

基于模体的高低阶网络结构鲁棒性

邢之尧¹, 项林英^{2*}

(1. 天津工业大学电子与信息工程学院, 天津 300387; 2. 天津工业大学人工智能学院, 天津 300387)

摘要: 现实中的多智能体网络系统普遍处于攻击与防御相互博弈的动态环境之中. 攻击方通过破坏关键节点或交互结构削弱系统功能, 而防御方则采取相应的修复与重构策略以维持系统整体性能, 二者交替作用, 形成复杂且高度非线性的对抗演化过程. 此类多智能体系统通常可抽象为复杂网络模型, 其中节点表示智能体, 边刻画其相互作用关系. 基于传统图结构的建模方法在描述节点之间的二元交互关系方面具有较强优势, 已被广泛用于网络鲁棒性分析与攻防博弈研究. 然而, 该类方法在刻画多智能体之间普遍存在的多元协同、群体交互以及高阶耦合行为时仍存在一定局限, 难以全面反映现实系统中复杂的协作机制. 近年来, 随着复杂系统研究的不断深入, 高阶网络建模方法逐渐受到关注, 并被引入多智能体系统分析框架中. 相较于传统低阶网络, 高阶网络为研究多智能体系统中复杂协同行为的形成机制与演化规律提供了更加丰富的结构表征手段. 在此背景下, 本文从复杂网络低阶结构出发, 引入高阶网络建模框架, 系统研究多智能体网络在攻防博弈条件下的结构鲁棒性演化问题. 首先, 围绕多智能体系统可能面临的攻击与防御场景, 构建多种典型的攻击与防御策略, 并在此基础上分析不同策略组合对高阶网络结构鲁棒性的影响. 重点考察在不同攻击模式和防御机制下, 高阶网络与对应低阶网络在鲁棒性演化过程中的差异特征, 以及高阶结构在提升或削弱系统抗攻击能力中的作用机理. 具体而言, 本文从模体结构出发, 深入分析高阶网络中不同类型模体对系统整体鲁棒性的影响机制, 并进一步探讨低阶网络平均度等结构参数对高阶网络鲁棒性的调节作用. 研究采用数值仿真与理论分析相结合的方法, 选取四类典型低阶网络模型, 构建其对应的高阶网络结构. 在此基础上, 引入四种具有代表性的攻击策略, 对智能体节点的失效过程进行模拟, 系统刻画攻防交互过程中网络结构的动态演化特征. 通过计算网络最大连通分支的相对规模, 定量评估不同攻防策略下网络鲁棒性的变化规律. 结果表明, 与传统低阶网络相比, 高阶网络在面对攻击时呈现出显著不同的鲁棒性响应特征. 系统鲁棒性不仅依赖于节点之间的二元连接关系, 还受到高阶模体结构分布以及低阶网络平均度等因素的共同影响. 合理的模体组织形式和适当的低阶结构参数能够在一定程度上增强系统对攻击的抵抗能力. 本文的研究结论为揭示多智能体系统中多元协同行为的鲁棒性形成机制提供了新的理论视角, 同时也为高阶网络结构设计及攻防策略的优化提供了有价值的参考依据.

关键词: 高阶网络; 结构鲁棒性; 模体; 多智能体系统

基金项目: 国家自然科学基金(No.62473284)

中图分类号: TN94

文献标识码: A

文章编号: 0372-2112(2025)12-4592-15

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.12263/DZXB.20250683

Motif-Based Structural Robustness of Lower- and Higher-Order Networks

XING Zhi-yao¹, XIANG Lin-ying^{2*}

(1. School of Electronics and Information Engineering, Tiangong University, Tianjin 300387, China;

2. School of Artificial Intelligence, Tiangong University, Tianjin 300387, China)

Abstract: Real-world multi-agent networked systems are commonly embedded in dynamic environments characterized by the interplay between attacks and defenses. Attackers aim to degrade system functionality by disrupting critical nodes or interaction structures, whereas defenders adopt corresponding repair and reconfiguration strategies to preserve overall system performance. The alternating actions of these two sides give rise to complex and highly nonlinear adversarial evolutionary processes. Such multi-agent systems are typically abstracted as complex networks, where nodes represent individual agents and edges describe their interaction relationships. Traditional graph-based modeling approaches exhibit clear advantages in characterizing pairwise interactions between nodes and have been widely employed in studies of network robustness and attack-defense games. However, these approaches encounter inherent limitations when attempting to capture

the ubiquitous multi-agent coordination, group interactions, and higher-order coupling behaviors present in real-world systems, and thus fail to fully reflect the complexity of collective cooperation mechanisms. In recent years, with the rapid advancement of complex systems research, higher-order network modeling approaches have attracted increasing attention and have been incorporated into the analytical framework of multi-agent systems. Compared with conventional lower-order networks, higher-order networks provide richer structural representations for investigating the formation mechanisms and evolutionary dynamics of complex cooperative behaviors in multi-agent systems. In this context, this paper starts from lower-order network structures and introduces a higher-order network modeling framework to systematically investigate the structural robustness evolution of multi-agent networks under attack-defense games. Specifically, multiple representative attack and defense strategies are constructed to reflect realistic adversarial scenarios, and their combined effects on the structural robustness of higher-order network are systematically analyzed. Particular emphasis is placed on examining the differences in robustness evolution between higher-order networks and their corresponding lower-order counterparts under various attack modes and defense mechanisms, as well as on elucidating the role of higher-order structures in enhancing or weakening system resilience against attacks. More concretely, this study focuses on motif-based structures and conducts an in-depth analysis of how different types of motifs in higher-order networks influence overall system robustness. Furthermore, the moderating effects of lower-order structural parameters, such as the average degree of the underlying network, on higher-order network robustness are investigated. A combination of numerical simulations and theoretical analysis is employed. Four representative lower-order network models are selected to generate their corresponding higher-order network structures. On this basis, four typical attack strategies are introduced to simulate agent node failures, enabling a systematic characterization of the dynamic structural evolution of networks during attack-defense interactions. By computing the relative size of the largest connected component, the robustness variations of networks under different attack-defense strategies are quantitatively evaluated. The results demonstrate that, compared with traditional lower-order networks, higher-order networks exhibit distinctly different robustness response characteristics when subjected to attacks. System robustness depends not only on pairwise connections between nodes but is also significantly influenced by the distribution of higher-order motif structures and lower-order structural parameters such as the average degree. Appropriate motif organization and suitable lower-order structural configurations can, to some extent, enhance system resistance to attacks. The findings of this study provide a novel theoretical perspective for understanding the robustness formation mechanisms of multi-agent systems with complex cooperative behaviors and offer valuable insights for the design of higher-order network structures and the optimization of attack-defense strategies.

Key words: higher-order network; structural robustness; motif; multi-agent system

Foundation Item(s): National Natural Science Foundation of China (No.62473284)

1 引言

在现代社会背景下,多智能体系统的安全性与抗毁性已成为一个具有重要研究价值的课题.以互联网、电力网络和交通系统等关键基础设施为代表的复杂系统,常常面临各类故障和蓄意攻击的严峻挑战^[1-7].在复杂网络环境中,系统不仅要应对由随机故障或不确定扰动引起的性能退化,还需具备抵御恶意攻击所引发的级联失效能力.例如,在智能电网中,分布式能源节点之间的协同控制依赖多智能体系统所构成的通信拓扑结构.一旦关键节点遭受攻击导致信息交互中断,极有可能引发连锁反应,进而造成整个电网瘫痪等灾难性后果.因此,深入研究多智能体系统在面对攻击与故障时的结构鲁棒性,对于提升关键基础设施的安全保障水平具有重要的理论意义与实际价值.

多智能体网络系统风险的形成机制及其传播特性,已成为当前网络安全领域的核心研究方向之一. Albert 等人^[8]构建了一个选择性攻击的理论模型,通过

优先攻击网络中高度节点来破坏系统的整体连通性.大量已有研究从理论分析和数值模拟两个维度出发,系统性探讨了网络在面对单次随机故障或蓄意攻击时的稳定性特征^[9-16].例如, Schneider 等人^[11]基于渗流理论提出了用于评估节点攻击影响的鲁棒性指标; Zeng 等人^[13]在此基础上进一步扩展了该指标,以衡量边攻击情形下的链接鲁棒性.此外, Tanizawa 等人^[15]从网络拓扑结构出发,发现具有双峰度分布特征的网络在同时遭受蓄意节点攻击与随机节点扰动时,表现出更强的鲁棒性.这些研究为理解网络结构与抗毁能力之间的关系提供了坚实的理论基础.

然而,现实中的网络系统通常处于攻击与防御持续博弈的动态演化过程中,攻防双方通过交替实施破坏与修复行为,不断改变网络的结构状态. Nagaraja 等人^[17]基于进化博弈理论^[18]构建了一个重复攻防博弈的理论框架,其中攻击方以削弱网络连通性为目标,而防御方则致力于恢复网络功能并提升其结构鲁棒性.在

在此基础上, Kim 等人^[19]通过引入攻防操作的成本约束, 进一步扩展了该重复博弈模型, 并对三类典型的攻防策略进行了系统的实证分析. 该研究将攻防过程建模为一个迭代演化的动态系统: 在每一轮攻击阶段, 根据特定策略移除 n 个节点; 而在随后的防御阶段, 则依据相应的防御策略补充 n 个节点. 通过持续监测最大连通子图规模的变化, 研究评估了不同攻防策略在动态演化过程中的有效性, 为理解现实系统中攻防对抗的演化机制提供了理论支持与方法借鉴.

需要指出的是, 现有关于网络结构鲁棒性的研究主要集中于低阶网络模型^[8-19], 此类模型仅能刻画节点之间的二元交互关系. 在表征多节点间高阶交互所蕴含的复杂结构依赖性方面, 传统方法存在显著局限. 近年来, 随着高阶网络理论^[20,21]的不断发展, 围绕其结构鲁棒性的研究逐渐成为学术界关注的前沿方向^[22-24]. 例如, Zhao 等人^[25]构建了一个基于渗流理论的分析框架, 用于探讨有向高阶网络的鲁棒性特征; Ma 等人^[26]提出了容量-负载耦合模型, 实现了对高阶网络结构鲁棒性的定量评估; Zheng 等人^[27]则设计了一种基于优化理论的增强策略, 结合贪心算法与模拟退火算法, 有效提升了耦合高阶-低阶网络的结构鲁棒性. 这些研究成果为揭示高阶交互机制对系统鲁棒性的影响提供了重要理论支撑, 也为复杂系统的结构优化与防护策略设计提供了新的思路.

尽管多智能体网络系统的研究在低阶结构建模与高阶交互模式分析两个维度均取得了显著进展, 但二者之间的动态关联机制尚处于探索初期. Kim 等人^[19]提出的动态攻防博弈框架系统揭示了低阶网络在节点增减过程中鲁棒性的演化规律, 然而该模型尚未涉及高阶网络层面的结构演化与响应机制. 为此, 本文结合动态攻防策略, 系统分析了高低阶网络结构鲁棒性的级联演化过程, 重点探讨了以下两个关键问题: 一是, 不同模体拓扑结构在攻防动态演变中如何影响高阶网络的结构鲁棒性? 二是, 低阶网络的平均度对高阶网络鲁棒性演化机制有何影响? 相关研究不仅有助于深化对跨尺度网络鲁棒性形成机制的理论理解, 也为关键基础设施系统的网络韧性优化提供了新的研究视角与方法论支持.

本文主要贡献总结如下:

(1) 区别于已有关于静态或低阶网络模型的鲁棒性研究, 本文通过引入“模体”作为核心拓扑单元, 构建了动态攻防场景下的高阶网络分析框架. 研究发现, 模体 $M_8 \sim M_{13}$ 的拓扑结构对高阶网络鲁棒性提升作用显著优于 $M_1 \sim M_7$, 其中基于模体 M_9 构建的高阶网络, 其鲁棒性曲线与对应低阶网络变化趋势最为吻合, 拟合效果最优. 该发现将研究视角从静态属性深化为

对动态、群体性拓扑作用机制的理解.

(2) 不同于以往将高阶效应与底层网络宏观统计量(如平均度)分别讨论的做法, 本文系统揭示了低阶网络平均度作为关键控制参数对高阶鲁棒性的基础性调制作用. 研究发现, 当以模体 M_9 构建高阶网络时, 其鲁棒性数值趋近于 1, 显著优于其他拓扑构型; 同时, 当局域世界网络的平均度超过某一临界阈值后, 其高阶网络鲁棒性显著提升, 而 ER (Erdős-Rényi)、WS (Watts-Strogatz)、BA (Barabás-Albert) 等对比网络模型则未呈现类似单调趋势. 该结论阐明了网络生成机制与高阶鲁棒性动态之间未被充分揭示的耦合关系, 为设计与理解更具韧性的复杂系统提供了新的理论依据.

综上所述, 模体结构与网络平均度对高阶网络鲁棒性具有重要影响, 研究揭示了网络生成机制与鲁棒性动态之间的内在关联, 为高阶网络鲁棒性设计与优化提供了理论依据与技术支持.

2 预备知识

在多智能体网络系统研究中, 关键节点的识别及其对网络鲁棒性的影响是网络科学中的核心问题之一. 本章围绕该主题展开系统论述, 从网络结构特征、节点重要性评估到系统鲁棒性分析, 逐层深入探讨其理论基础与应用价值. 首先, 介绍模体 (Motif)—网络中的基本功能单元, 揭示局部连接模式如何影响整体的动力学行为; 其次, 基于高阶网络理论, 分析超越成对连接的多节点交互机制, 以更精细地刻画复杂系统的组织结构与多元协同特性; 然后, 讨论多种节点重要性评估指标, 比较不同方法在关键节点识别过程中的适用性与区分能力; 最后, 通过引入网络鲁棒性评估指标, 分析节点失效或遭受攻击时对整体网络性能的影响程度. 上述四部分内容从微观结构到宏观特性, 层层递进地展开, 为理解关键节点在网络稳定性中的作用提供了理论支撑, 并为提升多智能体网络系统的鲁棒性设计提供了方法参考.

2.1 模体

网络作为解析和调控复杂系统的重要工具, 可将系统中的大量组成单元抽象为节点, 将它们之间的交互关系抽象为边, 从而构建复杂网络模型进行系统性研究. 基于节点间连接关系构建的邻接矩阵可有效反映网络的低阶结构特征(如节点和边), 但现实中复杂系统内部常常存在涉及多个节点的高阶交互模式^[28,29]. 这类交互在局部网络中通常表现为特定的小规模子图结构. 其中, 模体是一种典型而有力的高阶结构表征工具. Milo 等人^[30]将模体定义为由有限数量节点构成的特定连接模式, 其在实际网络中出现的频率

显著高于对应随机重连网络的统计预期值. 为了进一步以矩阵形式量化网络中的高阶结构特征^[31,32], Benson 等人^[31]创新性地提出了模体邻接矩阵, 用于度量节点对在形成特定模体过程中共同参与的频次. 在多数实际网络中, 三节点模体广泛存在, 且具有显著的高频特

征. 这些模体不仅在拓扑上分布广泛, 更代表了网络高阶交互模式的基本构件和典型特征. 因此, 本文以三节点模体为研究基础, 深入探讨其在网络结构鲁棒性分析中的作用. 如图 1 所示, 本文研究的三节点模体共包括 $M_1 \sim M_{13}$ 在内的 13 种基本类型.

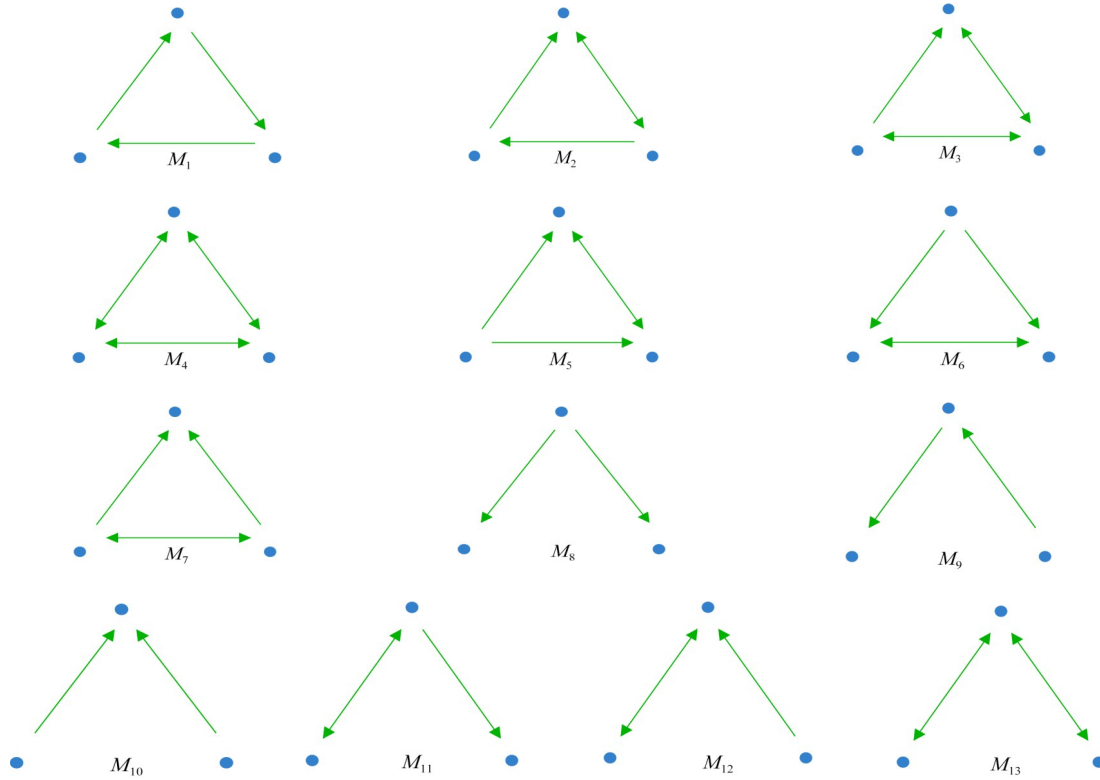


图 1 13 种模体拓扑结构

2.2 高阶网络理论

一个具有 N 个节点的高阶无向网络表示为 $G_{\text{high}} = (V, E, \mathbf{W}_M)$, 其中 $V = \{v_i | i = 1, 2, \dots, N\}$ 表示节点集, $E = \{(v_i, v_j)\}$ 表示边集, \mathbf{W}_M 是基于模体 M 的高阶邻接矩阵. 给定一个模体 M , 对于具有 N 个节点的低阶有向网络 G , 其基于 M 的高阶邻接矩阵可以定义为 $\mathbf{W}_M = \{w_{ij}\}_{N \times N}$, 矩阵元素 w_{ij} 为 G 中连边 e_{ij} 在模体 M 中出现的次数, 定义为

$$w_{ij} = \begin{cases} \sum 1, & e_{ij} \in M \text{ 且 } i \neq j \\ 0, & \text{其他} \end{cases} \quad (1)$$

其中, $e_{ij} = (v_i, v_j)$ 是一条由节点 v_i 指向节点 v_j 的连边.

基于模体的高阶网络生成过程如图 2 所示. 其中, 图 2(a) 是一个具有 6 个节点的低阶有向网络, 图 2(b) 是图 2(a) 基于模体 M_6 生成的高阶邻接矩阵, 图 2(c) 是基于图 2(b) 生成的高阶无向网络.

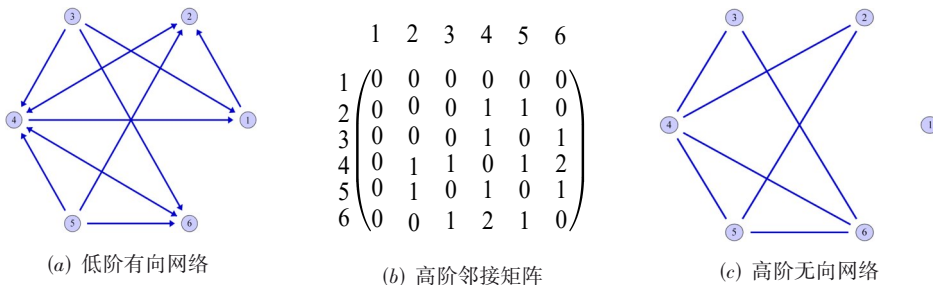


图 2 基于模体 M_6 生成的高阶网络

2.3 节点重要度评价指标

为刻画节点之间的局部结构相似性,阮逸润等人^[33]提出了一种结合节点度与邻域拓扑重合度的相似性评估方法.在此基础上,本文针对有向复杂网络,提出了一种新的邻域相似性重要度指标 LLS_{directed} ,以更准确地反映有向网络中节点间的结构相似关系.

首先给出节点 a 的邻域相似度定义.如果 b 和 c 是节点 a 的邻居节点,那么节点 a 的邻域相似度定义为

$$\text{Sim}_{\text{directed}}(b, c) = \begin{cases} \frac{|n_{\text{in}}(b) \cap n_{\text{in}}(c)| + |n_{\text{out}}(b) \cap n_{\text{out}}(c)|}{|n_{\text{in}}(b) \cup n_{\text{in}}(c)| + |n_{\text{out}}(b) \cup n_{\text{out}}(c)|} & (2) \\ 1 \end{cases}$$

其中,如果节点 b 和 c 之间没有双向边,则 $\text{Sim}_{\text{directed}}(b, c) = \frac{|n_{\text{in}}(b) \cap n_{\text{in}}(c)| + |n_{\text{out}}(b) \cap n_{\text{out}}(c)|}{|n_{\text{in}}(b) \cup n_{\text{in}}(c)| + |n_{\text{out}}(b) \cup n_{\text{out}}(c)|}$;若节点 b 和 c 之间有双向边,则 $\text{Sim}_{\text{directed}}(b, c) = 1$. 这里的邻域节点特指两跳内的低阶邻居节点, $n_{\text{in}}(i)$ 和 $n_{\text{out}}(i)$ 分别表示节点 i 的入度邻居集合和出度邻居集合.易知, $\text{Sim}_{\text{directed}} \in [0, 1]$, 节点局部网络拓扑的重合程度越高,则节点相似度越大.

节点 a 的相似度重要度评估指标 LLS_{directed} 的量化方法如下.首先,获取目标节点的全部相邻节点集合.对于每个邻接节点,分别提取其出度邻居集合与入度邻居集合.基于该信息,分别计算邻接节点间的出度邻居相似性和入度邻居相似性,并将两者的平均值作为该节点对的综合相似性指标.随后,遍历目标节点的所有邻居节点对,计算其两两之间的综合相似度,并使用式(3)对所有相似度值进行整合,最终得到反映节点邻域拓扑结构特征的量化指标.

$$LLS_{\text{directed}}(i) = \sum_{b, c \in n(i)} (1 - \text{Sim}_{\text{directed}}(b, c)) \quad (3)$$

其中, $n(i)$ 表示节点 i 的邻居节点集合.该指标综合考虑了节点的度信息与邻居节点之间的相似性. LLS_{directed} 值越大,说明节点的度越大,且其邻居节点之间的邻域重合程度越低,即节点所在局部结构越异质.

2.4 网络鲁棒性评估

本文研究的网络鲁棒性特指“结构鲁棒性”,是指网络中的节点或边受到攻击后,整个网络保持结构连通性的能力. Schneider 等人^[11]研究了在蓄意攻击下最大连通分支的规模变化,并提出了一种网络鲁棒性的度量方法.结合本文所采用的攻击与防御策略的特点,本文采用如下的网络结构鲁棒性度量指标:

$$R = \frac{1}{r^*} \sum_{i=1}^{r^*} Q(i) \quad (4)$$

其中, r^* 表示当前所进行的轮次数目; $\frac{1}{r^*}$ 为归一化系数; $Q(i)$ 表示当网络中 i 个节点被攻击后,最大连通子图

的节点数占网络剩余节点总数的比例. $R \in [0, 1]$, R 值越大,表示网络的鲁棒性越强; R 值越小,表示网络的鲁棒性越弱. $Q_{\text{low}}(i) = \frac{N_i^{\text{low}'}}{N_i^{\text{low}}}$, 其中, $N_i^{\text{low}'}$ 表示第 i 轮次后低阶网络中最大连通分支包含的节点数, N_i^{low} 为低阶网络第 i 轮次后总的节点数; $Q_{\text{high}}(i) = \frac{N_i^{\text{high}'}}{N_i^{\text{high}}}$, 其中, $N_i^{\text{high}'}$ 表示第 i 轮次后高阶网络中最大连通分支包含的节点数, N_i^{high} 为高阶网络第 i 轮次后总的节点数.基于式(4),本文用 R_{high} 和 R_{low} 分别表示高阶和低阶网络的结构鲁棒性.

3 迭代攻防模型

在迭代攻防框架中,攻击方的目标是最大化网络的破坏程度,而防御方则致力于最小化该破坏.本文设定攻防双方均具备一定的网络破坏与修复能力.基于文献[19]提出的模型,本文所构建的框架不允许防御方对现有连接进行重构,即网络结构的调整仅通过节点或边的增减来实现.在此基础上,本文从节点重要度评估的角度,进一步引入第四种攻防策略,即下文3.1节中所描述的高邻域相似度去除和相似度均衡补充.下面将详细介绍针对有向复杂网络所采用的四种攻防策略,所有策略均通过最大连通分支的规模变化进行评估.

3.1 攻击策略

(1) 随机去除: 随机选取一个节点,删除它及其连接的边.重复这个过程 k_a 次.

(2) 高度去除: 选择度值最大的节点,删除它及其关联的边.重复这个过程 k_a 次.这里对所有节点计算度值并进行降序排序,节点 a 的度值 $d(a) = d_{\text{in}}(a) + d_{\text{out}}(a)$.

(3) 高中心性去除: 选择介数中心性最高的节点,去除及其相关的边.重复这个过程 k_a 次.节点 u 的介数中心性 $b_{\text{directed}}(u)$ 定义为当前网络中通过所有节点对之间的最短路径的比例,即

$$b_{\text{directed}}(u) = \frac{1}{N_{\text{reachable}}} \sum_{s \neq u, t \neq u \in V, \sigma_{s,t} > 0} \frac{\sigma_{s,t}(u)}{\sigma_{s,t}}$$

其中, $\sigma_{s,t}$ 为源节点 s 到目标节点 t 的最短路径总数; $\sigma_{s,t}(u)$ 为源节点 s 到目标节点 t 经过节点 u 的最短路径数; $N_{\text{reachable}}$ 为满足 $\sigma_{s,t} > 0$ 的节点对 (s, t) 的总数.

(4) 高邻域相似度去除: 计算出所有节点的相似度重要度评估指标 LLS_{directed} , 然后根据降序排序结果依次进行选取节点删除攻击,并去除其及其相关的边.重复这个过程 k_a 次.

3.2 防御策略

(1) 随机补充: 创建一个新节点并将其添加到低阶网络中,使该节点连接到 m 个随机选择不同的节点.重

复此过程 k_d 次。

(2) 度值优先补充: 创建一个新节点并添加到低阶网络中, 这样节点与 m 个不同节点连接产生 m 条新边的概率与节点的度值成正比例关系 (节点连接到一个现有节点 u 的概率 $P(u) = \frac{d(u)}{\sum_{v \in V} d(v)}$, $d(u)$ 是节点 u 在图 G 的度值)。重复此过程 k_d 次。

(3) 介数均衡补充: 创建一个新节点, 并将其添加到低阶网络中, 使该节点连接到 m 个不同的节点, 连接概率与其介数中心性成反比。该节点连接到现有节点的概率为

$$P(u) = \frac{(b_{\text{directed}}(u) + \varepsilon)^{-1}}{\sum_{v \in V} (b_{\text{directed}}(v) + \varepsilon)^{-1}},$$

其中, $b_{\text{directed}}(u)$ 是节点 u 在图 G 中的介数中心性; ε 是非常小的常数, 以防止除以 0。重复此过程 k_d 次。

(4) 相似度均衡补充: 创建一个新节点, 并将其添加到低阶网络中, 使该节点连接到 m 个不同的节点, 连接概率与其相似度重要度成反比。该节点连接到现有节点的概率为

$$P(u) = \frac{(\text{LLS}_{\text{directed}}(n(u) + \varepsilon))^{-1}}{\sum_{v \in V} (\text{LLS}_{\text{directed}}(n(v) + \varepsilon))^{-1}},$$

其中, $\text{LLS}_{\text{directed}}(n(u))$ 是节点 u 在图 G 中的相似度重要度; ε 是非常小的常数, 以防止除以 0。重复此过程 k_d 次。

通过上述定义的防御策略, 经过 k_d 次以后, 都添加了相同数量的 k_d 个节点和 $m \cdot k_d$ 条边, 这是因为每一轮防御中都会有一个新节点与图 G 中已经存在的 m 个节点进行连接, 对应产生 m 条新边, 所以经过 k_d 次以后, 会新增 k_d 个节点和 $m \cdot k_d$ 条边。

4 高阶网络鲁棒性演化特征

高阶网络的鲁棒性不仅受到底层拓扑结构的影响, 还与网络中的高阶交互模式密切相关。本章通过理论分析与数值仿真相结合的方法, 系统研究了高阶网络鲁棒性的演化规律。首先, 基于前述定义的网络鲁棒性评估指标, 分析不同类型的网络模型在模拟攻击策略下的鲁棒性变化趋势。随后, 针对四种典型网络模型, 结合仿真实验深入探讨其高阶鲁棒性特征, 揭示网络生成机制与模体生成机制对鲁棒性的关键影响。最后, 进一步分析高阶网络鲁棒性对模体结构的依赖性, 阐明特定模体模式在增强或削弱网络结构鲁棒性方面所起的作用。上述分析为理解高阶交互特征在复杂网络鲁棒性中的作用提供了新的研究视角和实证支持,

有助于推动高阶网络结构与功能关系的深入探索。

4.1 仿真结果

本节针对四种网络模型在不同攻防迭代策略下的鲁棒性进行分析。鉴于四种攻防策略下网络的结构鲁棒性在整体趋势和变化规律上表现出高度一致性, 为提高叙述的简洁性与聚焦性, 本文仅展示在介数中心性攻防策略下的仿真结果。参数设置为 $k_a = 2, k_d = 1$, 初始网络节点总数 $N = 150$, 攻防总轮次数为 100。仿真结果如图 3~6 所示, 展示了不同网络模型在该策略下的鲁棒性演化特征。

4.2 BA 无标度网络及 WS 小世界网络高阶鲁棒性波动特性及成因分析

基于图 3~图 6 的实验结果分析可知, 在由模体 $M_1 \sim M_7$ 构建的高阶网络中, BA 无标度网络模型表现出显著的数值波动特征, 其鲁棒性指标 R_{high} 曲线相较于其他三类网络模型, 呈现出更大幅度的振荡以及更高的数值水平。这一现象的成因可从以下两方面加以阐述。

首先, BA 无标度网络具有少数高度中心节点 (枢纽节点) 和大量低度节点的结构特性, 这种异质性结构导致其在面对攻击时呈现出“鲁棒而脆弱”的双重特性, 即对随机攻击具有较强的鲁棒性, 但在遭受蓄意攻击时则极为脆弱。当攻击策略优先针对高连接度节点时, 网络极易失去巨型连通分支, 从而导致整体结构迅速崩溃。然而在防御过程中, 若优先修复这些枢纽节点, 由于它们在网络中起到“桥梁”作用, 能够快速重建被破坏的关键路径, 因此网络鲁棒性也会迅速提升。此外, BA 网络中节点的连接遵循“优先连接”机制, 新加入节点倾向于连接至已有高度节点, 这一结构演化规律导致网络在攻防交替过程中结构波动显著, 进而在鲁棒性指标上表现出较大幅度的数值起伏。其次, BA 网络的局部聚集性较低, 节点之间难以形成高密度的局部连接群体, 因此模体 $M_1 \sim M_7$ 的引入会显著改变其局部结构特征, 进而放大了鲁棒性数值的波动性。相较之下, WS 小世界网络本身具有较高的聚类系数和较短的平均路径长度, 其本身结构与所引入模体在拓扑上存在相似性, 因此模体的嵌入不会显著扰动其原有结构, 导致 R_{high} 的波动幅度相对较小。对于 ER 随机网络而言, 其连接方式为均匀随机, 缺乏明显的枢纽节点, 高阶模体的引入对整体结构影响较为均衡, 不易因局部拓扑异质性而导致特定区域结构剧变, 因此鲁棒性指标 R_{high} 变化相对平稳。而局域世界网络的连接主要局限于局部子网, 模体的引入影响范围有限, 主要集中在局部区域, 难以对全局结构产生系统性扰动, 因此 R_{high} 的数值波动也较为温和。

其次, 模体 $M_1 \sim M_7$ 均为封闭的有向三角形结构, 使

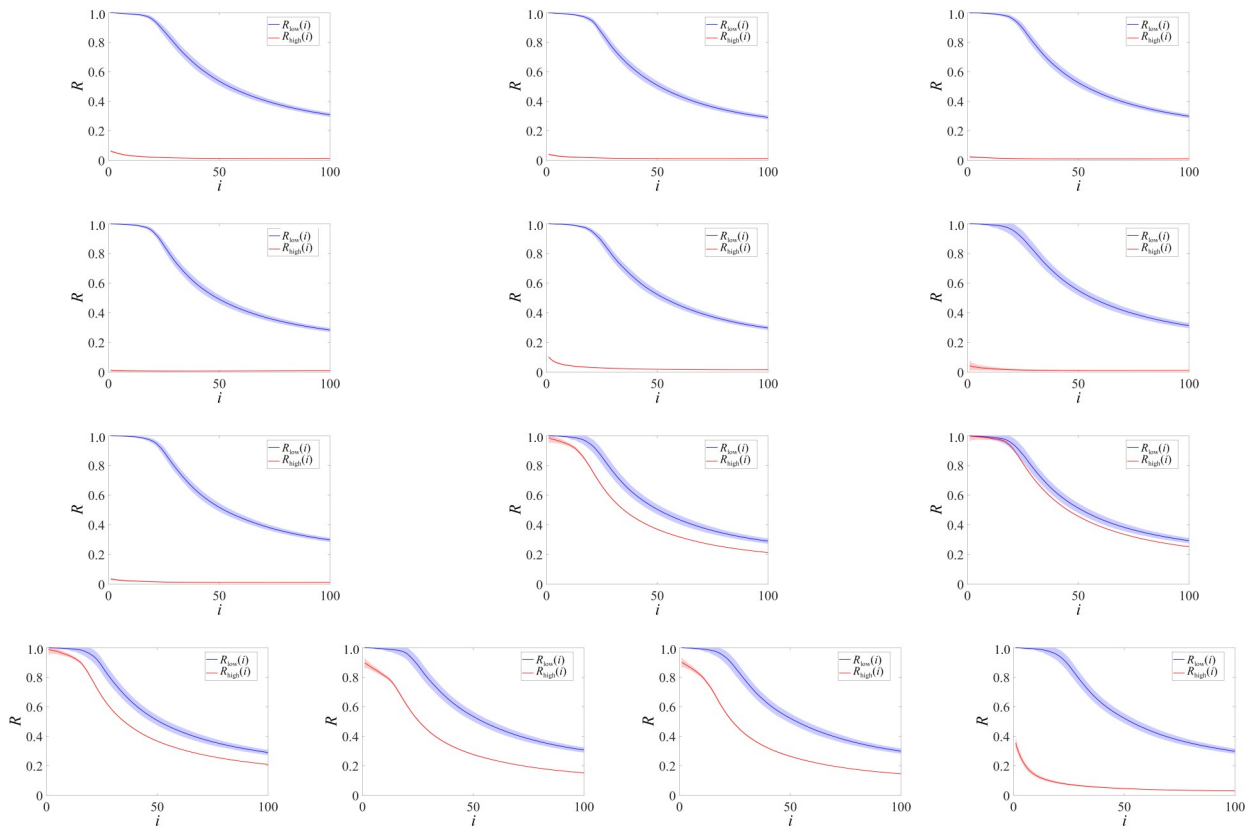


图3 ER随机高低阶网络鲁棒性演化特征仿真结果

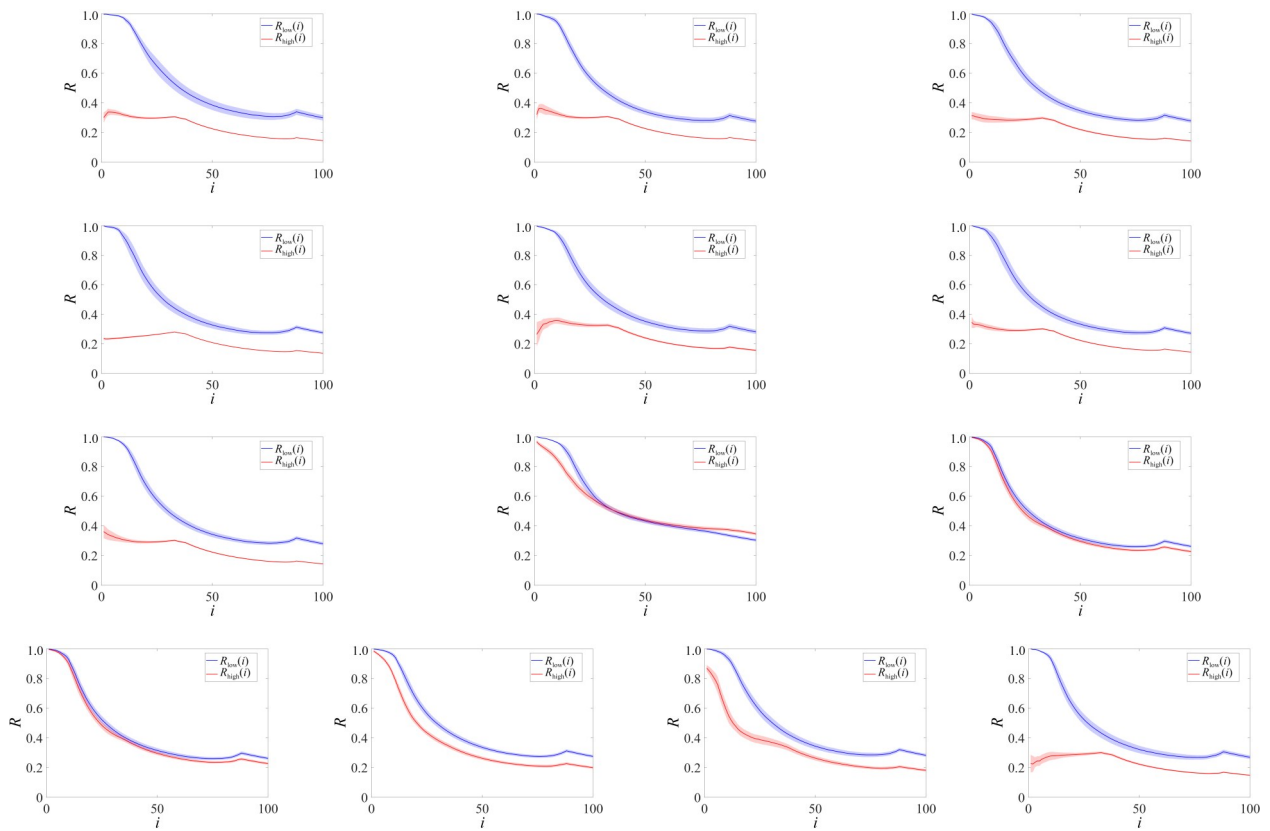


图4 WS小世界高低阶网络鲁棒性演化特征仿真结果

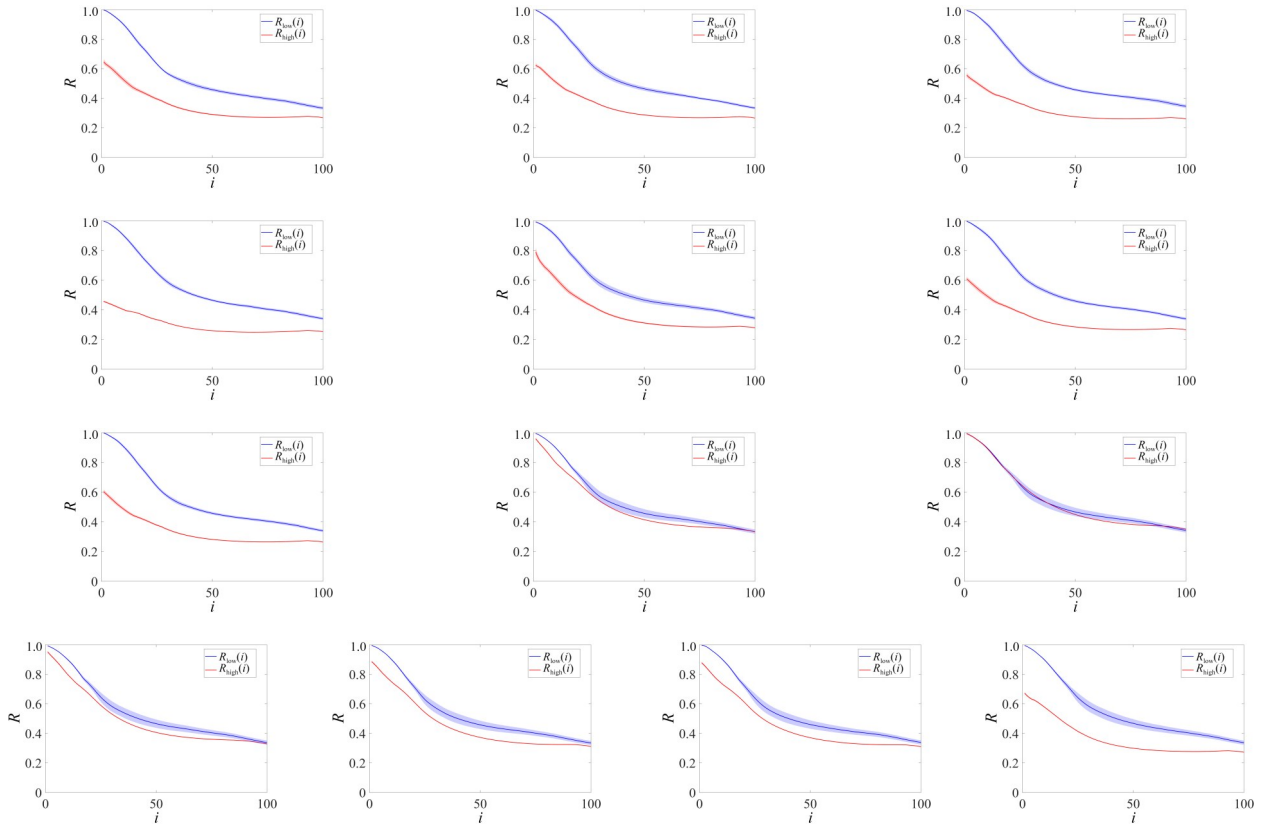


图5 BA无标度高低阶网络鲁棒性演化特征仿真结果

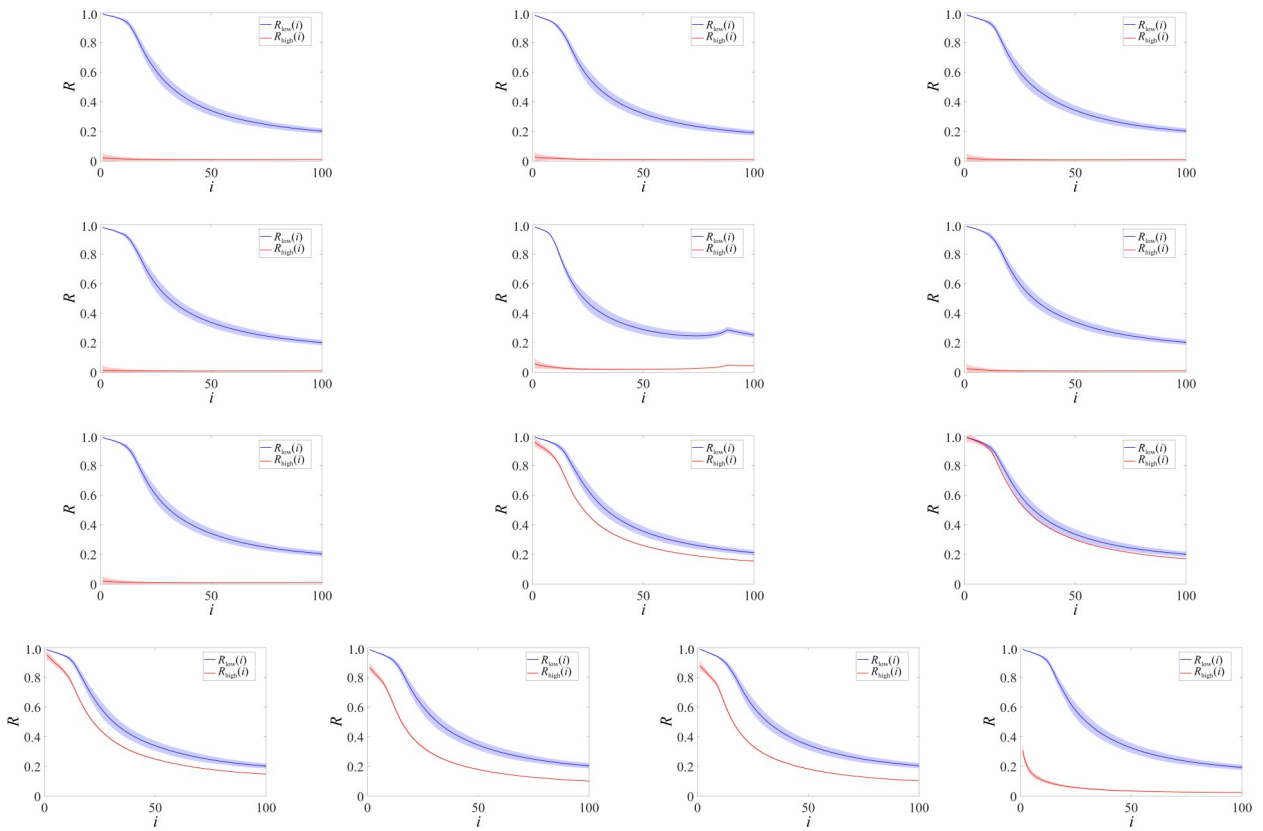


图6 局域世界高低阶网络鲁棒性演化特征仿真结果

得其所在的局部子网对结构完整性高度依赖,缺乏足够的冗余路径,从而导致整体网络的冗余性不足.在这种结构下,网络对高介数中心性节点的攻击尤为敏感,易引发局部结构的快速瓦解,进一步削弱了网络的局部鲁棒性.在BA网络中,原有的少数高连接度节点由于其“优先连接”机制,本就具有关键的结构地位,在引入模体 $M_1\sim M_7$ 后,这些高度节点的结构重要性被进一步放大.因此,当攻防策略针对这些关键节点实施时,网络结构的脆弱性显著增强,导致高阶鲁棒性指标出现剧烈波动.

如图3~图6所示,WS小世界网络基于不同模体生成的高阶网络在鲁棒性指标 R_{high} 上整体表现较好,表明以小世界网络拓扑为基础构建的高阶网络模型具有显著的结构鲁棒性优势.WS网络具备“短路径”与“少量长程连接”的结构特性,其中,短路径保障了局部连接的高效性,而长程边则显著提升了网络的全局容错能力.在攻击阶段,即使局部枢纽节点被删除,长程边依然能够维持全局网络的连通性;而在防御阶段,新增节点可通过长程边快速融入其他子网,提升结构修复效率.长程连接在网络中提供了全局冗余机制,有效缓解了模体 $M_1\sim M_7$ 所引入的局部结构脆弱性,避免系统对个别局部枢纽的过度依赖.此外,对于模体 $M_8\sim M_{13}$ 所构成的链式结构,其与WS网络中的长程边形成协同机制:链式结构提供基础的路径框架,而长程边则作为补充路径,显著增强了路径的多样性和冗余性,从而进一步提升了整体网络拓扑的鲁棒性.

4.3 高阶网络结构鲁棒性的模体依赖性分析

如图3~图6所示,基于模体 $M_8\sim M_{13}$ 构建的高阶网络在鲁棒性指标上表现出明显的优势,其数值显著高于由模体 $M_1\sim M_7$ 所生成的高阶结构.这种差异主要源于模体 $M_8\sim M_{13}$ 所具备的结构特性,例如更均匀的节点连接分布、对关键枢纽节点依赖程度较低等,从而使生成的高阶网络在整体上具有更强的全局连通性和结构冗余性,在面临攻击时能够更有效地保持网络的连通性.具体而言,模体 $M_8\sim M_{13}$ 所构建的网络具有较均衡的度分布,显著减少了高介数中心性节点的比例.因此,在遭受针对性攻击(如高度节点或高中心性节点)时,单个节点的移除对全局连通性的破坏作用有限.同时,由于存在更多的冗余路径,网络能够维持基本的功能不受重大影响.因此,诸如介数均衡补充或相似度均衡补充等防御策略更适用于此类结构,能够在攻击后迅速修复关键路径,有效提升鲁棒性指标.相比之下,模体 $M_1\sim M_7$ 是连通三角形结构,具有高度的局部紧密性.特别地,模体 $M_2\sim M_7$ 都含有双向边,表明节点间的依赖关系更为强烈,攻击任一节点将导致多个双向连接同时中断,进而对局部结构造成严重破坏.此外,这

些模体更易产生高度节点,而这些节点通常在网络中具有较高的介数中心性,参与多条最短路径.一旦此类关键节点被删除,将导致多个关键路径同时断裂,进而加速网络的分裂过程.由于该类网络结构在连通性上高度依赖局部枢纽与紧密连接区域,常规的防御策略难以有效修复其结构,造成整体网络恢复能力较弱.因此,以模体 $M_1\sim M_7$ 构建的高阶网络,其鲁棒性指标表现也相对较差.

基于模体 $M_8\sim M_{13}$ 构建的高阶网络中,其鲁棒性指标 R_{high} 曲线与对应低阶网络的鲁棒性 R_{low} 曲线显示出较高的重合度,两者在数值动态变化上的一致性显著.这表明该类模体在构建高阶网络时较好地保留了低阶网络的拓扑特征,如节点度分布、路径长度等.低阶有向网络(如WS小世界网络)通常具有较短的平均路径长度和一定的局部聚集性,但其连接结构未必完全封闭.模体 $M_8\sim M_{13}$ 所采用的非封闭有向边结构更贴近实际低阶网络的连接模式,因此构建出的高阶网络能够更有效地继承低阶网络的动态结构特性.低阶网络的鲁棒性通常依赖于节点度分布的均衡性以及路径的冗余程度,而通过模体 $M_8\sim M_{13}$ 所生成的高阶网络在保留稀疏有向边的同时,能够维持上述关键特性,从而使高低阶网络在鲁棒性表现上具有协同效应.综上所述,模体结构中边的方向性与封闭性是影响高阶网络鲁棒性的关键因素.非封闭、方向明确的结构不仅更符合原始网络的本征属性,也有助于构建具有更高动态一致性和鲁棒性的高阶网络模型.

5 鲁棒性与平均度之间的联系

网络的平均度作为衡量低阶网络连接密度的关键指标,对高阶网络鲁棒性的演化具有重要影响.为探究其内在作用机制,本章结合系统的仿真实验与理论分析,深入研究高阶网络鲁棒性与低阶网络平均度之间的关联关系.首先,分析在不同平均度条件下,四类典型网络模型(ER随机网络、WS小世界网络、BA无标度网络和局域世界网络)所构建的高阶网络鲁棒性表现,揭示网络平均度对高阶鲁棒性的调控规律,重点探讨局域世界网络在平均度变化下呈现出的高阶鲁棒性单调演化特征.其次,从模体结构角度出发,进一步阐释高阶鲁棒性的形成机制与优势,分析高阶交互如何增强网络在面对攻击时的稳定性与恢复能力.综上所述,本章研究从连接密度与结构模式两个维度出发,系统揭示了高阶网络鲁棒性与低阶网络平均度之间的深层联系,为理解复杂网络的结构-功能关系提供了新的理论视角,也为面向鲁棒性优化的网络设计与调控策略提供了重要的参考依据.

5.1 仿真结果

本节从网络平均度的角度,系统分析了局域世界网络及三种经典网络模型在结构鲁棒性方面的演化特征. 平均度 $d \in [0.5, 3]$ 描述了网络从稀疏向稠密的结构演变过程. 考虑到四种攻防策略在仿真结果中展现出高度一致的整体趋势与规律特征,为便于分析与表述,后续内容选取基于介数中心性的攻防策略作为代表进行展示. 在实验参数设置方面,设 $k_a=2, k_d=1$,初始网络节点总数为 $N=150$,攻防总轮次数为 100. 相应的仿真结果如图 7~图 10 所示.

如图 10 所示,在局域世界网络模型中,基于模体

$M_1 \sim M_7$ 构建的高阶网络,其鲁棒性指标 R_{high} 在平均度 $d \in [0.5, 2.2]$ 区间内数值变化较为平稳;当 $d > 2.2$ 时, R_{high} 呈现显著上升趋势,并在 $d=2.8$ 时达到较高水平. 相比之下,基于模体 $M_8 \sim M_{13}$ 生成的高阶网络在 $d > 2.2$ 时,其鲁棒性指标 R_{high} 逐渐趋近于 1. 其中,模体 M_9 构型网络的鲁棒性表现尤为突出,且在 $d \in [0.5, 2.2]$ 范围内波动幅度较小,展现出良好的稳定性. 此外,在 ER 随机网络、WS 小世界网络和 BA 无标度网络这三类经典模型中(分别见图 7~图 9),无论采用哪一类模体构建高阶网络,在低阶网络层面实施四种攻防策略时,其鲁棒性指标 R_{high} 均未出现显著波动,整体数值变化较小,未表现出明显的上升或骤降趋势.

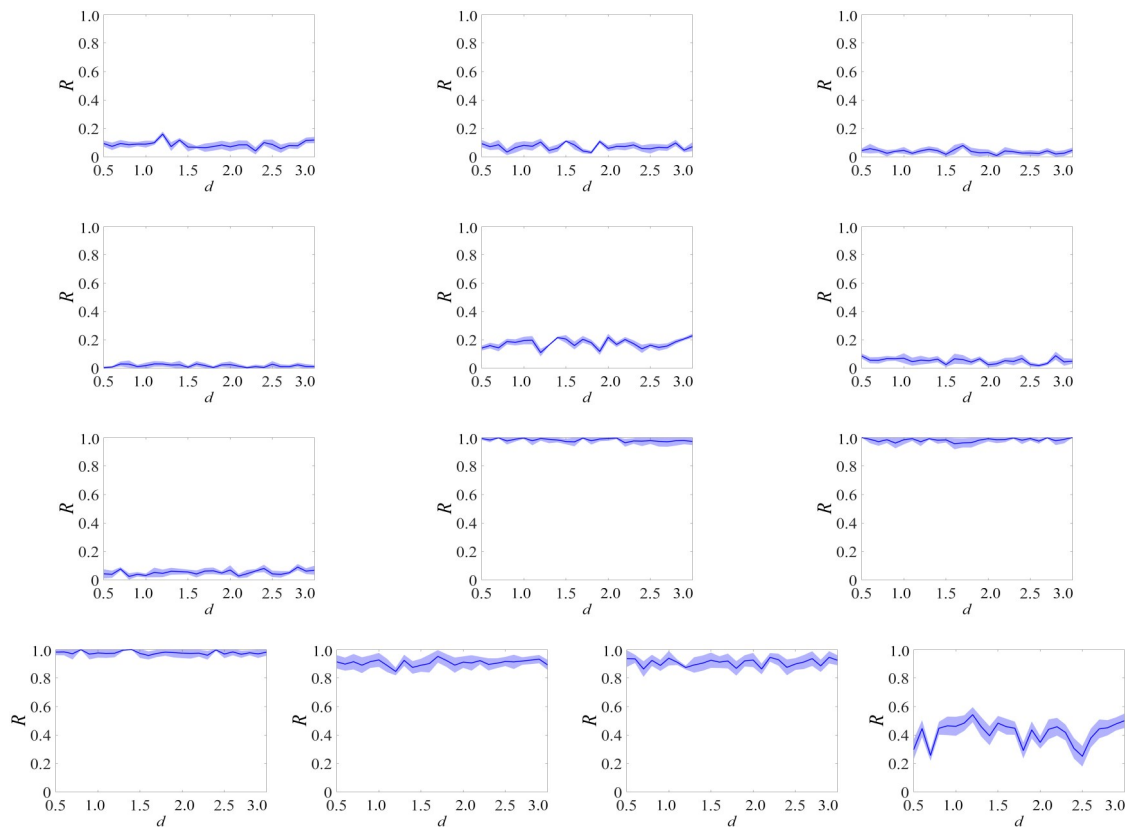


图 7 ER 随机网络模体结构依赖的高阶网络鲁棒性随平均度演化规律

5.2 局域世界网络鲁棒性的变化趋势

如图 7~图 10 所示,随着低阶网络平均度 d 的增加,前三类经典网络模型的高阶鲁棒性指标 R_{high} 整体呈现波动幅度较小的特征,变化较为平缓;而局域世界网络在平均度达到特定阈值后, R_{high} 则表现出明显的上升趋势,且波动幅度显著增大. 上述差异性的演化行为可归因于局域世界网络独特的拓扑相变机制:当系统平均度跨越某一临界阈值时,其网络结构属性及相关动力学特征会发生质的转变,进而显著提升其高阶鲁棒性表现.

具体而言,局域世界网络的生成机制,即新节点优

先连接到局部子网(而非全局随机连接),局部优先连接使得形成多个紧密子网络结构. 这样的生成机制对高阶网络 R_{high} 会产生如下影响:在攻击阶段,删除局部结构的枢纽节点会影响子网络连通性,但由于在全局连接中存在的情况较少,所以 R_{high} 下降较平缓;在防御阶段,新增节点优先连接局部子网络结构,对模体内部节点连接和子网络修复效果稳定,使得 R_{high} 值恢复趋势平缓. 并且攻击和防御的影响主要局限于子网,不会引发全局网络结构产生突变,即使平均度增加,新增连接仍集中在局部子网,不会显著改变全局动态,所以

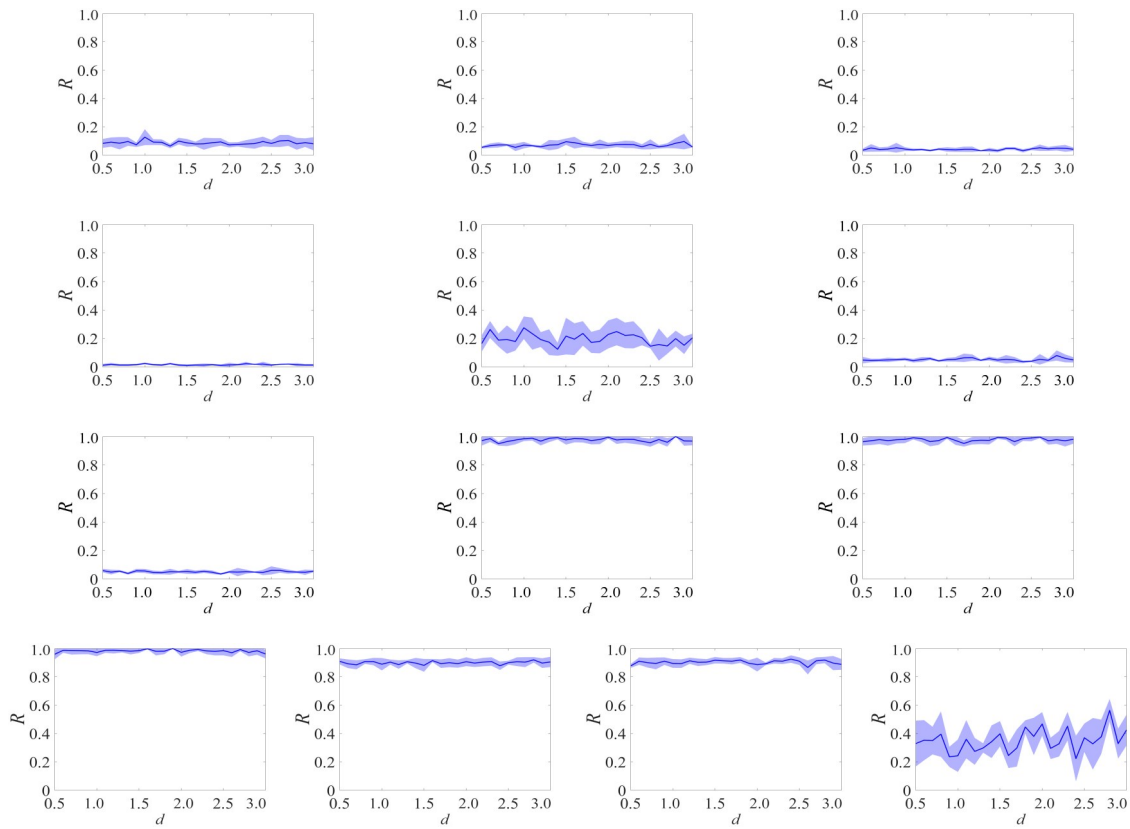


图8 WS小世界网络模体结构依赖的高阶网络鲁棒性随平均度演化规律

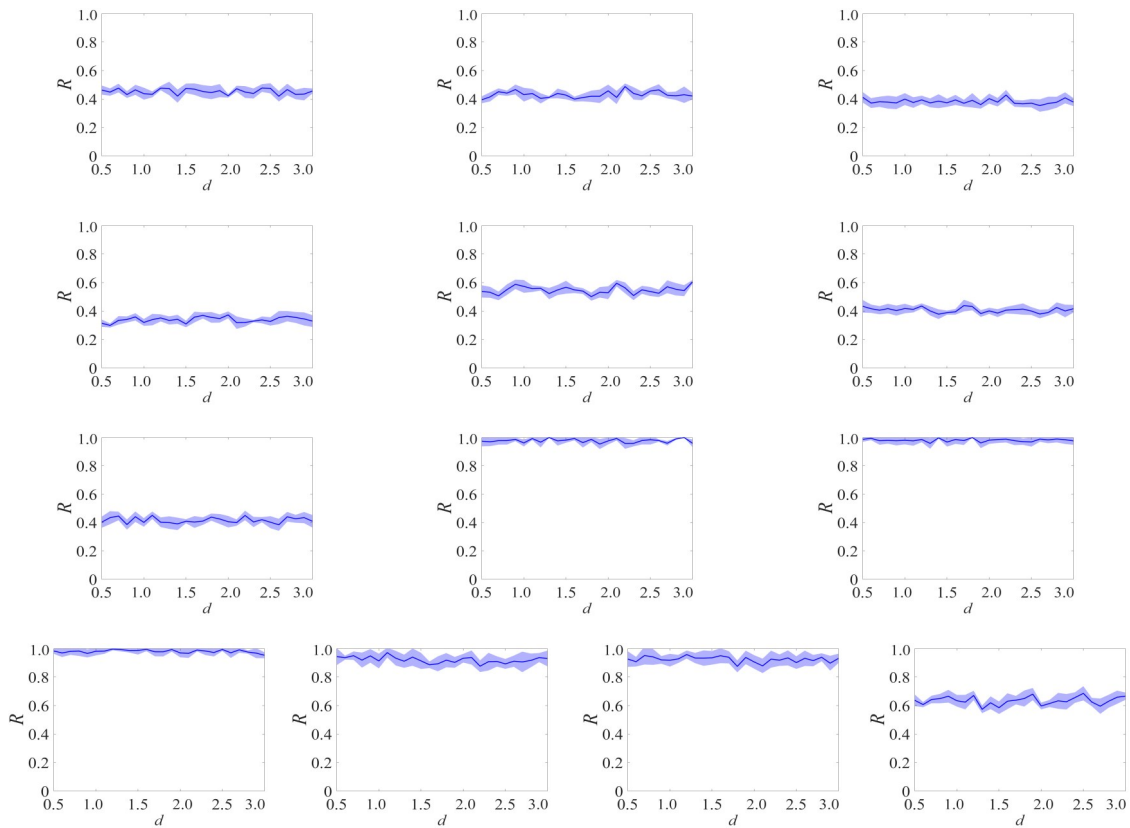


图9 BA无标度网络模体结构依赖的高阶网络鲁棒性随平均度演化规律

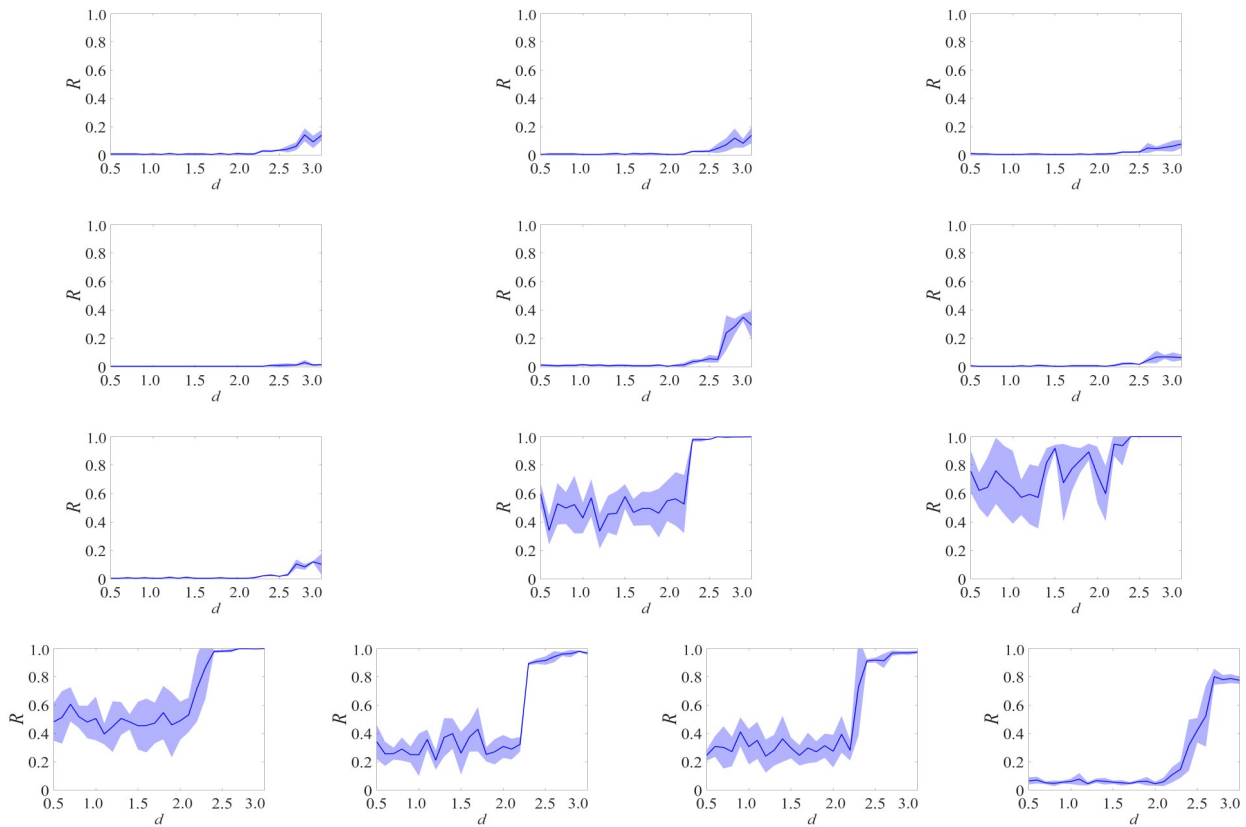


图 10 局域世界网络模体结构依赖的高阶网络鲁棒性随平均度演化规律

R_{high} 值变化平滑. 在 d 达到阈值 2.2 后, 高阶网络 R_{high} 发生明显上升趋势. 当系统跨越该临界阈值时, 网络经历拓扑相变, 原本孤立的局域模块开始形成全局连通结构, 模体和低阶网络结构二者协同作用导致高阶网络鲁棒性增强, $d \approx 2.8$ 网络的全局冗余性得到了较大提升, 因此 R_{high} 达到较大值. 反观另外三类网络, ER 随机网络完全随机连接, 边均匀分布, 无局部优先连接特性; BA 无标度网络生长机制虽有优先连接, 但新增节点的连接是全局随机的; WS 小世界网络通过随机重连机制打破局部规则性, 具有长程边生成的可能性可以降低蓄意攻击对网络结构造成的损害. 这三种网络的随机性使得对平均度 d 的变化响应更连续, 进而高阶网络鲁棒性波动较小.

5.3 基于 M_9 模体的高阶鲁棒性优势

如图 7~图 10 所示, 基于模体 M_9 生成的高阶网络鲁棒性 R_{high} 趋近于 1 的情况相较于其他模体情况较多. 此种差异化的演变模式主要来源于模体结构的局部连接特性与网络全局平均度的动态耦合, 决定了高阶网络在攻击下的结构鲁棒性演化.

模体 $M_8 \sim M_{13}$ 的自身结构适应稀疏连接, 在 $d \in [0.5, 2.2]$ 网络结构较为稀疏连接时仍能维持一定连通性. 随着网络平均度 d 的增加, 新增边会优先连接不同模

体, 将其从简单的链路结构重组为交互的子网络结构, 使得 R_{high} 快速趋近于 1. 反观模体 $M_1 \sim M_7$, 即使 $d > 2.2$, 新增边会连接其他不同的局局部子网, 提升网络全局鲁棒性, 但是模体结构封闭性仍限制全局冗余, 导致 R_{high} 数值普遍低于基于模体 $M_8 \sim M_{13}$ 的情况. 特别地, 模体 M_9 不需要完全闭合的连接, 对边的依赖性较低, 并且网络中路径的选择具有灵活性, 即使部分节点被攻击, 剩余的边仍可能通过其他路径维持网络的整体连通性. 而且在平均度 d 较高时, 链式结构 ($M_8 \sim M_{13}$) 可以通过新增边快速形成替代路径使得网络结构具有一定的冗余性, 提升网络全局连通性, 因此高阶网络 R_{high} 趋近于 1 的情况较多. 而其他模体拓扑结构复杂度相比模体 M_9 较高, 其冗余路径生成效率显著降低, 网络整体连通性能得不到很好的提升, 进而高阶网络 R_{high} 趋近于 1 的情况较少.

综上, 可以得到如下结论:

(1) 平均度的阈值效应. $d=2.2$ 是局域世界网络从局部依赖转向全局冗余的临界点. 由于在模体 $M_1 \sim M_7$ 中, 每个模体维持结构的完整性要求较高, 所以 $d \approx 2.8$ 才能突破这个限制, 此时网络的全局冗余性得到了提升, R_{high} 达到较大值.

(2) 模体的核心作用. 模体 $M_1 \sim M_7$ 在 d 较小时网络

连接稀疏,含有的封闭结构(如三角形)数量少,攻击少数边或节点可能导致模体快速解体,进而引发级联失效; d 较大时修复网络连通性效率低,即使网络连接稠密(平均度 d 较大),模体因结构复杂(如多节点互连),局部受损后需重构大量边才能恢复功能,因此需更高连接成本. 此模体结构适合对局部鲁棒性要求高的应用场景. 模体 $M_8 \sim M_{13}$ 在 d 较小时,结构简单,较少发生节点产生的级联失效现象,所以高阶网络鲁棒性较好; d 较大时,新增边会优先连接不同模体,将原本孤立的链式结构转化为交互的网络结构,使得网络连通性能提升,进而可以提升全局鲁棒性.

(3)模体 M_9 是平衡高阶网络具有冗余与复杂度的较优选择. M_9 的简单链式结构在低阶网络中展现出特殊的拓扑稳定性,其线性连接模式能有效保留低阶网络的局部路径结构,使得生成的高阶网络连通性性能尽可能地保持较好,进而 R_{high} 趋近 1 的情况较多.

这些结论对网络设计也具有一定的启示,稀疏网络易被破坏但修复成本低,稠密网络难被破坏但修复成本高. 如果要求高阶网络鲁棒性较高,选择模体如 M_9 , 优先提升平均度至 $d > 2.2$. 若资源有限(平均度 d 较小),采用模体 $M_8 \sim M_{13}$ 可以较好地保留低阶网络的拓扑特性. 这一研究结果揭示了网络结构连接密度与模体结构的协同效应,为高阶网络鲁棒性优化提供了理论依据.

6 总结与展望

本文系统研究了多智能体网络系统在低阶与高阶结构层面的鲁棒性演化特征. 通过对低阶网络施加多组差异化的迭代攻防策略,并基于预设模体规则构建相应的高阶网络,进一步对比分析了两者在结构鲁棒性量化指标上的表现,揭示其鲁棒性演化的动态特征. 研究得出以下结论:首先,采用多种攻防策略对典型网络模型进行测试,结合高阶网络鲁棒性指标的动态响应曲线分析发现,相较于封闭结构模体 $M_1 \sim M_7$, 开放结构模体 $M_8 \sim M_{13}$ 对网络鲁棒性的提升作用更为显著;其次,在高阶与低阶网络鲁棒性曲线的拟合程度方面,由模体 $M_8 \sim M_{13}$ 构建的高阶网络表现出更高的一致性,其中以模体 M_9 构型所生成的高阶网络拟合效果最佳,其鲁棒性曲线与对应低阶网络高度吻合.

此外,通过调控网络平均度参数开展对比实验发现,低阶网络的平均度变化对高阶网络的结构鲁棒性具有显著影响. 尤其在基于模体 M_9 构建的高阶网络中,鲁棒性指标 R_{high} 常趋近于 1. 当平均度高于某一个阈值时,局域世界网络的高阶鲁棒性呈现出明显的上升趋势,而其余三类经典网络模型则整体维持相对平稳的波动状态. 这些实验结果充分表明,模体的拓扑结

构特征以及低阶网络的平均度参数共同决定了高阶网络鲁棒性的演化趋势与稳定性.

尽管本文揭示了模体结构和平均度对高阶网络鲁棒性的影响,但仍有诸多值得进一步探索的研究方向. 未来的工作可聚焦于动态网络中模体演化与攻击策略之间的交互机制,例如在自适应攻击场景下,模体结构发生重构的临界条件. 另一方面,有必要构建多尺度鲁棒性评估指标,以更系统地量化模体的局部结构特性与高阶网络整体鲁棒性之间的关联. 此外,结合图神经网络等机器学习方法实现关键模体配置的自动识别,将为高阶网络分析提供新工具,并有望在生物网络中关键功能模体的识别与验证方面发挥重要作用.

参考文献

- [1] JEONG H, TOMBOR B, ALBERT R, et al. The large-scale organization of metabolic networks[J]. Nature, 2000, 407(6804): 651-654.
- [2] ALBERT R, ALBERT I, NAKARADO G L. Structural vulnerability of the North American power grid[J]. Physical Review E, 2004, 69(2): 025103.
- [3] 温广辉, 周佳玲, 吕跃祖, 等. 多导弹协同作战中的分布式协调控制问题[J]. 指挥与控制学报, 2021, 7(2): 137-145.
WEN G H, ZHOU J L, LÜ Y Z, et al. Distributed coordination control in multi-missile cooperative tasks[J]. Journal of Command and Control, 2021, 7(2): 137-145. (in Chinese)
- [4] 江碧涛, 温广辉, 周佳玲, 等. 智能无人集群系统跨域协同技术研究现状与展望[J]. 中国工程科学, 2024, 26(1): 117-126.
JIANG B T, WEN G H, ZHOU J L, et al. Cross-domain cooperative technology of intelligent unmanned swarm systems: Current status and prospects[J]. Strategic Study of CAE, 2024, 26(1): 117-126. (in Chinese)
- [5] 吕金虎, 于江龙, 董希旺. 飞行器集群协同制导新进展[J]. 自动化学报, 2025, 51(4): 727-743.
LÜ J H, YU J L, DONG X W. New progress in cooperative guidance for aircraft swarm system[J]. Acta Automatica Sinica, 2025, 51(4): 727-743. (in Chinese)
- [6] 郑志明, 吕金虎, 韦卫, 等. 精准智能理论: 面向复杂动态对象的人工智能[J]. 中国科学: 信息科学, 2021, 51(4): 678-690.
ZHENG Z M, LÜ J H, WEI W, et al. Refined intelligence theory: Artificial intelligence regarding complex dynamic objects[J]. Scientia Sinica (Informationis), 2021, 51(4): 678-690. (in Chinese)

- [7] 吴忠强, 程洪强. 网络攻击下考虑状态受限的微电网安全运行与控制[J]. 电子学报, 2024, 52(9): 3240-3250.
WU Z Q, CHENG H Q. Safe operation and control of microgrid considering state constraints under network attacks[J]. Acta Electronica Sinica, 2024, 52(9): 3240-3250. (in Chinese)
- [8] ALBERT R, JEONG H, BARABÁSI A L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(6794): 378-382.
- [9] COHEN R, EREZ K, BEN-AVRAHAM D, et al. Resilience of the Internet to random breakdowns[J]. Physical Review Letters, 2000, 85(21): 4626-4628.
- [10] COHEN R, EREZ K, BEN-AVRAHAM D, et al. Breakdown of the Internet under intentional attack[J]. Physical Review Letters, 2001, 86(16): 3682-3685.
- [11] SCHNEIDER C M, MOREIRA A A, ANDRADE J S JR, et al. Mitigation of malicious attacks on networks[J]. Proceedings of the National Academy of Sciences of the United States of America, 2011, 108(10): 3838-3841.
- [12] BUSSER P, DAOLIO F, TOMASSINI M. Optimizing the robustness of scale-free networks with simulated annealing[C]//Adaptive and Natural Computing Algorithms. Berlin: Springer, 2011: 167-176.
- [13] ZENG A, LIU W P. Enhancing network robustness against malicious attacks[J]. Physical Review E, 2012, 85(6): 066130.
- [14] ZHOU M X, LIU J. A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks[J]. Physica A: Statistical Mechanics and its Applications, 2014, 410: 131-143.
- [15] TANIZAWA T, PAUL G, COHEN R, et al. Optimization of network robustness to waves of targeted and random attacks[J]. Physical Review E, 2005, 71(4): 047101.
- [16] 王尔申, 王玉伟, 庞涛, 等. 基于边攻击成本的复杂网络鲁棒性研究[J]. 电子学报, 2018, 46(5): 1166-1172.
WANG E S, WANG Y W, PANG T, et al. Research on robustness of complex networks with edge's attack cost[J]. Acta Electronica Sinica, 2018, 46(5): 1166-1172. (in Chinese)
- [17] NAGARAJA S, ANDERSON R. The topology of covert conflict[EB/OL]. (2005-08-01) [2025-10-10]. <https://eprint.iacr.org/2005/250>.
- [18] AXELROD R, HAMILTON W D. The evolution of cooperation[J]. Science, 1981, 211(4489): 1390-1396.
- [19] KIM H, ANDERSON R. An experimental evaluation of robustness of networks[J]. IEEE Systems Journal, 2013, 7(2): 179-188.
- [20] SHI D H, CHEN G R. Simplicial networks: A powerful tool for characterizing higher-order interactions[J]. National Science Review, 2022, 9(5): nwac038.
- [21] XIA R Y, XIANG L Y. Pinning control of simplicial complexes[J]. European Journal of Control, 2024, 77: 100994.
- [22] ZHAO D D, LI R C, PENG H, et al. Percolation on simplicial complexes[J]. Applied Mathematics and Computation, 2022, 431: 127330.
- [23] 余文倩, 马福祥, 陈阳, 等. 基于自适应的高阶网络鲁棒性分析[J]. 复杂系统与复杂性科学, 2025, 22(4): 15-23.
YU W Q, MA F X, CHEN Y, et al. High-order networks robustness analysis based on self-adaptive[J]. Complex Systems and Complexity Science, 2025, 22(4): 15-23. (in Chinese)
- [24] 张成军, 姚辉, 雷毅, 等. 高低阶耦合网络的鲁棒性研究[J]. 复杂系统与复杂性科学, 2024, 21(3): 17-22, 29.
ZHANG C J, YAO H, LEI Y, et al. Study on the robustness of high-low-order coupling networks[J]. Complex Systems and Complexity Science, 2024, 21(3): 17-22, 29. (in Chinese)
- [25] ZHAO D D, LING X W, ZHANG X T, et al. Robustness of directed higher-order networks[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2023, 33(8): 083106.
- [26] MA F X, YU W Q, MA X J. Study on the robust control of higher-order networks[J]. Scientific Reports, 2025, 15: 7033.
- [27] ZHENG C L, HU Y L, ZHANG C J, et al. Optimizing the robustness of higher-low order coupled networks[J]. PLoS One, 2024, 19(3): e0298439.
- [28] BATTISTON F, CENCETTI G, IACOPINI I, et al. Networks beyond pairwise interactions: Structure and dynamics[J]. Physics Reports, 2020, 874: 1-92.
- [29] ZHAO X M, YU H T, ZHANG J P, et al. Important nodes mining based on a novel personalized temporal motif pagerank algorithm in temporal networks[J]. International Journal of Modern Physics C, 2022, 33(12): 2250161.
- [30] MILO R, SHEN-ORR S, ITZKOVITZ S, et al. Network motifs: Simple building blocks of complex networks[J]. Science, 2002, 298(5594): 824-827.
- [31] BENSON A R, GLEICH D F, LESKOVEC J. Higher-order organization of complex networks[J]. Science, 2016, 353(6295): 163-166.

- [32] SIZEMORE A E, GIUSTI C, KAHN A, et al. Cliques and cavities in the human connectome[J]. *Journal of Computational Neuroscience*, 2018, 44(1): 115-145.
- [33] 阮逸润, 老松杨, 王竣德, 等. 基于领域相似度的复杂网络节点重要度评估算法[J]. *物理学报*, 2017, 66(3):

371-379.

RUAN Y R, LAO S Y, WANG J D, et al. Node importance measurement based on neighborhood similarity in complex network [J]. *Acta Physica Sinica*. 2017, 66(3): 371-379. (in Chinese)

作者简介



邢之尧 男,1997年7月出生于安徽省阜阳市. 现为天津工业大学电子与信息工程学院博士研究生. 主要研究方向为复杂网络与复杂系统.
E-mail: 19290727592@163.com



项林英 女,1980年11月出生于浙江省建德市. 现为天津工业大学人工智能学院教授、博士生导师. 主要研究方向为多智能体系统协同控制、复杂网络控制与优化.
E-mail: xianglinying@tiangong.edu.cn