图神经网络在新型配电系统风险管控中的应用

赵天阳[1†]，罗嗣朋[1]，谢海鹏[1]，司渭滨[2]，王 鹏[3]，别朝红[1]

(1. 西安交通大学电气工程学院，陕西 西安 710054；
2. 国网陕西省电力有限公司安康供电公司，陕西 安康 725000；
3. 南洋理工大学电气与电子工程学院，新加坡 639798)

摘 要: 随着我国新型配电系统建设深入推进, 配电系统正演进为以柔性化、数字化、智能化为核心特征的有源双向交互系统. 然而, 海量分布式资源接入与开放交互环境, 使系统面临设备健康退化、故障停运与状态越限, 量测稀疏、拓扑未知与 FDI 攻击, 以及通信拥塞、链路中断、丢包与 DoS/DDoS 攻击等多维风险. 这些风险在能量流与信息流中深度耦合, 极易引发复杂的跨空间级联失效. 针对上述多层级耦合风险, 通过“物理-数字-信息”三层空间架构, 在梳理各层级风险演化机理的基础上, 系统综述了图神经网络在新型配电系统风险管控中的前沿应用. 提炼了系统多维风险特征与具体图学习任务及各类图神经网络架构的适配映射关系, 重点探讨了其在挖掘非欧拓扑关联与应对跨层耦合风险方面的核心优势. 最后分析了现有数据驱动方法的局限性, 并从物理机制引导、跨层多模态图融合及云边协同计算等方面展望了未来的技术演进方向, 以期为高弹性新型配电系统的安全运行提供参考.

关键词: 新型配电系统；风险管控；图神经网络；信息物理系统；状态估计；网络攻击

中图分类号: TM76 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2026.0489

引用格式: 赵天阳, 罗嗣朋, 谢海鹏, 等. 图神经网络在新型配电系统风险管控中的应用 [J]. 控制与决策, xxxx, x(x): xxxx-xxxx.

Applications of graph neural networks in risk management of new distribution systems: A review

ZHAO Tian-yang[1†]，*LUO Si-peng*[1]，*XIE Hai-peng*[1]，*SI Wei-bin*[2]，*WANG Peng*[3]，*BIE Chao-hong*[1]

(1. School of Electrical Engineering，Xi'an Jiaotong University，Xi'an 710054，China；2. Ankang Power Supply Company，State Grid Shaanxi Electric Power Company Limited，Ankang 725000，China；3. School of Electrical and Electronic Engineering，Nanyang Technological University，Singapore 639798，Singapore)

Abstract: With the continued development of new distribution systems in China, distribution networks are being transformed into active bidirectional systems characterized by flexibility, digitalization, and intelligence. However, multidimensional risks are being introduced by the large-scale integration of distributed resources and increasingly open communication environments, including equipment degradation, component outages and operating-limit violations; measurement sparsity, unknown topology and false data injection (FDI) attacks; and communication congestion, link failures, packet loss and denial-of-service/distributed denial-of-service (DoS/DDoS) attacks. These risks are deeply coupled through energy and information flows, through which complex cross-domain cascading failures can be triggered. To address such multilayer coupled risks, a three-layer physical-digital-information architecture is established, and recent applications of graph neural networks (GNNs) in risk management and control for new distribution systems are systematically reviewed after the risk evolution mechanisms at each layer are analyzed. The relationships among multidimensional risk characteristics, specific graph learning tasks, and different GNN architectures are identified and summarized, while particular emphasis is placed on the advantages of GNNs in capturing non-Euclidean topological dependencies and addressing cross-layer coupled risks. Finally, the limitations of existing data-driven methods are analyzed, and future research directions are outlined in terms of physics-guided modeling, cross-layer multimodal graph fusion, and cloud-edge collaborative computing. A reference for the secure

收稿日期: 2026-05-25；**录用日期:** 2026-09-15.
基金项目: 智能电网重大专项 (2030)；多类型新型主体接入配电网安全关键技术及示范工程 (2025ZD0805900).
责任编委: 马大中.
[†]通信作者. E-mail: zhaoty@xjtu.edu.cn.

operation of highly resilient new distribution systems is expected to be provided through this review.

Keywords: new distribution systems； risk management； graph neural networks； cyber-physical systems； state estimation；cyber attacks

0 引 言

随着《关于促进电网高质量发展的指导意见》等政策的深入推进, 我国配电系统正经历深刻的结构性变革, 逐步演进为以新能源为主体、有源双向交互的新型配电系统. 该系统以柔性化、数字化、智能化为核心特征, 通过先进信息通信与电力电子技术的赋能, 实现了多类型新型主体的灵活互联与全局智能调控[1]. 然而, 随着柔性化、数字化与智能化的推进, 新型配电系统的动态特性与风险演化机理趋于复杂化. 一方面, 高比例电力电子设备与海量分布式资源的接入, 不仅加剧了设备健康退化与突发停运的资产管控压力, 还导致源荷双向剧烈波动, 极易引发运行状态越限与局部脆弱区域的级联故障. 另一方面, 系统对高精度态势感知的依赖, 与有限的量测配置及频繁的开关动作产生矛盾, 导致量测稀疏与拓扑未知风险日益凸显; 同时, 海量数据的高并发交互也受制于客观的传输瓶颈, 频繁面临通信拥塞与信息丢包等挑战. 此外, 高度开放的交互环境进一步放大了网络安全威胁, 系统极易遭受隐蔽的虚假数据篡改以及耗尽通信资源的拒绝服务攻击[2-3]. 这些多维度的风险诱因在能量流与信息流中深度耦合, 衍生出复杂的跨空间级联失效路径, 对新型配电系统的安全风险管控提出了严峻挑战.

图神经网络 (Graph Neural Network, GNN) 作为面向非欧几里得图数据的前沿机器学习方法, 为新型配电系统风险管控提供了新的技术路径. 新型配电系统本质上可抽象为由节点和支路构成的复杂图结构, 而 GNN 能够通过邻域聚合、消息传递和图表示学习机制, 挖掘系统运行状态中的拓扑关联、时空依赖和跨层耦合特征[4]. 近年来, GNN 已在新型配电系统的潮流计算、拓扑识别、状态估计、负荷预测和安全控制等方面取得了显著进展, 但现有研究多聚焦于单一任务或常规运行工况, 尚缺乏从系统级风险管控视角出发, 对 GNN 在新型配电系统风险管控中的应用进行系统梳理.

面向新型配电系统多层级耦合与多状态演变的复杂风险特征, 本文构建"物理-数字-信息"三层空间架构, 对风险管控技术展开系统综述. 首先, 分析各层级风险演化的主导因素与数学表征, 讨论现有方法在应对上述挑战时的理论局限与应用瓶颈. 其次, 阐明 GNN 在契合系统非欧拓扑关联、破解多维耦合风险方面的核心优势, 并梳理其在风险管控各环节的前沿应用. 进一步地, 本文系统提炼了多维风险特征、图学习任务与各类 GNN 架构的适配映射关系, 为复杂场景下的模型选型提供理论参考. 最后, 针对现有数据驱动方法的不足, 对该领域未来的技术演进方向进行展望.

1 文献来源与筛选策略

为提高文献覆盖的完整性和代表性, 本文采用数据库检索与参考文献追溯相结合的文献筛选策略. 文献检索主要基于 Web of Science、IEEE Xplore、ScienceDirect、SpringerLink、中国知网、万方数据库等学术资源平台, 并结合高被引文献、重要综述文献及其参考文献进行补充核查. 检索时间范围主要为 2021 年至 2026 年, 同时纳入部分与信息物理系统、图神经网络和配电系统风险管控密切相关的经典文献.

检索关键词围绕三类主题构建: 新型配电系统与信息物理系统, 如"distribution system", "active distribution network", "cyber-physical power system", "smart distribution grid"以及"配电系统""主动配电网""信息物理电力系统"等; 风险识别与安全管控, 如 "risk assessment", "fault diagnosis", "resilience", "cybersecurity", "false data injection", "state estimation", "topology identification"以及"风险评估""故障诊断""韧性恢复""网络安全""状态估计""拓扑辨识"等; 图学习方法, 如"graph neural network", "graph convolutional network", "graph attention network", "spatio-temporal graph neural network"以及"图神经网络""图卷积网络""图注意力网络""时空图神经网络"等.

文献筛选过程包括关键词组合检索、重复文献剔除、题名摘要初筛、全文复筛、参考文献追溯和主题分类整理. 本文重点纳入研究对象与配电系统、主动配电网、信息物理电力系统或新型电力系统相关, 方法上涉及图神经网络、图表示学习、图信号处理或拓扑建模, 且面向状态估计、故障诊断、拓扑辨识、虚假数据注入检测、风险评估、韧性恢复、网络安全或调度控制等风险管控场景的文献; 排除缺乏电力系统应用背景、与风险管控主题关联较弱、重复发表、全文不可获取或与本文物理-数字-信息三层风险管控框架关联较弱的文献.

2　新型配电系统异构图建模

新型配电系统本质上是电力系统与信息系统深度融合的系统, 其风险管控问题可通过信息物理耦合系统架构加以刻画. 信息物理系统 (Cyber-Physical System, CPS) 及其在电力系统中的扩展形式, 包括信息物理电力系统 (Cyber-Physical Power System, CPPS)、信息物理能源系统 (Cyber-Physical Energy System, CPES) 和信息物理配电系统 (Cyber-Physical Distribution System, CPDS), 强调电网物理运行与感知量测、通信传输、计算分析、控制执行之间的闭环耦合关系, 为新型配电系统跨层风险分析提供了基础[5]. 然而, 现有 CPDS 架构通常采用物理层与信息层的二层划分, 或采用物理设备层、通信网络层和控制应用层的功能划分, 容易将状态估计、拓扑辨识等环节笼统归入信息层, 难以揭示数字表征偏差在风险传播中的作用. 将数字层从广义信息层中独立出来的根本动因在于, 新型配电系统的调度控制并不直接基于物理真实状态, 而是基于由量测数据、状态估计、拓扑辨识的数字孪生表征共同生成的数字状态. 当量测配置不足、通信数据丢失、拓扑记录错误、状态估计算法失准或 FDI 攻击存在时, 数字状态可能显著偏离物理真实状态, 进而误导信息层生成不合理的调度或保护指令, 并最终反作用于物理层, 诱发状态越限、误切负荷或级联失效[6]. 因此, 本文以 CPDS 为基础, 将数字表征环节从广义信息层中独立出来, 构建物理层、数字层和信息层三层风险管控架构, 以显式刻画"物理真实状态-数字表征状态-信息决策指令-物理状态响应"的闭环风险传播链条. 图 1 为新型配电系统物理-数字-信息三层架构图.

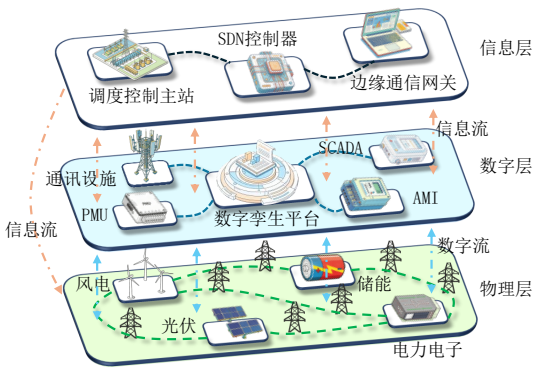

图 1　新型配电系统物理—数字—信息三层架构

因此, 物理-数字-信息新型配电系统可以抽象为一个多层异构动态图. 定义时刻t的系统图为:

$$\mathcal{G}_t = (\mathcal{V}, \mathcal{E}_t), \tag{1}$$

其中: $\mathcal{V}$表示节点集合, $\mathcal{E}_t$表示时刻t的边集合. 节点集合按照系统功能划分为三类:

$$\mathcal{V} = \mathcal{V}^P \cup \mathcal{V}^D \cup \mathcal{V}^I, \tag{2}$$

其中: $\mathcal{V}^P$表示物理层节点, $\mathcal{V}^D$表示数字层节点, $\mathcal{V}^I$表示信息层节点. 边集合按照图论中的层内连接与跨层映射关系划分为六类:

$$\mathcal{E}_t = \mathcal{E}_t^{PP} \cup \mathcal{E}_t^{PD} \cup \mathcal{E}_t^{DD} \cup \mathcal{E}_t^{DI} \cup \mathcal{E}_t^{II} \cup \mathcal{E}_t^{IP}, \tag{3}$$

其中: $\mathcal{E}_t^{PP}$表示物理层内部边, 主要刻画线路、变压器和开关等元件形成的电气连接、能量传输与潮流分布关系; $\mathcal{E}_t^{PD}$表示物理层到数字层的跨层量测映射边, 主要刻画物理节点或支路状态经由 AMI、SCADA、PMU 等量测终端映射为数字量测数据的过程; $\mathcal{E}_t^{DD}$表示数字层内部边, 主要刻画多源数据融合、状态估计、拓扑辨识和数字孪生状态更新等数据处理关系; $\mathcal{E}_t^{DI}$表示数字层到信息层的跨层决策支撑边, 主要刻画数字状态、拓扑辨识结果和风险评估结果对调度控制模块的输入关系; $\mathcal{E}_t^{II}$表示信息层内部边, 主要刻画通信传输、路由协同、保护配合和调度决策协同关系; $\mathcal{E}_t^{IP}$表示信息层到物理层的跨层控制执行边, 主要刻画调度指令、保护动作、拓扑重构和恢复策略对开关、储能、柔性负荷及分布式电源等物理实体的反作用关系.

从业务流属性看, $\mathcal{E}_t^{PP}$主要承载电力流; $\mathcal{E}_t^{PD}$和$\mathcal{E}_t^{DD}$主要承载数据流; $\mathcal{E}_t^{DI}$、$\mathcal{E}_t^{II}$和$\mathcal{E}_t^{IP}$主要承载信息流或控制信息流. 由此, 三层架构中的层内关系与跨层耦合关系被统一刻画为多层异构有向图中的不同类型边.

进一步地, 按照物理层、数字层和信息层的节点顺序排列, 系统整体邻接矩阵可表示为如下分块形式:

$$A_t = \begin{pmatrix} A_t^{PP} & A_t^{PD} & 0 \\ 0 & A_t^{DD} & A_t^{DI} \\ A_t^{IP} & 0 & A_t^{II} \end{pmatrix}. \tag{4}$$

其中, A_t^{PP}、A_t^{DD}和A_t^{II}分别表示三层内部的邻接关系, A_t^{PD}、A_t^{DI}和A_t^{IP}分别表示物理—数字、数字—信息和信息—物理之间的跨层耦合关系.

在新型配电系统图模型中, 节点并不局限于传统电气母线, 而是跨越物理、数字与信息边界, 涵盖物理实体、数字实体和信息决策实体三类. 物理层节点旨在表征配电系统中的真实电气实体, 其节点特征$X_t^P = \{x_{i,t}^P \mid i \in \mathcal{V}^P\}$可表示为:

$$x_{i,t}^P = [V_{i,t}, \delta_{i,t}, P_{i,t}^{\mathrm{G}}, Q_{i,t}^{\mathrm{G}}, P_{i,t}^{L}, Q_{i,t}^{L}, h_{i,t}^{\mathrm{dev}}], \tag{5}$$

其中: $V_{i,t}$为节点电压幅值, $\delta_{i,t}$为电压相角, $P_{i,t}^{\mathrm{G}}$和$Q_{i,t}^{\mathrm{G}}$为电源有功、无功出力, $P_{i,t}^{L}$和$Q_{i,t}^{L}$为负荷有功、

无功需求. 值得注意的是, $h_{i,t}^{\mathrm{dev}}$代表设备的健康状态表征. $h_{i,t}^{\mathrm{dev}}$并非原始传感器数据, 而是由底层特定设备的健康评估子模块映射至统一特征空间后的低维向量或归一化健康指数. 这种映射机制不仅屏蔽了底层物理设备的异构性, 还保证了图神经网络在进行全局拓扑消息传递时的维度一致性与计算稳定性.

数字层节点表示通过量测、状态估计、拓扑辨识得到的物理网络的数字化表征, 数字层节点特征$X_t^D=\{x_{i,t}^D \mid i\in\mathcal{V}^D\}$可表示为:

$$x_{i,t}^D=[z_{i,t},\hat{x}_{i,t},a_{i,t}^D], \tag{6}$$

其中: $z_{i,t}$为量测数据, $\hat{x}_{i,t}$为数字层对物理节点i状态的估计值, 对应物理层节点状态估计集合$\hat{X}_t^P$中的第i个元素, $a_{i,t}^D$表示 FDI 攻击 (False Data Injection, FDI) 强度或攻击标识.

信息层节点表示调度、控制、保护、通信和恢复决策实体. 假设信息层采用支持流量工程的软件定义网络或具有类似队列管理机制的先进通信架构, 其节点特征$X_t^I=\{x_{i,t}^I \mid i\in\mathcal{V}^I\}$可表示为:

$$\begin{aligned}x_{i,t}^I=[&E_{i,t},\mathrm{V}_{i,t}^{mob},F_{i,t},q_{i,t}^{ED},q_{i,t}^{FS},\\&QSR_{i,t},\tilde{c}_{i,t},\bar{c}_{i,t},p_{i,t}^{\mathrm{fwd}},d_{i,t}^{\mathrm{drop}},T_{i,t}^{\mathrm{hist}}],\end{aligned} \tag{7}$$

其中: $E_{i,t}$表示路由器的剩余能量, $\mathrm{V}_{i,t}^{mob}$表示移动通讯实体的移动速度, $F_{i,t}$为通讯节点故障标识, $q_{i,t}^{ED}$和$q_{i,t}^{FS}$分别表示高优先级与低优先级队列的实时缓存长度, $QSR_{i,t}$表示当前分配的队列服务速率, $\tilde{c}_{i,t}$和$\bar{c}_{i,t}$分别表示当前归一化拥塞计时器以及 GNN 预测的未来拥塞状态, $p_{i,t}^{\mathrm{fwd}}$为数据包正常转发率, $d_{i,t}^{\mathrm{drop}}$为恶意选择性丢包率, $T_{i,t}^{\mathrm{hist}}$为历史综合信任分数.

电力流边$\Xi_t^P=\{\xi_{ij,t}^P \mid e_{ij,t}^P\in\mathcal{E}_t^{PP}\}$表示物理层中电气连接、能量传输、潮流分布和故障传播关系, 其边特征可写为:

$$\xi_{ij,t}^P=[\sigma_{ij,t},r_{ij},x_{ij},b_{ij},S_{ij,t},I_{ij,t},T_{ij,t},h_{ij,t}^{\mathrm{line}}], \tag{8}$$

其中: $\sigma_{ij,t}$为支路通断状态, r_{ij}、x_{ij}、b_{ij}分别为线路电阻、电抗和电纳, $S_{ij,t}$为支路视在功率, $I_{ij,t}$为支路电流, $T_{ij,t}$为线路或设备温度, $h_{ij,t}^{\mathrm{line}}$为线路健康状态.

数据流边$\Xi_t^D=\{\xi_{ij,t}^D \mid e_{ij,t}^D\in\mathcal{E}_t^{DD}\cup\mathcal{E}_t^{PD}\}$表示量测采集、遥信上传和数字状态重构关系. 数据流边既可以连接物理节点与数字节点, 也可以连接数字层内部节点.

$$\xi_{ij,t}^D=[z_{ij,t},\hat{\xi}_{ij,t},a_{ij,t}^D], \tag{9}$$

其中: $z_{ij,t}$为物理边状态的量测数据, $\hat{\xi}_{ij,t}$为拓扑辨识得到的数据, $a_{ij,t}^D$为数据攻击或异常扰动.

信息流边$\Xi_t^I=\{\xi_{ij,t}^I \mid e_{ij,t}^I\in\mathcal{E}_t^{II}\cup\mathcal{E}_t^{DI}\cup\mathcal{E}_t^{IP}\}$表示调度策略、控制指令和应急恢复方案的传递与执行关系. 信息流边既可以连接数字层与信息层, 也可以连接信息层内部节点, 还可以连接信息层与物理层.

$$\xi_{ij,t}^I=[A_{ij},LQ_{ij,t},L_{ij,t},HC_{ij,t},\alpha_{ij,t}], \tag{10}$$

其中A_{ij}表示通信节点的邻接矩阵, $LQ_{ij,t}$表示通信链路质量 (如信噪比), $L_{ij,t}$为链路传输延迟, $HC_{ij,t}$为路由跳数, $\alpha_{ij,t}$为关系信任权重.

3 新型配电系统风险管控问题建模

新型配电系统的风险管控问题可解构为四个核心维度: 风险诱因、传播路径、作用后果及其发生概率. 具体而言, 风险诱因广泛潜伏于系统的各个层级. 这些扰动并不会孤立存在, 而是沿着物理-数字-信息的闭环控制链路, 形成跨空间级联扩散的传播路径. 最终的作用后果往往映射回物理实体, 引发设备故障或系统失稳. 量化上述演化过程的发生概率, 是实现主动防御与弹性管控的前提. 图 2 展示了新型配电系统多层异构动态图的风险传播路径.

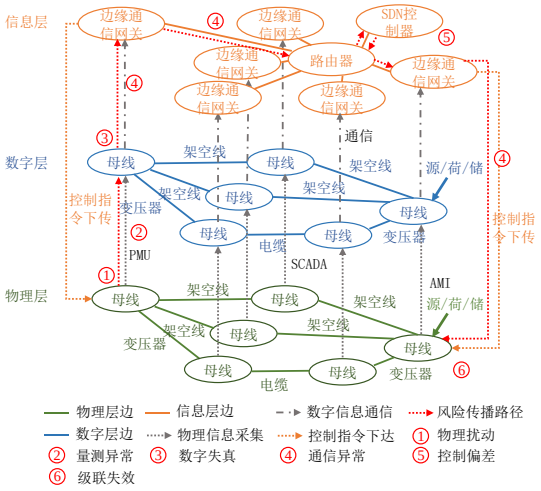

图 2 新型配电系统多层异构动态图风险传播路径

基于上述跨空间交互的风险演化机理, 新型配电系统风险传播路径建模如下:

$$0=F_P(x_t,y_t,\theta_t), \tag{11}$$

$$Z_t=\mathcal{H}_D(x_t)+\varepsilon_t+a_t^D, \tag{12}$$

$$\hat{x}_t=\Psi_D(Z_t,x_t^D), \tag{13}$$

$$\hat{Y}_t=\Pi_I(\hat{x}_t,x_t^I), \tag{14}$$

$$y_t=\mathcal{C}_I(\hat{Y}_t,x_t^I)+a_t^I, \tag{15}$$

式中, 上述模型刻画了物理层、数字层与信息层之间的闭环耦合关系, 即物理状态x_t经量测映射形成数字量测Z_t, 数字层基于Z_t重构估计状态$\hat{x}_t$, 信息层依据$\hat{x}_t$生成控制策略$\hat{Y}_t$, 并进一步形成实际作用于物

理层的控制指令y_t, 而y_t又通过物理层方程$F_P(\cdot)$反馈影响物理状态. 在物理层演化环节, $x_t = \{\mathcal{G}_t^P, X_t^P, \Xi_t^P\}$为$t$时刻的物理层状态变量, 包含拓扑结构、连续运行状态与离散设备状态; y_t为实际作用于物理层的控制指令; θ_t为物理层原生风险诱因; $F_P(\cdot)$表示物理层在控制指令和风险诱因作用下的运行约束或状态演化关系. 在数字层感知与估计环节, Z_t为量测结果; $\mathcal{H}_D(\cdot)$表示由物理状态和物理—数字量测映射关系共同决定的量测函数; $x_t^D = \{\mathcal{G}_t^D, X_t^D, \Xi_t^D\}$为数字层内部状态变量; ε_t为常规采样噪声; a_t^D为FDI 等量测环节的恶意风险诱因; $\Psi_D(\cdot)$表示数字层重构函数; $\hat{x}_t = \{\widehat{\mathcal{G}}_t^P, \widehat{X}_t^P, \widehat{\Xi}_t^P\}$为数字层基于量测数据对物理系统进行状态估计与拓扑辨识的输出结果. 在信息层决策与控制生成环节, $x_t^I = \{\mathcal{G}_t^I, X_t^I, \Xi_t^I\}$为信息层状态变量; $\Pi_I(\cdot)$表示信息层的风险评估与策略生成函数; $\hat{Y}_t$表示基于估计状态生成的理想控制策略; $\mathcal{C}_I(\cdot)$表示控制执行映射函数; a_t^I表示控制指令篡改、控制权劫持或执行逻辑异常等信息层扰动. 由此, 风险扰动可沿物理感知、数字重构、信息决策与控制反馈构成的闭环链路在三层空间中传播. 表 1 总结了新型配电系统风险问题及对应的管控方法.

表 1　新型配电系统多维风险问题与管控方法

系统层级	风险诱因	传播过程/数学模型	作用后果	管控方法
物理层	设备停运	孤岛划分与连通图模型	区域停电	故障定位
	设备健康退化	马尔可夫状态转移模型	设备损坏	设备健康监测
	负荷高频波动/源荷不匹配	功率平衡方程	电压/潮流越限	安全裕度监测, 潮流计算, 最优潮流
	薄弱子图	复杂网络理论	级联故障	薄弱环节辨识
数字层	量测设备不足	欠定方程组求解$Z_t = \mathcal{H}_D(x_t) + \varepsilon_t$	数据不足	状态估计
	开关频繁动作/拓扑记录不同步	隐马尔可夫模型/图结构动态演化模型	系统拓扑未知	拓扑检测与拓扑辨识
	FDI攻击	隐蔽攻击模型$a_t^D = Hc$	状态感知错误	FDI检测
信息层	通信拥塞和断路风险	网络演算延迟边界模型	时延, 无法及时接受信息	路由算法
	信息丢包	伯努利丢包模型/马尔可夫丢包通道模型	信息缺失, 影响决策过程	数据插补
	DoS/DDoS攻击	拒绝服务攻击动力学/博弈论攻防模型	决策背离物理实际情况/拒绝服务	紧急控制, 完整性校验

3.1　新型配电系统物理层风险问题

文献 [7] 指出, 电力灾难往往由局部的偶发事件 (如设备停运) 触发, 在系统被削弱后, 传输功率或者节点电压逼近稳定极限; 若叠加继电保护装置的潜在故障或系统结构的薄弱环节, 局部越限将演变为级联故障. 基于这一时空演化机理, 物理层的风险问题可以从资产管理、运行风险和系统脆弱性三个维度进行描述.

3.1.1　资产管理风险

新型配电系统的资产管理风险主要源于设备健康退化与设备停运两大诱因[8]. 其中, 单个设备的突发性停运可建模为连续时间的马尔可夫过程, 设备在正常运行与故障停运两个状态之间相互转移. 假设设备i的状态变量为$s_i(t)$, $s_i(t) = 1$表示该设备处于正常运行状态, $s_i(t) = 0$表示处于故障停运状态. 状态转移受设备的故障率λ_i和修复率μ_i驱动, 其状态转移概率矩阵可表示为:

$$\mathbf{P}(t) = \begin{pmatrix} P_{11}(t) & P_{10}(t) \\ P_{01}(t) & P_{00}(t) \end{pmatrix}, \tag{16}$$

式中, 矩阵元素$P_{xy}(t) = P(s_i(t) = y \mid s_i(0) = x)$代表设备由初始状态$x$经过时间$t$转移至状态$y$的条件概率. 例如, $P_{10}(t)$表征设备从正常运行跌落至故障停运的动态概率. 在长周期风险评估中, 当时间趋于无穷大 ($t \to \infty$) 时, 设备处于正常运行与故障停运的稳态概率分别收敛为:

$$P_{up,i} = \frac{\mu_i}{\lambda_i + \mu_i}, \tag{17}$$

$$P_{down,i} = \frac{\lambda_i}{\lambda_i + \mu_i}, \tag{18}$$

当设备跌入故障停运状态时, 配电系统动态图模型中的物理拓扑连通性函数$F_P(\cdot)$将受到直接破坏, 进而引发停电事故. 此时, 系统高度依赖数字层的数据交互与信息层的调度决策来隔离故障并缩小停电范围.

另一方面, 设备健康退化则被建模为服从威布尔分布的时变故障率过程. 与突发性停运的常数故障率不同, 设备健康退化表现为物理性能的长期退化, 其故障率$\lambda_i(t)$是随服役时间t单调递增的函数. 在资产风险评估中, 其数学模型可表示为:

$$\lambda_i(t) = \frac{\beta_i}{\eta_i}\left(\frac{t}{\eta_i}\right)^{\beta_i - 1}, \tag{19}$$

式中, β_i为形状参数, 表征老化速率; η_i为尺度参数, 表征设备的特征寿命. 随着老化的加剧, 设备发生不可逆损坏的风险显著上升, 同样会触发拓扑破坏与停电事故.

需要说明的是, 式 (16)–式 (18) 中的马尔可夫停运模型与式 (19) 中的威布尔老化模型分别对应不同时间尺度和不同风险口径. 前者主要用于描述短时间运行评估窗口内设备在正常运行、故障停运和修复恢复状态之间的随机切换, 其中故障率和修复率在给定评估窗口内近似为常数; 后者主要用于描述长时间服役尺度下设备老化退化导致的时变失效风险, 其故障率随服役时间变化. 因此, 二者分别用于刻画突发停运风险和长期老化失效风险, 并非在同一齐次马尔可夫模型中直接混用.

然而, 随着配电系统向柔性化与数字化演进, 海量分布式资源的接入使得单个设备的运行环境复杂化. 传统解析模型通常将设备视为孤立个体, 依赖静态、同质化的参数假设. 实际上, 设备的老化速率与停运风险已不再独立, 而是与局部的多向潮流、动态负荷波动以及邻近设备的工况高度耦合[9]. 面对这种设备状态的非线性特征与隐式的空间关联, 传统独立概率模型难以进行精准刻画. 因此, 在资产管理维度, 亟需引入能够天然处理非欧几里得空间拓扑、深度挖掘节点间隐式依赖关系的先进数据驱动方法, 从而实现对复杂工况下设备风险特征的精准提取与动态评估.

3.1.2 运行风险

新型配电系统的运行风险主要源于高频波动的负荷与海量分布式电源接入所带来的不确定性. 在运行层面, 这种不确定性表现为源荷功率的随机波动, 而不良后果则体现为系统电压越限或潮流过载, 进而危害系统的稳定性.

具体而言, 节点注入的有功功率$P_{i,t}^{inj}$与无功功率$Q_{i,t}^{inj}$不再是确定性参量, 而是服从特定概率分布的随机变量: $P_{i,t}^{inj}=P_{i,t}^{\mathrm{G}}-P_{i,t}^{L}$, $Q_{i,t}^{inj}=Q_{i,t}^{\mathrm{G}}-Q_{i,t}^{L}$.

这些随机波动作为扰动源, 通过非线性的潮流方程在电网拓扑中传播, 进而引发节点电压幅值$V_{i,t}$与相角$\delta_{i,t}$的随机偏移:

$$P_{i,t}^{inj}=V_{i,t}\sum_{j=1}^{N}V_{j,t}(G_{ij}\cos\delta_{ij,t}+B_{ij}\sin\delta_{ij,t}),\quad(20)$$

$$Q_{i,t}^{inj}=V_{i,t}\sum_{j=1}^{N}V_{j,t}(G_{ij}\sin\delta_{ij,t}-B_{ij}\cos\delta_{ij,t}),\quad(21)$$

式中, N为系统节点总数; G_{ij}与B_{ij}分别为节点导纳矩阵元素的实部 (电导) 与虚部 (电纳); $\delta_{ij,t}=\delta_{i,t}-\delta_{j,t}$为节点$i$与$j$之间的电压相角差.

因此, 运行风险可被量化为系统状态变量突破安全边界的概率. 传统的风险管控通常依赖概率潮流计算来获取状态变量的概率密度函数, 监测功率裕度, 并结合最优潮流进行预防性调度.

然而, 随着柔性资源的深度渗透, 系统呈现出高度的非线性与复杂的时空耦合特性. 传统基于物理模型的概率评估方法面临着严重的"维度灾难"与计算耗时瓶颈, 难以满足海量场景下实时预警的需求[10]. 此外, 源荷波动往往具有强烈的空间相关性, 传统解析方法难以捕捉这些拓扑依赖. 因此, 在运行风险评估维度, 亟需引入具备拓扑感知能力的智能算法. 这类方法能够直接从海量数据中学习不确定性在复杂网络中的非线性传播规律, 从而提升计算效率, 实现对越限风险的高效、端到端评估.

3.1.3 系统脆弱性风险

由于配电系统的辐射状拓扑特征与海量源荷的局部聚集, 造成节点间的运行越限与设备故障风险高度耦合, 极易出现抗扰动能力极差的脆弱连通区域, 构成了图论视角下的薄弱子图. 薄弱子图的存在使得系统在遭受扰动后极易引发级联故障, 导致事故范围扩大.

薄弱子图可以建模为配电系统全局动态图$\mathcal{G}=(\mathcal{V},\mathcal{E})$的一个连通子集$\mathcal{G}_{sub}=(\mathcal{V}_{sub},\mathcal{E}_{sub})$. 其中, $\mathcal{V}_{sub}\subseteq\mathcal{V}$为高风险节点集合, $\mathcal{E}_{sub}\subseteq\mathcal{E}$为连接这些节点的脆弱支路集合. 该模型不仅保留了局部的非欧几里得空间拓扑, 其节点与边还分别承载了物理层的节点特征与边特征.

需要说明的是, 薄弱子图风险概率是在给定运行场景、给定网络拓扑和给定扰动分布条件下定义的, 主要用于单一时间断面的静态风险评估. 该定义并不假设子图内节点越限事件与支路故障事件相互独立, 而是用于描述子图内至少一个节点发生电压越限, 或至少一条支路发生过载、断开等异常状态的并集事件概率. 若进一步考虑故障传播和保护动作引起的时序演化过程, 则应将该风险概率扩展为给定时间窗口内的时序联合风险事件. 实际计算中, 该概率可通过蒙特卡洛仿真、联合概率模型或数据驱动图模型近似获得. 考虑到子图内部强烈的时空相关性, 其整体风险概率$Pr(\mathcal{G}_{sub}^{risk})$可定义为子图内任意节点突破运行安全边界, 或任意支路发生物理故障的并集概率:

$$\begin{aligned}\Pr(\mathcal{G}_{\mathrm{sub}}^{\mathrm{risk}})=\Pr\{&\bigcup_{i\in\mathcal{V}_{\mathrm{sub}}}\{V_{i,t}\notin[V_{\min},V_{\max}]\}\\&\cup\bigcup_{j\in\mathcal{E}_{\mathrm{sub}}}(\{S_{j,t}>S_{j,\max}\}\cup\{\sigma_{j,t}=0\})\},\end{aligned}\quad(22)$$

式中, $V_{\min}$与$V_{\max}$分别为节点电压的安全运行下限与上限; $S_{j,t}$与$S_{j,\max}$分别为支路j的实时视在功率及其热稳定容量 (或传输极限) 上限; $\sigma_{j,t}=0$表示支路j发生物理断开.

由于薄弱子图内各元素的故障与越限并非独立事件, 传统基于解析方程的联合概率计算面临着高维积分难题[11]. 因此, 亟需引入能够聚合局部邻域高维特征的图表示学习技术, 通过信息传递机制直接逼近上述复杂的联合风险概率函数, 从而实现对薄弱子图的精准识别与风险量化.

3.2 新型配电系统数字层风险问题

在新型配电系统中, 数字层的核心任务是实现精准的系统态势感知与状态估计. 然而, 数字层在复杂运行环境下正面临多维度的风险威胁. 在客观观测条件方面, 受限于经济成本与通信带宽, 有限的量测配置与多源数据的时间异步交织, 导致系统长期处于量测稀疏的弱可观测状态; 同时, 频繁的物理开关动作若未被 DMS 实时同步, 将引发物理实体与数字记录不对称的拓扑未知风险. 在主观外部扰动方面, 高度开放的通信环境进一步使得系统暴露于 FDI 等恶意网络攻击之下, 直接破坏量测数据的完整性与真实性. 上述客观制约与恶意扰动的叠加, 将共同导致数字层的状态感知错误, 进而误导信息层的调度决策.

3.2.1 量测稀疏风险

由于新型配电系统规模庞大, 考虑到经济成本与通信带宽的限制, 仅依赖高频实时量测设备无法实现全网的完全可观测. 因此, 配电系统状态感知高度依赖于伪量测与虚拟量测来弥补实时数据的空间稀疏性. 这种量测结构的不足与多源数据的时间异步, 构成了数字层的量测稀疏风险[12].

具体而言, 基于公式 (12) 的量测映射模型, 数字层在t时刻的混合量测向量Z_t可表示为不同类型数据的堆叠:

$$Z_t=\begin{bmatrix}Z_t^{rt}\\ Z_t^{ps}\\ Z_t^{vi}\end{bmatrix}=\mathcal{H}_D(x_t)+\begin{bmatrix}\varepsilon_t^{rt}\\ \varepsilon_t^{ps}\\ \varepsilon_t^{vi}\end{bmatrix}, \tag{23}$$

式中, Z_t^{rt}为实时量测数据, 其误差ε_t^{rt}较小但空间分布极度稀疏; Z_t^{vi}为虚拟量测, 其误差$\varepsilon_t^{vi}\approx 0$; 而$Z_t^{ps}$为基于历史负荷曲线生成的伪量测.

在新型配电系统中, 由于分布式电源的接入与柔性负荷的随机波动, 传统基于单一高斯分布的伪量测建模已失效, 伪量测误差ε_t^{ps}表现出极强的不确定性, 通常需要采用高斯混合模型等多峰概率密度函数进行刻画. 此外, 不同量测设备间存在显著的时间异步与数据延迟, 进一步加剧了整体量测矩阵的误差.

因此, 量测稀疏风险可以被量化为: 在极高伪量测不确定性与时间异步扰动下, 数字层输出的状态估计值$\hat{x}_t$严重偏离物理层真实状态x_t的概率:

$$Pr(\mathcal{R}_{sparse})=Pr(||\hat{x}_t-x_t||_2>\epsilon \mid Z_t^{ps}\sim \mathrm{GMM},\Delta t), \tag{24}$$

式中, Δt表征多源量测数据的时间偏差扰动; ϵ为系统可容忍的估计误差上限.

传统的配电系统状态估计通常采用加权最小二乘法 (Weighted Least Square, WLS). 然而, 在量测极度稀疏的场景下, WLS 方法为了维持可观测性, 不得不大量引入高方差的伪量测. 这不仅可能导致雅可比矩阵呈现病态特征, 还会使估计结果被伪量测的巨大误差所淹没[13-14]. 因此, 在数字层感知维度, 亟需引入具备强大学习能力与拓扑感知特征的数据驱动方法, 在稀疏且异步的量测空间中实现对系统真实状态的重构.

3.2.2 拓扑未知风险

为了满足维护检修、负荷平衡以及极端天气后的抢修复电等需求, 配电系统会通过频繁切换断路器与联络开关状态进行动态重构. 然而, 这些频繁的物理层拓扑变更往往无法被实时、准确地同步记录至配电管理系统 (Distribution Management System, DMS) 中. 这种物理拓扑与数字层记录之间的信息不对称, 构成了数字层的拓扑未知风险.

具体而言, 数字层状态感知高度依赖于量测映射函数$\mathcal{H}_D(\cdot)$, 而该函数由系统的拓扑结构决定. 当发生未记录的拓扑重构时, DMS 中记录的数字层先验拓扑$\mathcal{G}_t^D$将偏离配电系统的真实物理拓扑$\mathcal{G}_t^P$(即物理状态x_t中的拓扑分量), 导致映射关系发生根本性错误. 这使得原本用于重构物理状态的函数$\Psi_D(\cdot)$建立在错误的基准之上.

在新型配电系统中, 由于分布式能源 (Distributed Energy Resources, DERs) 与电动汽车等负荷的快速增长, 源荷功率表现出剧烈的随机波动. 根据先验信息的缺失程度, 拓扑未知主要表现为拓扑检测与拓扑辨识. 在高度不确定的运行环境下, 拓扑错误引发的量测异常极易与正常功率波动相互混淆.

因此, 拓扑未知风险可以被量化为: 在依赖错误的先验拓扑进行状态估计时, 状态感知结果$\hat{x}_t$严重偏离真实状态x_t的概率:

$$Pr(\mathcal{R}_{topology})=Pr(||\hat{x}_t-x_t||_2>\epsilon \mid \mathcal{G}_t^D\neq\mathcal{G}_t^P), \tag{25}$$

式中, ϵ为系统可容忍的估计误差上限.

传统的配电系统状态估计通常将精确的运行拓扑作为构建雅可比矩阵与求解非线性方程的绝对前提. 然而, 当遭遇拓扑未知或错误时, WLS 方法会产生状态估计残差甚至直接发散[15]. 尽管传统解析方法试图通过归一化残差分析来纠正拓扑错误, 但在源荷剧烈波动下极易发生误判. 因此, 在数字层感知维度, 亟需引入具备强大学习能力与天然图结构处理能力的数据驱动方法, 在拓扑残缺或失真的恶劣数字环境下实现对系统真实状态的重构.

3.2.3 虚假数据注入风险

基于新型配电系统物理信息深度融合的特性, 恶意攻击者可能利用通信协议漏洞或设备后门, 绕过网络防火墙, 向 DMS 发送被篡改的虚假量测数据. 这种蓄意破坏数据完整性与真实性的网络攻击行为, 构成了数字层的虚假数据注入 (False Data Injection, FDI) 风险.

具体而言, 如风险传播模型所述, 在遭受 FDI 攻击时, 数字层接收到的混合量测向量Z_t中已被叠加了恶意的攻击向量a_t^D. 为了逃避传统状态估计的坏数据检测 (Bad Data Detection, BDD) 机制, 高阶攻击者通常会利用获取到的系统部分拓扑与参数信息, 构造隐蔽型攻击向量. 其核心逻辑是使得篡改后的量测数据仍然符合物理定律的映射关系, 即$a_t^D \approx \mathcal{H}_D(x_t + c) - \mathcal{H}_D(x_t)$, 其中$c$为攻击者期望引入的状态偏差.

在新型配电系统中, 海量 DERs 的接入与柔性负荷的剧烈波动, 为 FDI 攻击提供了天然的"掩护". 攻击者可以将其注入的虚假数据伪装成光伏出力的突变或电动汽车的集中充电行为. 此外, 配电系统频繁的拓扑重构使得量测映射函数$\mathcal{H}_D(\cdot)$处于动态变化之中, 攻击者可伺机在拓扑切换或系统处于弱可观测状态时发动攻击. 这种高隐蔽性与强欺骗性, 使得正常的物理波动与恶意的网络攻击在数据表征上难以区分.

因此, 虚假数据注入风险可以被量化为: 在攻击向量a_t^D成功绕过坏数据检测阈值τ_{th}的前提下, 导致数字层输出的状态估计值$\hat{x}_t$严重偏离物理层真实状态x_t的概率:

$$\begin{aligned}\Pr(\mathcal{R}_{\text{FDI}}) = \Pr(\|\hat{x}_t - x_t\|_2 > \epsilon \,|\, a_t^D \neq 0,\\ \|Z_t - \mathcal{H}_D(\hat{x}_t)\|_2 < \tau_{\text{th}}).\end{aligned} \tag{26}$$

式中, ϵ为系统可容忍的估计误差上限; $||Z_t - \mathcal{H}_D(\hat{x}_t)||_2 < \tau_{\text{th}}$表征该攻击具备极强的隐蔽性.

传统的配电系统坏数据检测通常基于 WLS 的量测残差分析. 然而, 由于隐蔽型 FDI 攻击在数学构造上天然保证了低残差特性, 传统基于解析方程的残差检验方法失效, 极易发生漏判[16]. 面对这种精心伪装的恶意扰动, 亟需引入具备强大学习能力与拓扑感知特征的数据驱动方法. 这类方法能够超越单一节点的数值检验, 通过深度挖掘全局拓扑空间中多源节点间的物理耦合不变量与时序演化规律, 在遭受恶意篡改的数字环境中实现对虚假数据的精准隔离与系统真实状态的鲁棒重构.

3.3 新型配电系统信息层风险问题

新型配电系统信息层承担着海量数据与控制指令的交互任务, 其通信可靠性直接决定了系统的稳定运行. 然而, 信息层在复杂交互环境中正面临多维度的风险威胁[17]. 一方面, 受限于通信带宽的物理上限与突发硬件故障, 数据传输不可避免地会遭遇常规的通信拥塞与链路断路, 导致控制信号严重滞后或彻底中断; 另一方面, 异构网络中的信道衰落与节点缓存溢出, 会引发高频次的常规信息丢包, 破坏感知与控制数据的连续性; 最后, 信息层极易遭受拒绝服务 (DoS) 等网络攻击, 攻击者通过蓄意耗尽带宽与算力资源, 发起跨空间的信息物理协同破坏. 上述多源扰动的叠加, 将直接摧毁闭环控制链路的可靠性, 进而威胁全网的安全稳定.

3.3.1 常规通信拥塞风险

新型配电系统的广域状态感知与闭环控制高度依赖于底层通信网络 (如光纤、5G、无线专网等) 的数据交互. 然而, 受限于通信带宽的物理上限、恶劣环境下的电磁干扰以及路由器或基站等硬件设备的突发故障, 数据在传输过程中不可避免地会遭遇排队拥塞. 这种由客观物理限制与环境干扰引发的数据传输滞后, 构成了信息层的常规通信拥塞风险问题.

具体而言, 基于网络演算与信道衰落理论, 信息层在t时刻接收到的实际信号$\tilde{y}_t$(如量测数据或控制指令) 可建模为理想信号y_t在时间与空间维度的畸变:

$$\tilde{y}_t = l_t y_{t-\tau_t}, \tag{27}$$

式中, τ_t为表征通信拥塞程度的时变延迟, 通常由排队延迟与传输延迟叠加而成; $l_t \in \{0, 1\}$为表征物理链路连通性的离散状态变量 (该变量直接对应于式 (4) 中信息流边的邻接矩阵元素A_{ij}的时变演化), $l_t = 1$表示链路正常, $l_t = 0$则表示发生通信断路, 此时接收端将完全丢失该时刻的信息.

在新型配电系统中, 海量 DERs 的即插即用与

微电网的孤岛切换等操作, 对信息交互的实时性提出了毫秒级的苛刻要求. 当系统发生短路故障或负荷剧烈波动时, 海量终端设备会同时向 DMS 并发海量告警数据, 极易引发"信暴"现象, 导致排队延迟τ_t呈指数级激增. 此外, 海量暴露在户外的无线物联网 (Internet of Things, IoT) 终端受气象条件影响极大, 其链路状态l_t呈现出强烈的随机跳变特征.

因此, 常规通信拥塞和断路风险可以被量化为: 在极端的时延扰动或物理链路断开的恶劣通信环境下, 系统实际运行状态x_t偏离安全基准x_{ref}或突破安全边界的概率:

$$\Pr(\mathcal{R}_{\text{comm}}) = \Pr(\|x_t - x_{\text{ref}}\|_2 > \epsilon \mid \tau_t > \tau_{\max} \ \vee \ l_t = 0). \tag{28}$$

式中, τ_{max}为系统闭环控制所能容忍的最大临界时延; ϵ为系统可容忍的最大状态偏差界限.

传统的配电系统应对通信延迟与中断的方法, 通常依赖于固定时延裕度的鲁棒控制, 或采用简单的"零阶保持器"(Zero-Order Hold, ZOH) 策略维持上一时刻的量测值. 然而, 在新型配电系统源荷剧烈波动的场景下, 长期的数据冻结或过度的保守裕度不仅会导致控制性能严重下降, 甚至会引发系统振荡与失稳[18]. 因此, 在信息层传输维度, 亟需引入具备时空序列建模与跨节点特征聚合能力的数据驱动方法. 这类方法能够打破孤立通信链路的局限, 通过深度挖掘全局网络中相邻健康节点间的空间相关性与历史时序规律, 在局部通信瘫痪的劣态环境下, 实现对缺失信息的精准推演与系统状态的弹性恢复.

3.3.2 常规信息丢包风险

在新型配电系统的广域量测与控制体系中, 数据包需要经过多级路由与异构通信网络 (如光纤与无线专网的混合组网) 进行传输. 受限于无线信道的衰落效应、环境噪声干扰以及网络节点的缓存溢出, 部分数据包在传输过程中会被不可逆地丢弃. 这种非恶意的、由客观通信环境与硬件瓶颈导致的数据缺失, 构成了信息层的常规信息丢包风险问题.

具体而言, 有别于通信断路导致的连续性信息中断, 常规丢包通常表现为离散的随机过程. 基于伯努利 (Bernoulli) 分布或吉尔伯特-埃利奥特 (Gilbert-Elliott) 马尔可夫通道模型, 信息层在t时刻接收到的混合量测向量$\tilde{Z}_t$可建模为理想量测向量Z_t经过丢包矩阵D_t过滤后的结果:

$$\tilde{Z}_t = (I - D_t)Z_t = \text{diag}(1 - d_{1,t}, 1 - d_{2,t}, \ldots, 1 - d_{m,t})Z_t. \tag{29}$$

式中, m为量测通道的总数; I为单位矩阵; $d_{i,t} \in \{0,1\}$为第i个通道在t时刻的丢包指示变量. 当$d_{i,t} = 0$时表示数据成功接收, 当$d_{i,t} = 1$时表示该数据包丢失. 在马尔可夫通道模型中, 丢包状态的转移概率受当前网络拥塞程度与信道质量的动态影响.

在新型配电系统中, 随着微型同步相量测量装置 (μPMU) 等高频量测设备的广泛部署, 数据采样率已提升至百赫兹级别. 这种海量高频数据的并发传输极易导致通信节点的队列缓存溢出, 引发突发性的大规模丢包. 此外, 配电系统末端的分布式电源与柔性负荷往往处于无线信号覆盖的边缘区域, 其量测数据在恶劣天气或电磁干扰下呈现出极高的随机丢包率. 这种高频次、空间分布不均的信息缺失, 严重破坏了数字层状态感知的完整性.

因此, 常规信息丢包风险可以被量化为: 在极高的随机丢包率或突发性连续丢包扰动下, 数字层基于残缺量测矩阵$\tilde{Z}_t$输出的状态估计值$\hat{x}_t$严重偏离物理层真实状态x_t的概率:

$$\Pr(\mathcal{R}_{\text{loss}}) = \Pr(\|\hat{x}_t - x_t\|_2 > \epsilon \mid \text{tr}(I - D_t) < m_{\text{obs}}). \tag{30}$$

式中, ϵ为系统可容忍的估计误差上限; $\text{Trace}(I - D_t)$表示当前成功接收的量测数据总数; m_{obs}为维持系统拓扑可观测性的最低量测数量阈值. 需要说明的是, 该数量阈值主要用于表征量测冗余不足的工程预警状态, 严格的可观测性还取决于量测类型、量测位置及网络拓扑等因素. 若将丢包后的有效量测雅可比矩阵记为H_t^{obs}, 待估计状态变量维度记为n_x, 则可观测性丧失可由如下秩条件刻画:

$$\text{rank}(H_t^{obs}) < n_x. \tag{31}$$

传统的配电系统应对丢包的方法通常采用简单的数据插值或基于卡尔曼滤波 (Kalman Filter) 的状态预测. 然而, 在新型配电系统中, 源荷功率的波动呈现出极强的非线性与非平稳特征, 简单的数学插值往往会引入巨大的截断误差; 而卡尔曼滤波在面对连续丢包导致的可观测性丧失时, 其预测协方差矩阵会迅速发散[19-20]. 因此, 在信息层数据恢复维度, 亟需引入具备时空相关性挖掘与高维特征重构能力的数据驱动方法. 这类方法能够超越单一时间维度的预测, 通过联合挖掘全局网络中相邻节点的空间耦合关系与历史演化规律, 在量测数据严重缺失的恶劣通信环境下, 实现对丢失信息的高精度插补与系统状态的连续重构.

3.3.3 DoS/DDoS 攻击风险

网络攻击分为数据完整性攻击和可用性攻击. 常规的数据完整性攻击 (如 FDI) 旨在篡改数据内容,

已被划分在数字层; 而信息层的网络攻击主要表现为破坏系统通信与算力资源的拒绝服务 (Denial of Service, DoS) 或分布式拒绝服务 (DDoS) 攻击. 这种蓄意阻断数据传输通道、导致决策指令或量测信息严重滞后甚至完全丢失的恶意行为, 构成了信息层的 DoS/DDoS 攻击风险问题.

具体而言, DoS/DDoS 攻击通过向目标节点 (如边缘计算网关或控制中心) 发送海量伪造请求, 耗尽其网络带宽或 CPU 算力. 在新型配电系统的闭环控制链路中, 该攻击可建模为时变的时延与丢包过程. 假设物理层在t时刻的真实状态量或控制指令为y_t, 信息层接收端获取的实际信号$\tilde{y}_t$可表示为:

$$\tilde{y}_t = (1-d_t)y_{t-\tau_t}, \tag{32}$$

式中, τ_t为信息传输的动态时延; $d_t \in \{0,1\}$为丢包指示变量 ($d_t=1$表示由于攻击导致数据包完全丢失). 在遭受 DoS 攻击时, 时延τ_t将急剧增加并远超系统的最大容忍时延τ_{max}, 同时伴随极高的丢包率.

在新型配电系统中, 海量 DERs 与柔性负荷的即插即用高度依赖于低延迟、高频次的信息交互. 传统的集中式调度正在向云边协同的分布式控制演进, 这使得暴露在户外的海量 IoT 终端与边缘计算节点成为 DoS 攻击的天然标靶. 当局部区域遭受可用性攻击时, 不仅会导致该区域的源荷失去控制, 这种信息流的阻塞还会通过物理层的功率耦合迅速向全网蔓延, 引发大面积的电压越限或频率失稳.

因此, 信息层的 DoS/DDoS 攻击风险可以被量化为: 在遭受 DoS 攻击导致严重时延或丢包的条件下, 系统实际运行状态x_t偏离安全基准x_{ref}或突破安全边界的概率:

$$\begin{aligned}\Pr(\mathcal{R}_{\mathrm{DoS}}) = \Pr(\|x_t - x_{\mathrm{ref}}\|_2 > \epsilon \,|\\ \tau_t > \tau_{\max} \ \vee \ d_t = 1).\end{aligned} \tag{33}$$

式中, ϵ为系统可容忍的最大状态偏差界限; τ_{max}为维持闭环控制稳定性的临界时延.

传统的防御机制通常依赖于网络层的流量清洗或基于解析模型的时延鲁棒控制算法. 然而, 面对新型配电系统海量节点的高维状态空间与极其复杂的非线性动态, 传统控制理论在处理这种极端的、大范围的信息缺失时, 往往面临模型失配与计算发散的困境[21]. 因此, 在信息层安全维度, 亟需引入具备时空序列建模与跨节点特征聚合能力的数据驱动方法. 这类方法能够利用未受攻击区域的健康数据与历史时序规律, 在通信链路局部瘫痪的恶劣环境下, 实现对缺失信息的精准插补与控制指令的智能重构.

4 GNN 在新型配电系统风险管控的应用

图神经网络具有面向非欧结构数据的特征提取能力, 可通过消息传递机制聚合节点状态、边属性及局部子图结构信息. 该机制与异构动态图风险模型中的节点风险映射、边风险映射和子图风险刻画具有内在一致性: 节点表示可用于描述电压裕度、设备状态和控制资源状态等节点级风险; 边表示可用于刻画电力流、数据流和信息流中的传输风险与耦合关系; 子图表示则可用于识别薄弱供电区域、拥塞通信链路集合和控制执行链路集合. 基于上述对应关系, GNN 可为新型配电系统物理-数字-信息三层架构风险管控问题提供统一的图学习支撑. 表 2 从系统层级、风险场景、代表文献、图学习任务、GNN 方法、验证算例和性能指标等维度, 对 2021 年至 2026 年基于 GNN 的新型配电系统风险管控代表性研究进行对比总结. 不同文献采用的测试系统、数据规模、量测配置、攻击强度和指标定义并不完全一致, 因此本文主要归纳其算例类型和评价指标, 不对不同文献中的数值结果进行简单排序.

4.1 GNN 在物理层风险管控中的应用

针对物理层中源荷波动引发的连续状态越限、设备停运、设备健康退化导致的离散节点失效, 以及局部故障跨区蔓延引发的级联崩溃等问题, GNN 凭借其强大的非欧几里得空间建模与拓扑感知能力, 为物理层风险管控提供了全新的数据驱动范式. 通过在快速潮流计算、资产健康建模、薄弱子图辨识以及拓扑重构等场景中的深度应用, GNN 能够实现对潜在风险的高效预警与主动阻断. 图 3 展示了 GNN 在物理层风险管控中的应用场景.

4.1.1 GNN 在资产管理风险问题中的应用

设备的老化退化与突发停运高度依赖于其所处的局部运行环境与网络拓扑. GNN 能够打破传统解析模型将设备视为孤立个体的局限, 通过图表示学习融合设备历史工况、气象环境、负载水平及邻域状态, 实现对资产健康状态的时空联合建模.

针对资产管理风险中的设备健康退化问题, GNN 能够融合设备历史运行数据、环境状态、负载水平、检修记录和邻域运行条件, 对节点设备和支路线路的健康状态进行时空建模. 文献 [22] 提出了一种残差感知时空 GNN 方法, 通过注意力机制构建随时间变化的传感器图, 利用切比雪夫 (Chebyshev) 谱图卷积聚合多变量数据采集与监视控制系统 (Supervisory Control and Data Acquisition, SCADA) 信号间的局部空间关联, 并结合带残差连接的门控

表 2　GNN 在新型配电系统风险管控中的代表性研究与算例指标对比

层级	风险场景	代表文献	图学习任务	GNN方法	典型算例	对应指标
物理层	设备停运与健康退化	[22,53-54]	故障定位、健康评估	GCN; GAT; STGNN; 时空GNN	IEEE 118、PowerGraph子图、风电场和变压器SCADA; 识别短路、接地、电压失稳、风机异常和变压器退化	Acc=95.1%、F1=0.896、AUC=0.945; 变压器预测RMSE=0.149, 异常检测F1最高0.91
	负荷高频波动/源荷不匹配	[55-60]	电压/潮流预测、安全裕度评估、OPF辅助	PG-GNN; MD-GCN; GCNII; Meta-GGAE; 异构GCN	IEEE多系统、Polish系统、759/2516节点配电网; 考虑风光、EV、储能、负荷不确定性、量测缺失、N-1/N-2和拓扑变化	潮流/MCS提速约4–100倍, OPF提速约250–800倍; 1 MW功率平衡容差满足率99.7%, 备用/削减误差低于0.22%, 成本误差低于0.4%
	薄弱子图	[61-65]	薄弱子图辨识	GCN; GCN-LSTM; PI-GNN; GPIAN; 统计增强GNN; HCGNN	IEEE 24/39/118、法国2868节点、PowerGraph、TEP和真实煤磨机组; 考虑高比例风电、三相接地、N-k停运、脱网及故障传播	IEEE 39节点Acc=99.1%, 118节点Edge/Node PR-AUC=0.991/0.973; GPIAN Acc=0.9873–0.9964, 推理约11.4k–12.6k FPS; 事故筛选Acc=0.98、F1=0.95
数字层	量测稀疏	[34,66-72]	状态估计	GCN; 物理信息GNN; TGCN; Power-GNN	低数据可用率、传感器噪声、发电机节点可观测和Kron降阶场景; 基于拓扑、潮流约束和少量量测估计电压/相角及等效导纳	估计误差接近稀疏感知状态估计器; TGCN类方法较张量补全方法提速约100–1000倍; 559节点拓扑识别Acc=92.1%, 平均3.18 s
	拓扑未知	[39,73-75]	拓扑辨识、拓扑检测	PFGCN; 物理约束GCN; 潮流图卷积	IEEE 33和改进IEEE 69节点配电网; 基于电压幅值、有功/无功功率、DDTW和AC潮流图卷积, 在无相角量测下识别拓扑和线路参数	IEEE 33系统电导/电纳MAPE=4.6%/5.7%, IEEE 69系统为3.0%/5.9%; R^2最高0.999, 0.2%量测误差下MAPE仍低于10%
	FDI攻击	[76-83]	FDI检测	GAE; CR-GAE; AAGAE; ARMA-GNN; 图谱GNN; Cheb-GCN; 时空图自编码器	IEEE 14/39/57/118/300节点和CPDS算例; 构造重放、随机、通用、战略重放、数据投毒及电压稳定FDIA, 融合潮流、D-PMU、通信日志和拓扑特征	GAE类方法检测率和泛化性优于传统非图模型; CR-GAE在投毒和未知FDIA下检测率仅降约1.6%–3.7%; ARMA-GNN支持毫秒级检测与母线定位, 时空图模型可区分Normal、Power、Cyber和Cyber-Power事件
信息层	通信拥塞和断路	[84-86]	路由优化	GCN-DRL; GCN-DQN; 图强化学习; 图注意力路由	TSN、IoT通信网络和CPS恶意流量检测; BA网络、20/50节点IoT拓扑和Raspberry Pi实时测试, 考虑队列、带宽、优先级、安全权重和流量特征	GCN-DRL较DQN/Q-learning/最短路径降低端到端时延, PER使收敛由约80轮降至约60轮; GCN-DQN在50节点推理0.257 s/episode; 恶意流量识别Acc=0.99、Precision=1.0
	信息丢包	[87-89]	数据插补	GAT; 图注意力插补; 时空GNN; 图结构缺失鲁棒学习	Texas 2000、Siemens 1648、IEEE 30/39/57/118、NPCC 140和NREL 1649站点; 考虑随机/行/列/块缺失、通信中断、FDIA和10%–90%时空缺失	图嵌入恢复在随机/行/列/块缺失下RRE=-55.36/-42.06/-53.26/-45.32 dB; 生成式恢复RMSE低至0.0016, IEEE 39恢复约0.14 s; GAT类光伏预测在1649站点上精度提升约6.31%–11.65%, GPU使用降低79%–82%
	DoS/DDoS攻击	[90-93]	紧急控制、完整性校验	CP-GNN; Cheb-GCN; GDN-PINN; GCN; GraphSAGE; GIN	IEEE 14/30网络物理平台、多源SCADA/ICS数据、SDN智能电网通信、CIC-IDS2017、改进New England 39节点和420 MW DFIG风电场; 检测DoS/DDoS、FDI、勒索、后门、远程跳闸和混合攻击	CP-GNN在IEEE 30节点DR=98.3%、FA=3.2%、F1=98.1%; Hybrid AI框架Acc=98.6%、F1=0.98, 可提前约2.3 s识别失稳; GDN-PINN Acc=98.30%、FNR=0.43%、响应0.73 s, 配套紧急控制可在10–15 s内稳定系统

注: Acc、DR、FA、FNR、PR-AUC、RRE、FPS等分别为准确率、检测率、误报率、漏报率、精确率–召回率曲线下面积、相对恢复误差和每秒处理帧数; N-k为k重元件停运, D-PMU、CPDS、TSN、PER、BA分别为配电同步相量测量单元、网络物理配电系统、时间敏感网络、优先经验回放和Barabási–Albert无标度网络. 不同文献结果不宜直接横向比较.

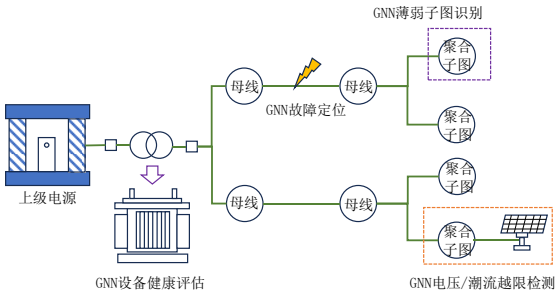

图 3　GNN 在物理层风险管控中的应用

循环单元 (Gated Recurrent Unit, GRU) 建模时间演化特征, 实现了对电力变压器健康状态的预测、健康指标构建和异常检测. 文献 [23] 综述 GNN 在工业物联网异常检测中的应用方法, 通过将传感器、设备及其运行关联关系建模为图结构, 利用 GNN 对点异常、上下文异常和群体异常进行关系挖掘与状态识别, 为智能能源场景下线路及相关设备的健康状态检测提供了图级异常检测思路.

针对设备故障停运问题, GNN 能够深度融合实

时量测、保护动作与全局拓扑信息, 实现故障停运的鲁棒辨识与定位. 文献 [24] 提出了一种基于图学习的配电系统停运检测框架, 利用全局结构编码器聚合全网运行特征, 并通过可微分池化提取稳健的局部子图表示, 从而同时捕捉拓扑相关的全局停运模式与拓扑不变的局部特征. 该方法结合加权因果推断削弱了混杂因素的干扰, 显著提升了模型在未知拓扑下的泛化能力. 此外, 针对拓扑重构场景下的故障定位难题, 文献 [25] 设计了两阶段图时空注意力网络 (Ts-GSAN). 该方法在低可观测条件下, 通过图注意力机制精准刻画了拓扑变更导致的故障电流传播路径变化及特征衰减规律, 实现了复杂工况下的精准故障定位.

4.1.2 GNN 在运行风险问题中的应用

在运行风险问题中, 源荷功率的剧烈波动通过非线性潮流方程在网络中传播. GNN 能够利用多跳邻域的消息传递机制, 直接从海量运行数据中逼近节点电压裕度、支路潮流与全局拓扑之间的非线性映射关系, 解决概率潮流计算的"维度灾难".

针对物理层的运行风险问题, GNN 能够通过边表示学习刻画支路状态的动态演变, 精准识别逼近稳定极限的脆弱节点与重载支路. 文献 [26] 提出了一种类比矩阵无关潮流算法的 GNN 电压稳定裕度估计方法, 在无需反复求解复杂交流潮流方程的前提下, 实现了系统级与节点级电压裕度的毫秒级预测. 文献 [27] 则采用监督学习训练 GNN, 在综合考虑风光出力与负荷随机波动的空间相关性基础上, 实现了对输电线路过载风险及支路潮流裕度的快速、端到端评估.

此外, 对于已经越限的节点或支路, GNN 能够辅助信息层快速生成近似最优潮流 (Optimal Power Flow, OPF) 的调度策略. 为了克服纯数据驱动方法可能违反物理定律的缺陷, 物理引导 (Physics-Informed) 成为 GNN 在该领域的关键技术. 文献 [28] 提出了一种物理引导图卷积网络用于变拓扑场景下的 OPF 计算, 通过在图卷积核中嵌入物理约束, 并利用关联学习损失函数惩罚功率不平衡, 使模型输出满足潮流方程与安全边界. 文献 [29] 进一步提出针对大规模随机电力系统的 GNN 方法, 通过对偶拉格朗日机制将电压与支路功率约束转化为无约束优化问题, 并结合在线迁移学习应对未见拓扑. 该方法不仅证明了模型的理论稳定性, 还能在突发拓扑变化下快速生成优于传统优化器的调度解, 从而高效实现电压与潮流的越限矫正.

4.1.3 GNN 在系统脆弱性风险问题中的应用

在系统脆弱性风险问题中, 局部故障跨区蔓延引发的级联崩溃是配电系统面临的最严峻挑战. 由于节点越限与支路故障存在极强的时空耦合, GNN 可通过多层信息汇聚、注意力权重分配与子图提取技术, 直接逼近高维联合风险概率分布, 从而精准识别具有风险集聚特征的薄弱连通区域.

文献 [30] 采用了图卷积网络 (Graph Convolutional Network, GCN) 辅助的级联故障搜索方法, 将电力系统拓扑、节点状态和支路运行信息表示为图结构, 通过离线训练 GCN 学习级联故障在电网拓扑中的传播规律, 并在在线阶段利用训练后的模型快速筛选可能引发严重后果的关键故障场景; 文献 [31] 使用了 GCN 方法实现了薄弱物理子图的检测. 该方法将电力系统建模为由节点和支路组成的图结构, 通过离线训练 GCN 学习级联故障在电网拓扑中的传播机理, 并在在线搜索阶段利用训练好的 GCN 模型快速识别可能引发严重级联故障的关键节点、关键线路及其局部关联区域.

4.1.4 GNN 在物理层风险管控中的应用讨论

总体来看, 物理层风险直接作用于配电系统的设备状态、潮流分布和网络连通性, 是最接近实际运行安全边界的一类风险. 设备故障或损坏会改变供电路径并引发局部停电, 设备健康退化会使故障概率随运行时间逐渐升高, 负荷高频波动和源荷不匹配会导致电压或潮流越限, 而局部故障与拓扑脆弱性耦合则可能诱发风险扩散和级联故障. 由于配电网天然具有节点—支路图结构, GNN 能够融合拓扑连接、设备状态和电气量测信息, 为故障识别、状态预测、越限评估和脆弱区域检测提供支撑.

具体而言, 在设备故障或损坏场景下, GCN、GAT 和图生成网络 (Graph Generative Networks, GGNs) 可学习故障前后拓扑连通性和节点状态的变化, 用于故障定位场景, 但在未见故障组合、大规模拓扑重构或多故障并发场景下泛化能力仍然不足, 且输出结果还需满足电气可行性约束. 在设备健康退化场景下, 图循环网络 (Graph Recurrent Networks, GRNs) 和图自编码器 (Graph Auto-Encoder, GAE) 可结合设备邻接关系和历史状态序列刻画退化趋势, 支撑健康评估和异常退化识别, 但其效果依赖长期高质量样本, 早期故障和极端退化样本不足会影响预测稳定性. 在负荷高频波动和源荷不匹配场景下, GCN、GAT 与 GRN 能够利用拓扑关系刻画节点间电气耦合, 实现电压预测、潮流近似和越限风险评估, 但多数方法仍属于数据驱动近似, 难以满足潮流

方程和安全约束. 在局部故障与拓扑脆弱性耦合场景下, GCN 和 GAT 可通过多层信息汇聚、注意力权重和子图学习识别关键节点、脆弱支路、薄弱子图和高风险传播路径, 但其结果受训练样本、扰动场景和模型结构影响较大, 对复杂扰动叠加下的因果解释能力仍然不足.

因此, GNN 在物理层风险管控中的优势主要体现在拓扑感知故障识别、时序状态退化建模、源荷波动下的越限评估以及系统脆弱性分析方面; 其应用瓶颈则集中表现为跨拓扑和未见故障场景下的泛化能力不足、物理约束嵌入不充分、真实故障样本稀缺以及复杂扰动条件下的解释可信度有限.

4.2 GNN 在数字层风险管控中的应用

针对数字层中量测稀疏导致的空间可观测性不足、频繁重构引发的拓扑先验未知, 以及 FDI 蓄意破坏造成的状态感知失真等问题, GNN 凭借其卓越的跨节点特征聚合、全局空间关联挖掘与图结构鲁棒学习能力, 进一步协助数字层风险管控的进行. 通过在稀疏量测状态估计、动态拓扑辨识以及隐蔽型坏数据检测等场景中的深度应用, GNN 能够有效突破传统解析方法的观测瓶颈, 实现恶劣数字环境下的系统真实状态精准重构与感知风险的主动防御. 图 4 展示了 GNN 在数字层风险管控中的应用场景.

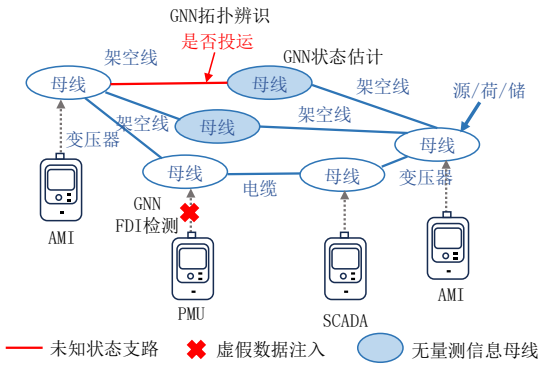

图 4 GNN 在数字层风险管控中的应用

4.2.1 GNN 在量测稀疏风险问题中的应用

在量测稀疏风险问题中, 有限的实时量测设备 (空间稀疏) 与多源异构设备 (如秒级 SCADA 与毫秒级μPMU) 采样率的极度不匹配 (时间稀疏), 导致传统状态估计面临严重的时空可观测性缺失. GNN 能够打破传统 WLS 对量测冗余度与时间同步性的绝对依赖. 针对这一复杂场景, 数字层状态估计在学术上被严格划分为静态状态估计 (Static State Estimation, SSE) 与动态状态估计 (Dynamic State Estimation, DSE). GNN 通过图结构中节点间的物理耦合与多跳消息传递机制, 不仅能在空间维度将高维稀疏特征映射为完整的系统状态, 还能结合时序模型在时间维度对齐异构采样率数据, 从而在极低量测覆盖率与严重时间异步的恶劣环境下实现全网状态的精准推演.

在 SSE 应用方面, GNN 主要致力于解决空间维度的量测极度稀疏问题, 旨在利用单一时间断面的残缺数据重构系统的稳态运行点. 在具体的数字层感知中, GNN 能够深度融合多源异构量测数据与底层通信网络状态 (如时延、丢包率、带宽占用与路由路径), 对信息-物理双重节点的运行状态进行联合感知. 针对 PMU 覆盖率严重受限与实时数据丢失问题, 文献 [32] 提出了一种基于深度几何学习的定制化图神经网络 (CGNN-SE) 方法. 该模型巧妙地在端到端框架内融合了图卷积与多头图注意力机制, 不仅有效克服了非高斯量测噪声与坏数据的干扰, 还从理论层面严格推导了状态估计误差随拓扑变化的上限. 这种方法在 PMU 故障与量测极度稀疏的恶劣环境下, 依然展现出了远超传统优化算法的稳态重构精度. 面对频繁的拓扑重构, 文献 [33] 设计了一种适应高频拓扑切换的完整配电系统状态估计 (Distribution System State Estimation, DSSE) 框架, 利用格拉姆角场 (Gramian Angular Field) 对量测数据进行预处理, 并通过图注意力网络将状态估计转化为图上的节点级回归预测问题, 在拓扑高频变动下展现出极强的鲁棒性.

在 DSE 应用方面, GNN 则重点攻克由采样率异构与源荷剧烈波动带来的时空双重稀疏挑战, 旨在追踪系统状态的连续动态演化轨迹. 与 SSE 的快照式回归不同, DSE 需要处理包含时间相关性的动态演化过程. 针对传统 GNN 仅能依赖相邻节点进行特征聚合的局部空间局限性, 文献 [34] 提出了一种物理感知的 DSSE 框架, 创新性地将结构感知循环神经网络 (Structure-aware RNN) 与带有卷积自回归滑动平均层的 GNN 深度融合. 该模型利用 RNN 与自回归机制, 精准捕捉了系统状态在时间维度上的历史依赖与动态演化特征, 不仅突破了空间局部感受野的限制, 还在未知的复杂网络拓扑与极端量测环境下, 展现出了卓越的动态时序追踪精度与跨场景泛化能力. 进一步地, 面对动态演化过程中物理拓扑不确定 (如噪声干扰、恶意攻击或拓扑缺失) 对追踪精度的致命影响, 文献 [35] 针对时序图卷积网络进行了架构创新, 通过量测数据自适应生成知识图谱 (Knowledge Graph) 来辅助甚至替代不可靠的物理图结构. 这种双图融合架构有效增强了模型在拓

扑不确定环境下的动态状态感知韧性, 为复杂配电系统的连续时序追踪提供了双重保障.

4.2.2 GNN 在拓扑未知风险问题中的应用

在拓扑未知风险问题中, 物理拓扑的频繁重构导致数字层先验信息失效, 进而引发量测映射矩阵的根本性错误. 根据先验信息的缺失程度, 该问题在学术上可严格区分为拓扑检测 (Topology Detection) 与拓扑辨识 (Topology Identification): 前者指在线路物理参数已知的前提下, 追踪网络中联络开关与断路器的实时开合状态; 后者则应对更极端的场景, 即线路参数与基础连接关系均处于未知状态. 面对这两种差异化挑战, GNN 能够将拓扑检测转化为高维空间中的边分类任务, 将拓扑辨识转化为图结构学习或边关系推断任务. 通过深度挖掘节点功率注入与支路潮流之间的隐式物理约束, GNN 能够在先验信息残缺或完全缺失的恶劣条件下, 自适应地重构系统的真实连接关系.

在拓扑检测应用方面, GNN 擅长捕捉开关动作引发的局部电气特征突变. 通过将通信节点、测量终端及边缘计算单元建模为图结构, GNN 能够利用节点表示学习精准刻画数字层拓扑连接的动态演化. 文献 [36] 提出了一种基于双图结构 GNN(DGS-GNN) 的近实时拓扑检测方法. 该方法巧妙地将开关状态追踪转化为多图数据集上的归纳式边推断任务, 在推理阶段无需输入任何结构信息, 仅依赖微型同步相量测量装置 (μPMU) 的节点属性特征即可恢复实际拓扑图, 在 DER 扰动与噪声环境下展现出极强的泛化能力. 此外, 文献 [37] 融合了长短期记忆网络 (Long Short Term Memory, LSTM) 与 GCN, 深度挖掘低压配电系统中源荷波动的时空动态依赖, 有效克服了正常功率波动与拓扑切换特征的混淆, 实现了对高频动态拓扑的精准检测与追踪.

在拓扑辨识应用方面, GNN 致力于在"零先验"或"弱先验"环境下, 从纯数据驱动的视角重构全局网络. 文献 [38] 提出了一种基于潮流图卷积网络 (PFGCN) 的联合估计方法. 该方法摆脱了对昂贵电压相角量测的绝对依赖, 通过节点相关性矩阵生成候选拓扑, 并将交流潮流方程的拓扑依赖性深度嵌入图卷积算子中. 通过伪潮流计算与神经网络训练的交替迭代, 该模型创新性地利用训练收敛性与损失函数值作为反馈信号来精准筛选验证真实拓扑, 实现了网络骨架与线路参数的高精度联合辨识. 此外, 面对量测数据缺失对辨识精度的致命影响, 文献 [39] 创新性地利用生成对抗网络补全严重缺失的量测特征, 在极度残缺的量测场景下, 显著提升了 GNN 拓扑辨识的可靠性与鲁棒图结构重构能力.

4.2.3 GNN 在虚假数据注入风险问题中的应用

在 FDI 风险问题中, 高阶攻击者通过构造符合物理定律的隐蔽攻击向量, 能够轻易绕过传统基于残差的坏数据检测机制. GNN 能够超越单一节点的数值特征检验, 通过学习全局网络中多源量测间的物理耦合不变量与时空演化规律, 在图谱域或空间域精准捕捉被篡改数据引发的结构性异常, 从而剥离出极具欺骗性的恶意注入.

在隐蔽 FDI 检测方面, GNN 能够充分利用电力系统量测间的拓扑相关性、状态估计残差的结构分布特征, 以及数字通信路径中的数据传输依赖, 精准识别具有"物理一致性"伪装特征的虚假数据. 文献 [40] 提出了一种基于谱图神经网络 (Spectral GNN) 的异常检测框架, 利用 Bernstein 多项式逼近谱图滤波器, 在图谱域高效提取空间结构关联与多频段异常特征, 实现了对微弱且高度隐蔽攻击的敏锐识别. 文献 [41] 则将霍奇图神经网络 (HodgeGNN) 与图注意力机制深度结合, 通过重构图模型将节点功率注入与分支潮流统一映射, 并利用霍奇拉普拉斯算子 (Hodge Laplacian) 的拓扑特性, 不仅实现了污染数据的精准隔离, 还完成了对攻击路径的溯源定位.

4.2.4 GNN 在数字层风险管控中的应用讨论

总体而言, 数字层风险主要源于状态感知、拓扑认知和数据可信性的不确定性. 量测覆盖不足会削弱系统可观测性, 开关频繁动作会造成数字模型与实际拓扑不一致, 而虚假数据注入攻击 (False Data Injection, FDI) 则可能使状态估计和控制决策偏离真实运行状态. 由于配电网的量测数据、拓扑连接和运行状态之间具有天然的图关联特征, GNN 能够为缺失量测恢复、动态拓扑感知和异常数据检测提供有效支撑.

具体而言, 在量测设备不足场景下, 图自编码器 (Graph Auto-Encoder, GAE) 和 GCN 可利用拓扑邻域信息补全缺失量测, 并生成伪量测以辅助状态重构, 从而降低对高冗余量测配置的依赖, 但其效果容易受到量测噪声、缺失模式变化和运行分布偏移的影响. 在开关频繁动作场景下, 图生成网络 (Graph Generative Networks, GGNs) 与图循环网络 (Graph Recurrent Networks, GRNs) 能够结合历史拓扑状态和实时量测信息刻画图结构演化过程, 支撑动态拓扑推断、拓扑辨识和状态追踪, 但面对未见拓扑、跨区域系统或大规模运行方式变化时, 仍通常需要重新训练或微调. 在 FDI 攻击场景下, GAE 和 GAT 可通过拓扑邻域一致性、结构相关性和重构误差识别

隐蔽异常, 提高攻击检测灵敏度, 但在自适应攻击、对抗样本和攻击样本稀缺条件下, 其误报率、漏检风险和鲁棒性仍面临挑战.

因此, GNN 在数字层风险管控中的优势主要体现在缺失量测补全、动态拓扑感知和隐蔽异常检测方面, 而其局限则集中表现为噪声与分布偏移下的重构可靠性不足、跨拓扑或跨系统迁移能力有限, 以及复杂攻击条件下的检测鲁棒性不足.

4.3 GNN 在信息层风险管控中的应用

面向信息层中因通信拥塞与链路断路引发的严重传输时延、信道衰落导致的数据丢包与控制决策失效, 以及恶意 DoS/DDoS 攻击诱发的指令滞后与数据阻断等严峻挑战, GNN 凭借其卓越的通信拓扑动态映射、跨节点交互挖掘与时空数据补全能力, 为信息层风险管控提供了全新的数据驱动范式. 通过在动态路由规划、缺失数据智能插补、异常流量辨识以及紧急控制决策等场景中的应用, GNN 能够实现对通信瓶颈的韧性抵御与网络威胁的主动阻断. 图 5 展示了 GNN 在信息层风险管控中的应用场景.

图 5 GNN 在信息层风险管控中的应用

4.3.1 GNN 在常规通信拥塞和断路风险问题中的应用

在常规通信拥塞和断路风险问题中, 海量并发业务与有限带宽资源之间的固有矛盾极易诱发局部流量过载, 而极端环境或设备故障则会导致通信链路物理中断. 这些问题使得传统基于静态规则的最短路径路由算法难以应对高维、高动态的网络状态变化. GNN 能够将信息层的通信节点与传输链路建模为动态图结构, 通过图卷积机制深度挖掘网络拓扑的隐式耦合特征与全局流量分布规律. 结合深度强化学习 (Deep Reinforcement Learning, DRL), GNN 能够实现从被动响应向主动预测的跨越, 在复杂的动态网络环境中完成快速弹性路由重构与拥塞规避.

在通信拥塞的拥塞感知与主动路由方面, 文献 [42] 指出, 面向智能电网的通信调度必须突破单一指标的局限, 综合权衡业务重要度、链路可靠性与实时流量状态. 为此, 文献 [43] 提出了一种基于 GNN 的拓扑感知预测模型. 该方法创新性地引入了稀疏转密集的预处理机制, 并利用 GNN 深度捕获信息层路由器间的空间交互特征, 成功克服了传统时序模型 (如 LSTM) 在稀疏流量下的预测失效问题, 实现了对全网拥塞态势的高精度感知. 在精准感知的基础上, 为实现高效的主动路由规划, 文献 [44] 提出了一种信任感知的深度强化学习与 GNN 融合框架 (TA-DRL-GNN). 该模型将设备的转发行为、链路质量与能量状态编码为图特征, 利用 GNN 捕获多跳依赖关系以规避不可靠节点, 并结合深度 Q 网络综合评估吞吐量与连接可靠性. 这种机制能够在动态网络环境中实时规划出低延迟、高能效的最优下一跳路由, 从底层传输机制上有效缓解了网络拥塞并提升了资源利用率.

在通信断路的拓扑突变与弹性重构方面, 文献 [45] 论证了 GNN 与深度强化学习融合的端到端网络架构的巨大潜力, 强调了 GNN 在提取节点与链路隐式耦合特征、支撑长期路由决策中的核心价值. 面对节点失效与链路断开引发的高维拓扑突变, 文献 [46] 提出了一种极具代表性的双模式软件定义路由策略. 在正常工况下, 启动主动路由模块 (PRM), 利用 GNN 与 Q-Learning 算法动态调整队列服务速率, 优先为事件驱动 (ED) 数据包规划低延迟路径以规避拥塞; 而在检测到严重拥塞或链路失效等断路工况时, 系统由 GNN 触发切换至弹性路由模块 (RRM), 结合 DQN 快速重构高冗余度的最优路径. 这种基于 GNN 的双模式架构不仅有效化解了突发流量引发的通信瓶颈, 更在底层拓扑突变时展现出了卓越的自愈能力. 进一步针对部分可观测条件下的拓扑恢复难题, 文献 [47] 提出了一种基于 GNN 的自适应拓扑重构与智能调度框架. 该框架采用两阶段架构: 首先利用基于图的编码器-解码器精准推断潜在的通信链路; 随后通过强化学习增强的 GNN 模块, 在重构的图结构上动态生成最优调度策略. 该方法显著提升了链路恢复的准确性, 为大规模电力通信网的断路自愈提供了强大的数据驱动支撑.

4.3.2 GNN 在常规信息丢包风险问题中的应用

在常规信息丢包风险问题中, 信道衰落、电磁干扰或路由器缓存溢出导致量测数据与控制指令在传输过程中不可避免地发生丢失. 这种时空不连续的数据缺失会直接破坏数字层的可观测性, 进而导致物理层的控制决策失效. 传统的数据插补方法 (如线性插值、矩阵分解) 往往忽略了电力系统底层的物理拓扑约束与动态演化规律. GNN 能够将丢包问题转化为图信号处理中的时空数据补全任务, 利用未丢

失节点的空间相关性与历史时间序列的时间依赖性, 对缺失数据进行高保真的重构.

在应对随机丢包与连续数据缺失方面, GNN 表现出了显著的跨时空特征提取与局部拓扑泛化能力. 传统深度学习插补方法往往缺乏对传感器网络中非线性时空依赖与关系归纳偏置的显式建模. 为此, 文献 [48] 首次将 GNN 引入多元时间序列插补领域, 提出了一种基于消息传递的时空图神经网络架构. 该模型通过在不同空间位置的传感器节点间传递时空表征, 充分挖掘了网络中隐藏的强关系信息, 为大规模互联传感器网络的数据高保真重构奠定了坚实的理论基础. 在此理论框架的启发下, 针对广域量测系统中极高缺失率与不完全可观测的严峻工程挑战, 文献 [49] 提出了一种基于辅助任务学习与 K-hop GNN 的缺失数据重构框架. 该方法创新性地利用 K 跳图神经网络直接在包含 PMU 节点的局部子图上进行特征学习, 打破了全局可观测性的限制; 同时, 通过主任务 (时空 GNN 提取依赖关系) 与辅助任务 (利用 PMU 数据低秩特性的无监督在线学习) 的协同优化, 赋予了模型在电力系统概念漂移与高丢包率下的强鲁棒性与自适应能力. 这种数据驱动的智能插补机制, 有效切断了"信息层丢包-数字层失真-物理层失控"的跨层风险传播链条.

4.3.3 GNN 在 DoS/DDoS 攻击风险问题中的应用

在 DoS/DDoS 攻击风险问题中, 恶意攻击者通过发起 DoS/DDoS 攻击蓄意制造海量垃圾流量, 导致通信信道严重拥塞、控制指令极度滞后甚至完全阻断. 这种非预想的信息层风险极易被放大并跨层蔓延, 最终引发物理层的级联崩溃. 面对 DoS/DDoS 攻击带来的高维状态空间爆炸与求解实时性约束, GNN 能够突破传统集中式优化算法的计算瓶颈, 通过物理信息引导的图结构学习与端到端决策机制, 实现极端 DoS/DDoS 攻击态势下的快速异常辨识、紧急控制与主动防御.

在应对攻击引发的控制迟滞与紧急控制方面, 文献 [50] 提出了一种基于 GraphSAGE-D3QN 的端到端紧急控制框架. 该模型利用 GraphSAGE 自适应提取频繁拓扑变化下的空间耦合特征, 并结合 D3QN 构建了从故障状态到控制动作的直接映射. 在遭受 DoS/DDoS 攻击导致通信严重迟滞的恶劣工况下, 该方法能够在毫秒级输出欠压切负荷指令, 有效克服了传统集中式优化在高维状态空间下求解缓慢的固有瓶颈, 为非预想故障下的控制策略快速生成提供了坚实保障.

在攻击态势下的紧急防御与跨层级联阻断方面, 文献 [51] 提出了一种融合生成对抗网络、GNN 和分布鲁棒优化的紧急防御与恢复框架. 该框架利用 GAN 合成极端攻击引发的故障演化场景, 由 GNN 精准预测级联故障的跨层传播路径, 再结合分布鲁棒优化输出不确定性环境下的自适应隔离策略. 该方法能够在多重攻击和未知扰动条件下, 有效阻断跨网络级联传播链条, 从根本上化解了非预想信息层风险中"错误控制放大物理风险"的难题. 此外, 文献 [52] 的系统性综述进一步总结指出, 融合时空建模和物理信息引导的 GNN 决策机制, 能够突破传统物理模型在复杂故障态势下的实时性约束, 为 DoS/DDoS 攻击下的快速拓扑重构、主动解列与系统恢复提供了不可或缺的理论支撑.

4.3.4 GNN 在信息层风险管控中的应用讨论

综合来看, 信息层风险主要源于通信链路状态和数据传输过程的不确定性, 典型表现为通信拥塞导致的控制时延, 信息丢包造成的状态感知不连续, 以及 DoS/DDoS 攻击引发的异常通信流传播和控制失效. 由于通信网络具有拓扑时变、数据流连续传输和攻击路径隐蔽扩散等特征, GNN 可通过图结构建模、时序依赖学习和异常传播识别, 为信息层风险感知与防御提供有效工具.

具体而言, 在通信拥塞场景下, GRN 能够结合通信拓扑和历史链路状态刻画时延传播过程, 辅助识别潜在拥塞链路和关键通信节点, 但其实时推理对边缘侧算力、通信带宽和响应时限要求较高. 在信息丢包场景下, GAE、GRN 和 GCN 可利用相邻节点之间的关联关系及历史时序信息恢复缺失数据, 提高状态感知的连续性, 但当丢包呈现连续性、集中性或非随机特征时, 补全结果的可靠性仍难以保证, 并可能进一步影响后续控制决策. 在 DoS/DDoS 攻击场景下, GAE、GAT 与 GGN 可通过邻域一致性、注意力权重和异常结构生成等方式识别攻击源及其传播路径, 为主动防御和弹性路由提供支撑, 但面对复合攻击、拓扑投毒和跨层级联攻击时, 其鲁棒性、可解释性和实时部署能力仍有待提升.

因此, GNN 在信息层风险管控中的优势主要体现在通信时延传播建模、缺失数据恢复和异常攻击路径识别方面, 而其应用瓶颈则集中表现为边缘侧实时推理压力、非随机丢包下的数据重构可靠性不足, 以及复杂攻击场景下的安全鲁棒性有限. 为进一步揭示不同风险场景下 GNN 方法的适用性边界, 表 3 从系统层级、风险诱因、工程现象、统计特征、图学习任务、适配 GNN 类型、优势及不足等维度, 对新型配电系统多维风险特征与 GNN 建模方法之

表 3　新型配电系统多维风险特征与 GNN 适配性及局限性分析

系统层级	风险诱因	工程现象	统计特征	图学习任务	GNN类型	优势	不足
物理层	设备故障或损坏	区域停电、供电路径中断	拓扑断裂、连通性突变	故障定位、故障区段识别	GCN、GAT、GGN	能刻画故障引起的拓扑连通性变化, 适合识别故障区段和关键断点	对未见故障组合和大规模拓扑重构泛化不足, 且输出结果可能缺少电气可行性约束
	设备健康退化	设备老化、绝缘劣化、故障概率升高	状态缓慢漂移、退化趋势累积	设备健康评估、退化趋势预测	GRN、GAE	可融合设备邻接关系与时序退化特征, 适合挖掘局部退化向区域风险扩散的规律	依赖长期高质量历史样本, 极端退化和早期故障样本不足会影响预测鲁棒性
	负荷高频波动/源荷不匹配	电压越限、潮流越限	强时空相关、节点状态联动	电压/潮流预测、安全裕度评估、最优潮流辅助	GCN、GAT、GRN	能利用配电网拓扑捕捉节点间电气耦合, 提高电压和潮流预测效率	多为数据驱动近似, 难以满足潮流方程和安全约束, 跨运行场景泛化仍需验证
	局部故障与拓扑脆弱性耦合	级联故障、风险扩散、局部扰动放大	关键节点/边主导传播、长尾风险突出	薄弱环节辨识、风险传播路径挖掘	GAT	注意力和子图学习机制有助于识别关键设备、脆弱支路和高风险传播路径	可解释结果易受训练样本和模型结构影响, 对复杂扰动叠加下的因果解释能力不足
数字层	量测设备不足	可观测性下降、状态估计误差增大	图信号缺失、采样稀疏	状态估计、图信号补全	GAE、GCN	可利用拓扑邻域信息补全缺失量测, 降低对高冗余量测配置的依赖	对量测噪声和缺失模式敏感, 训练样本与实际量测分布不一致时性能易退化
	开关频繁动作/拓扑记录不同步	拓扑未知、运行方式变化	图结构动态变化、边连接不确定	拓扑检测、拓扑辨识、开关状态识别	GGN、GRN	能刻画拓扑随时间变化的动态特征, 适合支撑配电网拓扑辨识和状态追踪	对未见拓扑和跨系统迁移能力有限, 通常需要针对新系统重新训练或微调
	FDI攻击	状态感知偏差	隐蔽异常、局部扰动、特征分布偏移	图异常检测、FDI检测	GAE、GAT	可通过邻域一致性和结构相关性识别隐蔽异常, 提高攻击检测灵敏度	对自适应攻击和对抗样本鲁棒性不足, 误报率受数据不平衡和攻击样本稀缺影响较大
信息层	通信拥塞和断路	时延增加、控制指令滞后	时延累积、链路状态时变	拥塞识别、时延预测、弹性路由辅助	GRN	能建模通信链路之间的时空依赖, 适合识别拥塞传播路径和关键通信节点	实时推理对算力和通信带宽要求较高, 边缘部署和低时延响应仍面临挑战
	信息丢包	数据不连续、决策信息缺失	图信号缺失、时序间断、随机丢失	缺失数据重构、图信号补全	GAE、GRN、GCN	能结合邻域节点和历史时序信息恢复缺失数据, 提高状态感知连续性	对连续丢包和非随机缺失场景适应性不足, 补全结果可能放大后续控制误差
	DoS/DDoS攻击	拒绝服务、错误路由、控制失效	异常通信流、攻击路径传播、对抗扰动	攻击检测、攻击源定位、攻击路径识别	GAE、GAT、GGN	可结合拓扑结构和通信状态识别攻击传播路径, 并支撑主动防御和弹性路由	对复合攻击、拓扑投毒和跨层级联攻击的鲁棒性不足, 工程部署需兼顾实时性和安全性

间的关系进行了系统归纳. 该表不仅刻画了各类风险在图结构、图信号和时序动态上的表现形式, 也进一步比较了不同 GNN 架构在特定任务中的建模优势与局限性, 尤其突出其在跨拓扑泛化、物理一致性、真实数据依赖、鲁棒安全和实时部署方面仍面临的关键瓶颈.

5　面临挑战与未来展望

尽管 GNN 在新型配电系统物理、数字与信息层的风险管控中展现出了卓越的性能, 但现有方法在物理一致性、跨系统泛化、真实数据依赖、鲁棒安全和实时部署等方面仍面临瓶颈. 面对新型配电系统日益复杂的跨层耦合动态与极高的安全可靠性要求, 未来的研究亟需在以下几个关键方向寻求突破.

5.1　物理机制与数据驱动的深度融合

当前多数应用于配电系统的 GNN 模型仍以数据驱动为主, 在小样本、未见拓扑和极端运行场景下容易出现物理不可行输出. 为缓解这一问题, 现有研究通常采用物理引导图神经网络 (Physics-Informed GNN, PI-GNN), 通过在损失函数中加入潮流残差、功率平衡误差或安全约束惩罚项, 引导模型学习符合物理规律的映射关系. 然而, PI-GNN 本质上多属于软约束方法, 其约束满足程度受惩罚权重、训练样本分布和优化收敛质量影响, 难以保证模型在推理阶段满足基尔霍夫定律、潮流方程和运行安全边界.

因此, 未来研究需要进一步从 PI-GNN 向物理编码图神经网络 (Physics-Encoded GNN, PEGNN) 拓展. PEGNN 的核心思想是将导纳矩阵、潮流方程、功率平衡关系和安全可行域嵌入图卷积算子、消息传递机制或输出投影层, 使网络结构本身具备物理一致性. 与依赖损失函数惩罚的 PI-GNN 相比, PEGNN 能够在训练和推理过程中更严格地满足物理规律, 从而提升小样本学习能力、输出精度、跨拓扑泛化能力和极端工况下的安全可靠性. 该方向对于状态估计、潮流计算、最优潮流和紧急控制等安全关键任务具有重要应用潜力, 但仍需解决非线性交

流潮流约束嵌入、多相不平衡配电网建模和大规模动态图计算复杂度等问题.

5.2 跨系统泛化与图神经算子驱动的可迁移建模

现有 GNN 泛化研究多集中于同一系统内部的拓扑扰动或有限场景迁移, 对跨设备类型、跨馈线结构、跨电压等级和跨区域系统的泛化能力关注不足. 由于不同配电系统在节点规模、线路参数、量测配置、分布式电源渗透率和运行控制策略等方面存在差异, 同一模型迁移至新系统后往往会出现性能退化, 通常需要依赖目标系统样本进行二次训练或参数微调. 对于持续改造和扩建的新型配电系统而言, 频繁再训练会显著增加数据采集、模型维护和工程部署成本, 难以满足在线风险管控对快速适应性的要求.

图神经算子 (Graph Neural Operator, GNO) 为突破上述瓶颈提供了新的技术路径. 不同于传统 GNN 在固定或有限维图结构上学习输入输出映射, GNO 通过在函数空间中学习系统状态、拓扑结构与风险响应之间的算子映射关系, 有望提升模型对不同节点规模、不同网架结构和不同离散化分辨率的适应能力. 未来若能将潮流方程、设备退化机理和通信动力学等物理先验嵌入 GNO 框架, 则有望构建面向跨系统、跨规模和跨任务迁移的新型配电系统风险评估模型, 为快速扩建场景下的在线风控与自适应决策提供支撑.

5.3 跨层异构图的统一建模与多模态协同

当前 GNN 在电力系统风险管控中的图建模通常采用单层建模和简单统一图建模两类. 前者通常面向物理层、数字层或信息层中的单一风险对象, 能够刻画特定层级内部的拓扑关联, 但难以描述信息层攻击、数字层感知异常与物理层控制失效之间的跨层级联关系. 后者虽将多层对象纳入同一图结构, 但若采用同质化节点、边和消息传递机制, 则容易忽略不同层级在对象属性、连接语义、动态时间尺度和约束机制上的差异. 例如, 物理层边权主要反映线路阻抗、电气距离或潮流容量, 数字层边权侧重量测依赖、数据关联或估计置信度, 信息层边权则更多体现通信带宽、时延、丢包率或攻击路径. 简单统一图表示可能弱化不同层级的风险传播机理, 影响跨层风险识别与防御决策的准确性.

未来, 跨层异构动态图建模有望成为刻画信息物理耦合风险的重要方向. 通过引入异构图神经网络, 可将母线、线路、量测装置、控制终端、通信节点和网络链路等对象表示为不同类型的节点与边, 并针对电力流、数据流和控制流设计差异化消息传递机制. 该方法能够在保留各层级差异性的同时刻画层间耦合关系, 有望支撑跨层级联故障溯源、关键脆弱环节识别和多模态协同防御, 为新型配电系统全域信息物理协同风控提供统一建模框架.

5.4 云边协同架构下的轻量化与分布式计算

随着新型配电系统规模扩张及分布式资源和物联网终端大量接入, 图结构与时序量测数据快速增长. 集中式 GNN 依赖全网数据上传和云端统一计算, 易受带宽、算力、数据同步、隐私及单点故障制约, 难以兼顾在线风控所需的快速响应、局部自治与全局协调.

未来, 基于云边协同的分布式图学习有望成为 GNN 工程化部署的重要支撑. 边缘侧可利用局部子图开展实时状态感知、风险初筛和快速控制, 云端则负责全局图表征学习、跨区域模型更新和协同决策优化. 通过联邦图学习、动态图采样、子图推理和增量更新等机制, 可在保护底层数据隐私的同时降低通信开销. 进一步结合知识蒸馏、网络剪枝、参数共享和事件触发推理等轻量化技术, 可构建兼顾精度、时延和能耗的边缘侧 GNN 模型, 推动新型配电系统风险管控从集中式离线分析向分层自治和实时闭环控制转变.

6 结 论

随着新型配电系统向柔性化、数字化与智能化深度演进, 传统的单层级、解析驱动的风险管控模式已难以应对跨空间耦合的复杂安全挑战. 本文构建了"物理-数字-信息"三层异构动态图风险管控架构, 系统分析了设备健康退化、量测稀疏、FDI 攻击与 DoS/DDoS 攻击等多源扰动在能量流、数据流与信息流中的级联演化机理. 针对上述多维耦合风险, 本文梳理了 GNN 在新型配电系统风险管控中的前沿应用, 并系统提炼了系统多维风险特征、具体图学习任务与各类 GNN 架构的适配映射关系. 具体而言, GNN 在各层级的核心优势体现在:

1) 在物理层, GNN 凭借其强大的非欧拓扑建模能力, 有效克服了传统概率潮流与联合风险评估的"维度灾难", 实现了对设备健康状态、运行越限风险与薄弱子图的高效预警.

2) 在数字层, GNN 通过跨节点特征聚合与物理不变量挖掘, 打破了对量测冗余度与拓扑先验的绝对依赖, 在极度稀疏量测、拓扑未知与隐蔽 FDI 攻击的恶劣环境下, 实现了系统真实状态的鲁棒重构.

3) 在信息层, GNN 结合时空序列建模与深度强

化学习, 将传统的被动响应转化为主动防御, 为应对极端通信拥塞、随机丢包与 DoS 攻击提供了毫秒级的弹性路由规划与紧急控制支撑.

总体来看, GNN 凭借与配电系统拓扑结构天然契合的消息传递机制, 已成为支撑高维非线性建模和跨层级联风险分析的重要技术工具. 面向工程化应用, 未来研究应重点突破物理编码约束、跨系统泛化、跨层异构融合和云边协同部署等关键问题, 推动基于 GNN 的风险管控从离线评估走向在线态势感知、主动防御和闭环控制, 为构建安全、弹性、智能的新型配电系统提供理论支撑与技术路径.

参考文献 (References)

[1] 国家发展改革委, 国家能源局. 关于促进电网高质量发展的指导意见: 发改能源 (2025) 1710 号[EB/OL]. (2025-12-31)[2026-04-17]. https://www.ndrc.gov.cn/xxgk/zcfb/tz/202512/t20251231_1402949.html.

[2] 翁世清, 翁品迪, 周京, 等. FDI 攻击下互联电力系统的分布式安全状态估计[J]. 控制与决策, 2023, 38(7): 1935-1941.
(Weng S Q, Weng P D, Zhou J, et al. Distributed secure state estimation for interconnected power systems under FDI attacks[J]. Control and Decision, 2023, 38(7): 1935-1941.)

[3] 邓超, 唐旗, 郭方洪, 等. FDI 攻击下有源配电网储能系统安全控制[J]. 控制与决策, 2023, 38(8): 2346-2354.
(Deng C, Tang Q, Guo F H, et al. Security control for energy storage systems in active distribution network under FDI attacks[J]. Control and Decision, 2023, 38(8): 2346-2354.)

[4] Li Y Z, Xue C, Zargari F, et al. From graph theory to graph neural networks (GNNs): The opportunities of GNNs in power electronics[J]. IEEE Access, 2023, 11: 145067-145084.

[5] 杨挺, 刘亚闯, 刘宇哲, 等. 信息物理系统技术现状分析与趋势综述[J]. 电子与信息学报, 2021, 43(12): 3393-3406.
(Yang T, Liu Y C, Liu Y Z, et al. Review on cyber-physical system: TechnologyAnalysis and trends[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3393-3406.)

[6] Kim M, Ghobadi F, Tayerani Charmchi A S, et al. Digital twins for clean energy systems: A state-of-the-art review of applications, integrated technologies, and key challenges[J]. Sustainability, 2026, 18(1): 43.

[7] 薛禹胜. 时空协调的大停电防御框架 (一) 从孤立防线到综合防御[J]. 电力系统自动化, 2006, 30(1): 8-16.
(Xue Y S. Space-time cooperative framework for defending blackouts part I from isolated defense lines to coordinated defending[J]. Automation of Electric Power Systems, 2006, 30(1): 8-16.)

[8] 中国标准化研究院. 资产管理综述、原则和术语: GB/T 33172-2016[S]. 中国标准出版社, 2016.

[9] Raghuveer R M, Bhalja B R, Agarwal P. Real-time energy management system for an active distribution network with multiple EV charging stations considering transformer's aging and reactive power dispatch[J]. IEEE Transactions on Industry Applications, 2025, 61(5): 7723-7735.

[10] De Caro F, Collin A J, Giannuzzi G M, et al. Review of data-driven techniques for on-line static and dynamic security assessment of modern power systems[J]. IEEE Access, 2023, 11: 130644-130673.

[11] Zhao H, Maltba T E, Maldonado D A, et al. Data-driven estimation of failure probabilities in correlated structure-preserving stochastic power system models[PP/OL]. 2024, arXiv: 2401.02555.

[12] Primadianto A, Lu C N. A review on distribution system state estimation[J]. IEEE Transactions on Power Systems, 2017, 32(5): 3875-3883.

[13] Ćetenović D, Zhao J B, Levi V, et al. Variational Bayesian unscented Kalman filter for active distribution system state estimation[J]. IEEE Transactions on Power Systems, 2025, 40(1): 476-491.

[14] Xygkis T C, Löfberg J, Korres G N. Investigation of optimal phasor measurement selection for distribution system state estimation under various uncertainties[J]. IEEE Transactions on Instrumentation and Measurement, 2025, 74: 9006616.

[15] Zhang T T, Zhang W, Zhao Q, et al. Forecasting-aided joint topology/state estimation for distribution systems via Bayesian non-parametric modeling[J]. IEEE Transactions on Smart Grid, 2024, 15(1): 1014-1029.

[16] Wei S, Xu J, Wu Z, et al. A false data injection attack detection strategy for unbalanced distribution networks state estimation[J]. IEEE Transactions on Smart Grid, 2023, 14(5): 3992-4006.

[17] 杨飞生, 汪璟, 潘泉, 等. 网络攻击下信息物理融合电力系统的弹性事件触发控制[J]. 自动化学报, 2019, 45(1): 110-119.
(Yang F S, Wang J, Pan Q, et al. Resilient event-triggered control of grid cyber-physical systems against cyber attack[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.)

[18] Chaves L S, Callegari J M S, Araujo L S, et al. Impact of latency and packet error on communication in centralized microgrid control: Modeling and guidelines[J]. IEEE Access, 2025, 13: 82732-82746.

[19] Zhang S Y, Li J, Mei Z, et al. Consistent power system time series imputation via denoising diffusion probabilistic models[J]. IEEE Transactions on Smart Grid, 2026: 1.

[20] Babayomi O, Madonski R, Zhang Z B, et al. Robust model predictive control of converter-based microgrids[J]. IEEE Transactions on Power Electronics, 2025, 40(11): 17124-17146.

[21] Zeng P, Chu G. Residual-aware health prediction of power transformers via spatiotemporal graph neural networks[J]. Plos One, 2025, 20(11): 1-19.

[22] Wu Y L, Dai H N, Tang H N. Graph neural networks for anomaly detection in industrial Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(12): 9214-9231.

[23] Lin Z P, Hu W H, Cao D, et al. Topology-robust distributed grid outage detection via weighted graph causal neural network[J]. CSEE Journal of Power and Energy Systems, DOI: 10.17775/CSEEJPES.2025.02810.

[24] Hu X G, Ma J L, Zhang R, et al. Ts-GSAN: A two-stage graphical spatiotemporal attention network fault localization method for distributed energy systems[J]. IEEE Transactions on Instrumentation and Measurement, 2025, 74: 3516408.

[25] Guddanti K P, Weng Y, Marot A, et al. Graph neural networks for voltage stability margins with topology flexibilities[J]. IEEE Open Access Journal of Power and Energy, 2023, 10: 73-85.

[26] Zhang Y, Karve P M, Mahadevan S. Graph neural networks for power grid operational risk assessment under evolving grid topology[PP/OL]. 2024, arXiv: 2405.07343.

[27] Gao M S, Yu J, Yang Z F, et al. A physics-guided graph convolution neural network for optimal power flow[J]. IEEE Transactions on Power Systems, 2024, 39(1): 380-390.

[28] Yang M, Qiu G, Liu J Y, et al. Topology-transferable physics-guided graph neural network for real-time optimal power flow[J]. IEEE Transactions on Industrial Informatics, 2024, 20(9): 10857-10872.

[29] Liu Y X, Zhang N, Wu D, et al. Searching for critical power system cascading failures with graph convolutional network[J]. IEEE Transactions on Control of Network Systems, 2021, 8(3): 1304-1313.

[30] Zhu Y H, Zhou Y Z, Wei W, et al. Cascading failure analysis based on a physics-informed graph neural network[J]. IEEE Transactions on Power Systems, 2023, 38(4): 3632-3641.

[31] Moshtagh S, Azimian B, Golgol M, et al. Topology-aware graph neural network-based state estimation for PMU-unobservable power systems[J]. IEEE Transactions on Power Systems, 2025, 40(6): 4547-4560.

[32] Ren Z X, Chu X D, Ye H. State estimation for reconfigurable distribution systems using graph attention network[J]. IEEE Access, 2023, 11: 107237-107250.

[33] Kim J H, Kang J, Baek K, et al. Physics-aware recurrent and graphical learning for robust distribution system state estimation across unseen networks[J]. IEEE Transactions on Smart Grid, 2026, 17(5): 4334-4346.

[34] Haghshenas S H, Naeini M. Resilient temporal graph convolutional network for smart grid state estimation under topology inaccuracies[J]. IEEE Open Access Journal of Power and Energy, 2025, 12: 529-540.

[35] Ebtia A, Ghafouri M, Debbabi M, et al. Power distribution network topology detection using dual-graph structure graph neural network model[J]. IEEE Transactions on Smart Grid, 2025, 16(2): 1833-1850.

[36] Tang H S, Xu T Q, He Z L, et al. Topology identification of low-voltage distribution network nodes and dynamic adjustment of user nodes based on LSTM-GCN[J]. Electric Power Systems Research, 2026, 253: 112566.

[37] Wang Y, Shen X D, Tang X S, et al. A joint estimation method of distribution network topology and line parameters based on power flow graph convolutional networks[J]. Energies, 2024, 17(21): 5272.

[38] Wu H Y, Xu Z, Zhao J, et al. Gridtopo-GAN for distribution system topology identification[J]. IEEE Transactions on Industrial Informatics, 2023, 19(4): 5356-5366.

[39] Li N, Zhang J, Ma D M, et al. Enhancing detection of false data injection attacks in smart grid using spectral graph neural network[J]. IEEE Transactions on Industrial Informatics, 2025, 21(6): 4543-4553.

[40] Xia W, Li Y, Yu L S, et al. Locational detection of false data injection attacks in the edge space via hodge graph neural network for smart grids[J]. IEEE Transactions on Smart Grid, 2024, 15(5): 5102-5114.

[41] Zhong J, Xu Z W, Chen C, et al. Advancing resilience with SDN: A comprehensive review of cyber-physical strategies for smart grid[J]. Smart Power & Energy Security, 2025, 1(4): 186-203.

[42] Islam M A, Ismail M, Boyaci O, et al. Graph neural network based prediction of data traffic in cyber-physical smart power grids[C]. 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. Singapore, 2022: 322-327.

[43] Su Q X. Routing optimization in communication networks using trust-aware deep reinforcement learning with graph neural networks[C]. 2025 5th International Conference on Mobile Networks and Wireless Communications. Tumkur, 2026: 1-5.

[44] Tam P, Ros S, Song I, et al. A survey of intelligent end-to-end networking solutions: Integrating graph neural networks and deep reinforcement learning approaches[J]. Electronics, 2024, 13(5): 994.

[45] Islam M A, Atat R, Ismail M. Software-defined networking-based resilient proactive routing in smart grids using graph neural networks and deep Q-networks[J]. IEEE Access, 2024, 12: 111169-111186. [LinkOut].

[46] Pu H, Yang X. Topology reconstruction and intelligent scheduling optimization for power communication networks based on graph neural networks[C]. 2025 International Conference on Advances in Electrical Engineering and Computer Applications. IEEE, 2025: 189-193.

[47] Cini A, Marisca I, Alippi C. Filling the gaps: Multivariate time series imputation by graph neural networks[PP/OL]. 2022, arXiv. 2108.00298.

[48] Li B, Chen Z J, Zhong H W, et al. A graph neural

network with auxiliary task learning for missing PMU data reconstruction[PP/OL]. 2025, arXiv: 2512.24542.

[49] Pei Y Z, Yang J, Wang J D, et al. An emergency control strategy for undervoltage load shedding of power system: A graph deep reinforcement learning method[J]. IET Generation, Transmission & Distribution, 2023, 17(9): 2130-2141.

[50] Wu X Y, Cao Y C, Wu H T, et al. Hybrid learning-based fault prediction and cascading failure mitigation in multi-network energy systems[J]. Scientific Reports, 2025, 15: 33938.

[51] Liu T, Liu F Y. Graph neural networks for evaluating the reliability and resilience of infrastructure systems: A systematic review of models, applications, and future directions[J]. IEEE Access, 2025, 13: 164883-164904.

[52] 贾文瑞. 基于图神经网络的电网设备拓扑感知型故障预测的算法[J]. 计算机科学与应用, 2025(6): 128-140.
(Jia W R. A topology-aware fault prediction algorithm for power grid equipment based on graph neural networks[J]. Computer Science and Application, 2025(6): 128-140.)

[53] 郑毅, 王承民, 刘保良, 等. 基于多层级时空图神经网络的风电机组在线异常检测[J]. 电力系统自动化, 2024, 48(5): 107-119.
(Zheng Y, Wang C M, Liu B L, et al. Online anomaly detection of wind turbines based on hierarchical spatio-temporal graph neural network[J]. Automation of Electric Power Systems, 2024, 48(5): 107-119.)

[54] Donon B, Clément R, Donnot B, et al. Neural networks for power flow: Graph neural solver[J]. Electric Power Systems Research, 2020, 189: 106547.

[55] Yang M, Qiu G, Liu T J, et al. Probabilistic power flow based on physics-guided graph neural networks[J]. Electric Power Systems Research, 2024, 235: 110864.

[56] Zhang Y D, Karve P M, Mahadevan S. Operational risk quantification of power grids using graph neural network surrogates of the DC optimal power flow[J]. Sustainable Energy, Grids and Networks, 2025, 43: 101748.

[57] Gao M S, Yu J, Yang Z F, et al. Physics embedded graph convolution neural network for power flow calculation considering uncertain injections and topology[J]. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(11): 15467-15478.

[58] Su T, Zhao J B, Pei Y S, et al. Probabilistic physics-informed graph convolutional network for active distribution system voltage prediction[J]. IEEE Transactions on Power Systems, 2023, 38(6): 5969-5972.

[59] Prashal G, Sumathi P, Padhy N P. Matrix completion-based learning of probabilistic power flow using a meta-graph generative autoencoder network[J]. IEEE Transactions on Industrial Informatics, 2026, 22(8): 6883-6893.

[60] Zhu Y H, Zhou Y Z, Wei W, et al. Real-time cascading failure risk evaluation with high penetration of renewable energy based on a graph convolutional network[J]. IEEE Transactions on Power Systems, 2023, 38(5): 4122-4133.

[61] Gorka J, Hsu T, Li W, et al. Cascading blackout severity prediction with statistically-augmented graph neural networks[J]. Electric Power Systems Research, 2024, 234: 110738.

[62] Sevak B, Jadhav S, Bui V H. Physics-informed graph neural jump ODEs for cascading failure prediction in power grids[PP/OL]. 2026, arXiv: 2603.20838.

[63] Yang K H, Xue F, Huang T, et al. Lightweight model for power grid cascading failures risk evaluation based on graph physics-informed attention network[J]. Expert Systems with Applications, 2025, 291: 128468. [LinkOut].

[64] Zhong K, Xu Y, Deng Y, et al. Hierarchical causal graph neural networks with cascading failure analysis for complex systems root cause identification[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2026, 56(3): 1659-1670.

[65] Pagnier L, Chertkov M. Physics-informed graphical neural network for parameter and state estimations in power systems[PP/OL]. 2021, arXiv: 2102.06349.

[66] Madbhavi R, Natarajan B, Srinivasan B. Graph neural network-based distribution system state estimators[J]. IEEE Transactions on Industrial Informatics, 2023, 19(12): 11630-11639. [LinkOut].

[67] Azam M F, Vanin M, Hermans C, et al. Physicsinformed factor graph neural networks for constrained state estimation in low observable distribution networks[J]. Sustainable Energy, Grids and Networks, 2026, 46: 102291.

[68] Berezin A, Balduin S, Oberließen T, et al. On zero-shot learning in neural state estimation of power distribution systems[PP/OL]. 2024, arXiv: 2408.05787.

[69] Jiao H, Wu C, Wei L, et al. A data-driven state estimation based on sample migration for low-observable distribution networks[J]. Algorithms, 2025, 18(3): 121. [LinkOut].

[70] Hu Z J, Zhu H, Lan L, et al. Low-observability distribution system state estimation by graph computing with enhanced numerical stability[J]. Eng, 2025, 6(7): 134. [LinkOut].

[71] Habib B, Isufi E, van Breda W, et al. Deep statistical solver for distribution system state estimation[J]. IEEE Transactions on Power Systems, 2024, 39(2): 4039-4050.

[72] 代钰欣, 郑涛, 鲁晓毅, 等. 基于 μ PMU 量测的配电网自适应拓扑识别方法[J]. 电力自动化设备, 2024, 44(8): 100-108.
(Dai Y X, Zheng T, LU X Y, et al. Adaptive topology identification method of distribution network based on μPMU measurement[J]. Electric Power Automation Equipment, 2024, 44(8): 100-108.)

[73] Li H R, Weng Y, Vittal V, et al. Distribution grid topology and parameter estimation using deep-shallow neural network with physical consistency[J]. IEEE

Transactions on Smart Grid, 2024, 15(1): 655-666. [LinkOut].

[74] Lei Y, Yang F, Feng Y, et al. A topology identification strategy of low-voltage distribution grids based on feature-enhanced graph attention network[J]. Energies, 2025, 18(11): 2821.

[75] Fahim S R, Atat R, Kececi C, et al. Graph neural network-based approach for detecting false data injection attacks on voltage stability[J]. IEEE Open Access Journal of Power and Energy, 2025, 12: 12-23. [LinkOut].

[76] Boyaci O, Narimani M R, Davis K R, et al. Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks[J]. IEEE Transactions on Smart Grid, 2022, 13(1): 807-819. [LinkOut].

[77] Takiddin A, Atat R, Ismail M, et al. Generalized graph neural network-based detection of false data injection attacks in smart grids[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2023, 7(3): 618-630. [LinkOut].

[78] Peng S, Zhang Z, Deng R, et al. Localizing false data injection attacks in smart grid: A spectrum-based neural network approach[J]. IEEE Transactions on Smart Grid, 2023, 14(6): 4827-4838.

[79] Jorjani M, Seifi H, Varjani A Y. A graph theory-based approach to detect false data injection attacks in power system AC state estimation[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2465-2475. [LinkOut].

[80] Feng H T, Han Y H, Si F Y, et al. Detection of false data injection attacks in cyber-physical power systems: An adaptive adversarial dual autoencoder with graph representation learning approach[J]. IEEE Transactions on Instrumentation and Measurement, 2024, 73: 9000411. [LinkOut].

[81] Takiddin A, Ismail M, Atat R, et al. Robust graph autoencoder-based detection of false data injection attacks against data poisoning in smart grids[J]. IEEE Transactions on Artificial Intelligence, 2024, 5(3): 1287-1301. [LinkOut].

[82] Ahmed A, Basumallik S, Gholami A, et al. Spatio-temporal deep graph network for event detection, localization, and classification in cyber-physical electric distribution system[J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 2397-2407. [LinkOut].

[83] Li X Z, Zhang T, Wang J, et al. Achieving network resilience through graph neural network-enabled deep reinforcement learning[J]. IEEE Network, 2025, 39(6): 279-287. [LinkOut].

[84] Yang L, Wei Y F, Yu F R, et al. Joint routing and scheduling optimization in time-sensitive networks using graph-convolutional-network-based deep reinforcement learning[J]. IEEE Internet of Things Journal, 2022, 9(23): 23981-23994. [LinkOut].

[85] Mestry P, Rathi A. Deep learning-based real-time malicious network traffic detection system for cyber-physical systems[C]. 2022 IEEE International Conference on Blockchain and Distributed Systems Security. Pune, 2022: 1-9. [LinkOut].

[86] Song K, Kim M, Kim H. Graph-based large scale probabilistic PV power forecasting insensitive to space-time missing data[J]. IEEE Transactions on Sustainable Energy, 2025, 16(1): 160-173. [LinkOut].

[87] Pei J H, Wang J Y, Shi D Y, et al. Detection and imputation-based two-stage denoising diffusion power system measurement recovery under cyber-physical uncertainties[J]. IEEE Transactions on Smart Grid, 2024, 15(6): 5965-5980. [LinkOut].

[88] Wu T, Zhang Y A, Liu Y, et al. Missing data recovery in large power systems using network embedding[J]. IEEE Transactions on Smart Grid, 2021, 12(1): 680-691. [LinkOut].

[89] Ansari M, Ghafouri M, Ameli A. Graph deviation network with physics-informed detection and robust Hınfty control for cyberattack resilience in wind-integrated power grids[J]. IEEE Transactions on Power Systems, 2026, 41(3): 2296-2316. [LinkOut].

[90] Agarwal L, Jaint B, Mandpura A K. Hybrid AI framework for detecting cyberattacks and predicting cascading failures in power systems[J]. Sustainable Computing: Informatics and Systems, 2025, 48: 101222.

[91] Sweeten J, Elshazly A, Takiddin A, et al. Cyber-physical fusion for GNN-based attack detection in smart power grids[J]. IEEE Open Access Journal of Power and Energy, 2025, 12: 515-528. [LinkOut].

[92] Saidane A, ElKamel A, Youssef H. A survey on graph neural networks for DDoS detection[J]. SSRN Electronic Journal, 2026.

作者简介

赵天阳 (1989−), 男, 副教授, 博士, 博士生导师, 主要研究方向为弹性电网/电力系统可靠性、车网互动技术、科学机器学习, E-mail: zhaoty@xjtu.edu.cn;

罗嗣朋 (2002−), 男, 博士生, 主要研究方向为配电系统仿真、图神经网络、状态估计, E-mail: sipengluo@stu.xjtu.edu.cn;

谢海鹏 (1989−), 男, 教授, 博士, 主要研究方向为配电系统安全风险防控、量子信息学的应用, E-mail: haipengxie@xjtu.edu.cn;

司渭滨 (1989−), 男, 正高级工程师, 主要从事电力系统安全稳定研究工作, E-mail: siweibin@dky.sn.sgcc.com.cn;

王鹏 (1955−), 男, 教授, 博士, 主要研究方向为智能电网、电力系统运行、规划、可靠性, E-mail: epwang@ntu.edu.sg;

别朝红 (1970−), 女, 教授, 博士, 主要研究方向为电力系统极端事件防御及弹性提升, E-mail: zhbie@mail.xjtu.edu.cn.