

DOI:10.3969/j.issn.1671-0673. 2026. 04. 001

复杂通信网络脆弱性分析方法综述

侯春峰, 周 刚, 李珠峰

(信息工程大学, 河南 郑州 450001)

摘要: 通信网络是众多领域信息化应用的基础设施依托, 其安全性至关重要。系统性地分析与评估通信网络的脆弱性, 已成为网络安全与复杂系统研究中的重要课题。首先, 从复杂网络角度界定了通信网络脆弱性的内涵, 归纳了包括结构、功能和动力学层面的常用评价指标。其次, 在复杂网络关键节点识别的统一框架下, 分析了节点重要性排序、网络瓦解与级联失效 3 类典型研究方法的内在联系, 分别综述了各类方法的研究进展和适用特点。最后, 结合通信网络的现实特征, 分析了面临的主要挑战, 展望了未来研究的发展方向。

关键词: 通信网络; 复杂网络; 关键节点; 网络脆弱性

中图分类号: TN915; TP393.08

文献标识码: A

文章编号: 1671-0673(2026)04-0379-12

Survey of Vulnerability Analysis of Communication Networks Based on Complex Network

HOU Chunfeng, ZHOU Gang, LI Zhufeng

(Information Engineering University, Zhengzhou 450001, China)

Abstract: Communication networks constitute the foundational infrastructure supporting informationized applications across numerous domains, and their security is therefore of critical importance. Systematic analysis and evaluation of the vulnerability of communication networks have become a central research topic in the fields of network security and complex systems. Firstly, from the perspective of complex network theory, the concept of the vulnerability of communication networks is formally defined, and commonly used evaluation metrics at the structural, functional, and dynamical levels are summarized. Secondly, within a unified framework of critical node identification in complex networks, the intrinsic relationships among three representative research paradigms, which include node importance ranking, network dismantling, and cascading failure, are analyzed, and the representative methods and recent research advances under each paradigm are reviewed. Finally, in light of the practical characteristics of communication networks, the major challenges are discussed, and future research directions are outlined.

Key words: communication networks; complex network; key nodes; network vulnerability

伴随着信息化、智能化在工业、能源、交通、金融等领域的快速发展与普及, 通信网络作为基础设施支撑的地位也愈加重要。通信网络从早期的组织架构较为单一、功能模块相对固定的数据通信系统, 已逐渐发展为要素高度异质、信息域和物

理域强耦合, 且结构持续动态变化的复杂网络系统。这种变化在显著提升通信网络便利性的同时, 也暴露出了其前所未有的脆弱性。2015 年底乌克兰电网被攻击事件、2021 年美国输油管道遭勒索关停事件、2024 年 CrowdStrike 更新异常导

收稿日期: 2026-02-23; 修回日期: 2026-05-22

作者简介: 侯春峰(1982—), 男, 硕士生, 主要研究方向为数据智能处理。E-mail: cf2022xd@163.com

致全球性系统崩溃事件^[1]等,层出不穷的安全事件表明,通信网络的安全不仅与普罗大众的生活息息相关,更与国家的经济运行、社会发展和主权安全紧密相连。如何系统性地建模与分析通信网络的脆弱性,已经成为网络安全领域研究的热点问题。

传统的通信网络脆弱性分析方法,多依赖于工程化指标和具体场景,如误码率、吞吐量、时延抖动等,具有很强的针对性。但实际上,对通信网络造成巨大影响的通常来自关键节点或关键链路的故障。关键节点是指网络中承担了核心连接、流量汇聚或控制功能的重要网元。在通信网络中,这类节点主要包括核心路由器、骨干交换机、关键基站、SDN 控制器以及跨层耦合的网关设备等。而同样具有全局影响作用的关键链路,主要包括骨干光纤链路、跨域互联链路以及多层网络中的层间依赖链路等。这就涉及对关键节点和关键链路的分析识别,以及它们的失效与网络功能损失之间的关联机制分析等问题。此时,传统的分析方法往往力不从心。研究表明,通信网络具有小世界、无标度等复杂网络的典型特征,借助图论、统计物理学和传播动力学等复杂网络理论,能够对上述问题进行有效的分析与评估,从而反映通信网络的脆弱情况。近年来,围绕复杂网络的研究涌现出了大量成果,同时也出现众多以节点重要性排序(Node Ranking)^[2]、网络瓦解(Network Dismantling)^[3]和级联失效(Cascading Failures)^[4]等为主题的研究性综述。但这些综述文献多是在不同主题限定下,对相关方法有侧重的梳理和研究,对各个主题的内在联系研究方面仍相对缺乏。基于上述现状,本文从复杂网络理论出发,在回顾并分析已有的网络脆弱性概念的基础上,给出了更为贴合通信网络特征的通信网络脆弱性定义与内涵。进而根据复杂网络的结构破坏和性能退化机理,将上述3类主题研究按照静态拓扑分析、动态结构瓦解和功能级联失效的分析角度,纳入到以关键节点检测为手段的脆弱性分析统一框架中,从而梳理一条贯穿理论分析与现实应用的逻辑主线。

1 问题定义

与仅关注具体场景和工程指标的方法不同,基于复杂网络理论的方法,不仅关注节点在拓扑结构层面的影响,还关注因结构破坏而导致的网

络性能退化情况。本节将由此来定义通信网络的脆弱性,并给出其内涵分析,以及相应的评价指标体系。

1.1 通信网络脆弱性的定义与内涵

在复杂网络研究中,根据不同的研究阶段和理论依据,脆弱性(Vulnerability)有着不同的含义。早期的研究将网络脆弱性理解为节点和连边的移除对网络连通性的影响程度。此时的脆弱性概念通常等同于网络鲁棒性的损失,主要通过节点间距离和极大连通片(Giant Connected Component, GCC)的规模等指标来量化。鲁棒性又称为健壮性,是指网络在发生故障时维持其结构完整和基本功能的能力。之后出现了考虑节点间最短路径的网络效率概念,将脆弱性定义为移除节点后,信息在节点间传播效率的下降程度。这时的脆弱性主要指网络面临外部扰动时,其结构和功能发生退化的固有倾向。高脆弱性意味着更容易发生性能损失。在通信网络中通常表现为关键路由器被攻击后的路由表延迟收敛、骨干链路中断导致的业务流拥塞绕行等。随着网络动力学和多层相依网络研究的深入,发现系统在遭受特定攻击时会出现突变式的大范围功能失效现象,进而开始把网络发生级联失效的可能性与规模纳入到脆弱性的概念范畴。此时的网络脆弱性通常与节点依赖强度、故障传播能力和级联失效阈值密切相关。另外,级联失效脆弱性通常还包含韧性的概念,即网络在遭到破坏后,通过拓扑重构、资源重分配等自适应调整来逐步恢复原有功能的能力。虽然这与通信网络中链路失效后的动态路由协议重新收敛、软件定义的网络控制器对全局流量调度等机制相关,但与本文的关键节点检测主题存在一定的偏差,故暂不纳入讨论范围。同时,在复杂网络研究中,连边和节点能够相互转换表示,所以下文不对关键连边作另外的单独讨论。

尽管上述的脆弱性理解在各自的研究领域均具有重要意义,但无论哪一个都无法充分反映通信网络所体现的复杂结构、协议机制和服务导向等特性。因此,本文将通信网络脆弱性定义为在给定扰动假设下,由于拓扑结构的复杂性和功能之间的依赖关系,通信网络的连通性和服务性能在关键节点失效时所表现出的敏感性和退化程度。在复杂网络理论支撑下,该定义有以下3个方面的内涵。

1) 扰动模式。主要是指节点失效的方式,不

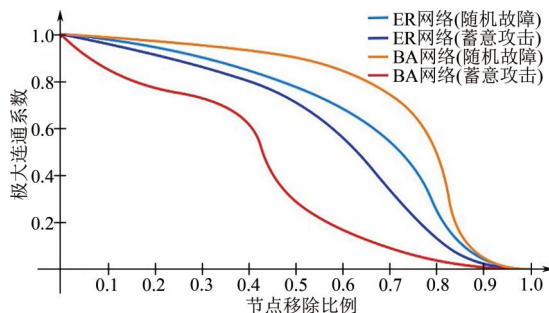
同的模式将直接影响网络脆弱性的分析结果。主要包括随机故障和蓄意攻击模式。在通信网络中,随机故障通常是设备宕机、链路故障等偶然的非恶意事件。蓄意攻击则通常是对核心路由器、骨干节点和关键自治域等进行有预谋的针对性攻击。无标度网络对随机故障具有高度的鲁棒性,但面对蓄意攻击时却极为脆弱,即复杂网络鲁棒且脆弱。由于随机故障不考虑节点的功能差异,往往会低估系统面临的风险。而蓄意攻击则假设掌握了部分网络信息,能够优先移除关键节点,因此对网络的威胁也更大。同时,蓄意攻击模式下的依次移除单个节点和同时移除一批节点,也将产生不同的脆弱性分析结果。

2) 关联要素建模。通信网络中各种要素主要通过网络来产生相互作用,所以对要素之间的关系表达主要通过网络抽象建模来体现。根据复杂程度和表达能力,可分为单层网络模型、多层相依网络模型和异质网络模型等。单层模型立足于描述网络的拓扑结构特征和节点之间的关系;多层模型不仅描述了层内节点之间的关系,更侧重于表达节点在功能上的跨层依赖关系;异质网络则融入了节点的属性语义信息,能够更全面细致地描述网络中各要素的特征与相互关系。不同的建模形式对应了不同的技术发展阶段,也催生了更多样和有效的脆弱性分析方法。例如,互联网骨干网层面的单层网络模型,可用来分析自治域之间的拓扑脆弱性;在分析5G核心层和用户功能层之间的关联关系时,多层相依模型更为适用;而在分析军事通信网络中不同装备实体的功能依赖时,语义增强的异质网络模型则能更灵活地适应不同的分析方法并得到更准确的分析结果^[5]。

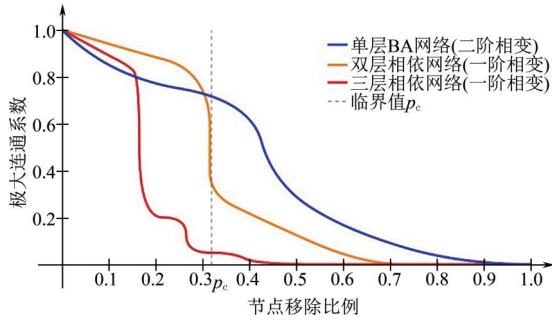
3) 分析维度。前文已分析指出,通信网络的脆弱性主要来自于关键节点的失效,而关键节点失效必将对网络产生一系列的不良影响。反过来看,可以通过分析节点失效所造成的影响来评判节点的关键程度,而分析维度正是对网络连通性和服务性能的变化情况进行不同角度的分析评估。首先是退化程度,可以通过节点可达性、服务可用性来反映。节点之间是否存在连通路是网络连通性的直接体现,GCC规模的变化幅度往往被视为网络是否存在结构性失效的衡量标准。服务可用性则关注网络中能够正常访问的服务的变化情况。某些情况下即使网络仍保持连通,但部分底层的数据节点失效,仍然将导致依赖于该节

点的关键服务不可用。而有时节点失效对网络性能的影响将通过路径重构和负载重分配等形式不断传播,进而导致大面积的网络服务不可用。现象上主要从吞吐量下降、传输时延增大和丢包率上升等通信特征来反映。其次是敏感性,主要是指针对不同的网络类型、耦合强度和扰动模式等参数,网络的连通性和服务性能在节点失效时的响应速度。例如,在蓄意攻击模式下,网络的GCC规模随着节点移除比例的增加而急剧下降,则称该网络对蓄意攻击高度敏感。敏感性也通常用渗流模型的相变现象来描述。渗流模型假设在以概率 p 打开的方格所组成的巨大网格中,当 p 很小时,由于打开的方格很少且相互孤立,流体无法穿透网络;当 p 超过某个特定值 p_c 时,打开的方格就会首次形成贯穿网络的通道。这一从封闭的不连通相到贯穿的连通相的变化过程即为相变,此时的 p_c 值被称为相变临界点,衡量连通程度的指标称为序参数。根据序参量曲线的变化特征,渗流相变可以分为二阶可导的二阶相变和仅一阶可导的一阶相变两种基本类型。

二阶相变又称为连续相变,特征是序参量曲线连续渐进式变化。一阶相变的序参量曲线则在 p_c 处发生不连续的跃变。在网络的GCC规模随节点移除比例而变化的敏感性分析中,针对随机故障和蓄意攻击,度数服从泊松分布的ER网络均表现为二阶相变且没有明显的相变临界点,但蓄意攻击时的曲线倾斜度明显更大;而度数服从幂律分布的BA无标度网络则表现明显不同,随机故障时曲线变化较为平缓且相变临界点更靠近于1,蓄意攻击时的曲线变为陡峭的二阶相变且相变临界点明显变小。当网络为多层相依网络时,由于层间节点存在较强的功能依赖,则网络功能随着节点失效比例的增加而表现出突变式的一阶相变,且网络层数越多、功能依赖越强,相变临界点也越小,表示网络对扰动越敏感。渗流相变示意图如图1所示。



(a) ER、BA网络在随机故障和蓄意攻击下的相变对比示意图



(b) 单层网络和多层相依网络的相变对比示意图

图1 渗流相变示意图

综上所述,本文的通信网络脆弱性定义涵盖扰动模式、关联要素建模和分析维度等方面,满足复杂网络理论研究的要求,与现实通信网络特征相契合,能更好地支撑网络脆弱性的分析与评估。

1.2 评价指标

根据脆弱性内涵,通信网络的脆弱性可从节点可达性、服务可用性与性能退化3个维度来评价。相应地,从结构层面、功能层面和动力学层面来归纳常用的评价指标。

1.2.1 结构层面

1)极大连通系数,表示为

$$S = \frac{1}{N} |V_{GCC}| \quad (1)$$

式中: $|V_{GCC}|$ 表示移除节点后网络中GCC所包含的节点数; N 表示网络的初始节点总数。该指标用于衡量网络的整体连通性,数值越大表示失效节点的影响越小,网络的脆弱性也越低。该指标直观且计算效率高,但是准确度相对较低。

2)连通片数量,表示为

$$N_c = L \quad (2)$$

式中, L 表示移除节点后网络碎裂形成的连通片数量。该指标反映了网络结构的碎片化程度。

3)平均最短路径长度,表示为

$$l = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij} \quad (3)$$

式中, d_{ij} 为网络中节点间的最短路径。该指标反映了网络的整体通信代价,当关键节点失效后,路径中断或绕行将明显提高最短路径的长度。

1.2.2 功能层面

1)网络效率。该指标从信息传播速度来衡量网络性能。节点移除后,若指标值变化不明显,表示信息流动强度未降低,相应网络脆弱性也越低,表示为

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \quad (4)$$

2)可用服务比例,表示为

$$A = \frac{|V_{service}^{active}|}{|V_{service}|} \quad (5)$$

式中: $V_{service}$ 表示服务节点总数; $V_{service}^{active}$ 表示可正常访问的服务节点数量。该指标在数据中心网络、云计算网络等多层网络研究中被广泛采用。

3)功能连通性指标。功能连通主要指是否存在满足带宽、路由策略和协议约束的有效通信路径,通过可达业务流比例来表示,即

$$C_f = \frac{1}{M} \sum_{k=1}^M \delta(f_k) \quad (6)$$

式中: M 表示业务流总数; f_k 表示任意业务流,若存在有效通信路径,则指示函数 $\delta(f_k)=1$,否则 $\delta(f_k)=0$ 。

1.2.3 动力学层面

1)级联失效规模。该指标反映一次扰动最终造成的系统性损伤程度,表示为

$$F = 1 - \frac{N_s}{N} \quad (7)$$

式中, N_s 表示级联过程结束后仍存活的节点数。

2)负载容量阈值。在负载—容量(Load-Capacity, L-C)模型中,节点容量通常定义为

$$C_i = (1 + \alpha)L_i \quad (8)$$

式中: L_i 为负载量; α 为容量冗余系数。则负载容量阈值的定义为

$$\alpha_c = \min \{ \alpha | F(\alpha) \leq \varepsilon \} \quad (9)$$

式中: $F(\cdot)$ 表示级联失效规模计算函数; ε 为可接受的系统失效上限,等式右边表示失效规模达到可接受的程度时 α 的最小取值,此时的 α 即为负载容量阈值 α_c 。易知, α_c 越大时,网络需要越多的冗余容量,也就越脆弱;同时,当 $\alpha \geq \alpha_c$ 时,网络系统维持稳定运行,当 $\alpha < \alpha_c$ 时系统对扰动高度敏感。

3)系统功能损失率。该指标用于描述网络性能随时间变化的退化过程,表示为

$$R(t) = 1 - \frac{P(t)}{P(0)} \quad (10)$$

式中, $P(t)$ 表示 t 时刻网络可承载的有效流量或服务能力。

2 考虑关键节点的脆弱性分析方法

通信网络作为典型的复杂网络系统,在节点移除、路径重构和负载转移等方面的变化特征与复杂网络理论高度一致。根据扰动粒度、移除策略约束条件和失效传播机制的不同,现有的通过

关键节点来衡量复杂网络脆弱性的研究主要有 3 种类型:节点重要性排序、网络瓦解和级联失效。三者 in 研究目标、分析对象与评价指标上既相互关联,又各有侧重。它们都可以看作是寻找网络的关键节点,移除这些使网络脆弱的关键节点将导致网络结构和功能的极大损失。若通过网络剩余 GCC 的规模来衡量这种损失,那么渗流模型的

相变过程则是比较直观的反映。3 种评估类型的特点比较如表 1 所示。可以看出,网络损失在相变的表现上逐步强烈,这也说明网络脆弱点识别的不断优化与精准度的提升。正因如此,本文采取以“关键节点检测”为主线,将节点重要性排序、网络瓦解和级联失效构成统一的分析框架,对相关方法和进展进行梳理分析。

表 1 3 种脆弱性评估类型的特点对比				
分析类别	研究内容	移除策略	渗流相变特点	通信网络应用场景
节点重要性排序	评估节点或连边对网络的影响程度并排序	依序移除	结构相关的渗流过程,序参量曲线为二阶相变,临界阈值较大	核心路由器重要性评估、基站关键度识别
网络瓦解	移除最小规模的节点或连边集合,使网络最大程度地瓦解	协同移除	最优渗流过程,序参量曲线为陡峭的二阶相变,临界区间明显压缩	关键链路切断策略、最小破坏集求解
级联失效	评估节点或连边的失效导致网络连锁崩溃的可能性与规模	少量移除	非线性渗流,突变式的一阶相变	拥塞扩散预测、故障传播控制

2.1 节点重要性排序

在该类型的研究中,网络通常被建模为静态或弱动态的单层图结构,利用网络统计指标来计算节点的重要性并排序,然后依序移除节点并分析其对网络的影响程度。节点重要性排序作为出

现最早的复杂网络问题,相关研究和综述文献较为常见。

本文为避免重复性表述,根据实现方法的差异度,仅划分为传统中心性方法和机器学习方法两大类。两者的特点比较如表 2 所示。

表 2 节点重要性排序方法分类对比				
方法分类	特点	优点	缺点	通信网络应用场景
传统中心性	主要利用节点在网络拓扑中的连接情况、位置特征等	多数算法复杂度低;思路简单,可解释性强	网络建模过于简单;区分度和稳定性均有限	中小规模网络的快速评估;实时性要求高的场景
机器学习	把问题转化为回归任务,构建模型来学习网络拓扑和节点特征	以任务为导向;特征表达能力强;准确度较高	依赖训练数据质量,泛化能力不足;可解释性较差	大规模网络预分析、异质信息网络节点评估

2.1.1 传统中心性方法

该类方法主要包括度中心性、介数中心性、特征向量中心性以及衍生的基于邻居信息、基于消息传播路径和 K-shell 分解等众多方法。Ma 等^[6]提出了基于度的拉普拉斯中心性,计算复杂度低且扩展性好。Zhu 等^[7]研究了基于距离的拉普拉斯能量改进模型,有效提高了排序精度,但计算成本也有所增加。传统的全局中心性方法依赖网络所有最短路径的遍历结果,在大规模网络中的计算代价极高。Salavati 等^[8]利用最近邻和次近邻信息来平衡节点的全局和局部结构特征,保持了较低的计算复杂度。Ma 等^[9]将结构洞理论和 K-shell 分解算法相结合,能够更准确地识别关键节点,但不适用于大规模网络。Ai 等^[10]利用资源分配机制来模拟信息在网络中的流动过程,结合共同邻居信息来量化节点之间的结构和功能相似性。该方法适用于大规模网络,但无法捕捉长距离的传播路径。

Kumar 等^[11]针对传统投票算法对邻域信息利用不足的局限,提出了基于邻域核心度来区分节点投票能力的 VoteRank 算法。Li 等^[12]进一步引入抑制因子和空间覆盖率概念对 VoteRank 算法进行改进,有效解决了节点影响范围重叠问题,从而提升了节点排序效率与准确度。Dong 等^[13]提出了基于通信概率和相对熵的多属性决策算法,能够更全面地刻画节点的重要性,该算法在军事通信网络中表现出较好的适用性。在通信网络中,上述中心性方法已广泛用于自治域网络的关键节点识别、无线网络中的关键网关定位^[14],以及电力通信网络中的关键站点评估^[15]等。然而,这些方法往往仅依赖于网络的拓扑结构,对影响网络功能的链路带宽、时延约束和协议特性等关键要素考虑较少,导致评估结果与实际情况存在一定的偏差。

2.1.2 机器学习的方法

机器学习的方法把节点重要性识别问题转化

为回归任务,利用传染病模型(SIR)和中心性指标生成节点标签,捕捉网络结构和节点重要性的潜在关系。在通信网络中,这类方法能够融合拓扑特征和流量特征,提升关键节点识别的准确性。Zhao等^[16]利用节点的邻域和网络拓扑特征来构建特征向量,训练了决策树、随机森林、SVM等多种分类器来预测节点的重要性。Asgharian等^[17]将节点的连通度和核心度等融合为节点的整体特征,从而证明了特征工程能够有效提升预测的准确率。Zhao等^[18]通过图卷积网络(Graph Convolutional Network,GCN)提出了端到端的深度学习框架,巧妙地融合了结构特征与深度学习的表示学习能力,但该方法依赖于大量的SIR模拟来生成标签,在大规模网络中较为耗时。Kumar等^[19]为了更好地捕捉网络的细节特征和降低分析复杂度,利用struc2vec技术将节点嵌入到低维向量,再通过SGNN(Shortest Path Graph Neural Network)模型来对节点进行分类。随着图注意力网络的出现,Park等^[20]利用注意力机制来区分不同的语义连接,并将中心性指标作为调节因子,形成了由评分网络和分数聚合层组成的图神经网络(Graph Neural Net-

works,GNN)新框架,解决了知识图谱(Knowledge Graph,KG)中重要实体挖掘难题,显著提升了评估精度。针对KG的多源异构特性,Ge等^[21]将KG中的关系属性转换为节点的交互强度,利用BERT来捕捉节点的语义属性,通过自注意力机制动态融合并输出节点的最终重要性分数。该方法解决了以往模型无法动态适应KG的结构差异问题。但该模型更大的计算开销也限制了其在大规模KG上的应用。同时由于依赖较大规模的标注训练数据支持,这在某些特定领域中存在一定难度。在通信网络领域,基于GNN的方法已被用于5G网络切片中的关键节点识别^[22]、软件定义网络中控制平面的关键控制器定位^[23],以及融合拓扑与流量特征的通信网络关键网元评估^[24]。这类方法的优势在于能够自动学习高阶结构特征,但可解释性不足限制了其在需要明确因果关系的网络运维场景中的应用。

表3为不同的节点重要性排序方法在标准数据集上的性能对比。可以看出,机器学习方法在精度上普遍优于传统中心性方法,但计算开销显著增加;而改进的传统方法在精度与效率之间取得了较好的平衡。

表3 节点重要性排序方法效果对比

方法	数据集特点	Kendall's tau	计算复杂度	适用的网络规模
度中心性	BA无标度网络	0.62	$O(N)$	大规模
介数中心性	BA无标度网络	0.78	$O(N^3)$	中小规模
K-shell方法	BA无标度网络	0.71	$O(N)$	大规模
VoteRank改进 ^[12]	真实社交网络	0.85	$O(N \cdot \log_2 N)$	中大规模
GCN ^[18]	合成网络+真实网络	0.91	$O(N \cdot E)$	中小规模
GNN+注意力 ^[20]	知识图谱	0.89	$O(N^2)$	中小规模

2.2 网络瓦解

网络瓦解的研究重点是在一定的约束条件下寻找最小规模的网络节点集合,本质上属于组合优化问题。

相关研究可追溯至20世纪60年代的数学规

划模型。随着网络规模的不断扩大,逐渐出现了以瓦解效果为优化目标的启发式方法,并朝着更智能、更高效的强化学习方法快速发展。本文将相关研究分为基于启发式的方法和基于深度学习的方法,两者的特点比较如表4所示。

表4 网络瓦解方法分类对比

方法分类	特点	优点	缺点	通信网络应用场景
启发式方法	利用贪心策略、禁忌搜索等启发式算法来高效地逼近最优解	准确度高;可解释性较强	难以捕捉高阶非线性的结构特征;有一定的复杂度;大规模网络中不适用	关键链路集识别、网络阻断策略优化
深度学习	神经网络学习结构特征和节点;强化学习优化节点移除策略;训练生成智能体进行目标判别	准确度高;智能体计算复杂度低;应用灵活	可解释性较弱;训练时复杂度高;对训练数据依赖性强	大规模网络实时瓦解、动态网络自适应攻击

2.2.1 基于启发式的方法

直接从传统的重要性排序结果中选取Top-k

的节点来作为解集的方法,虽然操作简单但效果却并不理想。因为网络瓦解是动态过程,每次删

除节点之后的网络结构将发生巨大变化,而基于传统中心性的排序结果也必将随之而改变。针对这一问题,研究者提出了基于贪心策略的启发式方法来动态求取关键节点集。Arulselvan 等^[25]提出了基于最大独立集的启发式算法,克服了传统方法在稀疏图中的局限性,不仅能够识别真正的瓶颈节点,而且还具有较高的计算效率,为后续的研究奠定了基础。Ren 等^[26]提出了反向贪心策略算法,从空网络开始反向构建诱导子图,依次选择对当前 GCC 影响最小的节点并加入网络,然后利用代价函数来衡量剩余节点的重要度。Addis 等^[27]提出了交替添加和删除节点的混合贪心策略,从而提升了搜索效率和解的质量。基于贪心策略的方法在每一步操作的基础上进行优化计算,所以存在易陷入局部最优解的问题。针对这一问题,Deng 等^[28]提出了基于禁忌搜索的启发式算法,通过交换节点状态来生成邻域解,并将最优交换组合记录在用于控制搜索范围的禁忌表中,然后通过回溯来跳出局部最优陷阱。实验表明,该算法能够有效防止陷入局部最优,在有限次迭代之后逼近甚至找到全局最优解。此后,该方法先后被扩展并应用于有向网络和多层网络。得益于较高的搜索效率和灵活的初始解生成机制,禁忌搜索算法已在多种场景中得到应用。除此之外,模拟退火算法、遗传算法和人工蜂群算法等启发式方法,也被用来研究和解决网络瓦解问题,但由于存在效率不高、适应性差及其他方面的问题而未能得到进一步的应用推广。启发式网络瓦解方法在通信网络中常被用于识别互联网骨干网的最小切断集^[29]、军事通信网络的关键中继节点集,以及光纤通信网络中的关键链路集^[30]等。这些方法通常以 GCC 大小或网络效率作为瓦解效果的评价指标,通过迭代移除节点直至网络性能降至既定阈值以下。

2.2.2 基于深度学习的方法

深度学习是近年来的研究热点,此类方法通过数据驱动来实现对大规模网络更精准和自适应的拆解,相关方法从监督学习到强化学习(Reinforcement Learning, RL)多种多样。Fan 等^[31]率先将 RL 应用于网络瓦解任务并提出了 FINDER 算法。该算法定义了深度 Q 网络(Deep Q-Network, DQN)和奖励函数的 RL 策略。DQN 通过移除节点后的收益 Q 值来学习最优的节点移除策略,奖励函数则不仅考虑当前移除操作的收益,还通过结构化奖励引导模型来学习网络最大化分解等长远目标。该算法利用已有的网络瓦解最优解进行离线训练,生成智能体后迁移应用。

实验表明,该算法能够更快地拆解网络,同时智能体对节点的筛选过程使得模型具有一定的可解释性。Grassia 等^[32]提出了几何深度学习的新框架(GDM),通过卷积网络提取节点特征,利用回归模型预测节点属于最优解的概率,在节点移除过程中持续评估网络的连通性来调整预测结果。此后,他们又进一步将该方法与经典的去环算法相结合(CoreGDM)^[33],通过学习可微分的评分函数来提升瓦解效率。Guo 等^[34]利用 GNN 来编码多层网络中层内节点在层间耦合的复杂关系,通过 DQN 决策来提升算法的动态适应性。该方法不仅在理论上表现优异,在交通、通信网络等实际网络中也验证了有效性。Gu 等^[35]针对更具实际意义的电网断路、通信网链路切断等边攻击方式,提出一种线图转换与深度强化学习结合的方法,并利用 GNN 进行高效的攻击序列挖掘。Pu 等^[36]提出了 SmartCore 算法,引入 k -core 累积大小来作为评估拆解效果的新指标,结合强化学习与图神经网络,在合成和真实数据集上均表现出优于现有方法的准确性和速度。网络瓦解相关的各类方法对比如表 5 所示。

表 5 网络瓦解各类方法效果对比

方法	核心策略	瓦解效果	计算复杂度	可扩展性	可解释性	典型应用场景
度排序移除	依度数降序移除	弱	低	百万级节点	强	快速筛选、高实时性场合
自适应度移除	动态重新计算度数移除	较弱	较高	十万级节点	强	网络快速瓦解评估
介数移除	依介数降序移除	较弱	高	千级节点	强	中小规模网络的精确瓦解分析
贪心策略 ^[26]	移除使 GCC 下降最多的节点	较强	较高	万级节点	较强	局部最优瓦解、基准方法对比
禁忌搜索 ^[28]	禁忌表机制+回溯搜索	较强	较高	万级节点	较强	中等规模网络的最优瓦解逼近
FINDER ^[31]	深度 Q 网络学习节点移除策略	强	高	万级节点	弱	同类型网络的批量瓦解
GDM ^[32]	几何深度学习预测节点	强	高	百万级节点	弱	社交网络等现实网络瓦解
CoreGDM ^[33]	CoreHD 与几何深度学习融合评分	强	高	十万级节点	较弱	精准瓦解与可扩展性平衡
SmartCore ^[36]	基于 k -core 的深度强化学习	强	高	十万级节点	较弱	精准瓦解与核心结构破坏

通过梳理不难看出,此类方法在利用深度学习提取网络的结构特征、利用强化学习优化节点移除策略等方面都有比较深入的研究,且在通信网络的现实应用中,能够处理百万级节点的互联网拓扑和拓扑随时间变化的移动自组网网络。但由于该方法的“黑箱”特性,节点优先被移除的原因往往难以充分解释,在需要确切的决策依据的场合中,如关键基础设施保护等,难以广泛应用。

2.3 级联失效

基于级联失效的复杂网络脆弱性研究,进一步引入网络动力学,关注局部扰动故障如何在网

络中传播,以及对网络的影响程度。在通信网络中,级联失效是最具破坏性的情况之一。如核心路由器的过载可能引发路由振荡,进而导致全网的数据拥塞;骨干链路的中断可能触发流量重分配,从而使备用链路相继过载瘫痪。通常假设网络节点之间存在负载、流量或者功能依赖关系,节点失效将影响相邻节点的状态变化,从而引发大面积的网络崩溃。此时的脆弱性体现为网络对微小扰动的放大能力及系统性崩溃倾向,是通信网络中最具破坏性的一类失效模式。根据级联失效机理的建模方式不同,大致可分为过载级联和耦合级联。两者比较如表6所示。

表6 级联失效方法分类对比

方法分类	特点	优点	缺点	通信网络应用场景
过载级联	节点因负载超过其容量上限而失效,通过负载重分配触发级联失效,常用在单层复杂网络中	物理含义直观,易解释;计算复杂度相对可控;易在现实网络中应用	忽略了跨系统的依赖关系;对参数设定敏感	路由器拥塞扩散、链路带宽超限
耦合级联	某一层网络内节点的失效通过依赖关系传导至其他层,在跨层反馈作用下引发的级联崩溃,常见于多层网络	能够捕捉更丰富系统性脆弱性;更贴近现实网络特征	模型复杂、参数量大;依赖关系难以获取;现实应用性相对较弱	电力与通信相依网络、5G控制与用户层面关联分析
流量级联	基于网络流的重分配机制,导致新路径上的节点过载失效	对应通信网络流量工程,物理意义明确	流量矩阵难以准确获取;重分配规则简化实际路由协议	互联网流量重分配、数据中心流量分析
高阶级联	考虑超边等高阶交互关系,节点失效通过高阶结构传播	能够描述群体交互效应,适用新型网络	模型复杂度高;高阶结构数据获取困难	组播网络、网络功能虚拟链

2.3.1 过载级联

过载级联模型起源于通信与电力的耦合网络运行机制的研究。Mottet^[37]构建了经典的负载容量(L-C)模型,定义了负载、容量和容量冗余系数 α 。

模型假设网络流量总是按最短路径传输,所以负载和容量均与节点的介数成正比。当扰动导致该节点失效后,重新计算其他节点的最短路径,并重新分配流量负载。若新负载超过某些节点的容量时,将导致新的节点失效。如此循环,直至达到新的平衡或网络崩溃。该研究指出,冗余系数 α 与是否产生级联失效和失效规模有着密切的联系。当 α 低于阈值 α_c 时,网络极易陷入大规模拥塞。此后的研究围绕负载和容量的具体含义,以及负载重分配策略进行了改进。当模型扩展至加权网络时,定义边权重为两端节点的度数乘积,节点负载为相连的所有边权重之和。考虑网络的功能效率时,可以将网络效率作为评估指标,而且网络的功能退化要比连通性下降更早出现。Qi等^[38]引入了非线性调控参数,定义了结构感知的容量

配置方式,能够在有限的资源下显著降低网络的脆弱性。张家瑞等^[39]在多层相依网络中应用L-C模型,根据节点的层内度、耦合度和层级设置初始负载,设计了判断节点状态的负载延迟重分配策略。Chen等^[40]针对多层网络设计了基于节点总度、层内度和层间度的节点移除策略,分析了耦合系数、调节参数对网络脆弱性的影响。irsoy等^[41]提出包含多类型流量的多重流模型,通过层内独立过载和层间影响过载两种故障方案,分别计算稳态下存活节点的比例。

在结合现实网络应用方面,Carreras等^[42]研究明确了由输电线路容量和发电能力两个因素限制下的级联失效临界值。Sun等^[43]针对北京市轨道交通网络数据,对客流过载与重分配进行研究。在通信网络领域,过载级联模型被用于分析互联网路由器在DDoS攻击下的拥塞扩散^[44]、数据中心网络在热点流量下的级联拥塞、以及无线传感器网络在能量耗尽后的级联失效^[45]等。

2.3.2 耦合级联

复杂系统研究中普遍认为,微观和介观层面存在着相互依赖关系。多层网络能够表达各层的属性和相互关系,为研究故障通过依赖关系传播提供了支撑。Buldyrev等^[46]基于渗流模型构建了典型的二部图模型,用于描述双层互依网络的级联失效脆弱性。其节点级联失效情形如图2所示。

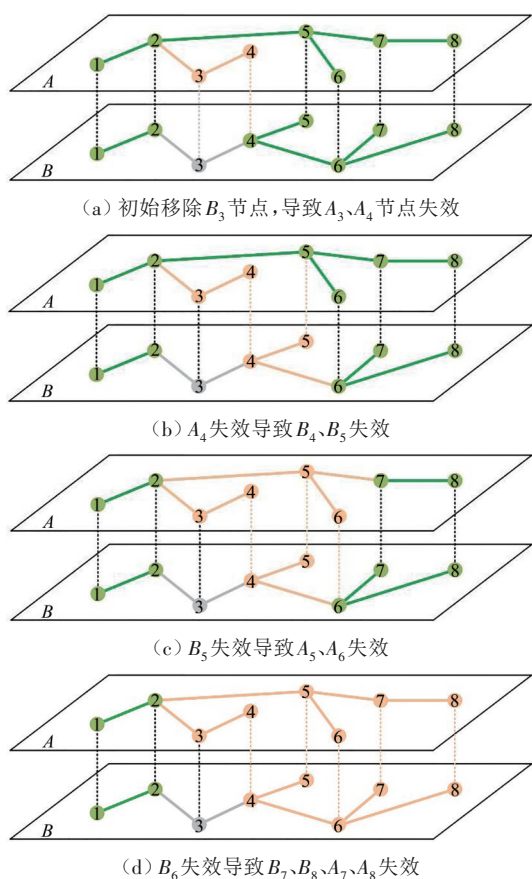


图2 耦合级联失效示意图

后续研究围绕耦合结构、依赖比例等展开。Parshani等^[47]提出部分依赖模型,即层内仅有部分节点与其他层节点存在一对一的有向依赖关系。研究指出,降低耦合节点比例时,级联失效的强度和规模将明显变弱。Dong等^[48]研究了多对多相依网络,发现耦合边密度增加时,反而能降低网络的脆弱性。Zhang等^[49]研究了非对称依赖网络,发现各层网络的相变现象并不相同。针对节点耦合在度相关性和聚类系数方面表现的关系特性,部分研究发现依赖节点具有较强的相似性时,网络的脆弱性更低。当一个节点的失效导致依赖它的节点完全失效时,称为它们之间为强耦合。但现实世界中更常见的是依赖节点的部分功能受损,称之为弱耦合机制。Liu等^[50]将弱耦合机制建模为有

一定概率断开连边,从而发现依赖失效和结构失效将交替作用。进一步的研究表明,多层弱依赖网络中,网络层的超级度越大,其渗流阈值也越大,相对应的就越脆弱。Li等^[51]研究了失效概率与依赖关系的非线性级联失效模型,发现优化层间分配比可以显著增强网络在低负载攻击下的鲁棒性。

在通信网络中,耦合级联模型被广泛用于分析电力通信相依网络的级联失效^[52]、5G控制层面与用户面功能的耦合失效^[53],以及SDN控制平面与数据平面的依赖失效^[54]。这些研究表明,通信网络的多层依赖性显著增加了系统的脆弱性,层间耦合强度与失效传播速度表现出明显的正相关性。

2.3.3 流量级联

流量级联模型针对通信网络中的数据流重分配机制进行研究。与过载级联关注节点的负载容量不同,流量级联更关注通信的链路容量和路径的选择策略。当网络中的某条链路失效后,受影响的业务流将按照预设的路由算法,如OSPF的最短路径优先、BGP的路径向量等,重新寻找传输路径。若重分配后的流量使某些链路的利用率超过其设计阈值,则可能引发新一轮的失效。Zhang等^[55]提出了基于边流量分配的级联失效模型,将流量按介数比例在剩余边上重分配,发现无标度网络中的高介数边的失效更容易引发大规模级联失效。Wu等^[56]研究了互联网AS级拓扑中的流量级联,指出少数高带宽链路的失效可能导致全网的吞吐量下降超过40%。在数据中心网络中,Pei等^[57]研究了等价多路径路由的内部通信流量均衡策略,发现在多链路相继失效时可能引发流量极化现象,即流量没有均匀地分配到所有可用的等价路径上,而是出现明显的偏向性,从而导致部分链路过载而严重拥塞。

2.3.4 高阶级联

高阶级联模型主要考虑网络中的高阶交互关系,即多个节点通过超边或单纯复形而出现的群体交互效应。通信网络中的高阶结构体现在组播组中的多接收者关系、网络功能虚拟化(NFV)中的服务链多节点依赖关系,以及多输入多输出通信中的多天线协同关系等。Jia等^[58]利用超图来建模多层高阶网络,研究了层间高阶依赖关系下的级联失效,发现高阶依赖显著降低了网络的渗流阈值。Qian等^[59]提出了多层高阶网络中级联失效的分析框架,通过递归方法分析了相变临界阈值和

GCC 规模的大小。Zheng 等^[60]研究了高阶网络中的 k -core 渗流,发现当 $k \geq 3$ 时,网络在相变临界点附近仅存在不连续相变。文献[61]利用高阶级联模型针对 NFV 服务链中虚拟网络功能(VNF)实例进行级联失效分析,发现当某个 VNF 实例失效后,依赖于该实例的服务链需要重新编排,并可能引发其他 VNF 过载而失效。

综上所述,过载级联关注节点容量约束与负载重分配机制,是通信网络拥塞控制研究的经典方法;耦合级联描述了多层网络中层间依赖导致的故障跨层传播现象,能够反映通信系统中控制层面与用户层面分离的架构脆弱性;流量级联则从路由协议层面反映了协议设计与实现对通信系统的影响;高阶级联则通过超图和单纯复形来表达群体依赖效应。4 类方法从不同的层面构成了通信网络级联失效分析的方法体系,为系统分析通信网络的脆弱性提供了有力支撑。表 7 汇总了部分级联失效模型在节点数为 1 000、平均度为 4 的 BA 无标度网络数据集上的表现对比。

表 7 部分级联失效模型表现对比				
模型方法	负载 阈值 α_c	级联 规模 $F_{\max}$	相变类型	通信网络 适用性
L-C 模型	0.25	0.85	混合相变	高
加权 L-C 模型	0.30	0.78	二阶相变	高
多层 L-C 模型	0.35	0.92	一阶相变	中
弱依赖	0.28	0.72	混合相变	中
流量级联 ^[55]	0.22	0.80	二阶相变	高
高阶级联 ^[58]	0.18	0.88	一阶相变	低

3 问题与挑战

尽管利用关键节点来评估网络脆弱性的研究已取得了显著成果,但结合通信网络的特征,当前研究仍面临一系列亟待解决的关键挑战。

3.1 模型抽象与工程现实之间的差距

复杂网络理论的核心优势在于,通过高度抽象的网络模型揭示系统层面的共性规律,但这种抽象不可避免地与实际通信网络的工程细节之间存在差距。过度简化的拓扑模型增加了理论分析的便利性,但却难以准确反映工程指标约束和节点异质性要素;过于精细的建模又会导致分析复杂度的急剧上升,难以在大规模网络中应用。如何平衡模型复杂度与现实准确性需求是需要未来持续探索的问题。目前已初具规模的层次化与语义增强建模给出了相对明确的方向。既在宏观层

面保留统计特性与拓扑结构,又在微观层面引入工程约束与属性语义,从而实现不同分析目标之间的灵活变换。

3.2 扰动模式的动态适应性不足

当前脆弱性分析仍依赖于理想化的蓄意攻击模式,比如已知拓扑结构下的最优瓦解、具备全局观测能力的强化学习策略。这在研究网络脆弱性在理论上的极限情况时具有重要价值,但在实际应用场景中并不一定具有可行性。一是无法完全掌握网络信息。在基于贪婪策略的启发式网络瓦解中,局部最优要明显差于全局最优的瓦解效果。二是网络拓扑随时间动态变化。Maurer 等^[62]对动态通信网络进行了研究,发现在高峰时段的脆弱性明显低于低谷时段,因为高峰时段的网络拓扑更为密集,从而提供了更多的冗余路径。三是攻防博弈对抗改变了传播环境。文献[63]研究了攻防博弈下的网络脆弱性,指出纳什均衡状态下的网络脆弱性明显低于静态时的分析结果。如何构建既具有分析价值、又能贴近现实能力的扰动模式是一个值得深入研究的问题。未来可结合不完全信息、攻击成本、时序约束以及防御反馈机制等,使攻击模式从最坏情形分析向探索型风险评估转变,从而更好地服务实际的网络安全决策。

3.3 结构破坏与功能退化之间的量化映射困难

尽管结构脆弱性分析已形成了成熟的理论框架,但如何将其结果有效地映射为实际的功能退化仍是一个尚未完全解决的问题。GCC 的瓦解并不意味着服务完全不可用。而即使拓扑仍保持连通,关键服务也可能已严重受损。这表明结构指标与功能指标之间并不存在固定不变的量化映射关系。有研究表明,在随机故障模式下,GCC 大小与网络效率的相关系数约为 0.85~0.95。而在蓄意攻击时,该数值则下降至 0.60~0.75,因为虽然网络结构严重碎片化,但剩余节点仍可通过局部聚类来维持一定的功能。未来亟需研究结构变化如何通过路由、流量和控制机制等,量化映射为功能退化结果。这不仅有助于提升脆弱性分析结果的可解释性,也有助于复杂网络理论在更多领域更好地应用。总体而言,复杂网络理论为理解与分析通信网络脆弱性提供了强有力的分析工具,但进一步发展仍依赖于上述挑战的持续探索。通过在理论抽象、攻击建模、跨层映射方面建立更紧密的联系,未来将在保持理论研究深度的同时,显著提升对现实应用的解释力和指导意义。

参考文献:

- [1] Kotha N R. Analyzing the 2024 CrowdStrike outage: implications for SaaS-dependent cybersecurity architectures [J]. *International Journal for Research in Applied Science and Engineering Technology*, 2024, 12(11): 2156-2161.
- [2] 郭程远,陈鸿昶,王庚润,等.复杂网络节点重要性排序算法及应用综述[J].*信息工程大学学报*, 2021, 22(3): 313-320.
- [3] 吴俊,邓烨,王志刚,等.复杂网络瓦解问题研究进展与展望[J].*复杂系统与复杂性科学*, 2022, 19(3): 1-13.
- [4] 赵彪,王梦麟,张其增.级联失效指挥控制网络抗毁性研究[J].*信息工程大学学报*, 2024, 25(5): 601-607.
- [5] 郭昊明,汪霜玲,燕雪峰,等.基于复杂网络的军事通信网络建模与脆弱性分析[J].*西北工业大学学报*, 2024, 42(6): 1126-1134.
- [6] Ma Y, Cao Z L, Qi X Q. Quasi-Laplacian centrality: a new vertex centrality measurement based on Quasi-Laplacian energy of networks [J]. *Physica A: Statistical Mechanics and Its Applications*, 2019, 527: 121130.
- [7] Zhu X Y, Hao R X. Identifying influential nodes in social networks via improved Laplacian centrality [J]. *Chaos, Solitons & Fractals*, 2024, 189: 115675.
- [8] Salavati C, Abdollahpouri A, Manbari Z. Ranking nodes in complex networks based on local structure and improving closeness centrality [J]. *Neurocomputing*, 2019, 336: 36-45.
- [9] Ma J L, Kong L K, Li H J. An effective edge-adding strategy for enhancing network traffic capacity [J]. *Physica A: Statistical Mechanics and Its Applications*, 2023, 609: 12 8321.
- [10] Ai J, He T, Su Z. Identifying influential nodes in complex networks based on resource allocation similarity [J]. *Physica A: Statistical Mechanics and Its Applications*, 2023, 627: 129101.
- [11] Kumar S, Panda B S. Identifying influential nodes in social networks: neighborhood coreness based voting approach [J]. *Physica A: Statistical Mechanics and Its Applications*, 2020, 553: 124215.
- [12] Li Y X, Yang X Z, Zhang X W, et al. An improved voter-ank algorithm to identifying a set of influential spreaders in complex networks [J]. *Frontiers in Physics*, 2022, 10: 95527.
- [13] Dong C, Xu G Q, Meng L, et al. CPR-TOPSIS: a novel algorithm for finding influential nodes in complex networks based on communication probability and relative entropy [J]. *Physica A: Statistical Mechanics and its Applications*, 2022, 603: 127797.
- [14] Wang X, Du J, Zou R C, et al. Key node identification of wireless sensor networks based on cascade failure [J]. *Modern Physics Letters B*, 2020, 34(34): 2050394.
- [15] 张诗琪,李琰,徐天奇.基于信息熵的电力信息耦合网络重要节点评估[J].*科学技术与工程*, 2022, 22(17): 7042-7049.
- [16] Zhao G H, Jia P, Huang C, et al. A machine learning based framework for identifying influential nodes in complex networks [J]. *IEEE Access*, 2020, 8: 65462-65471.
- [17] Asgharian Rezaei A, Munoz J, Jalili M, et al. A machine learning-based approach for vital node identification in complex networks [J]. *Expert Systems with Applications*, 2023, 214: 119086.
- [18] Zhao G H, Jia P, Zhou A M, et al. InfGCN: identifying influential nodes in complex networks with graph convolutional networks [J]. *Neurocomputing*, 2020, 414: 18-26.
- [19] Kumar S, Mallik A, Khetarpal A, et al. Influence maximization in social networks using graph embedding and graph neural network [J]. *Information Sciences*, 2022, 607: 1617-1636.
- [20] Park N, Kan A, Dong X L, et al. Estimating node importance in knowledge graphs using graph neural networks [C]//*Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*. New York, USA: ACM, 2019: 596-606.
- [21] Ge K, Han Q B. Node importance estimation for knowledge graphs based on multi-perspectives attention fusion mechanism [J]. *International Journal of Pattern Recognition and Artificial Intelligence*, 2024, 38(14): 2459017.
- [22] Boroujeni T S, Osgouei A G. Analytical performance model for sliced 5G core network [C]//*proceedings of the 2024 11th international symposium on telecommunications*. Piscataway, USA: IEEE, 2024: 101-103.
- [23] Jacob J, Shinde S, Narayan D G. An efficient controller placement algorithm using clustering in software defined networks [J]. *Journal of Telecommunications and Information Technology*, 2023, 4(2023): 9-17.
- [24] Meng B, Rezaeipanah A. Development of a multidimensional centrality metric for ranking nodes in complex networks [J]. *Chaos, Solitons & Fractals*, 2025, 191: 11 5843.
- [25] Arulselvan A, Commander C W, Elefteridou L, et al. Detecting critical nodes in sparse graphs [J]. *Computers & Operations Research*, 2009, 36(7): 2193-2200.
- [26] Ren T, Li Z, Qi Y, et al. Identifying vital nodes based on reverse greedy method [J]. *Scientific Reports*, 2020, 10: 4826.
- [27] Addis B, Aringhieri R, Grosso A, et al. Hybrid constructive heuristics for the critical node problem [J]. *Annals of Operations Research*, 2016, 238, 637-649.
- [28] DENG Y, WU J, TAN Y. Optimal attack strategy of complex networks based on tabu search [J]. *Physica A: Statis-*

- tical Mechanics and its Applications, 2016, 442: 274-281.
- [29] Herrera M, Pérez-Hernández M, Jain A K, et al. Critical link analysis of a national Internet backbone via dynamic perturbation [J]. IFAC-PapersOnLine, 2020, 53 (3): 155-160.
- [30] Qu B B, Wang H F, Gao H S, et al. Optimization of backbone optical network for power communication based on critical link [J]. Journal of Physics: Conference Series, 2021, 2030(1): 012032.
- [31] Fan C J, Zeng L, Sun Y Z, et al. Finding key players in complex networks through deep reinforcement learning [J]. Nature Machine Intelligence, 2020, 2(6): 317-324.
- [32] Grassia M, De Domenico M, Mangioni G. Machine learning dismantling and early-warning signals of disintegration in complex systems [J]. Nature Communications, 2021, 12: 5190.
- [33] Grassia M, Mangioni G. CoreGDM: geometric deep learning network decycling and Dismantling [C]//Complex networks XIV. Cham, Switzerland: Springer, 2023: 86-94.
- [34] Guo F W, Chen C, Zeng L, et al. Finding key edges in complex network through line graph transformation and deep reinforcement learning [J]. Expert Systems with Applications, 2025, 289: 128121.
- [35] Gu W W, Yang C, Li L, et al. Deep-learning-aided dismantling of interdependent networks [J]. Nature Machine Intelligence, 2025, 7(8): 1266-1277.
- [36] Pu T L, Zeng L, Chen C. Deep reinforcement learning for network dismantling: a k -core based approach [J]. Mathematics, 2024, 12(8): 1215.
- [37] Motter A E, Lai Y C. Cascade-based attacks on complex networks [J]. Physical Review E, 2003, 66 (6Pt2): 065102.
- [38] Qi X G, Yang G Z, Liu L F. Robustness analysis of the networks in cascading failures with controllable parameters [J]. Physica A: Statistical Mechanics and Its Applications, 2020, 539: 122870.
- [39] 张家瑞, 黄健, 高家隆. 负载目标下基于延迟分配的多层级相依网络级联失效模型 [J]. 国防科技大学学报, 2024, 46(5): 79-89.
- [40] Chen M J, Wang N, Wei D J. Study on Cascading Failures Based on Intra-Layer and Inter-Layer Structures of Multi-player Networks [J]. 数学理论与应用, 2025, 45 (3): 107-124.
- [41] İrsoy O, Yağan O. Analysis and optimization of robustness in multiplex flow networks against cascading failures [J]. IEEE Transactions on Network Science and Engineering, 2026, 13: 1705-1722.
- [42] Carreras B A, Lynch V E, Dobsoni, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts [J]. Chaos, 2002, 12(4): 985-994.
- [43] Sun L S, Huang Y C, Chen Y Y, et al. Vulnerability assessment of urban rail transit based on multi-static weighted method in Beijing, China [J]. Transportation Research Part A: Policy and Practice, 2018, 108: 12-24.
- [44] Xu X H, Huang A L, Shalaby A, et al. Exploring cascading failure processes of interdependent multi-modal public transit networks [J]. Physica A: Statistical Mechanics and Its Applications, 2024, 638.
- [45] Liu S, Yin C S, Chen D J, et al. Modelling and impact analysis of interdependent characteristics on cascading overload failure of syncretic railway networks [J]. PLoS One, 2020, 15(9): e0239096.
- [46] Buldyrev S V, Shere N W, Cwiltch G A. Interdependent networks with identical degrees of mutually dependent nodes [J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2011, 83(1 Pt 2): 016112.
- [47] Parshani R, Rozenblat C, Iettri D, et al. Inter-similarity between coupled networks [J]. Europhysics Letters, 2010, 92.
- [48] Dong G G, Chen Y, Wang F, et al. Robustness on interdependent networks with a multiple-to-multiple dependent relationship [J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019, 29(7): 073107.
- [49] Zhang H, Zhou J, Zou Y, et al. Asymmetric interdependent networks with multiple-dependence relation [J]. Physical Review E, 2020(2): 22314.
- [50] Liu R R, Li M, Jia C X. Cascading failures in coupled networks: the critical role of node-coupling strength acts networks [J]. Scientific Reports, 2016, 6: 35352.
- [51] Li M J, Yang L X, Zhang Y Q, et al. Analysis of cascading failure in interdependent networks concerning failure probability and dependent relationship [J]. Physica A: Statistical Mechanics and its Applications, 2025, 674: 130732.
- [52] Wang J, Huang Y H. An edge load cascading failure model and vulnerability analysis of coupled critical infrastructure networks: considering functional and geographical interdependency [J]. Reliability Engineering & System Safety, 2026, 266: 111719.
- [53] Chen B, Wu J J, Chen Y Y, et al. Cascading failures in interdependent transportation networks: a generalized coupled map lattice model with intermodal dynamics [J]. Physica A: Statistical Mechanics and Its Applications, 2025, 675: 130836.
- [54] Gao Y L, Liang C S, Zhou J, et al. Robustness optimization of aviation-high-speed rail coupling network [J]. Physica A: Statistical Mechanics and Its Applications, 2023, 610: 128406.