

基于时空双模态的电力网络弹性安全态势感知策略

周轶喆¹, 朱贤伟¹, 胡文杰¹, 吴天杰¹, 陈 磊², 从 宇³, 王冰茹⁴

(1. 国能浙江北仑第一发电有限公司, 宁波 315000; 2. 浙江移动数智科技有限公司宁波分公司, 宁波 315000;
3. 北京科技大学自动化学院, 北京 100083; 4. 北京科技大学计算机与通信工程学院, 北京 100083)

摘 要: 5G 风筝专网作为 6G 场景化移动通信的核心理念, 致力于应对电力行业中终端高频移动、拓扑动态重构与业务低时延保障等实际问题。为解决 5G 风筝专网在高移动性与弹性拓扑环境中面临的安全态势感知精度不足及适应性较弱的问题, 本文提出一种基于时空双模态的电力网络弹性安全态势感知方法。通过采集核心特征数据, 构建多源输入向量; 采用长短期记忆(Long short-term memory, LSTM)网络进行时序异常检测, 并结合孤立森林算法识别空间异常, 以此融合生成增强特征矩阵。进一步引入二分 K-means 聚类算法与动态权重调整机制, 通过自适应优化特征权重, 实现对稳定、脆弱和威胁三级安全态势的精确划分。最后借助加权主成分分析实现降维可视化。仿真实验结果表明, 该方法能够有效响应网络状态变化, 在不同场景下的态势判别准确率得到提升, 为 5G 风筝专网的安全运维提供了可靠支撑。

关键词: 5G 风筝专网; 时空双模态; 安全态势感知; 弹性适配; 异常检测

中图分类号: TN929.5

文献标志码: A

引用格式: 周轶喆, 朱贤伟, 胡文杰, 等. 基于时空双模态的电力网络弹性安全态势感知策略[J]. 数据采集与处理, 2026, 41(5): 1548-1560. ZHOU Yizhe, ZHU Xianwei, HU Wenjie, et al. A spatiotemporal dual-modal-based strategy for elastic security situation awareness in power networks[J]. Journal of Data Acquisition and Processing, 2026, 41(5): 1548-1560.

引 言

随着 5G 通信技术在电力行业等关键基础设施领域的深度落地, 下一代 6G 通信技术的前瞻性研究已成为学术界与工业界的核心探索方向^[1]。目前面向 5G-A 特征的风筝专网深度赋能电力系统的数字化转型, 其高移动性适配、弹性拓扑调整等技术方向的探索, 不仅是应对当前电力生产控制需求的务实响应, 更是 6G 场景化弹性安全理念在电力行业的初步实践, 为后续 6G 技术深度融入远程精准操控、全域巡检协同等核心业务奠定了关键基础^[2]。5G 风筝专网凭借其超大带宽、超低时延与海量连接的技术优势, 已成为支撑电力、交通等关键行业数字化转型的核心基础设施。在电厂场景中, 电厂生产控制大区现有态势感知平台积累了大量历史安全数据, 而一体化安全管理平台则汇聚了设备状态、威胁情报、安全事件和网络流量等核心安全要素, 二者为构建全局化的网络安全态势感知体系提供了关键数据基础。5G 风筝专网为生产控制大区的远程监测、智能巡检及协同调度等业务提供了灵活、高效的通信保障, 推动了生产方式向更加智能化、网络化的方向演进。

然而, 5G 风筝专网的高移动性与弹性拓扑特性, 使传统网络安全态势感知方法面临显著的适配难题^[3]。传统的网络安全态势感知体系多沿用固定网络的感知逻辑, 无法适配专网的特殊架构与场景需

求,难以形成跨5G风筝专网、安全接入区与生产控制大区的统一、实时的安全态势视图。具体而言,现有方案在实际应用中面临三大核心挑战:一是终端移动过程中容易产生非安全类的异常值,如信号衰减导致的设备状态临时降级,这些干扰数据混入安全特征后易导致安全态势被误判;二是传统算法如K-means聚类算法依赖固定初始质心,在设备状态、网络流量等特征频繁波动时易导致算法陷入局部最优,出现稳定态势、脆弱态势和威胁态势的边界模糊等问题,在生产控制场景中可能带来误判风险;三是传统方法采用固定特征权重,但5G风筝专网存在动态场景切换,不同场景下影响态势的核心特征不同,固定权重无法适配场景变化,导致感知精度下降。因此,如何有效融合电厂系统现有的历史安全数据与实时安全要素,构建一个适应5G风筝专网特性的网络安全态势感知模型,成为当前电厂安全运维亟需解决的关键问题。

网络安全态势感知领域经过多年发展,已形成较为完善的理论体系与技术框架,研究者们针对不同场景提出了多种方法。基于深度学习的方法展现出显著优势,如王康喆^[4]采用卷积神经网络和长短记忆网络提取网络特征,实现了高精度的态势评估与预测,平均评估误差仅0.006;杜秋阳^[5]结合反向传播算法构建残差卷积神经网络,有效提升了攻击模式识别精度,优化了模型性能;吴少欢等^[6]将GA与BP神经网络结合,通过遗传算法优化网络参数,提升了态势预警效率。针对复杂场景的动态性,丁小娜等^[7]等提出改进因子加权算法,引入动态权重调整机制,在智慧实验室环境中实现了高拟合度的态势感知。面对多源数据融合难题,夏卓群等^[8]等基于改进D-S证据理论,结合深度自编码器和神经网络,提升了智慧水利网络态势评估的客观性与准确性。李晓霞^[9]则利用大数据技术构建分层架构系统,通过分布式处理与机器学习算法,显著提升了复杂攻击检测与预警响应速度。总体而言,现有方法在特征提取、动态适配及数据融合等方面取得进展,但在5G风筝专网等动态场景的适应性、多技术融合深度及极端环境鲁棒性上仍需突破,为关键行业网络安全提供更可靠的技术支撑。

本文的研究目标是构建面向电厂5G风筝专网的弹性安全态势感知模型,以解决其高移动性、弹性拓扑场景下感知精度低、适应性差及聚类稳定性不足的问题。整合生产控制大区现有态势感知平台的历史安全数据与一体化安全管理平台的核心安全要素,通过动态调整设备状态、威胁情报、安全事件和网络流量等各级指标的权重,实现威胁态势、脆弱态势、稳定态势三级安全态势的精准划分,输出网络安全总体态势的实时结果,最终达成对5G风筝专网、安全接入区、生产控制大区网络安全的全面感知监测。围绕上述目标,本文的主要贡献体现在以下方面:首先,提出了一种适用于电厂5G风筝专网场景的多源融合态势感知架构^[10],在实现历史数据与实时数据有机结合的同时提高数据精度,为态势评估提供了全面的数据支撑;其次,改进聚类算法避免局部最优问题,并设计基于网络运行状态的动态权重调整策略,实现指标权重的智能优化,提升了模型在不同场景下的评估精度;最后,构建三级态势评估体系,结合多源融合结果与动态权重配置,输出网络安全总体态势的实时结果,并通过可视化技术实现了对5G风筝专网全域安全状态的直观展示,为电厂安全运维提供了有效的决策支持。

1 系统模型

面向5G风筝专网高移动性、拓扑弹性化的应用场景,传统安全态势感知方法在移动干扰抑制、聚类稳定性及场景适应性方面存在明显不足。为此,本文提出一种融合多维度数据采集与处理、智能聚类分析及弹性适配策略的时空双模态弹性安全态势感知模型,旨在实现对5G风筝专网安全态势的精确感知与可视化展示。该模型的总体架构如图1所示,其核心工作流程包含多源数据采集与预处理层、特征增强层、智能聚类分析层和态势映射层。其中, x_t 表示时刻 t 的四维输入特征向量; A 表示基于LSTM重构误差与动态阈值的时序异常检测与特征增强过程; h_t 表示经时序异常检测后,将检测结果与原始特征融合形成的增强特征数据。聚类结果表示为3个安全态势簇,记为 $C1$ 、 $C2$ 和 $C3$,分别对应稳定态势、脆弱态势和威胁态势,后续通过态势映射规则实现安全态势等级判定。

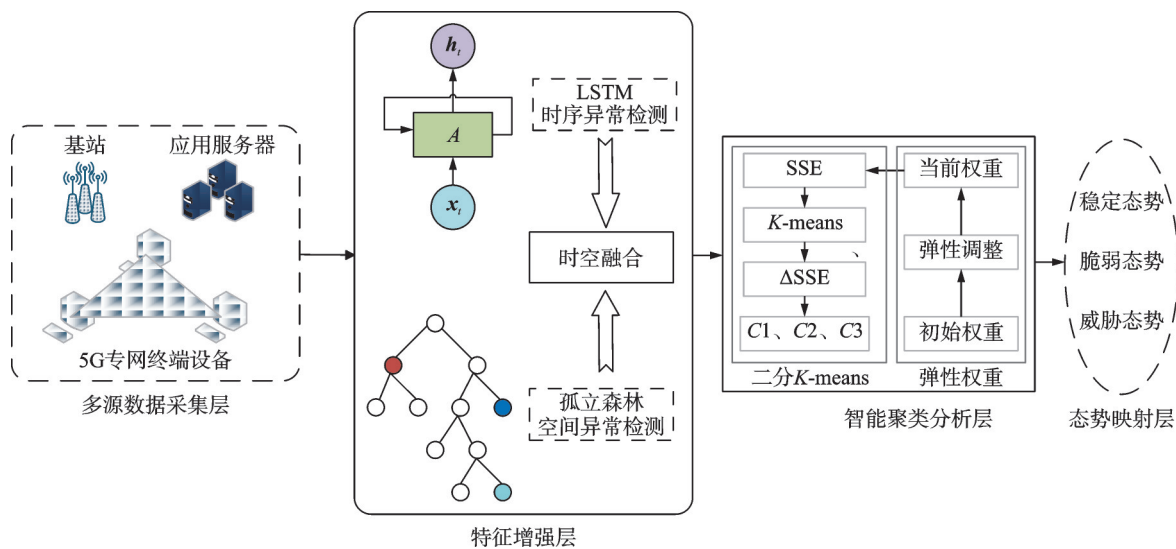


图1 态势感知总体架构图

Fig.1 Overall architecture diagram of security situation awareness

多源数据采集与预处理层作为系统的输入源,负责从5G风筝专网环境中实时采集异构安全数据,主要包括4个维度:设备状态数据通过网元监测接口获取,涵盖CPU负载、链路丢包率等关键性能指标;威胁情报数据来自专网威胁情报平台,提供实时攻击特征匹配信息;安全事件数据源自安全管理平台,记录异常接入与违规操作等日志信息;网络流量数据通过流量探针捕获,用于反映业务流量与异常波动情况。上述多源数据经清洗、标准化等预处理后,构成态势感知的基础数据体系。

特征增强层主要承担深层特征提取任务。该层采用双模态检测策略:一方面基于长短期记忆(Long short-term memory, LSTM)网络对时序数据进行建模,通过重构误差计算与动态阈值判断识别时序异常^[11];另一方面,运用孤立森林算法检测空间分布异常。最终将时序与空间检测结果融合,构建包含时空稳定性特征的五维增强特征矩阵,为后续聚类分析提供更高层次的特征表示。

智能聚类分析层采用二分K-means算法对增强特征进行无监督学习。该算法从单一簇出发,通过迭代分裂并根据误差平方和(Sum of squared errors, SSE)确定最优分裂节点,有效缓解了传统K-means算法对初始中心敏感、易陷入局部最优的问题,能够自适应地生成稳定、脆弱和威胁这3类安全态势簇。该层还集成了动态权重调整机制,依据实时网络状态自适应调整特征权重,通过加权欧氏距离优化样本与簇的归属关系。

态势映射层为整个模型提供可视化输出。该层通过规则化映射模块,依据聚类结果的空间与时间评分,将聚类输出映射为3种安全态势等级,并采用主成分分析(Principal component analysis, PCA)进行降维与可视化呈现,从而为运维人员提供直观的决策支持。

2 基于时空双模态的二分K-means算法

2.1 核心数据处理

本方法的数据基础整合了电厂生产控制安全接入区的历史安全数据与一体化安全管理平台的实时核心安全要素,构成了一个多源融合的数据集。该数据集具体包含4个维度的特征:(1)设备状态数据,来自网元监测接口,包括CPU负载、内存使用率和链路丢包率等,原始量纲为百分比,归一化后1表示设备健康、0表示故障或高负载;(2)威胁情报数据,来自专网威胁情报平台,表现为实时攻击特征如

恶意IP、漏洞利用流量的匹配置信度,原始值域为 $[0,1]$,归一化后1代表高威胁、0代表无威胁;(3)安全事件数据,从一体化安全管理平台获取,统计单位时间内异常接入、违规操作等事件的次数,归一化后1表示事件高频发生、0代表无安全事件;(4)网络流量数据,通过流量探针捕获,包括流量速率及其波动幅度,归一化后1代表流量严重异常或拥塞、0代表流量平稳。

5G风筝专网多源数据存在量纲差异、移动干扰及数据噪声等问题,需通过清洗、标准化与干扰抑制实现数据优化^[12],为后续时空双模态异常检测与态势聚类提供可靠输入。

首先进行数据清洗,删除无实际意义的数据记录,此类数据通常占比低于0.5%,剔除后不影响数据完整性。对于短时数据缺失,采用线性插值法补充;对于长时缺失,则标记为数据断层,后续分析中排除该时段数据,避免插值误差扩大。然后进行标准化处理,对这4类数据采用离差标准化方法进行归一化,计算公式为

$$p_{\text{norm}} = \frac{p - p_{\min}}{p_{\max} - p_{\min}} \quad (1)$$

式中: p_{norm} 为归一化后的数据,其范围在 $[0,1]$; p 为原始数据; $p_{\max}$ 为原始数据最大值; $p_{\min}$ 为原始数据最小值。

针对不同指标的标准化逻辑需结合其意义调整,将所有数据映射到0~1区间,消除量纲差异,让不同类型的数据能参与后续计算。同时部署滑动窗口算法应对高移动性产生的非安全类异常值,对流量和设备状态数据实时监测,若检测到瞬时异常则判定为移动切换噪声,并用窗口内相邻数据的均值替换噪声点,保障数据的连续性,避免干扰后续聚类。

2.2 时空双模态异常检测

5G风筝专网的态势数据兼具时间上的连续性与特征空间中的分布特性,属于典型的时空数据。为精准捕捉其异常模式,本文分别采用LSTM与孤立森林进行时序与空间维度的异常检测。在时序检测方面,与自回归积分滑动平均模型(Autoregressive integrated moving average, ARIMA)等线性模型相比,LSTM凭借其门控机制能有效建模流量、负载等指标中的复杂非线性时序依赖;而与门控循环单元(Gated recurrent unit, GRU)等变体相比,其在处理缓慢渗透类攻击所引发的长程依赖问题上更具优势。在空间检测方面,孤立森林基于隔离思想,无需对底层数据分布进行假设,具有线性计算复杂度,相较于基于密度的局部离群因子(Local outlier factor, LOF)或基于核函数的一类支持向量机(One-class support vector machine, One-Class SVM),更适用于高维、海量网络数据的实时异常筛查。LSTM与孤立森林分别从时序规律与特征分布两个正交视角识别异常,二者融合构成的时空稳定性特征能够更全面地表征样本点的安全状态,从而为后续聚类分析提供判别力更强的输入依据。

在5G风筝专网中,设备状态、网络流量等特征随时间呈现强关联性,这种时序依赖关系需通过具备长序列建模能力的模型捕捉^[13]。LSTM凭借门控机制可有效记忆长时序中的关键信息,适用于5G风筝专网时序异常检测。以多源数据预处理后的标准化四维特征为基础,采用滑动窗口法构建时序样本,以捕捉特征的动态演变规律。设标准化后的四维时序数据为 $X=[x_1, x_2, \dots, x_L]$,其中每个 x_t 是一个4维向量 $[x_t^1, x_t^2, x_t^3, x_t^4]$,分别为对应设备状态、威胁情报、安全事件、网络流量在时刻 t 的归一化值。采用滑动窗口法构建样本:窗口长度设为 $T=10$,第 i 个样本的输入序列为 $X_i=[x_i, x_{i+1}, \dots, x_{i+T-1}]$,维度为 $(T, 4)$,对应的目标输出为 $y_i=x_{i+T}$,最终得到样本集合 $\{(X_i, y_i)\}$,其中 $i=1, 2, \dots, m$; $m=L-T$ 。

随后构建LSTM模型^[14],其输入层形状为 $(T, 4)$ 的序列,包含64个LSTM单元与32个ReLU激活的全连接单元,输出层为4个单元,使用线性激活,输出预测值 $\hat{y}_i$ 。模型采用Adam优化器,以均方误差

(Mean squared error, MSE)为损失函数进行训练,损失函数公式为

$$\text{Loss} = \frac{1}{m} \sum_{i=1}^m (\mathbf{y}_i - \hat{\mathbf{y}}_i)^2 \quad (2)$$

式中: m 为训练样本数, $\mathbf{y}_i$ 为真实值, $\hat{\mathbf{y}}_i$ 为预测值。

训练完成后,计算每个预测样本的重构误差

$$\text{MSE}_i = \frac{1}{4} \sum_{j=1}^4 (y_i^j - \hat{y}_i^j)^2 \quad (3)$$

为避免固定阈值导致的误判,采用四分位距(Interquartile range, IQR)法^[15]确定动态异常阈值:先计算所有重构误差的上四分位数 $Q3$ 与下四分位数 $Q1$,得到四分位距 $\text{IQR} = Q3 - Q1$,则异常阈值为 $\theta = Q3 + 1.5 \times \text{IQR}$,当某样本的 $\text{MSE}_i > \theta$ 时,判定该时间点为时序异常点,其索引为 $i + T$ 。对于正常点,根据历史窗口内的 MSE 均值与阈值的比值计算时间稳定性得分,即

$$\text{stability} = 1 - \min(\text{mean}(\text{MSE})/\theta, 1) \quad (4)$$

同时,采用孤立森林算法^[16]对同一时段内的四维样本进行空间异常检测,输入为标准化四维特征数据集 $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_L]$,其中 $\mathbf{x}_i = [x_i^1, x_i^2, x_i^3, x_i^4]$,输出为异常分数 $a_i \in [0, 1]$,越接近 1 表示越异常,当 $a_i > 0.6$ 时判断为空间异常。将空间异常结果与时间异常结果融合,若时间检测或空间检测异常,则时空稳定性为 0;若时空检测均正常,则时空稳定性为 stability ,最终将原始四维特征与时空稳定性特征拼接,构建五维增强矩阵。

2.3 动态权重与二分 K-means

5G 风筝专网的动态场景特性要求态势聚类需同时满足场景适配性与聚类稳定性。动态权重调整的核心是以场景特征定权重优先级,实时优化特征权重占比,确保核心场景下关键特征的贡献度最大化^[17]。基于 5G 风筝专网的安全风险特征分析,本文构建了包含设备状态、威胁情报、安全事件、网络流量和时空稳定性这 5 类特征的权重向量。首先,初始权重的设定基于对电厂安全事件数据库的历史数据分析,首先采用皮尔逊相关系数公式量化设备状态 F_1 、威胁情报 F_2 、安全事件 F_3 、网络流量 F_4 、时空稳定性 F_5 与核心风险的关联强度 r_j ,计算公式为

$$r_j = \frac{\sum_{i=1}^N (x_{ij} - \bar{x}_j)(e_i - \bar{e})}{\sqrt{\sum_{i=1}^N (x_{ij} - \bar{x}_j)^2} \cdot \sqrt{\sum_{i=1}^N (e_i - \bar{e})^2}} \quad (5)$$

式中: N 为安全事件样本总数,源自电厂近 3 年运维标注数据; x_{ij} 为第 i 个样本中第 j 类特征的归一化值; $\bar{x}_j$ 为第 j 类特征的样本均值; e_i 表示第 i 个样本的事件标识, $e_i = 1$ 表示该样本对应异常事件, $e_i = 0$ 表示正常状态; $\bar{e}$ 表示安全事件的发生频率。

通过归一化得到基础权重 ω_j^{base} ,并结合风险优先级校准因子 α_j 由电力安全工程师结合技术规范确定,取值为 $[0.9, 1.1]$,最终得到初始权重向量 ω^{init}

$$\omega_j^{\text{base}} = \frac{r_j}{\sum_{k=1}^5 r_k} \quad (6)$$

$$\omega_j^{\text{init}} = \frac{\omega_j^{\text{base}} \alpha_j}{\sum_{k=1}^5 \omega_k^{\text{base}} \cdot \alpha_k} \quad (7)$$

动态调整以实时监测的终端移动速度 v 和专网带宽使用率 η 为触发条件,当 $v > 50 \text{ km/h}$ 时,引入场景风险修正因子 $\beta_{j,1}$

$$\beta_{j,1} = \frac{\gamma_{j,1}}{\gamma_{j,0}} \quad (8)$$

式中: $\beta_{j,1}$ 为第 j 类特征在移动性增强场景下的风险修正因子, $\beta_{j,1} > 1$ 表示该场景下特征重要性提升, $\beta_{j,1} < 1$ 表示重要性降低; $\gamma_{j,1}$ 第 j 类特征在移动性增强场景下的实际风险贡献度,通过 500 组场景实测样本统计得到; $\gamma_{j,0}$ 第 j 类特征在正常场景下的风险贡献度。

经归一化公式得到调整后的权重向量 ω^{s1}

$$\omega_j^{s1} = \frac{\omega_j^{\text{init}} \beta_{j,1}}{\sum_{k=1}^5 \omega_k^{\text{init}} \cdot \beta_{k,1}} \quad (9)$$

当 $\eta > 80\%$ 时,同理通过修正因子及归一化公式得到负载升高场景的权重向量 ω^{s2} 。

基于动态权重计算加权欧式距离作用于聚类过程,确保高权重特征对簇归属的影响更大,其计算公式为

$$d(h, \mu) = \sqrt{\sum_{i=1}^5 w_i (h_i - \mu_i)^2} \quad (10)$$

式中: h 为增强数据, μ 为簇中心, w_i 为第 i 类特征权重。

二分 K -means 算法通过迭代分裂、误差优化的策略^[18],从初始单簇逐步分裂为目标簇数,避免传统 K -means 随机初始质心导致的局部最优问题。首先进行聚类参数初始化,结合专网安全需求明确划分威胁、脆弱和稳定 3 类态势,设定目标簇数 $k=3$ 。在二分聚类迭代过程中,将预处理后的所有数据视为一个初始簇,使用基础 K -means 算法将初始簇划分为 2 个子簇 C_a 和 C_b ,计算分裂后两个子簇的误差平方和 SSE_a 和 SSE_b 。其计算公式为

$$\text{SSE} = \sum_{h \in C} (h - \mu_C)^2 \quad (11)$$

式中: h 为增强数据, μ_C 为簇 C 的质心。

再分别用基础 K -means 算法临时划分 C_a 得到 C_{a1} 和 C_{a2} ,临时划分 C_b 得到 C_{b1} 和 C_{b2} 。计算簇 C_{a1} 和 C_{a2} 的 SSE 之和 $\text{SSE}_{a1} + \text{SSE}_{a2}$,以及簇 C_{b1} 和 C_{b2} 的 SSE 之和 $\text{SSE}_{b1} + \text{SSE}_{b2}$ 。计算误差减少量 $\Delta \text{SSE}_a = \text{SSE}_a - (\text{SSE}_{a1} + \text{SSE}_{a2})$ 以及 $\Delta \text{SSE}_b = \text{SSE}_b - (\text{SSE}_{b1} + \text{SSE}_{b2})$ 。比较 ΔSSE_a 和 ΔSSE_b 的大小,最终选择误差减少量最大的簇正式划分为两个新簇,最终形成 3 个稳定簇。根据聚类结果,将每个样本都添加簇归属标签,用于后续可视化渲染。当 5G 风筝专网场景发生变化时,用新的距离重新进行样本与簇中心的匹配,更新样本的簇归属,确保聚类结果贴合当前网络状态。

2.4 态势映射与可视化

态势映射以聚类中心的特征值为核心依据,量化聚类中心的空间得分与时间得分,每个聚类中心的空间得分

$$R_s = \sum_{j=1}^4 w_j \times c_j \quad (12)$$

式中: w_j 为第 j 维特征权重, c_j 为聚类中心的第 j 维特征值。

时间得分 R_t 取第 5 维特征值,即时空稳定性特征。结合电厂生产控制大区的安全等级划分需求与 5G 风筝专网的风险特征,制定如下预设规则判定态势:若 $R_s > 0.6$ 且 $R_t > 0.6$ 为“稳定态势”;若 $R_s <$

0.4且 $R_i < 0.3$ 为“威胁态势”;其余为“脆弱态势”。

在可视化呈现过程中,采用主成分分析法^[19]将五维空间特征向量压缩至二维空间,再进行可视化渲染。降维过程的输入为增强数据集,作为原始五维数据矩阵 X 。降维核心在于寻找一个最优的线性投影变换,该变换首先计算五维矩阵 X 的协方差矩阵 C ,计算公式为

$$C = \frac{1}{m-1} \cdot (X - \bar{X})^T \cdot (X - \bar{X}) \quad (13)$$

式中: m 为样本数量, $\bar{X}$ 为所有样本的均值向量。

然后对协方差矩阵 C 进行特征分解,获取5个特征向量 $u_1、u_2、u_3、u_4、u_5$,即5个主成分。各主成分按其对应的特征值大小降序排列。本文选取前两个最大特征值所对应的特征向量构成投影矩阵 M 。将五维矩阵 X 与此投影矩阵 M 相乘,得到二维数据矩阵 Y ,其中每行代表一个样本在二维空间的新坐标。在获得二维投影坐标后,依据每个样本的簇归属标签分类可视化数据,并归属于对应的态势,生成态势图。总体算法流程如图2所示。

3 仿真与结果分析

3.1 仿真设置

实验设备包括AMD Ryzen 5 5500U with Radeon Graphics @ 2.10 GHz,内存16 GB, GPU为AMD Radeon (TM) Graphics,显存2 GB。仿真实验环境包括64位操作系统,基于×64的处理器,仿真软件为PyCharm,编程语言为PyThon3.8,深度学习框架为PyTorch 1.0.2。在仿真实验中,仿真参数设置如表1所示。目标簇数 k 设定为3,以应对稳定、脆弱与威胁这3类预定义的安全态势等级;滑动窗口长度 T 设为10个采样点;LSTM网络结构包含64个单元用于时序建模,后接32个节点的全连接层进行特征变换,输出层4个单元与4类输入特征维度保持一致。

3.2 仿真结果与分析

本文采用肘部法则^[20]确定最佳聚类数,该方法通过计算不同 k 值对应的聚类误差平方和SSE,并观察其随 k 值增大的变化趋势,从而识别出平衡模型复杂度与聚类效果的拐点值。

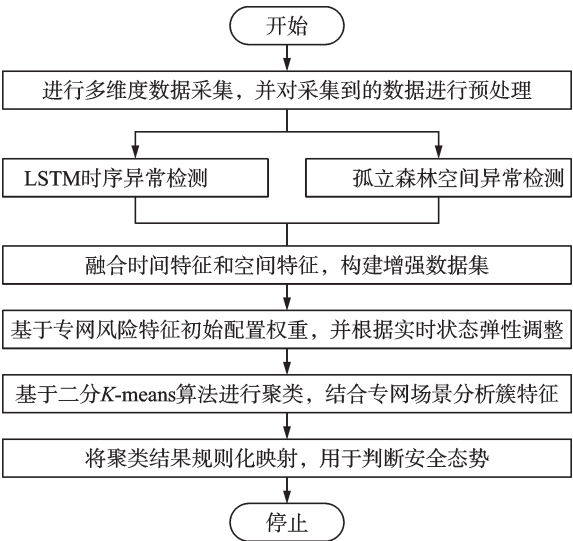


图2 算法流程

Fig.2 Algorithm flowchart

表1 仿真参数设置

Table 1 Setting of simulation parameters

参数类别	参数名称	参数值
仿真框架参数	目标簇数 k /个	3
	滑动窗口长度 T	10
	空间异常阈值	0.6
	移动性增强判定阈值/($\text{km}\cdot\text{h}^{-1}$)	50
	高负载判定阈值/%	80
LSTM模型参数	优化器	Adam
	初始学习率	0.001
	学习率衰减策略	余弦退火
	批量大小	32
	训练周期	100
	Dropout率	0.3
	LSTM单元数	64
孤立森林参数	全连接层数	32
	输出层单元数	4
	损失函数	MSE
	树的数量	100
	最大样本数	256
	最大特征数	5

如图3所示,横坐标为 k 值,纵坐标为SSE。从曲线趋势可见,随着 k 值的增加,SSE总体呈现单调递减特征,当 $k=3$ 时,SSE下降趋势出现明显拐点,表明进一步增加聚类数对提升模型拟合度的贡献有限。因此,本文将目标簇数设定为 $k=3$,与稳定、脆弱、威胁3类安全态势的设计一致,验证了聚类数选择的合理性。

为验证动态权重调整机制的有效性,本文对比了3种权重策略下的聚类效果。初始权重为 $W_0=[0.15, 0.35, 0.25, 0.15, 0.10]$,以威胁情报和安全事件为核心侧重,设备状态与网络流量权重均衡,时空稳定性权重最低,适配5G风筝专网正常运行场景。图4为初始权重下加权PCA降维后的聚类分布结果,从图4可见3类态势在二维空间中区分显著,绿色部分为稳定态势,样本数占比90.8%;橙色部分为脆弱态势,样本数占比7.0%;红色部分为威胁态势,样本数占比2.2%。

移动性增强权重为 $W_1=[0.05, 0.35, 0.25, 0.20, 0.15]$,设备状态权重从0.15降至0.05,网络流量权重从0.15升至0.2,时空稳定性权重从0.1升至0.15。图5为移动性增强情况下加权PCA降维后的聚类分布结果,其中稳定态势样本数占比87.4%,脆弱态势样本数占比9.9%,威胁态势样本数占比2.7%。负载升高权重为 $W_2=[0.15, 0.20, 0.35, 0.15, 0.15]$,威胁情报权重从0.35降至0.2,安全事件权重从0.25升至0.35,时空稳定性权重从0.1升至0.15。图6为负载升高情况下加权PCA降维后的聚类分布结果,其中稳定态势样本数占比82.5%,脆弱态势样本数占比13.2%,威胁态势样本数占比4.3%。

图7为不同场景下安全态势比例分布。如图7所示,相比于5G风筝专网正常运行场景,移动性增强和负载升高场景的稳定态势比例下降,脆弱态势和威胁态势比例增加。移动性增强会导致终端频繁

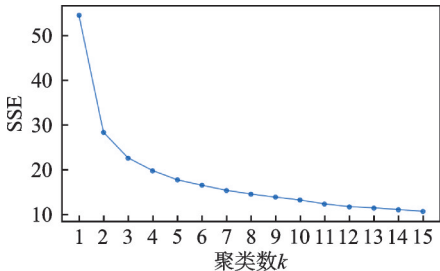


图3 肘部法则:SSE随聚类数 k 变化趋势

Fig.3 Elbow method: SSE versus number of clusters k

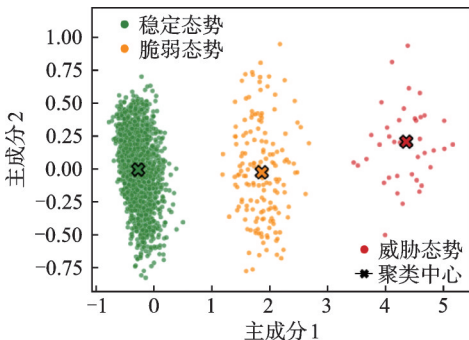


图4 正常场景下安全态势分布

Fig.4 Security situation distribution under normal operating condition

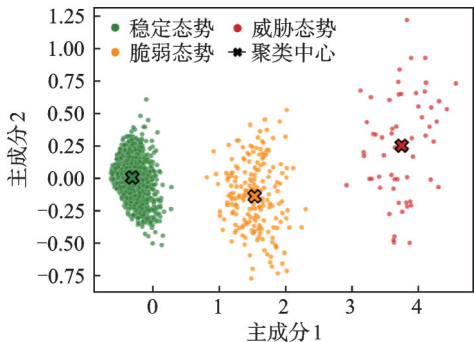


图5 移动性增强场景下安全态势分布

Fig.5 Security situation distribution under mobility-enhanced scenario

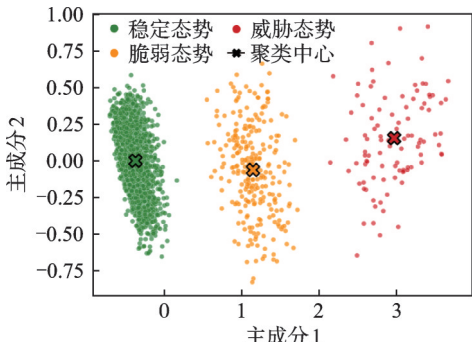
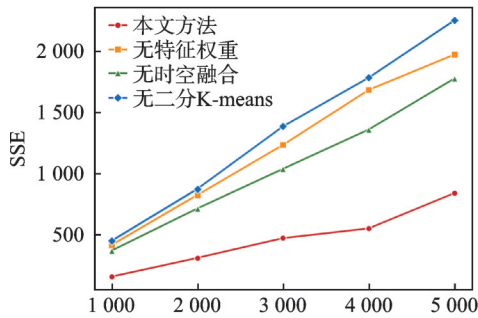


图6 负载升高场景下安全态势分布

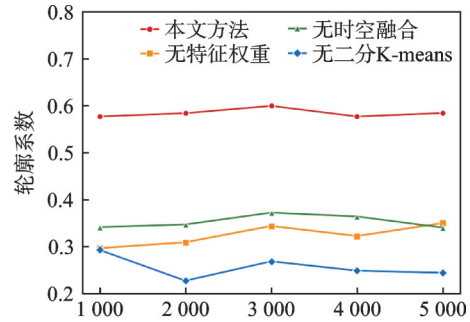
Fig.6 Security situation distribution under high-load scenario

切换、链路质量波动增大,原本稳定的连接可能变为不稳定,从而使得部分稳定态势样本被重新判定为脆弱态势,脆弱态势被判定为威胁态势;而在高负载场景下,网络拥堵加剧、资源竞争激烈,不仅放大了潜在的安全风险,也可能掩盖外部攻击行为,导致系统将更多样本识别为脆弱甚至威胁态势。动态权重调整机制通过捕捉这些场景的变化,提升相应特征的权重,使聚类结果真实反映了网络状态的恶化趋势,证明了该模型对5G风筝专网弹性安全态势的精准感知能力。

为验证本文所提感知模型中各模块的有效性,本文分别移除了动态特征权重调整、时空双模态融合和二分K-means聚类这3个关键模块进行对比实验,结果如图8所示。从图8可以看出,完整方法在SSE和轮廓系数两个指标上均表现最优。各模块对模型性能均产生了不同程度的影响,移除特征权重模块和移除时空融合模块均引起了SSE的大幅增加与轮廓系数的降低,并且二分K-means模块的移除对模型性能影响最为突出。这些结果充分证明了各模块在提升模型性能中的重要作用,特别是二分K-means算法对聚类稳定性的贡献尤为显著,以及动态权重机制在适应5G风筝专网动态场景中的必要性。



(a) SSE指标对比
(a) Comparison of SSE



(b) 轮廓系数对比
(b) Comparison of silhouette coefficients

图8 消融实验性能对比

Fig.8 Ablation study performance comparison

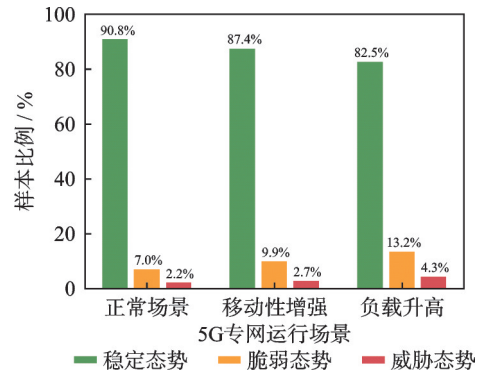


图7 不同场景下安全态势比例分布

Fig.7 Comparative distribution of security situations across different scenarios

最后,为验证本文所提算法的性能,将其与传统高斯混合模型(Gaussian mixture model, GMM)^[21]和基于密度的噪声应用空间聚类算法(Density-based spatial clustering of applications with noise, DBSCAN)^[22]进行对比,结果如图9所示。从图9可以看出,相较于GMM方法,本文方法在SSE指标上显著降低,轮廓系数也有提升;而与DBSCAN方法对比,由于其对参数配置较为敏感且在动态拓扑环境中适应性受限,本文方法在两项指标上均表现出更为突出的性能改善。实验分析表明,传统聚类方法在5G风筝专网的高移动性环境中存在固有局限,GMM依赖于高斯分布假设,而DBSCAN在参数选择与密度适应性方面存在不足,而本文方法通过融合时空双模态特征并引入动态权重机制,可有效提升在复杂网络环境下的聚类稳定性与准确性,为电力网络安全态势感知提供了更可靠的技术方案。

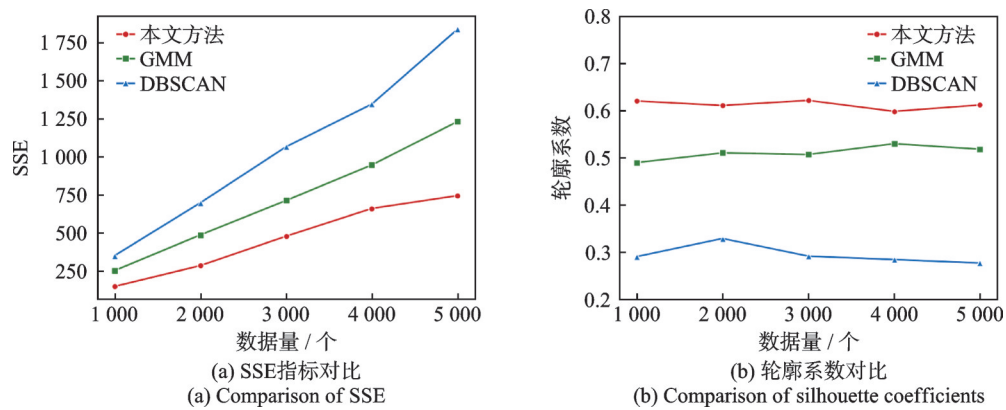


图9 本文方法与传统方法性能对比

Fig.9 Performance comparison of the proposed method with traditional methods

4 结束语

本文面向具有5G-A特征的电力5G风筝专网开展研究,该架构作为向6G演进的关键过渡形态,有效应对了电力业务中的核心痛点。针对5G风筝专网高移动性、弹性拓扑场景下面临的安全态势感知难题,提出了一种基于时空双模态的电力网络弹性安全态势感知方法。通过融合LSTM时序异常检测与孤立森林空间异常检测,构建增强特征矩阵,并结合二分K-means聚类与场景自适应的权重调整机制,实现了对稳定、脆弱、威胁这3类安全态势的精准划分与弹性感知。仿真结果表明,该方法能够有效响应移动性增强与负载升高场景的变化,提升态势感知的准确性与鲁棒性,为5G风筝专网安全运维提供了可靠的技术支撑。未来研究将进一步结合6G通感一体的网络架构特性,推动电力通信安全态势感知技术向6G演进。

参考文献:

- [1] 张平,陈岩,吴超楠. 6G: 新一代移动通信技术发展态势及展望[J]. 中国工程科学, 2023, 25(6): 1-8.
ZHANG Ping, CHEN Yan, WU Chaonan. 6G: Development trends and prospects of next-generation mobile communication technology[J]. Strategic Study of CAE, 2023, 25(6): 1-8.
- [2] 杨立,薛妍,谢峰. 面向6G移动通信新系统的感知体系和流模型的设计[J/OL]. 中兴通讯技术, 1-9[2021-08-12]. <https://kns.cnki.net/kcms/detail/34.1228.TN.20210812.1545.002.html>.
YANG Li, XUE Yan, XIE Feng. Design of sensing architecture and flow models for new 6G mobile communication systems [J/OL]. ZTE Communications, 1-9[2021-08-12]. <https://kns.cnki.net/kcms/detail/34.1228.TN.20210812.1545.002.html>.
- [3] 梅文明,刘智铭,胡柏吉,等. 基于主客观分析的电力5G虚拟专网安全风险评估方法设计[J]. 北京邮电大学学报, 2025, 48(5): 121-127.
MEI Wenming, LIU Zhiming, HU Baiji, et al. Design of a security risk assessment method for power 5G virtual private networks based on subjective and objective analysis[J]. Journal of Beijing University of Posts and Telecommunications, 2025, 48(5): 121-127.
- [4] 王康喆. 基于深度学习的通信网络安全态势感知方法[J]. 成都工业学院学报, 2025, 28(4): 29-36.
WANG Kangzhe. A deep learning-based security situation awareness method for communication networks[J]. Journal of Chengdu Technological University, 2025, 28(4): 29-36.
- [5] 杜秋阳. 基于反向传播算法的网络安全态势感知方法[J]. 信息技术与信息化, 2025(6): 76-79.
DU Qiuyang. A network security situation awareness method based on the backpropagation algorithm[J]. Information Technology and Informatization, 2025(6): 76-79.

- [6] 吴少欢,李镭. 基于GA-BP神经网络的安全态势预测系统构建[J]. 网络安全技术与应用, 2025(6): 47-50.
WU Shaohuan, LI Lei. Construction of a security situation prediction system based on GA-BP neural network[J]. Network Security Technology and Application, 2025(6): 47-50.
- [7] 丁小娜,王书静,李国政,等. 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[J]. 信息技术与信息化, 2025(6): 101-104.
DING Xiaona, WANG Shujing, LI Guozheng, et al. A communication network security situation awareness method for smart laboratories based on an improved factor weighting algorithm[J]. Information Technology and Informatization, 2025(6): 101-104.
- [8] 夏卓群,周子豪,邓斌,等. 一种基于改进D-S证据的智慧水利网络安全态势评估方法[J]. 计算机科学, 2025, 52(S1): 950-955.
XIA Zhuoqun, ZHOU Zihao, DENG Bin, et al. A smart water conservancy security situation assessment method based on improved D-S evidence theory[J]. Computer Science, 2025, 52(S1): 950-955.
- [9] 李晓霞. 基于大数据的网络安全态势感知与预警系统研究[J]. 中国宽带, 2025, 21(5): 46-48.
LI Xiaoxia. Research on network security situation awareness and early warning system based on big data[J]. China Broadband, 2025, 21(5): 46-48.
- [10] 张晏斌,邓峰,沈海洋. 电力系统数据安全态势感知技术研究与应用[J]. 电气技术与经济, 2025(9): 116-118.
ZHANG Yanbin, DENG Feng, SHEN Haiyang. Research and application of power system data security situation awareness technology[J]. Electrical Equipment and Economy, 2025(9): 116-118.
- [11] 孙诗蕾,徐澍,李春国,等. 面向6G无线组网的基于GCN-LSTM网络的业务流量预测算法[J]. 数据采集与处理, 2025, 40(5): 1239-1249.
SUN Shilei, XU Shu, LI Chunguo, et al. A GCN-LSTM-based service traffic prediction algorithm for 6G wireless networking [J]. Journal of Data Acquisition and Processing, 2025, 40(5): 1239-1249.
- [12] 杨洪芳. 火电厂DCS系统数据异常识别与处理方法研究[J]. 锅炉制造, 2025(5): 62-64.
YANG Hongfang. Research on abnormal data identification and processing method for DCS systems in thermal power plants[J]. Boiler Manufacturing, 2025(5): 62-64.
- [13] 宋雅洁,步兵. 基于网络流量与设备状态的CBTC入侵检测系统[J]. 中国安全科学学报, 2019, 29(S2): 161-167.
SONG Yajie, BU Bing. An intrusion detection system for CBTC based on network traffic and equipment status[J]. China Safety Science Journal, 2019, 29(S2): 161-167.
- [14] 王科,阳浩,王洪林,等. 基于卷积神经网络与双向长短期记忆网络的电流互感器故障诊断方法研究[J/OL]. 自动化技术与应用, 1-11[2025-09-16]. <https://link.cnki.net/urlid/23.1474.tp.20250916.1021.008>.
WANG Ke, YANG Hao, WANG Honglin, et al. Research on current transformer fault diagnosis based on convolutional neural networks and bidirectional long short-term memory networks[J/OL]. Techniques of Automation and Applications, 1-11 [2025-09-16]. <https://link.cnki.net/urlid/23.1474.tp.20250916.1021.008>.
- [15] 宫永立,王玉超,刘志文,等. 基于四分位数和Sigmoid改进模型的风电数据清洗方法[J]. 电力科学与工程, 2025, 41(3): 55-62.
GONG Yongli, WANG Yuchao, LIU Zhiwen, et al. Wind power data cleaning method based on quartiles and Sigmoid improved model[J]. Electric Power Science and Engineering, 2025, 41(3): 55-62.
- [16] 宫晓婷,董培信. 基于改进孤立森林算法的交通流异常数据检测模型[J]. 重庆交通大学学报(自然科学版), 2024, 43(5): 61-69, 90.
GONG Xiaoting, DONG Peixin. Traffic flow anomaly data detection model based on improved isolation forest algorithm[J]. Journal of Chongqing Jiaotong University (Natural Science), 2024, 43(5): 61-69, 90.
- [17] 姜维龙,陈璐,易彬,等. 动态权重自适应分配的LSTM洪水演进方法[J]. 华中科技大学学报(自然科学版), 2026, 54(7): 20-26.
JIANG Weilong, CHEN Lu, YI Bin, et al. Flood evolution method based on adaptive allocation of dynamic weights for LSTM [J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2026, 54(7): 20-26.
- [18] 张雅茹. 基于改进二分K-means算法的网络异常检测技术研究[J]. 鄂州大学学报, 2022, 29(6): 97-99.
ZHANG Yaru. Research on network anomaly detection technology based on improved bisecting K-means algorithm[J]. Journal of Ezhou University, 2022, 29(6): 97-99.
- [19] 杨建,舒龙勇,张书林,等. 基于PCA-Transformer的工作面瓦斯浓度预测算法研究[J]. 工矿自动化, 2025, 51(5): 1-7.

YANG Jian, SHU Longyong, ZHANG Shulin, et al. Research on coal mine working-face gas concentration prediction algorithm based on PCA-Transformer[J]. Journal of Mine Automation, 2025, 51(5): 1-7.

[20] 乔世超,陈衡,李博,等.基于K-Means聚类与Ridge回归算法的煤炭发热量预测研究[J].发电技术,2025,46(1): 135-144.

QIAO Shichao, CHEN Heng, LI Bo, et al. Research on coal calorific value prediction based on K-means clustering and Ridge regression algorithms[J]. Power Generation Technology, 2025, 46(1): 135-144.

[21] SALARI A, SHIRVANIMOGHADDAM M, SHAHAB M B, et al. NOMA joint channel estimation and signal detection using rotational invariant codes and GMM-based clustering[J]. IEEE Communications Letters, 2022, 26(10): 2485-2489.

[22] HANAFI N, SAADATFAR H. A fast DBSCAN algorithm for big data based on efficient density calculation[J]. Expert Systems with Applications, 2022, 203: 117501.

作者简介:



周轶喆(1976-),男,高级工程师,研究方向:电力企业信息化,E-mail:12111847@ceic.com。



朱贤伟(1971-),通信作者,男,高级工程师,研究方向:电力企业信息化,E-mail:12023533@ceic.com。



胡文杰(1992-),男,工程师,研究方向:电力企业信息化。



吴天杰(1984-),男,工程师,研究方向:电力企业信息化。



陈磊(1988-),男,工程师,研究方向:5G工业互联网。



从宇(1996-),男,博士研究生,研究方向:电力无线通信。



王冰茹(2003-),女,硕士研究生,研究方向:电力无线通信。

(编辑:王静)

A Spatiotemporal Dual-Modal-Based Strategy for Elastic Security Situation Awareness in Power Networks

ZHOU Yizhe¹, ZHU Xianwei^{1*}, HU Wenjie¹, WU Tianjie¹, CHEN Lei², CONG Yu³,
WANG Bingru⁴

(1. Guoneng Zhejiang Beilun First Power Generation Co., Ltd., Ningbo 315000, China; 2. Zhejiang Mobile Digital Intelligence Technology Co., Ltd. (Ningbo Branch), Ningbo 315000, China; 3. School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China; 4. School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: As an embodiment of the core 6G vision of scenario-based mobile communication, the 5G kite private network is designed to address practical challenges in the power industry such as high-frequency terminal mobility, dynamic topological reconfiguration, and low-latency service guarantees. To tackle the issues of insufficient accuracy and weak adaptability in security situation awareness within highly mobile and elastic topological environments of 5G kite private networks, this paper proposes a spatiotemporal dual-modal based elastic security situation awareness method for power networks. The approach constructs a multi-source input vector by collecting core feature data, employs long short-term memory (LSTM) networks for temporal anomaly detection, and integrates isolation forest for spatial anomaly detection, thereby generating an enhanced feature matrix. Furthermore, a bisecting K-means clustering algorithm and a dynamic weight adjustment mechanism are introduced to adaptively optimize feature weights, enabling accurate classification of security situations into three levels: Stable, vulnerable, and threatened. Finally, the weighted principal component analysis is applied for dimensionality reduction and visualization. Simulation results demonstrate that the proposed method effectively responds to changes in network state, improves situational judgment accuracy across various scenarios, and provides reliable support for the security maintenance of 5G kite private networks.

Highlights:

1. Propose a spatiotemporal dual-modal security situation awareness framework for 5G kite private networks, integrating multi-source data with LSTM-based temporal and isolation forest-based spatial anomaly detection.
2. Develop a dynamic-weighted bisecting K-means method that adaptively adjusts feature weights according to network mobility and load, improving clustering stability and security situation classification.
3. Validate the proposed method through scenario-based and ablation experiments, demonstrating improved clustering performance and adaptive perception of three security situations under varying network conditions.

Key words: 5G kite private network; spatiotemporal dual-modal; security situation awareness; elastic adaptation; anomaly detection

Foundation item: National Energy Group Science and Technology Innovation Project (No.E621000029).

Received: 2025-09-29; **Revised:** 2025-12-17

***Corresponding author, E-mail:** 12023533@ceic.com.