文章编号:1671-4598(2025)04-0306-07 DOI:10.16526/j.cnki.11-4762/tp.2025.04.041 中图分类号:TP271 文献标识码:A

基于遗传神经网络的通信网络安全威胁智能评估方法

张立达[1]，郝 明[1]，高天昊[2]
(1.中国电子科技集团公司 第54研究所，石家庄 050081；
2.大连理工大学 求实书院，辽宁 大连 116024)

摘要：针对当前的通信网络安全威胁评估方法面临着数据量大、威胁类型多样、环境动态变化等挑战，基于规则和简单统计分析的传统评估方法难以满足实时性、准确性需求的局限性，提出了一种基于遗传神经网络的通信网络安全威胁智能评估方法；通过构建包含通信网络受攻击程度、受攻击后的通信质量和通信容量等方面的通信网络安全评估指标体系，并采用非数值型指标量化、正向化处理、无量纲标准化对评估指标进行规范化处理，设计了基于遗传算法优化的神经网络评估模型，实现对通信网络安全威胁的准确、智能评估；通过TOPSIS方法生成的数据集对所提出的评估方法进行了实验验证，结果显示评估准确率达到了92%，证明了该评估方法的有效性。

关键词：通信网络；网络安全；威胁评估

Intelligent Evaluation Method for Communication Network Security Threat Based on Genetic Neural Network

ZHANG Lida[1], HAO Ming[1], GAO Tianhao[2]
(1. The 54th Research Institute of CECT, Shijiazhuang 050081, China;
2. Qiushi College, Dalian University of Technology, Dalian 116024, China)

Abstract: Facing the challenges of large amounts of data, diverse threat types, and dynamic environmental changes in current communication network security threat assessment methods, traditional assessment methods based on rules and simple statistical analysis are difficult to meet demands for real-time and accuracy. To address these limitations, this paper proposes an intelligent assessment method for communication network security threats based on genetic neural networks. Construct a communication network security assessment index system, including the degree of attack on the communication network, the communication quality and capacity after the attack. Non-numerical indicator quantification, positive processing, and dimensionless standardization are used to standardize assessment indicators, a neural network assessment model optimized by genetic algorithms is designed to achieve accurate and intelligent assessment of communication network security threats. The proposed assessment method is validated on the dataset generated by the TOPSIS method, and the results show an assessment accuracy rate of 92%, proving the effectiveness of the assessment method.

Keywords: communication network; network security; threat evaluation

0 引言

随着信息化建设的快速发展，各种基于通信网络的信息系统被广泛应用于作战指挥、通信保障及火力控制等领域[1]。随着对通信网络依赖程度的增加，相应地，面临的风险也会随之增大。当前，各类通信网络攻击呈现出专业化、定向性等特点，已由单个攻击方式逐渐向分布式协作、大范围、有组织的、复杂的攻击方式转变，通信网络安全威胁[2]已成为最严峻的威胁之一。所以，探索和研究通信网络威胁的特点，建立通信网络安全威胁指标模型，评估通信网络安全威胁的潜在影响、增强通信网络的防护能力至关重要。

通信网络安全威胁评估技术在通信网络的防护中扮

收稿日期:2024-09-29； **修回日期**:2025-01-01。
作者简介:张立达(1983-),男,硕士,高级工程师。
引用格式:张立达,郝 明,高天昊.基于遗传神经网络的通信网络安全威胁智能评估方法[J].计算机测量与控制,2025,33(4):306-312.

演着关键角色。作为防御者，通过在模拟或实际的通信网络环境中引入网络安全威胁，对网络的性能进行有效评估，能够识别出潜在的安全漏洞。这种评估有助于强化网络的防御知识，从而有效提升防御安全威胁的整体能力。作为攻击者，通过对通信网络的威胁进行评估，评估出哪些威胁最大，从而提升对通信系统的威胁程度。如何通过对通信网络中的态势要素进行系统评估工作，通过量化方法对通信网络安全威胁的危害程度进行评估，进而可为用户提供防护依据，提升系统安全性，是未来研究发展的重要方向之一。

经过多年的发展及积累，我国在通信网络建设、网络对抗手段、网络威胁评估等方面从数量到覆盖面上都有了长足的发展和进步[3-6]，比较常用的分析评估方法主要有模糊综合评估法[7-8]、层次分析法[9-12]、网络分析法[13]和数据包络法[14]等。但普遍存在的问题是：具有指标权重计算过程主观性强等问题，存在着人为因素导致的偏差，导致模型精度不够高等问题。随着大数据、人工智能技术的发展，神经网络[15]通过学习大量数据，自动提取特征并进行评估，减少了人为主观因素导致的偏差。同时神经网络能够处理复杂的非线性关系，提供更为精确的评估结果，解决了传统评估方法在数据量大时面临的性能瓶颈。但神经网络，特别是深度学习模型，在训练过程中容易陷入局部最优解，导致无法达到全局最优，影响模型的泛化能力和评估准确性。遗传算法[16]是通过模拟生物进化中的选择、交叉和变异等过程，进行全局优化搜索，在广阔的解空间中寻找到最优的解决方案，有助于解决神经网络在初始阶段容易遇到的局部最优问题。

综上所述，本文将遗传算法和神经网络结合起来，提出了一种基于遗传神经网络的通信网络安全威胁智能评估方法，首先建立评估指标体系、规范化处理指标，再将规范化处理后的数据送入遗传神经网络中进行评估，以遗传算法搜索深度学习模型的最优参数，减小传统评估方法中人为主观影响偏差，解决神经网络评估时陷入局部最优而影响评估准确率的问题，实现对通信网络安全威胁的准确、智能评估。

1　评估指标体系构建及规范化处理

1.1　评估指标体系构建

在通信网络安全威胁智能评估方面[17-19]，一般从通信网络所受攻击程度、通信质量、通信容量等多个维度构建评估指标体系。一般而言，网络攻击的整个流程包括：首先要侦测到要攻击的对象，通过各种手段获取目标的相关信息以及识别其防御体系中的弱点；然后根据被攻击对象的防守薄弱环节，执行破坏性行为或窃取敏感信息等行为。

本文构建的通信网络安全威胁智能评估指标体系如图 1 所示，按照网络攻击方式，将其划分为信息窃取和设备毁瘫。其中，信息窃取类攻击主要关注攻击所用时间、攻击者获得的系统权限以及信息被利用的程度等指标；设备毁瘫类攻击则侧重于评估攻击对通信系统功能的影响，包括通信质量和通信容量两个方面。在通信质量方面，评估指标包括系统的响应能力和处理能力，这些指标能够反映系统在遭受攻击后的稳定性和恢复能力。在通信容量方面，评估指标则涵盖了系统的传输速率和资源利用程度，这些指标有助于衡量攻击对网络整体性能的影响，包括数据传输速率和网络资源的可用性等指标。通过这些指标，可以更全面地理解和评估通信

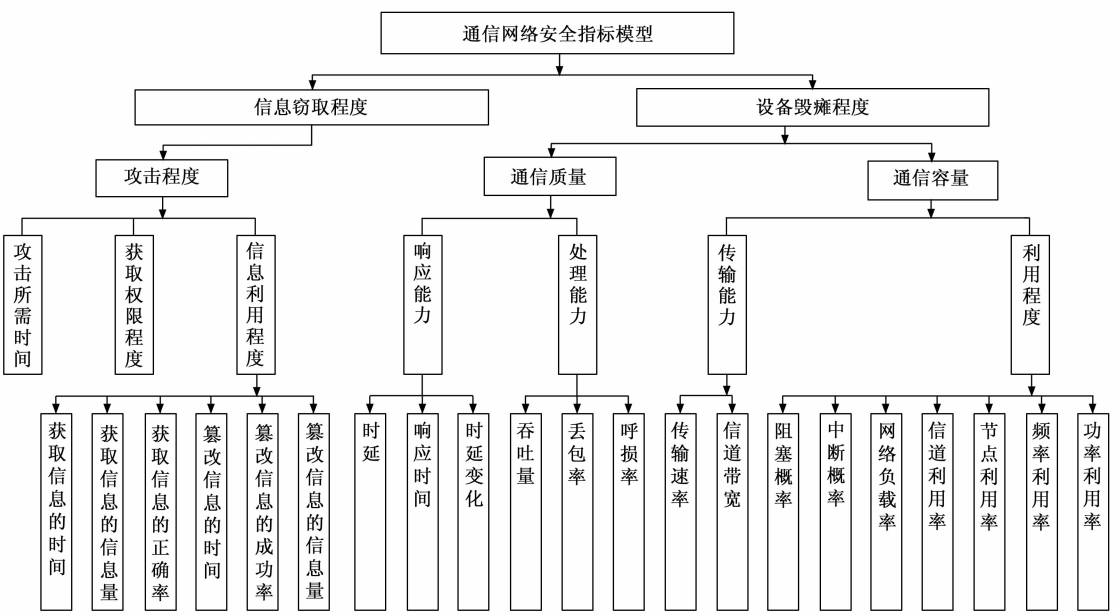


图 1　通信网络安全威胁智能评估指标体系

网络面临的安全威胁，从而制定有效的防御策略和应对措施。

1.2 评估指标规范化处理

针对多种通信网络攻击，分析各类攻击手段下通信网络的多种性能指标，构建每种攻击下通信网络性能指标集合。在此基础上，对各性能指标集合中数据进行正向化处理、标准化处理，利用“TOPSIS 评估法”建立通信网络安全威胁评估数据集，随后将该数据集输入遗传神经网络，以训练智能评估模型。上述过程中指标规范化处理流程如图 2 所示。

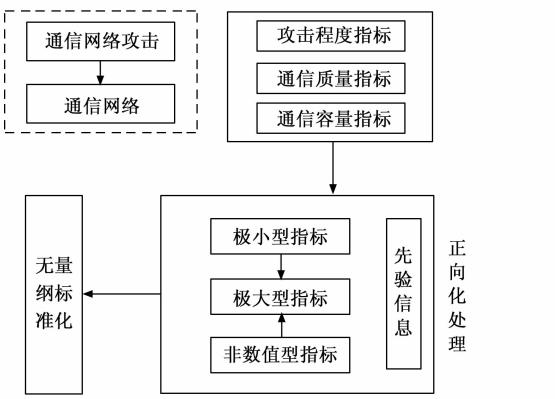


图 2 评估指标规范化处理流程

在数据正向化处理方面，目的是对指标属性进行同向化处理，将极小型指标和非数值型指标都转化为极大型指标，避免尺度混淆；无量纲标准化则通过消除各指标量纲的影响，使得数据能够在同一尺度下进行比较。通过这些关键步骤，可以有效地构建用于通信网络安全威胁智能评估模型训练的数据集。

1.2.1 非数值型指标量化

首先对于非数值类型的指标获取权限程度进行量化。一般情况下，在攻击的初始阶段，攻击者只能获得目标主机的访客或用户权限，对于攻击者来说，没有系统的管理权限就无法执行诸如修改防火墙规则和修改注册表等操作。所以，攻击者需要把访问权限从访问者、用户到管理员，一步步提升，攻击权限的终极目标就是获得服务器的最大权限，实现对目标的控制。依据前述特性，我们对不同权限级别所带来的威胁程度进行量化评估，具体量化结果如表 1 所示。

表 1 获取权限程度的威胁度值量化

获取权限	威胁度值
User	0.4
Administrator	0.6
System	0.8
TrustedInstaller	1

1.2.2 数据正向化处理

数据正向化处理的目的是将原始数据转换为无量纲的正向指标，使得所有的属性都可以在同一标准下进行比较。当一个维度的指标呈现极大型的数值，而另一个维度的指标呈现极小型的数值时，会引发尺度不一致的问题。为了解决这一问题，本文将所有指标统一转换为极大型指标，以确保数据的一致性和可比性。

通信质量和通信容量两个指标相对于威胁度评估的任务属于极小型指标，需要转化为极大型指标。

$$x' = X - x_i \tag{1}$$

其中：X 表示指标，x_i 表示可能取到的最大值。

1.2.3 无量纲标准化

由于评估方案中各评估指标维度不同、物理含义不同、表现形式不同、对总体目标影响程度不同，无法比较，需要无量纲化，取出各评估指标的量纲后，再进行综合评估。对已量化和正向化后的矩阵集中的指标做无量纲化，将各列的元素都除以当前列向量的范数。

$$z_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{n} x_{ij}^2}} \tag{2}$$

经过上述 3 项操作，可得到规范化的评估指标向量 $\hat{X}$ 。

2 通信网络安全威胁评估算法

本文提出的通信网络安全威胁评估算法通过结合遗传算法优化神经网络的参数，以解决神经网络在计算量增加过快的情况下易陷入局部最优，从而影响评估准确率等问题。本文算法的框架如图 3 所示。首先确定残差网络的结构和参数，包括网络的层数、每层的神经元数量、激活函数等，其次利用遗传算法在多代迭代中不断优化网络结构和参数，获得一个适应度高的残差网络模型。再利用遗传算法生成的参数初始化残差网络，从数据中提取关键特征，进行网络训练，实现通信网络安全威胁智能评估。

2.1 残差网络单元结构

残差学习法[20-22]的核心思想是引入了“残差块”(Residual Blocks)，如图 4 所示，这些块旨在让网络学习输入和输出之间的残差映射，即 $H(x) = F(x) + x$ ，网络不仅学习如何从输入到输出映射，而且还学习如何从输入直接映射到残差，然后将这个残差加到输入上。这种方法的优势在于，当网络层数增加时，即使学习到的残差映射 $F(x)$ 接近于零，网络的性能也不会因此退化。这是因为残差块允许梯度直接流向更深的层，而不是通过复杂的层级结构。这样，即使在非常深的网络中，梯度也能够有效地反向传播，从而保持网络的训练效率和性能。

本文的智能评估模型网络结构由 4 个残差网络单元、池化层及全连接层组成，4 个残差网络单元被组织成一系列深度逐渐增加的层，残差单元结构如图 5

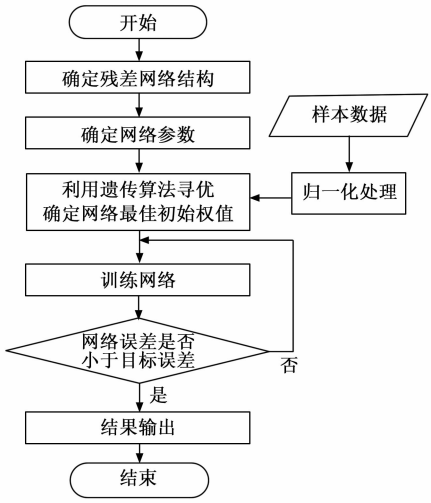


图 3　评估算法原理框图

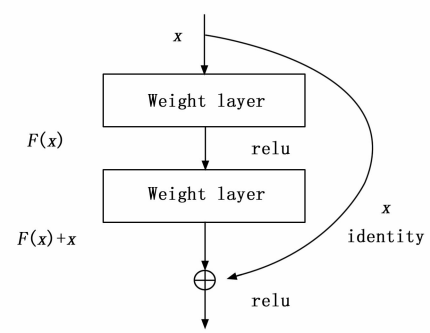


图 4　残差模块示意图

所示，其中卷积层的卷积核大小为 3×3。通过堆叠多个小型卷积核，网络能够逐层深入地提取数据中更多的细节和特征。为了优化训练过程并增强模型的稳定性，每层卷积层后都引入了批量归一化（Batch Normalization）层，同时网络中选用 ReLU（Rectified Linear Unit）函数作为激活机制，减少梯度消失问题，加快收敛速度。同时在残差网络单元之间同样引入了最大池化层。

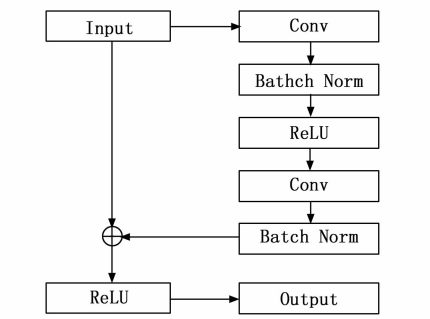


图 5　残差网络单元结构

最后，经过一系列残差单元和池化层的处理后的特征图被展平，并输入到全连接层将池化后的特征向量映射到最终的输出空间进行分类任务，完成从特征到威胁等级的转换，实现对通信网络安全威胁的智能评估。

2.2　遗传神经网络模型

遗传神经网络模型的核心在于应用遗传算法[23-25]来调整神经网络的权值，并通过这些优化后的权重来构建网络，得到最终的通信网络安全威胁评估模型。基于遗传算法的智能评估算法描述了基于遗传算法的通信网络安全威胁智能评估算法流程，该算法通过持续迭代的选择、交叉和变异，逐步提升个体的适应度，优化网络结构和权重分配，以满足更精准的评估需求。

基于遗传算法的智能评估算法：

1）输入：训练数据集，种群大小 N，交叉率 p_c，交叉变异率 p_m，最大迭代次数 G。

2）初始化：随机生成一组个体 $\{M_{0,n}\}_{n=1}^{N}$，每个个体代表一个神经网络权重的编码。

3）for $g = 1, 2, \cdots\cdots, G$ do.

4）评估：使用训练数据集对网络进行训练，计算每个个体的评估准确率。

5）选择：根据个体的评估准确率，在 $\{M_{g,n}\}_{n=1}^{N}$ 上用轮盘赌选择父代个体。

6）交叉：对于选定的父代个体 $\{(M_{g,2n-1}, M_{g,2n})\}_{n=1}^{[N/2]}$，随机选择交叉点，以概率 p_c 交叉，交换父代个体间的遗传信息以产生后代。

7）变异：对于后代个体以概率 p_m 进行权重微小扰动，完成变异。

8）end for.

输出：在最后一代 $\{M_{g,n}\}_{n=1}^{N}$ 中具有最高评估准确度的一组个体。

遗传神经网络在通信网络安全威胁智能评估中运用步骤如下：

1）将网络权重转换为二进制格式，为遗传算法做准备；

2）基于个体的评估准确率来定义适应度函数，以衡量每个个体的性能，是遗传算法中评估个体优劣的关键；

3）对于具有较大的适应度的个体，对其采取直接向下遗传的方法；

4）对当前群体采取交叉、变异操作产生下一代的群体，增加种群的多样性，提高搜索效率；

5）持续进行迭代过程，不断优化，逐步逼近最优解，直到满足预设的最大迭代次数或适应度阈值。

6）使用优化后的网络配置对残差神经网络进行训练，并通过测试集评估其性能。

3　仿真实验

3.1　仿真数据集

构建通信网络安全威胁评估数据集的过程中，首先

使用网络监控工具来捕获受攻击的网络流量数据，获取受攻击程度、通信质量、通信容量等关键性指标。对收集到的数据进行一系列的预处理操作，以确保数据的质量和可用性。其中预处理步骤包括数据清洗，以去除异常值和重复值，确保数据的准确性；数据正向化，将所有指标转化为极大型指标；以及数据标准化，消除不同指标量纲的影响，使得数据在同一尺度下可比较。

预处理后数据集共包含 20 000 个样本，将预处理后的数据构建成一个评分矩阵，每一行代表一个评估对象，每一列代表一个评估指标。应用 TOPSIS 方法对评分矩阵内的数据进行分析，计算每个评估对象与理想最优解和最劣解的距离，基于这些距离，计算出每个对象的总体评分。

在计算出每个评估对象的总体评分后，根据这些评分值，按照预设的威胁等级划分标准，将威胁等级进行分类。威胁等级划分标准如表 2 所示。通过这一系列的步骤，构建出了一个全面、准确的通信网络安全威胁评估数据集，为通信网络安全威胁智能评估提供有力的数据支持。

表 2 威胁度等级划分标准

威胁度值	威胁等级
$0 \leqslant S \leqslant 0.1$	1
$0.1 < S \leqslant 0.2$	2
$0.2 < S \leqslant 0.4$	3
$0.4 < S \leqslant 0.6$	4
$0.6 < S \leqslant 1$	5

威胁等级作为数据标签，其中 60％作为训练集，30％作为验证集，10％作为测试集，这样的划分比例有助于模型在训练过程中学习到足够的特征，同时通过验证集对模型进行调优，并最终在测试集上验证模型的泛化能力。

将训练集和验证集输入残差网络中，利用遗传算法来优化残差网络的参数，寻找到最优的残差网络配置。将残差神经网络设置为最优配置，输入训练集、验证集对模型进行训练，经过多轮迭代充分训练，得到通信网络安全威胁智能评估网络模型；然后将 10％测试集数据送入安全威胁智能评估网络模型中，测试模型性能。上述过程如图 6 所示。

3.2 仿真结果及分析

为验证本文提出方法的有效性，进行了 3 种消融实验对比，3 种消融模型包括未进行数据预处理的评估模型（模型一）、未引入残差网络和遗传算法的评估模型

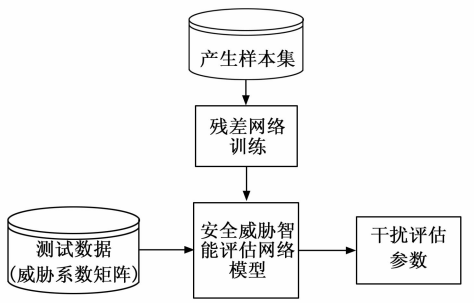


图 6 基于残差网络的智能评估技术流程图

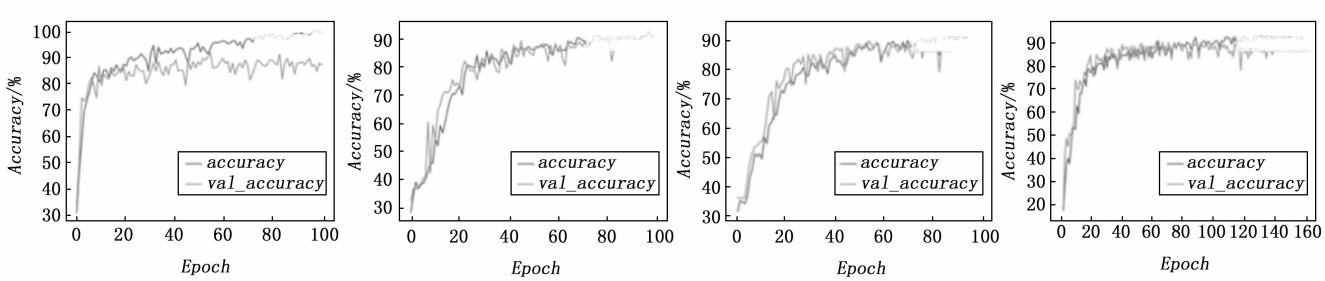
（模型二）和未引入遗传算法的评估模型（模型三）。在模型一中，直接将 23 个指标值作为网络模型的输入未进行数据正向化、标准化处理，未采用 TOPSIS 算法计算综合得分，未进行威胁等级映射，旨在让网络模型直接从原始数据中学习指标与安全威胁等级之间的关系。模型二则首先对指标进行标准化处理，然后将标准化后的数据输入到全连接网络模型中。而在模型三中，指标数据同样经过标准化处理，然后这些标准化的数据被进一步输入到残差网络中进行分析和处理。

将 4 个模型在同一训练数据上进行训练、比较、分析，其训练过程如图 7 所示，图 7 分别为模型一二三和本文所提方法训练过程中准确率的变化；图 8 分别为模型一二三和本文所提方法训练过程中损失值的变化。

将不同方法得到的训练模型在相同的测试数据上进行测试，表 3 为 4 个模型在测试数据的评估结果对比。

表 3 4 个模型评估指标对比

评估指标	模型一	模型二	模型三	本文模型
平均准确率	0.789 9	0.875 0	0.884 9	0.920 8
平均损失	0.784 1	0.421 6	0.355 8	0.299 9
准确率均差	0.057 6	0.013 7	0.021 6	0.012 1
损失均方差	0.059 2	0.014 1	0.020 5	0.011 7



（a）模型一 （b）模型二 （c）模型三 （d）本文模型

图 7 4 个模型训练准确率的变化

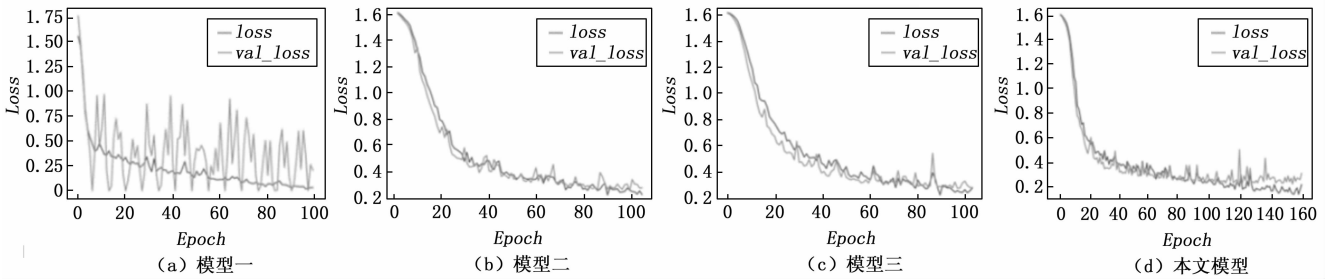


图 8　4 个模型训练损失值的变化

根据实验结果，我们从网络模型的准确率、收敛速度和稳定性等方面对通信网络安全威胁评估模型进行了对比分析。

1）准确性：通过分析图 8 中的准确率变化，能够观察到模型一的准确率趋于稳定在 80%的水平，相比之下，模型二、三、四的准确率则均保持在 90%以上。进一步地，表 3 的数据也显示出对于测试数据，本文模型具有最高的评估准确率和最低的损失值。这些结果表明，本文模型能够对通信网络安全威胁进行有效评估。

2）模型收敛速度：对比 4 个模型在相同训练数据的准确率、损失值的变化，模型二、三在经过 60 轮迭代才开始收敛，本文所提模型在 30 轮左右已经得到了收敛。通过比较分析，可以得出结论：对指标数据实施正向化和标准化处理，有助于加快网络模型的收敛速度。

3）稳定性：通过表 3 中对 4 种模型在同一测试集上的评估精度、损失值的均方差的对比，本文提出的模型在评估准确率和损失值方面展现出了最小的均方误差，这表明模型具有最佳的稳定性。同时 TOPSIS 评估方法依赖于预先定义的理想最优解和最劣解，这限制了评估模型泛化到新数据的能力，而基于遗传神经网络的智能评估方法通过学习大量的训练数据，能够泛化到未见过的数据，提供更精准的评估。

综上所述，模型一由于缺乏数据预处理，在处理原数据时会遇到更多的挑战；模型二虽然进行了数据标准化，但没有利用残差网络和遗传算法的优势，在处理复杂或深层的数据特征时表现不佳；模型三虽然引入了残差网络，但没有遗传算法对网络参数进行优化，无法达到最佳的网络配置，从而影响模型的最终性能。

在对比 3 种消融模型与本文提出的方法时，实验结果证明，通过数据预处理、TOPSIS 算法、基于遗传算法优化的残差神经网络，本文方法在训练过程中展现出了更高的准确率和更低的损失值。通过这些实验，能够得出结论，综合运用数据预处理、先进的网络结构和优化算法，能够显著提升通信网络安全威胁评估智能模型的性能。

4　结束语

本文深入探讨了通信网络安全威胁的智能评估问题，分析了实际应用需求及国内外技术发展的进展，并归纳了当前技术演进的方向。本文提出了一种基于遗传神经网络的通信网络安全威胁智能评估方法，就评估指标体系构建、评估流程和评估方法等方面进行了设计和讨论，并进行了仿真验证。本文方法通过使用遗传神经网络输出得到 1～5 之间的威胁等级，从而获取到当前的网络安全状态，提高了评估的效率。本方法通过结合通信网络的安全威胁评估体系的构建、数据处理技术和神经网络模型，实现了对通信网络安全威胁的准确、智能评估，有助于提升网络的安全性和防御能力。

参考文献：

[1] 何贤德，王　磊，骆　骁. 一种卫星通信网络管理系统分布式部署方法［C］// 中国通信学会卫星通信委员会，中国宇航学会卫星应用专业委员会. 第十九届卫星通信学术年会论文集，2023：228－231.

[2] 梁　程. 卫星通信网络面临的安全威胁及防范分析［J］. 网络安全技术与应用，2023（3）：8－10.

[3] 江　铁，聂秀山，段芳敏. 卫星通信系统地面网络安全防御问题研究［C］// 中国通信学会卫星通信委员会，中国宇航学会卫星应用专业委员会. 第十八届卫星通信学术年会论文集，2022：19－25.

[4] 吴　巍. 6G 网络覆盖扩展的安全防护问题思考［J］. 无线电通信技术，2021，47（6）：732－739.

[5] KANG M，PARK S，LEE Y. A survey on satellite communication system security［J］. Sensors，2024，24（2897）：1－45.

[6] TEDESCHI P，SCIANCALEPORE S，PIETRO R D. Satellite-based communications security：a survey of threats，solutions，and research challenges［J］. Computer Networks，2022（216）：1286－1389.

[7] 焦利彬，霍永华，喻　鹏，等. 基于改进 BP 神经网络的网络态势评估方法［J］. 无线电工程，2021，51（6）：440－445.

[8] 曾辰熙，吴泉源，李爱平，等. 基于模糊层次分析的木马攻击效果评估技术研究［J］. 网络与信息安全学报，2016，2（7）：49－58.

[9] 高　翔，祝跃飞，刘胜利，等. 基于模糊 Petri 网的网络风险评估模型［J］. 通信学报，2013，34（s1）：126－132.

[10] 胡 楠，黄 玥，徐春玲，等. 基于模糊层次分析法的计算机网络安全评价探析 [J]. 通讯世界，2016 (9)：73－74.
[11] SAATY T L. How to make a decision：the analytic hierarchy process [J]. European Journal of Operational Research，1990，48 (1)：9－26.
[12] SAATY T L. Decision making with the analytic hierarchy process [J]. International Journal of Services Sciences，2008，1 (1)：83－98.
[13] 李雄伟，周希元，杨义先. 基于层次分析法的网络攻击效果评估方法研究 [J]. 计算机工程与应用，2005 (24)：157－159.
[14] 刘 进，王永杰，张义荣，等. 层次分析法在网络攻击效果评估中的应用 [J]. 计算机应用研究，2005 (3)：113－115.
[15] 吕 可，郑 威，赵严冰. 雷达对抗侦察装备作战能力的 ANP 幂指数评估方法 [J]. 火力与指挥控制，2016，41 (12)：59－63.
[16] 杨 欢. 基于云理论和 DEA 方法的炮兵轮式指挥车作战效能评估 [J]. 舰船电子工程，2012，32 (6)：27－30.
[17] KRIZHEVSKY A，SUTSKEVER I，HINTON G E. ImageNet classification with deep convolutional neural networks [C] // International Conference on Neural Information Processing Systems，Curran Associates Inc，2012：1097－1105.
[18] HOLLAND J H. Adaptation in natural and artificial systems：an introductory analysis with applications to biology，control，and artificial intelligence [J]. Quarterly Review of Biology，1992，6 (2)：126－137.
[19] ALSAFWANI N，FAZEA Y，ALNAJJAR F. Strategic approaches in network communication and information security risk assessment [J]. Information，2024，15 (6)：353.
[20] 廉新科，闫 卿. 基于攻击面的安全评估体系研究 [J]. 通信技术，2020，53 (10)：2567－2572.
[21] 张建廷，周万宁，晏谢飞，等. 基于指标隶属度和残差网络的海上目标多级威胁评估方法 [J]. 中国电子科学研究院学报，2023，18 (3)：213－220.
[22] 张博轩，王少博，赵天白，等. 基于对抗残差网络的复杂海况舰船目标类型识别技术研究 [J]. 无线电工程，2024，54 (10)：2355－2361.
[23] 陈路路，张建民，白 洁，等. 基于遗传算法和 ELM 神经网络的目标威胁估计 [J]. 无线电工程，2023，53 (7)：1719－1724.
[24] 苏 佳，杨泽超，易卿武，等. 基于遗传算法优化 BP 神经网络的 GNSS 干扰源定位技术 [J]. 无线电工程，2024，54 (5)：1175－1182.
[25] PANG J，LIU C. Network security evaluation based on improved genetic algorithm and weighted error backpropagation algorithm [J]. International Journal of Advanced Computer Science & Applications，2024，15 (5)：781－789.

(上接第 291 页)

[18] MEZIANI S，THOMAS M，ZAROUR D. Diagnosis of bearing defects by variational modes decomposition from vibratory and acoustic emission measurements [J]. International Journal of Vehicle Noise and Vibration，2019，15 (1)：21－41.
[19] YANG H，GAO L，LI G. Underwater acoustic signal prediction based on correlation variational mode decomposition and error compensation [J]. IEEE Access，2020，8：103941－103955.
[20] LIU L，CHEN L，WANG Z，et al. Early fault detection of planetary gearbox based on acoustic emission and improved variational mode decomposition [J]. IEEE Sensors Journal，2021，21 (2)：1735－1745.
[21] LI H D，XU Y，AN D，et al. Application of a flat variational modal decomposition algorithm in fault diagnosis of rolling bearings [J]. Journal of Low Frequency Noise，Vibration and Active Control，2020，39 (2)：335－351.
[22] CHEN X J，YANG Y M，CUI Z X，et al. Wavelet denoising for the vibration signals of wind turbines based on variational mode decomposition and multiscale permutation entropy [J]. IEEE Access，2020，8：40347－40356.
[23] HAO Y. Research on acceleration signal denoising of press slide based on variational mode decomposition and wavelet transform [C] // 2023 5th International Conference on Intelligent Control，Measurement and Signal Processing (ICMSP)，Chengdu，2023：887－890.
[24] LIU W Y，LIU Y Q. Optimizing VMD parameters and wavelet thresholding in speech denoising [C] //Greenville：2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC)，2021：500－503.
[25] LI D，LI M，YANG L，et al. Rolling bearing fault diagnosis in strong noise background based on vibration signals [J]. Signal，Image and Video Processing，2024，18 (2)：1295－1303.
[26] 王婷婷，李 方，霍雨佳，等. 基于 AO 优化 VMD-小波包的岩石破裂声发射信号去噪算法 [J]. 采矿与岩层控制工程学报，2023，5 (6)：82－95.
[27] QIN Z X，PAN D Z. Improved dual-center particle swarm optimization algorithm [J] Mathematics，2024，12 (11)：1698.
[28] 陈 祥，杨志强，田 镇，等. GA-VMD 与多尺度排列熵结合的 GNSS 坐标时序降噪方法 [J]. 武汉大学学报(信息科学版)，2023，48 (9)：1425－1434.
[29] 周东红，周建科，夏同星，等. 三参数小波变换自适应阈值压制地震数据高频随机噪声 [J]. 地球物理学报，2023，66 (5)：2095－2111.