复杂网络能控性鲁棒性研究进展

楼 洋 [1, 2] 李均利 [1] 李 升 [1] 邓 浩 [1]

摘 要 研究复杂网络能控性鲁棒性对包括社会网络、生物和技术网络等在内的复杂系统的控制和应用具有重要价值. 复杂网络的能控性是指: 可通过若干控制节点和适当的输入, 在有限时间内将系统状态驱动至任意目标状态. 能控性鲁棒性则是指在受到攻击的情况下, 复杂网络依然维持能控性的能力. 设计具有优异能控性鲁棒性的复杂网络模型和优化实际网络的能控性鲁棒性一直是复杂网络领域的重要研究内容. 本文首先比较了常用的能控性鲁棒性定义及度量, 接着从攻击策略的角度分析了 3 类攻击的特点及效果, 包括随机攻击、基于特征的蓄意攻击和启发式攻击. 然后比较了常见模型网络的能控性鲁棒性. 介绍了常用优化策略, 包括模型设计和重新连边等. 目前的研究在攻击策略和拓扑结构优化方面都取得了进展, 也为进一步理论分析提供条件. 最后总结全文并提出潜在研究方向.

关键词 复杂网络, 能控性鲁棒性, 攻击, 优化

引用格式 楼洋, 李均利, 李升, 邓浩. 复杂网络能控性鲁棒性研究进展. 自动化学报, 2022, **48**(10): 2374−2391

DOI 10.16383/j.aas.c200916

Recent Progress in Controllability Robustness of Complex Networks

LOU Yang[1, 2] LI Jun-Li[1] LI Sheng[1] DENG Hao[1]

Abstract The study of controllability robustness is valuable to the control and application of various complex systems, including social, biological, and technological networks. The concept of controllability of complex networks refers to the ability of a network being steered by external inputs from any of its initial state to any desired target state under an admissible control input within a finite duration of time. The controllability robustness reflects how well the system can maintain the controllability against malicious attacks by means of node removals or edge removals. This survey gives a systematic investigation in the recent progress of the controllability robustness of complex networks. Firstly, the definitions and measures of controllability robustness are introduced. Then, the controllability robustness is considered from the perspective of attacks. Three types of attack strategies are discussed, including random attacks, feature-based targeted attacks, and heuristic-based attacks. Optimization methods toward stronger controllability robustness are investigated, including network modeling, edge rewiring, etc. Recent progresses have been achieved in both effective attack strategies and efficient topological optimizations, which provide a basis for further theoretical analysis. Finally, some potential future works are suggested.

Key words Complex network, controllability robustness, attack, optimization

Citation Lou Yang, Li Jun-Li, Li Sheng, Deng Hao. Recent progress in controllability robustness of complex networks. *Acta Automatica Sinica*, 2022, **48**(10): 2374−2391

复杂网络作为现今科学研究中的一个热点学科, 在过去 20 年里得到了巨大的发展[1−4]. 复杂网络普遍存在, 如互联网、神经网络、交通运输网[5]等. 同时许多系统, 如人际社会关系[6]、学术合作[7]、人类迁徙[8] 等都可以抽象为复杂网络, 以进行系统地分析和研究. 除了广泛应用于数学、工程、经济等学科之外, 复杂网络更与我们的日常生活息息相关, 如在信息的传播[9]、语言的演变[6, 10−12]、流行病的传播和阻断[13−15]、网络群体智能[16−17] 等方面, 复杂网络都提供了极有价值的参考模型和分析工具.

复杂网络能控性 (Controllability) 是复杂网络研究的一个核心问题[18−33], 其概念是指在有限时间内, 通过适当的控制输入, 控制网络从任意初始状态到达一个目标状态的能力. 人类对自然系统和技术系统的理解, 最终体现在如何有效地控制它们, 使之为人类的生存和发展服务. 作为一个跨学科的研究领域, 网络科学与控制系统理论之间的跨学科研究在过去 20 年里得到迅速的发展.

收稿日期 2020-11-04 录用日期 2021-02-09
Manuscript received November 4, 2020; accepted February 9, 2021
国家自然科学基金 (62002249), 浙江大学 CAD & CG 国家重点实验室开放课题 (A2112) 资助
Supported by National Natural Science Foundation of China (62002249) and the Open Project Program of the State Key Laboratory of CAD & CG, Zhejiang University (A2112)
本文责任编委 曹向辉
Recommended by Associate Editor CAO Xiang-Hui
1. 四川师范大学计算机科学学院 成都 610101 中国 2. 香港城市大学电机工程学系 香港 999077 中国
1. School of Computer Science, Sichuan Normal University, Chengdu 610101, China 2. Department of Electrical Engineering, City University of Hong Kong, Hong Kong 999077, China

由于复杂网络通常具有大量的节点和连边, 其中高维动态节点系统相互连接, 这给经典控制理论和技术带来了新的机遇, 但同时也带来了巨大的挑战. 对于复杂的动态网络, 要达到最佳控制目标, 往往只需要通过外部输入控制小部分节点或连边. 作为实现网络优化控制的实用方法之一, 牵引控制 (Pinning control) 策略[34] 旨在通过高效的算法来回答 "牵引控制多少节点和哪些节点" 的问题, 以最少的能量消耗和代价, 达到牵一发而动全身的最优效果.

复杂网络在攻击下维持能控性的能力称为能控性鲁棒性 (Controllability robustness). 本文中 "攻击" 的表现形式为删除节点或连边. 近年来, 对复杂网络的攻击成为主要关注的问题之一[35−45]. 这些随机或恶意的攻击可能导致系统瘫痪等严重后果. 复杂网络的能控性理论为研究神经网络结构和功能之间的联系提供了分析工具, 如分析秀丽线虫 (Caenorhabditis elegans) 的各神经元功能及其与肌肉运动的联系[46]. 而能控性鲁棒性则为进一步研究提供分析基础, 如秀丽线虫部分神经元损坏可导致生物功能障碍和疾病[46], 这里神经元损伤可看作网络拓扑结构受到攻击, 即网络中的节点和连边受到破坏和攻击. 此外, 能控性鲁棒性的研究对交通运输、电力、社交网络的鲁棒控制具有重要的指导意义.

在不同背景下, 复杂网络抵御攻击的能力 (或称 "抗毁性") 具有不同的定义和度量[47]. 在维持连通性能力 (Connectedness)[37, 45, 47−48] 的研究中, 抗毁性是指复杂网络在攻击情况下保持连通性的能力. 在能控性研究中, 抗毁性是指网络维持能控性的能力. 为避免混淆, 本文将保持连通的抗毁性称为 "连通鲁棒性"; 将保持能控性的抗毁性称为 "能控性鲁棒性", 也是本文的主要讨论对象. 良好的能控性以较强的连通性为基础, 但是, 强的连通性却不能保证良好的能控性. 同样地, 良好的能控性鲁棒性以良好的连通鲁棒性为基础, 而良好的连通鲁棒性并不能保证良好的能控性鲁棒性. 能控性鲁棒性较好的网络系统具有好的抵御攻击的能力, 同时能延迟系统的整体瘫痪, 为攻击后的补救争取时间. 相反地, 能控性鲁棒性差的系统则容易在受到攻击以后, 迅速导致网络系统的整体失效. 因此, 实用的控制网络模型应同时兼备良好的能控性和能控性鲁棒性. 基于当前理论研究的局限和日益发展的超级计算能力, 复杂网络的能控性鲁棒性研究以仿真实验研究为主[49−50]. 同时, 深度学习的发展也为这一领域提供新的研究技术[51−53]. 不同类型网络系统具有不同的能控性计算方式, 如有向和无向网络, 无权和有权网络, 以及单输入单输出和多输入多输出系统等, 因而其能控性鲁棒性的研究与优化也有所不同. 本文主要阐述针对有向网络的能控性鲁棒性研究, 主要关注以下 3 个关键问题:

1) 如何定义和度量复杂网络的能控性鲁棒性? 能控性鲁棒性的定义和度量为不同拓扑结构的优劣提供比较标准, 为不同攻击方式的破坏能力提供参考, 也为复杂网络的优化提供依据. 不同的定义方式具有不同的理论依据及其侧重点, 导致不同的比较结果. 在计算方式上, 基于仿真的能控性鲁棒性的计算得到的结果真实准确, 但需要较大的计算量, 而基于深度神经网络的能控性鲁棒性预测则可以较小的计算代价取得相对准确的估值.

2) 常见的攻击方式有哪些? 哪些攻击对能控性的危害最大? 针对不同的攻击方式, 复杂网络可能表现出不同的能控性鲁棒性, 所以研究攻击方式对于复杂网络的能控性鲁棒性有重要意义. 通过分析常见的攻击方式及其危害程度, 可以理解网络中节点、连边和其他特征对能控性鲁棒性的重要程度; 找到危害最大的攻击对于评价网络的性能也有着重要的意义, 启发式攻击由计算智能算法自主选择攻击对象, 可以达到相较于传统方法更大的破坏效果. 同时, 对网络攻击的研究也有助于对网络优化的研究, 对网络的攻击的理解和将其应用于优化犹如理解 "矛与盾" 的关系, 既相互抑制, 又相互促进.

3) 怎样提高能控性鲁棒性? 如何达到最优的能控性鲁棒性? 对复杂网络的能控性鲁棒性优化问题属于 NP (Nondeterministic polynomial time) 难问题. 但是由于能控性鲁棒性度量方式, 攻击方式, 以及限制条件等的不同, 使其成为一个多目标优化问题. 同时, 由于基于仿真的能控性鲁棒性度量普遍耗时较多, 以及节点和连边特征与能控性鲁棒性之间相关性不够明确等问题, 给该优化问题带来了挑战.

围绕以上 3 个问题, 本文就能控性鲁棒性研究现状与进展进行归纳总结, 指出当前研究中存在的问题与技术挑战, 并探讨了未来发展趋势.

1 复杂网络的能控性鲁棒性

1.1 预备知识

1.1.1 无权有向网络

对于一个无权有向网络 $G = (\mathcal{V}, \mathcal{E})$, 其中, $\mathcal{V} = \{1, 2, \cdots, N\}$ 和 $\mathcal{E} = \{A_{ij} | i, j \in \mathcal{V}\}$ 分别为节点和连边集合. 邻接矩阵 A 中元素 A_{ij} 定义为

$$A_{ij}=\begin{cases}1, & \text{若存在连边}\ (i,\ j)\\ 0, & \text{否则}\end{cases} \tag{1}$$

其各节点的出度和入度可由邻接矩阵计算, 即

$$\begin{cases}k_i^{\text{out}}=\displaystyle\sum_{j=1}^{N}A_{ij}\\ k_i^{\text{in}}=\displaystyle\sum_{j=1}^{N}A_{ji}\end{cases} \tag{2}$$

各节点的介数可由式 (3) 计算, 即

$$b_i=\sum_{i\neq s\neq t}\frac{\sigma_{st}\,(i)}{\sigma_{st}} \tag{3}$$

其中, σ_{st} 是从节点s 到节点t 的所有最短路径总数, $\sigma_{st}\,(i)$表示这些路径经过节点i的次数. 对于有向网络, 如果从节点s到t存在最短路径, 则称节点s到t可达, 否则称为不可达.

1.1.2 复杂网络能控性

复杂网络能控性的概念由卡尔曼[54] 在 1960 年首先提出. 对于一个复杂网络系统或线性时不变 (Linear time invariant, LTI) 系统

$$\dot{\boldsymbol{x}}=A\boldsymbol{x}+B\boldsymbol{u} \tag{4}$$

其中, A 和B 分别为$N\times N$ 和$N\times N_D$ 常系数矩阵, 分别代表网络的邻接矩阵和 LTI 系统外部控制器所控制的节点, $\boldsymbol{x}$是状态向量, $\boldsymbol{u}$ 是控制输入, 卡尔曼准则 (Kalman criterion)[54] 提出该系统能控的充分必要条件是系统的能控性矩阵

$$C=[B\ AB\ A^2B\ \cdots\ A^{N-1}B] \tag{5}$$

满足行满秩, 该能控性称为复杂网络的状态能控性 (State controllable). 结构能控性的概念是状态能控性的泛化. 对于常参数系数矩阵 A 和B, 如果存在一组非零参数值可以确保系统是状态能控的, 那么则称该系统是结构能控的 (Structural controllable). 对于一个能控系统, 其状态向量$\boldsymbol{x}$可以通过适当的控制输入$\boldsymbol{u}$ ($N_D\times 1$ 向量), 从任意初始状态驱动至任意目标状态.

1.1.3 匹配

匹配 (Matching) 是指由连边所组成的集合, 该集合中的任意两条连边不共享起始节点和终止节点. 连边集合$\mathcal{E}$ 中除了匹配连边, 其余均为非匹配. 最大匹配 (Maximum matching) 包含了最大可能的匹配数目. 最大匹配并不唯一. 如果一个节点是一条匹配连边的终止节点, 则该节点是匹配节点 (Matched node), 否则是非匹配节点. 在完全匹配 (Perfect matching) 中, 所有的网络节点均为匹配节点. 图 1(a) 链式网络的最大匹配包含 3 条连边, 除了起始节点 1 之外都是匹配节点; 图 1(b) 所示 4 节点星型网络的最大匹配包含 1 条连边, 且不唯一 (3 种情况); 图 1(c) 网络的最大匹配包含 5 条连边, 且不唯一 (最大匹配可包含连边 (5, 6) 或 (5, 7)). 其类仙人掌型结构具有较好的能控性[55].

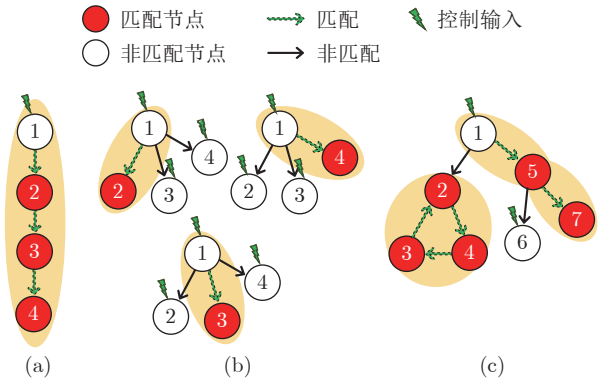


图 1 匹配和节点控制中心性的例子

Fig. 1 Examples of matching and node control centrality

1.1.4 节点控制中心性

节点控制中心性 (Control centrality)[38] 度量单个节点做为控制节点的控制范围, 其定义为

$$C_c(G,\ i)\equiv \text{rank}_g(C^{(i)}) \tag{6}$$

其中, $C_c(G,\ i)$ 表示复杂网络G 中节点i 的节点控制中心性, C 表示网络能控性矩阵 (Controllability matrix), 可由式 (5) 计算; $\text{rank}_g(C^{(i)})$ 表示能控子空间的一般维度, 可根据 Hosoe 理论[56] 计算. 控制中心性大的节点能控制的范围较大, 适合作为控制节点. 图 1 中阴影部分表示每个网络中节点 1 的能控子空间. 图 1 给出了节点控制中心性的相关例子: 图 1(a) 中节点 1 的控制中心性为 4; 图 1(b) 中节点 1 在 3 种情况下的控制中心性都为 2; 图 1(c) 中节点 1 的控制中心性为 6.

1.1.5 关键连边和关键节点

Liu 等[18] 将有向网络连边依据其对能控性的贡献分为 3 类: 1) 关键连边, 删除任一关键连边会导致系统能控性下降, 也就是需要额外增加一个控制节点; 2) 冗余连边, 删除任一冗余连边不影响系统的能控性; 3) 普通连边, 删除一条普通连边不会导致能控性下降, 但是会改变可能的最大匹配. 其中冗余连边和普通连边可称为非关键连边. 图 2(a) 和图 2(c) 分别举例说明了关键连边与普通连边.

Lou 等[57] 依据其对结构能控性 (见式 (8)) 鲁棒性的贡献, 将所有连边分为 3 类: 1) 关键连边, 定义与文献 [18] 相同; 2) 亚关键 (Subcritical) 连边,

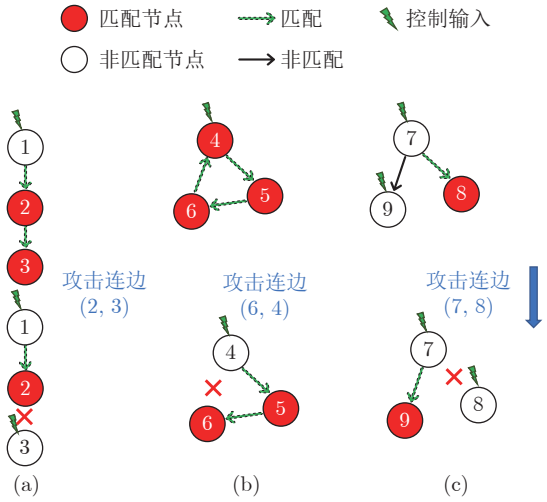


图 2　按文献 [57] 连边分类举例

Fig. 2　An example of edge classification according to [57]

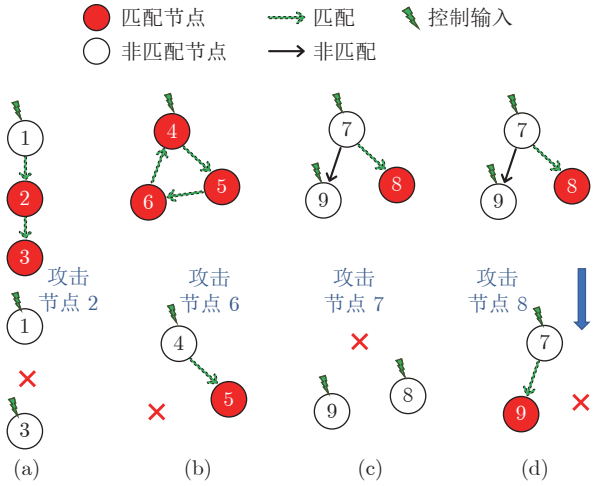


图 3　按文献 [57] 节点分类举例

Fig. 3　An example of node classification according to [57]

遭攻击后不会改变控制节点数, 但是会增加 1 个非匹配节点; 3) 普通连边, 被攻击后既不会影响控制节点数, 也不会增加非匹配节点数. 注意文献 [57] 定义的 “普通” 连边包含了文献 [18] 定义的 “普通” 和 “冗余” 连边.

图 2 分别给出了关键连边 (图 2(a))、亚关键连边 (图 2(b)) 和普通连边 (图 2(c)) 的例子. 同时, 文献 [57] 将该分类扩展到节点, 将所有节点分为 4 类: 1) 关键节点, 其遭攻击后须额外增加 1 个控制节点; 2) 亚关键节点, 遭受攻击后不影响控制节点数, 但会使非匹配节点增加 1; 3) 普通节点, 其遭攻击既不影响控制节点数, 也不影响非匹配节点数; 4) 冗余节点, 其遭受攻击后使得所需控制节点数下降 1, 冗余节点是从能控性角度的 “孤立节点” (不一定与其他节点没有连边).

图 3 给出了节点分类举例. 图 3(a) 中节点 2 是关键节点, 遭攻击后节点 1 和 3 分别须单独的控制输入; 图 3(b) 中节点 6 是亚关键节点, 遭攻击后虽然控制节点数不变, 但节点 4 由匹配节点变为非匹配节点; 图 3(c) 中节点 7 为普通节点, 遭攻击后控制节点数不变, 非匹配节点数也不变 (原先非匹配节点为 7 和 9, 攻击后非匹配节点为 8 和 9); 图 3(d) 中节点 8 为冗余节点, 将其删除后, 系统所需控制节点减少 1.

1.2　能控性度量

通常, 复杂网络能控性可由控制节点的密度 (n_D) 来量化表示, 即

$$n_D \equiv \frac{N_D}{N} \tag{7}$$

其中, N_D 是系统所需控制节点的总和, N 是系统中节点数总和. $n_D \in [1/N, 1]$, 当 $n_D = 1/N$ 表示当前网络的 N 节点只需一个控制节点, 此时的能控性最佳; 而当 $n_D = 1$ 则表示当前网络的每个节点都需要一个单独的控制器, 此时网络能控性最差. 系统具有较小的 n_D 值, 表示该系统的能控性较好.

常用的控制节点数 N_D 计算方法有两种, 分别根据结构能控性[18] 和精确能控性 (Exact controllability)[20]. 结构能控性可由匹配 (Matching) 计算, 依据最小输入理论 (Minimum inputs theorem)[18], 控制节点数可由最大匹配计算得到, 即

$$N_D = \max\{1, N - |E^*|\} \tag{8}$$

其中, $|E^*|$ 是最大匹配 E^* 中的连边数. 式 (8) 说明网络所需控制节点数等于网络中非匹配节点的个数. 当网络非完全匹配时, 需 $N_D = N - |E^*|$ 个控制节点, 即将控制器加载于 N_D 个非匹配节点. 当网络为完全匹配时, 仅需 $N_D = 1$ 个控制节点, 此时控制器可加载于任意节点.

为了识别任意结构以及加权网络达到能控状态所需的最小驱动节点数, Yuan 等[20] 根据卡尔曼准则的等价条件 PBH (Popov-Belevitch-Hautus) 秩提出精确能控性, 其所需控制节点个数可由式 (9) 计算获得, 即

$$N_D = \max\{1, N - \mathrm{rank}(A)\} \tag{9}$$

如果矩阵 A 满秩, 需 $N_D = 1$ 个控制节点; 否则, 需 $N - \mathrm{rank}\,(A)$ 个控制节点.

1.3　能控性鲁棒性定义

复杂网络能控性描述了当前系统的能控性状态; 而能控性鲁棒性则刻画在受到攻击的情况下, 复杂

网络能控性的变化情况.

常用的能控性鲁棒性定义包括基于能控性曲线的定义, 基于节点控制中心性的定义, 以及基于排序的定义. 其中基于能控性曲线的定义参照常用的连通鲁棒性定义. 常用的连通鲁棒性度量基于最大连通子图 LCC (Largest connected component)[37], 在节点攻击情况下, 其计算为

$$R_{\mathrm{LCC}}^{N}=\frac{1}{N}\sum_{i=1}^{N}Q\left(i\right) \tag{10}$$

其中, $Q\left(i\right)$ 表示当网络中 i 个节点被攻击之后, 最大连通子图的节点数占当前网络节点总数的比例, 其范围是 $[1/N,\,1]$, 当 $Q\left(i\right)=1/N$ 表示该网络包含 N 个离散节点, 而当 $Q\left(i\right)=1$ 则表示该网络节点互相连通. 类似地, R_{LCC} 在连边攻击时计算为

$$R_{\mathrm{LCC}}^{E}=\frac{1}{M}\sum_{i=1}^{M}Q\left(i\right) \tag{11}$$

其中, $Q\left(i\right)$ 表示当网络中 i 条连边被攻击之后, 最大联通子图的节点数占当前网络节点总数的比例; M 为网络中的连边总数. 式 (10) ~ (15) 中的上标 N 和 E 分别表示节点攻击和连边攻击.

1.3.1 基于能控性曲线的定义

能控性鲁棒性即系统在遭受节点或连边攻击之后, 余下网络的能控性. 它是一组能控性值的序列, 其中节点攻击下能控性鲁棒性定义为

$$n_{D}^{N}\left(i\right)\equiv\frac{N_{D}\left(i\right)}{N-i},\ i=0,\,1,\,\cdots,\,N-1 \tag{12}$$

其中, $N_{D}\left(i\right)$ 是当 i 个节点遭受攻击后, 所需的控制节点数; $N-i$ 为 i 个节点遭攻击后的网络剩余节点数, 随着每次攻击逐一减少. 同样地, 连边攻击下能控性鲁棒性定义为

$$n_{D}^{E}\left(i\right)\equiv\frac{N_{D}\left(i\right)}{N},\quad i=0,\,1,\,\cdots,\,M \tag{13}$$

其中, $N_{D}\left(i\right)$ 是当 i 条连边遭受攻击后, 所需的控制节点数; N 和 M 分别表示网络节点和连边数. 注意在连边攻击下节点数不变, 而连边数逐一减少. 当 $i=0$, $n_{D}^{N}\left(0\right)=n_{D}^{E}\left(0\right)$ 表示遭受攻击前的初始网络能控性.

式 (12) 和式 (13) 定义了攻击情况下能控性变化的动态过程. 而整体的能控性鲁棒性可由平均得到, 如式 (14) 和式 (15) 所示.

$$R_{c}^{N}=\frac{1}{N}\sum_{i=0}^{N-1}n_{D}^{N}\left(i\right) \tag{14}$$

$$R_{c}^{E}=\frac{1}{M+1}\sum_{i=0}^{M}n_{D}^{E}\left(i\right) \tag{15}$$

其中, 较小的 R_{c}^{N} 或 R_{c}^{E} 值分别表示在节点或连边攻击的情况下, 具备较好的整体能控性鲁棒性. 该度量方式与常用的连通性鲁棒性的度量 LCC[37] 类似. 式 (14) 与式 (10) 区别在于: 1) 函数 $n_{D}^{N}(\cdot)$ 和 $Q(\cdot)$ 的物理意义和计算方式不同; 2) 考虑到各网络的初始能控性 $n_{D}^{N}\left(0\right)$ 不同, 因而须从 $i=0$ 开始累加, 而一般情况下, 网络的初始状态均连通, 即 $Q\left(0\right)=1$, 因而可忽略.

1.3.2 基于节点控制中心性的定义

Usman 等[58] 将能控性鲁棒性定义为节点和连边受攻击以后能控子空间 (Controllable subspace) 的剩余维度, 提出了预期鲁棒控制中心性 ERCC (Expected robust control centrality). 假设对复杂网络 G 中任意 n 个节点进行攻击, 则节点 i 做为控制节点的预期鲁棒控制中心性可由如下计算得到, 即

$$\mathrm{ERCC}\left(i,\,n\right)=\mathrm{E}\left[C_{c}\left(G'\left(n\right),\,i\right)\right] \tag{16}$$

其中, $G'\left(n\right)$是由 G删除 n节点后得到的网络; $C_{c}(G,\,i)$ 表示网络 G 中节点 i 的节点控制中心性; $\mathrm{E}[\cdot]$ 表示数学期望. 作为预期鲁棒控制中心性的扩展, 即

$$\mathrm{GRCC}\left(i\right)=\mathrm{E}\left[C_{c}\left(G'\left(e\right),\,i\right)\right] \tag{17}$$

其中, e 是节点 i 可达的任意一条边. 相较于 ERCC 而言, GRCC (Generic robust control centrality) 不限定在当前网络中攻击 n 个节点这一条件. ERCC 和 GRCC 适用于度量随机攻击情况下, 某节点 i 的控制范围的鲁棒程度, 因而可根据 ERCC 或 GRCC 选择适当的控制节点.

由于式 (16) 和式 (17) 计算量巨大, Usman 等[58] 提出了一种均匀采样的估值方式, 降低了部分计算量. 该鲁棒性度量适合于评估选择哪些节点适于作为鲁棒的控制节点.

1.3.3 基于排序的能控性鲁棒性度量

Chen 等[50] 提出一种基于排序比较的能控性鲁棒性度量. 该度量计算在相同的受攻击程度下 (受攻击的节点或连边比例相同), 不同网络的能控性 (根据式 (7) 计算) 的排序, 依照排序确定能控性鲁棒性: 排序靠前的较好, 排序靠后的较差.

图 4 列举了两个复杂网络 net1 和 net2 在受到同种攻击情况下的能控性曲线, 其中 R_{c} 表示基于能控性曲线的能控性鲁棒性, R_{k} 表示基于排序的能控性鲁棒性. 对两个网络在相同的受攻击节点比例下进行比较排序, 例如, 当受攻击节点比例为 0.1 时, net2 排序为 1, net1 排序为 2. R_{k} 为其排序的整体平均值.

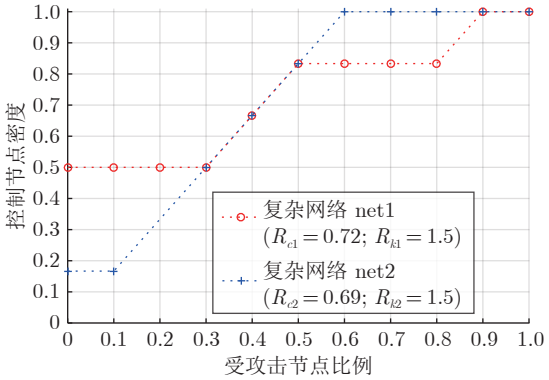


图 4　能控性鲁棒性度量方式比较举例

Fig. 4　Comparison of two different controllability robustness measurements

从网络攻击的过程来看, net2 的初始能控性较好, 而受到攻击时能控性下降 (所需控制节点密度上升) 速度较快, net1 的初始能控性较差, 但是在攻击中维持较好. 根据能控性曲线的平均值 (R_c (net1) = 0.72, R_c (net2) = 0.69), net2 的能控性鲁棒性更好; 而根据基于排序的度量 (R_k (net1) = R_k (net2) = 1.5), 两者能控性鲁棒性等价.

两种度量的侧重点不同, 相对基于能控性曲线的定义, 基于排序的度量更注重鲁棒性, 而弱化了能控性本身和初始能控性的比重; 其缺点在于该方法只能根据给定方法和结果比较, 无法推广到的一般情况. 基于上述理由, 本文对能控性鲁棒性的讨论以第 1.3.1 节的基于能控性曲线的定义为基准.

1.4　能控性鲁棒性的预测

对一个 N 节点 M 连边的复杂网络, 其点攻击和边攻击次数范围分别为 $[0, N-1]$ 和 $[0, M]$, 每次攻击以后以式 (8) 或式 (9) 计算网络的当前能控性, 可得能控性曲线. 以 Hopcroft-Karp 算法为例, 计算式 (8)的复杂度为 $O(M\times\sqrt{N})$ [59]; 以 Coppersmith-Winograd 算法为例, 计算式 (9) 的复杂度为 $O(N^{2.37})$ [60]. 通过仿真获得的曲线精确但耗时. Sun 等[61] 提出了在随机和蓄意攻击下的能控性曲线近似预测. Lou 等[52] 通过训练卷积神经网络[62], 获得能控性鲁棒性曲线的近似预测, 其预测误差小于样本方差, 同时将计算速度提升 $10^2\sim10^3$ 倍[52]. 进一步地, 文献 [63−64] 通过加入先验知识, 提高了卷积神经网络的预测精度, 同时比较得出该预测精度优于谱度量 (Spectral measures)[65] 和异质性 (Heterogeneity)[66] 等方法. 值得一提的是, 深度学习也应用于分析和预测其他非解析的网络属性[53, 67].

1.5　能控性鲁棒性研究框架

目前的研究成果主要集中在对复杂网络的拓扑结构的探索和优化两个方面.

对拓扑结构的探索体现在研究复杂网络中节点和连边对维持能控性鲁棒性的重要性, 即寻找网络中的关键节点和连边. 由于目前尚没有可以预测能控性鲁棒性优劣的可靠详实的理论依据, 而且经验指标也不充足, 这一研究目标主要依靠设计高效的攻击策略来实现. 本文第 2 节回溯了随机攻击、基于特征的蓄意攻击和启发式攻击, 其中基于特征的蓄意攻击和启发式攻击的研究对探索预测能控性鲁棒性优劣的指标 (或经验指标) 具有重要意义.

对拓扑结构的优化主要包括模型优化设计和重新连边. 本文第 3 节回顾了主要的优化策略, 同时介绍了全齐性和模体 (包括环和链等) 结构对提高能控性鲁棒性的重要意义.

2　针对能控性鲁棒性的攻击

能控性鲁棒性体现了在攻击下, 系统保持能控状态的优劣. 在不同攻击方式下, 不同的复杂网络系统呈现出不同的鲁棒性. 攻击的类别基于对象可分为节点攻击和连边攻击. 通常, 对节点攻击后, 该节点及其所有连边从当前网络中删除; 对连边攻击后, 仅该连边从当前网络中删除.

按攻击目标的不同可分为随机攻击和蓄意攻击. 随机攻击指无差别地破坏、删除复杂网络中的节点或连边; 蓄意攻击则优先攻击被认为最重要的节点或连边, 例如度数最高的节点. 同时, 不同的攻击方式针对不同的复杂网络功能, 如图 5 所示, 一种对网络连通性的破坏较大的攻击, 对于能控性的破坏未必较大. 图 5(a) 中的星型网络, 其所需控制节点数为 4, 其最大连通子图 LCC[37] 为 6 (即 6 个节点之间均有连边相连); 当中心节点被攻击后, 其所需控制节点数为 5 (增加 25%), 而其最大连通子图降为 1 (减少 83%).

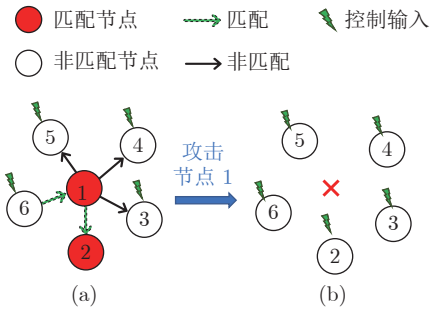


图 5　能控性鲁棒性与连通性鲁棒性

Fig. 5　Controllability robustness and connectedness robustness

由于网络连通性和能控性既有一定的相关性又存在差别, 即能控必须连通, 而连通未必能控. 本文讨论的攻击以破坏网络能控性为主, 文中描述的攻击效果以破坏网络能控性为目标.

2.1 随机攻击

随机攻击是指均匀随机地选择复杂网络中的节点或连边进行攻击. Sun 等[61] 指出, 在随机攻击下, 网络所需控制节点数的增量, 可以根据网络中关键连边的数量估算得到, 即

$$\Delta N_D = \frac{M_r \times M_c}{M}, \quad 若\ M_r \leq M_c \tag{18}$$

当被攻击的连边数小于关键连边数时, 关键连边会以 $p(M_c) = M_c/M$ 的概率被攻击. 每攻击一条关键连边, 所需的控制节点数增加 1; 若攻击到非关键连边, 所需控制节点数保持不变. 如果被攻击的连边总数大于关键连边数 (即 $M_r > M_c$), 则式 (18) 不成立, 因为此时网络中的关键连边已经发生变化. 实际上, 攻击 1 条连边就可能引起关键连边的变化, 如图 6 举例所示. 在图 6(a) 中 连边 (2, 4) 原本是非关键连边, 当连边 (2, 3) 和 (3, 4) 被攻击以后, 则变成了关键连边; 在图 6(b) 中节点 2, 3, 4 原本都是关键节点, 但当节点 1 被攻击以后, 它们都成为非关键节点; 接着, 当节点 4 遭受攻击之后, 节点 2 又成为关键节点.

Liu 等[38] 利用有向网络中的层级结构, 设计了随机上/下游攻击, 旨在攻击随机选取的节点的上游或者下游节点. 该攻击比普通随机攻击以更大的概率攻击到枢纽 (Hub) 节点, 因而比普通随机攻击更有效. 以图 1(c) 中节点 5 为例, 其上游节点为节点 1, 下游节点为节点 6 和 7.

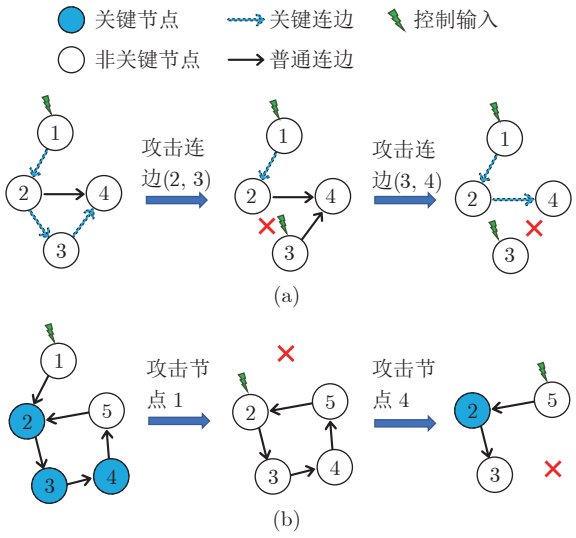


图 6 关键连边和关键节点在遭受攻击过程中变化

Fig. 6 Critical edges and nodes may change during attacks

2.2 基于特征的蓄意攻击

区别于随机攻击, 蓄意攻击的攻击者选取主观认为的最有效对象进行攻击, 因此, 蓄意攻击的效果一般比随机攻击更显著. 通常假设攻击者具有对被攻击网络的必要知识, 如最大度数节点、最大介数连边等, 并且该知识能在攻击后得到更新. 常用于破坏复杂网络连通性的攻击特征包括度数和介数, 以及邻里相似度 (Neighborhood similarity)[68]、分支权重 (Branch weighting)[69]、结构孔 (Structural holes)[70] 等. 通常, 攻击者主观地认为该知识 (网络特征) 能带来最优的破坏效果, 然而, 度量复杂网络节点和连边在维持能控性方面的重要性, 是一个复杂而艰巨的任务, 尤其是对较大规模网络. 绝大部分基于单一特征的攻击并不能给网络带来持续的、最有效的破坏.

网络拓扑结构与能控性之间关联的研究较多[27, 32, 71−73], 而与能控性鲁棒性相关的指标或特征研究相对较少. 目前尚无可以预测能控性鲁棒性优劣的可靠详实的理论依据, 而且经验指标也不充足. 节点攻击的研究较多, 而连边攻击的研究较少[74], 其原因是: 1) 节点攻击相对有效, 攻击节点时其连边也同时被删除, 而连边攻击并不影响节点; 2) 节点的特征属性相对明确, 而连边的属性相对模糊, 如有向图的节点具有明确的出度和入度定义, 而连边的出度和入度不同定义较多[35, 47, 75].

2.2.1 基于度数和介数的攻击

基于度数的攻击旨在攻击网络中度数最大的节点 (或连边). Holme 等[35] 将基于度和介数的节点攻击分别分为基于初始分布的攻击和重新计算分布的攻击. 前者依据最初网络的度数或介数分布, 由大到小依次攻击, 而后者则在每次攻击后重新计算. 由于网络的统计特征在攻击后通常会发生较大变化, 重新计算的攻击效果要优于基于初始分布的攻击[35, 76], 因而本文默认基于度数或介数的攻击中, 度数或介数最大的节点需要在每次攻击后重新计算.

基于度数和介数的攻击既是破坏网络连通性的最常见攻击方式, 也是破坏能控性的常用方式. 基于度数的攻击是局部策略, 其重点是尽可能快地减少总连边; 而基于介数攻击是全局策略, 专注于尽可能多地破坏全局最短路径. 基于度数和介数的节点攻击分别定义为

$$i^* = \begin{cases} \arg\max\limits_{i\in\mathcal{V}} k_i^{\text{out}}, & \text{若考虑出度} \\ \arg\max\limits_{i\in\mathcal{V}} k_i^{\text{in}}, & \text{否则} \end{cases} \tag{19}$$

$$i^* = \arg\max_{i\in\mathcal{V}} b_i \tag{20}$$

其中, k_i^{out}, k_i^{in} 和 b_i 分别为节点 i 的出度、入度和介数, i^* 表示选择攻击的节点序号. 同样地, 基于度数和介数的连边攻击定义只需将式 (19) 和式 (20) 中的节点集合 $\mathcal{V}$ 替换为连边集合 $\mathcal{E}$ 即可.

Nguyen 等[77] 观察发现基于介数攻击在攻击后期效果变弱, 由此设计了一个约束条件, 即如果当前 (全局) 介数最高节点属于最大连通子图, 则攻击该节点; 否则攻击最大连通子图 (局部) 介数最大的节点.

作为最常用的攻击度量, 度数和介数经常一起用于攻击. Nie 等[76] 通过预先给度数最大和介数最大的节点分配权值来分配两者被攻击的概率, 即

$$p_i = \alpha \times \frac{k_i}{\sum\limits_{i=1}^{N} k_i} + \beta \times \frac{b_i}{\sum\limits_{i=1}^{N} b_i} \tag{21}$$

其中, k_i 和 b_i 分别为节点 i 的度数和介数, p_i 是攻击该节点的概率, α 和 β 为预先设定的权值. Gao 等[78] 将式 (21) 中的 β 替换为 $1-\alpha$. 进一步地, Hao 等[79] 设定了 3 个参数 α, β 和 γ 来控制度数、介数和谐波接近度 (Harmonic closeness) 在攻击中的权重. 这些攻击策略应用于互依网络 (Interdependent networks)[78−82]、网络的网络 (Networks of networks)[83−84] 以及加权网络 (Weighted networks)[85] 等.

研究发现, 基于度数的节点攻击[86] 比随机节点攻击更能有效地破坏随机网络和无标度网络的能控性. Lu 等[87] 发现节点攻击的破坏力大于连边攻击, 同时, 异质网络的能控性鲁棒性要劣于同质网络. 此外, 对于许多实际网络来说, 基于介数攻击对能控性破坏力最强[87].

对于本地世界网络 (Local-world network)[88−89], Sun 等[90] 发现基于度数的节点攻击对本地世界规模较大的网络更具破坏力, 而对本地世界规模小的网络破坏力较小. 文献 [90] 的研究包括连通鲁棒性和能控性鲁棒性. Lou 等[57] 以最大度数和最大介数为依据, 每次选取破坏程度较大的对象进行攻击. 基于负载 (介数) 的连边攻击[91] 能有效地破坏网络能控性. 连边攻击不仅能破坏连通性和能控性, 也能引起无标度网络的级联故障.

2.2.2 其他蓄意攻击

Wang 等[92] 提出的基于破坏力的攻击 (Damage-based attack) 以破坏程度作为选择攻击的度量, 即攻击带来破坏程度最大的节点. 这里的破坏程度以攻击前后 LCC 大小的变化来度量. Lou 等[57] 提出在每次攻击中找到度数和介数最大的节点, 选择带来破坏力较大的节点作为攻击对象, 该方法对能控性的破坏力接近于基于度数攻击和基于介数攻击的破坏力上限. 这类基于破坏程度的攻击要求攻击者具备比其他攻击更多的对攻击对象的知识.

基于模块的攻击 (Module-based attack) 策略[93−94] 旨在攻击具有多社区 (Community) 结构的网络中连接各社区的公共连边 (Inter-community edge), 从而达到破坏整体性能的效果. Ma 等[95] 让攻击与防御交替进行, 并以此优化网络结构.

Sun 等[61] 提出了基于关键连边的攻击策略. 该策略首选搜集网络中的所有关键连边, 将其存储于列表并优先攻击, 待列表中的关键连边全部攻击后, 采用随机攻击策略. 如图 6(a) 所示, 一条关键连边在一次攻击之后就可能转换成非关键连边. Lou 等[57] 在文献 [61] 的基础上, 提出了层级攻击 (Hierarchical attack): 层级连边攻击依次删除网络中的关键连边、亚关键连边和普通连边. 类似地, 层级节点攻击依次删除网络中的关键节点、亚关键节点、普通节点和冗余节点. 关键连边和节点的定义及举例见第 1.1.5 节. 同时, 连边和节点的层级划分在每次攻击后得到更新. 该方法计算复杂度较高但获得了有效的攻击效果.

2.3 启发式攻击

启发式算法 (Heuristic algorithm) 属于计算智能, 是一种用于解决 NP 难问题的有效方法, 常见的算法包括模拟退火算法 (Simulated annealing)、遗传算法 (Genetic algorithm)、禁忌搜索 (Tabu search)、粒子群算法 (Particle swarm optimization) 等.

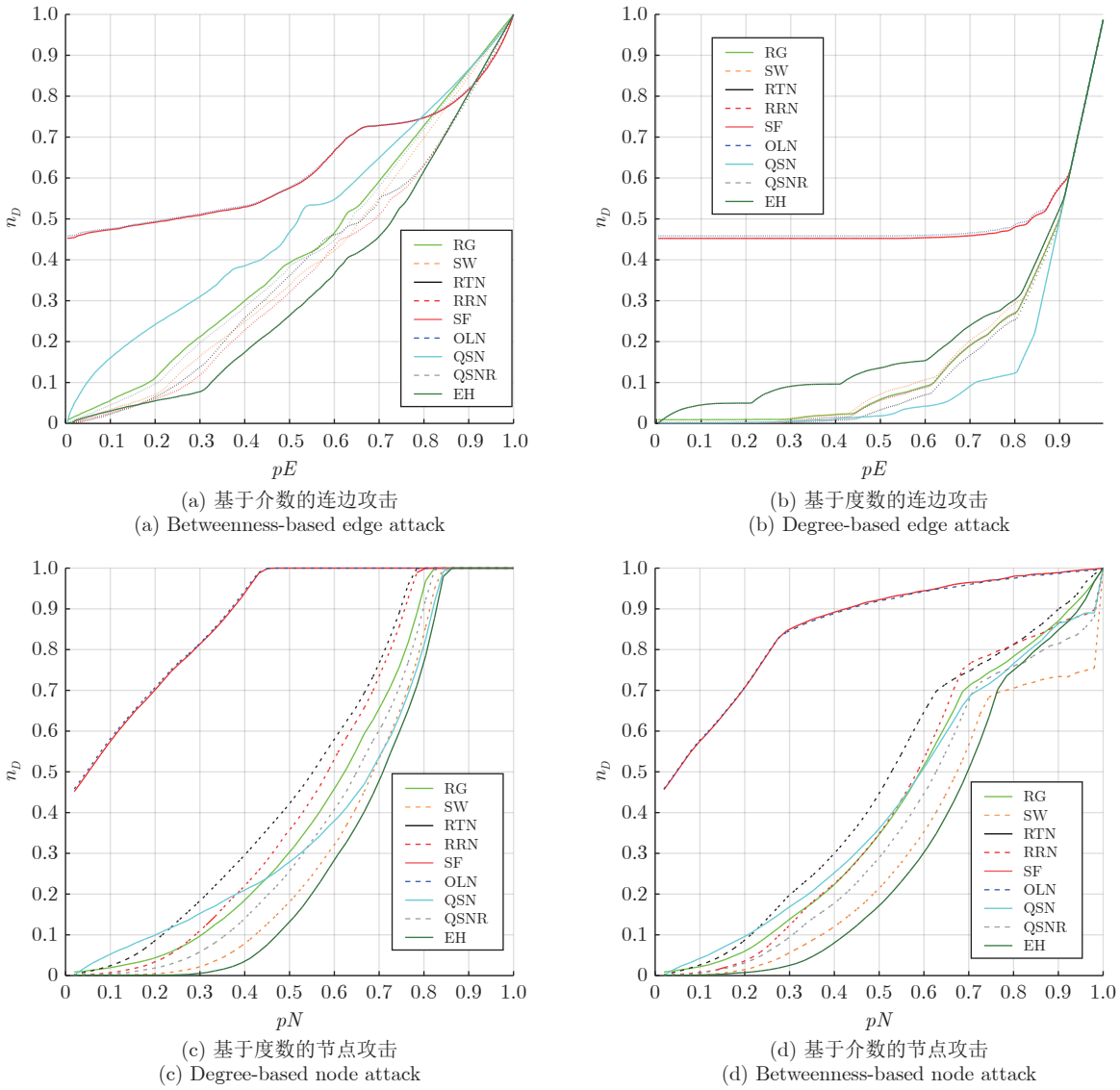
前述的随机攻击和蓄意攻击通过预设的策略逐个选取攻击节点或连边; 而启发式攻击则将整个攻击过程视作一个优化问题, 通过启发式算法搜索最优攻击序列 (即破坏效果最佳的攻击序列). 对于一个 N 节点网络, 其攻击序列的解空间大小为 $N!$; 对于一个 M 节点网络, 其攻击序列的解空间大小为 $M!$. 常用的编码方式为自然序号, 即预先按 1 到 N (或 M) 分别标记每个节点 (或连边), 通过选用适当的优化目标函数以达到优化攻击序列的效果. Zhang 等[96] 采用遗传算法, 以连边的自然序号作为遗传编码, 设计了可剔除重复基因的交叉和遗传算

子, 这里 “重复基因” 表示在同一个攻击序列中存在多个位置指向同一节点或连边. 孙昱等[97] 使用禁忌搜索最优攻击序列, 通过局部交换, 生成新的攻击序列, 如果该序列在禁忌列表中 (在一定时间范围内生成且已经评价的相同攻击序列), 则放弃该序列. 该算法的计算成本高, 适用于较小规模网络. Ventresca[98] 利用启发式算法搜索网络中的关键节点. Deng 等[99] 通过禁忌搜索关键节点集合, 提高网络解体的攻击效果, 该方法计算成本较高. Qi 等[100] 以禁忌搜索提高多层网络的分解效果. Lozano 等[101] 以网络中最大介数为目标函数, 通过人工蜂群算法 (Artificial bee colony) 来最小化这一目标函数, 从而优化攻击效果. Li 等[102] 以邻域信息增强随机算法搜索关键节点集合的能力, 显著提高攻击效率.

2.4 不同攻击下的能控性鲁棒性

本小节和第 3.2 节可视为同一问题的不同角度分析. 对于同一种网络在不同攻击下, 使其能控性下降最快速明显的攻击为最有效攻击; 将同一种攻击方式用于不同拓扑结构, 其中能控性保持最好的网络可视为能控性鲁棒性最好的拓扑结构.

图 7 给出了常见的 9 种网络模型在基于介数和度数的连边和节点攻击下的能控性曲线变化, 包括随机图网络 RG (Random graph)[103], 小世界网络 SW (Small-world)[104−105], 随机三角形网络 RTN (Random triangle network)[50, 106], 随机四边形网络 RRN (Random rectangular network)[50], 无标度网



(a) 基于介数的连边攻击
(a) Betweenness-based edge attack

(b) 基于度数的连边攻击
(b) Degree-based edge attack

(c) 基于度数的节点攻击
(c) Degree-based node attack

(d) 基于介数的节点攻击
(d) Betweenness-based node attack

图 7 常见的网络模型在攻击下的能控性曲线变化

Fig. 7 The controllability curves of 9 network topologies under 4 different attack strategies

络 SF (Scale-free)[107−108], 洋葱型网络 OLN (Onion-like network)[109−112], q-回路网络 QSN (q-snapback network)[113−114], q-回路及反向连边 QSNR (QSN with re-directed edges) 模型[115], 以及极同质 EH (Extremely homogeneous) 网络[116]. 图中 $pE = M_r/M$ 和 $pN = N_r/N$ 分别表示已被攻击的连边和节点的比例. 网络规模为节点数 $N = 1\,000$, 连边数 $M = 5\,000$, 所有数据来自 20 次攻击的平均结果.

由图可见, 极同质 EH 网络在图 7(a) 基于介数的连边攻击、图 7(c) 基于度数的节点攻击和图 7(d) 基于介数的节点攻击过程中, 始终保持所需控制节点比例较低, 相较于其他网络, EH 具有最佳能控性鲁棒性; 而在图 7(b) 基于度数的连边攻击中表现较差. 而无标度 SF 网络和洋葱型 OLN 网络则具有相似的能控性曲线, 两者均为能控性鲁棒性最差的网络结构. 在不同攻击下, 各网络表现出不同的能控性鲁棒性, 如 QSN 在图 7(a) 基于介数攻击下的能控性只优于 SF 和 OLN, 而劣于其他网络; 但在基于度数的连边攻击下, QSN 表现出最好的能控性鲁棒性, 尤其在攻击的中后期. 值得一提的是, 使用不同的连边度数定义也会影响比较结果.

3　能控性鲁棒性优化

能控性鲁棒性优化旨在提高复杂网络对各种攻击的抵御能力. 以第 1.3.1 节的度量为例, 定义如下.

定义 1. 一个复杂网络 G^* 称为能控性鲁棒性最优网络 (简称最优网络), 当且仅当

$$G^* = \arg\min_{G\in\Omega} R_c \tag{22}$$

成立, 其中, Ω 为适用解空间, 即所有满足约束条件的复杂网络 G 构成的解空间; R_c 可由式 (14) 或式 (15) 计算得到.

由于能控性鲁棒性优化属 NP 难问题, 而进化算法 (Evolutionary algorithm)[117−118] 和群智能算法[119] 等智能计算[120−121] 方法本身的计算代价较小, 其计算成本通常取决于待优化问题的评价. 因而, 智能计算方法常应用于这一优化问题.

网络模型优化设计和对网络进行重新连边为常用的能控性鲁棒性优化手段. 全齐网络拓扑结构在研究中认为是具有最优的能控性鲁棒性. 此外, 复杂网络中模体对保持网络能控性鲁棒性具有一定的促进作用. 表 1 列举了常见优化策略的优点与不足. 以下各小节针对这几个方面分别进行讨论.

3.1　网络模型优化设计

Yan 等基于同余论 (Congruence theory) 构造了同余网络 MCN (Multiplex congruence network)[122], 其生成方式如下: 首先对所有 N 节点进行 1 到 N 编号, 如果两个节点 i 和 j 满足:

$$j \equiv r \,(\mathrm{mod}\, i), \quad i < j \tag{23}$$

则存在一条连边 A_{ij}, 其中 r 为 j 除以 i 得到的余数. 相同余数的所有节点构成同于网络的一层. 同余网络的每一层是无标度网络, 属异质 (Heterogeneous) 网络, 其出度分布服从

$$p\left(k^{\mathrm{out}}\right) = \frac{1}{k^{\mathrm{out}}\left(k^{\mathrm{out}}+1\right)} \tag{24}$$

通常认为异质网络的能控性和能控性鲁棒性都较差[18, 50], 而同质 (Homogeneous) 网络的能控性和能控性鲁棒性都较好[18, 116]. 但是由于主链 ($r = 1$ 层) 的存在, 使得同余网络具有较好的能控性和能控性鲁棒性, 同时揭示了度分布非影响能控性鲁棒性的唯一原因.

Lou 等[113−114] 发现多链和多环结构有助于提高能控性鲁棒性, 提出了基于工业流水线的 q-回路网络 QSN, 由一条主链和若干回路构成, 回路的数量由参数 $q \in [0, 1]$ 控制. 其第 r ($r = 1, \cdots, N-1$) 层第 i ($i = 1, \cdots, N$) 节点的出度可由下式计算:

$$k_i^{\mathrm{out}} = \begin{cases} 1, & i \in [1, r] \\ 1 + q\left\lfloor \dfrac{i-1}{r} \right\rfloor, & i \in [r+1, N-1] \\ q\left\lfloor \dfrac{i-1}{r} \right\rfloor, & i = N \end{cases} \tag{25}$$

其中, $\lfloor\cdot\rfloor$ 表示下取整函数. QSN 网络的度均匀分布.

表 1　常用能控性鲁棒性优化策略的优点与不足

Table 1　Pros and cons of the strategies for controllability robustness optimization

优化策略	优点	不足
模型优化设计	基于特定理论, 模型简单易实现 (如同余论[122]、Henneberg[106] 理论)	容易受理论约束 (如同余论限制生成网络的度数不能任意调整)
重新连边	根据实际需求, 对网络结构做一定范围的调整	具有一定的随机性, 且通常需要较大的计算量
全齐网络	经验上的能控性鲁棒性最优结构	通常不符合实际网络特征与需求 (如交通网络无法设计为全齐网络)
模体	在优化设计或重新连边过程中, 刻意增加网络中特定模体的数量	不同模体对能控性鲁棒性的理论价值和意义有待进一步理清

q-回路及反向连边 QSNR 模型[115] 基于 QSN 模型, 同时加入随机反向连边, 并保证主链不受影响. QSNR 的度分布服从泊松分布. 虽然在不同攻击方式下, 各网络的能控性鲁棒性稍显不同, 整体而言, QSNR 和 QSN 优于 MCN, 其中 QSNR 又稍优于 QSN[115].

随机三角形网络 RTN[50, 106] 基于 Henneberg 增长, 由大量的有向三角形构成. 将其扩展到四边形, 就形成了随机四边形网络 RRN[50]. 在这两个模型中, 任意一个节点都至少处于一个三角形/四边形 (有向环) 当中. 这些多环结构的存在, 使它们的能控性鲁棒性较好.

极同质 EH 网络[116] 中任一节点 i ($i = 1, 2, \cdots, N$) 的出度和入度被限定在极小范围 $[\lfloor M/N \rfloor, \lceil M/N \rceil]$ 内, 也就是

$$\left\lfloor \frac{M}{N} \right\rfloor \leq k_i^{\text{out}},\ k_i^{\text{in}} \leq \left\lceil \frac{M}{N} \right\rceil \tag{26}$$

其中, $\lfloor \cdot \rfloor$ 和 $\lceil \cdot \rceil$ 分别表示上取整和下取整函数. 严格满足式 (26) 的网络即是极同质网络. 环是在 $N = M$ 情况下能控性鲁棒性最优的拓扑结构, 也是最简单的极同质网络.

3.2 不同网络拓扑结构的能控性鲁棒性比较

Chen 等[50] 以第 1.3.3 节基于排序的度量比较了包括随机图网络 RG[103]、无标度网络 SF[107−108]、同余网络 MCN[122]、q-回路网络 QSN[113−114]、随机三角形网络 RTN[50, 106] 和随机四边形网络 RRN[50] 等 6 种网络在 6 种不同攻击 (包括随机节点和随机连边攻击, 基于度数的节点和连边攻击, 以及基于介数的节点和连边攻击) 下的能控性鲁棒性, 发现 ER 和 RRN 能较好地抵御节点攻击, 而 RRN 和 RTN 能较好地抵御各种连边攻击.

文献 [115] 通过实验比较得出当反向连边概率为 0.5 时, QSNR 网络的能控性鲁棒性最佳, 此时 QSNR 的能控性鲁棒性优于 QSN.

现有研究证实, 极同质 EH 网络[116] 是在给定网络规模 (N 节点和 M 连边) 情况下, 能控性鲁棒性最优的结构 (如图 7 所示). 同时, Lou 等[116] 提出的随机连边矫正 RER (Random edge rectification) 策略, 可将任何网络结构, 改变为 EH 网络, 同时, 与 EH 网络越近似则该网络的能控性鲁棒性越好.

表 2 列举了几种能控性鲁棒性优化的网络结构. 这些网络都由优化设计得到, 其中 QSNR 和 EH 需要进行重新连边优化. 仅 EH 结构具有全齐属性. 除了 MCN 仅具有多链结构, 其余 5 种网络同时具有多链和多环结构.

表 2 能控性鲁棒性优化的网络结构

Table 2 Comparison of network topologies with optimized controllability robustness

网络结构	优化设计	重新连边	全齐网络	模体	
				链	环
MCN	√			√	
QSN	√			√	√
QSNR	√	√		√	√
RTN	√			√	√
RRN	√			√	√
EH	√	√	√	√	√

3.3 重新连边优化

重新连边 (Rewiring)[119] 通常分为 3 种形式: 1) 基于度保持 (Degree-preserving) 的重新连边: 保持各节点出度和入度不变, 重新调整连边; 2) 保持网络基本骨架不变, 对连边的方向进行调整; 3) 保持网络整体节点和连边数目不变, 对网络进行任意重构. 其中第 1 种方式为最常用的策略. 本小节只讨论前两种方式, 第 3 种将在第 3.4 节讨论. 不同的重新连边策略本质上是对式 (22) 的 Ω 进行了不同约束, 而优化的目标是相同的.

重新连边常用于连通鲁棒性的优化. 基于度保持的重新连边策略保持每个节点的出度和入度均不变, 即将连边 A_{ij} 和 A_{st} ($i \neq s$ 或 $j \neq t$) 重新连接为 A_{it} 和 A_{sj}, 从而保持节点 i 和 s 的出度不变; 节点 j 和 t 的入度不变. 异质网络 (例如无标度网络等) 在应用基于度保持的重新连边策略后, 网络趋于洋葱型 (Onion-like) 结构, 即度数相近的节点之间普遍连接, 同时抑制度数相差较大的节点之间的连接, 洋葱型网络具有较好的连通鲁棒性[36, 110−112, 123], 同时也能提高网络的 k-壳组成.

重新连边可看作优化问题, 基于不同的目标函数, 网络的优化趋向不同. Chan 等[65] 以谱度量[124−128] 为目标函数, 通过基于度保持的重新连边策略来优化连通鲁棒性. 谱度量是常用的用于估算和预测复杂网络连通鲁棒性的工具[129]. 然而, 目前尚未发现谱度量或其他复杂网络特征与能控性鲁棒性具有较强的相关性[49].

Xiao 等[130] 提出的基于度保持的重新连边策略首先选择特定度范围的 4 个节点, 然后交换其连边. 该方法在增强网络连通鲁棒性的同时, 也降低了网络同配性系数 (Assortativity coefficient)[131].

Louzada 等[132] 提出的智慧重新连边 (Smart rewiring) 策略通过增强枢纽节点的相邻节点之间的联系, 来增加网络抵御基于度数攻击的鲁棒性. 该方法假设枢纽节点为首要攻击目标, 很多情况下,

当枢纽节点遭受攻击后, 其相邻节点之间的联系随即消失. 通过智慧重连策略可使枢纽节点遭受攻击后, 网络仍保持较好的连通性.

启发式算法不仅应用于网络攻击 (见第 2.3 节), 同时也应用于优化复杂网络鲁棒性. 启发式算法包含一个种群的解, 其中每个解代表一个网络结构, 通过变异和交叉, 以适当地选择算子来引导解的演化趋势, 从而产生出高质量的解, 即鲁棒性好的网络结构.

Buesser 等[133] 用模拟退火 (Simulated annealing) 算法来优化网络连通鲁棒性. Zhou 等[134] 以式 (10) 作为目标函数, 用文化基因算法 (Memetic algorithm) 来优化无标度网络的连通鲁棒性.

由于抵御连边攻击的连通鲁棒性往往不能随着抵御节点攻击的鲁棒性的提高而提高[135], Zeng 等[135] 以混合贪婪算法 (Hybrid greedy algorithm) 来同时提高网络对抗节点攻击和连边攻击的连通鲁棒性. Liu 等[136] 提出了以多目标优化 (Multi-objective optimization) 来同时优化对抗节点攻击和连边攻击的鲁棒性. Wang 等[137] 以多目标优化, 同时优化网络的连通鲁棒性和抵御级联故障的鲁棒性. 多目标优化不仅可以优化网络的不同鲁棒性, 同时连通鲁棒性的多种度量也可以被同时优化[138]. Ma 等[95] 通过攻击和防守交替的策略提高网络鲁棒性, 其中防守策略是指通过随机、优先或平衡的方式来补充被攻击的节点或连边. 对于异质网络的连通鲁棒性优化来说, 一个普遍共同结果是产生洋葱型结构网络[37, 110−112].

与攻击方式一样, 已有研究大部分侧重于提高连通鲁棒性. 能控性鲁棒性的优化可借鉴连通鲁棒性的优化方法, 但是由于评价标准和优化目标的不同, 能控性鲁棒性的优化有其自身特点. 通过删除冗余连边和增加关键或普通连边的方式[139−140], 减少网络中非匹配节点数, 可以提高复杂网络能控性. Wang 等[141] 以合作者比例 (维持合作能力) 和式 (14) 所示能控性鲁棒性定义作为两个优化目标, 以多目标进化算法来同时优化它们.

Hou 等[142] 保持了网络的架构和规模 (节点数和连边数) 不变, 通过只改变连边的方向来优化能控性. Lou 等[115] 通过改变非主链连边的方向, 不仅将原先均匀度分布改变成泊松分布, 同时也增加了模体的数量和跨度, 提高了 QSN 的能控性鲁棒性. 虽然一般来讲, 同质网络较异质网络具有较好的能控性和鲁棒性, 但是同余网络的存在否定了这一共识结论[122]. 然而, Lou 等[116] 提出对于给定数量的节点和连边, 能控性鲁棒性最优的网络结构 (满足式 (22)) 应具有极同质结构, 即所有节点的出度和入度均相等 (或者其差值小于等于 1). Shi 等[143] 提出的全齐性 (Totally homogeneous) 网络给出了较极同质网络更为全面的数学定义, 且提出全齐性网络具有最优同步性等多种最优指标. 通常地, 多链结构和多环结构具有较好的能控性鲁棒性[50, 113, 115, 122].

3.4　全齐网络

基本的网络结构, 如链式、环式、星型等结构无法解决一些新涌现的网络问题, 如能控性网络子结构的设计和优化网络同步性等问题. Shi 等[143] 借鉴庞加莱的剖分思想, 把网络分解为全齐性子网络. 以团 (Clique) 为基本单位建立一系列二元域上的向量空间表述网络结构. 模型和实际网络中都存在大量全齐性子网络, 是支持网络功能的重要基础结构, 对网络同步性[144]、能控性[18, 33]、连通鲁棒性[37] 等具有重要意义. Fan 等[145] 研究了网络的圈结构, 提出刻画网络圈结构的边界矩阵和衡量节点重要性的圈指标.

Lou 等[116] 基于小规模网络的遍历搜索, 归纳了经验必要条件 ENC (Empirical necessary condition). ENC 指出满足式 (22) 的最优网络结构, 应满足式 (26). Lou 等[116] 发现对于给定 N 节点和 M 连边, 其所有网络结构、满足 ENC 的网络、以及最优网络之间的关系如图 8 所示.

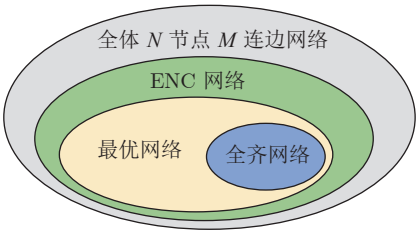


图 8　所有 N 节点和 M 连边网络, 满足 ENC 的网络、全齐网络, 以及最优网络之间的关系图

Fig. 8　The relationship diagram of the N-node M-edge networks, ENC networks, totally homogeneous networks, and the optimal networks

同时, Lou 等[116] 提出了随机连边矫正 RER (Random edge rectification) 策略, 该策略使复杂网络趋于满足式 (26) 的结构, 此外, 使用 RER 策略的次数与网络能控性鲁棒性的提高成正比. RER 属于第 3 种重新连边优化方式, 即保持网络整体节点数 N 和连边数 M 不变, 对网络进行 (任意) 重构, 以达到优化能控性鲁棒性的目的.

经验地, 全齐网络满足 ENC 条件, 同时也是最优网络; 然而显然并非所有的最优网络都属于全齐网络, 其关系如图 8 所示.

3.5 模体

模体 (Motif)[146] 是复杂网络中高频出现的具有统计意义的导出子图. 近年来模体的研究广泛深入到各个领域, 如电力系统网络[147] 和大肠杆菌代谢网络[148] 等. 在网络控制方面, Badhwar 等[149] 发现秀丽线虫神经元网络中, 前馈模体的数量对能控性的影响较大. Dey 等[150] 研究了不同攻击策略下网络中模体的变化情况, 并分析了欧洲国家的电力系统网络的连通鲁棒性差异. 贾承丰等[151] 提出了基于模体的攻击策略, 仿真结果表明基于模体攻击对模体特征明显的网络可造成的更大损害.

同余网络 MCN[122] 中存在较多链式模体结构. 每一条链仅用一个控制器即可保证链路能控性. 在受到攻击时, 针对驱动节点的攻击不会破坏链路能控性; 反而随机攻击更容易造成链路断裂, 从而增加额外控制器. Lou 等[113] 进一步将链式模体扩展至环式模体. 环式模体的反馈连接比链式的前馈连接具有更好的能控性鲁棒性. QSN 网络中含有大量的链式和环式模体[113]. 多模体结构的 QSN 和 MCN 在抵御攻击方面优于一般的无标度网络. 进一步地, 对 QSN 的非主链连边随机反向重连可增加 3-环、4-环和 4-链 (n-环/链指由 n 个节点构成的环/链) 结构, 增强了能控性鲁棒性.

Chen 等[50] 比较了具有链式模体的 MCN, 具有环式模体的 QSN, 以 3-环为基础结构 RTN, 以 4-环为基础结构的 RRN 等在不同攻击下的能控性鲁棒性, 发现 3-环和 4-环的 RRN 和 RTN 结构在各种连边攻击下, 保持较好的能控性.

4 展望与总结

本文围绕 3 个问题进行归纳与总结:

1) 复杂网络能控性鲁棒性的定义和度量. 不同的定义因侧重点不同而稍有区别, 须根据实际应用场景选取适当的定义和度量方式.

2) 常见的复杂网络攻击方式及其对网络连通性和能控性的危害. 随机攻击的危害较小, 对攻击者来说需要掌握的网络相关信息较少; 基于特征的蓄意攻击依据预先设定的特征对网络的节点或连边实施攻击, 取得的攻击效果往往较好, 对攻击者来说需要掌握较多网络相关信息; 启发式攻击以智能计算优化攻击, 往往需要具备较全面的网络相关信息和较多的计算资源, 同时攻击效果的提升也较为显著.

3) 能控性鲁棒性的优化问题. 对于尚未建立的网络可采取优化建模, 对于已有网络可采取 (全部或部分) 重新连边策略. 如果能够掌握攻击者的信息, 则可更有效地针对某一类攻击做出防御. 一般的, 在各类攻击情况下, 极同质网络具有较好的能控性鲁棒性.

针对以上 3 个问题, 未来可研究内容包括:

1) 深度学习和计算智能可更广泛地应用于复杂网络能控性鲁棒性的预测、分析和优化. 目前, 利用深度学习预测复杂网络能控性鲁棒性的研究和利用计算智能来生成优化网络拓扑结构的研究处于起步阶段. 深度学习和计算智能处理大规模问题能力的进一步发展, 将会对包括能控性鲁棒性在内的复杂网络各项研究带来新的机遇和挑战.

2) 相关网络特征与能控性鲁棒性的相关性值得进一步探索和研究, 包括相关拓扑结构特征、关键节点和关键连边的定义与搜索等. 这一研究方向的难点在于网络规模、拓扑结构、攻击方式等同时具有多样性. 同时, 在实际网络中, 各节点和连边存在权值等因素, 因此, 相对不容易形成一般性可泛化的理论结果.

3) 全齐性网络和经验必要条件的进一步研究和理论拓展. 全齐性网络和经验必要条件的研究从简单结构开始, 逐步推向一般情况, 简单的网络拓扑结构比一般实际网络更容易研究分析, 实现理论突破. 对经验必要条件的理论证明, 以及对经验和理论充分条件的探索, 将从理论上实现复杂网络能控性鲁棒性的最优化.

附录 A 本文所用符号列表

A	邻接矩阵
A_{ij}	邻接矩阵中节点 i 和 j 之间的连边
b_i	节点 i 的介数
B	输入矩阵
C	能控性矩阵
$\mathcal{E}$	网络连边集合
G	复杂网络
k_i	节点 i 的度数
k_i^{out}	节点 i 的出度
k_i^{in}	节点 i 的入度
M	网络连边数
M_c	关键连边数
M_r	当前已攻击的连边数
N	网络节点数
N_D	网络所需控制节点数
ΔN_D	网络所需控制节点数增量
N_r	当前已攻击的节点数
n_D	网络所需控制节点密度
$p(M_c)$	关键连边比例
R_c	平均能控性鲁棒性

R_{LCC}	平均连通鲁棒性
$\boldsymbol{u}$	控制向量
$\mathcal{V}$	网络节点集合
$\boldsymbol{x}$	状态向量
σ_{ij}	从节点 i 到 j 的最短路径
Ω	适用解空间

References

1 Barabási A L. *Network Science*. Cambridge: Cambridge University Press, 2016.

2 Newman M E J. *Networks: An Introduction*. Oxford: Oxford University Press, 2010.

3 Chen G R, Wang X F, Li X. *Fundamentals of Complex Networks: Models, Structures and Dynamics*. John Wiley & Sons, 2014.

4 Wang Xiao-Fan, Li Xiang, Chen Guan-Rong. *Complex Network Theory and Its Applications*. Beijing: Tsinghua University Press, 2006.
(汪小帆, 李翔, 陈关荣. 复杂网络理论及其应用. 清华大学出版社, 2006.)

5 Chen D X, Shao Q, Liu Z Y, Yu W W, Chen C L P. Ride-sourcing behavior analysis and prediction: A network perspective. *IEEE Transactions on Intelligent Transportation Systems*, 2022, **23**(2): 1274−1283

6 Chen G R, Lou Y. *Naming Game: Models, Simulations and Analysis*. Cham: Springer, 2019.

7 Ding Y. Scientific collaboration and endorsement: Network analysis of coauthorship and citation networks. *Journal of Informetrics*, 2011, **5**(1): 187−203

8 Davis K F, D′Odorico P, Laio F, Ridolfi L. Global spatio-temporal patterns in human migration: A complex network perspective. *PLoS One*, 2013, **8**(1): e53723

9 Xiong Xi, Qiao Shao-Jie, Wu Tao, Wu Yue, Han Nan, Zhang Hai-Qing. Spatio-temporal feature based emotional contagion analysis and prediction model for online social networks. *Acta Automatica Sinica*, 2018, **44**(12): 2290−2299
(熊熙, 乔少杰, 吴涛, 吴越, 韩楠, 张海清. 基于时空特征的社交网络情绪传播分析与预测模型. 自动化学报, 2018, **44**(12): 2290−2299)

10 Lou Y, Chen G R. Analysis of the "naming game" with learning errors in communications. *Scientific Reports*, 2015, **5**: 12191

11 Lou Y, Chen G R, Hu J W. Communicating with sentences: A multi-word naming game model. *Physica A: Statistical Mechanics and Its Applications*, 2018, **490**: 857−868

12 Lou Y, Chen G R, Fan Z P, Xiang L N. Local communities obstruct global consensus: Naming game on multi-local-world networks. *Physica A: Statistical Mechanics and Its Applications*, 2018, **492**: 1741−1752

13 Huang Chun-Lin, Liu Xing-Wu, Deng Ming-Hua, Zhou Yang, Bu Dong-Bo. A survey on algorithms for epidemic source identification on complex networks. *Chinese Journal of Computers*, 2018, **41**(6): 1376−1399
(黄春林, 刘兴武, 邓明华, 周杨, 卜东波. 复杂网络上疾病传播溯源算法综述. 计算机学报, 2018, **41**(6): 1376−1399)

14 Kabir K M A, Kuga K, Tanimoto J. Analysis of SIR epidemic model with information spreading of awareness. *Chaos, Solitons and Fractals*, 2019, **119**: 118−125

15 Firth J A, Hellewell J, Klepac P, Kissler S, CMMID COVID-19 Working Group, Kucharski A J, Spurgin L G. Using a real-world network to model localized COVID-19 control strategies. *Nature Medicine*, 2020, **26**(10): 1616−1622

16 Zhang Y F, Wu G, Liu X L, Yu W W, Chen D X. Maximum Markovian order detection for collective behavior. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2020, **30**(8): 083121

17 Chen D X, Liu X L, Xu B W, Zhang H T. Intermittence and connectivity of interactions in pigeon flock flights. *Scientific Reports*, 2017, **7**(1): 10452

18 Liu Y Y, Slotine J J, Barabási A L. Controllability of complex networks. *Nature*, 2011, **473**(7346): 167−173

19 Wang W X, Ni X, Lai Y C, Grebogi C. Optimizing controllability of complex networks by minimum structural perturbations. *Physical Review E*, 2012, **85**(2): 026115

20 Yuan Z Z, Zhao C, Di Z R, Wang W X, Lai Y C. Exact controllability of complex networks. *Nature Communications*, 2013, **4**: 2447

21 Pósfai M, Liu Y Y, Slotine J J, Barabási A L. Effect of correlations on network controllability. *Scientific Reports*, 2013, **3**: 1067

22 Menichetti G, Dall′Asta L, Bianconi G. Network controllability is determined by the density of low in-degree and out-degree nodes. *Physical Review Letters*, 2014, **113**(7): 078701

23 Zhou Tao, Zhang Zi-Ke, Chen Guan-Rong, Wang Xiao-Fan, Shi Ding-Hua, Di Zeng-Ru, et al. The opportunities and challenges of complex networks research. *Journal of University of Electronic Science and Technology of China*, 2014, **43**(1): 1−5
(周涛, 张子柯, 陈关荣, 汪小帆, 史定华, 狄增如, 等. 复杂网络研究的机遇与挑战. 电子科技大学学报, 2014, **43**(1): 1−5)

24 Hou Lv-Lin, Lao Song-Yang, Xiao Yan-Dong, Bai Liang. Recent progress in controllability of complex network. *Acta Physica Sinica*, 2015, **64**(18): 188901
(侯绿林, 老松杨, 肖延东, 白亮. 复杂网络可控性研究现状综述. 物理学报, 2015, **64**(18): 188901)

25 Nie Sen. Research on Controllability of Complex Networks [Ph.D. dissertation], University of Science and Technology of China, China, 2015.
(聂森. 复杂网络可控性研究 [博士学位论文], 中国科学技术大学, 中国, 2015.)

26 Motter A E. Networkcontrology. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2015, **25**(9): 097621

27 Wang L, Chen G R, Wang X F, Tang W K S. Controllability of networked MIMO systems. *Automatica*, 2016, **69**: 405−409

28 Liu Y Y, Barabási A L. Control principles of complex systems. *Reviews of Modern Physics*, 2016, **88**(3): 035006

29 Wang L, Wang X F, Chen G R. Controllability of networked higher-dimensional systems with one-dimensional communication. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2017, **375**(2088): 20160215

30 Wang L Z, Chen Y Z, Wang W X, Lai Y C. Physical controllability of complex networks. *Scientific Reports*, 2017, **7**: 40198

31 Zhang Y, Zhou T. Controllability analysis for a networked dynamic system with autonomous subsystems. *IEEE Transactions on Automatic Control*, 2017, **62**(7): 3408−3415

32 Xiang L Y, Chen F, Ren W, Chen G R. Advances in network controllability. *IEEE Circuits and Systems Magazine*, 2019, **19**(2): 8−32

33 Duan Guang-Ren. High-order system approaches: Ⅱ. Controllability and full-actuation. *Acta Automatica Sinica*, 2020, **46**(8): 1571−1581
(段广仁. 高阶系统方法-Ⅱ. 能控性与全驱性. 自动化学报, 2020, **46**(8): 1571−1581)

34 Chen G R. Pinning control and synchronization on complex dynamical networks. *International Journal of Control, Automation and Systems*, 2014, **12**(2): 221−230

35 Holme P, Kim B J, Yoon C N, Han S K. Attack vulnerability

of complex networks. *Physical Review E*, 2002, **65**(5): 056109

36 Shargel B, Sayama H, Epstein I R, Bar-Yam Y. Optimization of robustness and connectivity in complex networks. *Physical Review Letters*, 2003, **90**(6): 068701

37 Schneider C M, Moreira A A, Andrade J S Jr, Havlin S, Herrmann H J. Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences of the United States of America*, 2011, **108**(10): 3838−3841

38 Liu Y Y, Slotine J J, Barabási A L. Control centrality and hierarchical structure in complex networks. *PLoS One*, 2012, **7**(9): e44459

39 Bashan A, Berezin Y, Buldyrev S V, Havlin S. The extreme vulnerability of interdependent spatially embedded networks. *Nature Physics*, 2013, **9**(10): 667−672

40 Xiao Y D, Lao S Y, Hou L L, Bai L. Optimization of robustness of network controllability against malicious attacks. *Chinese Physics B*, 2014, **23**(11): 118902

41 Li Wen-Feng, Fu Xiu-Wen. Survey on invulnerability of wireless sensor networks. *Chinese Journal of Computers*, 2015, **38**(3): 625−647
(李文锋, 符修文. 无线传感器网络抗毁性. 计算机学报, 2015, **38**(3): 625−647)

42 Dong Zheng-Cheng, Fang Yan-Jun, Tian Meng. Review on invulnerability of interdependent networks. *Complex Systems and Complexity Science*, 2017, **14**(3): 30−44
(董政呈, 方彦军, 田猛. 相互依存网络抗毁性研究综述. 复杂系统与复杂性科学, 2017, **14**(3): 30−44)

43 Wang Er-Shen, Wang Yu-Wei, Pang Tao, Qu Ping-Ping, Jiang Yi. Research on robustness of complex networks with edge′s attack cost. *Acta Electronica Sinica*, 2018, **46**(5): 1166−1172
(王尔申, 王玉伟, 庞涛, 曲萍萍, 姜毅. 基于边攻击成本的复杂网络鲁棒性研究. 电子学报, 2018, **46**(5): 1166−1172)

44 Zhao Zhi-Gang, Zhou Gen-Gui, Du Hui. Research on cascading invulnerability of complex weighted supply chain networks. *Journal of Chinese Computer Systems*, 2019, **40**(12): 2591−2596
(赵志刚, 周根贵, 杜辉. 复杂加权供应链网络级联抗毁性研究. 小型微型计算机系统, 2019, **40**(12): 2591−2596)

45 Wang Zhe, Li Jian-Hua, Kang Dong, Ran Hao-Dan. Review on strategies enhancing the robustness of complex network. *Complex Systems and Complexity Science*, 2020, **17**(3): 1−26
(王哲, 李建华, 康东, 冉昊丹. 复杂网络鲁棒性增强策略研究综述. 复杂系统与复杂性科学, 2020, **17**(3): 1−26)

46 Yan G, Vértes P E, Towlson E K, Chew Y L, Walker D S, Schafer W R, Barabási A L. Network control principles predict neuron function in the *Caenorhabditis elegans* connectome. *Nature*, 2017, **550**(7677): 519−523

47 Liu J, Zhou M X, Wang S, Liu P H. A comparative study of network robustness measures. *Frontiers of Computer Science*, 2017, **11**(4): 568−584

48 Tan Yue-Jin, Wu Jun, Deng Hong-Zhong. Progress in invulnerability of complex networks. *Journal of University of Shanghai for Science and Technology*, 2011, **33**(6): 653−668
(谭跃进, 吴俊, 邓宏钟. 复杂网络抗毁性研究进展. 上海理工大学学报, 2011, **33**(6): 653−668)

49 Yamashita K, Yasuda Y, Nakamura R, Ohsaki H. On the predictability of network robustness from spectral measures. In: Proceedings of the 43rd IEEE Annual Computer Software and Applications Conference (COMPSAC). Milwaukee, USA: IEEE, 2019. 24−29

50 Chen G R, Lou Y, Wang L. A comparative study on controllability robustness of complex networks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2019, **66**(5): 828−832

51 Li X Y, Zhang Z J, Liu J M, Gai K K. A new complex network robustness attack algorithm. In: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure. Auckland, New Zealand: Association for Computing Machinery, 2019. 13−17

52 Lou Y, He Y D, Wang L, Chen G R. Predicting network controllability robustness: A convolutional neural network approach. *IEEE Transactions on Cybernetics*, 2022, **52**(5): 4052−4063

53 Fan C J, Zeng L, Sun Y Z, Liu Y Y. Finding key players in complex networks through deep reinforcement learning. *Nature Machine Intelligence*, 2020, **2**(6): 317−324

54 Kalman R E. On the general theory of control systems. In: Proceedings of the 1st International Conference on Automatic Control. Moscow, 1960. 481−492

55 Ding J, Lu Y Z. Control backbone: An index for quantifying a node′s importance for the network controllability. *Neurocomputing*, 2015, **153**: 309−318

56 Hosoe S. Determination of generic dimensions of controllable subspaces and its application. *IEEE Transactions on Automatic Control*, 1980, **25**(6): 1192−1196

57 Lou Y, Wang L, Chen G R. A framework of hierarchical attacks to network controllability. *Communications in Nonlinear Science and Numerical Simulation*, 2021, **98**: 105780

58 Usman U, Mahmood A, Wang L. Robust control centrality. In: Proceedings of the 2019 Chinese Control Conference (CCC). Guangzhou, China: IEEE, 2019. 5486−5491

59 Annamalai C. Finding perfect matchings in bipartite hypergraphs. In: Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms. Arlington, USA: Society for Industrial and Applied Mathematics, 2016. 1814−1823

60 Williams V V. Multiplying matrices faster than coppersmith-winograd. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing. New York, USA: Association for Computing Machinery, 2012. 887−898

61 Sun P, Kooij R E, He Z D, Van Mieghem P. Quantifying the robustness of network controllability. In: Proceedings of the 4th International Conference on System Reliability and Safety (ICSRS). Rome, Italy: IEEE, 2019. 66−76

62 Lin Jing-Dong, Wu Xin-Yi, Chai Yi, Yin Hong-Peng. Structure optimization of convolutional neural networks: A survey. *Acta Automatica Sinica*, 2020, **46**(1): 24−37
(林景栋, 吴欣怡, 柴毅, 尹宏鹏. 卷积神经网络结构优化综述. 自动化学报, 2020, **46**(1): 24−37)

63 Lou Y, He Y D, Wang L, Tsang K F, Chen G R. Knowledge-based prediction of network controllability robustness. *IEEE Transactions on Neural Networks and Learning Systems*, 2022, **33**(10): 5739−5750

64 Lou Y, He Y D, Wang L, Tsang K F, Chen G R. Predicting the robustness of undirected network controllability. In: Proceedings of the 39th Chinese Control Conference (CCC). Shenyang, China: IEEE, 2020. 4550−4553

65 Chan H, Akoglu L. Optimizing network robustness by edge rewiring: A general framework. *Data Mining and Knowledge Discovery*, 2016, **30**(5): 1395−1425

66 Yan G, Martinez N D, Liu Y Y. Degree heterogeneity and stability of ecological networks. *Journal of the Royal Society Interface*, 2017, **14**(131): 20170189

67 Wang S, Liu J, Jin Y C. Surrogate-assisted robust optimization of large-scale networks based on graph embedding. *IEEE Transactions on Evolutionary Computation*, 2020, **24**(4): 735−749

68 Ruan Yi-Run, Lao Song-Yang, Wang Jun-De, Bai Liang, Chen Li-Dong. Node importance measurement based on neighborhood similarity in complex network. *Acta Physica Sinica*, 2017, **66**(3): 038902
(阮逸润, 老松杨, 王竣德, 白亮, 陈立栋. 基于领域相似度的复杂网络节点重要度评估算法. 物理学报, 2017, **66**(3): 038902)

69 Šimon M, Luptáková I D, Huraj L, Hostovecký M, Pospíchal J.

Combined heuristic attack strategy on complex networks. *Mathematical Problems in Engineering*, 2017, **2017**: 6108563

70 Yang H H, An S. Critical nodes identification in complex networks. *Symmetry*, 2020, **12**(1): 123

71 Wu-Yan E, Betzel R F, Tang E, Gu S, Pasqualetti F, Bassett D S. Benchmarking measures of network controllability on canonical graph models. *Journal of Nonlinear Science*, 2020, **30**(5): 2195−2233

72 Zhang R, Wang X M, Cheng M, Jia T. The evolution of network controllability in growing networks. *Physica A: Statistical Mechanics and Its Applications*, 2019, **520**: 257−266

73 Hao Y Q, Duan Z S, Chen G R. Further on the controllability of networked MIMO LTI systems. *International Journal of Robust and Nonlinear Control*, 2018, **28**(5): 1778−1788

74 Bröhl T, Lehnertz K. Centrality-based identification of important edges in complex networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2019, **29**(3): 033115

75 Thomas J, Ghosh S, Parek D, Ruths D, Ruths J. Robustness of network controllability to degree-based edge attacks. In: Proceedings of the 5th International Workshop on Complex Networks and their Applications. Milan, Italy: Springer, 2017. 525−537

76 Nie T Y, Guo Z, Zhao K, Lu Z M. New attack strategies for complex networks. *Physica A: Statistical Mechanics and Its Applications*, 2015, **424**: 248−253

77 Nguyen Q, Pham H D, Cassi D, Bellingeri M. Conditional attack strategy for real-world complex networks. *Physica A: Statistical Mechanics and Its Applications*, 2019, **530**: 121561

78 Gao Y L, Chen S M, Nie S, Ma F, Guan J J. Robustness analysis of interdependent networks under multiple-attacking strategies. *Physica A: Statistical Mechanics and Its Applications*, 2018, **496**: 495−504

79 Hao Y C, Jia L M, Wang Y H. Edge attack strategies in interdependent scale-free networks. *Physica A: Statistical Mechanics and Its Applications*, 2020, **540**: 122759

80 Huang X Q, Gao J X, Buldyrev S V, Havlin S, Stanley H E. Robustness of interdependent networks under targeted attack. *Physical Review E*, 2011, **83**(6): 065101

81 Dong G G, Gao J X, Tian L X, Du R J, He Y H. Percolation of partially interdependent networks under targeted attack. *Physical Review E*, 2012, **85**(1): 016112

82 Cui P S, Zhu P D, Wang K, Xun P, Xia Z Q. Enhancing robustness of interdependent network by adding connectivity and dependence links. *Physica A: Statistical Mechanics and Its Applications*, 2018, **497**: 185−197

83 Dong G G, Gao J X, Du R J, Tian L X, Stanley H E, Havlin S. Robustness of network of networks under targeted attack. *Physical Review E*, 2013, **87**(5): 052804

84 Liu X M, Peng H, Gao J X. Vulnerability and controllability of networks of networks. *Chaos, Solitons and Fractals*, 2015, **80**: 125−138

85 Bellingeri M, Cassi D. Robustness of weighted networks. *Physica A: Statistical Mechanics and Its Applications*, 2018, **489**: 47−55

86 Pu C L, Pei W J, Michaelson A. Robustness analysis of network controllability. *Physica A: Statistical Mechanics and Its Applications*, 2012, **391**(18): 4420−4425

87 Lu Z M, Li X F. Attack vulnerability of network controllability. *PLoS One*, 2016, **11**(9): e0162289

88 Li X, Chen G R. A local-world evolving network model. *Physica A: Statistical Mechanics and Its Applications*, 2003, **328**(1−2): 274−286

89 Fan Z P, Chen G R, Zhang Y N. A comprehensive multi-local-world model for complex networks. *Physics Letters A*, 2009, **373**(18−19): 1601−1605

90 Sun S W, Ma Y L, Wu Y F, Wang L, Xia C Y. Towards structural controllability of local-world networks. *Physics Letters A*, 2016, **380**(22−23): 1912−1917

91 Nie S, Wang X W, Zhang H F, Li Q L, Wang B H. Robustness of controllability for networks based on edge-attack. *PLoS One*, 2014, **9**(2): e89066

92 Wang H, Huang J Y, Xu X M, Xiao Y H. Damage attack on complex networks. *Physica A: Statistical Mechanics and Its Applications*, 2014, **408**: 134−148

93 da Cunha B R, González-Avella J C, Gonçalves S. Fast fragmentation of networks using module-based attacks. *PLoS One*, 2015, **10**(11): e0142824

94 Shai S, Kenett D Y, Kenett Y N, Faust M, Dobson S, Havlin S. Critical tipping point distinguishing two types of transitions in modular network structures. *Physical Review E*, 2015, **92**(6): 062805

95 Ma L L, Liu J, Duan B P. Evolution of network robustness under continuous topological changes. *Physica A: Statistical Mechanics and Its Applications*, 2016, **451**: 623−631

96 Zhang X K, Wu J, Wang H, Xiong J, Yang K W. Optimization of disintegration strategy for multi-edges complex networks. In: Proceedings of the 2016 IEEE Congress on Evolutionary Computation (CEC). Vancouver, Canada: IEEE, 2016. 522−528

97 Sun Yu, Yao Pei-Yang, Zhang Jie-Yong, Fu Kai. Node attack strategy of complex networks based on optimization theory. *Journal of Electronics and Information Technology*, 2017, **39**(3): 518−524
(孙昱, 姚佩阳, 张杰勇, 付凯. 基于优化理论的复杂网络节点攻击策略. 电子与信息学报, 2017, **39**(3): 518−524)

98 Ventresca M. Global search algorithms using a combinatorial unranking-based problem representation for the critical node detection problem. *Computers and Operations Research*, 2012, **39**(11): 2763−2775

99 Deng Y, Wu J, Tan Y J. Optimal attack strategy of complex networks based on tabu search. *Physica A: Statistical Mechanics and Its Applications*, 2016, **442**: 74−81

100 Qi M Z, Deng Y, Deng H Z, Wu J. Optimal disintegration strategy in multiplex networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2018, **28**(12): 121104

101 Lozano M, García-Martínez C, Rodríguez F J, Trujillo H M. Optimizing network attacks by artificial bee colony. *Information Sciences*, 2017, **377**: 30−50

102 Li Q, Liu S Y, Yang X S. Neighborhood information-based probabilistic algorithm for network disintegration. *Expert Systems with Applications*, 2020, **139**: 112853

103 Erdös P, Rényi A. On the evolution of random graphs. *Mathematical Institute of the Hungarian Academy of Sciences*, 1960, **5**: 17−61

104 Newman M E J, Watts D J. Renormalization group analysis of the small-world network model. *Physics Letters A*, 1999, **263**(4−6): 341−346

105 Watts D J, Strogatz S H. Collective dynamics of "small-world" networks. *Nature*, 1998, **393**(6684): 440−442

106 Yang D, Liu M Y, Zhang Y C, Lin D, Fan Z P, Chen G R. Henneberg growth of social networks: Modeling the Facebook. *IEEE Transactions on Network Science and Engineering*, 2020, **7**(2): 701−712

107 Goh K I, Kahng B, Kim D. Universal behavior of load distribution in scale-free networks. *Physical Review Letters*, 2001, **87**(27): 278701

108 Sorrentino F. Effects of the network structural properties on its controllability. *Chaos: An Interdisciplinary Journal of Nonlin-*

ear Science, 2007, **17**(3): 033101

109 Herrmann H J, Schneider C M, Moreira A A, Andrade J S Jr, Havlin S. Onion-like network topology enhances robustness against malicious attacks. *Journal of Statistical Mechanics: Theory and Experiment*, 2011, **2011**: P01027

110 Wu Z X, Holme P. Onion structure and network robustness. *Physical Review E*, 2011, **84**(2): 026106

111 Tanizawa T, Havlin S, Stanley H E. Robustness of onionlike correlated networks against targeted attacks. *Physical Review E*, 2012, **85**(4): 046109

112 Hayashi Y, Uchiyama N. Onion-like networks are both robust and resilient. *Scientific Reports*, 2018, **8**(1): 11241

113 Lou Y, Wang L, Chen G R. Toward stronger robustness of network controllability: A snapback network model. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2018, **65**(9): 2983−2991

114 Lou Y, Wang L, Chen G R. Local diversity-stability of the q-snapback network model. *Physica A: Statistical Mechanics and Its Applications*, 2019, **536**: 121020

115 Lou Y, Wang L, Chen G R. Enhancing controllability robustness of q-snapback networks through redirecting edges. *Research*, 2019, **2019**: 7857534

116 Lou Y, Wang L, Tsang K F, Chen G R. Towards optimal robustness of network controllability: An empirical necessary condition. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2020, **67**(9): 3163−3174

117 Eiben A E, Smith J. From evolutionary computation to the evolution of things. *Nature*, 2015, **521**(7553): 476−482

118 Ding Qing-Feng, Yin Xiao-Yu. Research survey of differential evolution algorithms. *CAAI Transactions on Intelligent Systems*, 2017, **12**(4): 431−442
(丁青锋, 尹晓宇. 差分进化算法综述. 智能系统学报, 2017, **12**(4): 431−442)

119 Lou Y, Xie S L, Chen G R. Searching better rewiring strategies and objective functions for stronger controllability robustness. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2021, **68**(6): 2112−2116

120 Lin Shi-Jie, Dong Chen, Chen Ming-Zhi, Zhang Fan, Chen Jing-Hui. Summary of new group intelligent optimization algorithms. *Computer Engineering and Applications*, 2018, **54**(12): 1−9
(林诗洁, 董晨, 陈明志, 张凡, 陈景辉. 新型群智能优化算法综述. 计算机工程与应用, 2018, **54**(12): 1−9)

121 Lou Y, Yuen S Y, Chen G R. Non-revisiting stochastic search revisited: Results, perspectives, and future directions. *Swarm and Evolutionary Computation*, 2021, **61**: 100828

122 Yan X Y, Wang W X, Chen G R, Shi D H. Multiplex congruence network of natural numbers. *Scientific Reports*, 2016, **6**: 23714

123 Bai L, Xiao Y D, Hou L L, Lao S Y. Smart rewiring: Improving network robustness faster. *Chinese Physics Letters*, 2015, **32**(7): 078901

124 Wu J, Barahona M, Tan Y J, Deng H Z. Natural connectivity of complex networks. *Chinese Physics Letters*, 2010, **27**(7): 078902

125 Chakrabarti D, Wang Y, Wang C X, Leskovec J, Faloutsos C. Epidemic thresholds in real networks. *ACM Transactions on Information and System Security*, 2008, **10**(4): 1

126 Estrada E, Hatano N, Benzi M. The physics of communicability in complex networks. *Physics Reports*, 2012, **514**(3): 89−119

127 Fiedler M. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 1973, **23**(2): 298−305

128 Ghosh A, Boyd S, Saberi A. Minimizing effective resistance of a graph. *SIAM Review*, 2008, **50**(1): 37−66

129 Wu J, Barahona M, Tan Y J, Deng H Z. Spectral measure of structural robustness in complex networks. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 2011, **41**(6): 1244−1252

130 Xiao S, Xiao G, Cheng T H, Ma S, Fu X, Soh H. Robustness of scale-free networks under rewiring operations. *Europhysics Letters*, 2010, **89**(3): 38002

131 Newman M E J. Mixing patterns in networks. *Physical Review E*, 2003, **67**(2): 026126

132 Louzada V H P, Daolio F, Herrmann H J, Tomassini M. Smart rewiring for network robustness. *Journal of Complex Networks*, 2013, **1**(2): 150−159

133 Buesser P, Daolio F, Tomassini M. Optimizing the robustness of scale-free networks with simulated annealing. In: Proceedings of the 10th International Conference on Adaptive and Natural Computing Algorithms. Ljubljana, Slovenia: Springer, 2011. 167−176

134 Zhou M X, Liu J. A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks. *Physica A: Statistical Mechanics and Its Applications*, 2014, **410**: 131−143

135 Zeng A, Liu W P. Enhancing network robustness against malicious attacks. *Physical Review E*, 2012, **85**(6): 066130

136 Liu J, Abbass H A, Tan K C. Evolving robust networks using evolutionary algorithms. *Evolutionary Computation and Complex Networks*. Cham: Springer, 2019. 117-140

137 Wang S, Liu J. Designing comprehensively robust networks against intentional attacks and cascading failures. *Information Sciences*, 2019, **478**: 125−140

138 Gunasekara R C, Mohan C K, Mehrotra K. Multi-objective optimization to improve robustness in networks. *Multi-Objective Optimization: Evolutionary to Hybrid Framework*. Singapore: Springer, 2018. 115−139

139 Hou L L, Lao S Y, Jiang B, Bai L. Enhancing complex network controllability by rewiring links. In: Proceedings of the 3rd International Conference on Intelligent System Design and Engineering Applications (ISDEA). Hong Kong, China: IEEE, 2013. 709−711

140 Xu J Q, Wang J F, Zhao H, Jia S Y. Improving controllability of complex networks by rewiring links regularly. In: Proceedings of the 26th Chinese Control and Decision Conference (CCDC). Changsha, China: IEEE, 2014. 642−645

141 Wang S, Liu J. A multi-objective evolutionary algorithm for promoting the emergence of cooperation and controllable robustness on directed networks. *IEEE Transactions on Network Science and Engineering*, 2018, **5**(2): 92−100

142 Hou L L, Lao S Y, Small M, Xiao Y D. Enhancing complex network controllability by minimum link direction reversal. *Physics Letters A*, 2015, **379**(20-21): 1321−1325

143 Shi D H, Lü L Y, Chen G R. Totally homogeneous networks. *National Science Review*, 2019, **6**(5): 962−969

144 Shi D H, Chen G R, Thong W W K, Yan X Y. Searching for optimal network topology with best possible synchronizability. *IEEE Circuits and Systems Magazine*, 2013, **13**(1): 66−75

145 Fan T L, Lv L Y, Shi D H, Zhou T. Characterizing cycle structure in complex networks. *Communications Physics*, 2021, **4**, Article number: 272

146 Milo R, Shen-Orr S, Itzkovitz S, Kashtan N, Chklovskii D, Alon U. Network motifs: Simple building blocks of complex networks. *Science*, 2002, **298**(5594): 824−827

147 Menck P J, Heitzig J, Kurths J, Schellnhuber H J. How dead ends undermine power grid stability. *Nature Communications*, 2014, **5**: 3969

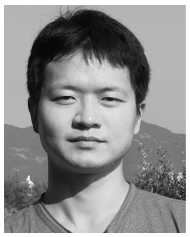
148 Gorochowski T E, Grierson C S, di Bernardo M. Organization

of feed-forward loop motifs reveals architectural principles in natural and engineered networks. *Science Advances*, 2018, **4**(3): eaap9751

149 Badhwar R, Bagler G. Robust sigmoidal control response of *C. elegans* neuronal network. In: Proceedings of the 2017 International Joint Conference on Rough Sets. Olsztyn, Poland: Springer, 2017. 393−402

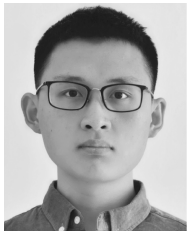
150 Dey A K, Gel Y R, Poor H V. What network motifs tell us about resilience and reliability of complex networks. *Proceedings of the National Academy of Sciences of the United States of America*, 2019, **116**(39): 19368−19373

151 Jia Cheng-Feng, Han Hua, Wan Yan-Juan, Lv Ya-Nan. Network destruction resistance based on network motif feature. *Complex Systems and Complexity Science*, 2017, **14**(4): 43−50 (贾承丰, 韩华, 完颜娟, 吕亚楠. 基于网络模体特征攻击的网络抗毁性研究. 复杂系统与复杂性科学, 2017, **14**(4): 43−50)

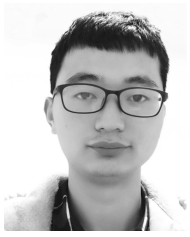


楼 洋 四川师范大学副研究员, 中国香港城市大学博士后. 2017 年获得中国香港城市大学博士学位. 主要研究方向为复杂网络, 进化算法和机器学习.
E-mail: felix.lou@my.cityu.edu.hk
(**LOU Yang** Associate professor at Sichuan Normal University and Postdoctoral Fellow at City University of Hong Kong, China. He received his Ph.D. degree from City University of Hong Kong, China in 2017. His research interest covers complex networks, evolutionary computation, and machine learning.)

李均利 四川师范大学研究员. 2002 年获得浙江大学博士学位. 主要研究方向为图像处理, 目标跟踪, 智能计算. 本文通信作者.
E-mail: li.junli@vip.163.com
(**LI Jun-Li** Professor at Sichuan Normal University. He received his Ph.D. degree from Zhejiang University in 2002. His research interest covers image processing, target tracking, and computational intelligence. Corresponding author of this paper.)



李 升 四川师范大学硕士研究生. 主要研究方向为复杂网络.
E-mail: yunchunrui@163.com
(**LI Sheng** Master student at Sichuan Normal University. His research interest covers complex networks.)



邓 浩 四川师范大学硕士研究生. 主要研究方向为进化计算, 复杂网络.
E-mail: 18108015390@189.cn
(**DENG Hao** Master student at Sichuan Normal University. His research interest covers evolutionary computing and complex networks.)