基于改进因子加权算法的智慧实验室通信网络安全态势感知方法

丁小娜[1,2] 王书静[1,2] 李国政[1,2] 李家良[1]
DING Xiaona WANG Shujing LI Guozheng LI Jialiang

摘 要 实验室环境复杂，存在网络信号干扰、设备故障等问题，导致在遭受网络攻击时难以对安全态势权重进行实时调整，使感知准确性较低，无法有效应对网络威胁。因此，文章提出了一种基于改进因子加权算法的智慧实验室通信网络安全态势感知方法。先明确安全态势指标，引入动态调整机制调整安全态势因子，并设计可信度函数，根据网络状态稳定性动态调整安全态势权重。然后，引入信号不确定度和能量函数，以量化感知要素的影响，并通过迭代计算条件熵定位关键感知要素。最后，评估攻击场景模块在通信网络架构的渗透程度与活跃状态，提取态势特征，并建立通信网络安全态势感知数学模型。实验结果表明，设计方法平均拟合度达 0.89，在测试时间为 150 min 时，预测态势值与实际值仅相差 0.02，验证设计方法在智慧实验室通信网络安全态势感知方法中具有更高的预测准确性，应用效果较好。

关键词 改进因子加权算法；智慧实验室；安全态势；感知等级

doi：10.3969/j.issn.1672-9528.2025.06.025

0 引言

随着信息技术的发展，智慧实验室的建设日益普及，其通信网络安全问题也更加凸显。传统的网络安全防护技术，难以应对复杂化的网络安全威胁。因此，发展网络安全态势感知技术，及时发现和应对网络安全威胁，成为保障智慧实验室通信网络安全的重要手段。

在网络安全态势感知领域，已有诸多研究成果。文献 [1] 通过量化网络节点的风险，实现对无线网络安全的态势感知。该方法受多种因素影响，导致准确性不足。文献 [2] 通过融合不同数据源，实现对网络安全态势的全面感知。但异构数据源的融合处理存在较大的难度，需解决数据格式、数据质量和数据安全等问题。文献 [3] 的贝叶斯网络融合人工智能领域的神经网络与贝叶斯统计学原理，实现通信网络信息安全态势感知。但贝叶斯网络要求所有传感器在抽象层次上依据贝叶斯概率进行响应输出，限制其准确性。文献 [4] 利用 RBF 神经网络在非线性系统建模中的优势，实现通信网络安全态势感知。但该方法在离散化处理时计算速率缓慢，导致时效性不高，难以获取网络安全态势。文献 [5] 通过构建分支结构对样本进行分类，实现对网络攻击数据的精准分类和预测。但若样本数据存在噪声，导致分类结果的准确性下降。

现有的网络安全态势感知方法在准确性方面仍存在不足，故提出运用改进因子加权算法的智慧实验室通信网络安全态势感知方法，以实现对网络安全态势的敏捷且有效的监测。

1 动态调整安全态势因子权重

传统的因子加权方式过于依赖经验值，无法根据实际情况动态调整权重。为改进这一点，引入动态调整机制，根据安全态势因子的实际表现调整安全态势因子权重 [6]。改进后的因子加权算法为：

$$r' = \sum_{i=1}^{n} \alpha_i f_i \tag{1}$$

式中：r' 为下一期的评估结果；f_i 为第 i 个因子的 t 期值；α_i 为第 i 个因子 t 期权重；n 为安全态势因子总数。

在此基础上，设计可信度函数，用于动态调整各安全态势因子的权重。当网络状态呈现不稳定，可信度函数会增大其方差，减小相关因子的权重；反之，当网络状态稳定且可信时，则提升因子的权重。可信度函数为：

$$T(x) = \frac{\alpha_i r_i}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{\frac{(x-\mu)^2}{2\sigma^2}} \tag{2}$$

1. 郑州西亚斯学院计算机与软件工程学院 河南郑州 451150
2. 河南省智能制造数字孪生工程研究中心 河南郑州 451150
[基金项目] 郑州西亚斯学院 2024 年度科研经费资助项目（2024XKB018）

式中：x 为安全态势权重的观测值；μ 为均值；σ^2 为方差；e 为自然对数的底数。

2 定位安全态势感知要素

为定位通信网络中的关键安全态势要素，选择最优安全态势权重进行分类，直至样本数据划分。并引入信号不确定度 $U(A)$，用于评估权重属性对感知要素的影响，公式为：

$$U(A)=\sum_{j=1}^{m} w_j \log_2 P_c T(x) \tag{3}$$

式中：w_j 为第 j 个感知要素的安全态势权重；m 为感知要素数量。

通过训练模型来优化态势感知的准确性。为实现这一目标，引入能量函数 E，作为衡量网络状态稳定性的工具。其公式为：

$$E(\theta,\boldsymbol{X})=\sum\left[w_i\cdot(x_i-\mu_i)^2\right]+\sum\left[\lambda_i\cdot f_i(\theta,\boldsymbol{X})\right]+C \tag{4}$$

式中：θ 表示模型的参数；$\boldsymbol{X}$ 表示网络状态向量；w_i 表示权重系数；μ_i 表示安全指标的期望值；$(x_i-\mu_i)^2$ 表示安全指标与期望值的平方差；λ_i 表示正则化系数；$f_i(\theta,\boldsymbol{X})$ 表示正则化项；C 表示常数项。通过调整模型参数 θ，可使模型更好地拟合实际网络状态，从而提高态势感知的准确性。

当能量函数达到最低点时，标志着网络达到了最为稳固的状态[7]，此时最大化利用输出权重属性来联合概率 P_θ 感知各个要素，其公式为：

$$P_\theta=\frac{U(A)}{Z(\theta)}\mathrm{e}^{-E(\theta,X)} \tag{5}$$

式中：$Z(\theta)$ 为配分函数，用于归一化概率分布。

为量化安全态势感知要素的重要性，计算每组联合概率的条件熵 H，其公式为：

$$H_k=\sum P_\theta \log_2 P_k\left(w_j\mid m\right) \tag{6}$$

3 建立通信网络安全态势感知数学模型

安全态势感知要素能确定网络安全监测重点，指导制定防护策略。基于此，分析关键要素，构建通信网络安全态势感知数学模型[8]。模型划分攻击场景模块，评估各模块在网络架构中的渗透与活跃状态。定义攻击场景活跃强度指数 $B(s)$ 为：

$$B(s)=\sum_{k=1}^{N} H_k a_k(s) \tag{7}$$

式中：N 为攻击场景模块的数量；H_k 为各模块的条件熵；$\alpha_k(s)$ 第 k 个模块在时刻 s 的活跃强度。

为建立通信网络安全态势感知数学模型，根据 $B(s)$ 提取态势特征。构建通信网络安全态势感知的数据集合 $y=[y_1,y_2,\cdots,y_t]$，集合中 y_t 是在 t 时间点所收集的观测信息，R_t 为平滑预测值，满足 $R_t=y_{t+1}$，即 t+1 时的预测数据，态势特征提取公式为：

$$T(y)=\sum_{k=1}^{N} B(s) y_t \log\frac{B(s)y_t}{B(s)R_t} \tag{8}$$

在提取特征后，建立通信网络安全态势感知数学模型，其公式为：

$$F=\sum_{l=1}^{M} S_l\left[T(y)\right] \tag{9}$$

式中：S_l 为第 l 个节点的安全态势评分。

4 实现智慧实验室通信网络安全态势感知

通信网络安全态势感知数学模型构建为智慧实验室的网络安全管理提供理论支持和技术手段。以构建模型为基础，对漏洞状态实施动态转化分析。设定状态转化系数 b，公式为：

$$b=\frac{\Delta VF}{\Delta q}\eta \tag{10}$$

式中：ΔV 为漏洞状态在时间 Δq 内的变化量；η 为转换效率因子。

以这一状态转化系数 b 为基础，为削弱局部误差对感知结果的干扰，利用改进因子加权算法简化态势值向量元素，公式为：

$$Z_d=\sum_{g=1}^{G} w_g F_g \tag{11}$$

式中：w_g 为第 g 个态势值的权重；F_g 为状态转化系数中第 g 个态势值的观测值；G 为态势值总数。

随后，将态势值向量元素扩展，得到矩阵 $\boldsymbol{O}$ 表达式为：

$$\boldsymbol{O}=Z_d(\boldsymbol{W}\boldsymbol{X}+B) \tag{12}$$

式中：$\boldsymbol{W}$ 为权重矩阵；$\boldsymbol{X}$ 为输入特征矩阵；B 为偏置项。

将状态转化系数与态势值向量元素相结合，对矩阵 $\boldsymbol{O}$ 进行优化，以提高通信网络安全态势感知数学模型的预测能力。采用公式表示最终输出网络安全态势感知结果：

$$\boldsymbol{O}'=\arg\min_{\boldsymbol{W},B}\sum_{v=1}^{V}\left\|\boldsymbol{y}_v-F(\boldsymbol{X}_v\boldsymbol{W}'+B')\right\|^2 \tag{13}$$

式中：$\boldsymbol{W}'$ 和 B' 分别为最优的权重矩阵和偏置项；V 为训练样本的数量；$\boldsymbol{y}_v$ 为第 v 个训练样本的真实态势值向量；$\boldsymbol{X}_v$ 为第 v 个训练样本的输入特征矩阵。

5 实验与分析

5.1 实验环境

本实验环境构建于某智慧实验室 Docker 平台，内部设置 8 台配置相近的通信服务器，各通信服务器均运行同一套安全监测系统。采用网络安全态势模拟软件实施多样化攻击，实验环境架构如图 1 所示。

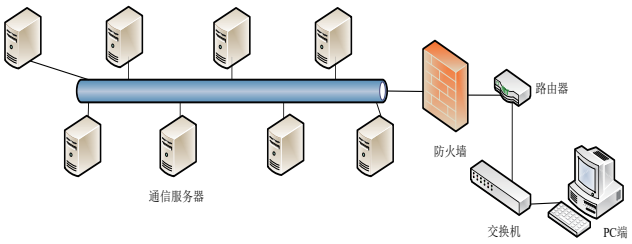

图 1 实验环境架构

在此实验环境下，服务器集群、升级版的防火墙设备、各类 PC 的定制化操作系统，以及分配的公网与私有 IP 地址，具体如表 1 所示。

表 1 实验环境配置表

序号	设备 / 组件	细节 / 数据
1	路由器	型号：Cisco ISR4331
2	交换机	型号：Huawei S5735S-28P-LI
3	PC（攻击端）	Win10、Ubuntu 20.04、macOS Catalina
4	服务器集群	Web 服务器（2 台，配置：Intel Xeon E-2124，16 GB RAM） 数据库服务器（1 台，配置：AMD Ryzen 7 3700X，32 GB RAM）
5	防火墙	型号：Palo Alto Networks PA-3200 配置：高级威胁防护，URL 过滤
6	PC（受害端）	Win7、CentOS 8、iOS
7	公网 IP 地址	攻击端：123.45.67.89，123.45.67.90，123.45.67.91 受害端：98.76.54.32，98.76.54.33
8	私有 IP 地址	攻击端：192.168.1.1-192.168.1.10 受害端：10.0.0.1-10.0.0.10

5.2 实验准备

基于优化后的因子加权算法，实验室准备通信网络安全态势感知方法的实验，构建通信网络。设计 6 款独特的代码攻击样本，针对预设的实验室通信网络结构实施攻击。攻击样本紧密围绕当前互联网安全领域的主流威胁，将评估并优化所提出的网络安全态势感知方法，如表 2 所示。

表 2 六类差异化的代码攻击场景

序号	攻击类型	攻击目标	预期影响
1	放大攻击	网关设备	导致网关设备过载，影响网络通信
2	僵尸网络	核心业务系统	获取控制权，窃取敏感数据
3	密码暴力破解	管理系统	破解登录密码，获得管理权限
4	Web 服务器漏洞	Web 服务器	控制服务器，执行恶意操作，如数据篡改、删除
5	潜伏式入侵	数据中心	长期窃取数据，破坏网络正常运行，造成重大损失
6	服务拒绝	云服务资源	导致云服务无法访问，影响业务连续性

构建包含 504 个样本的数据集，并挑选 30 个关键指标作为特征向量，向量均带有真实态势值。数据经过预处理后，制作态势预测所需的样本，并据此进行网络态势安全感知的初步实验。根据信息采集的时间顺序，设定 1.5 h 的预测周期，并分为 6 个时段，每时段为 10 min。在 504 样本选出 420 个作为训练集，剩余 84 个样本则为验证与测试。

为确保实验的全面性和对比性，采用相同的样本集，但应用文献 [1] 基于节点风险量化的无线网络安全态势感知方法、文献 [2] 基于异构数据源的信息网络安全态势感知方法、文献 [3] 基于改进贝叶斯网络的通信网络信息安全态势感知方法、文献 [4] 基于 RBF 神经网络的通信网络安全态势感知方法、文献 [5] 基于改进决策树的通信网络安全态势感知方法和本文的基于改进因子加权算法的智慧实验室通信网络安全态势感知方法进行测试。

5.3 拟合度结果分析

将上述 6 种方法的安全态势预测等级与实际安全态势等级进行对比，拟合度结果如图 2 所示。

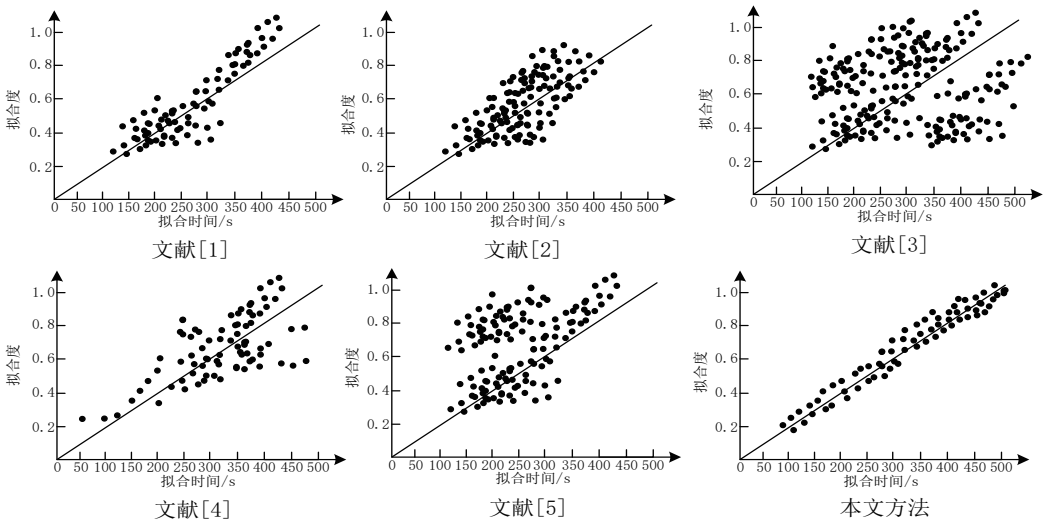

图 2 拟合度结果

根据图 2 可知，文献 [1] 的平均拟合度为 0.765，文献 [2] 的平均拟合度为 0.805，文献 [3] 的平均拟合度为 0.79，文献 [4] 的平均拟合度为 0.84，文献 [5] 的平均拟合度为 0.835。相比之下，本文方法的平均拟合度达 0.89，高于对比方法。结果表明，基于改进因子加权算法的智慧实验室通信网络安全态势感知方法，在提高预测准确性方面具有明显优势。随着样本数的增加，本文方法的拟合度呈现上升趋势，验证其准确性。

5.4 态势值结果分析

在实验室环境下，使用专业工具模拟攻击，以捕获实时态势值，公式为：

$$S(t)=\sum_{q=1}^{Q} w_q \frac{A_q(s)-A_q(s-1)}{\Delta s} \tag{14}$$

式中：Q 为攻击类型的数量；w_q 为第 q 种攻击类型的权重；$A_q(s)$ 和 $A_q(s\text{-}1)$ 分别为在时刻 s 和 s-1 第 q 种攻击类型的频率；Δs 为时间间隔。

对比包括本文方法在内的 6 种态势感知方法，态势值与实际值对比结果如图 3 所示。

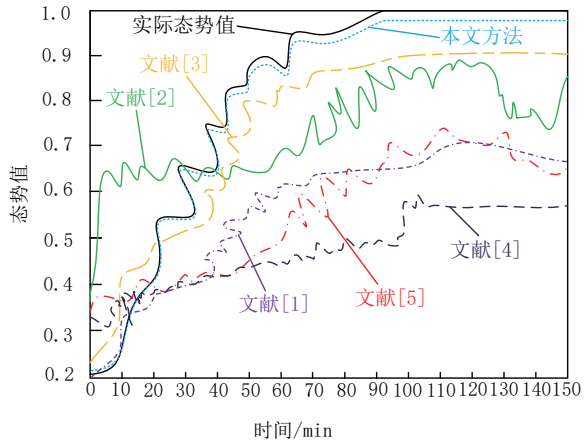

图 3 态势值对比结果

根据图 3 可知，随着测试时间的推移，实际态势值呈现逐步上升的趋势，最终趋于稳定。在对比各方法的预测态势值时，发现文献 [1-5] 的方法虽然在整体上能够反映出态势的变化趋势，但在数值上与实际态势值存在偏差。相比之下，本文方法所得态势值与实际值更为接近，偏差范围较小。具体而言，在测试时间为 150 min 时，实际态势值与本文方法的预测态势值仅相差 0.02。表明，本文方法在态势感知准确性方面具有较高的性能，能够更准确地反映实验室环境的通信网络安全态势。

6 结语

综上所述，本文提出的基于改进因子加权算法的创新方案，通过分析现有态势感知技术的局限性，融合多源异构信息，并引入因子加权算法，以提升态势感知的准确性和时效性。该方法不仅考虑网络流量的实时数据，还结合历史数据和专家经验，通过综合评估，实现对网络安全态势的全面感知。本研究不仅为智慧实验室的网络安全管理提供技术支持，也为其他领域的网络安全态势感知研究提供新思路。

参考文献：

[1] 李沈欣 . 基于节点风险量化的无线网络安全态势感知方法 [J]. 信息技术与信息化 , 2024(11): 149-152.

[2] 于继江 , 姜杰斯 , 董中平 . 基于异构数据源的信息网络安全态势感知方法 [J]. 自动化与仪器仪表 , 2024(8): 55-58.

[3] 李多 , 王铭 . 基于改进贝叶斯网络的通信网络信息安全态势感知方法 [J]. 长江信息通信 , 2023, 36(12): 173-175.

[4] 谢凯 , 代康 . 基于 RBF 神经网络的通信网络安全态势感知方法 [J]. 互联网周刊 , 2023(10): 82-84.

[5] 林立鑫 , 涂剑峰 , 喻燕华 . 基于改进决策树的通信网络安全态势感知方法 [J]. 信息与电脑 (理论版), 2023, 35(9): 223-225.

[6] 庄凯杰 , 刘锦旺 , 黄嘉铖 . 复杂环境下基于加权因子图的全源导航算法 [J]. 现代导航 ,2024,15(2):91-96.

[7] 王莹莹 , 刘秀朵 . 基于自适应加权算法的通信网络安全态势感知数学模型研究 [J]. 长江信息通信 ,2023,36(7):60-62.

[8] 陈兴望 , 辛阔 , 孙雁斌 , 等 . 基于加权朴素贝叶斯算法的调度指挥态势感知模块设计 [J]. 计算技术与自动化 , 2022, 41(3): 121-127.

【作者简介】

丁小娜（1986—），女，河南新乡人，硕士，副教授，研究方向：计算机应用、网络安全。

王书静（1999—），女，河南驻马店人，硕士，研究方向：网络信息安全。

李国政（1980—），男，山东潍坊人，硕士，高级工程师，研究方向：计算机应用。

李家良（2005—），男，河南驻马店人，本科在读，研究方向：计算机应用。

（收稿日期：2025-03-03 修回日期：2025-06-10）