基于反向传播算法的网络安全态势感知方法

杜秋阳[1]
DU Qiuyang

摘 要 高级持续性网络威胁具有的复杂、隐蔽和持久等特征，网络安全态势影响因素无法有效量化，使得网络正向传播无法深入提取高层次特征，导致网络安全态势感知精度下降现象。对此，文章提出了基于反向传播算法的网络安全态势感知方法。首先，采用卡尔曼滤波器和自回归滤波技术处理时间序列数据；然后，考虑网络漏洞严重性和网络受攻击的影响程度作为态势影响因素进行量化分析；最后，将态势影响因素作为卷积神经网络模型的输入信息，结合反向传播算法构建残差卷积神经网络模型，将态势影响因素作为输入信息 ResNet 通过多层卷积操作，从复杂的网络流量数据中提取高层次特征，识别攻击行为的细微模式，并通过反向传播优化，ResNet 不断调整模型参数，实现网络安全态势感知。实验结果显示：采用反向传播算法的网络安全态势感知技术，有效提升了检测精度，减少了误差，并优化了模型的性能表现。

关键词 态势感知；攻击检测；网络安全；网络防护；反向传播算法

doi：10.3969/j.issn.1672-9528.2025.06.019

0 引言

随着物联网和数字化的迅速发展，网络规模持续扩大，拓扑结构愈发复杂，网络安全管理的挑战性和难度也随之加剧。导致难以及时探测恶意行为，也无法全面掌控网络安全态势。相比之下，网络安全态势感知技术致力于捕捉并分析那些能影响网络状态变化的安全因素，进行理解、展示，并预测短期内的安全发展趋势。该技术通过辨识、理解和预测网络中的各种活动，为网络安全管理提供了更为全面和深入的视角。

文献 [1] 运用 Marchenko-Pastur 模型和单环定律，对网络安全态势的特征值在随机矩阵中的分步实施了谱分析，揭示了网络在稳定与异常状态下的变换规律，从而实现了电网调度系统的网络安全态势感知。然而，Marchenko-Pastur 模型和单环定律适用于高维随机矩阵的谱分析，在低维数据或非随机数据中会出现失效现象。文献 [2] 则借助网络流量探测器和入侵检测探测器监测流量，分别捕获了流量的基础特征和恶意活动特征，利用属性提炼技术从各探测器中提取核心属性数据作为输入，判断了各种攻击类型，进而把握了整个网络的安全态势。然而，依赖探测器捕获的基础特征和恶

1. 湖北民族大学智能科学与工程学院 湖北恩施 445000

[16] AL-SHAERY A M, AHMED S G, ALJASSMI H, et al. Open dataset for predicting pilgrim activities for crowd management during hajj using wearable sensors[J]. IEEE access, 2024,12:72828 - 72846.

[17] KIM T, SATHYANARAYANA S D, CHEN S Q, et al. MoDEMS: optimizing edge computing migrations for user mobility[C/OL]//IEEE INFOCOM 2022 - IEEE Conference on Computer Communications.Piscataway: IEEE, 2022[2024-05-25].https://ieeexplore.ieee.org/document/9796680. DOI:10.1109/INFOCOM48880.2022.9796680.

[18] SUN X, ANSARI N. EdgeIoT: mobile edge computing for the internet of things[J]. IEEE communications magazine, 2016, 54(12): 22-29.

【作者简介】

王哲（1994—），男，河南南阳人，博士，副教授、硕士生导师，研究方向：计算机网络、智能通信与智能算法。

邹经（1994—），通信作者（email: 645163640@qq.com），男，江西宜春人，硕士研究生，研究方向：计算机网络。

葛丽娜（1969—），女，广西环江人，博士，教授、硕士生导师，研究方向：计算机网络与信息安全。

（收稿日期：2024-12-24 修回日期：2025-04-29）

意活动特征可能不足以全面反映网络安全态势，尤其是对于新型攻击或隐蔽攻击。文献 [3] 采用分区采集与降维运算数据预处理，去除电力线载波信号干扰因素。利用隶属关联矩阵挖掘网络安全要素特征，构建层次化 Markov 网络安全态势感知模型。利用 BW 算法寻找目标参数最优解，来确定感知目标点位置，缩短挖掘时间，提高感知精准度。然而，Markov 模型假设未来状态仅依赖于当前状态，无法捕捉网络安全态势的长期依赖关系。文献 [4] 在态势理解环节，采用层次分析法（AHP）结合改进的熵权法，对各评价指标进行权重分配，并通过加权平均计算得出大电网安全态势的综合评估值，从而实现对电网安全态势的全面量化分析。在态势预测环节，构建了深度神经网络（DNN）模型，利用其强大的非线性拟合能力，完成对大电网安全态势的未来趋势预测。然而，层次分析法和改进的熵权法在权重分配过程中可能存在主观性，影响态势评估的客观性。

反向传播（BP）算法作为支持神经网络高效训练的基本方法，其在网络安全态势感知中的应用潜力巨大。在上述研究的基础上，本文研究了基于反向传播算法的网络安全态势感知方法。

1 网络安全态势感知设计

1.1 网络安全态势影响因素量化

网络安全态势是一个综合性的整体，涵盖多种网络组成部分。网络数据通常来自多个来源（如日志、传感器、爬虫等），这些数据可能存在格式不一致、冗余或冲突。通过加权平均法整合多源数据，可以消除不一致性，确保数据的全面性和可靠性 [5]。采用加权平均法，基于数据源的数量及其对应的数值，进行多源数据的初步融合计算，具体公式为：

$$Q=\sum_{i>1}^{n}\left(a(i)\times z(i)\right) \tag{1}$$

式中：n 代表数据源数量；z 代表数据源数值；a 代表数据源的权重。

原始数据中可能包含噪声（如测量误差、异常值等），这些噪声会干扰分析结果。利用卡尔曼滤波器和自回归滤波技术对时间序列数据进行平滑处理，可以去除噪声，提高数据的准确性和稳定性：

$$q(w)=Q(w-1)+W_w\left(e(w)-\boldsymbol{R}(w)\right) \tag{2}$$

式中：w 代表时刻；e 代表输出数据的测量数值；W 代表数组协方差；$\boldsymbol{R}$ 代表数据测量向量。

基于上述步骤进行网络数据预处理，结果如图 1 所示。可以看出，经过加权合并与平滑处理后，可以有效去除网络数据的噪声和不一致性。

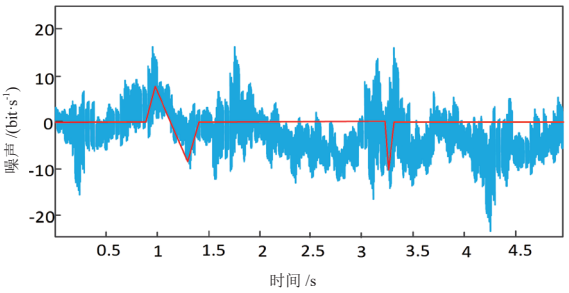

图 1 数据预处理结果

在此基础上，运用信息熵理论，针对离散随机变量，依据特定公式，开展信息熵的融合计算：

$$t=-\sum_{i>1}^{n}\partial\left(q_i(w)\right)\log_2\partial\left(q_i\right) \tag{3}$$

式中：∂ 代表数据空间的维度。

依据上述网络数据的信息熵指标，从网络安全状况的视角审视，剖析影响网络安全态势的关键要素。随着网络环境的日益复杂，一种高级持续性威胁的攻击方式逐渐崭露头角。相较于传统的网络攻击，APT 更加复杂、隐蔽和持久。往往针对特定的组织或机构，通过长期潜伏、逐步渗透的方式，窃取敏感信息或破坏网络系统 [6]。这种高级持续性威胁的存在，使得无法全面、准确地反映攻击行为对网络安全态势的影响。因为 APT 攻击往往不是单一的、突发的攻击事件，而是一系列精心策划、长期执行的攻击活动。因此，在考虑网络安全态势时，不仅要关注网络自身的漏洞严重程度，还要特别警惕网络受攻击的影响程度。基于此，本文对网络漏洞严重性的量化评估为：

$$u=\frac{\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}o_{ij}p_{ij}s_{ij}}{tE} \tag{4}$$

式中：o_{ij} 代表第 i 个主机上第 j 类漏洞的等级系数；p_{ij} 代表第 i 个设备对于网络中第 j 类漏洞的重要程度指标；α 代表网络中主机总数；s_{ij} 代表第 i 个主机中第 j 类漏洞的数量；t 代表信息熵；E 代表网络环境中漏洞总数；β 代表网络环境中漏洞的不同类别数。

根据上述网络漏洞等级的量化评估，本文将根据网络受攻击的影响程度，这是决定安全态势感知结果的关键因素，并据此进行安全态势量化分析，具体量化公式为：

$$L=\frac{\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\chi_{ij}p_{ij}\delta_{ij}}{uZ} \tag{5}$$

式中：u 代表网络漏洞的严重性量化值；Z 代表攻击的总次数；i 代表设备；j 代表攻击类型；χ_{ij} 代表第 i 个设备上 j 类型攻击的总次数；δ_{ij} 代表第 i 个设备上 j 类型攻击等级因子。

基于上述量化指标，将其作为安全态势数据融合模型的输入参数，为网络安全态势的感知与评估奠定可靠的基础 [7-8]。

1.2 基于反向传播构建残差卷积神经网络

本文设计的卷积网络通过反向传播计算损失函数的梯度，逐层调整网络参数（如权重和偏置），以最小化预测误差。ResNet 通过多层卷积操作，能够从复杂的网络流量数据中提取高层次特征[9]，识别攻击行为的细微模式。有效解决高级持续性威胁（APT）等复杂、隐蔽和持久网络攻击产生的威胁。

在该模型设计中，卷积层的输出网络安全态势影响因素状态规模由输入网络状态信息的大小、卷积核尺寸以及步长共同决定。通过对输入网络中各影响因素的安全态势量化结果 L、网络漏洞严重性的量化结果 u 进行加权平均，提取网络安全态势的关键影响因素状态 k。设定输入网络状态信息的尺寸为 $b \times c$，填充为 h，步长为 d，且卷积核大小为 $f \times f$。经过卷积操作后，各影响因素的量化结果将转化为网络安全态势影响因素状态 k，其计算公式为：

$$k = \frac{(b \times c) + 2h - f}{dLu} + 1 \tag{6}$$

在模型的训练过程中，传统前向传播过程的表达公式为：

$$y_1 = f_1 k\left(\eta_{(x_1)1} x_1 + \eta_{(x_2)2} x_2\right) \tag{7}$$

式中：x_1、x_2 代表输入的变量；$\eta_{(x_1)1}$、$\eta_{(x_2)2}$代表权重系数[10]。

在前向传播过程中，预测结果与真实值之间存在偏差，假设真实值为 ρ，则误差可表示为 $\sigma = \rho - y$。在此基础上，可进一步推导出每个神经元的误差值：

$$\sigma_1 = \eta_{(x_1)1} \sigma y_1 \tag{8}$$

在此基础上，本文采用反向传播算法对误差进行计算，进而推导出各神经元权重的梯度，并基于该梯度对权重进行优化调整。反向传播是训练神经网络的核心算法，其核心思想是通过计算损失函数的梯度，逐层调整网络参数（如权重和偏置），以最小化预测误差。权重的梯度计算公式为：

$$\eta'_{(x_1)1} = \eta_{(x_1)1} + \gamma \sigma_1 \frac{\mathrm{d}f(h)}{\mathrm{d}h} x_1 \tag{9}$$

式中：γ 代表速度参数，直接影响卷积残差神经网络模型的学习速度。

结合上述设计，通过对网络安全态势影响因素状态的一维离散函数执行卷积运算，可以推导出该卷积残差神经网络模型的表达式，具体公式为：

$$Y = k \times f\left(\sum \frac{\upsilon^*(Q,u,L)}{\eta'_{(x_1)1}}\right) + B \tag{10}$$

式中：(Q, u, L) 代表输入的网络状态信息；$f()$ 代表激活函数；$\upsilon()$ 代表卷积核；B 代表偏置项。

基于上述构建的模型，在网络安全态势感知过程中，网络流量数据中存在的冗余信息会降低判断的准确性，而该模型能够有效预筛选潜在的攻击数据[6]。因此，本文结合 PCA 技术进行特征提取与降维，从中选取最具代表性的特征子集。进一步，利用机器学习技术对节点进行聚类，将特征相似的节点归类为同一组，从而识别安全模式。最终，通过整合特征信息并应用安全态势评分函数，实现对网络安全状况的综合评估。

根据网络节点攻击概率的估算结果，对网络流量数据特征进行初步筛选，采用标准差作为衡量指标，评估网络流量的波动程度，具体计算公式为：

$$V = \sqrt{\frac{1}{\rho}\sum_{j>1}^{\rho}(Y - \partial)^2} \tag{11}$$

式中：V 代表波动系数。

在残差卷积神经网络模型筛选出的数据上进行特征提取后，利用 PCA 技术选取对安全态势感知具有显著价值的特征子集。基于这些特征子集，构建了网络流量特征数据的协方差向量，具体表达式为：

$$\theta = \boldsymbol{J} \times V(\Im)^2 \tag{12}$$

式中：$\boldsymbol{J}$ 代表特征向量；$\Im$代表对角数据向量。在完成特征子集的提取并构建相应的协方差向量之后，对多个特征进行融合处理，借助机器学习算法开展特征数据的节点聚类分析。依据聚类所得结果，构建了一套安全态势量化评估体系，用于对网络安全态势进行综合评价，其具体的量化计算公式为：

$$\mathrm{NUMBER} = \sum_{j>1}^{\rho} I(j) \times \theta(\psi) \tag{13}$$

式中：ψ 代表网络节点通信效率；I 代表特征的权重。最终输出结果即为安全态势感知结果。

2 实验测试与分析

2.1 实验准备

为检验基于反向传播算法的网络安全态势感知方法的有效性，进行了实验验证。实验环境中使用的开发平台采用 PyCharm x64，操作系统为 Windows 9 系统，编程语言选择 Python 3.8，同时集成了 TensorFlow 深度学习库。辅助工具包括 Pandas、Matplotlib 和 Scikit-learn 等。此外，实验数据来源于 KAD-SLM 数据集与实际校园网络环境采集的数据。KAD-SLM 数据集的数据分布具体记录如表 1 所示。

表 1 正常与攻击样本

数据类型		数据集记录	
		测试集	训练集
攻击	R2L	48 562	7 413
	COS	11 587	2 469
	U2R	565	2 940
	Probe	69	226
正常		64 898	9 482

网络安全态势感知的数据采集正在从依赖单一设备向整合多源设备转变，为确保网络态势评估的精准性，必须实现对网络各组成部分信息的广泛且多样化的收集。鉴于此，本

研究选取某高校校园网作为实例，深入探究网络安全态势感知，并进行相应的测试评估。在实验环节，将采用的反向传播算法与文献 [1] 和文献 [2] 中提及的算法进行对比测试，以实际验证这 3 种算法在安全态势感知方面的效能。

2.2 实验指标

收敛误差值用于衡量算法在训练过程中的稳定性，即算法输出与目标值之间的偏差。

$$CE=\frac{1}{T}\sum_{t=1}^{T}\left|y_t-\hat{y}_t\right| \tag{14}$$

式中：y_t 代表第 t 次迭代的目标值（即实际网络安全态势值）；$\hat{y}_t$ 代表第 t 次迭代算法预测的输出值；T 代表总迭代次数。

2.3 实验结果与分析

基于上述实验设定，本次测试首先对 3 种算法的实际安全态势感知效果进行分析，其测试结果如图 2 所示。

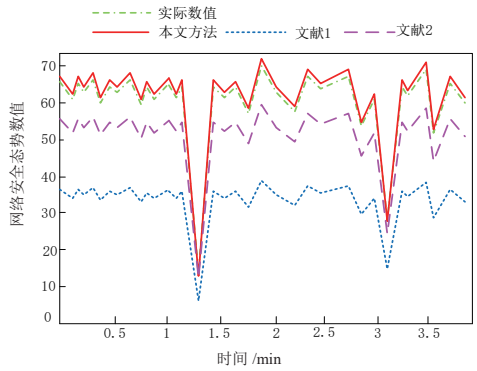

图 2 安全态势感知效果

由测试结果可知，反向传播算法在感知方面与实际网络安全态势保持一致，偏差不大，故能精确捕捉并体现网络安全的微小变动，有效屏蔽外界因素的干扰。

其次，对 3 种算法进行收敛误差值的测试，其结果如图 3 所示。

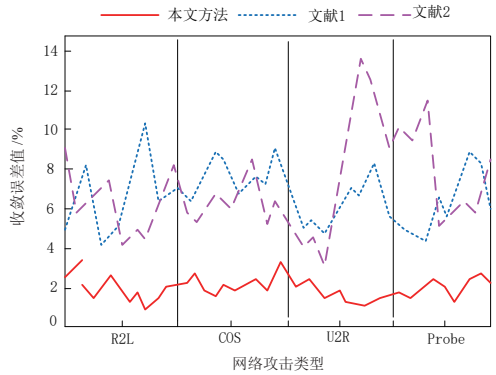

图 3 收敛误差值对比结果

根据以上结果，反向传播算法的收敛误差值在面对多种网络流量和攻击方式时均展现出良好的稳定性，并保持在较低水平。综上所述，基于反向传播算法的网络安全态势感知方法在实验研究中取得了显著的成果。该方法不仅提高了检测准确率，降低了误差率，同时优化了模型的性能表现。

3 结语

通过反向传播算法，成功实现对网络流量数据的深度学习与特征提取，有效识别出潜在的安全威胁与异常行为模式，为网络安全态势的实时监测与预警提供了强有力的技术支持。同时，算法的自适应学习特性确保了模型能够随着网络环境的变化而不断优化，增强了系统的适应性。尽管本研究取得了一定的成果，但网络安全是一个动态演进的领域，新的攻击手段与技术层出不穷。因此，未来的研究应继续聚焦于算法的改进与拓展，探索更多高级机器学习及深度学习技术在网络安全态势感知中的应用，以进一步提升系统的智能水平与响应速度。

参考文献：

[1] 朱文，江伟，周志烽，等．基于电网调度系统的网络安全态势感知方法研究 [J]. 电测与仪表 ,2024,61(7):21-27.

[2] 常利伟，刘秀娟，钱宇华，等．基于卷积神经网络多源融合的网络安全态势感知模型 [J]. 计算机科学 ,2023,50(5):382-389.

[3] 彭志超．基于改进 Markov 算法的电力线载波通信网络安全态势感知仿真研究 [J]. 电气自动化 ,2024,46(2):80-82.

[4] 于群，李浩，屈玉清．基于深度神经网络和内外部因素的大电网安全态势感知研究 [J]. 电测与仪表 , 2022, 59(2):16-23.

[5] 刘威，邓巍．基于 RBF 神经网络的主动配电网通信过程安全态势感知方法 [J]. 电网与清洁能源 ,2024,40(5):52-58.

[6] 吴昊，刘可．基于云计算的地震网络数据安全态势感知仿真 [J]. 计算机仿真 ,2024,41(4):330-334.

[7] 苏蕊，闫润珍，王亚婷．改进 ASON 网络架构的数据信息安全防攻破技术研究 [J]. 电子设计工程 ,2025,33(2):167-171.

[8] 高谨．基于大数据技术的网络安全态势感知平台设计 [J]. 软件 ,2024,45(5):43-45.

[9] 李岩．基于机器学习的网络安全态势感知关键技术探究 [J]. 教育教学研究前沿 ,2024,2(10):16-18.

[10] 辛亦轩，邓谦，刘姣，等．基于 5G 的智慧校园网络安全态势感知研究 [J]. 电信快报 ,2024(3):39-43.

【作者简介】

杜秋阳（1995—），男，湖北恩施人，硕士研究生，研究方向：网络安全。

（收稿日期：2025-02-19 修回日期：2025-06-10）