计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(6):39−46 [doi: 10.15888/j.cnki.csa.007464]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 CNN 和 SVM 的报文入侵检测方法①

徐雪丽, 段　娟, 肖创柏, 张　斌

(北京工业大学 信息学部, 北京 100124)
通讯作者: 徐雪丽, E-mail: 2530838736@qq.com

摘　要: 为了进一步提高网络异常检测的准确率, 本文在对现有入侵检测模型分析的基础上, 提出了一种基于卷积神经网络和支持向量机的网络报文入侵检测方法. 该方法首先将数据预处理成二维矩阵, 为了防止算法模型过拟合, 利用 permutation 函数将数据随机打乱, 然后利用卷积神经网络 CNN 从预处理后的数据中学习有效特征, 最后通过支持向量机 SVM 分类器将得到的向量进行分类处理. 在数据集选择上, 采用网络入侵检测常用的权威数据集—京都大学蜜罐系统数据集, 通过与 GRU-Softmax、GRU-SVM 等现有检测率较高的模型进行实验对比, 该模型在准确率上最高分别提高了 19.39% 和 12.83%, 进一步提升了网络异常检测的准确度. 同时, 本研究所提出方法在训练速度和测试速度上有较大提高.

关键词: 入侵检测; 卷积神经网络; 支持向量机; 文本分类; 深度学习

引用格式: 徐雪丽,段娟,肖创柏,张斌.基于 CNN 和 SVM 的报文入侵检测方法.计算机系统应用,2020,29(6):39–46. http://www.c-s-a.org.cn/1003-3254/7464.html

Network Packet Intrusion Detection Method Based on CNN and SVM

XU Xue-Li, DUAN Juan, XIAO Chuang-Bai, ZHANG Bin

(Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China)

Abstract: In order to further improve the accuracy of network anomaly detection, based on the analysis of existing intrusion detection methods, this study proposes a network packets intrusion detection method based on Convolutional Neural Networks (CNN) and Support Vector Machine (SVM). The method first preprocesses the data into a two-axis matrix. In order to prevent the algorithm model from over-fitting, the permutation function is used to randomly shuffle the data, and then the CNN is used to learn the effective features from the pre-processed data. Finally, this method uses SVM classifier to classify the vectors. In the dataset selection, we use the authoritative dataset commonly used in network intrusion detection—Kyoto University honeypot system dataset. This method proposed in this study is compared with the existing models with high detection rates, such as GRU-Softmax and GRU-SVM. The model has improved the highest accuracy by 19.39% and 12.83% respectively, which further improves the accuracy of network anomaly detection. At the same time, the method has greatly improved the training speed and test speed.

Key words: intrusion detection; Convolutional Neural Networks (CNN); Support Vector Machine (SVM); text classification; deep learning

① 基金项目: 国家自然科学基金 (61501008); 北京市自然科学基金 (4172002, 4172012); 北京市科技计划 (Z171100004717001); 北京市教委科技计划 (KM201910005029)

Foundation item: National Natural Science Foundation of China (61501008); Natural Science Foundation of Beijing Municipality (4172002, 4172012); Science and Technology Program of Beijing Municipality (Z171100004717001); Science and Technology Plan of Beijing Municipal Education Commission (KM201910005029);

收稿时间: 2019-11-21; 修改时间: 2019-12-16; 采用时间: 2019-12-25; csa 在线出版时间: 2020-06-10

1 引言

面对互联网带来的便利, 人们对网络的依赖程度愈来愈高, 互联网技术正在逐步改变人们的生活、工作和学习方式. 作为一种信息传递的载体, 显然网络已经是人们现实生活中必不可少的组成部分. 然而, 我们也面临着越来越多的网络安全威胁问题, 新型特征的网络攻击不断出现, 因此, 网络异常检测已经成为当前互联网安全问题中一个亟待解决的问题[1]. 常用的异常检测方法, 例如防火墙技术和身份验证机制等, 因其防护能力较弱, 也仅能够满足最基础的防护需求. 一旦遭到黑客的破坏性攻击, 普通的防护技术基本不起作用[2], 个人、公司甚至是国家的信息数据将面临着泄露等致命的危险. 近些年, 国内外学者对网络流量异常检测的研究也日益增多, 并且他们的研究方法已经取得了不错的效果, 网络异常检测方法也已经成为安全领域一项重要的研究[3,4], 此类系统的目的是识别已经发生或者正在进行的入侵行为[5].

网络异常检测本质上可以归类为网络数据报文的分类问题, 即正常网络数据报文和异常网络数据报文. 现有的主流文本分类有两种类型: 传统的机器学习分类算法和深度学习分类算法. 前者分类算法主要有 K 最近邻算法[6], Boosting 算法[7], 支持向量机[8], K 均值聚类算法[9], 朴素贝叶斯模型[10], 决策树模型[11]等. 大多数传统的机器学习算法属于浅层学习, 不适合超大批量的高维学习的预测要求, 并不能很好的解决现实网络环境中存在着的复杂入侵数据分类问题, 因此识别数据报文的准确度较低, 误报率较高[5]. 相反, 深度学习算法能够应对高维度特征的复杂数据, 与其它机器学习方法相比, 采用基于深度学习的分类方法能够从网络数据中提取更好的特征, 以创建较好的模型, 在入侵检测方面显著提高了分类的准确性[12]. 事实证明基于深度神经网络的研究方法在异常检测分类问题上较传统机器学习方法有较高的准确率和较低的误报率. 深度学习算法的优势在于它并不依赖于特征工程, 并能够智能有效的识别入侵行为的异常特征[13]. 目前, 深度学习在这一应用的分类算法主要有: 循环神经网络 (Recurrent Neural Network, RNN)[14], 深度神经网络 (Deep Neural Network, DNN)[15], 卷积神经网络 (Convolutional Neural Networks, CNN)[16]. 卷积神经网络 (CNN) 由于其学习高维数据特征的能力显著, 因此得到广泛应用.

2 相关工作

目前, 针对入侵检测问题的方法已有大量的国内外学者开展了相关方面的研究, 近些年, 随着机器学习算法愈来愈受到科研人员的重视, 众多方法被运用于网络流量入侵异常检测领域, 相对于传统的检测机制检测效果有了很大的提升, 是当前公认的有效算法之一.

在无监督学习方面, Wang Q[17]提出了一种新型的异常检测聚类方法 FCC,该方法引入了模糊连通性的概念用来计算不同数据类别的实例之间的相似性,算法不仅可以检测已确定的入侵类型特征,还可以检测它们的变体. Zhang J 等[18]将机器学习中的随机森林算法 RF 运用于网络入侵监测系统上, 检测网络传输流量中的异常值, 并对随机森林的离群值检测算法进行了修改, 降低了算法的计算复杂度, 提高了性能. 但是该算法表明随着网络攻击数量的逐步增加, 其性能表现出下降趋势. Wang ZH 等[19]将基于粒子群的模糊 C 均值的算法模型 FCM 运用到入侵检测监控系统上, 并能够让系统检测出未标识的原始网络流量数据. 该方法能够克服普通入侵异常监测系统较易陷于局部最优问题的缺点和不足. 使得检测的准确率有所提升并且该方法也扩大了适用性. 但该算法的需要耗费较长的时间, 增加了时间成本, 不能保证系统的实时性.

在有监督学习方面, Kim J 等[20]将循环神经网络算法模型 RNN-IDS 应用到入侵检测中,该模型将深度神经网络技术和 ReLU 修正线性单元激活函数相结合, 通过与随机森林、支持向量机等一些常用的机器学习算法完成了对比实验, 验证了该方法在二分类以及多分类中具有较好的检测效果. Dong B 等[21]归纳了普通的机器学习算法在入侵异常检测领域中的效果, 并给出了与深度学习的方法运用于入侵检测问题上的对比实验, 发现深度学习算法模型在准确率和误报率指标上表现的更好, 得出了深度学习技术改变了网络面临着的安全评估挑战的结论. Kwon D 等[22]建立了浅层 CNN, 中层 CNN, 深层 CNN 等 3 种用于异常检测问题的卷积神经网络模型, 并对不同深度所带来的影响作出了评价. 3 个模型在与传统的机器学习分类器的比较上具有较高的检测精度, 但是这些模型在平衡和非平衡数据集的检测精度方面具有差异. Roy SS 等[23]提出了一种运用深度神经网络的入侵异常检测的算法模型, 并与支持向量机 (SVM) 方法在该领域种的应用做了

实验比对, 其结论表明与 SVM 用于网络入侵系统的效果相当, 验证了深度神经网络作为入侵攻击分类器的潜在能力. Yin CL 等在文献[5]提出了一种基于循环神经网络的用于入侵异常监测 (RNN-IDS) 深度学习算法模型. 并研究了该模型在二元分类和多元分类中的性能, 以及所神经元包含的数量和多个不相同的学习速率对训练模型性能产生的影响, 表明了 RNN-IDS 优于传统机器学习算法, 更适合于对分类模型的建模. 但是该模型采用的循环神经网络存在着潜在的梯度消失和爆炸的风险.

当前, 基于深度学习的流量异常检测技术虽然得到众多国内外研究者的青睐, 并表现出来不错的检测效果, 但是还有很多待改进的空间, 目前还面临着以下问题: (1) 保证检测模型较高的准确率和较低的误报率一直以来都是国内外学者研究的重点, 现有的异常检测系统的大多数模型的准确率还有待进一步提高; (2) 大多数异常检测算法模型能够很好的识别训练数据, 然而在测试数据上显现出效果不佳的问题, 普遍存在着模型过拟合的情况; (3) 异常检测系统是实时在线监控数据的系统, 网络数据传输量巨大, 保障检测的实时性是目前在线监测系统需解决的关键性问题, 由于很多深度学习的模型复杂参数过多, 导致训练难度加大, 模型的训练速度变慢的问题, 不能很好的保证实时性, 因此, 提高训练速度至关重要; (4) 在大数据时代下, 计算机技术在持续发展, 网络环境也在不停地产生着改变, 对异常检测算法模型的适用性也会具有更高的要求.

本文针对以上存在的问题提出了一种基于卷积神经网络和支持向量机的网络流量入侵检测方法, 考虑到为了适于卷积神经网络对数据格式的要求, 本研究将每条网络数据报文处理成一个二维矩阵形式. 为了防止大多数网络模型存在的过拟合现象, 本文采用 permutation 将数据索引随机化, 然后将二维数据输入到卷积神经网络中, 从中学习数据的有效特征. 并运用支持向量机分类器做分类处理. 最后, 通过与本文所采用的数据集上其他两个主流模型对比, 验证了本模型有较高的准确率, 更适合处理网络异常检测问题.

3 基于 CNN 和 SVM 的报文入侵检测方法

3.1 数据预处理

本文运用 Google TensorFlow[23]来实现卷积神经网络对数据模型的训练, 本文模型包含了提出的模型和需要对比的两种模型. 在数据集的选择上, 本文使用 2013 年京都大学蜜罐系统的网络流量数据集[24]. 它包含 24 个统计特征, 即来自 1999 年 KDD CUP 数据集的 14 个特征[25], 以及 10 个附加特征. 在此基础之上, 为了适于本文所提出的算法模型 CNN-SVM, 通过以下步骤对数据集进行了处理: (1) 数据处理, 为了与已有的模型作实验对比以及适应本文算法模型, 本文在原有数据集的基础上对特征进行了补充, 但并不对原有数据集产生影响, 然后将数据集中的每条数据处理成一个 5×5 的二维矩阵; (2) 标签处理, 将原有数据集标签 0 处理成[1, –1], 标签 1 处理成[–1, 1]; (3) 数据打乱, 由于数据集固定顺序, 会限制梯度优化方向的可选择性, 导致收敛点选择空间变少, 以至于造成模型的过拟合. 为了防止训练模型过拟合, 在数据训练之前, 对数据集的顺序做随机改变, 从而打乱数据的顺序. 为了不改变原数据集的顺序, 该处理方式选用 permutation 函数来完成.

3.2 CNN-SVM 模型架构

随着愈来愈多的学者深入到深度学习知识层面, 推动着深度学习广泛应用与各个领域. 其中, 卷积神经网络也是深度学习领域的一种非常突出的训练模型的方法, 在图像识别、图像处理、人脸识别、音频检索、EGG 分析等应用[26]中获得了非常不错的效果. Agarap 等[27]提出了一种 GRU-SVM 模型, 并将其应用到入侵检测分类问题中, 取得了较好的效果, 受到该论文的启发, 本文提出了一种 CNN-SVM 处理模型, 利用卷积神经网络训练数据, 并将卷积神经网络的输出作为 SVM 的输入, 模型架构如图 1 所示.

3.3 CNN-SVM 算法原理

为适应本文 CNN-SVM 模型结构, 将数据集进行了预处理, 已经在数据预处理部分进行了介绍, 下面将会对本文算法过程进行详细介绍, 主要分为两大部分: 卷积神经网络的处理和支持向量机的处理.

在卷积神经网络中, 卷积核是最为核心的一个部分, 卷积核设计的好坏关系到数据特征提取效果的优劣, 它是一个需要特殊设计的带权值矩阵, 卷积核将输入数据对应部分作加权和, 通过激活函数的处理产生输出矩阵. 为了让模型学习到更多有效的特征, 并且尽可能的减少时间消耗, 本文模型采用两个卷积层, 同时考虑到本文从数据中提取到的特征数量, 所以本文模

型中第一个卷积层采用 32 个卷积核, 每个卷积核设计为一个 4×4 的二维矩阵. 第二个卷积层采用 16 个卷积核, 卷积核的大小是 2×2, 这样经过预处理后的输入数据, 再经过两个卷积层的卷积处理, 有效的采集了数据的局部特征, 这些特征会按一定形式组合在一起, 并以此作为卷积层部分的输出, 每经过一个卷积层的处理都会跟随一个用于特征处理的池化层, 进一步对数据进行提取, 本文使用的两个池化层卷积核大小均为 2×2. 在经过卷积层和池化层的两次处理后, 利用全连接层对数据进行处理. 另一方面, 考虑到 *ReLU* 激活函数具有较好的性能, 收敛速度快, 减小了梯度消失的可能性, 另一个优点是 *ReLU* 激活函数可以将负值输入转换成零, 如式 (1) 所示, 其中 x 表示输入信号, 因此小于零区域的输入不会将神经元激活, 从而稀疏了网络结构, 使得计算效率较高, 同时在结合本文模型实验过程中, 表现出了很好的性能, 因而使用 *ReLU* 作为了本文的激活函数. 本文模型的 CNN 模型结构参数如表 1 所示.

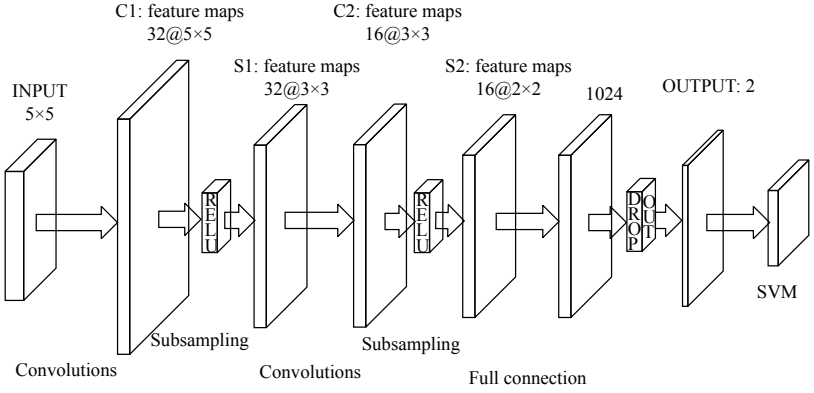

图 1 CNN-SVM 模型结构图

表 1 CNN 模型结构参数

名称	值
输入层	[–1, 5, 5, 1]
卷积层 1	*ksize*=[1, 4, 4, 32], *strides*=[1, 1, 1, 1], *activation=ReLU*
池化层 1	*ksize*=[1, 2, 2, 1], *strides*=[1, 2, 2, 1]
卷积层 2	*ksize*=[32, 2, 2, 16], *strides*=[1, 1, 1, 1], *activation=ReLU*
池化层 2	*ksize*=[1, 2, 2, 16], *strides*=[1, 2, 2, 1]
全连接层	*nodes*=1024, *activation=ReLU*
输出层	*nodes*=2

$$ReLU(x)=\begin{cases}0, & \text{if } x\le 0\\ x, & \text{if } x>0\end{cases} \tag{1}$$

深度学习是一个对输入数据不断迭代学习, 不断优化的过程, 数据在经过 CNN 模型处理后, 需要进行反向传播以便更新权重, 从而达到更好的分类效果. 因为网络异常检测属于典型的二分类问题, 同时支持向量机本质上就是为解决二分类问题而设计的, 所以本文采用了支持向量机 (SVM) 算法计算铰链损失 (hinge loss), 然后使用 Adam 优化函数来改变梯度. 支持向量机通过一定的映射准则把非线性的低维空间中的数据样本映射到高维空间, 在高维空间中构造一个最优的超平面$w\cdot x+b=0$, 其中w为该超平面的法向量, b为偏值. 对于卷积层和全连接层处理后的输出, 使用支持向量机能更好的将其划分为两类.

由于 L2-SVM 算法相比于 L1-SVM 具有更稳定的性能, 因此本文采用了 L2-SVM 算法, 其在一定程度上也降低了过拟合的风险, 数学表达式如式 (2) 所示.

$$\min\frac{1}{n}\|w\|_2^2+C\sum_{i=1}^{n}\max\left(0,1-y'_i(w^{\mathrm{T}}x_i+b)\right)^2 \tag{2}$$

其中, y'是实际标签值, w为该超平面的法向量, b为偏值, n是每批次处理的数据量. 通过设置适合于本文模型的惩罚参数C, 使用 L2-SVM 计算出铰链损失, 最后利用计算出的铰链损失以及设置合理的学习率, 使用 Adam 优化函数来优化网络参数, 这样便达到了更好的训练效果.

总的来说, 本文模型根据网络异常检测的特点, 使用卷积神经网络学习输入数据的有效特征, 最后使用 L2-SVM 算法计算出铰链损失, 从而根据损失来优化网络参数, 得到了更好的分类效果.

4 实验结果与分析

为了验证本文模型 CNN-SVM 的检测效果, 实验在 8 GB 内存、Intel(R) Core(TM)i5-4590 CPU2@3.30 GHz 的计算机上进行. 本文包含 3 个实验, 分别是本文模型 CNN-SVM、传统的入侵检测模型 GRU-Softmax 和 Agarap 等[27]提出的 GRU-SVM 模型, 实验将本文模型与其它两个模型在多方面进行了详细对比.

4.1 评价指标

为了更好的与另外两个模型进行实验对比, 在评价指标中使用了混淆矩阵, 该评价矩阵是 2×2 的情况分析表, 它非常适宜于对二分类运用情况的评价, 以矩阵形式汇总数据集中的真实值的类别和预测值的类别, 然后根据此矩阵进行判断, 模型评估的混淆矩阵如表 2 所示, 横向是预测的值, 纵向是真实的值. 其中, *TP* 代表着真实值属于正类, 预测值属于正类的数量; *TN* 代表着真实值属于负类, 预测值属于负类的数量; *FP* 代表着真实值属于负类, 预测值属于正类的数量; *FN* 代表着真实值属于正类, 预测值属于负类的数量.

表 2 模型评估的混淆矩阵

值	预测正类	预测负类
实际正类	*TP*	*FN*
实际负类	*FP*	*TN*

结合混淆矩阵, 本文对真阳性率、真阴性率、假阳性率以及假阴性率进行实验了对比, 其中, 式 (3) 至式 (6) 表示的是实验结果中的真阳性率, 真阴性率, 假阳性率和假阴性率的计算方法, 名词含义如表 3 所示.

$$TPR = \frac{TP}{TP+FN} \tag{3}$$

$$TNR = \frac{TN}{TN+FP} \tag{4}$$

$$FPR = \frac{FP}{FP+TN} \tag{5}$$

$$FNR = \frac{FN}{FN+TP} \tag{6}$$

另外, 本文实验在准确率、召回率、精准率以及误报率 4 个方面进行了对比, 各性能指标的公式如式 (7) 至式 (10) 所示, 各个公式的释义如表 4 所示.

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

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

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

$$error = \frac{FP+FN}{TP+FN+FP+TN} \tag{10}$$

表 3 名词含义

符号	含义
TPR	真阳性率 (True Positive Rate, *TPR*)
TNR	真阴性率 (True Negative Rate, *TNR*)
FPR	假阳性率 (False Positive Rate, *FPR*)
FNR	假阴性率 (False Negative Rate, *FNR*)

表 4 名词释义

符号	含义
accr	准确率: 表示准确预测的正反例与总数之比
recall	召回率: 表示准确预测的正类数量与实际值属于正类总数之比
precision	精确率: 表示准确预测到的正类数量与预测值属于正类总数之比
error	误报率: 表示错误预测的正反例数与总数之比

4.2 实验结果

为了更加真实、可靠的进行网络模型训练, 实验采用权威数据集—京都大学蜜罐系统的网络流量数据[24]进行实验, 其中, 用于训练模型的数据集和用于测试的数据集的具体分布情况如表 5 所示.

表 5 训练数据集和测试数据集的类别分布情况 (单位: 条)

类别	训练数据集	测试数据集
正常	794 512	157 914
入侵	1103 728	262 694

在进行实验过程中, 会使用到较多预先设定的超参数, CNN-SVM、GRU-Softmax 和 GRU-SVM 这 3 种网络算法模型所采用的超参数如表 6 所示, 其中, 超参数分别是 Batch_Size (每批处理的数据条数)、EPOCHS (训练的轮次数)、LEARNING_RATE (学习率)、CELL_SIZE (隐藏单元的个数)、NUM_CLASS (类别数量)、KEEP_PROB (元素被保留的概率)、SVM_C (惩罚参数).

通过实验, 模型 CNN-SVM、GRU-Softmax 和 GRU-SVM 测试后 *TP*、*TN*、*FP*、*FN* 统计情况分布如表 7 所示.

通过计算 CNN-SVM、GRU-Softmax 和 GRU-SVM 等 3 种网络模型的测试性能: 真阳性率、真阴性率、假阳性率、假阴性率如表 8 所示. 实验表明, 本文模型 CNN-SVM 通过上述 4 个方面参数比较, 误判率较低, 其性能都优于另外两个模型, 从而提高了网络异常检测的准确率.

表 6 3 种模型实验超参数设置

超参数	CNN-SVM	GRU-Softmax	GRU-SVM
Batch_Size	256	256	256
EPOCHS	10	10	10
LEARNING_RATE	1e–6	1e–6	1e–5
CELL_SIZE	1024	256	256
NUM_CLASS	2	2	2
KEEP_PROB	0.35	0.8	0.85
SVM_C	1	—	0.5

表 7 3 种模型测试的 *TP*、*TN*、*FP*、*FN* 数量分布

参数	CNN-SVM	GRU-Softmax	GRU-SVM
TP	253 619	225 258	200 784
TN	144 025	90 841	142 904
FP	9109	37 436	61 910
FN	13 855	67 073	15 010

表 8 3 种模型测试性能

参数	CNN-SVM	GRU-Softmax	GRU-SVM
真阳性率 *TPR*	0.948 20	0.770 56	0.930 44
真阴性率 *TNR*	0.940 52	0.708 16	0.697 73
假阳性率 *FPR*	0.059 48	0.291 84	0.302 27
假阴性率 *FNR*	0.051 80	0.229 44	0.069 56

另外, 实验对 CNN-SVM、GRU-Softmax 和 GRU-SVM 等 3 种网络模型测试数据的准确率、召回率、精准率以及误报率进行了统计, 结果如表 9 所示. 实验统计表明, 虽然 GRU-SVM 的性能相比于 GRU-Softmax 有较大的提升, 但本文模型相较于 GRU-SVM 模型有更大的提升, 从而证明了本文模型的可行性.

表 9 3 种模型在测试集中表现的评价指标的统计数据

参数	CNN-SVM	GRU-Softmax	GRU-SVM
accr	0.945 40	0.751 53	0.817 12
recall	0.948 20	0.770 56	0.930 44
precision	0.965 33	0.857 50	0.764 33
error	0.054 60	0.248 47	0.182 88

3 种模型的训练时间如表 10 所示, 其中本文模型 CNN-SVM 的训练和测试时间都优于其它两个模型. 3 种模型的在训练数据集中的准确率和测试数据集中的准确率如图 2 和图 3 所示, 从示意图中能够看出, 本文模型在训练数据以及测试数据上准确率都高于其它两种模型.

表 10 3 种模型所用的训练时间统计 (单位: s)

模型	训练时间	测试时间
CNN-SVM	685.09	32.86
GRU-Softmax	8933.64	86.89
GRU-SVM	9093.83	75.68

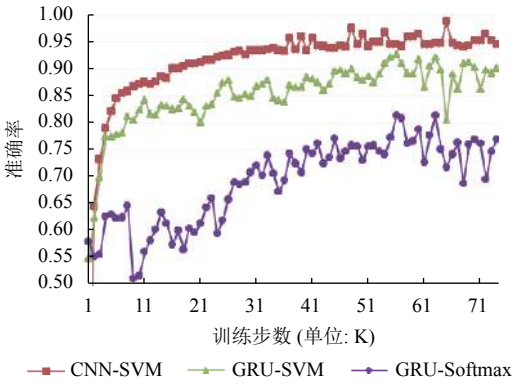

图 2 3 种模型在训练数据集中的准确率对比

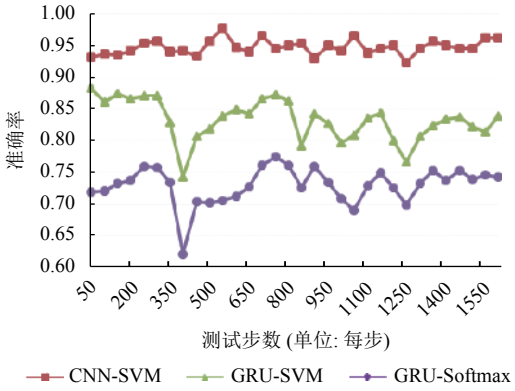

图 3 3 种模型在测试数据集中的准确率对比

3 种模型训练时的损失变化曲线如图 4、图 5 和图 6 所示.

从图 4~图 6 可以发现, GRU-Softmax 模型损失变化波动幅度较大, 相比之下 CNN-SVM 模型和 GRU-SVM 模型损失曲线相对平缓, 但从曲线变化趋势可以看出 CNN-SVM 要优于 GRU-SVM 模型, 因而可以看出本研究所提出的模型在收敛性方面表现最好.

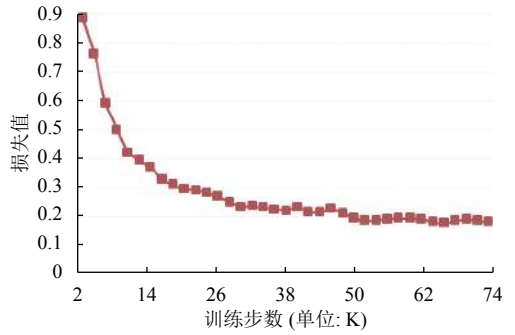

图 4 CNN-SVM 模型训练的损失变化曲线

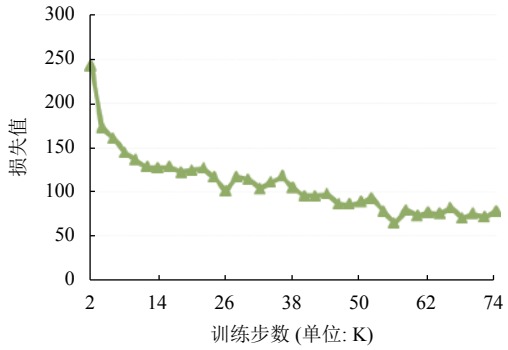

图 5 GRU-SVM 模型训练的损失变化曲线

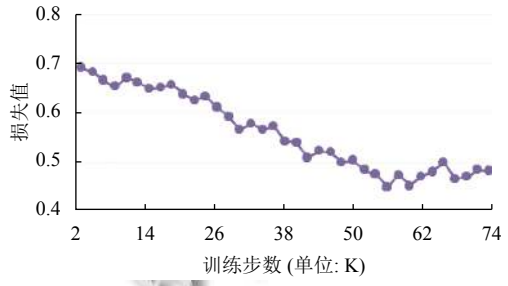

图 6 GRU-Softmax 模型训练的损失变化曲线

5 总结与展望

本文提出了一种新型的网络入侵异常检测方法模型 CNN-SVM, 该模型首先利用卷积神经网络对数据进行处理, 通过多个卷积层和池化层, 学习训练数据中的有效特征, 然后将卷积神经网络的输出作为支持向量机 (SVM) 的输入. 通过与传统模型 GRU-Softmax 和新模型 GRU-SVM 进行实验对比, 本文模型在准确率上分别提高了 19.39% 和 12.83%, 同时误报率较低, 本文模型也大大降低了训练时间和测试时间, 从而验证了本文模型在网络异常检测中具有更好的检测效果. 但是, 本文模型 CNN-SVM 仅在当前数据集上验证了模型的检测效果, 下一步将会把本文模型应用到多种数据集上, 并继续优化模型, 进一步提高检测效果.

参考文献

1 Bukhtoyarov V, Semenkin E. Neural networks ensemble approach for detecting attacks in computer networks. Proceedings of 2012 IEEE Congress on Evolutionary Computation. Brisbane, Australia. 2012. 1–6. [doi: 10.1109/CEC.2012.6252986]

2 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. 计算机科学, 2017, 44(3): 182–186. [doi: 10.11896/j.issn.1002-137X.2017.03.039]

3 Roy DB, Chaki R. State of the art analysis of network traffic anomaly detection. Proceedings of 2014 Applications and Innovations in Mobile Computing. Kolkata, India. 2014. 186–192.

4 Zhao L, Wang F. An efficient entropy-based network anomaly detection method using MIB. Proceedings of 2014 IEEE International Conference on Progress in Informatics and Computing. Shanghai, China. 2014. 428–432.

5 Yin CL, Zhu YF, Fei JL, *et al*. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 2017, 5: 21954–21961. [doi: 10.1109/ACCESS.2017.2762418]

6 Yin YB, Yang WZ, Yang HT, *et al*. Research on short text classification algorithm based on convolutional neural network and KNN. Computer Engineering, 2018, 44(7): 193–198.

7 Bloehdorn S, Hotho A. Boosting for text classification with semantic features. Proceedings of the 6th International Workshop on Knowledge Discovery on the Web, WebKDD 2004. Seattle, WA, USA. 2004. 149–166.

8 Sun AX, Lim EP, Liu Y. On strategies for imbalanced text classification using SVM: A comparative study. Decision Support Systems, 2009, 48(1): 191–201. [doi: 10.1016/j.dss.2009.07.011]

9 Song J, Huang XL, Qin SJ, *et al*. A bi-directional sampling based on K-means method for imbalance text classification. Proceedings of the IEEE/ACIS 15th International Conference on Computer and Information Science. Okayama, Japan. 2016. 1–5. [doi: 10.1109/ICIS.2016.7550920]

10 程岚岚, 何丕廉, 孙越恒. 基于朴素贝叶斯模型的中文关键词提取算法研究. 计算机应用, 2005, 25(12): 2780–2782.

11 Pal M, Mather P M. An assessment of the effectiveness of decision tree methods for land cover classification. Remote Sensing of Environment, 2003, 86(4): 554–565. [doi: 10.1016/S0034-4257(03)00132-9]

12 LeCun Y, Bengio Y, Hinton G. Deep learning. Nature, 2015, 521(7553): 436–444. [doi: 10.1038/nature14539]

13 张玉清, 董颖, 柳彩云, 等. 深度学习应用于网络空间安全的现状、趋势与展望. 计算机研究与发展, 2018, 55(6): 1117–1142. [doi: 10.7544/issn1000-1239.2018.20170649]

14 Al-Subaie M, Zulkernine M. The power of temporal pattern processing in anomaly intrusion detection. Proceedings of 2007 IEEE International Conference on Communications. Glasgow, UK. 2007. 1391–1398. [doi: 10.1109/ICC.2007.234]

15 Kang MJ, Kang JW. Intrusion detection system using deep neural network for in-vehicle network security. PLoS One,

2016, 11(6): e0155781. [doi: 10.1371/journal.pone.0155781]

16 Wu KH, Chen ZG, Li W. A novel intrusion detection model for a massive network using convolutional neural networks. IEEE Access, 2018, 6: 50850–50859. [doi: 10.1109/ACCESS.2018.2868993]

17 Wang Q, Megalooikonomou V. A clustering algorithm for intrusion detection. Proceedings of the SPIE 5812, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005. Orlando, FL, USA. 2005. 31–38.

18 Zhang J, Zulkernine M. Anomaly based network intrusion detection with unsupervised outlier detection. Proceedings of 2006 IEEE International Conference on Communications. Istanbul, Turkey. 2006. 2388–2393.

19 Wang ZH. Unsupervised intrusion detection algorithm based on association amendment. Proceedings of the 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery. Xiamen, China. 2014. 909–913. [doi: 10.1109/FSKD.2014.6980960]

20 Kim J, Shin N, Jo SY, *et al*. Method of intrusion detection using deep neural network. Proceedings of 2017 IEEE International Conference on Big Data and Smart Computing. Jeju, Republic of South Korea. 2017. 313–316. [doi: 10.1109/BIGCOMP.2017.7881684]

21 Dong B, Wang X. Comparison deep learning method to traditional methods using for network intrusion detection. Proceedings of the 2016 8th IEEE International Conference on Communication Software and Networks. Beijing, China. 2016. 581–585.

22 Kwon D, Natarajan K, Suh SC, *et al*. An empirical study on network anomaly detection using convolutional neural networks. Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems. Vienna, Austria. 2018. 1595–1598. [doi: 10.1109/ICDCS.2018.00178]

23 Roy SS, Mallik A, Gulati R, *et al*. A deep learning based artificial neural network approach for intrusion detection. Proceedings of the Third International Conference on Mathematics and Computing. Haldia, India. 2017. 44–53.

24 Song J, Takakura H, Okabe Y. Description of Kyoto University benchmark data. http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf. (2016-03-15).

25 Stolfo SJ, Fan W, Lee W, *et al*. Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection: Results from the JAM project [Technical report]. New York: Columbia University. 2000.

26 周飞燕, 金林鹏, 董军. 卷积神经网络研究综述. 计算机学报, 2017, 40(6): 1229–1251. [doi: 10.11897/SP.J.1016.2017.01229]

27 Agarap AFM. A neural network architecture combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for intrusion detection in network traffic data. Proceedings of the 2018 10th International Conference on Machine Learning and Computing. Macau, China. 2018. 26–30. [doi: 10.1145/3195106.3195117]