doi：10.13413/j.cnki.jdxblxb.2024176

基于小生境遗传算法的网络入侵节点智能检测方法

王 建 刚
（西安石油大学 理学院，西安 710065）

摘要：为降低网络入侵的风险，提出一种基于小生境遗传算法的网络入侵节点智能检测方法. 首先，针对网络入侵的攻击行为进行聚合处理，利用双人攻防博弈模型分析网络的攻防状态，通过比对攻击与防御的效用强度，对网络的安全性进行全面分析，再根据分析结果，通过卷积神经网络实现对攻击源的定位. 其次，基于粗糙集理论，利用小生境遗传算法确定网络入侵节点检测的适应度函数，根据网络入侵节点智能检测规则，建立网络入侵节点智能检测模型，获得最终的检测结果. 实验结果表明，该方法可有效提升对入侵攻击源的定位准确性和入侵节点检测准确性，该方法检测结果的宏 F_1 分数大于 0.96，表明该方法可有效实现设计预期.

关键词：小生境遗传算法；网络入侵；入侵节点；粗糙集理论；适应度函数；入侵检测
中图分类号：TP393 **文献标志码：**A **文章编号：**1671-5489(2025)04-1099-06

Intelligent Detection Method for Network Intrusion Nodes Based on Niche Genetic Algorithm

WANG Jiangang
(*College of Science, Xi'an Shiyou University, Xi'an* 710065, *China*)

Abstract: In order to reduce the risk of network intrusion, the author proposed an intelligent detection method for network intrusion nodes based on niche genetic algorithm. Firstly, aggregation processing was implemented for the attack behavior of network intrusion, a two-person attack and defense game model was used to analyze the attack and defense status of the network. By comparing the utility strength of attack and defense, a comprehensive analysis of the network's security was carried out. Based on the analysis results, the localization of the attack source was achieved through convolutional neural networks. Secondly, based on rough set theory, the fitness function for network intrusion node detection was determined by using niche genetic algorithm. According to the intelligent detection rules of network intrusion nodes, an intelligent detection model for network intrusion nodes was established to obtain the final detection results. Experimental results show that this method can effectively improve the accuracy of locating intrusion attack sources and detecting intrusion nodes. The macro F_1 score of the detection results of this method is greater than 0.96, indicating that this method can effectively achieve the design expectations.

收稿日期：2024-04-22.
作者简介：王建刚(1977—)，男，汉族，硕士，讲师，从事最优化理论与算法的研究，E-mail：wangjg@xsyu.edu.cn.
基金项目：国家自然科学基金(批准号：11801441).

Keywords: niche genetic algorithm; network intrusion; intrusion node; rough set theory; fitness function; intrusion detection

随着网络信息技术的快速发展，网络安全挑战愈发严峻[1-2]，网络入侵事件呈现显著增长的趋势，因此，如何有效且精准地检测网络入侵节点已成为网络安全领域需要解决的主要问题之一. 传统网络入侵检测方法大部分依赖于固定的规则和模式，难以有效应对日益多变的网络攻击方法[3-4]. 而智能检测方法可采用机器学习和深度学习等技术完成对未知入侵行为的有效检测. 例如，马泽煊等[5]将WaveNet和BiGRU有效融合进行网络入侵检测，但该方法对较复杂的网络攻击检测准确度偏低. 陈晨等[6]通过PSOGWO算法对支持向量机(SVM)中的参数进行优化处理，获取最优检测模型，利用模型完成入侵检测，但该方法中的SVM对数据的分布和质量较敏感，尤其是数据较集中或出现异常值时，会影响SVM的性能，进而影响最终检测结果. 刘金硕等[7]通过联邦学习框架同时将自动编码模型的深度神经网络(DNN)作为通用模型，构建网络入侵检测模型进行检测，但该方法的收敛速度不理想，会影响最终的检测性能. Wang等[8]通过深度学习算法实现网络入侵检测，但该方法的检测结果准确性偏低. 为提高对网络入侵节点的检测准确性，本文结合小生境遗传算法，提出一种新的网络入侵节点智能检测方法.

1 网络入侵节点智能检测方法设计

本文首先通过聚合处理网络入侵的攻击行为数据，简化分析复杂度. 其次，利用双人攻防对弈模型深入分析网络的安全状态，比较攻击与防御的效用，为全面评估网络安全性提供依据. 再次，借助卷积神经网络精确定位攻击源，为后续的入侵节点检测提供关键信息. 在此基础上，结合粗糙集理论辅助处理数据，并利用小生境遗传算法优化检测过程，确定适应度函数，构建智能检测模型. 最后，通过该模型获得网络入侵节点的检测结果，为网络安全管理提供有力支持.

1.1 网络入侵攻击源定位

1.1.1 网络入侵攻击行为聚合处理

当网络遭受攻击时，需充分考虑其时空变化特性. 因此，本文用自回归系数法 ϕ 确定网络中的随机变量，通过对网络状态的动态分析，能更准确把握网络受攻击时的变化规律，从而更有效地应对各种攻击场景.

考虑到网络的实际特点，将网络行为分量表示为 $N(s,t_k)$，在网络各分簇中设定攻击行为的平均数量为 c，则网络入侵攻击行为聚合结果可表示为

$$x_k=\frac{\theta_s}{c}\times(\beta_s+N(s,t_k))+\kappa, \tag{1}$$

其中 β_s 表示网络攻击源相关函数，θ_s 表示网络攻击源短期时变过程，s 表示网络节点集合，κ 表示特定分布下的加性高斯白噪声.

1.1.2 网络攻防状态分析

网络中的近似形式状态方程为

$$x_{k+1}=f_{x_k}+\bar{\boldsymbol{E}}_kG, \tag{2}$$

其中 $\bar{\boldsymbol{E}}_k$ 表示网络中攻击源对应的特征矢量，f_{x_k} 表示状态方程，G 表示网络拓扑.

为有效简化聚合过程，在网络受到攻击后，设各链路出现数据丢失及发送错误的概率一致. 在设定时间段内，可将网络攻击源的聚合结果 x_k 表示为

$$x_k=b_s\times\frac{1}{u}\sum_{j=1}^{J}b_j, \tag{3}$$

其中 u 表示网络节点的数量，b_s 和 b_j 分别表示攻击源节点在设定时隙采集到感知数据的均值和方差，J 表示发送数据包集合的数量.

当网络遭受攻击时，数据丢失的风险急剧上升，显著削弱了网络的安全性和稳定性，严重影响了

整体网络的可信赖性. 为此，采取评估网络安全的方法判定网络的安全性. 若评估结果显示网络存在安全风险，则必须立即对网络攻击源进行精准定位.

本文利用双人攻防博弈模型对网络安全进行深度评估，将网络的安全防御和攻击行为设定为博弈主体. 在该模型中，假设攻击方从网络的某一特定节点发起攻击，攻击者攻击网络与防御者抵御攻击时各自的效用函数 τ_1 和 τ_2 定义为

$$\begin{cases} \tau_1 = (P_j^1 - \lambda) \times P_j^2, \\ \tau_2 = \lambda \times P_j^2 - g, \end{cases} \tag{4}$$

其中 P_j^1 和 P_j^2 分别表示第 j 处网络的安全漏洞和维度信息，λ 表示网络受到攻击时的正面影响，g 表示网络针对 p_j 处攻击选择第 k 个防御策略对网络产生的负面影响.

在此基础上，判断网络是否安全，若 $\tau_1 \leqslant \tau_2$，则说明网络处于安全状态；若 $\tau_1 > \tau_2$，则说明当前网络不安全，需要对网络攻击源进行定位.

1.1.3　网络攻击源定位

本文通过卷积神经网络实现对网络攻击源的定位. 在定位过程中，需有效解决网络中的大量非线性问题. 因此，采用 $f(x)$作为卷积神经网络的激活函数：

$$f(x) = \max\{0, x\}, \tag{5}$$

其中 x 表示卷积神经网络的输入样本，max 表示输入样本中的最大值. 将网络输出结果转换为多维矩阵的形式，通过多维矩阵进行卷积计算，表示为

$$\begin{cases} I_{\text{out}} = f\left(\dfrac{I_{\text{in}} - I_0}{2} + 1\right), \\ C_{\text{out}} = f\left(\dfrac{C_{\text{in}} - C_0}{2} + 1\right), \end{cases} \tag{6}$$

其中 C_{out}和 I_{out}分别表示卷积神经网络输出的宽度和高度，I_0，C_0 分别表示卷积核的高度和宽度，I_{in}，C_{in} 分别表示卷积层的高度和宽度.

在完成卷积处理后，直接将样本数据输入池化层中. 池化层处理中，大幅度降低了数据特征的维度，有效实现了数据的压缩和精炼. 经过池化层处理的数据被传递至全连接层，该层负责更深入地分析网络数据的类别特征，实现更细致的分类划分. 同时，该流程还推动了网络的正向传播，使整个网络能更高效地进行学习和推理. 不断重复上述操作，每完成一次迭代后，需计算其网络损失，同时判定其是否达到最小值. 损失函数 R 定义为

$$R = \sum_{y=1}^{n} [y\ln(d)(1-y)\ln(1-d)], \tag{7}$$

其中 y 表示网络预测输出值，d 表示网络期望输出值.

由于网络攻击源应源自相同位置，因此将式(7)中的损失函数设定固定值 1 作为判别标准，即 $R_{\min} = 1$. 一旦满足 $R = R_{\min}$的条件，网络即能迅速且准确地定位并直接输出攻击源数据. 若不满足该条件，则需启动反向传播机制，对网络的偏差量进行精确计算，并对连接权重进行求导调整，计算过程如下：

$$\begin{cases} \dfrac{\partial R}{\partial q} = \sum\limits_{x=1}^{n} (f(x) - y)x, \\ \dfrac{\partial R}{\partial \boldsymbol{\omega}} = \sum\limits_{x=1}^{n} (f(x) - y), \end{cases} \tag{8}$$

其中 q 和 ω 分别表示网络偏差量和连接权重. 通过式(8)进行反向传播，再利用式(7)进行正向传播，假设 $R_{\min} = 1$，则继续进行迭代计算；反之，则终止迭代，同时输出网络入侵攻击源定位结果，实现对网络攻击源的定位处理.

1.2　方法设计

在确定网络入侵攻击源位置后，基于粗糙集约简理论，利用小生境遗传算法精准地构建入侵检测

的适应度函数[9]，再确定检测规则，以检测规则为依据组建网络入侵节点智能检测模型，从而实现对入侵行为的精确检测.

在该过程中，粗糙集理论在处理不确定性和模糊性方面具有独特优势，其能描述并处理数据的粗糙性和不确定性，有助于更准确地识别网络入侵节点. 小生境遗传算法则可以在此基础上进行全局搜索和优化，通过选择、交叉和变异操作，找到最合适的网络入侵节点检测规则. 这种结合可提高网络入侵节点检测的准确性和效率，使检测结果更可靠.

为全面分析网络中的入侵数据，首先，将所有相关数据整合到一个统一的信息表中，并通过决策值与其对应的关系进行精确匹配[10]. 其次，为进一步提升检测的准确性和效率，引入辨识度矩阵进行细致的分类检测，以确保每种入侵行为都能得到精准识别并有效应对：

$$\psi(D_\theta \rightarrow E_t)=\frac{D_\theta \times E_t}{\boldsymbol{S}}, \tag{9}$$

其中 D_θ 表示策略参数变量，E_t 表示约简辨识度，$\boldsymbol{S}$ 表示识别检测阵列. 基于此，组建模糊判别矩阵 $\boldsymbol{H}^R$ 为

$$\boldsymbol{H}^R=H_{ij}^R \times \psi(D_\theta \rightarrow E_t) \times R, \tag{10}$$

其中 H_{ij}^R 表示模糊属性. 完成上述操作后，即形成初始网络入侵节点检测小生境遗传算法，步骤如下：

1) 输入决策表并进行辨识 CORE 计算.

2) 确定辨别矩阵.

3) 备选网络入侵属性信息.

4) 为构建粗糙集，引入小生境遗传算法进行离散化处理，进而获取最优解，操作步骤为：

① 筛选合适的样本数据输入到网络中，同时对全部样本数据进行离散化处理，形成网络入侵检测规则表；

② 对①得到的网络入侵检测规则表进行约简，获取最小属性规则集；

③ 如果计算的种群个体适应度满足设定终止条件，则输出规则；反之，则需进行选择等操作，直至其适应度取值满足终止条件时停止操作.

完成上述操作后，根据得到的网络入侵检测规则，给出满足输出需求的检测决策变量：

$$X=\begin{cases}\eta \times t(Z_k-\boldsymbol{H}^R), & \text{random}(0,1)=0,\\ \eta \times t(\boldsymbol{H}^R-Y_k), & \text{random}(0,1)=1,\end{cases} \tag{11}$$

其中 η 表示决策因子，t 表示进化次数，Z_k 和 Y_k 分别表示交叉因子和目标决策变量.

由目标决策变量可知，在网络入侵节点智能检测过程中易受变异算子影响形成检测误差. 为有效解决该问题，需先构建一个智能化的网络入侵节点检测模型，再用模型对网络入侵攻击信息进行精准评估. 在实际操作中，对原始网络入侵节点的分类至关重要，因此需先构建入侵检测向量. 为提升检测的准确性，采用极值理论构建概率密度分布函数，并确保该函数具有较强的鲁棒性. 根据以上分析，将模型的比例参数 r 定义为

$$r=\| h_j-l_j \| \times \zeta, \tag{12}$$

其中 h_j 和 l_j 分别表示网络入侵数据适配因子和变动因子，ζ 表示攻击样本对应的权重值. 根据上述参数组建网络入侵节点智能检测模型 V，通过模型完成检测：

$$V=1-\left(\frac{X-j}{\vartheta}\right)^{\mathrm{e}^{|r/\rho_s|}}, \tag{13}$$

其中 ϑ 表示网络内待检测节点数量，ρ_s 表示入侵概率权重.

2 实验及结果分析

为验证基于小生境遗传算法网络入侵节点智能检测方法的有效性，分别将其与文献[5]和文献[6]的方法进行实验比较. 搭建实验平台的相关参数如下：处理器为 Intel Core i5，操作系统为 Windows10，显卡为 GTX590，内存为 128 GB，Python3.7.6，Tensorflow2.0.0，Keras2.3.1，工具包

采用 Imbalanced learn.

2.1　网络入侵攻击源定位性能测试

分别在以下 4 种不同环境下进行网络入侵攻击源定位处理.

1）高负载环境：在该环境下，网络流量较大，包含大量正常请求和可能的入侵攻击. 模拟在网络负载较高情况下进行入侵节点智能检测，考察本文方法对检测性能的影响.

2）低负载环境：在低负载环境中，网络流量相对较少，入侵节点可能更难被检测到. 该环境下可以评估本文方法在低负载情况下的检测效果.

3）动态环境：该环境下网络流量、攻击类型、攻击强度等会不断变化，模拟网络环境的持续变化，测试本文方法在动态环境下的适应性和稳定性.

4）混合环境：在混合环境中，同时存在不同种类的网络流量和攻击，包括常见的 DDoS 攻击、SQL 注入攻击、恶意软件传播等. 通过在该环境下进行测试，可以评估本文方法对多样化攻击的适应能力.

不同网络测试环境下本文方法的入侵攻击源定位结果如图 1 所示. 由图 1 可见，采用本文方法可精准定位网络入侵攻击源所在位置，获取高准确率的定位结果，为后续网络入侵节点智能检测提供参考.

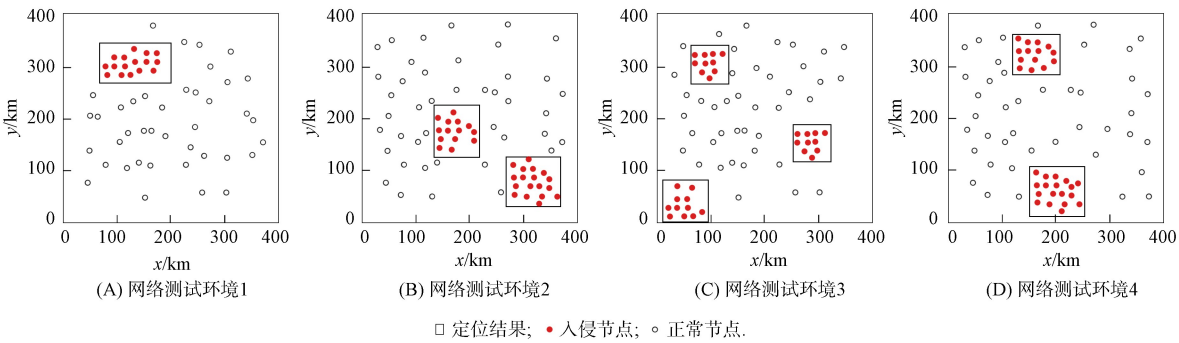

图 1　不同网络测试环境下本文方法的入侵攻击源定位结果

Fig. 1　Intrusion attack source localization results of proposed method in different network testing environments

2.2　网络入侵节点智能检测性能测试

实验选取宏 F_1 分数 macro-F_1 作为测试指标对各检测方法的整体性能进行分析，该指标定义为

$$\text{macro-}F_1=\frac{2\times F_{1_n}\times \text{Precision}\times \text{Recall}}{n\times(\text{Precision}+\text{Recall})},\tag{14}$$

其中 Precision 表示精确率，Recall 表示召回率，n 表示测试类别数，F_{1_n} 表示第 n 类的 F_1 分数. 宏 F_1 分数取值越接近于 1，说明检测性能越好. 图 2 为不同检测方法的宏 F_1 分数测试结果. 由图 2 可见，本文方法在宏 F_1 分数上表现更佳，数值始终大于 0.96，更接近于 1，表明了其在精确率和召回率方面的优越性. 而其他两种方法宏 F_1 分数偏低，显然存在优化和完善的空间.

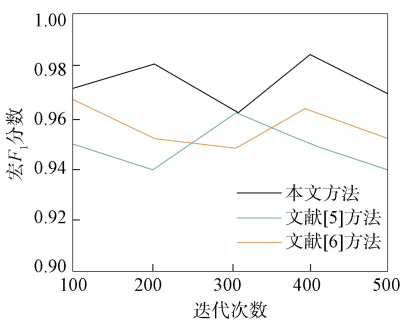

图 2　不同检测方法的宏 F_1 分数测试结果

Fig. 2　Macro F_1 score test results of different detection methods

分别采用 3 种不同方法进行网络入侵节点智能检测，实验结果如图 3 所示. 由图 3 可见，采用文献[5]和文献[6]方法进行入侵节点检测时，分别出现了误检以及漏检的情况，无法有效确保网络的安全运行. 而采用本文方法可精准检测入侵检测，充分验证了本文方法在入侵检测方面的优越性能.

综上所述，针对传统入侵检测方法存在的不足，本文提出了一种基于小生境遗传算法的网络入

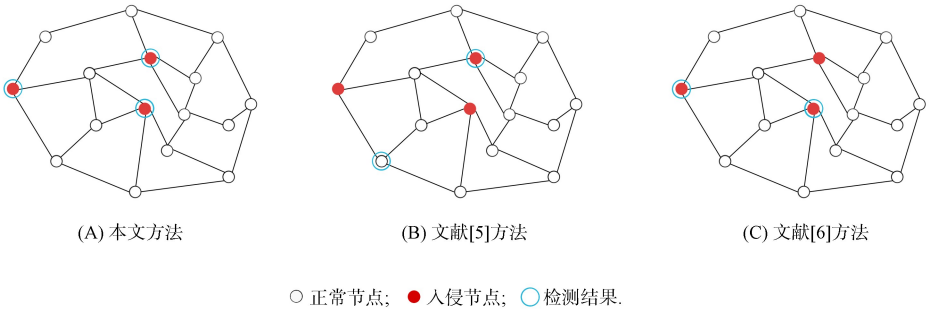

图3 不同方法的网络入侵节点检测结果

Fig. 3 Network intrusion node detection results of different methods

侵节点智能检测方法. 实验结果表明,该方法可有效且精准定位网络入侵攻击源,同时还可有效提升宏 F_1 分数,获取高准确率的入侵节点检测结果,有效确保网络的正常运行.

参 考 文 献

[1] 李晶,黄杰,朱国威,等. 基于自适应一维CNN的网络入侵检测方法[J]. 武汉大学学报(工学版),2022,55(11):1176-1185. (LI J, HUANG J, ZHU G W, et al. Network Intrusion Detection Method Based on Adaptive One-Dimensional CNN [J]. Engineering Journal of Wuhan University, 2022, 55(11): 1176-1185.)

[2] 胡向东,李之涵. 基于胶囊网络的工业互联网入侵检测方法[J]. 电子学报,2022,50(6):1457-1465. (HU X D, LI Z H. Intrusion Detection Method Based on Capsule Network for Industrial Internet [J]. Acta Electronica Sinica, 2022, 50(6): 1457-1465.)

[3] 马明艳,陈伟,吴礼发. 基于CNN-BiLSTM网络的入侵检测方法[J]. 计算机工程与应用,2022,58(10):116-124. (MA M Y, CHEN W, WU L F. CNN-BiLSTM Network Based Intrusion Detection Method [J]. Computer Engineering and Applications, 2022, 58(10): 116-124.)

[4] 李珊珊,李兆玉,赖雪梅,等. 基于概率神经网络的增量式入侵检测方法[J]. 计算机仿真,2022,39(9):476-482. (LI S S, LI Z Y, LAI X M, et al. Incremental Intrusion Detection Method Based on Probabilistic Neural Networks [J]. Computer Simulation, 2022, 39(9): 476-482.)

[5] 马泽煊,李进,路艳丽,等. 融合WaveNet和BiGRU的网络入侵检测方法[J]. 系统工程与电子技术,2022,44(8):2652-2660. (MA Z X, LI J, LU Y L, et al. Network Intrusion Detection Method Based on WaveNet and BiGRU [J]. Systems Engineering and Electronics, 2022, 44(8): 2652-2660.)

[6] 陈晨,刘曙,王艺菲,等. 基于PSOGWO-SVM的网络入侵检测方法[J]. 空军工程大学学报(自然科学版),2022,23(2):97-105. (CHEN C, LIU S, WANG Y F, et al. A Network Intrusion Detection Method Based on PSOGWO-SVM [J]. Journal of Air Force Engineering University (Natural Science Edition), 2022, 23(2): 97-105.)

[7] 刘金硕,詹岱依,邓娟,等. 基于深度神经网络和联邦学习的网络入侵检测[J]. 计算机工程,2023,49(1):15-21. (LIU J S, ZHAN D Y, DENG J, et al. Network Intrusion Detection Based on Deep Neural Network and Federated Learning [J]. Computer Engineering, 2023, 49(1): 15-21.)

[8] WANG W, JIAN S L, TAN Y S, et al. Robust Unsupervised Network Intrusion Detection with Self-supervised Masked Context Reconstruction [J]. Computers & Security, 2023, 128: 103131-1-103131-11.

[9] 黄学臻,翟翟,周琳,等. 基于轻量级密集神经网络的车载自组网入侵检测方法[J]. 电子技术应用,2022,48(7):67-73. (HUANG X Z, ZHAI Z, ZHOU L, et al. Intrusion Detection Method for VANET Based on Light Dense Neural Network [J]. Application of Electronic Technique, 2022, 48(7): 67-73.)

[10] 张安琳,张启坤,黄道颖,等. 基于CNN与BiGRU融合神经网络的入侵检测模型[J]. 郑州大学学报(工学版),2022,43(3):37-43. (ZHANG A L, ZHANG Q K, HUANG D Y, et al. Intrusion Detection Model Based on CNN and BiGRU Fused Neural Network [J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(3): 37-43.)

(责任编辑:韩 啸)