文章编号: 1001-0920(2019)11-2310-07 **DOI:** 10.13195/j.kzyjc.2019.0132

割点失效对复杂网络可控性的影响

王立夫†, 赵云康, 段 乐, 余牧舟

(东北大学秦皇岛分校 控制工程学院，河北 秦皇岛 066004)

摘 要: 信息物理系统个体间的相互作用能够应用复杂网络描述,复杂网络中的某些节点遭到攻击或破坏会造成网络故障,导致整个网络系统不受控. 割点是网络中的一类关键节点,受攻击或故障后将导致网络连接断开,在保证网络连通性方面发挥着重要作用,但割点失效对网络可控性的影响尚不清楚. 鉴于此,给出复杂网络中割点失效的可控性模型,研究割点失效对可控性的影响,同时选取节点的随机失效和以度为依据的蓄意攻击作为对比. 研究发现:随机失效对可控性的影响较小,割点失效和蓄意攻击对可控性的影响较大;平均度较低时割点失效和蓄意攻击对可控性影响基本相同,但平均度增大后,割点失效比蓄意攻击对可控性的影响更大;另外,平均度的增加能够提高网络对割点失效的控制鲁棒性.

关键词: 复杂网络；信息物理系统；网络可控性；网络割点；节点失效

中图分类号: TP11 **文献标志码:** A

Effect of cut vertexes-removal on controllability of complex networks

WANG Li-fu†, ZHAO Yun-kang, DUAN Le, YU Mu-zhou

(School of Control Engineering，Northeastern University at Qinhuangdao，Qinhuangdao 066004，China)

Abstract: Interactions between individuals in cyber-physical systems can be described by complex networks. Complex network failures caused by attacking or corrupting on certain nodes would lead the network out of control. Cut vertexes are a kind of key nodes whose removal will disconnect a network. Cut vertexes play an important role in ensuring the connectivity of a network, however, it is still uncertain about the effect of cut vertexes-removal on network controllability. Therefore, we firstly investigate the model of network controllability based on cut vertexes-removal, and study the effect of cut vertexes-removal on controllability, meanwhile, random failures of nodes and target attacks based on degree are chosen as comparisons. The results demonstrate that random-failures have little effect on controllability, while cut vertexes-removal and target-attacks have a greater influence; when the average degree is low, the cut vertexes-removal and the target-attacks have nearly the same effect on controllability, but as the average degree grows, the cut vertexes-removal are more effective on controllability comparing with target-attacks; in addition, the controllable robustness of a network against cut vertexes-removal can be improved with the increase of average degree.

Keywords: complex networks；cyber-physical systems；network controllability；cut vertexes；nodes failure

0 引 言

近年来,信息物理融合系统(cyber physical systems, CPS)及其相关技术的快速发展,推动了汽车、工业自动化、医疗保健、工业控制系统、智能建筑、智慧道路、智能交通系统、电力系统等领域关键技术的升级换代和跨越发展[1],与CPS有关的概念包括: 物联网、工业互联网、智慧城市、智慧电网等. 绝大多数CPS是一个复杂系统,是由相互作用和相互依赖的若干组成部分结合而成的有机整体. 如果用节点表示系统的各个组成部分,边表示各个组成部分之间的相互作用,则网络就为研究系统提供了一种新的描述方式. 复杂网络是复杂系统的一种高度抽象,大量真实的CPS都可以抽象为复杂网络. 例如,神经系统可以看作是由大量神经细胞通过神经纤维相互连接形成的网络;计算机网络可以看作是自主工作的计算机通过通信介质相互连接形成的网络;类似的还有电力网络、社会关系网络、交通网络等. 对于复杂网络的研究最初主要集中在网络的拓扑结构特征上,如网络的无标度、小世界特性[2],通过对网络模型以及节点和边的相互作用等拓扑结构、动力学行为

收稿日期: 2019-01-27；**修回日期:** 2019-05-24.

基金项目: 国家自然科学基金项目(61402088)；河北省自然科学基金项目(F2016501023, F2017501041)；中央高校基本科研业务费项目(N172304030).

责任编委: 李韬.

†通讯作者. E-mail: wlfkz@qq.com.

的研究,揭示复杂网络的内在规律,有助于理解现实世界网络,提高网络运行效率.

复杂网络研究的最终目标是寻找有效的手段来控制网络的行为使其更好地为人类服务[3]. 因此,复杂网络的控制技术近年来越来越受关注[4-5],牵制控制、离散控制、自适应控制等控制方法均已应用于网络中使网络达到控制目标. 然而,控制复杂网络的前提是解决可行性问题,研究网络到底能不能被控制,即网络的可控性问题. 近年来,对于复杂网络可控性的研究取得了丰硕的成果,Liu 等[6] 通过将结构可控性理论引入复杂网络,利用图的最大匹配[7] 计算网络的可控性,解决了有向网络的可控性问题. 为了研究无向网络的控制,Yuan 等[8] 利用可控性 PBH(Popov-Belevitch-Hautus) 判据提出复杂网络的严格可控性判据,该理论适用于任意结构和边权值的网络,解决了无向网络的可控性问题.

复杂信息-物理网络的概念近年来被人们明确提及,与传统复杂网络研究不同,复杂信息物理网络更关注安全控制和信息-物理安全性[9]. 现实生活中的网络通常会遭到潜在的攻击或故障,导致网络崩溃和失控,如交通网络遭受攻击或发生故障时引起的节点或边失效会造成大面积的交通拥堵、互联网络的节点或边失效会导致互联网络瘫痪、电力网络故障会使电力网络中断等事故[10],这些网络故障对社会生产生活造成较大影响. 因此,为提高网络发生故障时正常运行的能力,对复杂网络控制鲁棒性的研究越来越受到关注. 网络受到攻击或故障,对网络的损害取决于故障部分在系统中的重要性[11]. 节点度和边介数是常用的重要性衡量方法[12],Nie 等[13] 研究了网络中节点遭到攻击时网络可控性的变化; Lu 等[14] 研究了网络中边发生故障对网络可控性的影响; Pu 等[15] 研究了网络中最长简单路径受到攻击的情况. 以上研究发现网络对随机攻击[16] 有较高的鲁棒性,但对基于节点度、边介数以及最长的简单路径攻击时的鲁棒性较差. 肖延东等[17] 发现维护无标度网络可控的难度明显大于随机网络,极少的节点失效也能破坏网络的可控性. 由于复杂网络的结构复杂,节点之间相互作用,网络部分结构的故障会导致整个网络的崩溃,人们提出网络的级联失效. 陈世明等[18] 对级联失效模型和网络遭到随机失效和蓄意攻击下级联失效过程中的可控性进行了研究. 相互依存网络的鲁棒性研究也逐渐受到人们的关注,相依网络中的节点与另一层网络相互依存发挥作用,因此其相关性质也不同于单一网络[19]. 另外,针对网络可能遭受的攻击[20] 和级联故障[21], Wang 等[22] 提出了一种新的高鲁棒性网络模型,用于降低这些故障造成的影响.

割点是网络中的一类节点,受攻击或故障删除后将导致网络连接断开,这类节点在确保基础设施网络、蛋白质交互网络、恐怖主义通信网络等许多现实世界网络的连通性方面发挥着关键作用[23]. 尽管它们具有如此的重要性,但当前针对网络控制鲁棒性的研究仍主要集中在节点度最大攻击、介数最大攻击等方法,尚缺乏割点对复杂网络可控性影响的研究. 鉴于此,本文研究割点失效对复杂网络可控性的影响,利用深度优先搜索算法寻找复杂网络中的割点[24],攻击寻找到的割点使其失效,探究割点失效对网络可控性的影响. 在此基础上,选取以最大度节点为目标的蓄意攻击和随机选择节点攻击两种攻击策略,与割点失效过程进行对比分析.

1　复杂网络可控性

考虑具有 N 个节点的复杂网络上的线性时不变动力学网络系统,其动力学方程表示为

$$\dot{x}(t) = Ax(t) + Bu(t). \tag{1}$$

其中: $x(t) = (x_1(t), x_2(t), \cdots, x_N(t))^{\mathrm{T}}$ 为复杂网络中节点的状态, $x_j(t)$ 为第 j 个节点在 t 时刻的状态; $A \in R^{N\times N}$ 为网络的邻接矩阵, $a_{ij} = 0$ 表示从节点 j 到节点 i 没有连接关系,即节点 j 不影响节点 i, $a_{ij} \neq 0$ 表示节点 j 影响节点 i 的强度, a_{ij} 的正负表示这种影响是积极的还是消极的; $u(t) = (u_1(t), u_2(t), \cdots, u_N(t))^{\mathrm{T}}$ 为输入的控制信号, $u_j(t)$ 为外部对第 j 个节点施加的控制输入;矩阵 $B \in R^{N\times M}$ 为输入矩阵,表示外部输入与内部节点的耦合关系, b_{ij} 表示输入信号 $u_j(t)$ 与节点 i 之间的耦合连接.

对于复杂网络系统 (1),若存在一个分段连续的输入 $u(t)$,能够在有限时间 $[t_0, t_f]$ 内使得系统从任意初始状态 $x(t_0)$ 转移到任意终止状态 $x(t_f)$,则此系统是可控的. 在控制理论中,可通过 Kalman 可控性判据判断一个系统是否可控,即复杂网络系统 (1) 完全可控的充分必要条件是矩阵

$$W = [B, AB, A^2B, \cdots, A^NB] \in R^{N\times NM} \tag{2}$$

满秩, $\mathrm{rank}(W) = N$, W 称为可控性矩阵. 由 Kalman 可控性判据,对于给定的复杂网络,邻接矩阵 A 是确定的,使网络达到完全可控是找到合适的输入矩阵 B,使得系统 (1) 能够满足 Kalman 可控性判据. 可见,若对网络中的每个节点都施加一个外部输入,则网络一定能达到完全可控,但是对于有成千上万个节点的复杂网络而言是不现实的. 因此,应该尽可能少地选

择网络中的节点施加外部输入控制,即矩阵B尽可能少地包含输入节点. 但是,复杂网络具有成千上万的节点,而Kalman判定定理的计算复杂度为2^N-1,计算量非常巨大,同时现实世界中的网络节点间的连接权重a_{ij}很大一部分是未知或不确定的. 为了克服这些困难,Liu等[6]通过将图的匹配理论方法与结构可控性相结合,提出了一种基于最大匹配算法求解最小驱动节点集的分析复杂网络可控性的框架,并给出最小输入定理,证明实现网络结构可控所需独立控制的节点集合等于非最大匹配的节点集合,其中需要被独立控制的节点称为网络的驱动节点,驱动节点个数用N_D表示.

尽管Liu等提出的结构可控性框架提供了控制有向网络的通用方法,该方法适用于结构矩阵表示的有向网络,即边权值为零或独立的自由参数,但对于网络邻接矩阵对称的无向网络和边权值已知的网络不再适用. Yuan等[8]基于PBH判据提出了一种严格可控性框架,该框架适用于求解任意结构网络的可控性,包括有向网络、无向网络、加权网络、无权网络、含自环的网络和无自环网络等. 具体内容是复杂网络系统(1)完全可控所需要的最少驱动节点数N_D为其邻接矩阵A的最大几何重数,即

$$N_D=\max_i\{\mu(\lambda_i)\},\tag{3}$$

其中$\mu(\lambda_i)$为邻接矩阵A的特征值$\lambda_i(i=1,2,\cdots,N)$的几何重数. 对于大型稀疏网络,严格可控性理论给出了只需要邻接矩阵A的秩来确定驱动节点数N_D的方法,即

$$N_D=\max\{1,N-\mathrm{rank}(A)\}.\tag{4}$$

网络的可控性由控制网络所需要的最小驱动节点数占总节点数的比例定义,即网络中的驱动节点密度,记为

$$n_D=N_D/N.\tag{5}$$

其大小反映复杂网络控制的难易程度,该值越小,表明控制网络所需的驱动节点占总节点数的比例越小,网络越容易控制,反之网络越不容易被控制.

2 研究方法

复杂网络中的割点失效会使网络连接断开,从而影响网络的连通性. 针对这种现象,在复杂网络可控性问题中引入割点失效的概念,研究割点失效对网络可控性的影响.

2.1 割点失效可控性模型

网络中的某个节点发生故障或者被攻击后,该节点与网络不再连接,同时与该节点相连的边也不再发挥作用,网络结构发生变化导致控制信号流改变,从而导致网络的驱动节点发生改变. 为了研究复杂网络中的割点失效对可控性的影响,按一定规则去除网络中的割点,具体步骤如下.

Step 1: 以深度优先搜索算法遍历复杂网络的所有节点找到网络中的割点,记为$V_i(i=1,2,\cdots,M)$,M为搜索到的割点数量.

Step 2: 寻找目标失效割点. 分别计算每个割点失效后网络的连通子图数,以失效后能使网络分解出最多连通子图数的割点作为目标割点,记为$V_{\max}$. 寻找目标失效割点的算法如下.

割点V_i失效后网络的连通子图个数记为C_{V_i}.

for $i=1$ to M

  if $C_{V_i}>C_{V_{\max}}$

    $C_{V_{\max}}=C_{V_i}$

    $V_{\max}=V_i$

  end if

end

割点$V_{\max}$即为目标失效割点.

Step 3: 计算割点$V_{\max}$失效后的可控性n_D. 由式(4)和(5)得

$$n_D=\frac{N_D}{N}=\frac{\max\{1,N-\mathrm{rank}(A)\}}{N}.\tag{6}$$

Step 4: 检查网络中是否仍存在割点,若存在则返回Step 1,若不存在则结束操作.

这是一个迭代删除的过程,Step 2删除一个使网络分解出最多连通子图数的割点,但网络中可能仍含有割点,同时节点和边的移除也可能使网络中出现新的割点. 因此需要检查网络中是否仍然含有割点,如果仍有割点则继续迭代删除,直到网络中不再含有割点为止.

如图1(a)所示节点数为45,边数为64的无向网络,通过深度优先搜索算法寻找到的割点$V_i(i=1,2,\cdots,10)$以大圆标识,在找到的割点中寻找能使网络分解出最多连通子图的割点作为目标失效割点,以空心大圆标识,图1(a)中空心割点失效后网络连通子图数$C_{V_i}=5$,其他割点失效后网络连通子图均小于5,因此选取该割点作为目标失效割点. 删除该割点和与之相连的边后网络如图1(b)所示. 按照此方法,重新检查图1(b)网络中仍含有割点,进行第2次割点删除,删除后的网络如图1(c)所示. 继续按照上述步骤迭代删除,经过多次割点移除后,网络中不再含有割点的情形如图1(d)所示. 每次割点失效后,网络结构发生变化,网络的可控性也发生变化,利用严格可控性重新计算此时网络的可控性.

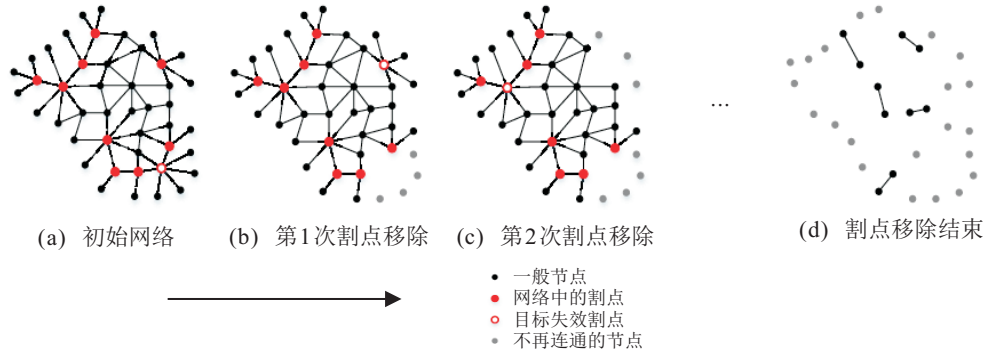


图 1　割点失效过程

为对比研究割点失效与其他节点失效的不同之处,简单介绍另外两种节点失效(攻击)方式:

1) 节点随机失效:每一步随机删除网络中一个节点和与之相连的边,直至删除节点数量达到预设值.

2) 以度为依据的蓄意攻击:每一步删除网络中度最大的节点及与之相连的边,然后重新计算剩余节点的度,再次执行删除过程,直至删除节点数量达到预设值.

需要注意的是,不同网络中割点分布和数量是不相同的,为了能够有效对比,在执行节点的随机失效和以度为依据的蓄意攻击时,攻击节点数量的预设值应与割点失效数量相同.

2.2　复杂网络控制的鲁棒性

复杂网络控制的鲁棒性定义为复杂网络在外界的影响下,网络仍然能维持其可控的能力. 假设初始网络节点总数为N,完全控制网络所需要的驱动节点数为N_D,若网络有V个节点失效导致网络结构发生变化,网络的驱动节点数变为N'_D,以节点失效前后网络可控性的变化衡量网络控制的鲁棒性,有

$$\Delta n_D = n'_D - n_D = \frac{N'_D}{N-V} - \frac{N_D}{N}. \tag{7}$$

Δn_D的大小反映了网络在外界影响下可控性的变化,Δn_D越小,表明维持其可控的能力越强,网络的鲁棒性越好,反之表明网络的鲁棒性越差.

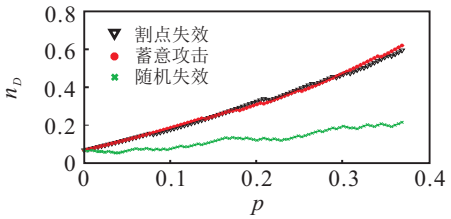
3　系统仿真

本节通过ER (Erdös-Rényi)随机网络和BA (Barabási-Albert)无标度网络,对网络割点失效、蓄意攻击以及节点随机失效时的可控性进行对比,分析割点失效对网络可控性的影响.

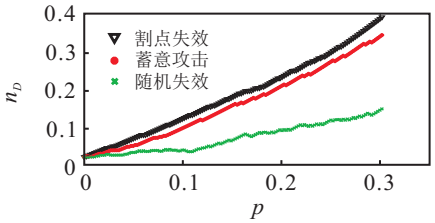
3.1　节点失效方式对可控性的影响

3.1.1　ER随机网络

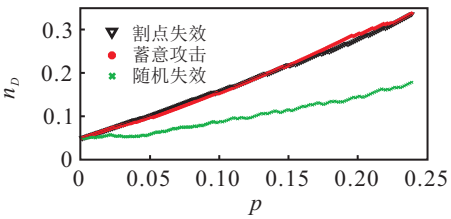
首先生成节点数分别为300、500、800,平均度为3的ER随机网络. 按照上节所述的割点失效、蓄意攻击、随机失效过程,观测可控性变化与节点失效比例的关系如图2所示. 由图2可见,3种攻击方式都使网络的可控性降低(驱动节点比例n_D变大),但随机失效后的Δn_D较小,割点失效和蓄意攻击后的Δn_D较大,即随机失效对网络的可控性影响较小,而割点失效和蓄意攻击对网络的可控性影响相对较大. 但此时割点失效和蓄意攻击对可控性的影响并无明显区别,表明ER网络对节点随机失效有较高的鲁棒性,对割点失效以及蓄意攻击较为脆弱.



(a)　节点数为300的ER网络



(b)　节点数为500的ER网络

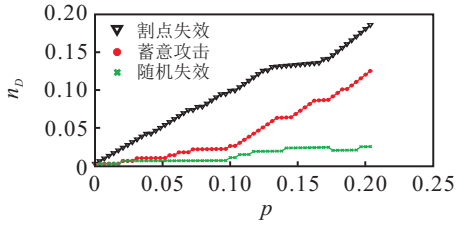


(c)　节点数为800的ER网络

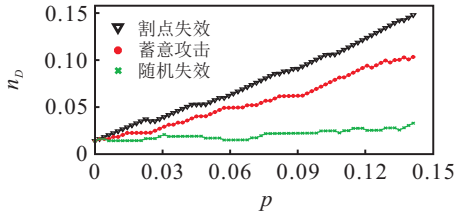
图 2　平均度为3的ER网络

考虑到网络的可控性与网络平均度(边的密度)具有相关性[25],重新生成节点总数300、500、800不变,平均度为5的ER随机网络,观测可控性变化与节点失效比例的关系如图3所示. 由图3可见,与平均度为3时类似,随机失效对网络的可控性影响较小,割点失效和蓄意攻击对网络的可控性影响相对较大. 但是与平均度为3时相比,蓄意攻击和割点失效

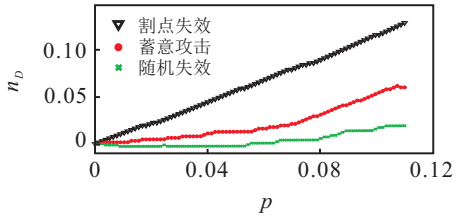
两种方式对可控性的影响有较大差异,割点失效对可控性的影响明显大于蓄意攻击对可控性的影响.



(a) 节点数为300的ER网络



(b) 节点数为500的ER网络



(c) 节点数为800的ER网络

图 3 平均度为5的ER网络

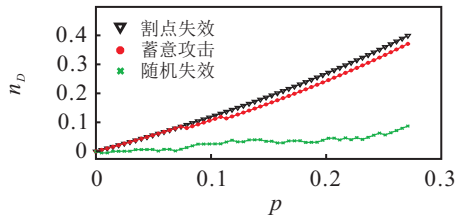
3.1.2 BA无标度网络

ER随机网络度分布相对均匀,是同质网络,而无标度网络的度分布很不均匀,为异质网络[16],节点度分布的均匀性对网络的可控性有影响. 下面分析3种节点失效方式对BA无标度网络可控性的影响.

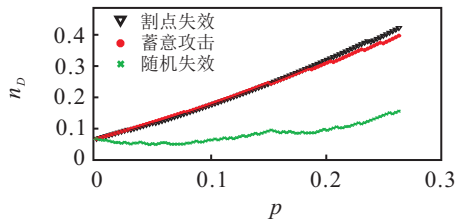
生成节点总数分别为300、500、800,平均度为3的BA无标度网络,按照割点失效、蓄意攻击、随机失效过程,观测可控性变化与节点失效比例的关系如图4所示. 对于平均度为10的BA无标度网络,按照3种失效过程观测可控性变化与节点失效比例的关系如图5所示. 由图4、图5可见,与ER随机网络类似,3种攻击方式都使BA无标度网络的可控性降低(驱动节点比例n_D变大),但随机失效后的Δn_D变化较小,割点失效和蓄意攻击后的Δn_D较大,平均度为3的BA网络,随机失效对网络的可控性影响较小,割点失效和蓄意攻击对网络的可控性影响相对较大,割点失效和蓄意攻击对可控性的影响并无明显区别. 平均度为10时,割点失效和蓄意攻击两种方式对可控性的影响有较大差异,割点失效对可控性的影响明显大于蓄意攻击对可控性的影响.

3.2 割点失效和蓄意攻击的对比

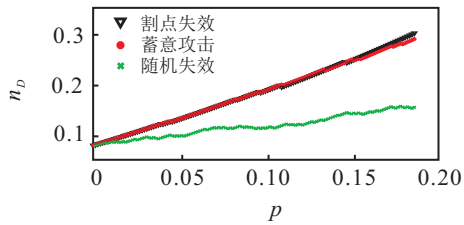
根据以上分析可知,无论是ER网络还是BA网络,当平均度较低时,割点失效和蓄意攻击对网络可控性的影响无明显区别,而平均度增大后,割点失效对网络可控性的影响明显大于蓄意攻击对网络可控性的影响,所以可以认为平均度的增加影响了网络可控性. 下面进一步考察不同平均度网络下割点失效和蓄意攻击两种方式对可控性影响的差异. 在相同



(a) 节点数为300的BA网络

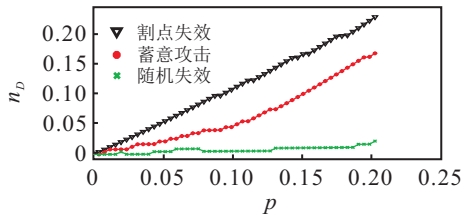


(b) 节点数为500的BA网络

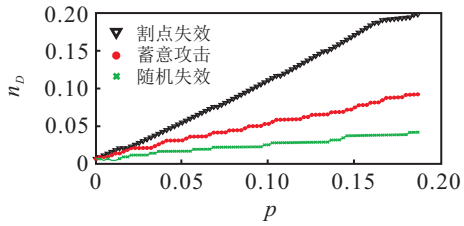


(c) 节点数为800的BA网络

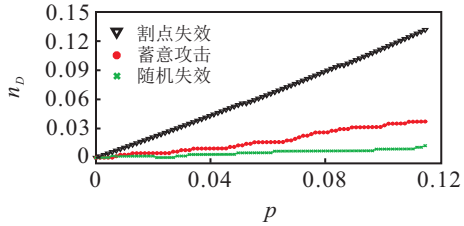
图 4 平均度为3的BA网络



(a) 节点数为300的BA网络



(b) 节点数为500的BA网络



(c) 节点数为800的BA网络

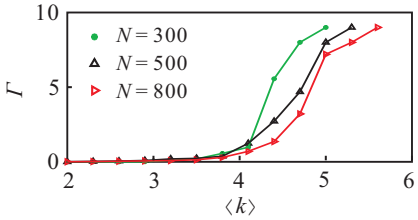
图 5 平均度为10的无标度网络

失效比例下,以割点失效与蓄意攻击对网络可控性影响的相对大小度量两者之间的差异,记为Γ,有

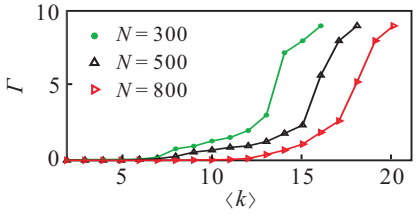
$$\Gamma=\sum_{i=1}^{qN}\frac{N_{D\_ap}-N_{D\_de}}{N_{D\_de}}\Big/qN. \tag{8}$$

其中: N 为网络总节点数, N_{D_ap} 为割点失效后网络的驱动节点数, N_{D_de} 为度最大节点失效后的驱动节点数, q 为失效节点的比例, qN 为失效节点数量. 该指标越大表示割点失效与蓄意攻击相比对网络可控性的影响越大.

节点数分别为300、500、800的ER随机网络, Γ 随平均度的变化情况如图6(a)所示. 由图6(a)可见,当网络的平均度较小(小于3)时, Γ 较小,接近为零,表明两种节点失效方式对可控性的影响相差不大. 实际上,此时网络中大部分度最大的节点同时也是割点,即网络的平均度较小时,网络中的割点与度最大的节点有相当多的重合,因此两种失效方式对网络可控性的影响相差不大. 当网络的平均度较大(大于4)时,随着平均度的增加, Γ 也随之变大,表明随着网络越来越稠密,相比于蓄意攻击,割点失效对网络可控性的影响更大. 割点失效使网络分解出多个连接子图,导致控制的匹配链[6]断裂,分解出的连接子图需要单独增加控制信号保持其可控,网络可控性变差. 蓄意攻击虽然也会导致匹配链重新分配,但增加驱动节点的几率较小,因此割点失效相比蓄意攻击对网络可控性的影响更大.



(a) ER随机网络



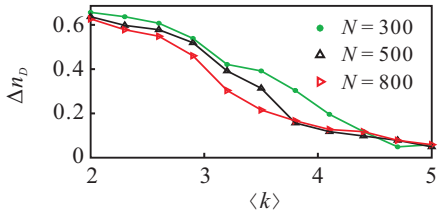
(b) BA无标度网络

图 6　Γ 随网络平均度的变化情况

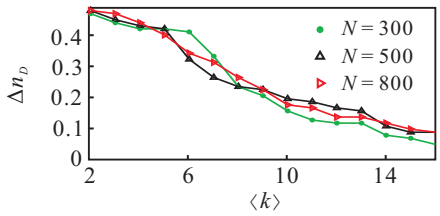
节点数分别为300、500、800的BA无标度网络, Γ 随平均度的变化情况如图6(b)所示. 与ER网络类似,网络的平均度较小(小于6)时, Γ 较小,接近于零,当网络的平均度较大(大于6)时,随着平均度的增加, Γ 也随之变大. 但与ER网络相比,因为无标度网络中Hub节点的存在,导致无标度网络的 Γ 阈值更大.

3.3　割点失效的控制鲁棒性

本节分析不同平均度网络对割点失效的鲁棒性,网络控制鲁棒性应用节点失效前后网络的可控性变化 Δn_D 来衡量. 节点数分别为300、500、800的ER随机网络,所有割点失效后 Δn_D 随平均度的变化如图7(a)所示. 由图7(a)可见,平均度为2时, Δn_D 较大,表明此时割点失效对网络的可控性影响较大,即网络控制鲁棒性较差. 随着平均度的增加, Δn_D 逐渐减小,割点失效对网络的可控性影响减小,表明网络的控制鲁棒性增强. 且当ER网络的平均度大于5时,割点失效对可控性的影响已经很小,此时网络对割点失效有较高的鲁棒性. 研究发现,随着平均度的增加,网络中割点数量占节点总数的比例逐渐减小,失效节点比例减少导致割点失效对网络可控性的影响减小.



(a) ER随机网络



(b) BA无标度网络

图 7　不同平均度下网络的控制鲁棒性

节点数分别为300、500、800的BA无标度网络,所有割点失效后 Δn_D 随平均度的变化如图7(b)所示. 由图7(b)可见,与ER随机网络类似,无标度网络的 Δn_D 也随着网络平均度的增加而减小,表明随着网络平均度的增加,网络对割点失效的鲁棒性逐渐增强. 同样,当无标度网络的平均度大于某一数值后,割点失效对可控性的影响已经非常有限.

4　结　论

本文针对网络中存在的节点失效问题,提出了基于割点失效的网络可控性模型,分析了割点失效对网络可控性的影响,并与节点的随机失效和以度为依据的蓄意攻击进行对比. 研究结果表明,节点的随机失效对ER随机网络和BA无标度网络可控性的影响较小,蓄意攻击和割点失效对可控性有较大影响. 同时发现蓄意攻击和割点失效对可控性的影响在不同平均度下有较大差异,在平均度较小时,两种失效方式对网络可控性的影响基本相同;随着平均度的增

加,割点失效相比蓄意攻击对网络可控性的影响更大. 进一步研究了不同平均度网络对割点失效的控制鲁棒性,结果发现,虽然相比蓄意攻击而言割点失效对可控性的影响更大,但随着网络平均度的增加,割点失效对ER网络和BA网络可控性的影响逐渐减小,网络对割点失效的控制鲁棒性随着平均度的增加而增强. 因此,提高网络的平均度能够有效增强网络对割点失效的控制鲁棒性.

参考文献(References)

[1] 管晓宏, 关新平, 郭戈. 信息物理融合系统理论与应用专刊序言 [J]. 自动化学报, 2019, 45(1): 1-4.
(Guan X H, Guan X P, Guo G. Preface of the special issue on theory and applications of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 1-4.)

[2] Barabási A L. Network science[M]. United Kingdom: Cambridge University Press, 2016: 3-18.

[3] Ding J, Tan P, Lu Y Z. Optimizing the controllability index of directed networks with the fixed number of control nodes[J]. Neurocomputing, 2016, 171: 1524-1532.

[4] Yan G, Ren J, Lai Y C, et al. Controlling complex networks: How much energy is needed?[J]. Physical Review Letters, 2012, 108(21): 218703.

[5] Parekh D, Ruths D, Ruths J. Reachability-based robustness of network controllability under node and edge attacks[C]. The 10th International Conference on Signal-Image Technology and Internet-based Systems. Piscataway: IEEE, 2014: 424-431.

[6] Liu Y Y, Slotine J J, Barabási A L. Controllability of complex networks[J]. Nature, 2011, 473(7346): 167-173.

[7] Lin C T. Structural controllability[J]. IEEE Transactions on Automatic Control, 1974, 19(3): 201-208.

[8] Yuan Z, Zhao C, Di Z, et al. Exact controllability of complex networks[J]. Nature Communications, 2013, 4: 2447.

[9] Wen G, Yu W, Yu X, et al. Complex cyber-physical networks: From cybersecurity to security control[J]. Journal of Systems Science and Complexity, 2017, 30(1): 46-67.

[10] Wei X, Gao S, Huang T, et al. Complex network based cascading faults graph for the analysis of transmission network vulnerability[J]. IEEE Transactions on Industrial Informatics, 2019, 15(3): 1265-1276.

[11] 汪小帆, 李翔, 陈关荣. 复杂网络理论及其应用 [M]. 北京: 清华大学出版社, 2006: 243-256.
(Wang X F, Li X, Chen G R. Complex network theory and its application[M]. Beijing: Tsinghua University Press, 2006: 243-256.)

[12] Lou Y, Wang L, Chen G. Toward stronger robustness of network controllability: A snapback network model[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2018, 65(9): 2983-2991.

[13] Nie S, Wang X, Zhang H, et al. Robustness of controllability for networks based on edge-attack[J]. PloS One, 2014, 9(2): e89066.

[14] Lu Z M, Li X F. Attack vulnerability of network controllability[J]. PloS One, 2016, 11(9): e0162289.

[15] Pu C L, Cui W. Vulnerability of complex networks under path-based attacks[J]. Physica A: Statistical Mechanics and Its Applications, 2015, 419: 622-629.

[16] Xiao Y D, Lao S Y, Hou L L. Optimization of robustness of network controllability against malicious attacks[J]. Chinese Physics B, 2014, 23(11): 118902.

[17] 肖延东, 老松杨, 侯绿林, 等. 基于节点负荷失效的网络可控性研究 [J]. 物理学报, 2013, 62(18): 180201.
(Xiao Y D, Lao S Y, Hou L L, et al. Research on network controllability based on node load failure[J]. Acta Physica Sinica, 2013, 62(18): 180201.)

[18] 陈世明, 邹小群, 吕辉. 面向级联失效的相依网络鲁棒性研究 [J]. 物理学报, 2014, 63(2): 028902.
(Chen S M, Zou X Q, Lv H. Research on robustness of dependent network for cascading failure[J]. Acta Physica Sinica, 2014, 63(2): 028902.)

[19] Zhang Z, Yin Y, Zhang X. Optimization of robustness of interdependent network controllability by redundant design[J]. PloS One, 2018, 13(2): e0192874.

[20] Yan X Y, Wang W X, Chen G R, et al. Multiplex congruence network of natural numbers[J]. Scientific Reports, 2016, 6: 23714.

[21] Rahimian M A, Aghdam A G. Structural controllability of multi-agent networks: Robustness against simultaneous failures[J]. Automatica, 2013, 49(11): 3149-3157.

[22] Wang L, Fu Y, Chen M Z Q, et al. Controllability robustness for scale-free networks based on nonlinear load-capacity[J]. Neurocomputing, 2017, 251: 99-105.

[23] Tian L, Bashan A, Shi D N, et al. Articulation points in complex networks[J]. Nature Communications, 2017, 8: 14223.

[24] Cui L, Li G, Lin Q, et al. A novel artificial bee colony algorithm with depth-first search framework and elite-guided search equation[J]. Information Sciences, 2016, 367: 1012-1044.

[25] Nie S, Wang X W, Wang B H, et al. Effect of correlations on controllability transition in network control[J]. Scientific Reports, 2016, 6: 23952.

作者简介

王立夫 (1980−), 男, 副教授, 博士, 从事复杂网络、同步控制、能控性、交通网络等研究, E-mail: wlfkz@qq.com;

赵云康 (1995−), 男, 硕士生, 从事复杂网络、控制理论的研究, E-mail: 2812136909@qq.com;

段乐 (1996−), 女, 硕士生, 从事时变网络、网络控制的研究, E-mail: 648455387@qq.com;

余牧舟 (1997−), 男, 本科生, 从事复杂网络的研究, E-mail: 1115768976@qq.com.

(责任编辑: 郑晓蕾)