以及 LSTM,实验结果如表 5 所示。

表 5　在 CICIDS2017 数据集上的结果　%

模型	AC	*P*	*R*	F1
ResNet-50	98.76	97.92	99.03	98.45
VGG-19	99.03	98.32	99.31	98.80
LSTM	98.33	97.35	98.56	97.93
文中	99.15	98.56	99.35	98.94

处理后的数据集在一定程度上解决了类别不平衡的问题,因此每个模型在测试集上都获得了良好的表现,但该文提出的方法在不同指标上的表现更加突出。提出的方法在准确率上,比 ResNet-50 提高了 0.39 百分点,比 LSTM 的方法提高了 0.82 百分点。结果表明,提出的方法使得模型在不同数据集上都有了不错的性能提升。

3.4.3　模型效率分析

该文提出的方法可以看作是一个附加的辅助网络,为了研究该方法的效率,展示了 ResNet-18 模型在 3×32×32 大小的样本下的训练时间和推断时间,如表 6 所示。在训练过程中,原始的 ResNet-18 模型训练每个 Batch 平均需要 95 s,修改的模型需要 103 s,其中每个 Batch 包含 128 个样本。在测试过程中,原始的 ResNet-18 模型在测试阶段需要 0.007 s;而修改的模型则需要 0.011 s。从实验结果中可以看出,提出的方法并没有导致太多的额外计算时间消耗。

表 6　时间损耗的结果　s

ResNet-18	训练阶段	推断阶段
原始模型	95	0.007
文中模型	103	0.011

4 结束语

构建了一个特征增强的方法,使用梯度得分来获取对模型分类有益的特征,同时为了避免在反向求导获得梯度信息的过程中造成资源的浪费,通过使用一个辅助网络,在训练过程中与原始分类网络一起训练。通过这种方法,使模型在训练过程中,重点关注对分类结果有促进作用的特征,同时减少不重要特征的影响,使模型的准确率有了明显的提升。今后需要进一步提升模型提取特征的能力,增强模型在类别不平衡数据集上的表现,并提升模型的运行效率。

参考文献:

[1] BENAIM S,WOLF L. One-shot unsupervised cross domain translation[C]//Advances in neural information processing systems. Montreal:NIPS,2018:2104-2114.

[2] SANTORO A,BARTUNOV S,BOTVINICK M,et al. Meta-learning with memory-augmented neural networks[C]//International conference on machine learning. New York: PMLR,2016:1842-1850.

[3] ZHANG Y,TANG H,JIA K. Fine-grained visual categorization using meta-learning optimization with sample selection of auxiliary data[C]//Proceedings of international European conference on computer vision. Munich:Springer,2018:233-248.

[4] LAKE B M,SALAKHUTDINOV R,TENENBAUM J B. Human-level concept learning through probabilistic program induction[J]. Science,2015,350:1332-1338.

[5] QI H,BROWN M,LOWE D G. Low-shot learning with imprinted weights[C]//Proceedings of IEEE conference on computer vision & pattern recognition. Salt Lake City:IEEE,2018:5822-5830.

[6] SHYAM P,GUPTA S,DUKKIPATI A. Attentive recurrent comparators[C]//International conference on machine learning. Sydney:PMLR,2017:3173-3181.

[7] CHAWLA N V,BOWYER K W. Smote:synthetic minority over-sampling technique[J]. Journal of Artificial Intelligence Research,2002,16(1):321-357.

[8] LIU X Y,WU J,ZHOU Z H. Exploratory undersampling for class-imbalance learning[J]. IEEE Transactions on Systems,Man,and Cybernetics,Part B (Cybernetics),2008,39(2):539-550.

[9] 张志武,薛 娟,陈国兰. 深度学习框架下类别不平衡数据情感分析[J]. 现代情报,2021,41(10):75-82.

[10] SOMMER R,PAXSON V. Outside the closed world:on using machine learning for network intrusion detection[C]//2010 IEEE symposium on security and privacy. Oakland:IEEE,2010:305-316.

[11] TSAI C F,HSU Y F,LIN C Y,et al. Intrusion detection by machine learning:a review[J]. Expert Systems with Applications,2009,36(10):11994-12000.

[12] LEE H,SONG J Y,PARK D. Intrusion detection system based on multi-class SVM[C]//Rough sets,fuzzy sets,data mining and granular computing. Berlin:Springer,2005:511-519.

[13] WANG W,ZHU M,WANG J,et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//2017 IEEE international conference on intelligence and security informatics (ISI). Beijing:IEEE,2017:43-48.

[14] YIN C L,ZHU Y F,FEI J L,et al. A deep learning approach for intrusion detection using recurrent neural networks[J]. IEEE Access,2017,5:21954-21961.

[15] STAUDEMEYER R C. Applying long short-term memory recurrent neural networks to intrusion detection[J]. South African Computer Journal,2015,56(1):136-154.

[16] LIN W H,LIN H C,WANG P,et al. Using convolutional neural networks to network intrusion detection for cyber threats[C]//2018 IEEE international conference on applied system invention (ICASI). Chiba:IEEE,2018:1107-1110.

[17] KIM J,KIM H,KIM H,et al. CNN-based network intrusion detection against denial-of-service attacks[J]. Electronics,2020,9(6):916-920.

[18] DENG C,QIAO H. Network security intrusion detection system based on incremental improved convolutional neural network model[C]//2016 international conference on communication and electronics systems (ICCES). Coimbatore:IEEE,2016:1-5.

[19] PANIGRAHI R,BORAH S. A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems[J]. International Journal of Engineering & Technology,2018,7(3):479-482.