基于深度卷积神经网络的入侵检测研究

丁红卫 万 良 周 康 龙廷艳 辛 壮

(贵州大学计算机科学与技术学院 贵阳 550025) (贵州大学计算机软件与理论研究所 贵阳 550025)

摘 要 当今网络数据呈现出更为庞大、复杂和多维的特性。传统的基于机器学习的方法在面临高维数据特征时需要手动提取大量特征,特征提取过程复杂且计算量大,达不到入侵检测的准确性和实时性的要求。深度学习在处理复杂数据方面具有较好的优势,可以自动从数据中提取更好的表示特征。为此,文中创新性地提出了一种基于深度卷积神经网络的入侵检测方法。首先,提出了一种将网络数据转换为图像的方法;然后,针对转换之后的图像设计了一个深度卷积神经网络模型,该模型使用两层的卷积层和池化层对图像进行降维处理,并引入了 Relu 函数作为新的非线性激活来代替传统的神经网络中常用的 Sigmoid 或 Tanh 函数,以加快网络的收敛速度,且该模型引入了 Dropout 方法来防止网络模型发生过度拟合的现象;最后,通过构建完成的深度卷积神经网络模型对转换之后的图像进行训练和识别。实验结果表明,与已有方法相比,所提方法具有更好的检测准确率、更低的误报率和更快的检测速率。

关键词 入侵检测,深度学习,卷积神经网络,特征提取,过度拟合

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/jsjkx.180801429

Study on Intrusion Detection Based on Deep Convolution Neural Network

DING Hong-wei WAN Liang ZHOU Kang LONG Ting-yan XIN Zhuang

(College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

(Institute of Computer Software and Theory, Guizhou University, Guiyang 550025, China)

Abstract Compared with the previous network data, network data shows more huge, complex and multidimensional characteristics nowadays. In face of the high dimensional data features, traditional machine learning methods need to extract a large number of features manually. Besides, feature extraction process is complex and computational, which is not conducive to the current network intrusion detection real-time and accuracy requirements. Deep learning methods have good advantages in dealing with complex data, which can automatically extract better representation features from the data. In this paper, an intrusion detection method based on deep convolution neural network was proposed. Firstly, a method of transforming network data into images was proposed. Then a deep convolution neural network model was designed for the transformed image, which uses the two-layer convolution layer and the pool layer to reduce the dimension of the image, and introduced the Relu function as a new nonlinear activation in place of the traditional neural network. The sigmoid or Tanh function was used to speed up the convergence of the network, and the Dropout method was introduced in the model to prevent the network model from over-fitting. Finally, the image was trained and identified by constructing the completed depth convolution neural network model. The experimental results show that the proposed method has better detection accuracy, lower false alarm rate and higher detection rate compared with the existing methods.

Keywords Intrusion detection, Deep learning, Convolution neural network, Feature extraction, Over-fitting

1 引言

随着互联网的迅速更新和发展,网络的安全性问题变得尤为突出,已经成为了阻碍网络发展的重要因素。网络数据容易受到各种类型的攻击,从而降低网络或系统的使用效率,因此如何保障网络的安全性,减少网络攻击对企业和个人造成的威胁,已经成为业内人员和网络安全技术人员密切关注的问题。

入侵检测系统[1-2]作为保障网络安全的重要技术之一,越来越受到业界人士的密切关注。目前已有多种入侵检测

到稿日期:2018-08-02 返修日期:2019-01-20 本文受贵州省科学基金黔科合 J 字[2011](2328),贵州省科学基金黔科合 LH 字[2014](7634)资助。

丁红卫(1992-),男,硕士生,CCF 会员,主要研究方向为信息安全和机器学习,E-mail:1760901417@qq.com;万 良(1974-),男,博士,教授,主要研究方向为信息安全、计算机软件与理论,E-mail:wanliangtr@163.com(通信作者);周 康(1993-),男,硕士,主要研究方向为信息安全和深度学习;龙廷艳(1993-),女,硕士,主要研究方向为信息安全;辛 壮(1994-),男,硕士,主要研究方向为信息安全和机器学习。

方法，许多预测都是通过机器学习方法[3-7]完成的。神经网络作为一种智能性的算法，已被成功应用于入侵检测领域。神经网络算法具有良好的自学功能、联想存储功能、高速寻优功能，以及高效的并行分布处理功能，非常适用于处理目前网络流量中的复杂数据。

当今网络数据呈现出了更为庞大、复杂和多维的特性，传统的基于机器学习的入侵检测方法已逐渐失效。而深度学习在处理当今海量复杂数据方面具有较好的优势，它可以从数据中提取更好的表示特征。对此，本文利用深度卷积神经网络在处理图像方面的高效性和有效性，提出了一种将网络数据转换为图片，然后利用深度卷积神经网络进行检测识别的方法，即基于深度卷积神经网络(Convolutional Neural Network，CNN)的入侵检测方法，以期为入侵检测研究提供一种新的思路。

2 相关研究

自 Hinton 等提出深度学习[8]的理论之后，深度学习作为机器学习的一个重要分支领域，越来越受到研究者们的关注。一些研究入侵检测的学者们也开始逐渐将深度学习方法引入到入侵检测领域。Roy 等[9]提出了一种基于深度学习的人工神经网络入侵检测方法，该方法通过描述受数据约束类的后验分布来提供区分模式分类的能力，从而得到一个较为有效的分类模型。Yin 等[10]提出了基于循环神经网络的入侵检测模型(RNN-IDS)，该模型不仅具有很强的入侵检测建模能力，而且在二分类和多分类中都具有较高的检测精度。Alom 等[11]提出了一种基于深度置信网络的入侵检测模型，该方法使用堆叠的受限玻尔兹曼机生成的深度置信网络来进行网络数据的检测，通过较少的迭代训练实现了较高的入侵检测准确率。Javaid 等[12]提出了一种基于深度学习的方法来开发高效、灵活的 NIDS，实现了一种基于稀疏自编码器和 softmax 回归的入侵检测方法。Potluri 等[13]提出了一种加速 DNN 体系结构，用于识别网络数据中的异常，并用加速器平台处理海量数据集，在输入数据集上找到复杂的关系来识别不同的攻击类型。实验结果表明，将该方法应用到入侵检测中是可行并且有效的。Yu 等[14]实现了一种基于 SDA 的深层体系结构来自动学习僵尸网络的基本特征，从而提出了基于会话的方法来构造原始网络流量下的入侵检测数据集，并对数据集上不同深度学习方法的性能进行了评估。Kwon 等[15]对深度学习模型进行了相关研究，重点讨论了数据约简、降维、分类等技术，提出了一种 FCN 模型，并通过对比传统的机器学习技术，证明了 FCN 模型对网络流量分析的有效性。王明等[16]提出了一种基于卷积神经网络的入侵检测系统，该系统可以有效地提取原始样本信息，从而提高分类准确率。

基于深度学习的入侵检测中，常见的方法有 DBN，RBM 和 RNN 等。但是，这些方法的网络结构和训练过程通常都较为复杂，并且网络结构中的参数较多，从而增加了网络训练的难度。而在 CNN 网络中，可以通过权值共享有效地解决传统神经网络中参数较多的问题，而且通过卷积层和池化层对图像进行降维处理可以有效地降低网络的复杂度，从而有效地加快入侵检测速率。基于 CNN 在图像识别方面的高效性和有效性，本文提出了一种将网络数据转换为图像的方法，从而使得同类型的数据得到相同或相似的图像，然后使用 CNN 模型进行图像分类识别。

3 数据图像化处理

3.1 数据集准备

为了验证文中所提方法的有效性，使用公共入侵检测数据集(KDD CUP99 数据集)进行实验。KDD CUP99 数据集[17]是当前入侵检测常用的标准数据集，其中的每一条实例数据包含 41 个特征属性和 1 个标签属性。数据分为 5 个大类型，其中异常数据有 4 类，异常数据又被细分为 39 类攻击，其中 22 种攻击类型在训练集中出现，另外 17 种未知攻击类型在测试集中出现。5 类标签分别是 Normal，DOS，Probe，R2L，U2R。通常使用 10% 的 KDD CUP99 数据集作为训练集，将 Corrected 数据集作为测试集，数据详情如表 1 所列。

表 1 KDD CUP99 数据

Table 1 KDD CUP99 data

KDD CUP99	Normal	Dos	Probe	U2R	R2L	Total
10% 的 KDD	97278	391458	4107	52	1126	494021
Corrected	60593	225893	4166	228	16189	311029

3.2 数据预处理

由于 CNN 模型只能识别数值型数据，而原始的 KDD CUP99 数据集中包含字符型数值，因此，为了能够将 KDD CUP99 数据作为 CNN 模型的输入数据，本文对原始的数据集进行了预处理操作。预处理过程主要包含数值化和归一化两个过程，如图 1 所示。

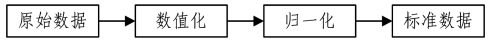

图 1 数据预处理过程

Fig. 1 Data preprocessing process

3.2.1 数值化

原始的 KDD CUP99 数据集中有 3 个属性为字符型的特征属性，分别为 protocol_type，service，flag。文中分别对这 3 种字符型数值进行了数值化编码处理，具体过程如图 2 所示。

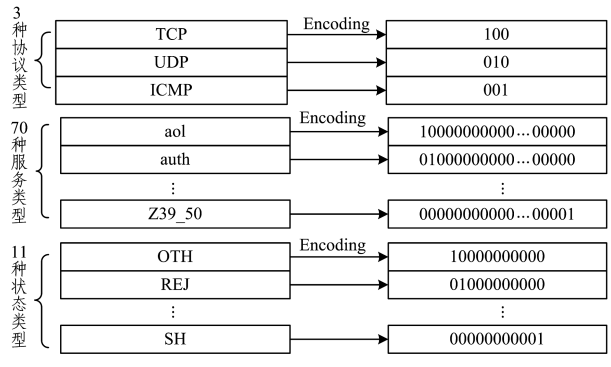

图 2 字符编码

Fig. 2 Character encoding

3.2.2 归一化

进行数值化处理之后，数值间量纲差异较大，如特征属性 duration(连接持续时间)，其取值范围为[0，58329]。数值差异较大时容易引起网络收敛较慢和神经元输出饱和等问题，

因此需要对原始数据进行归一化处理。文中使用最大-最小归一化方法将数据集中的数据归一化到[0，1]区间之内。其公式为：

$$x^* = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

其中，x^* 为归一化后的数据，x 为当前原始数据，$x_{\min}$ 为当前属性中的最小数据值，$x_{\max}$ 为当前属性中的最大数据值。

3.3　图像化处理

进行数据预处理之后得到了取值在[0，1]之间的数值型数据集，该数据集中每条数据的维度为 122。如果使用传统的入侵检测方法进行处理，会因为数据集的维度过大而导致训练和测试较慢。因此，本文将数据转换为图像，使用 CNN 模型进行训练和检测。一方面，CNN 模型在图像识别方面有优异的检测效果；另一方面，对 CNN 模型中的卷积层和池化层的特征进行降维后，不会因为数据的维度过大而导致训练和预测缓慢的情况。为了能够得到一组有效的图片，且不影响实验效果，对 122 维度的数据进行了简化处理，删除其中一维在训练集和测试集中特征值全为 0 的数据，将 122 维数据变为 121 维数据。最后，将 121 维数据转换为 11 * 11 的图像。5 类数据转换为图像之后的相似性对比如图 3 所示，数据样例如表 2 所列。通过对比结果可知，同种类型的数据转换为图像之后有极大的相似性。

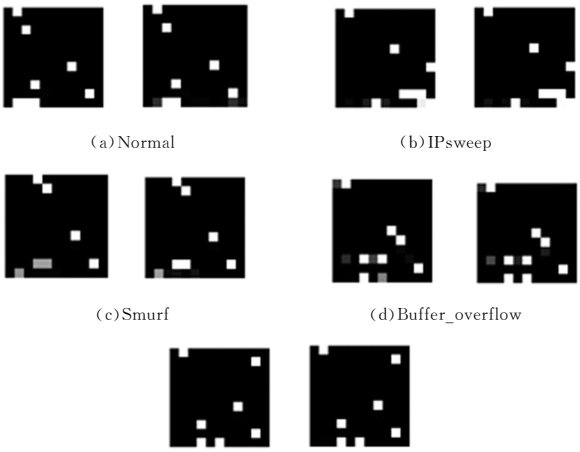

图 3　数据转图像

Fig. 3　Process of data to image

表 2　样例说明

Table 2　Sample description

样例	Normal	Ipsweep	Smurf	Buffer_overflow	Warezclient
攻击类型	Normal	Probe	Dos	U2R	R2L

4　基于 CNN 的入侵检测方法

4.1　CNN 网络结构

CNN[18] 是在对视觉皮层细胞的研究中获得启发而研究得来的，其重要特性是通过局部感受野、权值共享以及时间或空间亚采样等思想来减少网络中自由参数的个数，从而获得某种程度的位移、尺度、形变不变性。

本文使用的 CNN 网络结构如图 4 所示，该网络结构由 8 层结构组成，其中第 1 层为数据输入层；第 2 层和第 4 层为卷积层；第 3 层和第 5 层为池化层；第 6 层和第 7 层为全连接层；最后一层为 CNN 结构的输出层。

图 4　CNN 网络结构

Fig. 4　CNN network structure

各层网络的结构描述如下。

(1)CNN 结构的第 1 层为网络的输入层。数据可视化后转换为图像的维度为 11 * 11，因此本层网络的输入维度为 11 * 11。

(2)第 2 层和第 4 层为卷积层，主要是对图像进行卷积操作。深度 CNN 网络引入了 Relu 函数作为新的非线性激活，用于代替传统神经网络中常用的 sigmoid 或 tanh 函数，可以有效地加快网络收敛和训练的速度。第 2 层使用 16 种滤波器，第 4 层使用 8 种滤波器，因此第 2 层和第 4 层使用每一种滤波器去卷积输入矩阵，可以分别得到 16 个和 8 个特征图。第 2 层和第 4 层的卷积核大小设定为[5 * 5]。

(3)第 3 层和第 5 层为池化层(下采样层)，主要是对输入进行降采样，常用的池化方法主要为最大值法和均值法。本文第 3 层和第 5 层使用最大池化层方法，即利用最大子采样函数取采样区域内所有神经元的最大值，采样核大小设置为[2 * 2]。

(4)第 6 层和第 7 层为全连接层，其结合前一层和输出层共同构成分类部分。每层网络的激活函数同样使用 Relu 激活函数，并在这两层引入 Dropout 方法来防止过度拟合。第 6 层和第 7 的神经元个数分别为 100 和 50。

(5)最后一层为网络的输出层，该层主要用于分类预测，使用 softmax 作为该层的分类器。

4.2　CNN 的学习过程

卷积神经网络的学习过程采用反向传播算法，即在输入层输入训练数据，然后经过卷积层、池化层、全连接层和输出层的计算得出预测值，最后使用误差函数计算真实值与预测值的差值，从而反向迭代更新网络的权值和阈值。

4.2.1　卷积层

在 CNN 中，多层卷积层的组合构成了卷积神经网络中的特征提取模块。通过卷积操作，原始信号特征得到加强，而噪声会相对减弱[19]。CNN 正是利用卷积层的这一特性，来达到强化图像的固有特性并模糊次要特征的目的。每个卷积层均包含卷积操作和非线性激活两个过程。当前层的特征图可由卷积核和前一层的输出特征图或原始特征图进行卷积操作得到，具体过程如式(2)所示：

$$X_j^l = \sum_i \boldsymbol{X}_i^{l-1} \otimes \boldsymbol{K}_{ij}^{l-1} + b_j^l \tag{2}$$

其中，X_j^l 表示经过卷积之后第 l 层特征图中的第 j 个位置的

输入；$\boldsymbol{X}_i^{l-1}$ 表示第 $l-1$ 层中的第 i 个输入矩阵；$\boldsymbol{K}_{ij}^{l-1}$ 表示在第 l 层和第 $l-1$ 层之间连接第 i 个输入矩阵和第 j 个位置的卷积核；b_j^l 表示第 l 层特征图中第 j 个位置的偏置量。

通过式(2)计算得到的输出矩阵，还需要进行非线性激活操作。非线性激活过程可以除去数据中的冗余信息并保留原始数据特征的映射信息，同时也可以加强网络模型的非线性表达能力，让 CNN 拟合更为复杂的特征。常用的激活函数有 sigmoid，tanh 和 Relu(见式(3))等。由于 Relu 相较于其他的激活函数具有更优的性质，可以使得网络更快地收敛，因此本文所使用的非线性激活函数为 Relu 激活函数：

$$f(x)=\max(0,x) \tag{3}$$

其中，当 x 的取值小于 0 时，$f(x)$ 的取值为 0；当 x 的取值大于 0 时，$f(x)$ 的取值为 x。

4.2.2 池化层

通过卷积层的卷积操作之后，使用 m 个滤波器可以得到 m 个特征图。由于经过卷积之后的图像特征依然很多，网络的复杂度依然很高，因此还需要对其进行池化层的操作。池化层的主要作用是对特征图进行压缩处理。池化层的压缩操作不但可以减少特征图的维度，还降低了网络的复杂度，而且可以对特征图进行特征压缩，保留特征图的主要特征。

常用的池化操作有 Avy Pooling(平均池化)和 max pooling(最大池化)两种方法。Avy Pooling 方法是取池化矩阵窗口中的平均值作为输出值，max pooling 方法是取池化矩阵中数据的最大值作为输出值。池化操作的滑动步长通常设定为大于或者等于 2 的值，这样可以起到有效的降维作用。

4.2.3 全连接层

经过池化层之后，得到的特征图中的每个神经元都和全连接层中的神经元相连。与传统的多层感知机的神经元输入计算公式类似，全连接层的神经元的输出计算公式如下：

$$y_j^l=\sum_i w_{ij}^l * x_i^{l-1}+b_j^l \tag{4}$$

其中，y_j^l 表示第 l 层全连接层神经元中第 j 个神经元经计算后的输入结果；w_{ij}^l 表示 $l-1$ 层中特征图的第 i 个特征与 l 层中第 j 个神经元的连接权重；x_i^l 为 $l-1$ 层中特征图的第 i 个特征值；b_j^l 为第 l 层全连接层神经元中第 j 个神经元的偏置值。Relu 在深层网络中有着优异的表现，被广泛应用于深层结构[20]。因此，本文全连接层的激活函数依然选用 Relu。本文在 CNN 结构的全连接层引入了 Dropout 方法，该方法可以有效地防止因为训练集的不足或是过度训练而导致的过度拟合现象的发生。

4.2.4 分类预测层

分类预测层作为神经网的最后一层，用于网络的输出预测。常用的分类模型主要有 logistic 回归和 softmax 回归。logistic 回归主要用于解决二分类的问题，softmax 回归主要用于解决多分类的问题。本文的数据样本共分为 5 类，因此使用 softmax 作为最后的分类预测模型。softmax 将 x 预测为类别为 j 的概率公式如式(5)所示：

$$p(y^{(i)}=j/x^{(i)};\theta)=\frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^{k} e^{\theta_j^T x^{(i)}}} \tag{5}$$

其中，θ 为模型的参数。

在卷积层之后，高层逻辑推理通过全连接层完成，即全连接层的神经元与前一层的所有输出相连接。全连接层后还需要使用代价函数来度量深度神经网络训练输出值和真实值之间的差异，在不同的应用中使用不同的代价函数[21]。本文对比了不同的代价函数对实验结果的影响，具体的实验验证见第 5 节。

4.3 CNN-IDS 模型

本文提出的入侵检测框架如图 5 所示。

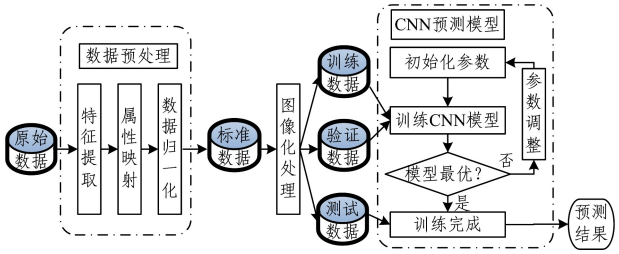

图 5 基于 CNN 入侵检测系统的结构

Fig. 5 Structure based on CNN intrusion detection system

该入侵检测框架的具体步骤描述如下。

Step1 从网络上获取原始的网络数据包。

Step2 对原始的网络数据进行预处理。预处理过程主要分为 3 个步骤：

1)特征提取。使用特征提取器对原始的网络数据包进行特征提取。

2)属性映射。将提取之后的字符型网络数据转换为数值型的数据。

3)数据归一化。由于同种属性的数据之间相差较大，影响了神经网络的训练，因此将数据归一化到[0,1]区间内。

Step3 图像化处理：将得到的标准数据集进行图像化处理。

Step4 数据分离：将得到的图像数据分为训练数据、验证数据和测试数据。其中，训练数据用于训练 CNN 模型，验证数据用于检验 CNN 模型训练过程中的效果，测试数据用于测试训练完成的模型的效果。

Step5 模型训练：对深度卷积神经网络进行训练和参数调优。

1)初始化 CNN 模型参数。

2)训练 CNN 模型，使用验证数据集对每轮训练完成的深度卷积神经网络进行验证，待神经网络训练完成后，根据验证结果调整深度卷积神经网中的各参数，直到模型达到最优。

3)最后得到一个训练完成的最优深度 CNN 模型。

Step6 将 Step2 中经过预处理之后的测试数据集输入到训练完成的深度 CNN 模型，进而得到每条数据的分类预测结果。

5 实验与分析

5.1 实验评价标准

本文实验采用准确率(Accuracy，AC)、误报率(False Alarm Rate，FA)和召回率(Recall，RE)等作为实验效果优劣的评判标准：

$$AC=\frac{TP+TN}{P+N} \tag{6}$$

$$FA=\frac{FN}{P} \tag{7}$$

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

参数的具体含义如表 3 所列。

表 3　参数定义

Table 3　Parameter definitions

P	*N*	*TP*	*FN*	*TN*	*FP*
正样本数	负样本数	正样本被判正样本	正样本被判负样本	负样本被判负样本	负样本被判正样本

5.2　结构验证分析

5.2.1　参数设置

通过多次对比实验对 CNN 方法的参数进行设置，结果如表 4 所列。经过图像化处理之后的 KDDCUP99 数据集中，原始的一维数据会转换为 11 * 11 的二维数据，标签属性被映射为 5 维。因此，输入层维度被设置为 11 * 11 的矩阵，输出层节点数被设置为 5。

表 4　CNN 模型的参数设置

Table 4　Setting of CNN model parameters

CNN 参数	值
输入层	Input_dim=(11,11)
卷积层 1	卷积核个数=16，stride=(5,5)，activation=relu
池化层 1	Stride=(2,2)
卷积层 2	卷积核个数=8，stride=(5,5)，activation=relu
池化层 2	Stride=(2,2)
全连接层 1	节点数=100，activation=relu
全连接层 2	节点数=50，activation=relu
输出层	节点数=5，activation=softmax
训练轮数	Epochs=30

5.2.2　结构分析

神经网络中，网络的结构对实验结果有较大的影响，因此本文对不同结构的 CNN 模型结构进行了实验探讨。本文选择 40000 条训练数据和 10000 条测试数据，具体情况如表 5 所列。实验设置了 3 种不同结构（一组卷积和池化层结构，两组卷积和池化层结构，以及三组卷积和池化层结构）的 CNN 模型来比较各自的性能，结果如图 6 所示。

表 5　各类数据的详情

Table 5　Details of various types of data

Data set	Normal	Dos	Porbe	U2R	R2L	Records
Train	10000	24719	4107	52	1122	40000
Test	2700	6004	1010	35	251	10000

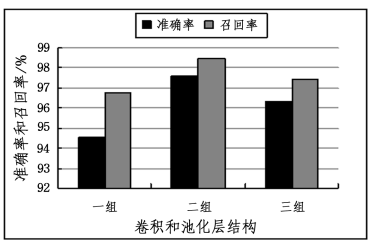

图 6　准确率和召回率的对比

Fig. 6　Comparison between accuracy rate and recall rate

由上述两组实验结果的对比可知，具有两组卷积和池化层结构的 CNN 网络在准确率、召回率方面都要优于其他两组结构。具有两组卷积和池化层结构的 CNN 网络在迭代 30 次后，训练集和验证集的准确率和损失函数曲线如图 7 和图 8 所示，其中 acc 和 val_acc 分别代表训练集和验证集的准确率，loss 和 val_loss 分别代表训练集和验证集的损失函数曲线。由两组图像可知，使用具有两组卷积结构的神经网络进行入侵检测实验时，检测曲线呈现稳定上升的趋势，代价函数值呈现稳定下降的趋势，表明该结构的神经网络具有良好的训练效果，可有效地避免过度拟合现象。因此，本文选择具有两组卷积和池化层结构的 CNN 模型作为实验模型。

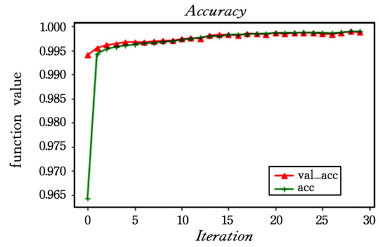

图 7　准确率曲线

Fig. 7　Accuracy rate curve

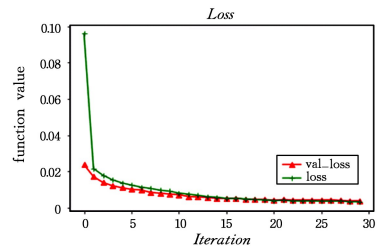

图 8　损失函数曲线

Fig. 8　Loss function curve

5.2.3　损失函数分析

损失函数在不同的神经网络和分类器中有不同的应用，本文对不同的损失函数做了对比实验，结果如图 9 所示。实验对比了 mse，mape，categorical_hinge，logcosh，categorical_crossentropy，cosine_proximity 和 binary_crossentropy 等损失函数，通过实验结果可知，binary_crossentropy 损失函数相比其他损失函数在准确率上更具优势。因此，本文将 binary_crossentropy 损失函数作为计算真实值和预测值之间差异的函数。

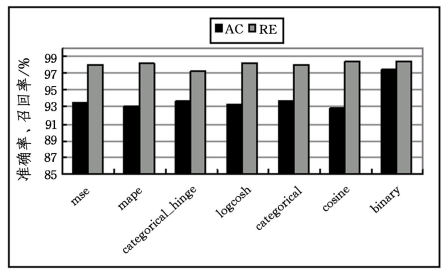

图 9　不同损失函数的对比结果

Fig. 9　Comparison results of different loss functions

5.3　不同类别数据的结果分析

网络中的攻击类型通常较为复杂，因此本文设置了不同的攻击组合类型来测试本文算法应对复杂网络攻击的有效性。

表 6 列出了图 10 所示的攻击组合中所包含的攻击类型。其中，“T”表示攻击组合中包含了该类攻击；“F”表示攻击组合中没有包含该类攻击，但该类攻击被作为一个单独的攻击类型进行实验。

表 6 攻击组合说明

Table 6 Attack combination description

类别	Attack			
	DOS	Probe	R2L	U2R
1	T	T	T	T
2	F	T	T	T
3	F	F	T	T
4	F	F	F	T

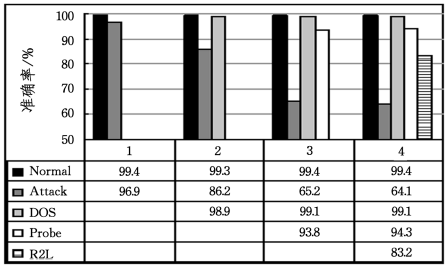

图 10 各类数据的准确率

Fig. 10 Accuracy rate of all kinds of data

从图 10 的结果可以看出，使用 CNN 模型结构进行入侵检测实验，当只包含 Normal 和 Attack 2 类数据时，其对 Normal 和 Attack 的检测率都较高；当包含 3 类数据时，其对 Normal 类型和 DOS 攻击类型具有很好的检测效果；当包含 4 类数据时，其对 Normal 类型、DOS 类型和 Probe 类型的数据都具有较好的检测效果。由于 U2R 和 R2L 类型攻击的训练数据很少，导致训练不足，因此得到的检测结果在 5 种数据类型中的检测率稍低。总体来说，这些实验结果都要优于传统的入侵检测算法的结果[22]。

5.4 传统方法的对比分析

从数据集中随机抽取了 4 组数据进行入侵检测的实验验证，4 组数据所包含的数据信息如表 7 所列。

表 7 4 组数据的抽样结果

Table 7 Four sets of data sampling results

（单位：条）

数据集	训练集			测试集		
	正常	异常	总量	正常	异常	总量
D1	10280	9619	19899	6139	2536	8675
D2	11223	12410	23633	6856	2709	9565
D3	9302	11708	21010	9352	2439	11791
D4	10626	13410	24036	8436	2138	10574

5.4.1 准确率和误报率的对比

本节通过对比目前常用的入侵检测算法（如 KPCA-SVM[23]，BPNN，RNN[24] 和 DBN[25] 等）的准确率（AC）、误报率（FA）和检测速率（训练时间（Tr），测试时间（Te））来验证本文算法的有效性，准确率和误报率的对比结果如图 11、图 12 所示。

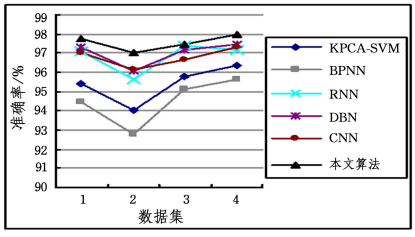

图 11 各分类模型的准确率对比

Fig. 11 Comparison of accuracy rate of each classification model

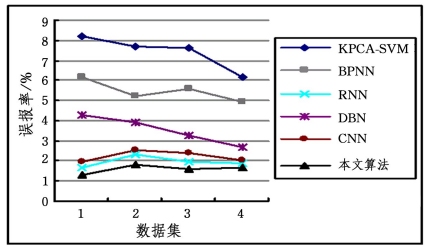

图 12 各分类模型的误报率对比

Fig. 12 Comparison of false positives rate for each classification model

由图 11 和图 12 可知，深度 CNN 模型在准确率和误报率方面都要优于其他常用的入侵检测算法。深度神经网络方法通过卷积层和池化层的特征降维，有效地简化了网络计算复杂度，并在一定程度上可以防止过度拟合的发生；另外，本文通过引入 Relu 激活函数和 Dropout 防止过拟合方法有效地加快了网络收敛速率，从而提高了网络的训练速率和分类准确率。

5.4.2 各种攻击类型准确率的对比

本文在随机抽取的 D4 数据集上针对各类攻击做了进一步的实验验证，通过分析不同分类模型的预测准确率来比较各分类器的有效性。由表 8 可知，本文提出的方法相比于其他 5 类方法在 Normal，DOS 和 Probe 检测中都取得了较高的检测率。6 种分类器对 U2R 和 R2L 的检测准确率都相对较低，但基于深度卷积神经网络的方法比其他几类方法的检测率有较大的提升。

表 8 不同攻击类型的准确率对比

Table 8 Comparison of accuracy rates for different attack types

分类器	AC/%				
	Normal	DOS	Probe	U2R	R2L
KPCA-SVM	98.87	98.59	93.27	26.48	72.12
BPNN	96.23	97.52	91.56	23.21	64.11
RNN	98.78	98.98	93.21	28.53	73.55
DBN	99.01	98.95	94.16	32.51	75.86
CNN	99.03	99.01	94.13	55.31	76.29
本文	99.47	99.13	94.35	64.10	83.21

结束语 在互联网飞速发展的今天，网络数据更为庞大和复杂，传统的入侵检测方法已经不足以应对现今复杂的网络入侵。因此，本文针对当前入侵检测算法在处理复杂的高维数据时易出现检测准确率低、误报率高和检测速率慢的问题，结合深度学习方法在自动提取特征方面的优势，将深度卷积神经网络方法应用到入侵检测中。本文通过将数据预处理之后的数据转换为图像，结合 CNN 对图像有较好的识别率的优势，提出使用深度 CNN 模型对转换后的图像进行识别。本文首先通过对比不同 CNN 模型结构的检测结果，来得到最优的 CNN 模型结构；然后，使用该 CNN 模型结构分别对正常数据和各类入侵数据进行验证实验；最后，将本文方法与 BPNN，RNN 和 DBN 等常用的入侵检测算法进行对比。实验结果表明，CNN 算法适用于高维、复杂的入侵数据，提高了入侵检测的准确率，降低了入侵检测的误报率，并缩短了检测时间。

参 考 文 献

[1] ASHFAQ R A R，WANG X Z，HUANG Z X，et al. Fuzziness

based semi-supervised learning approach forintrusion detection system[J]. Information Sciences，2017，378(C)：484-497.

[2] QING S H，JIANG J C，MA H T，et al. Research on intrusion detection technique：a survey[J]. Journal on Communications，2004，25(7)：19-29. (in Chinese)
卿斯汉，蒋建春，马恒太，等. 入侵检测技术研究综述[J]. 通信学报，2004，25(7)：19-29.

[3] ROY S S，MITTAL D，BASU A，et al. Stock market forecasting using LASSO linear regression model[C]// Afro-European Conference for Industrial Advancement. Cham：Springer，2015：371-381.

[4] BASU A，ROY S S，ABRAHAM A. A Novel Diagnostic Approach Based on SupportVector Machine with Linear Kernel for Classifying the Erythemato-Squamous Disease[C]// International Conference on Computing Communication Controland Automation. New York：IEEE Press，2015：343-347.

[5] ROY S S，VISWANATHAM V M. Classifying Spam Emails Using Artificial Intelligent Techniques[J]. International Journal of Engineering Research in Africa，2016，22：152-161.

[6] TAN B，TAN Y，LI Y. Research on Intrusion Detection System Based on Improved PSO-SVM Algorithm[J]. Chemical Engineering Transaction，2016，51：583-588.

[7] MITTAL D，GAURAV D，ROY S S. An effective hybridized-classifier for breast cancer diagnosis[C]// IEEE International Conference on Advanced Intelligent Mechatronics. New York：IEEE Press，2015：1026-1031.

[8] HINTON G E，SALAKHUTDINOV R R. Reducing the Dimensionality of Data with Neural Networks[J]. Science，2006，313(5786)：504-507.

[9] ROY S S，MALLIK A，GULATI R，et al. A deep learning based artificial neural network approach for intrusion detection[C]// International Conference on Mathematics and Computing. Singapore：Springer，2017：44-53.

[10] YIN C，ZHU Y，FEI J，et al. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks[J]. IEEE Access，2017，5(99)：21954-21961.

[11] ALOM M Z，BONTUPALLI V R，TAHA T M. Intrusion detection using deep belief networks[C]// Aerospace and Electronics Conference. New York：IEEE Press，2016：339-344.

[12] JAVAID A，NIYAZ Q，SUN W，et al. A Deep Learning Approach for Network Intrusion Detection System[C]// Eai International Conference on Bio-Inspired Information and Communications Technologies. Pittsburgh：ICST，2016：21-26.

[13] POTLURI S，DIEDRICH C. Accelerated deep neural networks for enhanced Intrusion Detection System[C]// IEEE，International Conference on Emerging Technologies and Factory Automation. New York：IEEE Press，2016.

[14] YU Y，LONG J，CAI Z. Session-Based Network IntrusionDetection Using a Deep Learning Architecture[M]// Modeling Decisions for Artificial Intelligence. Berlin：Springer Netherlands，2017：144-155.

[15] KWON D，KIM H，KIM J，et al. A survey of deep learning-based network anomaly detection[J]. Cluster Computing，2017(5)：1-13.

[16] WANG M，LI J. Network Intrusion Detection Model Based on Convolutional Neural Network[J]. Journal of Information Security Research，2017，3(11)：990-994. (in Chinese)
王明，李剑. 基于卷积神经网络的网络入侵检测系统[J]. 信息安全研究，2017，3(11)：990-994.

[17] TAVALLAEE M，BAGHERI E，LU W，et al. A detailed analysis of the KDD CUP 99 data set[C]// IEEE International Conference on Computational Intelligence for Security & Defense Applications. New York：IEEE，2009：1-6.

[18] SZARVAS M，YOSHIZAWA A，YAMAMOTO M，et al. Pedestrian detection with convolutional neural networks[C]// Intelligent Vehicles Symposium. New York：IEEE Press，2005：224-229.

[19] KRIZHEVSKY A，SUTSKEVER I，HINTON G E. ImageNet classification with deep convolutional neural networks[C]// International Conference on Neural Information Processing Systems. New York：IEEE Press，2012：1097-1105.

[20] ZHANG Y L，ZHANG Z Q，WU H T，et al. Perimeter intrusion detection method based on improved convolution neural network[J]. Computer Science，2017，44(3)：182-186. (in Chinese)
张永良，张智勤，吴鸿韬，等. 基于改进卷积神经网络的周界入侵检测方法[J]. 计算机科学，2017，44(3)：182-186.

[21] CHEN L，QU H，ZHAO J，et al. Efficient and robust deep learning with Correntropy-induced loss function[J]. Neural Computing & Applications，2016，27(4)：1019-1031.

[22] SADEK R A，SOLIMAN M S，ELSAYED H S. Effective Anomaly Intrusion Detection System based on Neural Network with Indicator Variable and Rough set Reduction[J]. International Journal of Computer Science Issues，2013，10(6)：227-233.

[23] KUANG F，XU W，ZHANG S. A novel hybrid KPCA and SVM with GA model for intrusion detection[J]. Applied Soft Computing Journal，2014，18(C)：178-184.

[24] YIN C，ZHU Y，FEI J，et al. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks[J]. IEEE Access，2017，5(99)：21954-21961.

[25] GAO N，GAO L，HE Y Y. Deep belief nets model oriented to intrusion detection system[J]. Systems Engineering and Electronics，2016，38(9)：2201-2207. (in Chinese)
高妮，高岭，贺毅岳. 面向入侵检测系统的 Deep Belief Nets 模型[J]. 系统工程与电子技术，2016，38(9)：2201-2207.