基于密集连接卷积神经网络的入侵检测技术研究

缪祥华 单小撤*

(昆明理工大学信息工程与自动化学院 昆明 650500)

摘 要：卷积神经网络在入侵检测技术领域中已得到广泛应用，一般地认为层次越深的网络结构其在特征提取、检测准确率等方面就越精确。但也伴随着梯度弥散、泛化能力不足且参数量大准确率不高等问题。针对上述问题，该文提出将密集连接卷积神经网络(DCCNet)应用到入侵检测技术中，并通过使用混合损失函数达到提升检测准确率的目的。用KDD 99数据集进行实验，将实验结果与常用的LeNet神经网络、VggNet神经网络结构相比。分析显示在检测的准确率上有一定的提高，而且缓解了在训练过程中梯度弥散问题。

关键词：入侵检测；卷积神经网络；密集连接；梯度弥散

中图分类号：TN918.91 **文献标识码**：A **文章编号**：1009-5896(2020)11-2706-07

DOI: 10.11999/JEIT190655

Research on Intrusion Detection Technology Based on Densely Connected Convolutional Neural Networks

MIAO Xianghua SHAN Xiaoche

(*School of Information Engineering and Automation, Kunming University of Science and Technology, Kunming* 650500, *China*)

Abstract: Convolutional Neural Network (CNN) is widely used in the field of intrusion detection technology. It is generally believed that the deeper the network structure, the more accurate in feature extraction and detection accuracy. However, it is accompanied with the problems of gradient dispersion, insufficient generalization ability and low accuracy of parameters. In view of the above problems, the Densely Connected Convolutional Network (DCCNet) is applied into the intrusion detection technology, and achieve the purpose of improving the detection accuracy by using the hybrid loss function. Experiments are performed with the KDD 99 data set, and the experimental results are compared with the commonly used LeNet neural network and VggNet neural network structure. Finally, the analysis shows that the accuracy of detection is improved, and the problem of gradient vanishing during training is alleviated.

Key words: Intrusion detection; Convolutional Neural Network (CNN); Dense connection; Gradient vanishing

1 引言

随着卷积神经网络结构[1]的不断优化和提出，使在处理问题的效率方面的得以升华。在入侵检测领域中，LeNet神经网络模型几乎是研究者们所热衷的，例如Liu[2]提出基于LeNet-5卷积神经网络的网络入侵检测方法来提升检测准确率；此外GoogleNet, VggNet模型也有被参照，刘月峰等人[3]提出的多尺度卷积神CNN模型用于网络入侵检测；赵昱博[4]在基于卷积神经网络的入侵检测技术研究中提出改进的Vgg入侵检测模型。

从各神经网络结构的引用可以看出，虽然深层次的卷积神经网络能使网络的样本识别能力和性能上均有提升，但是却存在梯度弥散或消失、检测的准确率不一定高、泛化能力差等缺陷。此外传统的softmax损失函数不足以在分类任务上实现最大化类间差异，从而导致特征识别效率不佳。

本文根据上述所存在的问题，提出如下解决方案。一是将密集连接卷积神经网络(Densely Connected Convolution Network, DCCNet)[5]应用到入侵检测中，来提取网络数据的全局特征，有效利用每条数据之间的特征信息并有效地解决梯度急速扩散和泛化能力弱的难题。二是对于softmax损失函数的缺点提出了混合损失函数，可以有效地缩小类内差异和增加类间距离，较好地解决了类内特征差异性较大及类间相互重叠所导致的检测效果差问题。

收稿日期：2019-08-29；改回日期：2020-05-09；网络出版：2020-05-28
*通信作者： 单小撤 2258868766@qq.com

2　密集连接入侵检测模型框架

根据提出的解决方案，本文设计一种基于密集连接卷积神经网络的入侵检测模型，如图1所示。

原始数据集经预处理后变成密集连接神经网络所能够识别的输入数据，密集连接神经网络根据输入数据训练调整参数，找到最优性能的模型。通过改进的中心损失函数与softmax 损失函数构成的混合损失函数来提升特征类型的检测准确率。

2.1　DCCNet网络结构

一个完整的DCCNet网络结构应该包括：密集连接块(dense block)、过渡层(transition layer)、增长率(growth rate)及变换函数(composite function)等各方面。如图2所示是一个完整的DCCNet网络结构模型。其中，包括3个密集连接块，每个密集连接块之间由过渡层连接。

密集连接块：如图3所示，是一个5层的密集连接块，每一层数据经过非线性变换函数H_l(composite function)传递给下一层。H_l实际上是一个复合的函数集，它包括BN(Batch-Normalization)、激活函数、卷积3种操作(BN→RELU→Conv(3×3))。第L层的输出为

$$\boldsymbol{X}_l = \boldsymbol{H}_l[x_0, x_1, \cdots, x_{l-1}] \tag{1}$$

其中，$\boldsymbol{X}_{l-1}$表示模块的第l–1层特征的连接。若每层经过H_l处理后会生成k个特征图，那么第l层的输入特征有$k(l-1)+k_0$个，其中，k被称为增长率用来控制网络宽度的增长，k_0表示输入层的通道数。

过渡层：由于每个密集连接块产生的特征大小不一，为保证每个密集连接模块后的特征维度的统一，将过渡层设置在两个密集连接块之间，一般按照归一化，激活函数及1×1卷积和2×2池化顺序执行。

2.2　混合损失函数

在卷积神经网络中softmax 交叉熵损失函数被

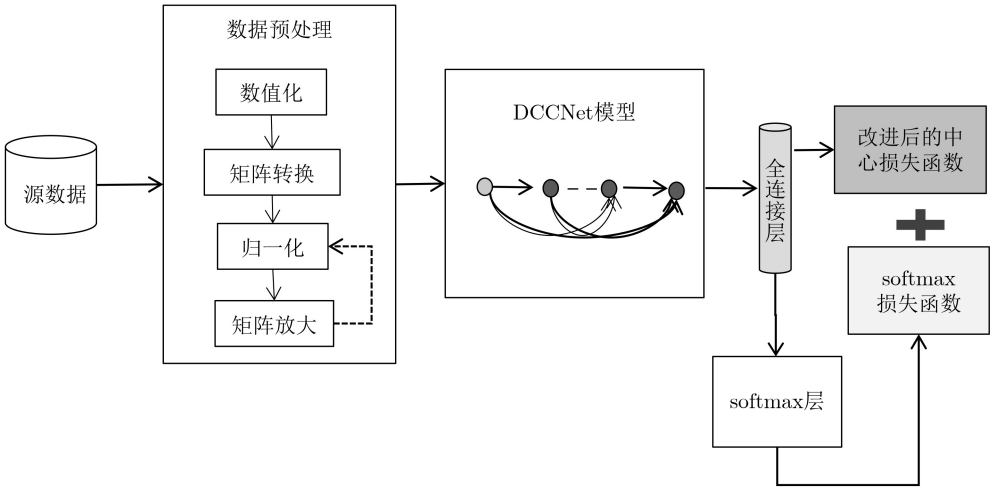

图 1 密集连接入侵检测模型框架

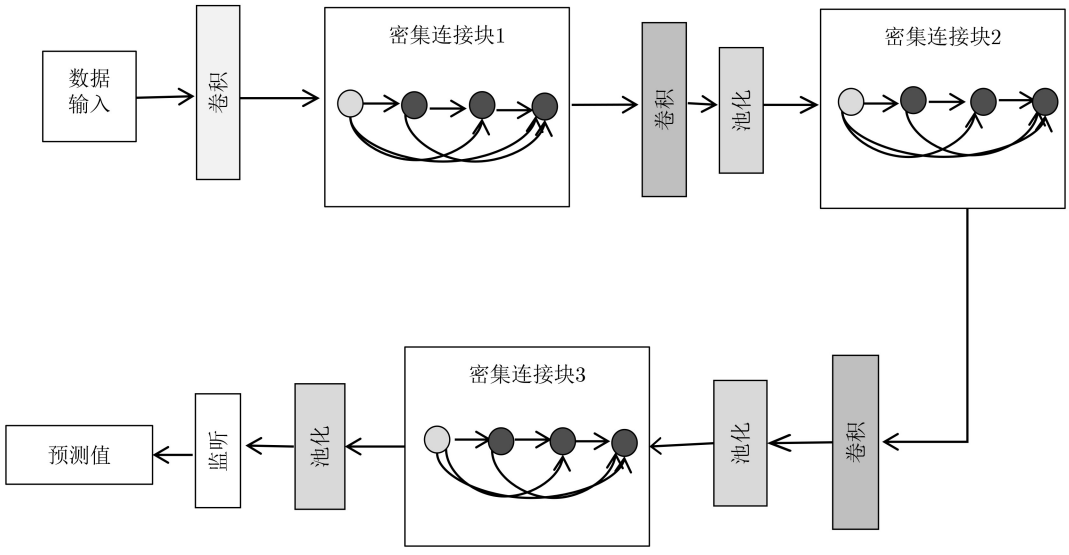

图 2 3个密集连接模块的完整密集连接神经网络

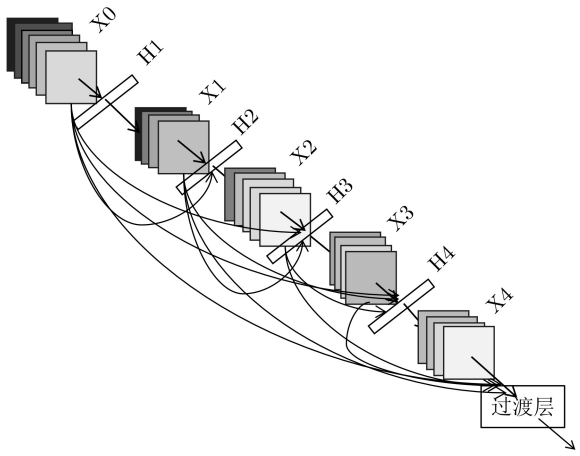

图 3 一个5层密集连接模块

用于多分类问题，softmax 损失函数由softmax函数和交叉熵(cross entropy)函数共同构成，通过指数函数使得多分类问题收敛更加容易。但是并没有有效地解决类内特征离散化和类间特征局部重叠的问题。中心损失函数(center loss[6])主要用于减少类内(intra-class)距离，使同一特征的样本之间的距离拉近，使其相似性变大并尽量往特征中心靠拢。softmax 损失函数与中心损失函数的结合[7]一定程度上减小了类内距离，但对于类间局部重叠问题并没有改善。

针对上述问题对中心损失函数提出改进，即在中心损失函数中添加一项类间特征距离，保证在其减小类内距离的同时增大类间距离，以达到提升网络结构的检测准确率的目的。改进后的中心损失函数为

$$L^* = L_{\mathrm{c}} + \lambda' \sum_{\boldsymbol{c}_i \in T} \sum_{\substack{\boldsymbol{c}_j \in T \\ \boldsymbol{c}_i \neq \boldsymbol{c}_j}} \left(\frac{\boldsymbol{c}_i \cdot \boldsymbol{c}_j}{\|\boldsymbol{c}_i\|_2 \|\boldsymbol{c}_j\|_2} + 1 \right) \tag{2}$$

其中，T表示特征类型的集合，$\boldsymbol{c}_i$和$\boldsymbol{c}_j$分别表示第i个和第j个类中心向量，$\|\boldsymbol{c}_i\|_2$和$\|\boldsymbol{c}_j\|_2$是对应坐标与原点之间的距离，λ'为平衡因子。因此，混合损失函数被定义为

$$L = L_{\mathrm{s}} + \lambda L* \tag{3}$$

其中，L_{s}为softmax损失函数。混合损失函数的类中心向量的更新如式(4)所示

$$\boldsymbol{c}_j = \frac{\sum_{i=1}^{m} \delta(y_i = j) \cdot (\boldsymbol{c}_j - x_i)}{1 + \sum_{i=1}^{m} \delta(y_i = j)} + \frac{\lambda'}{|N| - 1} \cdot \sum_{\substack{\boldsymbol{c}_j \in N \\ \boldsymbol{c}_i \neq \boldsymbol{c}_j}} \frac{\boldsymbol{c}_i}{\|\boldsymbol{c}_i\|_2 \|\boldsymbol{c}_j\|_2} - \left(\frac{\boldsymbol{c}_i \cdot \boldsymbol{c}_j}{\|\boldsymbol{c}_i\|_2 \|\boldsymbol{c}_j\|_2^3} \right) \boldsymbol{c}_j \tag{4}$$

其中，y_i是样本数据i的类别标签，$|N|$表示攻击类型的标签个数。

3 分析与讨论

3.1 数据集介绍

本文实验所选用的KDD 99数据集[8]是1998年DARPA在MIT林肯实验室对各种用户类型、网络流量和攻击手段仿真所形成的大约5×10^6条入侵检测领域内的经典数据，其更接近一个真实的网络环境。虽然年代有些久远，但KDD 99数据集仍然是网络入侵检测领域的事实基准，为基于计算智能的网络入侵检测研究奠定基础。KDD 99数据集中分成具有标识的训练数据和未加标识的测试数据。测试数据和训练数据有着不同的概率分布, 测试数据包含了一些未出现在训练数据中的攻击类型, 这使得入侵检测更具有现实性。

因此，在目前没有新的入侵检测数据集公开时，KDD 99数据集仍是当前研究入侵检测领域中首选的数据集。在数据集中，每条数据共42项，其中最后一项为标记类(label)表示该条数据是正常(normal)或异常(attack)。异常类又分为4种攻击类型，具体如下表1所示。前41项为每条数据的特征，包括38项数字特征和3项字符型特征。

3.2 模块设计

在第2节已经介绍了DCCNet神经网络的基本原理和结构，本文为了探寻较优的入侵检测DCCNet网络结构，设置了4个不同层次的密集连接网络，分别是46层、62层、102层和126层，每个完整的密集连接神经网络有3个密集连接块，其具体结构如表2所示。

4 实验结果与分析

4.1 数据预处理

本文在数据的选择上删除在分类上不起作用的1个特征，该特征位于31～41之间，只起到统计作用并没有在分类上提供任何有效信息。

4.1.1 数值化

本文对数据的数值化操作采用独热编码(one-hot)算法，将原本的40维特征被映射为121维。例如在KDD 99数据集中每条数据的协议类型(protocol-type)

表 1 4种攻击类型

攻击类型	备注
Dos	拒绝服务攻击
R2l	远程主机的未授权访问
U2r	授权的本地超级用户特权访问
Probe	端口监视或扫描

表 2　密集连接卷积神经网络具体结构

层结构	输出尺寸	46层网络结构	62层网络结构	102层网络结构	126层网络结构
卷积层	24×24	3×3卷积，步长=2			
密集连接块1	12×12	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times4$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times6$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times12$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times12$
过渡层1	12×12	1×1卷积			
	6×6	2×2平均池化			
密集连接块2	6×6	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times6$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times10$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times24$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times24$
过渡层2	6×6	1×1卷积			
	3×3	2×2平均池化			
密集连接块3	3×3	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times10$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times12$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times12$	$\begin{bmatrix}1\times1\text{conv}\\3\times3\text{conv}\end{bmatrix}\times24$
特征分类层	1×1	3×3全局平局池化			
	1×1	250D全连接			
	1×1	1000维损失函数层			

有3种分别是***TCP***, ***UDP***和***ICMP***，转换后得到***TCP***=[1, 0, 0], ***UDP***=[0, 1, 0], ***ICMP***=[0, 0, 1]。采用独热编码的好处在于，一是解决了分类器不好处理属性数据的问题；二是在一定程度上也起到了扩充特征的作用。

4.1.2　特征向量转为特征矩阵

为满足卷积神经网络的数据输入形式，对数值化后仍保持特征向量的数据通过向量-矩阵变化，将121维的特征向量转化层11×11的特征矩阵。

4.1.3　归一化处理

每条数据的各个特征数值之间相差显著，归一化的特征数值处理可以帮助分类结果更加精确。本文采用Min-Max处理函数，将特征数据值映射在[0, 1]之间，转换公式为

$$X' = \frac{X_{ij} - \text{Min}}{\text{Max} - \text{Min}} \tag{5}$$

其中，X'表示经归一化后映射在[0, 1]之间的特征值；X_{ij}表示第i条网络连接数据中的第j个特征数据值；Max表示该条特征属性的最大值，Min表示最小值。

4.1.4　矩阵放大

本文采用2维空间中最常用的基于Bicubic基函数的插值方法即双三次插值(Bicubic interpolation)算法[9]来对特征矩阵进行放大。Bicubic基函数的表现形式为

$$S(x) = \begin{cases} 1 - 2x^2 + |x|^3, & 0 \le |x| \le 1 \\ 4 - 8|x| + 5x^2 - |x|^3, & 1 < |x| \le 2 \\ 0, & |x| \ge 2 \end{cases} \tag{6}$$

在这种方法中，插值后的坐标点对应的值是原坐标点相邻近16个采样点加权平均得到的函数值。插值公式为

$$F(i+v, j+u) = \sum_{\text{row}=-1}^{2} \sum_{\text{col}=-1}^{2} f(i+\text{row}, j+\text{col}) \cdot S(\text{row}-v) S(\text{col}-u) \tag{7}$$

其中，其中，$(i+v,j+u)$表示源矩阵中的坐标点，i, j表示坐标点整数部分；v表示行数偏差，u表示列数偏差，注意v, u与row, col的对应；$f(i, j)$表示的是源坐标点(i, j)的值。

将处理好的11×11的矩阵经上述步骤用双三次插值法进行放大，得到大小为48×48的特征矩阵集。放大后的矩阵仍需要进一步的归一化，使得变为卷积神经网络所能识别的数据。

4.2　DCCNet网络结构设计

本文在3.2节的基础上设置两种增长率，即k值分别为24和32。

从图4在KDD99数据集上不同条件下的检测准确率的4组实验结果分析发现：检测的准确率随网络深度的增加而上升；在相同深度的网络层次下增长率大的检测准确率相对较高，但各个组之间存在差异；深度为102层，增长率为32时检测准确率相

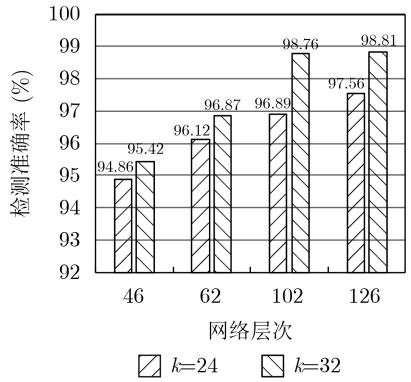

图 4 在KDD 99数据集上不同条件下的检测准确率

差最大。通过本次实验得到如下结论：在DCCNet网络结构模型下一定程度上增加网络的深度和增长率有利于提高网络入侵检测数据的准确率。为了使密集连接卷积神经网络的效果达到最优，使检测的准确率和训练的时间达到均衡状态，本文在没有特别说明的情况下均选择深度为102和k值为32的DCCNet网络结构进行实验。

4.3 实验步骤及参数配置

4.3.1 评价标准

本实验选择用10%的KDD 99数据集为实验数据，将准确率(ACcuracy rate, AC)、误报率(False Alarm rate, FA)作为验证指标[10]。计算公式为

$$\left.\begin{aligned}\mathrm{AC}&=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}}\\ \mathrm{FA}&=\frac{\mathrm{TN}}{\mathrm{TN}+\mathrm{FP}}\end{aligned}\right\} \tag{8}$$

其中，TP表示攻击类型被正确分类；TN表示正常类型被正确分类；FP表示正常类型被错误分类(误报)；FN表示攻击类型被错误分类(漏报)。

4.3.2 实验步骤说明

根据数据集的特征找到最合适的卷积神经网络结构是保证检测准确率的首要条件，根据模型的检测结果有评价标准得出该模型的利弊。具体的实验步骤为：

(1) 对KDD 99数据集进行10%的取样，并进行数据的预处理，具体步骤如4.1节所示，包括数值化、归一化、矩阵放大等操作。

(2) DCCNet网络结构的设计，针对所选数据集的特点从深度和Z两个方面设计出最合适的网络结构模型，并将模型的初始学习速率设置为0.1，根据epoch迭代设置不同时期的学习速率，使检测的准确率不断提升。

(3) 用训练数据集对模型进行训练，根据每次的结果有针对性的对结构中的参数改进调试，重复上一步使模型更接近理想型，模型训练完成。

(4) 将测试集作为模型输入数据，对训练好的DCCNet模型进行验证，以准确率、误报率为评价标准，并对验证过程进行记录对比实验结果。

4.3.3 参数配置

根据对DCCNet神经网络结构的不断训练和调整，本文所用的网络结构均是选择k为32,深度为102的DCCNet神经网络结构，具体的结构设置如表1所示。实验采用mini-batch随机梯度下降法训练样本，小批量处理大小设置为128，迭代次数设置为300次。网络学习速率的初始值为0.1，在网络收敛没达到预期值之前，学习速率每隔一段时间调至原来的1/10，混合损失函数中的λ，λ'的大小均为0.005。

4.4 实验对比及分析

4.4.1 损失函数有效性实验

为了验证所提出的混合损失函数的有效性，在保证其他参数设置不变的情况下对不同损失函数进行测试，如图5所示在不同损失函数下的5种特征类型的检测准确率。

从图5不难看出，本文所选用的混合函数的检测率高于其他3中函数的检测率，尤其是对于正常数据的准确率相比于其他损失函数效率有着明显的提升，最大差值为4.30%,可以体现出在中心损失函数中添加类间特征距离所带来的显著优势。

4.4.2 模型结果与分析实验

本文将DCCNet卷积神经网络模型与应用在入侵检测中的其他4种卷积神经网络结构对比，把检测的准确率和误报率作为本次实验的评价标准。结果如下表3所示。

通过横向对比分析得出：在准确率方面本文的检测准确率最高，比拥有最高检测准确率的IRes模型高出1.53%，相对于有较低误报率的IBIDM模型其准确率提升了5.82%；本文的误报率要低于IRes模型和MSCNN模型。另一方面可以看出，在将卷积神经网络应用于入侵检测的过程中网络结构深度逐渐加深，这也是后两者模型的误报率偏高的一种因素。主要由于随着网络结构的加深梯度弥散(gradient vanish)的现象明显，但DCCNet卷积神

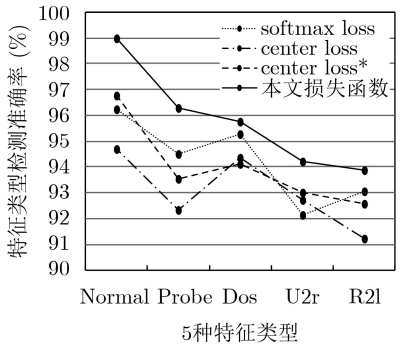

图 5 不同损失函数下的5种特征类型检测准确率

表 3 本文实验模型数据与其他模型结果对比(%)

模型	准确率AC	误报率FA
本文	98.76	1.32
LeNet	92.18	0.97
IBIDM	92.94	0.76
IRes	97.23	2.73
MSCNN	92.36	8.08

经网络特殊结构保证了在深度层次下改善了梯度弥散这一问题。

4.4.3 泛化性能实验

DCCNet神经网络结构相比于其他结构的神经网络有较好的泛化能力已经在Cortes等人[11]提出的文章中得以证明。本文为验证所设计的DCCNet神经网络结构具有优良的泛化能力，使用NSL-KDD数据集[12]进行实验。

实验将检测的准确率(AC)和召回率(Rec)作为评价标准[13]，计算公式为

$$\left.\begin{aligned} \mathrm{AC} &= \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \\ \mathrm{Rec} &= \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \end{aligned}\right\} \tag{9}$$

实验结果如表4所示。

表 4　NSL-KDD数据集在不同模型下的准确率和召回率

模型	准确率AC	召回率Recall
本文	0.973	0.915
LSTM-RESNET[14]	0.965	0.695
文献[15]	0.872	0.928
cPCA-AMSOM[16]	0.946	0.944

通过表4可以发现，本文在选用密集连接卷积神经网络对NSL-KDD数据集进行训练和测试取得了很好的效果。相对于LSTM-RESNET模型而言虽在检测准确率方面仅提升了0.008但其召回率高出了0.22，表现出本文模型在保持高准确率的同时对被错误分类特征召回的有效性；与此同时在召回率方面相比于高召回率的文献[15]和cPCA-AMSOM模型有着较高的检测准确率。体现出本文所提出的网络结构具有很好的泛化能力。

5　结束语

本文提出将密集连接卷积神经网络用于入侵检测并根据输入数据的分类特点使用改进后的中心损失函数与softmax 损失函数结合形成混合损失函数取得了一定的成果。实验结果表明，DCCNet网络结构不仅保证了有较高的检测准确率还有着较低的误报率，梯度消失问题也得到缓解。后续工作将致力于减少训练时间加快收敛速度，针对参数提出优化[17]提升模型的性能。同时为保证所提出的密集连接卷积神经网络结构在入侵检测的实际应用中有很好的效果，会寻找机会将其应用到具体的网络环境中，在实践中检验本文提出的基于密集连接聚集神经网络的入侵检测技术的合理性。

参 考 文 献

[1] LU Na, WU Yidan, FENG Li, *et al*. Deep Learning for fall detection: Three-dimensional CNN combined with LSTM on video kinematic data[J]. *IEEE Journal of Biomedical and Health Informatics*, 2019, 23(1): 314–323. doi: 10.1109/JBHI.2018.2808281.

[2] LIU Pengju. An intrusion detection system based on convolutional neural network[C]. The 11th International Conference on Computer and Automation Engineering, Perth, Australia, 2019. doi: 10.1145/3313991.3314009.

[3] 刘月峰, 王成, 张亚斌, 等. 用于网络入侵检测的多尺度卷积CNN模型[J]. 计算机工程与应用, 2019, 55(3): 90–95, 153. doi: 10.3778/j.issn.1002-8331.1712-0021.

LIU Yuefeng, WANG Cheng, ZHANG Yabin, *et al*. Multiscale convolutional CNN model for network intrusion detection[J]. *Computer Engineering and Applications*, 2019, 55(3): 90–95, 153. doi: 10.3778/j.issn.1002-8331.1712-0021.

[4] 赵昱博. 基于卷积神经网络的入侵检测技术的研究[D]. [硕士论文], 哈尔滨工程大学, 2018.

ZHAO Yibo. Research on intrusion detection technology based on convolutional neural network[D]. [Master dissertation], Harbin Engineering University, 2018.

[5] WANG Shengwei, WANG Hongkui, XIANG Sen, *et al*. Densely connected convolutional network block based autoencoder for panorama map compression[J]. *Signal Processing: Image Communication*, 2020, 80: 115678. doi: 10.1016/j.image.2019.115678.

[6] WEN Yandong, ZHANG Kaipeng, LI Zhifeng, *et al*. A discriminative feature learning approach for deep face recognition[C]. The 14th European Conference on Computer Vision, Amsterdam, Netherlands, 2016: 499–515. doi: 10.1007/978-3-319-46478-7_31.

[7] 郭晨, 简涛, 徐从安, 等. 基于深度多尺度一维卷积神经网络的雷达舰船目标识别[J]. 电子与信息学报, 2019, 41(6): 1302–1309. doi: 10.11999/JEIT180677.

GUO Chen, JIAN Tao, XU Congan, *et al*. Radar HRRP target recognition based on deep multi-scale 1D convolutional neural network[J]. *Journal of Electronics & Information Technology*, 2019, 41(6): 1302–1309. doi: 10.11999/JEIT180677.

[8] 范晓诗, 雷英杰, 王亚男, 等. 流量异常检测中的直觉模糊推理方法[J]. 电子与信息学报, 2015, 37(9): 2218–2224. doi: 10.11999/JEIT150023.

FAN Xiaoshi, LEI Yingjie, WANG Yanan, *et al*. Intuitionistic fuzzy reasoning method in traffic anomaly detection[J]. *Journal of Electronics & Information Technology*, 2015, 37(9): 2218–2224. doi: 10.11999/JEIT150023.

[9] 颜伟, 耿路, 周雷, 等. 基于海情和三次样条插值算法的舰船雷

达散射截面优化分析方法[J]. 电子与信息学报, 2018, 40(3): 579–586. doi: 10.11999/JEIT170562.

YAN Wei, GENG Lu, ZHOU Lei, *et al*. Optimization analysis method on ship RCS based on sea conditions and cubic spline interpolation algorithm[J]. *Journal of Electronics & Information Technology*, 2018, 40(3): 579–586. doi: 10.11999/JEIT170562.

[10] CHAWLA A, LEE B, FALLON S, *et al*. Host based intrusion detection system with combined CNN/RNN Model[C]. Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Dublin, Ireland, 2019. doi: 10.1007/978-3-030-13453-2_12.

[11] CORTES C, GONZALVO X, KUZNETSOV V, *et al*. AdaNet: Adaptive structural learning of artificial neural networks[J]. arXiv: 2016, 1607.01097.

[12] SHARMA S, GIGRAS Y, CHHIKARA R, *et al*. Analysis of NSL KDD dataset using classification algorithms for intrusion detection system[J]. *Recent Patents on Engineering*, 2019, 13(2): 142–147. doi: 10.2174/1872212112666180402122150.

[13] POTLURI S, AHMED S, and DIEDRICH C. Convolutional neural networks for multi-class intrusion detection system[C]. The 6th International Conference on Mining Intelligence and Knowledge Exploration, Cluj, Romania, 2018: 225–238. doi: 10.1007/978-3-030-05918-7_20.

[14] YANG Yingen and WANG Zhongyang. Intrusion detection technology based on deep neural network[J]. *Network Security Technology & Application*, 2019(4): 37–41.

[15] SHONE N, NGOC T N, PHAI V D, *et al*. A deep learning approach to network intrusion detection[J]. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018, 2(1): 41–50. doi: 10.1109/TETCI.2017.2772792.

[16] 吴德鹏, 柳毅. 基于可变网络结构自组织映射的入侵检测模型[J]. 计算机工程与用, 2019, 5: 1–9.

WU Depeng and LIU Yi. Intrusion detection model based on self-organizing mapping of variable network stucture[J]. *Computer Engineering and Applications*, 2019, 5: 1–9.

[17] 陈红松, 陈京九. 基于循环神经网络的无线网络入侵检测分类模型构建与优化研究[J]. 电子与信息学报, 2019, 41(6): 1427–1433. doi: 10.11999/JEIT180691.

CHEN Hongsong and CHEN Jingjiu. Recurrent neural networks based wireless network intrusion detection and classification model construction and optimization[J]. *Journal of Electronics & Information Technology*, 2019, 41(6): 1427–1433. doi: 10.11999/JEIT180691.

缪祥华：男，1972年，博士后，副教授，研究方向为信息安全、网络安全、移动通信安全.

单小撤：男，1992年，硕士生，研究方向为信息安全、入侵检测.

责任编辑：马秀强