电力信息网络中的基于图神经网络的网络攻击检测研究

吴让乐[1] 刘 钘[1] 尉 颖[1] 何乃彩[1]
WU Rangle LIU Xing YU Ying HE Naicai

摘 要 针对当前电力信息网络攻击检测方法存在的误报率较高和 F_1-score 较低的问题，文章提出了一种基于图神经网络的电力信息网络攻击检测方法。首先，通过生成电力信息网络的拓扑图，以图结构的形式详细表示了用户服务器之间的网络拓扑结构以及它们之间的交互关系。然后，利用图神经网络的强大功能，对电力信息网络拓扑图中的攻击特征进行有效提取和分类。这种方法能够深入分析网络中的复杂关系和模式，从而实现对电力信息网络中各种网络攻击的准确检测。通过一系列实验验证，文章设计的方法在电力信息网络攻击检测中表现出色。具体而言，误报比例被控制在不超过 0.1% 的水平，而 F_1-score 则达到了不低于 90% 的高值。表明该方法在检测电力信息网络攻击时具有较高准确度和可靠性。因此，基于图神经网络的电力信息网络攻击检测方法在电力信息网络攻击检测领域具有广阔的应用前景，能够为电力系统的安全稳定运行提供有力的技术支持。

关键词 电力信息网络；图神经网络；网络攻击；网络拓扑图；卷积操作；F_1-score

doi：10.3969/j.issn.1672-9528.2025.01.020

0 引言

电力信息物理融合系统是一种高度集成的系统，通过深度融合计算、通信和控制技术，将电网的物理环境与信息网络紧密地结合在一起。这种系统具有多维度和异质复杂的特点，能够实现实时感知、动态调控和提供信息服务的综合功能。电力信息物理融合系统的出现，显著提升了电力系统的智能化水平和运行效率，但同时也带来了新的安全挑战。随着电网规模的不断扩大、用电负荷的持续增加以及电力系统自动化水平的不断提高，电力信息网络的运行机制变得越来越复杂，这种复杂性使得电力信息网络的安全问题变得更加突出。电力信息网络的安全不仅关系到电力系统的稳定运行，而且对国家经济安全和社会稳定具有深远影响。具体来说，电力信息物理融合系统通过先进的传感器、智能终端和高速数据通信技术，实现了对电网状态的实时监测和分析。这些技术的融合使得电力系统能够更加灵活地应对各种突发情况，提高供电的可靠性和质量。此外，通过大数据分析和人工智能算法，电力信息物理融合系统能够优化电力资源的配置，降低能源消耗，提高经济效益。然而，随着电力系统与信息网络的深度融合，系统的安全风险也相应增加。黑客攻击、网络病毒和内部威胁等安全问题可能导致电力系统的瘫痪，甚至引发大规模停电事件，对社会生产和人民生活造成严重影响。因此，加强电力信息物理融合系统的安全防护措施，建立健全的安全管理体系，已经成为电力行业面临的重要课题。

目前，国内外的学者们已经在电力信息网络攻击检测领域开展了一系列的研究，并取得了一定的成果。例如，文献 [1] 提出了一种基于改进 EfficientNet 的检测方法。该方法利用 EfficientNet 的深度可分离卷积技术，对网络流量进行深度特征提取，从而识别出异常流量和潜在的攻击行为。文献 [2] 提出了一种基于 GRU（门控循环单元）神经网络的检测方法。GRU 神经网络具有强大的序列建模能力，能够对网络流量进行实时分析。通过提取流量的统计特征和频域特征，训练 GRU 网络以识别异常流量模式，从而实现对网络攻击行为的检测。尽管在电力信息网络攻击检测领域已经取得了一定的进展，但仍然存在一些不足之处。特别是在面对高级持续性威胁（APT）等新型攻击手段时，传统检测方法往往无法实现精准检测。文献 [3] 提出基于差分波形奇异值极差的通用电力扰动检测方法，利用奇异值极差区分扰动与正常波形，实现扰动检测，具有较高的检测灵敏性。但是，该方法高度依赖前期采集的历史数据，一旦参考值失准，检测算法的准确性会大大降低。文献 [4] 提出基于频繁模式增长算法（frequent-pattern growth algorithm，FP-Growth）的新能源配

1. 甘肃同兴智能科技发展有限责任公司 甘肃兰州 730050

电网信息物理系统（cyber-physical systems，CPS）网络攻击检测方法，分析考虑网络攻击的有源配电网控制模型及 CPS 网络攻击影响机理，采用 FP-Growth 算法挖掘历史数据异常信号的频繁项集和强关联关系，实现对有源配电网 CPS 网络攻击的检测。但随着新能源接入设备的增加，数据规模不断增大，该算法的运行时间会显著增加，进而影响检测的实时性。因此，为了应对这些新的安全挑战，本文提出了一种在电力信息网络中基于图神经网络的网络攻击检测研究。图神经网络在处理图结构数据方面具有独特的优势，能够更好地捕捉电力信息网络中的复杂关系和模式，从而提高检测的准确性和效率。

1 电力信息网络图生成

在本文中，采用了图神经网络技术来对电力信息网络中的攻击行为进行有效的检测。图神经网络的输入向量通常以二维图像的形式展现，因此，在基于图神经网络的攻击行为检测流程开始之前，首先需要将电力信息网络的数据流转换成图像形式。这一转换过程使得用户服务器之间的网络拓扑结构和交互情况能够以图结构的形式得到清晰的表示。在这个图结构中，服务器的 IP 地址被抽象为图的基本构成单元，即节点（Vertex）。与此同时，服务器之间进行的数据交换或指令传递则被映射为连接这些节点的边（Edge）。这些边具有明确的方向性，它们从发起交互的源服务器直接指向接收交互的目的服务器，从而构建出一个具有方向性的有向图，其用公式表示为：

$$G = (V, L, N) \tag{1}$$

式中：G 表示电力信息网络拓扑图；V 表示节点集合，包含了所有参与交互的源服务器与目的服务器的 IP 地址；L 表示边集合，包含每一对服务器之间发生的交互事件；N 表示节点属性集合，包含每个节点的特征信息 [5]。由于电力系统遭受网络攻击时，数据包大小会显著偏离正常范围，打破正常的数据包大小分布规律，并且电力信息网络正常运行情况下，电力系统的各个环节都存在既定的通信节奏，通信频率维持在相对稳定水平，受电力运行规律约束。然而，遭遇网络攻击如中间人攻击时，服务器为重新同步信息会频繁交互，导致通信频率陡增。因此，本文中主要考虑平均请求数据包大小、通信频率两个属性。通过将平均请求数据包大小与 PP 通信频率整合至图的节点属性中，以此生成一个完整的电力信息网络拓扑图，直观展示电力信息网络拓扑结构。

2 基于图神经网络的攻击行为检测

生成电力信息网络拓扑图后，利用图神经网络对电力信息网络拓扑图深度挖掘，图神经网络自动从电力信息网络拓扑图中高效且全面地提取特征，区分图结构数据 [6]。图神经网络由输入层、卷积层、隐藏层和输出层组成，将电力信息网络拓扑图输入到网络中，利用经过训练的网络对当前电力信息网络拓扑图进行检测。电力信息网络拓扑图输入到输入层，在该功能中对图编码并将其发送到卷积层，卷积层对图结构进行攻击特征变换与攻击特征提取，生成图上各个节点的代表性向量，当面对一个由 N 个节点组成、每个节点拥有 M 维特征的图时，利用邻接矩阵刻画节点间的连接关系，以及特征矩阵捕捉节点的具体属性，根据邻接矩阵和特征矩阵对电力信息网络拓扑图进行卷积操作，其用公式表示为：

$$H(G) = \alpha(\boldsymbol{\varpi}\, \boldsymbol{A}^2 + \boldsymbol{W}\boldsymbol{D}^2)^{N\times M} \tag{2}$$

式中：$H(G)$ 表示卷积层卷积操作提取的电力信息网络拓扑图攻击特征；α 表示激活函数；$\boldsymbol{\varpi}$ 表示度数矩阵；$\boldsymbol{A}$ 表示邻接矩阵；$\boldsymbol{W}$ 表示可训练的参数矩阵；$\boldsymbol{D}$ 表示特征矩阵 [7]。引入自连接以增强节点自身的特征表示，并利用度数矩阵进行归一化处理，以确保信息的平滑传递。将提取的电力信息网络拓扑图特征输入到隐藏层，隐藏层对提取的特征降维处理，进一步压缩图的信息量并聚焦于最具代表性的节点，首先将节点或边的特征映射至新的向量空间，随后根据特定维度上的值进行排序，选取前 k 个节点进行降维操作。这一过程基于节点的评分或特征值大小，通过对选定节点的新向量进行平均或最大池化，合成一个新的图特征表示，节点的评分计算公式为：

$$z = \alpha(H(G)^{-1} + \mu \odot k) \tag{3}$$

式中：z 表示节点的自注意力重要度分数；μ 表示权重参数。获得重要性分数后，设定一个池化率（介于 0 和 1 之间），用于指定保留节点的比例 [8]。通过排序和筛选这些分数，更新邻接矩阵和特征矩阵，仅保留最重要的节点及其相连的边，从而实现图的有效下采样，其用公式表示为：

$$\boldsymbol{x} = \kappa \boldsymbol{A}_{\text{out}}(z, N)\boldsymbol{D} \tag{4}$$

式中：$\boldsymbol{x}$ 表示降维后的电力信息网络拓扑图攻击特征；κ 表示池化率；$\boldsymbol{A}_{\text{out}}$ 表示池化后的邻接矩阵 [9]。将降维后的网络拓扑图攻击特征输入到输出层，对攻击特征进行全局聚合操作，实现特征分类，确定电力信息网络拓扑图攻击特征所属类别，其用公式表示为：

$$y = \text{softmax}\ R(x_G) \tag{5}$$

式中：y 表示电力信息网络攻击属于各个类别的概率；R 表示分类器；$\boldsymbol{x}_G$ 表示攻击类别 G 的电力信息网络拓扑图特征。

图神经网络输出层输出概率最大的攻击类别，以此确定当前网络攻击行为，实现电力信息网络中的基于图神经网络的网络攻击检测。

3 实验论证

3.1 实验数据集及参数设置

为了深入评估和验证本文所提出的基于图神经网络的电力信息网络中网络攻击检测方法的性能，进行一系列对比实验。这些实验将涉及本文所提出的检测方法，并将其与文献 [1] 中介绍的基于改进 EfficientNet 的检测方法以及文献 [2] 中提出的基于门控循环单元（GRU）神经网络的检测方法进行比较。将使用一个公开的电力信息网络攻击检测数据集来进行这些实验。该数据集详细记录了包括 Web 攻击、拒绝服务（DoS）攻击、分布式拒绝服务（DDoS）攻击、暴力破解攻击以及渗透攻击等多种网络攻击类型，共计超过 10 种不同的攻击类别。为了实验的需要，将这个数据集划分为测试集和训练集两部分，以便于更准确地评估各种检测方法的有效性和准确性。具体的数据集划分情况和实验设置如表 1 所示。

表 1 数据集基本统计

数据集	负样本数量	正样本数量	流量数	项目数
训练集	30 000	25 000	542 564	223 641
测试集	15 000	10 000	362 484	168 465

从数据集中随机选取 2/3 数据构成图神经网络训练集，剩余作为方法性能验证集。根据需求对图神经网络参数设置为：层数设置为 3 层，节点特征为维度设置为 2 维，隐藏层维度设置为 2 维，嵌入传播深度设置为 1.25，学习率设置为 0.001，批量化处理大小设置为 128，迭代次数设置为 100，优化器随机梯度下降设置为 0.01，激活函数设置为 ReLU。在所有参数设置完毕后，将训练集输入到图神经网络中进行训练，目的是让模型学习到电力信息网络中的攻击特征。训练完成后，将验证集中的数据流输入到训练好的图神经网络中，通过模型对数据流进行分类，从而识别和检测网络攻击行为。最后将记录下测试数据的分类结果，以便进一步分析模型的性能和准确性。

3.2 实验指标

为了全面评估不同检测方法的性能表现，采用误报比例和 F_1-score 这两个关键指标。误报比例 = 错误检测样本数量 / 总检测样本数量。通过这个比例，可以直观了解在本次实验中，3 种不同的检测方法在检测精度方面的表现。鉴于实验测试集中攻击流量样本的数量相较于正常样本来说偏少，为了更准确地评估检测方法在面对潜在样本不平衡情况下的性能，引入了 F_1-score 指标。F_1-score 值域为 0~100%，F_1-score=2× 精确率 × 召回率 / 精确率 + 召回率，数值越高，则表示检测精度越高，检测方法的综合性能越好。通过综合运用误报比例和 F_1-score 这两个指标，可以对各种检测方法的性能进行全面而深入的评价。

3.3 实验结果与讨论

根据实验中电力信息网络攻击检测结果，表 2 统计了 3 种方法不同攻击类型的误报比例，并绘制 3 种方法电力信息网络攻击检测 F_1-score 分数图。

表 2 电力信息网络攻击误报比例

单位：%

攻击类型	本文方法	文献 [1] 方法	文献 [2] 方法
Web 攻击	0.06	3.06	5.23
DoS 攻击	0.02	3.52	5.42
DDoS 攻击	0.04	3.14	5.01
暴力破解攻击	0.06	3.62	5.69
渗透攻击	0.05	3.33	5.74
僵尸网络攻击	0.08	3.25	5.89
中间人攻击	0.07	3.27	5.42
拒绝服务攻击	0.09	3.16	5.36

从表 2 中数据可以看出，在电力信息网络攻击检测场景中，设计方法误报比例最低，不超过 0.1%，文献 [2] 方法误报比例最高。从图 1 可以看出，设计方法 F_1-score 分数最高，同样文献 [2] 方法 F_1-score 分数最低。本文方法在多种攻击类型下均表现出色，这是由于图神经网络能够对电力信息网络拓扑结构实现精准建模。

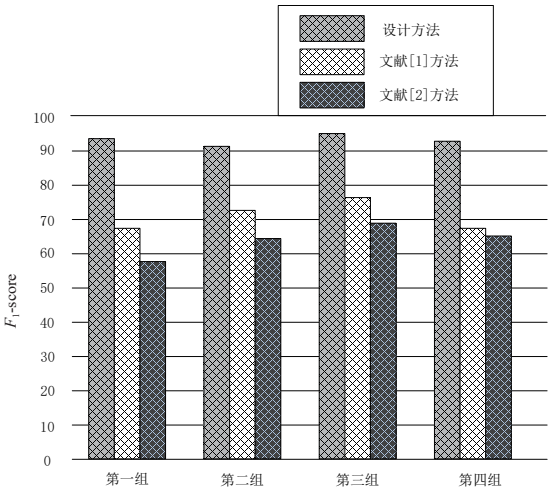

图 1 电力信息网络攻击检测 F_1-score

以 Web 攻击为例，该攻击常常通过伪装正常网页来渗透系统，传统方法可能仅关注流量表面特征而误判，但本

文方法考虑服务器间的复杂交互关系，基于所构建的拓扑图，可以清晰呈现 Web 服务器与后端数据库服务器、认证服务器之间的正常请求与响应模式，采用图神经网络捕捉异常连接或数据流向变化，有效降低误报率。对于 DoS 和 DDoS 攻击，本文方法通过分析拓扑图中各节点的通信频率变化，捕捉短时间内海量、重复的数据包冲击特征，能够迅速做出判断，及时发出警报。因此，上述实验证明本文设计的方法可以实现对电力信息网络攻击精准检测，具有良好的性能。

4 结语

在当今时代，电力信息网络的复杂性日益增加，同时面临的网络安全威胁也变得越来越严峻。在这种背景下，基于图神经网络的网络攻击检测研究提供了一种新颖且有效的解决方案。图神经网络因其强大的图结构数据处理能力，在处理复杂网络环境中的数据时，展现出了独特的优势。这种优势为电力信息网络的安全防护提供了新的视角和思路。

本文深入探讨了图神经网络在电力信息网络攻击检测中的应用，并设计了一系列基于图神经网络的检测算法。这些算法不仅能够有效识别网络中的异常流量和潜在攻击行为，还能够在一定程度上应对未知攻击和复杂多变的网络环境。实验结果表明，基于图神经网络的检测算法在电力信息网络环境中具有较高的检测精度和较低的误报率，为电力信息网络的安全防护提供了有力的技术支持。具体来说，图神经网络通过其独特的图结构数据处理能力，能够更好地理解和分析电力信息网络中的复杂关系和模式。这种理解能力使得图神经网络在检测网络攻击时，能够更准确地识别出异常行为和潜在威胁。此外，图神经网络还具有良好的泛化能力，能够应对未知攻击和复杂多变的网络环境。这意味着即使在面对新的攻击手段和不断变化的网络环境时，基于图神经网络的检测算法也能够保持较高的检测精度和较低的误报率。

总的来说，本文的研究为电力信息网络的安全防护提供了一种新的思路和方法。通过深入探讨图神经网络在电力信息网络攻击检测中的应用，并设计出一系列基于图神经网络的检测算法，为电力信息网络的安全防护提供了有力的技术支持。但是，图神经网络模型的训练对数据质量要求较高，一旦数据存在噪声、缺失值等，会严重影响模型的训练效果。未来研究可以着力于优化数据处理流程，结合智能技术，开发新型数据清洗与标注工具，进一步拓展图神经网络对复杂攻击模式的识别能力，为电力信息网络的安全防护提供更有力的技术支持。

参考文献：

[1] 李泽科 , 郭久煜 , 邓春荣 , 等 . 基于改进 EfficientNet 的电力资产信息数据流量异常检测的应用 [J]. 信息安全与通信保密 , 2024 (5): 42-53.

[2] 邱佳玉 . 基于 GRU 神经网络的 IPv6 DDoS 攻击实时检测与防御研究 [J]. 电脑编程技巧与维护 , 2024 (5): 163-165.

[3] 王常智 , 张文海 , 刘亮 , 等 . 基于差分波形奇异值极差的通用电力扰动检测方法 [J]. 电网技术 , 2023, 47(5):2147-2155.

[4] 李瑞 , 刘珊 , 闫磊 . 基于 FP-Growth 算法的新能源配电网 CPS 网络攻击检测方法 [J]. 电信科学 , 2024, 40(11):103-113.

[5] 何佳月 . 增量式学习支持下的电力监控系统网络安全攻击检测分析 [J]. 电工技术 , 2024 (13): 43-45+52.

[6] 王申全 , 刘若奇 , 赵昌北 . 虚假数据注入攻击下线性参数时变多智能体系统 H_-/H_ ∞攻击检测 [J]. 长春工业大学学报 , 2024, 45 (2): 97-103+193.

[7] 赵晓峰 , 王平水 . 基于组合加权 k 近邻分类的无线传感网络节点复制攻击检测方法 [J]. 传感技术学报 , 2024, 37 (6): 1056-1060.

[8] 王小宇 , 贺鸿鹏 , 马成龙 , 等 . 基于多模态神经网络流量特征的网络应用层 DDoS 攻击检测方法 [J]. 沈阳农业大学学报 , 2024, 55 (3): 354-362.

[9] 刘慧 , 纪科 , 陈贞翔 , 等 . 结合图卷积神经网络和集成方法的推荐系统恶意攻击检测 [J]. 计算机科学 , 2024, 51 (z1): 952-960.

【作者简介】

吴让乐（1989—），男，甘肃兰州人，本科，工程师，研究方向：信息安全。

刘钘（1993—），男，湖北天门人，本科，工程师，研究方向：电网数字化。

尉颖（1989—），女，甘肃兰州人，本科，工程师，研究方向：电网数字化。

何乃彩（1996—），女，甘肃靖远人，本科，工程师，研究方向：电网数字化。

（收稿日期：2024-10-12）