DOI:10.13718/j.cnki.xsxb.2021.09.013

大数据环境下基于 CNN 和 WDLSTM 的入侵检测①

李发陵, 彭 娟

重庆工程学院 软件学院, 重庆 400056

摘要: 针对传统网络入侵检测方法由于大数据复杂性、异构性和大规模性而难以有效实现入侵检测的问题, 提出一种基于卷积神经网络和加权丢弃长短期记忆(Convolutional Neural Network and Weight-Dropped Long Short-term Memory, CNN-WDLSTM)的混合深度学习模型, 用于大数据环境下的网络入侵检测. 该模型基于 CNN 利用入侵数据的权重共享特性来发挥其速度优势, 从入侵检测系统大数据中提取有意义的特征, 并使用 WDLSTM 保留提取特征之间的长期相关性, 防止对循环连接的过度拟合, 最后基于试错法对模型的超参数进行优化. 实验结果表明, 该方法在分类精度、误报率和平均执行时间方面具有良好的性能.

关 键 词: 深层卷神经网络; 大数据; 加权丢弃长短期记忆; 入侵检测

中图分类号: TP393 **文献标志码**: A **文章编号**: 1000-5471(2021)09-0103-06

Intrusion Detection Based on CNN and WDLSTM in Big Data Environment

LI Faling, PENG Juan

College of Software, Chongqing Institute of Engineering, Chongqing 400056, China

Abstract: To solve the program that traditional network intrusion detection methods are difficult to effectively implement intrusion detection due to the complexity, heterogeneity and large-scale of big data, a hybrid deep learning model based on convolution neural network and weight-dropped long short-term memory (CNN-WDLSTM) has beenproposed for network intrusion detection in big data environment. In this model,CNN is usedto take advantage of the speed-sharing feature of intrusion data to take advantage of its speed and extract meaningful features from the big data of intrusion detection systems. WDLSTM is usedto preserve the long-term correlation between the extracted features to prevent over-fitting to the cyclic connection. The hyper-parameters of the model are optimized based on trial and error. Experimental results show that the method has good performance in terms of classification accuracy, false positive rate and average execution time.

Key words: deep convoluted neural network; big data; weight-dropped long short-term memory; intrusion detection

① 收稿日期: 2020-01-06
基金项目: 国家自然科学基金项目(61572089); 重庆市教育委员会科学技术研究项目(KJQN201901908).
作者简介: 李发陵, 硕士, 副教授, 主要从事软件工程及大数据存储与分析研究.

社交媒体、移动应用、传感设备和物联网的快速发展导致全球数据量激增，由于它们的数量、种类、速度都很大且准确性高，因此将它们描述为大数据. 大数据网络蕴藏着许多有价值的信息[1-2]，由于大数据不断发展、结构不断变化和网络系统的速度不断提高，入侵的方法也在不断变化和调整，近年来，入侵检测系统(Intrusion Detection Systems，IDS)成为相关学者的重要研究课题[3-4]. 支持向量机、神经网络、隐马尔可夫模型和模糊逻辑等传统机器学习(Machine Learning，ML)方法，由于其较浅的体系结构不适合在大数据环境中处理入侵检测[5]，难以识别未知的攻击和处理大型数据集中常见的噪声，因此需要健壮、有力的ML技术来处理随时间变化而变化的动态入侵.

用于处理大数据的深度学习技术主要有：深度信任网络(Deep Belief Networks，DBN)、卷积神经网络(Convolutional Neural Network，CNN)和长短期记忆(Long Short-Term Memory，LSTM)网络[6]. DBN主要用于模式分析，比其他深度学习技术训练得更快[7]；CNN主要用于图像处理应用程序，具有比DBN更好的判别能力；LSTM网络是一种递归神经网络，可以更好地学习提取特征之间的依赖关系[8]，LSTM的另一个变体是加权丢弃长短记忆(Weight-Dropped Long Short-Trm Memory，WDLSTM)网络，正则化的循环神经网络(RNN)在LSTM的隐藏权重矩阵形成过程中使用了Drop Connect技术，以便保留提取特征之间的长期相关性，并防止对递归连接的过拟合.

文献[9]提出基于深度神经网络模型来检测和分类IDS中无法预见和预测的网络攻击模型，该模型采用具有深度神经网络的分布式深度学习模型来实时处理和分析超大规模数据，但未使用基准IDS数据集对其进行训练. 文献[10]将大数据和深度学习技术相结合以提高大数据平台上IDS的性能，使用深度神经网络、随机森林和梯度增强树以二进制和多类模式攻击对网络流量数据集进行分类. 文献[11]提出基于堆叠自动编码器和最大分类器的两阶段深度学习模型，实现高效的网络入侵检测. 该模型能够从大量未标注的数据中学习有用的特征表示，并对其进行自动有效的分类，具有较高的检测精度和执行效率.

在研究了现有IDS的基础上，为了进一步提高大数据环境下的入侵检测性能，本文提出用于大数据环境下网络入侵检测的基于卷积神经网络和加权丢弃长短期记忆(Convolutional Neural Network and Weight-Dropped Long Short-Term Memory，CNN-WDLSTM)的混合深度学习模型. 该模型使用深度CNN从网络数据流量中提取有意义的特征，利用其权重共享特性的提高速度，使用LSTM网络来保持提取特征之间的长期依赖关系，避免梯度消失问题. 在LSTM中对隐藏到隐藏权重矩阵使用Drop-Connect正则化技术避免过拟合问题，并基于试错法对模型的超参数进行优化，最后采用入侵检测的公共UNSW-NB15数据集对模型进行评估.

1 CNN和LSTM基本理论

1.1 卷神经网络(CNN)

卷积神经网络(Convolutional Neural Network，CNN)是一种将部分滤波器与输入相结合的神经网络[12]. 每个滤波器都是可以训练的权重向量，深度学习前馈网络在卷积层和最大池化层之间互换，顶层为稀疏或完全连接层，最后是最终决策层或分类层，这种深层CNN可以保证平移不变性并处理输入数据中的大小变化. 深度CNN训练通常通过监督学习完成，并且比训练其他类型的人工神经网络(ANN)要快，CNN中少量的权重使其比其他基于神经网络的特征提取方法更有效. 深度CNN用于识别、检测和分类一维、二维和三维数据中的模式或对象. CNN中每个神经元的输出根据其输入和网络结构中先前各层中神经元的权重和偏差来计算[13]. 由于卷积和池化是深度CNN隐藏层中两个不同的操作，因此这些隐藏层被称为卷积层和池化层.

1.2 长短期记忆(LSTM)

长短期记忆(Long Short-Term Memory，LSTM)是一种具有反馈连接的递归神经网络[14]，包括1个存储单元和3个调节器或门(输入门、输出门和忘记门)，用于控制LSTM单元内部的信息流. 存储单元保持输入特征之间的依赖性，输入门将新值输入到存储单元中，忘记门的控制值可以决定输入值是否保留在存储单元中，输出门使用存储单元中的值计算单元的输出，切线函数和S型函数是LSTM单元的常见激活函数.

2　基于 CNN-WDLSTM 的入侵检测

本文 CNN-WDLSTM 模型首先对输入的原始数据集使用数据转换和数据规范两种技术进行数据预处理，然后再对实时数据流量进行入侵分类.

2.1　数据预处理

使用数据转换和数据规范化两种主要技术进行数据预处理. 数据转换通过将流量特征从标称转换为数字来确保所有数据都是数字，供入侵检测模型处理. 数据归一化用于将特征大的方差减少到一定范围的值[15]，并在规范化过程中删除空值. 为了标准化较大的值并减少其影响，本文应用最小－最大缩放方法将值放置在 0～1 之间.

2.2　基于 CNN-WDLSTM 的入侵检测

CNN-WDLSTM 模型结合深度卷积神经网络(CNN)和加权丢弃长短期记忆(WDLSTM)优势对实时数据流量进行入侵分类，可以更有效地检测入侵. 深层的 CNN-WDLSTM 模型包含 2 个一维卷积层、1 个一维最大池化层、1 个一维 WDLSTM 层和 1 个完全连接层.

2.2.1　卷积层

在卷积层中，一组滤波器在输入上滑动生成特征向量，用于训练两个卷积层中训练模型的激活函数是整流线性单元(Rectified Linear Unit，RELU)函数.

2.2.2　最大池化层

在最大池化层中，池化操作(也称为下采样)降低了卷积层的输出维度，从而减少计算成本并避免过拟合. 实践中可以通过两种不同的池化机制来执行该操作：最大或平均.

2.2.3　WDLSTM 层

WDLSTM 是使用 drop-connect 技术进行正则化的 LSTM 神经网络，是 dropout 的一般形式，其中每个连接都以(1～p)概率丢弃，而不是丢弃每个输出单元. drop-connect 在权重 W 上为网络引入动态稀疏性，dropout 在网络单元的激活或输出向量上引入稀疏性.

2.2.4　完全连接层

完全连接层基于 Softmax 激活函数来对入侵进行分类并进行检测，Softmax 激活函数计算 n 个入侵类别的概率分布.

混合模型中最重要的参数是 CNN 滤波器的数量、epochs 的数量、学习率、WDLSTM 隐藏单元的数量、掉线率、批量大小和最大池化长度，所有这些参数都是在训练阶段通过试错法获得的.

3　实验结果与分析

本文所有实验均在配置为 Intel(R) core(TM)i7-4510 CPU @2.0 GHz 和 8 GB RAM 的 64 位windows 10 操作系统上采用 Pyth 3.5.2 进行实验，采用数据集 UNSW-NB15 对本文 CNN-WDLSTM 模型进行评估.

3.1　基准数据流

基准数据集 UNSW-NB15[16]是用于评估 IDS 的最新入侵检测技术之一，它包含超过 100 GB 的实际网络流量，在模拟周期内使用自动攻击生成工具“IXIA Perfect Storm”针对多台服务器实施实时的、当代的、正常的和综合的攻击. 在分析过程中检测到 9 类流量，其中 5%为拒绝服务攻击. 为了生成这些攻击，一个测试平台服务器专门用于发起攻击，而另外两台则产生一个通用的导航流. 该数据集总共包含2 540 044个实例，其中包含类标签在内的 49 列数据，使用 Bro-IDS 和 Argus 工具提取数据集中每个实例的值，并将其分为 5 组：内容特征、基本特征、时间特征、流量特征和其他原始特征. 记录中的空值被删除，产生 2 227 001个实例. 由于正常流量最多，因此机器学习分类器可以轻松地对数据进行过拟合，实现更高的精确度. 本文在使用深度学习表示网络流量后，运用正则化技术来解决过拟合问题.

3.2　评价指标

为了评价本文 CNN-WDLSTM 的性能，采用 4 个最常见的验证指标来评估 CNN-WDLSTM 模型的性

能：准确性(*Acc*)、精确度(*Pre*)、召回率(*Recall*)、误报率(*FAR*)和*F*1-得分(*F*1-*score*).

$$Acc = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

$$Pre = \frac{TP}{TP + FP} \tag{2}$$

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

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

$$F1 - score = 2 \times \frac{Pre \times Recall}{Pre + Recall} \tag{5}$$

式(1)中：*TP*是表示正常样本测试阳性数量的真阳性率，*TN*是表示正常样本测试阴性数量的真阴性率，*FP*是表示异常样本测试阳性数量的假阳性率，*FN*是表示异常样本测试阴性数量的假阴性率. 准确性衡量的是正确分类样本与测试集中所有样本的比率，精确度衡量的是正确分类样本与测试集中*TP*和*FP*总数的比率，召回率衡量的是*TP*样本与*TP*和*FN*样本总数的比率. 精确度和召回率的加权平均值用于计算*F*1-得分.

3.3 结果与比较

本文将实验数据流分为70%用于训练和30%用于测试，训练为模型的超参数选择了一个初始值的粗略范围，随后使用试错法对其进行调整获得最佳结果. 在优化过程中，当epochs设置为50、学习率设置为0.005、WDLSTM输出大小设置为70以及drop-connect比设置为0.1时，可以获得最佳结果. 此外，第1层和第2层卷积滤波器的数量分别设置为32和64，将内核大小设置为3，并将最大池化的长度值设置为2.

图1显示了本文CNN-WDLSTM模型训练阶段的准确性和损失，并使用测试集进行验证. 由图1可以看出，CNN-WDLSTM是稳定且收敛的. 考虑到模型处理数据集中方差的方式，过拟合显然得到了很好的抑制，这为训练和测试提供了更好的准确性.

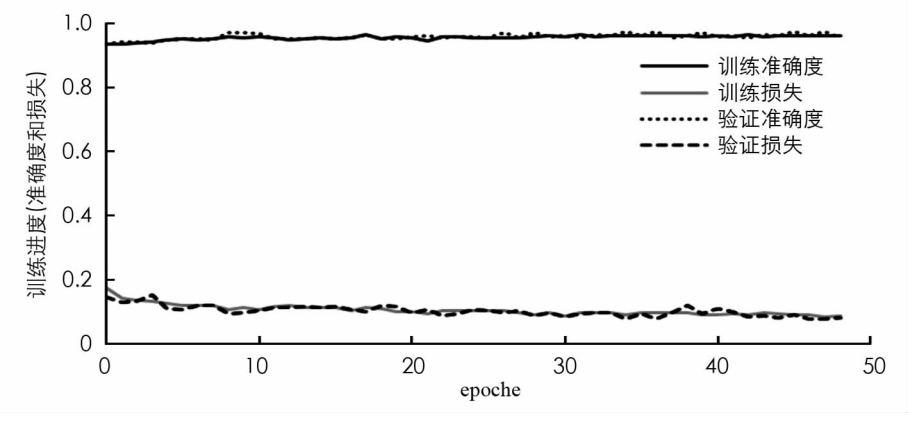

图1 训练阶段的精确度和损失值

表1和表2给出测试集中样本二进制分类和多分类的性能指标. 由表1、表2可以看出，CNN-WDLSTM模型对测试数据样本的二进制分类总体正确率为97.17%，对多分类数据的整体正确率为98.43%. *F*1分数对于Generic,Reconnaissance,Shellcode和Exploits类模型分别在0.99,0.84,0.81和0.71处获得最佳结果，最差的值是由比较少见的类(backdoor,worm和analysis类)实现的. 尽管类分布不平衡，但本文CNN-WDLSTM模型还是取得了非常好的效果.

表1 正常和异常二进制分类的性能指标

类别	精确度	召回率*F*1-得分	准确度	正确率/%
Normal	0.98	0.99	0.98	
Abnormal	0.94	0.82	0.88	97.17
Weighted avg.	0.97	0.97	0.97	

表 2　正常和多分类的性能指标

类别	精确度	召回率 *F*1-得分	准确度	正确率/%
Normal	1	1	1	
Exploits	0.64	0.8	0.71	
DoS	0.32	0.27	0.29	
Backdoor	0.5	0.07	0.12	
Analysis	0.44	0.09	0.15	
Fuzzers	0.71	0.61	0.66	98.43
Generic	1	0.99	0.99	
Reconnaissance	0.93	0.77	0.84	
Shellcode	0.82	0.79	0.81	
Worms	0.5	0.09	0.15	
Weighted avg.	0.98	0.98	0.98	

表 3 给出了本文提出的 CNN-WDLSTM 模型和文献[11]提出的 TSDL 模型进行入侵检测二进制分类的准确性、误报率和平均执行时间.

表 3　CNN-WDLSTM 模型和 TSDL 模型的分类性能

模型	准确性/%	误报率/%	平均执行时间/ms
TSDL[11]	89.13	0.7495	0.003 372
CNN-WDLSTM	97.17	0.5244	0.002 383

由表 3 可以看出，本文 CNN-WDLSTM 模型比 TSDL 模型具有更高的分类准确性、更低的误报率和更少的平均执行时间. 本文 CNN-WDLSTM 模型能够检测新的入侵类型，减轻不平衡的类分布的影响，对于实时入侵检测系统更有效. 这是因为本文算法使用深度 CNN 从 IDS 大数据中提取有意义的特征，并使用 WDLSTM 保留提取的特征间的长期相关性，防止过度拟合. 本文模型较低的平均执行时间和从大量训练特征中学习特征表示的高准确性，使其对于实时入侵检测系统更有效.

4　结　　语

为了提高网络入侵检测性能，本文针对大数据环境提出了基于卷积神经网络和加权丢弃长短期记忆(CNN-WDLSTM)的混合深度学习模型，用于大数据环境下的网络入侵检测. 深度 CNN 利用入侵数据的重量共享特性来发挥其速度优势，从入侵数据中提取有影响力的特征，在训练模型阶段使用 drop-connect 技术随机忽略一些神经元防止过度拟合，使用 WDLSTM 网络学习提取特征之间的相关性解决梯度消失问题，最后基于试错法优化模型的超参数. 实验结果表明，该模型在分类精度、误报率和平均执行时间方面具有良好的性能. 未来的工作是在更复杂和更大的数据集上对深层 CNN-WDLSTM 入侵检测系统进行分析，以获得实时的入侵检测系统.

参考文献：

[1] SIVARAJAH U, KAMAL M M, IRANI Z, et al. Critical Analysis of Big Data Challenges and Analytical Methods [J]. Journal of Business Research, 2017, 70: 263-286.

[2] GÜNTHER W A, REZAZADE MEHRIZI M H, HUYSMAN M, et al. Debating Big Data: a Literature Review on Realizing Value from Big Data [J]. The Journal of Strategic Information Systems, 2017, 26(3): 191-209.

[3] 刘　铭，黄凡玲，傅彦铭，等. 改进的人工蜂群优化支持向量机算法在入侵检测中的应用 [J]. 计算机应用与软件，2017，34(1)：230-235，246.

[4] ABUROMMAN A A, REAZ M B I. A Survey of Intrusion Detection Systems Based on Ensemble and Hybrid Classifiers [J]. Computers & Security, 2017, 65: 135-152.

[5] KABIR E, HU J K, WANG H, et al. A Novel Statistical Technique for Intrusion Detection Systems [J]. Future Generation Computer Systems, 2018, 79: 303-318.

[6] ZHANG Q C, YANG L T, CHEN Z K, et al. A Survey on Deep Learning for Big Data [J]. Information Fusion, 2018, 42: 146-157.

[7] ZHAO L, ZHOU Y H, LU H P, et al. Parallel Computing Method of Deep Belief Networks and Its Application to Traffic Flow Prediction [J]. Knowledge-Based Systems, 2019, 163: 972-987.

[8] FISCHER T, KRAUSS C. Deep Learning with Long Short-Term Memory Networks for Financial Market Predictions [J]. European Journal of Operational Research, 2018, 270(2): 654-669.

[9] VINAYAKUMAR R, ALAZAB M, SOMAN K P, et al. Deep Learning Approach for Intelligent Intrusion Detection System [J]. IEEE Access, 2019, 7: 41525-41550.

[10] FAKER O, DOGDU E. Intrusion Detection Using Big Data and Deep Learning Techniques [C]//Proceedings of the 2019 ACM Southeast Conference on ZZZ - ACM SE'19. New York: ACM Press, 2019.

[11] KHAN F A, GUMAEI A, DERHAB A, et al. A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection [J]. IEEE Access, 2019, 7: 30373-30385.

[12] DERHAB A, GUERROUMI M, GUMAEI A, et al. Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security [J]. Sensors (Basel, Switzerland), 2019, 19(14): E3119.

[13] CHEN H M, ENGKVIST O, WANG Y H, et al. The Rise of Deep Learning in Drug Discovery [J]. Drug Discovery Today, 2018, 23(6): 1241-1250.

[14] ZHANG C, SUN G Y, FANG Z M, et al. Caffeine: Toward Uniformed Representation and Acceleration for Deep Convolutional Neural Networks [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38(11): 2072-2085.

[15] GAO C, YAN J K, ZHOU S H, et al. Long Short-Term Memory-Based Deep Recurrent Neural Networks for Target Tracking [J]. Information Sciences, 2019, 502: 279-296.

[16] MOUSTAFA N, SLAY J. The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set [J]. Information Security Journal: A Global Perspective, 2016, 25(1/3): 18-31.

责任编辑 夏 娟