计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400227

基于时间因子和复合CNN结构的网络安全态势评估

赵冬梅[1,2]　宋会倩[1]　张红斌[3]
1 河北师范大学计算机与网络空间安全学院　石家庄 050024
2 河北师范大学河北省网络与信息安全重点实验室　石家庄 050024
3 河北科技大学信息科学与工程学院　石家庄 050018

摘　要　为了解决传统的网络安全态势感知研究方法在网络信息复杂情况下准确率不高等缺陷,文中结合深度学习,提出了一种基于时间因子和复合CNN结构的网络安全态势评估模型,将卷积分解技术和深度可分离技术相结合,形成4层串联复合最优单元结构;将一维网络数据转换为二维矩阵,以灰度值的形式载入神经网络模型,从而有效发挥卷积神经网络的优势。为充分利用数据间的时序关系,引入时间因子形成融合数据,使网络同时学习具备时序关系的原始数据和融合数据,增强模型的特征提取能力,同时利用时间因子和点卷积建立时序数据的空间映射,提高模型结构的完整性。实验结果证明,所提模型在两个数据集上的准确率分别达到了92.89%和92.60%,相比随机森林和LSTM算法提升了2%～6%。

关键词:态势感知;卷积网络;时间因子;深度可分离卷积;卷积分解
中图法分类号　TP393

Network Security Situation Based on Time Factor and Composite CNN Structure

ZHAO Dong-mei[1,2],SONG Hui-qian[1] and ZHANG Hong-bin[3]
1 College of Computer and Cyber Security,Hebei Normal University,Shijiazhuang 050024,China
2 Hebei Key Laboratory of Network and Information Security,Hebei Normal University,Shijiazhuang 050024,China
3 School of Information Science and Engineering,Hebei University of Science and Technology,Shijiazhuang 050018,China

Abstract　In order to solve the problem of low accuracy of traditional network security situation awareness research methods in the case of complex network information,combined with deep learning,this paper proposes a network security situation assessment model based on time factor and composite CNN structure,which combines volume integral solution technology and deep separable technology to form a four layer series composite optimal unit structure. The one-dimensional network data are transformed into two-dimensional matrix and loaded into the neural network model in the form of gray value,so as to give full play to the advantages of convolution neural network. In order to make full use of the time-series relationship between data,time factor is introduced to form fusion data,which makes the network to learn the original data and fusion data with time-series relationship at the same time,the feature extraction ability of the model is increased,the spatial mapping of time-series data is established by using time factor and point convolution,and the integrity of the model structure is increased. Experimental results show that the accuracy of the proposed model on two datasets is 92.89% and 92.60% respectively,which is 2%～6% higher than random forest and LSTM algorithm.

Keywords　Situational awareness,CNN,Time factor,Depthwise separable convolution,Convolution decomposition

1　引言

随着云计算、5G、物联网和人工智能等技术的高速发展,我们对网络的依赖越来越大,而构建高效的网络安全态势感知(Network Security Situation Awareness,NSSA)系统是维护网络安全的重要保障。

态势感知最早来源于美国军方在军事对抗中的研究,Endsley首次提出态势感知的概念,并用3层模型描述态势感知[1]。Bass于1999年将态势感知引入网络安全研究中[2]。近年来,Liu等提出了认知意识-控制模型[3],这表明我们对网

到稿日期:2021-04-21　返修日期:2021-09-05
基金项目:国家自然科学基金(61672206);中央引导地方科技发展资金项目(216Z0701G);河北省重点研发计划基金资助项目(20310701D);河北省自然科学基金(F2019205163)
This work was supported by the National Natural Science Foundation of China(61672206),Central Guide Local Science and Technology Development Fund Project(216Z0701G), Key Research and Development Program of Hebei Province(20310701D) and Natural Science Foundation of Hebei Province(F2019205163).
通信作者:赵冬梅(zhaodongmei666@126.com)

络安全态势感知的研究越来越深入。

国内外学者对网络安全态势感知的研究主要集中在数学模型、规则推理和概率统计等方面。由于网络态势的多源异构和不确定性，Zheng 提出了基于证据理论的态势评估办法[4]，该模型从安全设备的多个数据源收集、处理和评估攻击事件信息，不需要大量先验知识，但是推理过程的计算复杂度较高。Sun 将粒子群和支持向量机相结合，用于网络安全态势感知，提出了一种改进的 PSO-SVM 算法[5]，有效地提高了网络态势预测精度，但是在数据样本较大时无法进行准确分类。Lin 等提出了一种 PCA 和随机森林分类的入侵检测方法[6]，通过主成分分析法对数据进行处理后再进行训练，但是在训练过程需要较长的时间和较大的空间。Shen 等针对云环境网络安全态势预测在准确率和实时性方面的局限性，提出了基于灰色神经网络的云环境下的网络安全态势预测方法[7]，通过分类和融合技术构建了感知指标，但是该方法对网络的安全性和适应性提出了新的挑战。Liu 等将博弈论与态势感知相结合，建立了网络安全博弈模型[8]，但是该方法在评估指标及收益函数量化方面未建立统一的标准。在最新的研究中，针对大数据环境下网络攻击的复杂性和隐秘性的特点，Alaoui 等提出了大数据环境下的网络安全态势保护策略[9]，该策略能快速发现网络中的潜在攻击，进而指导网络管理者及时进行干预。Wang 等为了实现对网络攻击的实时监测，将模糊微分方程引入态势感知中，利用线性方程的泰勒级数展开法得到误差估计，描述了攻击监测过程并实现了对网络状况的定量分析[10]。为了提高网络恶意节点的检测准确性，Do 等和 Subramanian 等都将博弈论应用于态势感知领域，前者将网络安全应用场景分为安全和博弈两个类别，通过对物理安全、通信安全和隐私安全进行分析，提供了一种利用博弈论解决网络安全问题的思路[11-12]。后者通过构建无限重复博弈的方法来检测恶意节点[12]，从整体上提高了网络感知准确性。

近年来，随着网络环境越来越复杂，网络数据包含的信息也越来越多，网络数据样本量也日趋增大，这给传统的态势感知研究方法带来了巨大的挑战。学者们也不断探索出了新的态势感知研究思路，随着深度学习和神经网络的出现，该问题得以解决。

Zhao 等提出了一种基于小波神经网络和粒子群优化算法的态势感知方法，该方法采用基于粒子群算法的技术对小波神经网络的参数进行训练[13]，从而加快了网络收敛速度并提高了态势感知的拟合效果。Li 等将 LSTM 神经网络引入态势感知研究中[14]，提出了交叉熵和线性整理函数改进的 3 层 LSTM 深度学习结构，其模型准确率取得了一定的提升。Chen 等针对无线网络入侵检测中的过拟合缺陷，在 RNN 的基础上提出了基于窗口的算法以达到精简数据集的目的，进而提升分类的综合性能[15]。Chen 等将径向基函数(RBF)神经网络应用到态势感知研究中，利用混合递阶遗传算法进行参数寻优，结合退火算法来增加遗传算法的全局搜索能力[16]。卷积神经网络(Convolutional Neural Network，CNN)在深度学习中发挥着重要作用，目前国内外学者对卷积神经网络的研究主要集中在图片处理、情感分析、面部识别等领域。Demir 等将卷积神经网络同医疗相结合[17]，通过傅里叶变换将声音信号转换为图片信号，实现对人肺部疾病的分类。虽然国内外学者对卷积神经网络应用的研究越来越多，但是对网络安全态势感知的研究较少，因此本文的研究具有一定的创新性。

2 卷积神经网络

2.1 标准卷积神经网络

卷积神经网络通常包含输入层、隐藏层和输出层，其基本结构如图 1 所示。

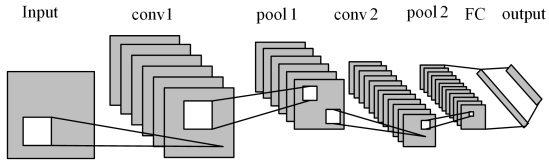

图 1 卷积神经网络的基本结构

Fig. 1 Basic structure of convolutional neural network

输入层可以处理一维和多维数据，本文主要采用 CNN 处理多维数据。本文将网络安全态势的属性值作为像素点，将一条完整的态势信息转换为一个矩阵并输入卷积神经网络。

隐藏层一般包含卷积层、池化层和全连接层，卷积层主要用于特征提取，包含多个卷积核；池化层主要用于对输出特征图进行信息过滤；全连接层主要是对提取的特征进行非线性组合并输出至输出层。

输出层通常为 Softmax 层，针对分类问题，Softmax 层可以得到输入样本属于不同类别的概率分布情况。

相比常见的神经网络，卷积神经网络直接对二维图像进行处理，特征提取过程相对简单，通过非线性组合从原始图像中提取抽象特征，不需要过多的人工参数调整即可从大量样本中学习到特征。其独特的下采样、局部感知和权值共享大大减少了网络参数，保留了网络的重要信息，减少了网络运行的时间和内存消耗。

标准卷积神经网络的操作如图 2 所示，神经网络的输入尺寸为 $H_1\times W_1\times C_1$，卷积核尺寸为 $M\times N$，输出特征图的尺寸为 $H_2\times W_2\times C_2$，则标准卷积层的参数量为：

$$P=M\times N\times C_1\times C_2 \tag{1}$$

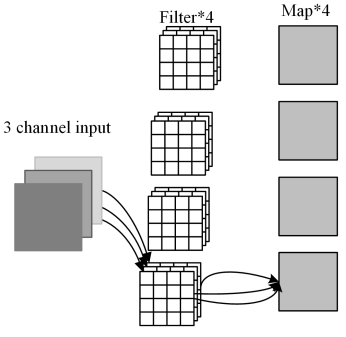

图 2 标准卷积神经网络卷积层示意图

Fig. 2 Convolution layer of standard convolutional neural network

2.2 卷积分解

卷积分解是将卷积分步骤在不同的方向进行卷积后再进行组合，卷积分解实质是对卷积核进行拆分，如图 3 所示。在进行卷积分解时可将其分解为 3 个方向，即通道方向、X 方向和 Y 方向，也可在部分方向上进行分解，本文主要在 X 和 Y 两个方向上进行分解，这种分解方法使网络具有更好的表达效果。卷积分解会降低网络的计算量并减少其参数量，同时会加深网络的深度，从而增强其非线性扩展模型的表达能力。

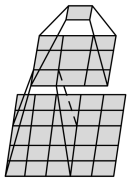

图 3 经典原理图

Fig. 3 Classic schematic diagram

对于输入尺寸为 $H_1\times W_1\times C_1$、卷积核大小为 $M\times N$、输出特征图尺寸为 $H_2\times W_2\times C_2$ 的网络来说，将卷积核在 X 和 Y 两个方向上分解为 $1\times M$ 和 $N\times 1$ 两个卷积核后，参数量分别为：

$$P_M=1\times M\times C_1\times C_2 \tag{2}$$

$$P_N=N\times 1\times C_1\times C_2 \tag{3}$$

即总的参数量为：

$$P_{S1}=(M+N)\times C_1\times C_2 \tag{4}$$

则标准卷积神经网络与分解卷积神经网络的参数对比为：

$$\frac{P}{P_{S1}}=\frac{M\times N\times C_1\times C_2}{(M+N)\times C_1\times C_2}=\frac{M\times N}{M+N} \tag{5}$$

相比标准卷积神经网络，卷积分解技术降低了网络参数，但是在输入特征和卷积输入输出通道数较大时，卷积分解技术对网络的表达能力没有明显提升。

2.3 深度可分离卷积

深度可分离卷积(Depthwise Separable Convolution)是将卷积分两步进行操作，将卷积通道相关和空间通道相关进行分离。深度可分离卷积不仅降低了计算复杂度，还减少了模型的参数量，并且不会对模型精度造成太大影响。对于输入尺寸为 $H_1\times W_1\times C_1$、卷积核大小为 $M\times N$、输出特征图尺寸为 $H_2\times W_2\times C_2$ 的网络来说，具体需要进行如下两步操作。

首先是在深度方向进行卷积，卷积核作用在所有的输入通道上，此时卷积核的通道数和特征图的输入通道数保持一致，即 C_1，以保证每个 channel 都有对应的 filter 进行卷积，卷积核的尺寸决定了最终的输出特征图大小，如图 4 所示(以输入 3 通道为例)。

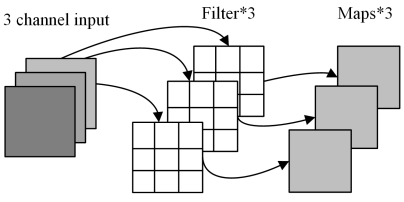

图 4 深度卷积示意图

Fig. 4 Depthwise convolution diagram

其次是点卷积，将 Depthwise 输出得到的卷积再做卷积。该步骤是为了建立同一位置不同通道之间的数据联系，其卷积核的输出通道和特征图最终的输出通道保持一致。如图 5 所示(以输出 4 通道为例)。

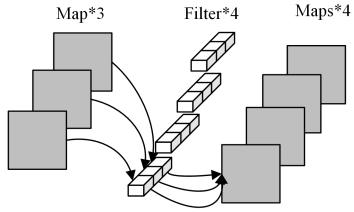

图 5 点卷积示意图

Fig. 5 Pointwise convolution diagram

对于深度可分离卷积网络，上述两步骤涉及的参数分别为：

$$P_D=C_1\times M\times N \tag{6}$$

$$P_P=C_1\times 1\times 1\times C_2 \tag{7}$$

即总的参数量为：

$$P_{S2}=(M\times N+C_2)\times C_1 \tag{8}$$

标准卷积神经网络与深度可分离卷积神经网络的参数对比为：

$$\frac{P}{P_{S2}}=\frac{M\times N\times C_1\times C_2}{(M\times N+C_2)\times C_1}=\frac{M\times N\times C_2}{M\times N+C_2} \tag{9}$$

相比标准神经网络的参数，深度可分离卷积在实现网络表达效果的前提下，大大减少了网络的参数量，在一定程度上加快了网络的训练速度，但是卷积核尺寸较大时，其参数量明显多于卷积分解神经网络。

3 基于时间因子和复合 CNN 的理解评估

3.1 复合结构单元

本文结合卷积分解技术和深度可分离技术的优势，提出了一种复合串联结构单元。首先将输入特征图利用卷积分解技术进行卷积，将输出的特征图重新载入深度可分离网络的第二阶段，即进行点卷积，最后结合下采样，复合串联结构单元如图 6 所示。

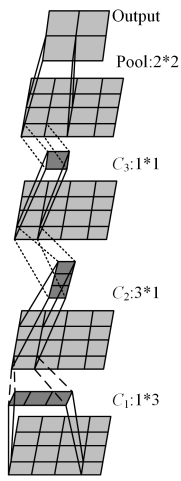

图 6 复合串联结构单元

Fig. 6 Composite series structure unit

本文提出的结构单元包含 4 层机构，其中前三层为卷积

网络，第四层为池化层。第一层卷积核大小为 $1\times M$，通道数根据网络效果进行调整；第二层卷积核大小为 $N\times 1$，通道数需和第一层保持一致；第三层卷积核大小为 1×1，通道数和输出通道数保持一致；第四层为池化层，在本文实际训练中采用最大池化，并将 2×2 池化和 1×1 池化交叉使用，以保证在充分提取网络特征的前提下最大化地降低网络参数，缩短模型的训练时间，减少内存消耗。

本文用相同尺寸的卷积核将数据分别载入标准卷积神经网络、卷积分解神经网络、深度可分离卷积网络和本文提出的复合串联结构单元，结果如表 1 所列。本文提出的复合串联结构单元具有好的特征提取能力，且模型训练运行时间较短。

表 1 不同卷积结构的准确率对比

Table 1 Comparison of accuracy of different convolution structures

Structure Type	Convolution Kernel	Accuracy/%
Standard convolution	3 * 3	91.02
Decomposition convolution	1 * 3-3 * 1	91.48
Depthwise separable convolution	3 * 3-1 * 1	90.41
Composite convolution	1 * 3-3 * 1-1 * 1	92.89

其准确率的直观展示如图 7 所示。

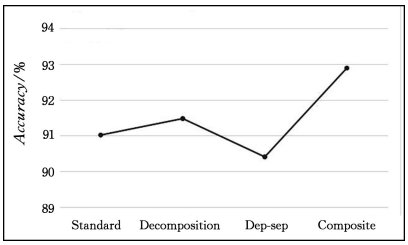

图 7 不同卷积神经网络结构准确率的对比

Fig. 7 Comparison of accuracy of different CNN structures

3.2 时间序列

传统的网络安全态势理解评估仅仅是对当下的网络状态进行分析，没有充分考虑到网络攻击前的网络状态，本文将时间序列引入态势理解评估中，将攻击时的网络状态和攻击前的网络状态进行融合，充分挖掘了网络时序状态联系。在进行态势理解评估时，每条融合信息会包含更多的网络状态信息，有利于更充分地对网络状态进行评估，通过调整时间因子(Timer)来控制网络状态的融合程度，Timer 值选择流程如图 8 所示。

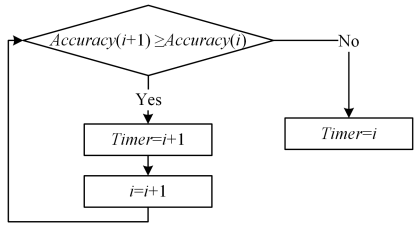

图 8 Timer 值选择流程图

Fig. 8 Timer value selection flow chart

针对卷积神经网络，设置不同的时间因子表现为卷积输入的维度不同，本文提出的时间序列使卷积神经网络输入的特征图为 $N(N\geqslant 3)$ 通道。对于 N 通道卷积的各通道来说，会在每个通道进行单独的二维卷积，再将各个通道对应位置的卷积输出进行加和，得到的结果即为该层卷积的输出。

3.3 激活函数

不添加激活函数的神经网络，即感知机，无论结构是否复杂，都只能输入现象函数，输出结果均是输入的线性组合，激活函数的出现增加了网络的非线性特征，有利于模型学习更加复杂的函数。常用的激活函数有 Sigmoid，Tanh，Relu，Relu6，Leaky-Relu，这 5 种函数的图像如图 9 所示。

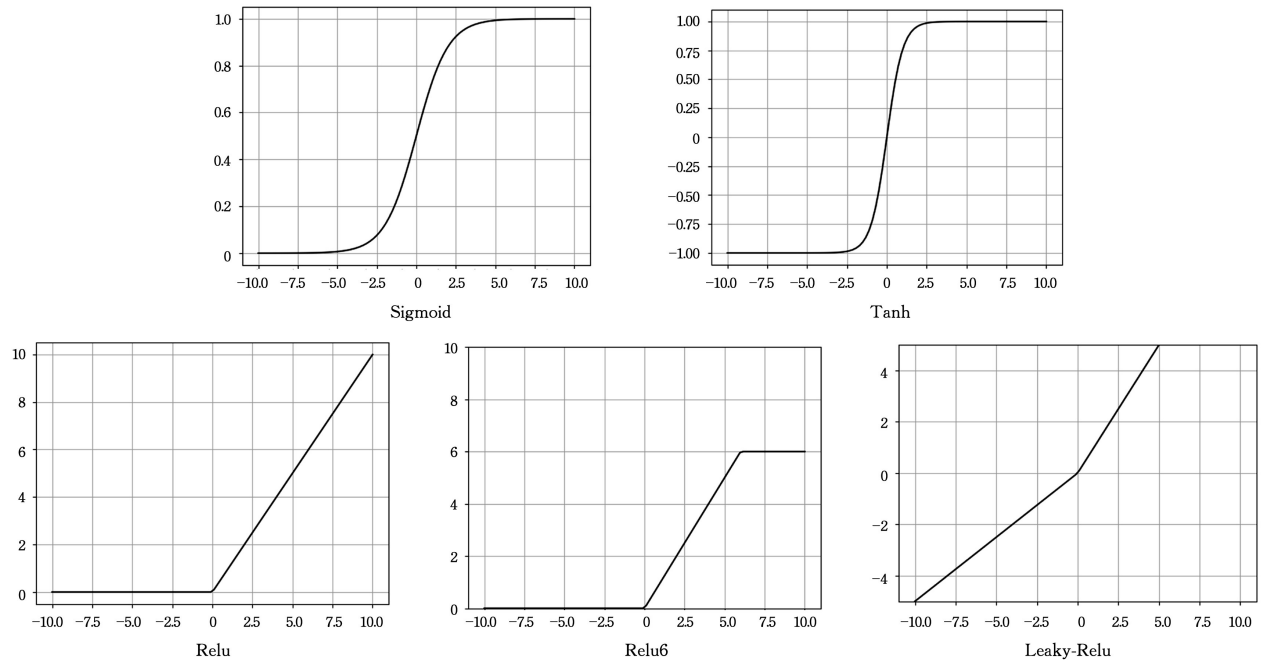

图 9 激活函数图像

Fig. 9 Activation function image

分别采用 5 种激活函数在相同的卷积框架和参数设置下进行对比实验，由表 2 可知，Relu6 函数表现出了更好的学习效果，因此在本实验中采用激活函数 Relu6 可得到最理想的结果。

表 2 激活函数对模型时间及准确率的影响

Table 2 Influence of activation function on model time and accuracy

Function type	Accuracy/%	Train time/s	Test time/s
Tanh	90.46	155.98	71.35
Sigmoid	73.90	152.99	70.60
Relu	83.56	232.88	66.01
Relu6	92.89	151.31	69.87
Leaky-Relu	92.18	210.694	94.83

3.4 不平衡数据的调整

在常见数据集中，网络安全态势感知主要有 5 种状态，即 Normal，Dos，Probing，R2L 和 U2R。其中，Dos 攻击的数量远大于 Probing 和 R2L 两种攻击的数量，更是 U2R 的千余倍。在卷积神经网络中，输入样本越多，模型越能表现出更好的效果，但是不平衡数据的出现使得模型并不能达到理想的学习结果。

针对上述问题，本文采用欠采样和过采样这两个步骤来解决。

(1)Dos 数据的欠采样，即丢失部分 Dos 数据。

(2)Probing，R2L 和 U2R 数据的过采样，即增加 Probing，R2L 和 U2R 数据的比重。

3.5 态势感知框架

基于本文提出的 DDST-CNN(Decomposition & Depth Separable & Timer-Convolution Neural Network)的网络安全态势感知的全流程主要分为以下 5 个步骤：

步骤 1 数据预处理，此时主要包含数据清洗、类型转换、独热编码和数据维度调整，最终使数据满足模型的要求。

步骤 2 将模型载入 DDST-CNN 模型中，此时需要将数据转换为二维矩阵，通过调整 Timer 值设定数据的融合程度，并确定模型的输入通道，结合 Timer 值将二维数据转换为多维数据，随后载入复合结构单元，在结构单元中将数据载入卷积分解技术，以上两层卷积需保持通道数相同。而后将特征图载入深度可分离卷积的第二阶段，调整输入输出通道，增加网络的非线性能力。随后为池化层，池化大小为 2×2。本文在基于 DDST-CNN 的网络安全态势感知研究中，结合数据特点，串联 3 组 DDST-CNN 模块，在第二个和第三个模块中池化层的大小分别为 1×1 和 2×2。

步骤 3 Flatten 层，该层的目的是将特征图的多维数据进行降维处理，即将其转换为一维数据，以便将输出数据过渡到全连接层，本文在实际应用中将输出数量设置为 1 024。

步骤 4 全连接层，该层的目的是调整输出的数量，在该层中将网络学习到的分布式网络特征映射到样本数据空间。本文提出的模型中串联两个全连接层，目的是增加网络的非线性能力，有效拟合数据分布。

以上层的目的是将 Flatten 层输出的一维数据转换为符合输入数据攻击类别的一维数据。

步骤 5 Softmax 层，该层的实质为分类器，其作用是将态势理解与评估以及预测的网络标签值映射到(0，1)范围内，其值表示模型判别输入数据属于输出各个类别的概率，其中最大值为我们需要的标签，即为模型判别出的网络攻击类型。基于 DDST-CNN 的网络安全态势感知流程如图 10 所示。

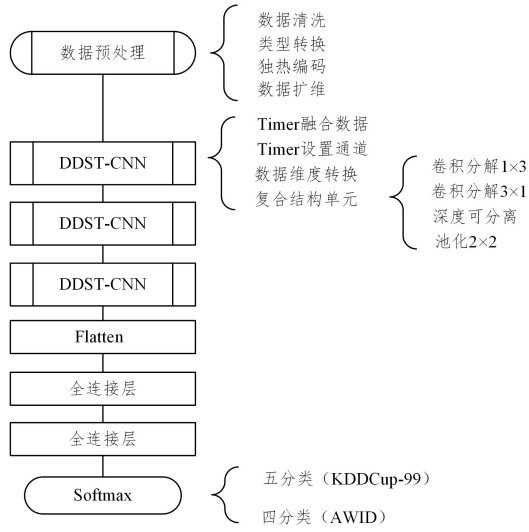

图 10 基于 DDST-CNN 的网络安全态势感知流程

Fig. 10 Network security situation awareness process based on DDST-CNN

4 仿真实验

本文实验中采取的软件环境为 Tensorflow-CPU V-1.9.0，采用的数据集为 KDDCup-99 和 AWID，分别代表无线网络环境和有线网络环境。KDDCup-99 数据集采集了连续 9 周的实验室网络状态。AWID 数据集是 Kolias 等在无线网络的基础上研发的数据集。在软件操作中，通过 Python 语言搭建基础算法，在算法设计中建立串联模型，通过算法接口载入数据集使模型进行自主建立和优化。

4.1 实验 1：KDDCup-99 数据集上的态势理解评估

4.1.1 数据预处理

本实验采用经典的 KDDCup-99 数据集，该数据集是模拟美国空军局域网上采集的连续数据，包含 1 个类标识和 41 个特征属性，其中包含 9 个离散型属性特征和 32 个连续性属性特征。本实验对数据集的处理主要包含符号型特征转换、独热编码和数据维度扩充。

(1)符号型特征转换

在 KDDCup-99 数据集中，需要将原数据集中的 3 种协议类型(Protocol_type)、70 种服务类型(Service)、11 种网络连接状态(Flag)以及五大类标签(Label)由符号型数据转换为数字标识，对应的数字标识如表 3 所列。

表 3 符号型特征转换对照

Table 3 Comparison of symbolic feature transformation

名称	类型	数据标识
Protocol_type	tcp,udp,icmp	0,1,2
Service	aol,auth,bgp,courier,csnet_ns,ctf,daytime,discard,domain,domain_u,echo,eco_i,ecr_i,efs,exec,finger,ftp,ftp_data,gopher,harvest,hostnames,http,http_2784,http_443,http_8001,imap4,IRC,iso_tsap,klogin,kshell,ldap,link,login,mtp,name,netbios_dgm,netbios_ns,netbios_ssn,netstat,nnsp,nntp,ntp_u,other,pm_dump,pop_2,pop_3,printer,private,red_i,remote_job,rje,shell,smtp,sql_net,ssh,sunrpc,supdup,systat,telnet,tftp_u,tim_i,time,urh_i,urp_i,uucp,uucp_path,vmnet,whois,x11,Z39_50	0,1,2,…,69
Flag	OTH,REJ,RSTO,RSTOS0,RSTR,S0,S1,S2,S3,SF,SH	0,1,2,…,10
Label	Normal	0
	Probing:ipsweep.,nmap.,portsweep.,satan.	1
	U2R: buffer-overflow.,loadmodule.,perl.,rootkit.	2
	R2L:ftp_write.,guess_passwd.,imap.,multihop.,phf.,spy.,warezclient.,warezmaster.	3
	Dos: back.,land.,neptune.,pod.,smurf.,teardrop.	4

(2)独热编码

卷积神经网络输出的数据特征类型为矩阵,对于原 41 维数据来说,转换为矩阵后数据特征图的尺寸较小,不利于深层卷积神经网络的特征提取,在进行池化时损失原始信息较多,对最终模型的训练有较大影响。为保证充分利用数据集的信息,并适配深层卷积网络,本文采用独热编码(One-Hot,OH),使用 K 位寄存器对 K 个不同的状态进行编码,原数据集索引对应的数据维度如表 4 所列。

表 4 属性特征维度转换对照

Table 4 Comparison of attribute feature dimension transformation

属性特征	原数据索引	OH 后的数据维度
Protocol_type	1	3
Service	2	70
Flag	3	11
Land	6	2
Logged_in	11	2
Root_shell	13	2
Su_attempted	14	2
Num_outbound_cmds	20	2
Is_hot_login	21	2
Label	41	5

(3)数据扩维

在原数据集进行独热编码后,数据属性特征维度由 41 维变为 128 维,标签维度由 1 维变成 5 维。对于卷积神经网络,为了方便对卷积核进行操作,通常我们希望输入网络的特征矩阵尽量为方阵,即矩阵尺寸为 $N\times N$,为此,我们将独热编码后的属性特征进行维度扩充,具体实现方法为在第 128 维后补充 16 维"0",使属性特征拓宽为 144 维,载入卷积神经网络时转换为 12×12 的特征图。

4.1.2 对比实验和分析

使用本文提出的网络模型,通过调整 Timer 设置对比实验,记录模型的评估时间,以准确率为评价指标,结果如表 5 所列。

表 5 Timer 值与模型评估时间及准确率对照

Table 5 Comparison of Timer value with model evaluation time and accuracy

Number	Timer	Time/s	Accuracy/%
1	3	88.07	90.60
2	4	90.42	90.65
3	5	90.13	90.70
4	6	90.54	90.58
5	7	92.33	90.82
6	8	92.61	92.89
7	9	94.48	92.09
8	10	94.03	90.75

由上述 8 组实验可得,随着 Timer 值的增大,模型评估时间会逐渐延长,模型准确率会先提高后降低,主要原因是第一阶段随着 Timer 值的增大,输入网络的特征图包含较多的网络数据,神经网络可以学习到更多的网络信息,使模型表现出越来越好的评估效果。当 Timer 值为 8 时,模型的准确率达到最高,此时输入卷积神经网络的特征图为 $12\times12\times8$。在第二阶段,随着 Timer 值的增大,网络包含的网络信息过多,导致在模型训练阶段出现过拟合现象。测试集的准确率变化趋势和评估时间如图 11 所示。

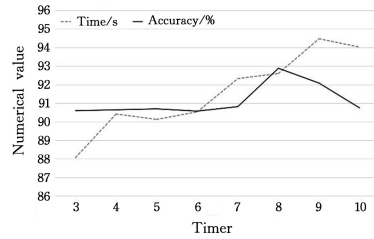

图 11 KDDCup-99 数据集上 Timer 值对态势理解评估时间和准确率的影响

Fig. 11 Influence of Timer value on situation understanding assessment time and accuracy on KDDCup-99

4.1.3 KDDCup-99 数据集上不同算法的对比实验

本文分别用文献[6]中提出的基于 PCA 和随机森林分类的入侵检测方法和文献[10]中提出的改进 LSTM 的网络安全态势评估算法以及 4.1.2 节中第 6 组实验模型进行 KDDCup-99 数据集上的态势评估对比实验,以态势评估准确率作为评价指标,实验结果如表 6 所列。

表 6 不同算法在 KDDCup-99 数据集上的态势评估效果

Table 6 Situation assessment effect of different algorithms on KDDCup-99 dataset

Type	Accuracy/%
PCA-RF	86.10
pro-LSTM	90.56
com-CNN	92.89

其直观准确率的对比图如图 12 所示。

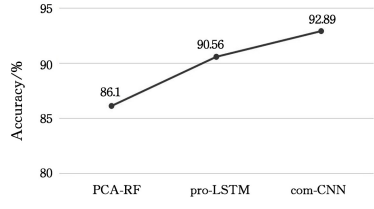

图 12 不同算法在 KDDCup-99 数据集上的态势评估效果

Fig. 12 Situation assessment effect of different algorithms on KDDCup-99 dataset

4.2 实验 2：AWID 数据集上的态势理解评估

4.2.1 数据预处理

本实验采用的是 AWID 数据集，AWID 数据集包含 155 维属性，其中标签包含 4 种状态，分别为 Normal，Impersonation，Injection，Flooding，这 4 种标签在训练集和测试集中对应的样本量如表 7 所列[18]。

表 7 AWID 数据集攻击类型的分布

Table 7 AWID dataset attack type distribution

Type	Train-Dataset	Test-Dataset
Normal	1 633 190	530 785
Impersonation	48 522	20 079
Injection	65 379	16 682
Flooding	48 484	8 097
SUM	1 795 575	575 643

对 AWID 数据集的预处理主要包括数据清洗、特征选择和空值补充。

(1)数据清洗

AWID 数据集中有 46 维属性特征，其中空缺值在 90% 以上，本文对这 46 维属性特征进行丢弃，丢弃后的数据为 109 维。

(2)特征选择

前文提到，我们希望载入神经网络模型的特征矩阵尽量为方阵，因此本文根据该数据集的属性重要度进行特征丢弃，丢弃属性为“wlan. wep. iv”“wlan. wep. icv”“wlan. ra”“wlan. da”“wlan. ta”“wlan. sa”“wlan. bssid”“frame. time_epoch”共计 8 维，此时处理后的 AWID 数据集为 101 维，其中包含 100 维属性特征和 1 维标签。

(3)空值补充

处理后的 AWID 数据集中有较多空值，本文对字符串型特征进行“miss”填充，对数字型特征进行均值填充。

4.2.2 对比实验与分析

使用本文提出的网络模型，通过调整 Timer 设置对比实验，记录模型评估时间，以准确率为评价指标，结果如表 8 所列。

表 8 Timer 值与模型评估时间及准确率的对照表

Table 8 Comparison of Timer value with model evaluation time and accuracy

Number	Timer	Time/s	Accuracy/%
1	5	208	78.62
2	6	216	81.51
3	7	219	89.68
4	8	211	92.45
5	9	218	92.60
6	10	217	90.75
7	11	221	91.84

由上述 7 组实验可得，随着 Timer 值的增大，模型准确率会先提高后降低，当 Timer 值为 9 时，模型的准确率达到最高，此时输入卷积神经网络的特征图为 10×10×9。由上述 7 组实验可得到，模型评估时间基本保持不变，但是相比 4.1.2 节中的实验，本组实验时间明显多于 4.1.2 节中的实验时间，这主要是因为 AWID 数据集的样本量远大于 KDDCup-99 数据集。综上，AWID 测试集的准确率变化趋势和评估时间如图 13 所示。

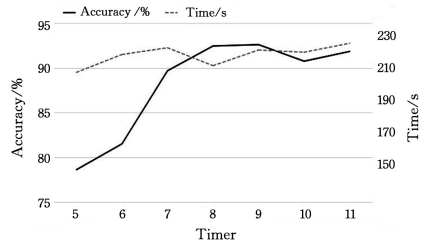

图 13 AWID 数据集下 Timer 值对态势理解评估时间和准确率的影响

Fig. 13 Influence of Timer value on situation understanding assessment time and accuracy on AWID

综上，本文提出的模型在 AWID 数据集上有较高的准确率和较好的稳定性。

结束语 本文提出了一种基于时间因子和复合 CNN 结构的网络安全态势感知模型，该模型将卷积分解技术和深度可分离技术相结合，利用两种结构的不同优势，形成串联复合单元结构，大大减少了网络参数，缩短了网络运行时间；同时，本文将网络数据转换为灰度值载入神经网络模型，引入时间因子以增加卷积网络的输入通道，使载入模型的复合样本包含更多的网络信息。实验结果证明，本文提出的网络安全态势理解和评估模型在 KDDCup-99 和 AWID 数据集上均表现出较高的准确率和较好的稳定性，对网络态势感知在深度学习领域的研究有一定的参考意义。

下一步将从以下方向开展工作：

(1)本文虽然对不平衡数据进行了调整和优化，但数据不平衡现象依旧对实验结果有较大影响，因此未来会对模型框架进行优化，尽量减小不平衡数据对模型准确性的影响。

(2)本文进行的实验均是仿真实验，未将提出的态势理解和评估以及预测方法应用到真实网络进行实践，因此未来会尝试将本文模型应用于真实环境，以发挥模型的优势，降低网络损失。

(3)本文虽然进行了态势呈现，但是呈现方式仍采用了较为传统的方法，未来将尝试多形式的态势呈现方法，将网络状态更加直观地呈现给读者。

参 考 文 献

[1] ENDSLEY M R. Toward a Theory of Situation Awareness in Dynamic Systems[J]. Human Actors: The Journal of the Human Factors and Ergonomics Society, 1995, 37(1): 32-64.

[2] BASS T. Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems [C]// 1999 Proceedings of the Iris National Symposium on Sensor & Data Fusion. 1999: 24-27.

[3] LIU X W, YU J G, LV W F, et al. Network security situation: from awareness to awareness-control[J]. Journal of Network and Computer Applications, 2019, 139: 15-30.

[4] ZHENG W. Research on situation awareness of network security assessment based on dempster-shafer[J]. MATEC Web of Conferences, 2020, 309(10): 02004.

[5] SUN W X. Pso and Svm for Network Security Situation Prediction[J]. Computer Applications and Software, 2019, 36(6): 308-316.

[6] LIN W N, CHEN M Z, ZHAN Y Q, et al. Research on an Intrusion Detection Algorithm Based on PCA and Random-forest Classification[J]. Netinfo Security, 2017(11): 50-54.

[7] SHEN L, WEN Z C. Network security situation prediction in the cloud environment based on grey neural network[J]. Journal of Computational Methods in Sciences and Engineering, 2019, 19(1): 153-167.

[8] LIU J W, LIU J J, LU Y L, et al. Application of game theory in network security situation awareness[J]. Journal of Computer Applications, 2017, 37(S2): 48-51.

[9] ALAOUI I E, GAHI Y. Network Security Strategies in Big Data Context[J]. Procedia Computer Science, 2020, 175: 730-736.

[10] WANG Z J, CHEN L, SONG S Y, et al. Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations[J]. Alexandria Engineering Journal, 2020, 59(4): 2725-2731.

[11] DO C T, TRAN N H, HONG C, et al. Game Theory for Cyber Security and Privacy[J]. ACM Computing Surveys, 2017, 50(2): 1-37.

[12] BALAJ S, JULIE E G, ROBINSON Y H, et al. Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model[J]. Computer Standards & Interfaces, 2019, 66(OCT): 103358.1-103358.10.

[13] ZHAO D M, LIU J X. Study on network security situation awareness based on particle swarm optimization algorithm[J]. Computers & Industrial Engineering, 2018, 125: 764-775.

[14] LI S, ZHAO D M. LSTM-based method for comprehension and evaluation of network security situation[C]// 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, 2019: 723-728.

[15] CHEN J G, QI Z H, CHEN T F. Network security situation awareness based on RBF neural networks[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition), 2019, 39(4): 88-95.

[16] CHEN H S, CHEN J J. 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.

[17] DEMIR F, SENGUR A, BAJAJ V. Convolutional neural networks based efficient approach for classification of lung diseases [J]. Health Information Science and Systems, 2020, 8(1): 1-8.

[18] SYDNEY M K, SUN Y X. A deep learning method with wrapper based feature extraction for wireless intrusion detection system [J]. Computers & Security, 2020, 92: 101752.1-101752.15.

ZHAO Dong-mei, born in 1966, Ph.D, professor, Ph.D supervisor, is a senior member of China Computer Federation. Her main research interests include network information security and computer application.