基于节点风险量化的无线网络安全态势感知方法

李沈欣 [1]
LI Shenxin

摘 要 无线网络安全态势的潜在威胁具有隐蔽性，导致识别到的测试样本较少，因此设计一种基于节点风险量化的无线网络安全态势感知方法至关重要。通过实时采集无线网络中各节点的安全参数，运用先进的数据整合与分析技术，构建节点风险量化框架，实现安全态势信息采集。并经过细致筛选与提炼，提取出影响网络安全的关键要素，基于这些要素，构建无线网络安全态势感知模型，能够全面反映网络安全的实时状态与潜在威胁。最终，计算风险等级实现对无线网络安全态势风险的精准感知。实验结果表明，在识别网络处于 1 级安全和 2 级较安全状态方面，设计方法分别识别出 22 和 35 份样本，高于其他两种方法，证明基于节点风险量化的无线网络安全态势感知方法，在整体识别效果和应对不同安全态势的能力上均表现出色，在实际应用中具有优势。

关键词 节点风险量化；风险特征；无线网络；安全态势；感知要素

doi：10.3969/j.issn.1672-9528.2024.11.035

0 引言

无线网络因其开放性和灵活性，面临多种安全威胁，如 DDoS 放大攻击、僵尸网络协同入侵、Web 应用 SQL 注入以及高级持续性威胁（advanced persistent threat，APT）等。这些不仅威胁到网络系统的稳定运行，还可能造成数据泄露、财产损失乃至国家安全风险。因此，如何有效监测、预警和防御无线网络中的安全威胁，成为当前网络安全领域亟待解决的重要问题。

回顾相关文献可知，文献 [1] 提出了基于云计算的无线传感网络安全态势感知方法，该方法利用云计算技术采集和分析无线传感网络中的安全数据，通过海量信息的处理与辨识，提高了安全威胁检测的准确率；文献 [2] 则设计了基于改进贝叶斯网络的通信网络信息安全态势感知方法，通过构建改进贝叶斯网络模型，提取通信网络中的安全态势感知要素，实现了对网络信息安全态势的精准预测和评估，在一定程度上提高了态势感知的准确性和实时性。然而，这些方法在面对高度复杂和隐蔽的 APT 攻击时，具有一定局限性，在这一背景下，基于节点风险量化的无线网络安全态势感知方法应运而生，节点风险量化通过收集节点的多维度数据，运用先进的数据分析与机器学习技术，构建出能够准确反映节点安全状况的风险评估模型。这一模型能够动态性计算每个节点的风险值，该值综合了节点自身安全状况及其在网络环境中可能遭受的威胁程度 [3]，为网络管理员提供了一个直观、量化的安全风险视图。该方法不仅提高了态势感知的准确性和实时性，还能够实现对网络安全的动态监测和预警。

1 基于节点风险量化采集无线网络安全态势感知信息

通过实时采集无线网络中各节点的安全参数，运用先进的数据整合与分析技术，构建节点风险量化框架，该框架结构如图 1 所示。

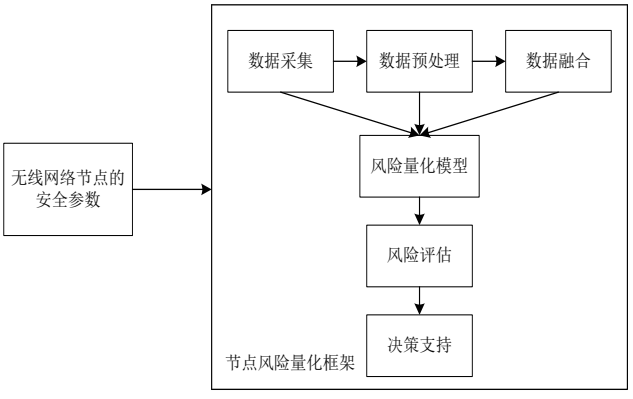

图 1 节点风险量化框架

在无线网络中风险节点的量化过程中，为了综合考量网络安防部署的稳固程度与各个节点潜在漏洞对潜在入侵攻击成功概率的影响，通过风险量化模型整合各入侵节点的风险态势值，以此来计算并反映整个无线网络的综合入侵风险态势。风险态势值计算公式为：

1. 中国刑警学院基础部 辽宁沈阳 110854

$$R=\sum_{i=1}^{M}w_iR_i \tag{1}$$

式中：R_i 表示第 i 个节点的原始风险值，w_i 表示第 i 个节点对应的权重，M 表示节点总数。

风险态势值即为无线网络安全态势感知的核心信息，是对当前无线网络安全状态的一种综合量化评估。初步采集的信息纷繁复杂，且往往包含大量冗余数据。为提升后续分析处理的效率与准确性，需对原始数据集进行精心预处理。此过程基于节点风险量化，引入权重因子 $\beta \in [0,1]$，针对每个节点的风险态势值进行加权求和，计算公式为：

$$Q(N)=\sum_{i=1}^{M}\beta R \tag{2}$$

式中：N 表示整个无线网络系统。经过上述预处理流程，数据集被赋予了集成化与一致性的特质，确保了数据在格式、结构和内容上的高度统一。

这一转变不仅优化了数据的存储与访问效率，还深度剖析无线网络安全态势的细微特征 [4]，构建出感知信息的多维度分布模型，其数学表达式为：

$$S=f\left[Q(N),R,D\right] \tag{3}$$

式中：f 表示调整函数，D 表示信息挖掘所得的关联分布集。

2 提取无线网络安全态势感知要素

在提取无线网络安全态势感知要素时，引入了基于 Internet 控制报文协议（internet control message protocol，ICMP）的扩展字段，在 ICMP 回显请求 / 应答的数据负载中嵌入 4 字节的时间戳 [5] 与校验和，以此增强数据包的唯一性与时效性。通过 DPDK 库，定制化地生成并发送伪造的 ICMP 应答包，其中应答源地址随机化模拟不同主机，以增强隐蔽性。同时，部署一个高效的事件驱动模型来捕获并分析网络流量，结合内存映射文件与数据库索引优化技术，有效管理伪造应答记录与实时数据包，减少 I/O 开销。该机制下，将无线网络安全态势感知信息作为输入，则：

$$P(t)=\left[S_1(t),S_2(t),\cdots S_n(t)\right] \tag{4}$$

式中：t 表示特定感知区间，$S_1(t)$, $S_2(t)$,…, $S_n(t)$ 表示无线网络安全态势感知信息集合。

选择一个合适的时间窗口 $[t_1, t_2]$，在这个窗口内对输入信号 $P(t)$ 进行采样，得到离散信号样本 P_1, P_2,…, P_n，计算 $P(t)$ 的平均功率方差来间接评估其不确定程度，表示为：

$$P_{[t_1,t_2]}=\sqrt{\frac{1}{n-1}\sum_{j=1}^{n}\left(P_j-\frac{1}{n}\sum_{k=1}^{n}P_k\right)^2} \tag{5}$$

式中：P_j 表示输入信号 $P(t)$ 在时间窗口 $[t_1, t_2]$ 内通过采样得到的第 j 个样本值，P_k 表示输入信号 $P(t)$ 在时间窗口 $[t_1, t_2]$ 内通过采样得到的第 k 个样本值。

在提取无线网络安全态势感知要素机制中，架构主要划分为感知层、分析单元与决策层 [6]。感知层负责采集输入信号 $P(t)$ 的不确定程度；分析单元则对这些不确定程度进行深度处理，识别潜在威胁与安全态势；决策层则基于分析结果，输出相应的安全策略与应对措施。此过程中，计算信息增益数值，公式为：

$$G=-\sum_{i}P_{[t_1,t_2]}\log_2 p \tag{6}$$

式中：p 表示数据集中危险样本所占的比例。

信息增益越大，说明数据集的不确定性减少得越多，即无线网络安全态势感知要素对于区分不同安全态势的贡献越大，无线网络安全态势感知要素，表示为：

$$Y=GT_k\times T_{P(t)} \tag{7}$$

式中：T_k 表示无线网络安全态势感知要素特征矢量，$T_{P(t)}$ 表示为输入信号 $P(t)$ 的输出矢量。

因此，在构建无线网络安全态势感知模型时，可以优先考虑那些信息增益较高的特征矢量。

3 构建无线网络安全态势感知模型

在构建无线网络安全态势感知模型时，将无线网络安全态势感知要素中的关键威胁源细分为多个攻击向量单元，每个单元代表一类具体的网络攻击手段。通过评估这些攻击向量单元在无线网络结构中的分布与活跃度，采用空间维度上的感知技术 [7] 来增强数据传输的安全性。具体地，定义攻击向量活跃度指数 $A(t)$ 为：

$$A(t)=\alpha I(t)+\gamma F(t) \tag{8}$$

式中：$I(t)$ 表示攻击向量对网络安全的影响程度；$F(t)$ 表示攻击发生频率；α、γ 表示权重系数，用于调整影响程度和频率在活跃度评估中的相对重要性。

在构建无线网络安全态势感知模型的过程中，本文创新性地引入了风险量化评估机制，通过定义风险最小化目标函数来构建模型。该目标函数与网络中各节点的安全态势评分紧密相关，具体地，采用数学公式表示为：

$$L=\left[\varphi VA(t)+\delta UA(t)\right] \tag{9}$$

式中：V 表示脆弱性评分；U 表示暴露程度评分；φ、δ 表示权重因子，用于调节脆弱性和暴露程度在总体风险计算中的相对重要性。

通过最小化目标函数 L，找到一种最优的安全策略，使

得在给定网络环境下，整体安全风险达到最低。该策略能有效降低节点的脆弱性，减少威胁的暴露面，同时提高安全响应的效率和准确性。以构建无线网络安全态势感知模型，其公式为：

$$H=\frac{1}{N}LA(t)\arg\mu(a\mid X) \tag{10}$$

式中：$\mu(a|X)$ 表示在特征类型 X 的前提下，威胁感知向量 a 的条件熵。

无线网络安全态势感知模型的核心逻辑聚焦于实时反馈机制。在数据流持续穿梭于网络架构的每一层级时，该模型迅速捕捉并分析服务器、网络协议层及终端设备的实时安全状态。通过精密算法，模型精准识别潜在的安全威胁与漏洞，动态评估风险等级。一旦关键风险指标被明确界定，将即时触发优化策略，迭代过程则聚焦于优化而非停滞，直至得到高效、精准的无线网络安全态势感知模型。

4 实现无线网络安全态势风险感知

在成功构建无线网络安全态势风险感知模型后，需融合三个核心动态维度：网络环境动态性、攻击行为演进性及系统脆弱性演变，进行全面而细致的分析。

首先，定义网络安全态势风险为一系列动态因素的函数，具体可表达为：

$$W=f(C_1,C_2,C_3) \tag{11}$$

式中：C_1 表示网络环境动态性，C_2 表示攻击行为的演进 [8]，C_3 表示系统脆弱性的演变。

在无线网络安全态势风险感知的过程中，鉴于执行策略的潜在风险性，为确保系统负载与实时态势波动相匹配，需维持风险等级评估的稳定性。为此，引入动态调整因子，将风险等级计算结果表达为：

$$Z=\sum_{m=1}^{M}\frac{bm\theta}{\sqrt{W}} \tag{12}$$

式中：m 表示动态因素数量，b 表示当前风险等级，θ 表示即时风险分数。

根据以上过程，实现无线网络安全态势感知。

5 实验测试分析

为了验证所提出的基于节点风险量化的无线网络安全态势感知方法的实际效果并评估其性能表现，设计一套在特定实验环境下实施的验证方案。该实验环境配置为 Windows 8 操作系统，辅以 8 GB 的内存资源，以确保实验条件的一致性和充分性。此次实验所构建的具体实验环境布局，如图 2 所示。

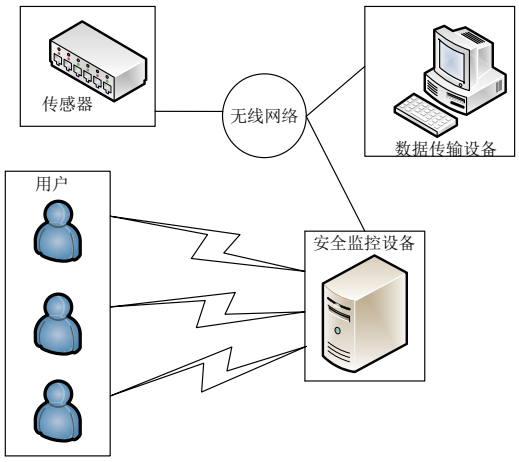

图 2 实验环境布局

为全面检验基于节点风险量化的无线网络安全态势感知方法的性能，策划如表 1 所示的六类差异化代码攻击场景，涵盖当前互联网中频发的安全威胁，DDoS 放大攻击、僵尸网络协同入侵、暴力破解密码库、Web 应用 SQL 注入、高级持续性威胁（APT）渗透及拒绝服务（DoS）变种。

表 1 六类差异化代码攻击场景

序号	攻击类型	描述	攻击目标
1	DDoS 放大攻击	利用公共 DNS 服务器等反射机制，放大攻击流量	无线网络带宽与服务器资源
2	僵尸网络协同入侵	控制大量被感染的计算机，发起协同攻击	网络中的关键节点与服务器
3	暴力破解密码库	尝试所有可能的密码组合，破解用户账户	用户账户系统
4	Web 应用 SQL 注入	通过 Web 表单提交恶意 SQL 代码，控制数据库	Web 服务器及其后端数据库
5	高级持续性威胁（APT）渗透	长期潜伏，逐步渗透并窃取敏感信息	网络深层架构及敏感数据存储
6	拒绝服务（DoS）变种攻击	消耗目标系统资源，使其无法正常提供服务	无线网络设备、服务器及应用程序

在筹备基于节点风险量化的无线网络安全态势感知方法实验时，规划了为期一周的密集测试周期，将每天细分为 30 个时段，总计 210 个观察点。为了提升模型训练的有效性与泛化能力，按照非连续间隔（如 1~7, 3~10, …, 199~205）的方式，从 210 个时段中精选出 180 个时段作为训练集，剩余的 30 个时段则作为独立的验证集，用于评估模型在未知情境下的表现。

对于实验中攻击类型进行的风险等级划分，制定了更为细致的五个层级（见表 2），以精确反映网络安全的动态变化。

表 2 无线网络安全态势危险等级划分

危险等级	范围值	包括攻击类型	描述
高度危险	[0.90, 1.00]	DDoS 放大攻击、Web 应用 SQL 注入、高级持续性威胁（APT）渗透、拒绝服务（DoS）变种攻击	网络核心受损，服务全面中断
中度危险	[0.70, 0.90)	DDoS 放大攻击、僵尸网络协同入侵、Web 应用 SQL 注入、拒绝服务（DoS）变种攻击	关键资产受损，多数接入点与服务端口失效
一般危险	[0.50, 0.70)	僵尸网络协同入侵、暴力破解密码库	网络性能下降，部分节点通信受阻
轻度危险	[0.30, 0.50)	暴力破解密码库	零星设备受侵，端口偶发异常
安全	[0.00, 0.30)	无	网络运行平稳，无显著安全威胁

针对 100 份测试样本进行了详尽的性能评估，随后依据既定的等级划分标准，将这些测试结果细致地归类至相应的安全态势等级中。为了确保实验结果的客观性和可比性，采用同一套样本集，并引入了 2 种不同的态势感知方法进行对比分析：文献 [1] 云计算方法和文献 [2] 改进贝叶斯网络方法。在此基础上，对每种方法的识别效果进行了量化对比，实验结果如图 3 所示。

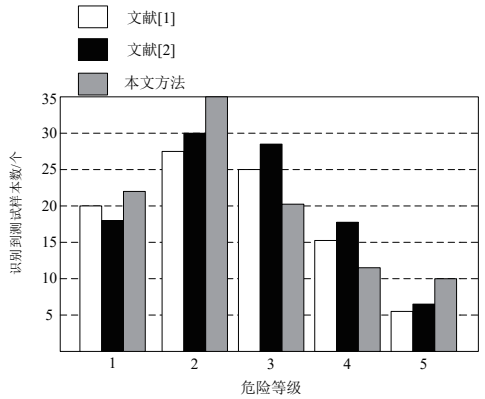

图 3 实验结果

根据图 3 可知，本文方法在处理 100 份测试样本时，识别网络处于 1 级安全和 2 级较安全状态方面，分别识别出 22 和 35 份样本，高于其他两种方法，这表明其在准确判定网络安全态势的基线水平方面表现更佳。在 3 级中等风险和 4 级较危险的识别上，虽然三种方法各有千秋，但本文方法通过精准量化节点风险，有效减少了误判和漏判，使得在需要特别关注的安全风险区间内，其识别结果更为可靠。在识别最为紧急和危险的 5 级态势时，本文方法识别出了 8 份样本，略高于其他两种方法，这证明了其在极端情况下能对于网络安全威胁快速响应。

6 结语

在无线网络安全领域，基于节点风险量化的态势感知方法为提升网络安全防护水平提供了有力支持。通过精准量化节点风险，得以全面、动态地把握网络安全态势，为制定有效防御策略提供科学依据。未来，随着技术和应用的不断深入，相信该方法将在保障无线网络安全方面发挥更加重要的作用，为构建安全、可信的网络环境贡献力量。

参考文献：

[1] 蔡斌 . 基于云计算的无线传感网络安全态势感知方法 [J]. 信息与电脑 (理论版), 2023, 35(24): 206-208.

[2] 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.

[3] 孙明炬 , 林冬 , 古冉 , 等 . 基于 RM-K-means 的储气库全生命周期风险量化分级评估方法 [J]. 科学技术与工程 , 2024, 24 (17): 7455-7461.

[4] 骆晨 , 冯玉 , 吴凯 , 等 . 多源大规模电网的多阶攻击风险感知量化和防御技术 [J]. 科学技术与工程 , 2023, 23(30): 12976-12984.

[5] 刘凯 , 宫旻 , 李晓峰 , 等 . 基于无线传感器网络的智能配电网安全态势感知方法 [J]. 电子设计工程 , 2023, 31(12): 142-146.

[6] 李芳 . 无线通信网络安全态势识别方法研究 [J]. 电子技术与软件工程 , 2022, 16(5): 41-44.

[7] 高贯银 , 曹京卫 , 余思阳 , 等 . 基于模糊综合评价理论的网络安全风险量化评估方法研究 [J]. 邮电设计技术 , 2023, 39(8): 71-74.

[8] 严康 , 陆艺丹 , 覃芳璐 , 等 . 配电网用户侧异构电力物联设备网络风险量化评估 [J]. 电力系统保护与控制 , 2023, 51(11): 64-76.

[9] 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.

[10] 李泽慧 , 徐沛东 , 邬阳 , 等 . 基于大数据的网络安全态势感知平台应用研究 [J]. 计算机应用与软件 , 2023, 40(7): 337-341.

【作者简介】

李沈欣 (1971—), 男, 辽宁沈阳人, 本科, 中级职称, 讲师, 研究方向：实验室管理及安全。

（收稿日期：2024-08-06）