基于 Stacking 集成学习的网络安全态势预测方法

曹　波，李成海*，宋亚飞，陈　晨
（空军工程大学防空反导学院，西安，710051）

摘要　针对现有的网络安全态势预测模型预测精确度低且泛化能力差等问题，提出一种基于 Stacking 模型融合的态势预测方法。该方法中，借助 Stacking 算法将 TCN 网络、WaveNet、GRU、LSTM 进行集成挖掘态势数据之间的相关性；之后利用逻辑回归进行预测得到最终态势值；利用粒子群优化算法进行参数寻优，提升模型性能。基于 2 个数据集进行验证，实验表明，所提预测方法具有较小的均方误差和平均绝对误差，收敛速度较快，拟合度均可达 0.999，可以很好解决预测精确度低的问题，提升了模型的泛化能力。

关键词　态势预测；集成学习；粒子群算法；卷积神经网络；循环神经网络
DOI　10.3969/j.issn.2097-1915.2022.05.016
中图分类号　TP393　　**文献标志码**　A　　**文章编号**　2097-1915(2022)05-0101-07

Research on Network Security Situation Prediction Method Based on Stacking Integrated Learning

CAO Bo, LI Chenghai*, SONG Yafei, CHEN Chen
(Air Defense and Missile Defense School, Air Force Engineering University, Xi'an 710051, China)

Abstract　To address the problem of low prediction accuracy of existing network security posture prediction models, a prediction method based on Stacking model fusion is proposed. In this method, the TCN network, WaveNet, GRU, and LSTM are integrated with the Stacking algorithm to explore the correlation among the situational data; after that, logistic regression is used to further predict the final situational values; the particle swarm optimization algorithm is used to optimize the parameters and improve the model performance. Based on two data sets for validation, the experiments show that the proposed prediction method has small mean square error and mean absolute error, fast convergence speed, and the fit degree can reach 0.999, which can well solve the problem of low prediction accuracy.

Key words　situation prediction; integrated learning; particle swarm algorithms; convolutional neural network; recurrent neural network

网络安全态势预测就是通过对历史网络数据即态势评估得来的态势值进行分析融合，挖掘数据之间的深层关系，运用专家知识等理论方法预测未来态势的发展趋势，为安全管理人员提供决策依据[1]。

伴随着机器学习的不断发展，神经网络在网络安全态势预测领域得到了广泛应用。神经网络通过

收稿日期：2022-03-09
基金项目：国家自然科学基金(62002362；61703426)；陕西省高校科协青年人才托举计划(2019038)；陕西省创新能力支持计划(2020KJXX－065)
作者简介：曹　波(1998—)，男，山西应县人，硕士生，研究方向为网络安全态势感知。E-mail：bobofighting2021@163.com
李成海(1966—)，男，山东东平人，教授，研究方向为网络安全态势感知、嵌入式操作系统。E-mail：lichenghai_ns@163.com

引用格式：曹波，李成海，宋亚飞，等. 基于 Stacking 集成学习的网络安全态势预测方法研究[J]. 空军工程大学学报，2022，23(5)：101-107.
CAO Bao, LI Chenghai, SONG Yafei, et al. Research on Network Security Situation Prediction Method Based on Stacking Integrated Learning [J]. Journal of Air Force Engineering University, 2022, 23(5): 101-107.

组合低层特征形成更加抽象的非线性的高层表示，进而挖掘数据之间的输入输出关系，在态势预测领域取得了较好的效果。文献[2]通过结合深度可分离卷积和卷积分解技术的思想对态势要素和态势值进行映射，但是该模型忽略了原始数据属性之间的重要性差异。文献[3]提出一种基于 BP 神经网络的态势预测模型，将模拟退火算法引入人群搜索算法中实现对模型参数的优化，取得较好效果。文献[4]提出一种基于差分 WGAN 的态势预测方法，该方法利用生成对抗网络(generating adversarial network，GAN)模拟态势的发展过程，引入 Wasserstein 距离作为 GAN 的损失函数，同时添加差分项提升态势值的预测精度。文献[5]提出一种改进遗传粒子群算法优化极限学习机的态势预测方法，但是样本数目和滑动窗口数设置不合理时对模型效果有很大的影响。文献[6]提出一个两层的长短期记忆网络和门控循环单元的预测模型，虽然提升了预测精度，但是也增加了模型复杂度和训练的时间成本。文献[7]提出一种动态 K-means 与粒子群的网络安全态势预测优化算法，通过动态 K-means 算法对态势数据进行聚类，再通过粒子群算法选择 RBF 网络的权值，模型预测精度提高了 14 倍。

为提升网络安全态势预测模型的预测精度和泛化能力，本文提出一种基于 Stacking 集成学习的网络安全态势预测方法。

1 基于 Stacking 算法的网络安全态势

基于 Stacking 算法的网络安全态势预测模型主要包括 4 个部分：数据预处理，基本预测模型，Stacking 融合以及粒子群算法优化，其具体结构见图 1。

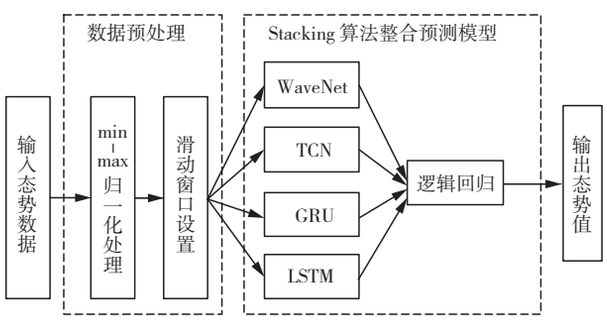


图 1 基于 Stacking 算法的网络安全态势预测模型结构示意图

1.1 数据预处理

态势数据预处理的主要流程为：

1)读取数据并进行数据清洗；

2)将清洗后的数据进行归一化处理，本文采用 min-max 归一化的方法将特征数据规范到－1 和 1 之间；

3)滑动窗口处理。为有效学习历史数据的变化趋势，采样滑动窗口法对归一化后的数据进行处理。假设滑动窗口设置为 $s=m+1$，样本总数为 n，则经过滑动窗口法后生成 $n-(m+1)+1$ 个样本。

1.2 基本预测模型：卷积神经网络

CNN 是一类具有稀疏连通性和权值共享特性的深度前馈神经网络，在 CNN 的演变过程中，出现了多种利用 CNN 来挖掘数据的时间特性的模型，如 WaveNet 和 TCN 等，在提取长距离依赖信息时表现出较好的性能，因此本文选择这两种神经网络。

时域卷积神经网络(temporal convolution network，TCN)是 Shaojie Bai 等人[8]在卷积神经网络的基础上提出的一种用于处理时间序列数据的网络结构。TCN 结构主要是由堆叠的一维全连接卷积层(fully-convolution network，FCN)组成，每个基本卷积层包含因果关系，这样可以避免从未来到过去的信息“泄露”，同时 TCN 还强调通过加深网络深度和扩展卷积相结合的方式提升学习时间序列特征的能力。简单来说，TCN 结构可由式(1)表示：

$$\mathrm{TCN}=1D\mathrm{FCN}+\mathrm{Casual\ Convolution} \tag{1}$$

本文首次将 TCN 网络引入网络安全态势预测任务中，它能够准确学习时间序列的长短依赖关系，同时拥有足够的记忆内存，从而取得较好的效果。

具体而言，假设模型输入 $X\in R^n$，$f\in R^k$ 表示一维空洞因果卷积核，则经过空洞因果卷积操作后的结果如式(2)所示：

$$F(s)=(X*_d f)(s)=\sum_{i=0}^{k-1}f(i)X_{s-di} \tag{2}$$

式中：d 代表膨胀因子；k 代表卷积核大小，$s-di$ 代表输入序列对应的位置点。从中可以看出当 $d=1$ 时，空洞因果卷积会对输入数据通过常规计算方式进行计算；$d\neq 1$ 时，对输入数据进行卷积运算。一般情况下，膨胀因子 d 会随着网络层数 i 按照式(3)的方式变化：

$$d=O(2^i) \tag{3}$$

这样的变化方式可以保证在卷积核尺寸 k 变化时，TCN 的感受域能够迅速增加，网络中高层卷积核的感受域可以覆盖输入时间序列的所有有效输入，进而对信息进行更好地融合，并且对序列中的长期模式进行有效建模。

WaveNet 是 2016 年 Google DeepMind 开发的一种用于处理音频信号开发的网络模型[9]。该网络模型结构由多个残差模块构成，每个残差模块均包

含多层扩张卷积和批量归一化层。它通过采用扩张卷积和跳跃连接的方式提升了神经网络对长距离依赖的学习能力，因而对于时间序列数据具有较好的提取特征能力.

1.3　基本预测模型：循环神经网络

循环神经网络是最基本的处理时间序列的深度学习模型。它以序列数据作为输入，在序列的演进方向进行递归且所有节点均按照链式进行连接。RNN 因其具有记忆性、参数共享且图灵完备的特性在序列的非线性特征进行学习时具有一定的优势。但是，由于 RNN 结构无法学习长距离依赖，因而在现代的机器学习问题中很少直接使用，同时产生诸如长短期记忆网络、门控循环单元等多种变种算法。GRU 和 LSTM 作为 RNN 的变种，通过门控单元的引入提升了其提取长距离信息的能力，因此本文通过这两种模型来学习原始态势数据在时间上的特征。

长短期记忆网络是最早提出的对于 RNN 的改进[10]，其主要由输入门、遗忘门和输出门来代替原来的循环单元，相较于 RNN 对系统建立的递归计算，LSTM 的 3 个门在 LSTM 单元的内部建立了自循环。输入门决定当前时间步的输入和前一个时间步的系统状态对内部状态的更新；遗忘门决定前一个时间步内部状态对当前时间步内部状态的更新；输出门决定内部状态对系统状态的更新。

2014 年，Cho 提出了更加简单的、将长短时记忆网络的单元状态和隐层状态进行合并的、还有一些其他的变动的 GRU 模型[11]。GRU 是 LSTM 的一种变体，能够有效的解决长期记忆和反向传播中的梯度问题。GRU 主要包含更新门、重置门两个部分。重置门来计算是否忘记之前计算状态，更新门决定将上一步多少信息继续迭代到当前步骤[12]。

1.4　Stacking 集成学习算法

集成学习是使用一系列学习器进行学习，并使用某种规则将所得结果进行整合从而获得比单一学习器效果更好的模型的方法，通常有 Bagging，Boosting，Stacking 等方式[13]。本文采用 Stacking 算法将基预测模型进行融合，进一步增强模型的泛化能力，提高预测模型的灵活性，进而获得更好的预测模型，其主要流程如图 2 所示。

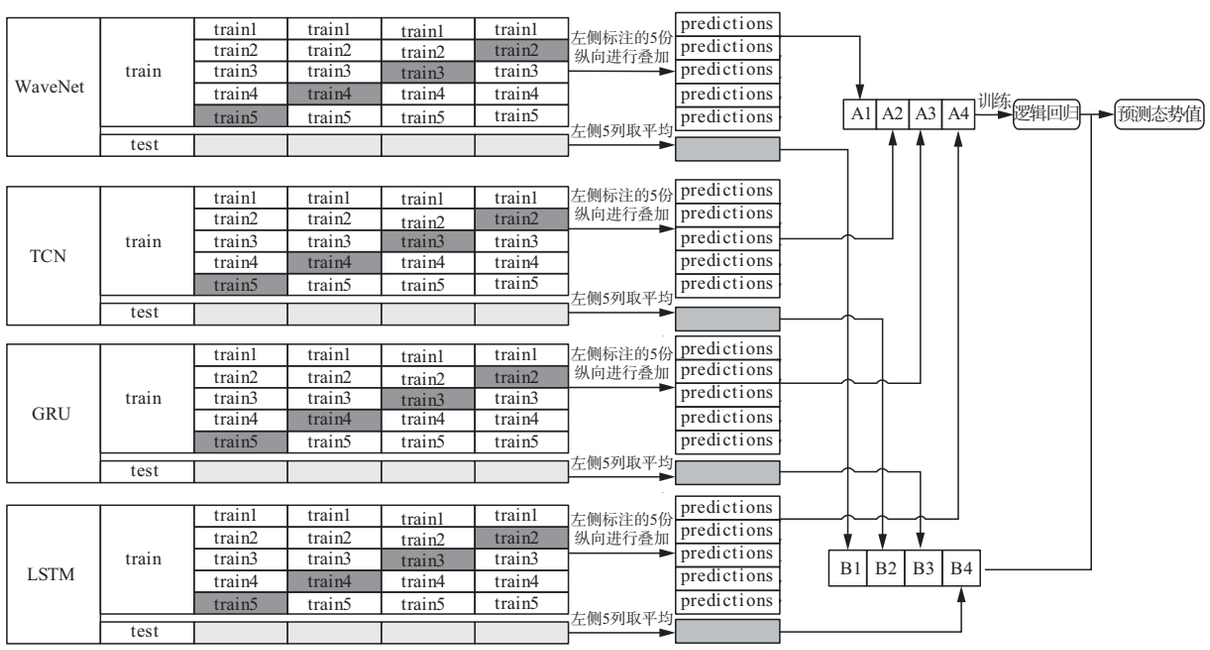


图 2　Stacking 集成学习算法流程图

2　实验仿真

2.1　实验设置

为验证所提 CNN-RNN 态势预测算法的性能，本文设置多组实验，预测模型实验和对比实验都在 64 位的 Windows Intel(R) Core(TM) i7-7700HQ CPU(2.80 GHz)上进行的，该 CPU 具有 16 GB RAM 和基于 python 的 Nvidia GeForce GTX 1050 GPU(4 GB)，使用 Python 的 TensorFlow 库编写本文的 TCN、Attention、GRU 模型和 PSO 优化算法。

本文所提态势预测模型在训练过程中需要对多个参数进行设定，包括 WaveNet、TCN 网络的膨胀

因子、GRU、LSTM 的神经元数、优化器的学习率、批处理大小等。这些参数的设置会直接影响模型训练的结果。本文采用粒子群算法[14]对涉及到的参数进行优化，寻找模型参数的最优组合。

本文实验参数具体设置如下：PSO 算法中种群大小为 5，迭代次数为 30，惯性权重为 0.6，学习因子 c_1、c_2 为 0.5。经过 PSO 算法优化后的网络模型参数具体如表 1 所示。

表 1 优化后模型参数设置

模型参数	参数设置
优化器	Adam
学习率	0.000 1
TCN 卷积核	4
TCN 膨胀因子	1/2/4/6/8
WaveNet 膨胀因子	1/2/4/6/8/10/12
GRU 神经单元数	239/250/185
LSTM 神经单元数	52/159/219
批处理大小	32

2.2 实验数据及评价标准

为了验证本文所提 CNN-RNN 态势预测算法，本文选择 2 个数据集进行实验，两组数据的具体情况如下：

数据 1：为了获取真实有效的网络安全态势值，本研究采用文献[15]中搭建的网络环境所得的实验数据：通过网络安全评估系统每隔 30 min 对主机遭受的攻击次数、攻击种类和攻击严重程度进行综合性评估，计算出当前时段的网络安全态势值，最终选取 150 个态势值经过归一化处理得到本次实验的样本数据如图 3 所示。

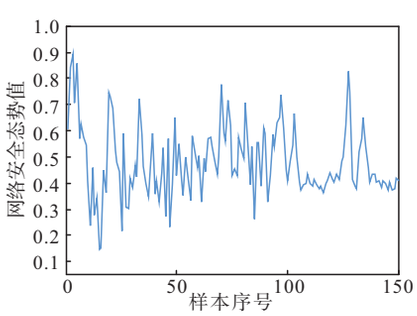


图 3 数据 1 网络安全态势值

数据 2：来源于国家互联网应急中心网站[16]公布的真实数据。本文选取该网站发布的自 2018 年 1 月 7 日至 2021 年 4 月 11 日共计 171 期的态势周报数据为基础进行实验验证。安全态势周报公布的数据主要从境内感染网络病毒的主机数量、境内被篡改网站总数、境内被植入后门网站总数、境内网站的仿冒页面数量和新增信息安全漏洞数量 5 个角度进行评估。为了直观体现网络安全态势，本文采用文献[17]中提到的态势评估方法进行量化，根据对网络安全威胁的程度高低分配不同权重，具体如表 2 所示，之后按照式(4)计算每周的态势值。

表 2 网络安全威胁权重分配

境内感染网络病毒的主机数量	境内被篡改网站总数	境内被植入后门网站总数	境内网站的仿冒页面数量	新增信息安全漏洞数量
0.30	0.25	0.15	0.15	0.15

$$SA = \sum_{i=1}^{5} \frac{T_i}{T_{i\max}} \omega_i \tag{4}$$

式中：T_i 代表某周某种网络安全威胁的数量(i 代表安全威胁的种类)；$T_{i\max}$ 代表是选取的 171 期数据中该种安全威胁的最大数量；ω_i 代表其对应的权重。经过归一化处理后的数据如图 4 所示。

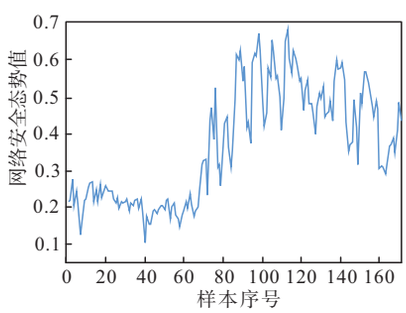


图 4 数据 2 网络安全态势值

为评价本文所提预测模型的效果，选取平均绝对误差(mean absolute error，MAE)、均方误差(mean square error，MSE)以及拟合优度决定系数(the coefficient of determination，R^2)3 个参数作为评价指标，评价指标的计算公式如下所示[18]：

$$MAE = \frac{1}{N}\sum_{i=1}^{N} | y_i - \hat{y}_i | \times 100\% \tag{6}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N} (y_i - \hat{y}_i)^2 \tag{7}$$

$$R^2 = \frac{\left[\sum_{i=1}^{N}(y_i - \bar{y})(\hat{y}_i - \bar{\hat{y}_i})\right]^2}{\left[\sum_{i=1}^{N}(y_i - \bar{y})^2\right]\left[\sum_{i=1}^{N}(\hat{y}_i - \bar{\hat{y}_i})^2\right]} \tag{8}$$

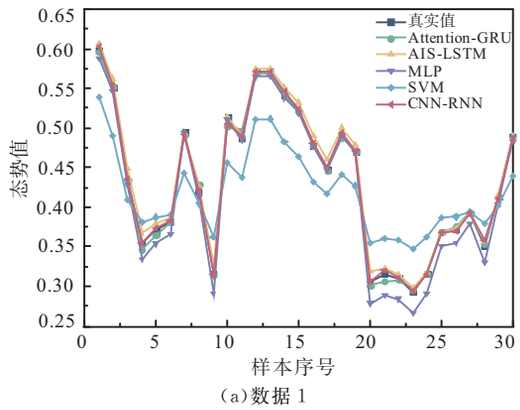
式中：y_i 为某样本的真实值；$\hat{y}_i$ 为某样本的预测值；N 为样本个数，$\bar{y}_i$ 为真实值的平均值；$\bar{\hat{y}_i}$ 为预测值的平均值。

2.3 实验结果分析

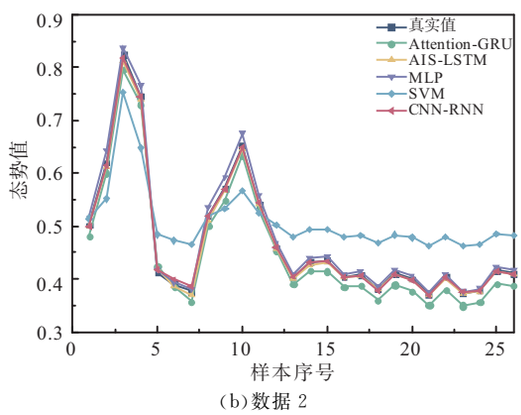
2.3.1 预测精度对比

为有效对比本文模型与其他模型预测能力的差别，设置以下实验：在相同的实验条件下设置滑动窗口数 $s=5$，基于数据 1、数据 2，分别用 Attention-

GRU、AIS-LSTM、MLP、SVM、CNN-RNN 这 5 种模型进行预测，得到预测态势值与真实态势值对比图如图 5 所示，不同模型评价指标见表 3。



(a)数据 1



(b)数据 2

图 5　不同模型预测结果对比

从图 5 中可以看出，对于数据 1、数据 2 而言，当滑动窗口设置为 5 时，对比的 5 种模型均可实现对于态势值的预测，但是不同模型的预测性能却有很大的差别。从图 5(a)中可以看出，对于数据 1 而言，文献[19]中提出的 Attention-GRU 模型预测效果一般，所得预测态势值如此，MLP 模型预测所得态势值同样普遍小于真实值，而 SVM 模型预测效果最差；从图(b)中可以看出，对于数据 2 而言，文献[20]中提出的 Attention-GRU 模型相较其他两个模型预测所得态势值与真实值之间有很大的偏差，而 SVM 模型虽能够预测态势值的变化趋势，但效果很差。分析原因发现：SVM 适用于解决小样本线性回归问题，当样本数目较多时，所得预测结果较差，误差较大；MLP 虽可以解决样本较多时的线性回归问题，但是其难以捕捉时间序列之间的长距离依赖关系，预测效果一般。本文 CNN-RNN 预测模型融合了 TCN、WaveNet、GRU 和 LSTM 在提取时间序列之间关系的特性，预测结果更加准确。

从表 3 中可以看出，本文所提 CNN-RNN 预测模型的误差值最小，相比其他模型有很大的优势。对于数据 1，CNN-RNN 模型相比 Attention-GRU 模型，MAE 降低了 34.43%，MSE 降低了 60%；相比 AIS-LSTM，MAE 降低了 65.57%，MSE 降低了 86.67%。对于数据 2，CNN-RNN 模型相比 Attention-GRU 模型，MAE 降低了 85.42%，MSE 降低了 97.62%；相比 AIS-LSTM，MAE 降低了 31.28%，MSE 降低了 66.67%。结果表明对于不同数据而言，CNN-RNN 模型对于网络安全态势值的预测较为有效，且相比其他模型预测精度较高。

表 3　不同模型评价指标对比

预测模型	数据 1		数据 2	
	MAE	MSE	MAE	MSE
Attention-GRU	0.003 34	0.000 02	0.019 14	0.000 42
AIS-LSTM	0.006 36	0.000 06	0.004 06	0.000 03
MLP	0.011 67	0.000 22	0.009 56	0.000 14
SVM	0.039 67	0.001 89	0.067 04	0.005 10
CNN-RNN	0.002 19	0.000 008	0.002 79	0.000 01

2.3.2　拟合度对比

为进一步验证本文所提 CNN-RNN 模型的有效性，基于数据 1、数据 2 对比测试结果的拟合度，如图 6 所示。

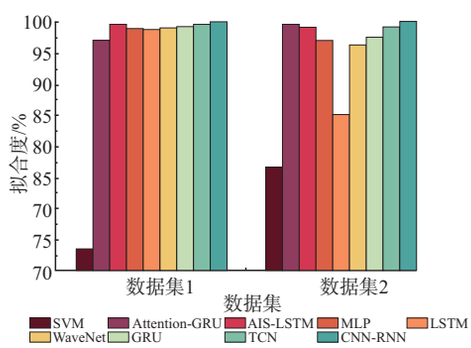
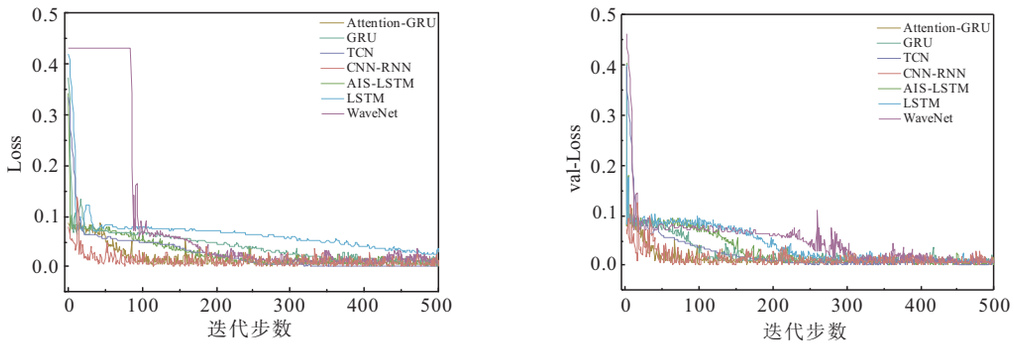


图 6　不同模型拟合度对比

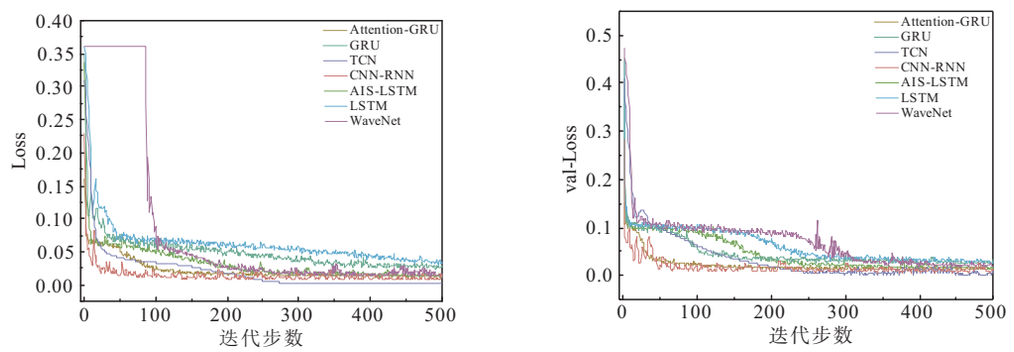
从图 6 中可以看出，CNN-RNN 模型的拟合度相较其他 8 种模型最高。对于数据 1，CNN-RNN 模型的拟合度高达 0.999 36；对于数据 2，CNN-RNN 模型的拟合度高达 0.999 02。进一步证明本文所提 CNN-RNN 预测模型所得到的预测曲线相较其他模型更加准确，同时也证明了 CNN-RNN 预测模型在预测态势值时的有效性和准确性。

2.3.3　收敛性分析

图 7 给出了模型训练误差随迭代步数变化曲线图，本文 CNN-RNN 预测模型在收敛速度和收敛精度上都优于其他模型，证明了该模型能够充分学习时序数据的特征，取得效果较好。



(a)数据 1



(b)数据 2

图 7 不同模型收敛性对比

2.3.4 运行时间分析

模型进行预测时不仅要考虑预测的精确度,同时还要考虑模型运行所需时间,即模型训练时间和预测时间。模型运行的时间与模型的复杂度、迭代次数、批处理大小等都有关系,通过实验得到不同预测模型的运行时间见表 4。

表 4 不同预测模型运行时间 单位:s

预测模型	数据 1			数据 2		
	训练	预测	总和	训练	预测	总和
Attention-RU	418.94	0.77	419.71	359.76	0.76	360.52
AIS-LSTM	46.96	1.16	48.12	44.53	0.17	44.7
MLP	0.085 6	0.001 9	0.087 5	0.002	0.089 8	0.091 8
SVM	0.06	0.001	0.061	0.001	0.001	0.002
GRU	39.59	1.08	40.67	39.59	1.08	40.67
LSTM	26.15	1.51	27.66	45.44	1.18	46.62
WaveNet	632.7	2.71	635.41	312.3	2.25	314.55
TCN	40.1	0.26	40.36	20.12	0.37	20.49
CNN-RNN	41.84	4.71	45.55	40.05	3.22	43.27

从表中可以看出,SVM、MLP 两种模型所用时间较少,但是二者在处理数据时较为简单,取得结果预测精度较低,不能够准确预测态势值;Attention-GRU 模型经过粒子群算法优化后得到批处理值为 1,因而预测时间较长;本文所提 CNN-RNN 模型在提升预测精确度的同时,花费时间较少。

3 结语

为了对网络安全态势值进行准确预测,同时降低过拟合风险并提高泛化能力,本文提出一种基于 Stacking 集成学习的态势预测模型,该模型首先通过 TCN、WaveNet 两种卷积神经网络结构以及 GRU、LSTM 两种循环神经网络结构挖掘并学习数据的时间特征,之后借助 Stacking 融合算法将这四种模型进行融合。随后通过逻辑回归算法实现最终态势值的预测。为进一步提升预测结果的准确度,引入粒子群算法对模型的参数进行优化。本文通过在两个数据集上进行的多个实验证明了模型在处理网络数据时具有较强的特征提取能力和较高的预测精度,说明了本文模型的高效性和实用性。

参考文献

[1] 杨林，于全. 动态赋能网络空间防御[J]. 北京：人民邮电出版社，2017.

[2] 张任川，张玉臣，刘璟. 应用改进卷积神经网络的网络安全态势预测方法[J]. 计算机工程与应用，2019，55(6)：86-93.

[3] 张然，刘敏，张启坤. 一种基于 SA-SOA-BP 神经网络的网络安全态势预测算法[J]. 小型微型计算机系统，2020，41(10)：2157-2163.

[4] 王婷婷，朱江. 基于差分 WGAN 的网络安全态势预测[J]. 计算机科学，2019，46(S2)：433-437.

[5] 唐延强，李成海，王坚. IGAPSO-ELM：一种网络安全态势预测模型[J]. 电光与控制，2022，29(2)：30-35.

[6] WANG B，KONG W，GUAN H，et al. Air Quality Forecasting Based on Gated Recurrent Long Short Term Memory model in Internet of Things[J]. IEEE Access，2019，7：69524-69534.

[7] 魏雅娟，刘兆，刘意先，等. 动态 K-means 与粒子群的网络态势预测优化算法[J]. 西安邮电大学学报，2020，25(5)：33-38.

[8] BAI S，KOLTER J Z，KOLTUN V. An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling[EB/OL].(2016-09-19). doi:https://doi.org/10.48550/arXiv. 1803.01271.

[9] OORD A，DIELEMAN S，ZEN H，et al. Wavenet：A Generative Model for Raw Audio[EB/OL](2018-03-01). doi：https：//doi. org/10. 48550/arXiv. 1609. 03499.

[10] YU Y，SI X，HU C，et al. A Review of Recurrent Neural Networks：LSTM Cells and Network Architectures [J]. Neural Computation，2019，31(7)：1235-1270.

[11] 吴茂贵，王冬，李涛，等. Python 深度学习基于 TensorFlow[M]. 北京：机械工业出版社，2019.

[12] XIE X，WANG B，WAN T，et al. Multivariate Abnormal Detection for Industrial Control Systems Using 1D CNN and GRU[J]. IEEE Access，2020，99：163-184.

[13] 张一鸣，刘晓锋. 基于多特征提取和 Stacking 集成学习的航空发动机余寿预测[C]//第六届空天动力联合会议暨中国航天第三专业信息网第 42 届技术交流会暨 2021 航空发动机技术发展高层论坛论文集(第 5 册). 2022：124-131. doi：10. 26914/c. cnkihy. 2022. 000068.

[14] 孙绳山，徐常凯，何亚群. 基于 RS-PSO-SVM 的航材消耗预测模型[J]. 南京航空航天大学学报，2021，53(6)：881-887.

[15] 江洋，李成海，魏晓辉，等. 改进 PSO 优化 RBF 的网络安全态势预测研究[J]. 测控技术，2018，37(5)：56-60.

[16] CNCERT.（2021）Weekly Report of CNCERT-Issue 40 [EB/DL].（2021-04-18). https：//www. cert. org. cn/. 2018-1-7/2021-4-11.

[17] 姜万菲. 基于多模型权重提取与融合的网络安全态势预测研究[D]. 兰州：兰州理工大学，2016.

[18] 朱江，陈森. 基于 NAWL-ILSTM 的网络安全态势预测方法[J]. 计算机科学，2019，46(10)：161-166.

[19] 何春蓉，朱江. 基于注意力机制的 GRU 神经网络安全态势预测方法[J]. 系统工程与电子技术，2021，43(1)：258-266

[20] MUNKHDALAI L. An End-to-End Adaptive Input Selection with Dynamic Weights for Forecasting Multivariate Time Series [J]. IEEE Access，2019，7：99099-99114.

（编辑：徐敏）