

复杂动态网络抗毁性仿真研究

邓宏钟 吴俊 李勇 吕欣 谭跃进

(国防科技大学信息系统与管理学院, 湖南长沙 410073)

**摘 要:** 复杂网络的抗毁性研究是复杂网络研究的一项重要内容, 复杂网络的抗毁性研究具有重要的理论意义和应用价值。通讯网络的抗毁性, 生物系统的健壮性, 物理系统的稳定性都与各自系统内部网络的抗毁性息息相关。传统的网络抗毁性研究主要是通过解析分析来研究网络在各种不同类型故障与遭受打击情况下的网络拓扑结构和性能的变化。如最大连通片尺寸、代数连通度等指标的变化。这种将复杂网络看作一个静态网络进行研究的方式存在许多不足。如没有考虑节点的抗毁性、动态性和复杂性, 以及网络微观结构等因素对网络抗毁性的影响。

本文针对复杂网络静态抗毁性研究的不足, 提出复杂网络理论与复杂适应系统理论相结合的研究思路, 通过建立复杂系统的复杂动态网络抗毁性模型, 以解析推导与计算机仿真相结合的方式研究复杂动态网络的抗毁性。论文研究了在考虑节点抗毁性情况下, 复杂网络拓扑结构对复杂网络抗毁性的影响, 网络微观连接模式对复杂网络抗毁性的影响。研究了网络节点随机移动行为及结构动态变化对复杂网络系统抗毁性的影响。并把仿真结果与解析分析的结果进行了对比分析。研究了结果不一致, 甚至出现矛盾的原因。通过对两种研究方法的深入分析, 我们发现解析推导结果只能反映出网络部分抗毁性能。原因在于复杂网络中节点间存在大量隐性关系, 这种关系即难发现, 又难描述表达, 即使表示出来了, 因为其过于复杂, 结果也根本无法推导出来。通过对上述问题的对比研究说明了解析分析方法在复杂动态网络抗毁性研究上的不足, 基于多 Agent 的复杂动态网络抗毁性仿真分析方法在复杂动态网络抗毁性研究上有效性。

**关键词:** 复杂动态网络, 抗毁性, 仿真, 多 Agent, 适应性

---

收稿日期:

基金项目: 国家自然科学基金资助项目 (70501032, 70071111)

作者简介: 邓宏钟 (1974—), 男, 湖南衡阳人, 副教授, hongzhongdeng@163.net

## The Simulation Study of Complex Dynamic Network's Invulnerability

DENG Hong-zhong, WU Jun, LI Yong, LIU Bin

( College of Information Systems and Management, National University of Defense Technology, Changsha 410073,  
P. R China )

**ABSTRACT:** The study of complex network's invulnerability is a one important research content of complex network, has important theoretic and applications value. The invulnerability of communication network, the robustness of biologic system, the stability of physical system has closely link with their interior connective network. The traditional study of complex network's invulnerability mainly is analytic drive the change of network's topology and performance under different type of error and attack. Such as the change of the size of the largest connected component, the algebra connectivity. The study regard the network as a static network has some disadvantage. They don't take the vertices' invulnerability, dynamic, complexity and such factors as network microstructure's influence on network's invulnerability into account.

The author suggest building the complex dynamic network invulnerability model, through the analytic deriving and simulating the complex network's invulnerability based on the complex network and complex adaptive system theory to resolve the disadvantage of traditional research method of complex static network listed above.

The author studied the influence of complex network's topologic structure, the network's microstructure on complex network's invulnerability based on vertices' invulnerability, studied the influence of vertices' random move and structure's dynamic change on complex network's invulnerability, compared the difference between the analyzing result and simulation result, studied the cause of difference and inconsistency between the results. After the deeply analyzing of both research methods, the author found that the analytic result can only reflect partial invulnerability of the network. The reason is that there have many recessive relations among vertices. This relation can't find out and express out as a mathematic expression easily, and can't derive out the useful result for their complexity.

The research results indicate that the analytic method isn't very competent for the study of complex dynamic network's invulnerability. The multiagent based simulation method is a valid complex dynamic network's invulnerability research method.

**Key words:** complex dynamic networks; invulnerability; simulation; multiagent; adaptive

### I、前言

复杂网络，特别是无标度网络（scale-free networks）研究是当前复杂性科学和信息科学的一个新的研究热点。随着无标度网络研究热的兴起，作为复杂网络最重要的研究问题之一，复杂网络抗毁性研究的重大理

---

收稿日期:

基金项目: 国家自然科学基金资助项目 (70501032, 70071111)

作者简介: 邓宏钟 (1980—), 男, 湖南衡阳人, 副教授, hongzhongdeng@163.net

论意义和应用价值也日益凸显出来。

几乎所有的复杂系统都可以抽象成网络模型，这些网络往往具有大量的节点，节点之间有着复杂的连接关系。复杂网络不仅仅指无标度网络，它还包括介于随机网络与无标度网络间的其他类型网络，我们把它们统称为复杂网络。随着人们对网络的依赖程度日益增高，一个广受关注的问题逐渐凸现出来：这些系统、网络到底有多可靠？我们所关心的复杂网络抗毁性就是指：在外界故意打击（包括硬打击和软件杀伤）下，复杂网络系统仍然能够维持其功能的能力。

日常生活中所涉及的大量网络，如何降低它们的失效概率，提高它们的抗毁性具有重要意义。例如，在历届奥运会期间，在高负载、出现突发事件情况下，如何提高物资运输和人流输送网络的高效性、抗毁性，对于确保奥运会的正常进行，对于提高举办国的形象和地位具有极其重要的意义。提高通信网络的抗毁性对确保人民的正常生活秩序，确保经济系统的正常运行，提高经济效率和效益就有重要意义和实际价值。提高大型企业的销售业务网的抗毁性就是提高企业的竞争力。生物领域也存在同样的问题，基因网络中的一些核心基因的故障会带来灾难性的后果。1979年，P53被确认为第一种抑制肿瘤发展的基因。约翰斯·霍普金斯大学的沃格尔斯坦说：“P53看来是一个活动中心。它是少数这样的基因之一，其故障在细胞中造成灾难性的后果。”沃格尔斯坦、雷恩和莱文在《自然》杂志上发表的一篇论文中，把细胞中P53的失灵以及癌症的发展比作万维网上的一个核心网站的崩溃及其所带来的灾难性后果。

军事系统中的各种复杂网络的抗毁性研究更具意义和价值。40多年以来，军事指挥控制网络系统的体系结构发生了很大的变化，已演变为以通信、平台（战车、飞机、舰艇等）、网络为中心，以网络为中心的战争将成为未来战争的主要样式。在战时，提高军事网络系统的抗毁性将影响可影响到战争的胜负。从2007年以色列就利用网络战成功避开了俄罗斯防空雷达网络，对叙利亚北部一个“建筑工地”的空袭战中可以很清晰地看出这一点。

## II、复杂网络的抗毁性研究方法的研究现状

目前在复杂网络抗毁性研究方法上，主要有基于图论的抗毁性研究，基于解析的抗毁性研究和基于仿真的抗毁性研究三种主要的研究思路。

### A、基于图论的抗毁性研究

基于图论的抗毁性研究是指在拓扑结构完全确定的网络中，在理想的破坏方案作用下，网络能够保持连通的能力。抗毁性不涉及网络节点和边的抗毁性，衡量的是破坏一个系统的难度，它假定破坏者具有关于系统结构的全部资料，并采用一种确定性破坏策略。抗毁性指标是确定性的，仅仅和网络的拓扑结构有关，常用的指标有连接度和粘聚度等，它们首先是由 Frank 等<sup>[1]</sup>提出的。事实上，粘聚度对应着网络的最小连接割集，连通度对应着网络的最小节点割集。建立在图论基础之上的，从各种角度提出的抗毁性测度为我们提供了网络抗毁性的评估方法。但我们可以从它的抗毁性定义知道，基于图论的复杂网络抗毁性研究仅仅只研究了确定的、静态网络拓扑结构上的抗毁性能。既没考虑节点和边本身的抗毁性，也没考虑网络的动态变化，包括节点和边本身的抗毁性变化，所以基于图论的复杂网络抗毁性研究存在很大的局限性。

## B、基于解析分析的复杂网络抗毁性研究。

2000年Cohen等<sup>[2]</sup>把网络抗毁性问题转化为于广义随机图 (generalized random graphs)<sup>[3]</sup>上的渗流问题, 利用渗流理论 (percolation theory)<sup>[4,5]</sup>解析地研究了复杂网络的抗毁性, 即节点正常对应于渗流问题中节点被占据, 节点失效对应于渗流问题中节点空缺。Cohen等提出了一个计算崩溃临界概率  $f_c$  的准则: 假设网络中的环可以忽略, 如果对于网络中的任意节点  $v_i$  在与极大连通片(giant component)中某个节点  $v_j$  连接的同时还与其它节点连接, 则网络存在极大连通片, 否则网络崩溃, 即临界条件为:

$$\langle k_i | i \leftrightarrow j \rangle = \sum_{k_i} k_i P(k_i | i \leftrightarrow j) = 2 \quad (5)$$

由条件概率公式可将临界条件可化简为

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} = 2 \quad (6)$$

对于初始度分布为  $P(k_0)$  的复杂网络, 在随机移除了百分比为  $f$  的节点后, 该节点的度由  $k_0$  变为  $k$  的概率为  $C_{k_0}^k (1-f)^k f^{k_0-k}$ , 从而新的度分布为

$$P'(k) = \sum_{k_0=k}^{\infty} P(k_0) C_{k_0}^k (1-f)^k f^{k_0-k} \quad (7)$$

由(7)式可将临界条件可化简为

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} = \frac{\langle k_0^2 \rangle (1-f_c)^2 + \langle k_0 \rangle f_c (1-f_c)}{\langle k_0 \rangle (1-f_c)} = \frac{\langle k_0^2 \rangle}{\langle k_0 \rangle} (1-f_c) + f_c = 2 \quad (8)$$

进而可以得到网络崩溃的临界移除比例

$$f_c = 1 - \frac{1}{\kappa_0 - 1} \quad (9)$$

其中  $\kappa_0 = \langle k_0^2 \rangle / \langle k_0 \rangle$  可由初始度分布  $P(k_0)$  计算出。

Cohen等的研究中最重要结论是对于度分布为  $P(k) = Ck^{-\lambda}$  ( $k = m, m+1, \dots, K$ ) 的无标度网络, 当  $K \gg m$  时, 近似地有

$$\kappa_0 \rightarrow \frac{|2-\lambda|}{|3-\lambda|} \times \begin{cases} m & \lambda > 3 \\ m^{\lambda-2} K^{3-\lambda} & 2 < \lambda < 3 \\ K & 1 < \lambda < 2 \end{cases} \quad (10)$$

这样当  $\lambda > 3$  时, 网络总是存在一个小于 1 的临界值  $f_c$ 。然而当  $\lambda < 3$  时, 如果  $N \rightarrow \infty$  则  $f_c \rightarrow 1$ , 这意味着在无限系统中随机失效几乎不可能使得网络崩溃, 用物理学语言来说, 网络几乎总是渗流的。其实

就算在有限网络中，例如因特网（ $\lambda \approx 2.5$ ， $N > 10^6$ ），要想摧毁它，我们也必须随机移除 99% 以上的节点。由于现实世界中的无标度网络的标度指数  $\lambda$  都位于 2 和 3 之间，这意味着现实世界中大多数无标度网络面对随机失效有着很强的抗毁性，这与前面的仿真分析和实证分析是一致的。

用相同的方法，Cohen 等<sup>[6]</sup>又解析地研究了复杂网络对选择性攻击的抗毁性。对于度分布为  $P(k) = Ck^{-\lambda}$  ( $k = m, m+1, \dots, K$ ) 的无标度网络，假设按照度的大小选择性移除百分比为  $f$  的节点导致百分比为  $\tilde{f}$  的边的移除，移除后网络中节点的最大度变为  $\tilde{K}$ ，这样选择性攻击百分比为  $f$  的节点就从本质上可以等价于随机移除百分比为  $\tilde{f}$  的边且使得最大度变为  $\tilde{K}$ 。Cohen 等推导出了  $\tilde{f}$ 、 $\tilde{K}$  和  $f$  之间的数学关系分别为  $\tilde{K} = mf^{1/(1-\gamma)}$  和  $\tilde{f} = f^{(2-\lambda)/(1-\lambda)}$ 。这样当  $\lambda \rightarrow 2$  时  $\tilde{f} \rightarrow 1$ ，这表明当  $\lambda \rightarrow 2$  时选择性攻击少数几个节点也会导致网络的崩溃。Cohen 等通过对临界移除比例  $f_c(m, \lambda)$  的解析分析还发现，当  $\lambda > 2$  时，对任意  $\lambda$  无标度网络都会在一个较小临界值  $f_c$  发生相变，且  $f_c(m, \lambda)$  在  $\lambda = 2.25$  附近取最大值后开始随  $\lambda$  递减，Cohen 等认为之所以高  $\lambda$  无标度网络会对选择性攻击更加敏感是因为原始网络是由一些独立连通片组成且极大连通片的规模随  $\lambda$  增加而减少。由于 Cohen 等在推导过程中对度分布进行了连续性近似，所以得到的临界移除比例  $f_c$  过大，Dorogovtsev 等<sup>[7]</sup>对其进行了更为精确的推导。他们得到的临界值  $f_c$  与标度指数  $\lambda$  的关系如图 2 中实线所示，用 Cohen 等的方法得到的结果如图 2 中虚线所示。

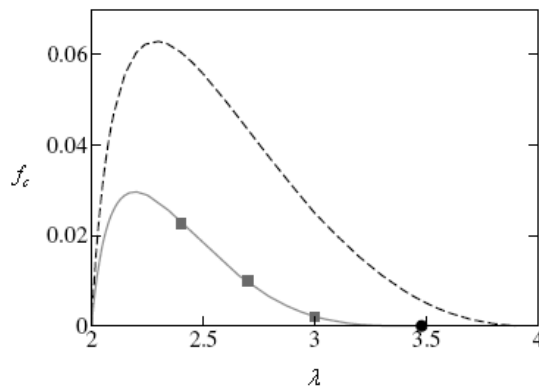


图 2 临界值  $f_c$  与标度指数  $\lambda$  的关系

和Cohen等一样，Callaway等<sup>[8]</sup>也把网络抗毁性问题转换为一个广义随机图上的渗流问题，但他们提出了一个更为普遍的母函数方法。在他们的方法中，一个度为  $k$  的节点其被占据的概率推广为节点度的任意函数  $q_k$ ，这样随机失效相当令  $q_k$  为常数，文献<sup>[9]</sup>中的选择性攻击（删除所有度大于  $k_{\max}$  的节点）相当于令  $q_k = \theta(k_{\max} - k)$ ，其中  $\theta$  为阶越函数。对于度分布为  $P(k) = Ck^{-\lambda}e^{-k/\kappa}$  ( $k \geq 1$ ) 的可调幂率网络<sup>[10]</sup>，Callaway等用母函数方法解析地给出了随机失效条件下的移除比例临界值为

$$f_c = 1 - \frac{1}{\frac{Li_{\lambda-2}(e^{-1/\kappa})}{Li_{\lambda-1}(e^{-1/\kappa})} - 1} \quad (11)$$

其中  $Li_n(x) = \sum_{k=1}^{\infty} x^k / k^n$ 。他们发现无标度网络对于随机失效很鲁棒，但对于选择性攻击极其敏感，只需删除很小部分的顶点就可以破坏整个网络，这与Cohen等的结果一致。2002年，Schwartz等<sup>[11]</sup>还将计算推广到了有向图。

在上面的分析中,网络的失效模式只有随机失效与选择性攻击两种这显然与现实并不完全相符。Gallos等<sup>[12]</sup>把网络的打击模式推广到了一般形式,他们给每个节点分配一个失效概率 $W$ ,它被定义为节点度的函数 $W(k_i) = k_i^\alpha / \sum_{j=1}^{N-1} k_j^\alpha$ ,其中 $-\infty < \alpha < +\infty$ 为控制参数。当 $\alpha < 0$ 时,网络中节点度越大失效概率越小,当 $\alpha = 0$ 时失效模式等价于随机失效,当 $\alpha \rightarrow +\infty$ 时,失效模式等价于选择性攻击。Gallos等研究得出了无标度网络中节点度最大的 $n$ 个节点失效概率 $w$ (它对应着攻击者获得的信息大小)与 $\alpha$ 和标度指数 $\lambda$ 的关系

$$w = \frac{1 - n^{(\lambda-1-\alpha)} m^{\alpha+1-\lambda}}{1 - N^{(\lambda-1-\alpha)} m^{\alpha+1-\lambda}} \quad (12)$$

其中 $m$ 为最小度, $N$ 为节点数目。Gallos等结合仿真和解析的方法研究了不同失效模式下网络崩溃临界值,指出随着攻击信息 $w$ 的增加,网络的崩溃临界值迅速减小,而且即使网络不崩溃,网络遭受的破坏也非常严重。

Vázquez等<sup>[13]</sup>还研究了考虑度关联条件下的网络抗毁性。他们提出了考虑度关联条件下网络崩溃的新临界条件:矩阵 $(k' - 1)P(k' | k)$ 的最大特征值等于1。他们发现如果网络中邻接顶点的度数是正相关的,即使是对有穷二阶距,移除比例临界值也可能趋近于1,反之,如果度数是负相关的,即使二阶距确实为发散的,临界值仍可能小于1。此外,Warren等<sup>[14]</sup>与Rozenfeld等<sup>[15]</sup>还研究了空间模型上的连续渗流。

### C、复杂网络抗毁性实证分析与仿真分析

2000年Albert开始关注拓扑结构对复杂网络抗毁性的影响。他们分别把随机网络(ER模型)和无标度网络(BA模型)置于两种类型的打击策略之下。在一种打击中,他们随机地移除网络中的节点,这与网络中的随机失效相对应;在另外一种打击中,则仅仅拿掉了网络中的活动中心,即按照节点连接度从大到小的顺序移除节点,这与网络面对的选择性攻击相对应。Albert等选择极大连通片尺寸与网络规模之比 $S$ 和极大连通片平均最短路径 $l$ 为指标,分别研究了不同网络面对不同打击条件下 $S$ 、 $l$ 与节点移除比例 $f$ 的关系。他的研究表明:面对随机失效,虽然无标度网络和随机网络的 $S$ 都随 $f$ 不断变小且都在某个临界值 $f_c$ 处变为0(网络崩溃),但是在这个过程中无标度网络中 $l$ 随 $f$ 的增长要比随机网络中 $l$ 随 $f$ 增长慢得多,并且峰值也不那么明显。这表明,在随机失效下,无标度网络相对随机网络有着更强的抗毁性。在选择性攻击下,无标度网络和随机网络的崩溃临界值 $f_c$ 都比随机失效条件下要小得多,但无标度网络要比随机网络崩溃的更早,只要少数“核心节点”被移除整个网络就陷入瘫痪。这表明无标度网络面对选择性攻击显得异常脆弱。无标度网络这种双重特性(robust-yet-fragile)也被称为“Achilles' heel”。在因特网和万维网上的实证分析验证了Albert等的结论。Albert等的研究激起了大量研究人员研究网络抗毁性的兴趣。

Broder<sup>[9]</sup>等在万维网的许多更大子集合上独立研究,发现了与Albert等相似的结果。然而,有趣的是,Broder等就他们的研究结果作出了另外的解释。他们发现,为了破坏万维网的连通性,必须删除所有度数大于5的节点,这给网络造成的攻击性似乎更猛烈,此处假定一些节点有上千条关联边。因此,他们得出结论认为,网络对有目标的攻击具有很强的抗毁性。然而,事实上,他们所得的结果之间并不存在冲突。因为,万维网的节点度分布高度倾斜,度数大于5的节点在所有节点中仅占一小部分。

在此之后,有很多学者对其它现实世界中的复杂网络抗毁性问题展开探讨,总体研究结果似乎都与Albert

等所得结果一致，多数网络对于随机的节点删除都表现出抗毁性，而面对以最大度节点为目标的选择性攻击却相当脆弱。例如Jeong等<sup>[16]</sup>研究了蛋白质网络，Dunne等<sup>[17]</sup>研究了食物链网络，Newman等<sup>[18]</sup>研究了电子邮件网络，Magoni等<sup>[19]</sup>研究了英特网，Samant等<sup>[20]</sup>研究了P2P网络。有关复杂网络抗毁性的仿真研究，特别全面的要数Holme等<sup>[21]</sup>所作的工作。他们不仅考虑了节点删除的情况，还考虑了边删除的情况，此外还考虑了基于的介数（betweenness centrality）<sup>[22-24]</sup>的攻击策略。

### III、复杂网络的抗毁性研究存在的问题与不足

从前面复杂网络抗毁性研究现状分析中可知：基于图论的抗毁性研究只研究了静态的、确定型网络其拓扑结构上的抗毁性。基于解析的抗毁性研究虽然部分考虑了节点本身抗毁性对网络抗毁性的影响，但没有考虑节点抗毁性和网络结构同时动态变化的情况。而复杂网络抗毁性的实证分析与仿真研究则主要是考虑了不同攻击策略下，复杂网络拓扑结构上的抗毁性，也没有考虑节点本身的抗毁性和网络动态变化的情况。在从复杂网络抗毁性研究现状的分析中，我们可以看出，上述研究方式还存在许多不足。

第一、部分抗毁性指标无法得到精确的计算结果。许多网络抗毁性指标的计算已经被证明是 NP 困难的。例如：抗毁性指标“离散度”（scattering number）的计算就是 NP 困难的。因此，对于实际网络系统，一般只能采用近似计算。近似计算与真实结果间存在一定差异。

第二：没有充分考虑节点、边抗毁性对复杂网络抗毁性的影响。目前，大部分抗毁性研究，只研究网络系统在拓扑结构上的抗毁性。但现实生活中的网络系统的抗毁性不仅与网络拓扑结构的好坏有关，更与网络节点及边的抗毁性有着重要关系。如一个由抗毁性能很好的节点所组成的网络，在抗毁性能上肯定要比一个由抗毁性能较差的节点所组成的网络。这好比一个小狮群要强于一个大羊群。

第三：没有考虑到节点类型的差异性。在传统的网络分析中，都是把所有节点都抽象或看作是同类型的节点来研究，只是在某些个体属性上存在一定的差异。如节点连接边数量，节点权值等，还没有考虑完全由不同类型节点所构成的网络。而现实中的许多网络是由大量的不同类型节点所构成的复杂网络。如通信网络，其节点不仅包括电台、通讯车等相对简单的通讯设备，还包括通讯卫星、大型雷达等属性、功能完全不同的大型复杂设备。把它们抽象成同类节点进行研究所得到的抗毁性与实际网络系统的抗毁性已是有天壤之别。

第四：没有考虑节点、边的动态性对抗毁性的影响。事实上，节点的动态变化，哪怕是随机移动也将影响到整个网络系统的抗毁性。具有相同拓扑结构的静态网络与动态网络，其抗毁性就会存在差别。现实中的复杂网络大多是动态网络，这种动态不仅反映在节点本身的增加、删除，节点空间位置的移动等上面，更反映在因节点动态变化所引起的节点间相互连接关系，如连接边数量的动态变化上，一个最明显的例子是：疾病传染网络。如果在疾病传染网络中的节点（人或动物）是固定不动的，则这种疾病会很好控制，但这是不可能的，也正是由于人的不规则、不可预知、不可控的移动导致了疾病传染网络结构的动态变化及疾病传染研究和控制的复杂性。

第五：没有考虑到节点的适应性和智能性。现实中的大量复杂网络系统，其节点是由具有适应能力或智能的个体组成。例如人际关系网络，演员合作关系网络。这些网络节点都是由智能人所组成。当网络系统发生变化，遭到打击时或破坏，人们能够自动地调整自身状态，更改与其它人间的联系以提高本身的生存活力和网络系统的抗毁性。人的这种智能调整行为（不仅仅是择优连接）使得复杂网络系统抗毁性研究变得极其

复杂，也使得复杂网络系统的抗毁性能得以大大提高。

第六：没充分考虑网络物理负载对网络抗毁性的影响。复杂网络上所传输的信息，运送的物资都是一种网络物理负载。都会对复杂网络的抗毁性产生重大的影响。例如，在上下班高峰时期，交通网的抗毁性就比非高峰时期交通网络的抗毁性要差。当网络总负载和网络各部分分配负载都是动态变化时，复杂网络系统的抗毁性将会更加复杂。

第七：没有考虑混合关联网络的抗毁性。现实中的许多复杂网络系统，其节点相互之间不仅仅只存在一种连接关系，节点间的连接关系往往是种类繁多且复杂，并且相互关联。是一种复杂的耦合关系。例如：人际关系网络中，人与人之间既存在同学关系网络，又存在朋友关系网络，还存在师生、合作关系网络等，这些连接关系相互关联，相互影响，耦合成一个看不透的复杂人际关系网络。在研究这种网络系统的抗毁性时，不能采用还原论的思路，把网络系统中的各种不同类型的关系网割裂开来，分别研究其抗毁性，然后再进行综合，以得到网络系统的整体抗毁性。因为在进行网络分割时，已经破坏了不同关系网络内在的、复杂的、非线性联系。这种联系不能采用线性方法综合获得。因为这种网络耦合行为对网络抗毁性的影响无法通过对网络抗毁性能的耦合获得。

第八：未能考虑系统外界环境对系统抗毁性的影响。传统的复杂网络抗毁性研究只考虑如不同打击方式对复杂网络系统的单向影响。但是，外界环境不仅仅包括前述的各种不同的攻击模式，还包括实际系统中的地形、气候、消息、政治环境等更为复杂因素对系统的影响。外界环境不是对复杂网络系统的简单输入。外界环境与网络系统存在着双向的相互作用、相互影响。当复杂网络系统抗毁性产生变化时，它也会对外界环境产生影响，最终又反馈回来，影响到复杂网络系统抗毁性上。

从上述分析可以看出，传统复杂网络抗毁性研究主要是对复杂静态网络拓扑结构的抗毁性研究。在复杂网络系统抗毁性研究，特别是复杂动态网络系统的抗毁性研究上，还远远不够。这也是我们所想解决的问题之一。

#### IV、基于多 Agent 仿真的复杂动态网络抗毁性研究方法

从前面复杂网络系统的特点及传统研究方法的不足上可以看出，由于复杂网络系统内部关系及节点的复杂性，部分复杂网络抗毁性指标的计算复杂性。整个网络系统的抗毁性能是无法用解析表达式描述清楚并计算出来，采用解析分析的方法已经不能满足对复杂网络系统的抗毁性研究。特别是对于复杂动态网络。事实上，Albert 也意识到这个问题。当复杂网络遭受到不间断的打击时，复杂网络在受打击下的动态变化过程需要用解析推导与计算机仿真相结合的方式研究。

基于多 Agent 的抗毁性建模仿真方法能通过对 Agent 的建模，充分体现复杂网络系统的智能性、动态性、随机性等特点，通过对系统环境的建模，能够将系统外界环境与网络系统间的相互作用和相互关系体现出来。

基于多 Agent 的抗毁性建模仿真方法的核心是通过建立反映网络节点和边的抗毁性模型及环境模型，研究在外界环境刺激，如打击下，因节点抗毁性能变化所引起的整个网络系统抗毁性变化。

基于多 Agent 的抗毁性建模仿真方法步骤包括：

##### 1、 复杂网络系统抗毁性的理解



主要是研究复杂网络系统的构成，分析影响复杂网络系统抗毁性相关因素。

## 2、 建立网络系统外界环境模型

根据对网络系统抗毁性的分析，将各种影响复杂网络抗毁性能的外界因素提炼出来，建立对复杂网络系统的一类刺激或输入，以影响网络系统的抗毁性，最明显的一个是打击模式，如随机打击，智能打击等。

## 3、 建立节点模型

根据对网络系统抗毁性的分析，建立节点的抗毁性模型，包括与网络系统抗毁性相关的一切行为。如节点本身的抗毁性能，节点的移动规则，打击模型，损伤模型，修复模型等。

## 4、 构造网络系统的拓扑结构模型

在已经建立的节点 Agent 模型基础上，建立它们间的连接网络。

# V、复杂动态网络抗毁性仿真模型

基于多 Agent 的复杂网络抗毁性模型可用一个二元组来描述：

$\langle \text{Agents}, \text{环境}(E) \rangle$

**Agents:** Agent 代表复杂网络系统中的节点。Agents 是所有 Agent 的集合。模型中允许不同种类 Agent 的存在，并且每一类 Agent 的数量可以变化。Agent 能够感知它所处的环境，对外部刺激作出反应，在环境不断变化过程中，不断调整自己的行为。

**环境:** 是复杂网络的外界环境，是 Agent 存在的空间。Agent 与 Agent 之间在环境中进行交互，如 Agent 间的通讯、合作等。Agent 与环境间也可进行各种交互，如 Agent 受环境刺激修改自己的边连接规则，调整自己的移动方向和位置等。模型中的环境因素有很多，如空间位置、空间距离、障碍、气候、政策、消息等。它们将对 Agents 的各种行为产生约束和影响。

在复杂网络抗毁性模型建模过程中，最重要的是 Agent 环境的设计和描述，Agent 结构设计与定义，Agent 规则的设计与表示。

## A、Agent 环境

Agent 环境是指 Agent 的生存空间，它可用一个三维坐标和坐标上的  $k$  个函数值来表示：

$$E = (x, y, z, f_1(x, y, z) \dots f_k(x, y, z)) \quad x \in R, \quad y \in R, \quad z \in R, \quad k \in N \quad (13)$$

$E$  是一个三维实数空间，其上任意两点  $(x_1, y_1, z_1)$  和  $(x_2, y_2, z_2)$  的距离可以是它们之间的几何距离：

$$L = ((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2)^{1/2} \quad (14)$$

在后面的仿真中，我们把 Agent 环境设计成一个  $n \times n$  的二维网格。这个二维网格就构成了 Agent 的外部环境，Agent 在网格的位置  $(x, y)$ ，网格上各点处的气候，经纬度  $f(x, y)$  等相关数值等都是 Agent 外部环

境的组成因素之一，它们影响着 Agent 的行为和抉择。网络边界则对 Agent 行为产生约束。

## B、Agent 结构

复杂网络抗毁性模型中，最复杂、最重要的是 Agent 的结构和性能。复杂网络系统的抗毁性都要是基于 Agent 的结构、规则、行为、智能的。在我们的模型中，每个 Agent 可用一个四元组来描述：

Agent = <标识，类型，规则集，属性>

标识：标识是 Agent 的编号，是模型中 Agent 的“身份证”，每个 Agent 有一个唯一的标识。

类型：它是指 Agent 所属的种类。由于系统中存在不同种类的 Agent，Agent 之间的关系可以是邻居关系，上下级关系，也可以是亲属关系，债权关系，Agent 之间的关系可以非常复杂，这些都要通过类型和标识结合起来对它们进行处理。

规则集：Agent 对外界环境刺激能够作出反应，就是把外部刺激当作外部输入，与规则集中的规则进行匹配，然后执行匹配规则输出部分的响应。

属性：属性主要是指 Agent 的特定性能和参数。如单个节点 Agent 的抗毁性，连接边数量，它的权重，它的移动速度、被失效概率和打击概率等。不同的 Agent 可能具有不同的属性值。

## C、Agent 规则

在建模过程中，如何将节点的所有与抗毁性相关行为表示出来是建模和仿真中要考虑的一个重要问题。由于复杂网络系统的节点数量巨大，如果每个节点 Agent 的行为又很复杂，则会使得在计算机上进行抗毁性仿真变得不可行。所以在建模中，Agent 的各种抗毁性规则应该既能反应节点的主要抗毁性性能，又比较简单。例如 Agent 移动规则，可以是简单的随机移动，也可以是规则的运动，也可以按预先设计的路线移动。最简单的规则是 IF-THEN 规则。

## VI、仿真设计

复杂动态网络抗毁性仿真设计的目标是通过设计复杂网络在不同的动态因素影响下的抗毁性差异和变化。例如网络拓扑结构对抗毁性的影响，网络微观连接结构对抗毁性的影响，网络节点的移动对网络抗毁性的影响等。仿真设计过程中要关注的主要有系统外界环境的设计，Agent 属性的设计和定义，Agent 规则定义。

### A、系统外界环境设计

在复杂网络抗毁性仿真中，我们采用了最简单的系统外界环境，即简单的 600\*600 大小的二维空间，环境对复杂网络系统的影响主要在两个方面，一是节点间存在空间距离，距离会影响节点的移动。二是外界对复杂网络系统所采用的打击模式。

在仿真中，我们设计了一种依次打击模式，其含义如下：

- 1、 每个仿真周期，按 Agent 的编号，依次选择一个 Agent，作为本周期的打击对象。如果 Agent 总数

为  $N$ ，则经过  $N$  个仿真周期（ $N$  为网络节点总数），每个 Agent 都将被选中一次。

- 2、 计算被选中 Agent 的毁伤概率  $P$ ，这个节点 Agent 经过  $T$  个仿真周期的延迟后，将以概率  $P$  被毁伤。 $P$  越大，Agent 被毁伤的可能性越大。当  $P$  很小时，Agent 即使多次被选中，也不会被毁伤。其中，延迟时间  $T$  为一个随机分布于  $[1, 10]$  整数。
- 3、 进入下一仿真周期。

## B、Agent 属性定义

节点 Agent 的属性主要包括 Agent 位置个体抗毁性能

Agent 位置：Agent 初始位置是随机分布在整个网络环境中。

Agent 状态：节点 Agent 在仿真中只有“存活”和“死亡”两种状态。当节点 Agent 连接边数量大于零时，其状态为“存活”，当节点被毁伤成孤立节点时，其状态变成“死亡”。

Agent 个体抗毁性  $P$ ：每个 Agent 的抗毁性与它所连接边的数量相关，我们认为，当节点 Agent 的边数量较多时，它能够通过网络获取更丰富、更精确的信息，能够提高它的抗毁性（相反情况，以可做类似分析）。 $P$  与节点连接边数量  $n$  间的关系如下：

$$p_v = a\rho^n \quad (a \in [0,1] \quad , \quad \rho \in (0,1]) \quad (15)$$

上式中， $a, \rho$  是调节参数。 $n$  表示节点所连接边的总数量。当节点遭到打击时，节点的连接边数量  $n$  会减少，节点 Agent 的毁伤概率提高，抗毁性降低。

Agent 还有其它的一些辅助属性，如 Agent 的编号，Agent 的颜色，Agent 的图像。

## C、Agent 规则定义

本仿真中，我们设计了一种 Agent 随机移动规则。

Agent 随机移动规则：每个仿真周期，Agent 随机选择周期一定范围内的随机位置，并移动到新位置。

## D、复杂网络系统拓扑网络结构定义

本仿真中我们设计了两种类型复杂网络。BA 网络和随机网络。网络拓扑结构生成过程如下：

- 1、 根据网络类型，生成符合特性的网络节点度序列值。例如一个具有 50 个节点，节点最小度为 2，标度指数  $\lambda = 2$  的 BA 网络度序列为：  
 $\{22,15,12,10,9,8,7,7,6,6,5,5,5,5,4,4,4,4,4,4,3,3,3,3,3,3,3,3,3,3,3,3,2,2,2,2,2,2,2,2,2,2,2\}$
- 2、 将度序列值分配给每个 Agent。
- 3、 每个节点按给定的度，采用相应的网络微观连接模式，选择对话应节点进行连接。

网络的微观连接模式有两种，一种同类混合，即节点度大的节点与节点度大的节点优先连接。另一种是非同类混合，即节点度大的优先与节点度小的节点连接。前一种是“富—富”相连，后一种是“富—贫”相

连。

## E、复杂网络系统抗毁性评价指标

复杂网络抗毁性的评价指标有许多，从我们设计的仿真模型来看，一个抗毁性较好的复杂网络应该能够经受更长时间的外界打击，所以我们设计了两个指标：

节点全毁伤时间：将所有的节点打击成“死亡”，即所有节点都成为孤立节点所需要的打击时间。

节点半毁伤时间：对于有些系统，当网络系统中有一半节点被毁伤时，系统基本上完全丧失其功能。例如军事系统，当一个营，其战损人员达到其总人数的 50% 时，这个营口基本上丧失作战能力。所以设定当将网络中一半节点打击成孤立节点所需时间为另一复杂网络系统抗毁性评价指标。

## VII、复杂网络抗毁性折解析分析

现在，我们用解析的方法分别分析具有不同拓扑结构的复杂网络的抗毁性，结果将用于后面与仿真结果的对比分析。

### A、网络全毁伤概率分析

设有一个复杂网络，其拓扑结构图为  $G = (V, E)$ ，其中  $V(G)$  是节点集， $E(G)$  是边集。节点总数量为  $N$ ，边的总数量为  $M$ 。 $d_i$  表示节点  $v_i$  的度。

因为每个节点的毁伤概率为： $p_{v_i} = a\rho^{d_i}$ ，则网络中全部节点都被毁伤的概率为：

$$\begin{aligned} p_{total} &= p_{v_1} \times p_{v_2} \times \cdots \times p_{v_N} \\ &= (a\rho^{d_1}) \times (a\rho^{d_2}) \times \cdots \times (a\rho^{d_N}) \\ &= a^N \rho^{(d_1+d_2+\cdots+d_N)} \\ &= a^N \rho^M \end{aligned} \quad (16)$$

结论：对于不同的网络，只要网络的节点数和总边数相同，则网络全毁伤的概率是一样的。

### B、网络半毁伤概率分析

#### 1、随机网络半毁伤概率分析

对于随机网络，要将它的一半节点毁伤，在节点的选择组合上，总共有  $C_N^{N/2}$  种选择方案，每种方案下，节点毁伤概率为：

$$\begin{aligned} p_{hl-ran} &= p_{v_i} \times p_{v_j} \times \cdots \times p_{v_k} \quad (i, j, \cdots k \text{ 总数为 } N/2) \\ &= (a\rho^{d_i}) \times (a\rho^{d_j}) \times \cdots \times (a\rho^{d_k}) \\ &= a^{N/2} \rho^{(d_i+d_j+\cdots+d_k)} \end{aligned} \quad (17)$$

一般情况下，随机网络中每个节点的度相差不大，而任选一半节点的组合之间的差异也小。

根据上述分析可得：第 I 种组合的毁伤概率：

$$\begin{aligned}
 &\because e_{v_i} \approx e_{v_j} \quad (v_i, v_j \in V(G)) \\
 &\therefore p_{v_i} \approx p_{v_j} \\
 &\therefore p_{hl-ran} = a^{N/2} \rho^{(d_i+d_j+\dots+d_k)} \approx a^{N/2} \rho^{M/2}
 \end{aligned} \tag{18}$$

则整个网络的半毁伤概率:

$$p_{half-random} = C_N^{N/2} \times p_{hl-ran} \approx C_N^{N/2} \times a^{N/2} \rho^{M/2} \quad )$$

## 2、BA 网络半毁伤概率分析

对于 BA 网络, 要将它的一半节点毁伤, 在节点的选择上也有  $C_N^{N/2}$  种选择方案, 每种方案下, 网络系统的半毁伤概率为:

$$\begin{aligned}
 p_{hl-BA} &= p_{v_i} \times p_{v_j} \times \dots \times p_{v_k} \quad (i, j, \dots, k \text{ 总数为 } N/2) \\
 &= (a\rho^{d_i}) \times (a\rho^{d_j}) \times \dots \times (a\rho^{d_k}) \\
 &= a^{N/2} \rho^{(d_i+d_j+\dots+d_k)}
 \end{aligned} \tag{20}$$

因为 BA 网络节点的度相差较大, 例如: 度序列排名在前一半的节点度之和要远大于后一半的节点度之和。在前面给出的度序列的例子中, 其总边数为 223, 前 25 个节点的总边数为 146, 后 25 个节点的总边数为 77, 两者相差近一倍。此时不能采用随机网络中所采用的近似方法进行处理。

由于  $C_N^{N/2}$  种组合的复杂性, 及每种组合的复杂性, BA 网络半毁伤概率已经无法用一种明确的解析表达出来。但我们可以比较随机网络与 BA 网络半毁伤概率的大小。

## 3、BA 网络与随机网络半毁伤概率大小比较

假设 BA 网络和随机网络的节点数, 总边数相等。则两种网络的半毁伤概率之差为:

$$p_{half-BA} - p_{half-ran} \approx p_{half-BA} - C_N^{N/2} \times p_{hl-ran} \tag{21}$$

通过对 BA 网络  $C_N^{N/2}$  种组合的分析, 我们发现, 在这  $C_N^{N/2}$  种组合中, 存在一种特殊关系。即如果存在一种组合  $A$ , 其中所选择毁伤的一半节点是  $(j_1, j_2, \dots, j_k)$ , 则必然存在另一种互补的组合  $\bar{A}$ ,  $\bar{A}$  中的节点正是没有被 A 选中, 剩下的另一半节点。这样, 在所有的  $C_N^{N/2}$  种组合中, 两两互补。我们可将这  $C_N^{N/2}$  种组合分成  $C_N^{N/2}/2$  种两两互补的组合对  $\left\{ (A_1, \bar{A}_1) \quad (A_2, \bar{A}_2) \quad \left( A_{C_N^{N/2}/2}, \bar{A}_{C_N^{N/2}/2} \right) \right\}$ 。

设组合  $A$  内的节点总边数为  $L$ , 则组合  $\bar{A}$  中的节点总边数为  $M-L$ 。组合对  $(A, \bar{A})$  中两种组合的半毁伤概率和为:

$$p_{h-(A, \bar{A})} = a^{N/2} \rho^L + a^{N/2} \rho^{(M-L)} = a^{N/2} [\rho^L + \rho^{(M-L)}] \tag{22}$$

这样 BA 网络与随机网络半毁伤概率之差为:

$$P_{half-BA} - P_{half-ran} \approx \sum_{k=1}^{\frac{C_N^{N/2}}{2}} \left\{ a^{N/2} [\rho^{L_k} + \rho^{(M-L_k)}] - 2a^{N/2} \rho^{M/2} \right\} \quad (23)$$

因为函数  $\rho^x$  ( $0 < \rho < 1$ ,  $x > 0$ ) 是一个递减的凹函数, 所以:

$$\begin{aligned} \rho^{x_i} + \rho^{x_j} &> 2\rho^{\frac{(x_i+x_j)}{2}} \quad \forall x_i, x_j \quad (0 < \rho < 1, \quad x_i, x_j > 0) \\ \Rightarrow \rho^L + \rho^{(M-L)} &> 2\rho^{M/2} \\ \Rightarrow P_{half-BA} &> P_{half-ran} \end{aligned} \quad (24)$$

即 BA 网络的半毁伤概率大于随机网络的半毁伤概率, 也就是说: 在设计的打击策略下, BA 网络半毁伤抗毁性能要比随机网络的抗毁性能差, 要将 BA 网络的一半节点毁伤所需要的时间比较随机网络的时间短。

根据上述网络半毁伤概率的分析可知: BA 网络的半毁伤概率分析过程同样适合于其它的节点度分布不均匀的情况, 即如果网络中节点的度差异性越大, 分布越不均匀, 则其网络半毁伤的概率越大, 抗毁性能越差。

### VIII、复杂网络抗毁性仿真分析

虽然我们已经推导了 BA 网络和随机网络在节点数和总边数相等情况下各自的抗毁性, 但仿真分析的结果如何呢? 是否一致? 如果不一致, 则不一致的原因在哪? 为此, 我们分别对当复杂网络具有不同类型网络结构, 网络微观连接模式时的抗毁性进行了仿真分析。

#### A、仿真初始条件

外界环境: 网络系统的外界环境为一个 600\*600 二维平面, 所有的网络节点

Agent 都必须在环境内部, 其移动不得超出环境的边界。外界环境如下图 3 所示:

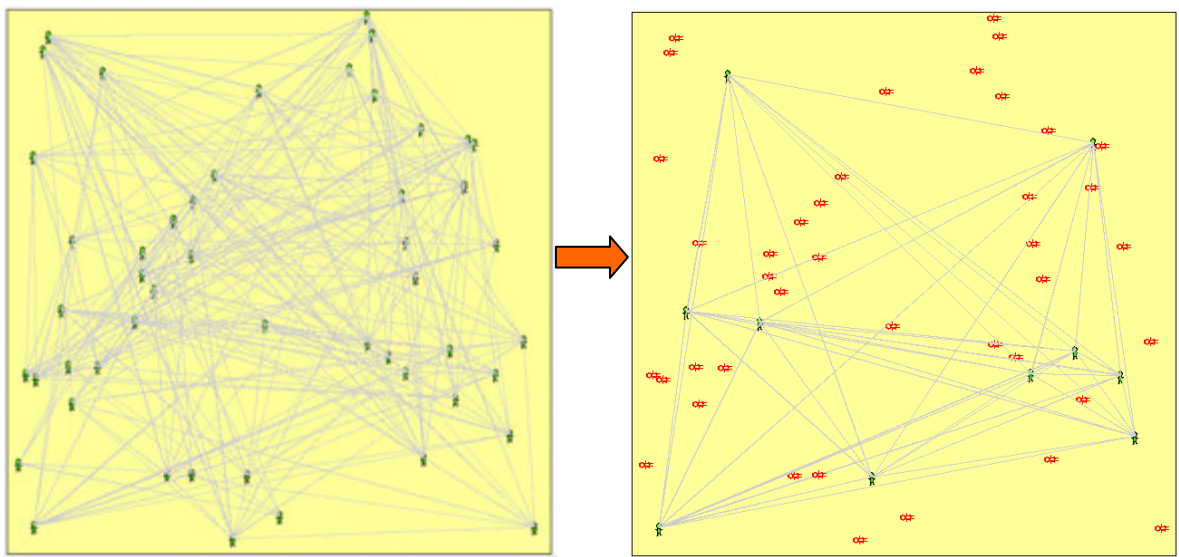


图 3: 复杂网络抗毁性仿真图

**网络节点数量：**从理论上讲网络数量可以无限多，但考虑到仿真计算的运算能力，如果节点数量太大，则仿真速度将很慢，不利于仿真结果的分析，所以节点数量选定为 50。

**网络节点位置：**任何一个节点可以定位于环境中的任一位置，但在我们的仿真中，我们设定所有的节点是随机分布在整个网络环境中。

**网络节点状态：**仿真中，网络节点只有两种状态，分别是“存活”与“死亡”当节点处于“存活”状态时，它用一个绿色的、站立的小人表示。当节点变成孤立节点，处于“死亡”状态时，它用一个红色的、躺着的小人表示。

**网络总边数：**在仿真中，我们设定网络的总边数为 250。这样，每个节点平均有 10 条连接边。

**网络结构：**在仿真中，我们设计了两种主要的网络结构。分别是 BA 网络和随机网络。BA 网络的度序列为：{43,38,34,29,27,24,22,19,18,16,15,14,13,12,11,10,9,9,8,8,8,7,7,6,6,6,5,5,5,5,4,4,4,4,4,4,3,3,3,3,3,3,3,2,2,2,2,2} 随机网络为一个所有节点的度均为 10 的随机连接网络。

**节点抗毁性参数：**在仿真中，设  $a = 0.8, \rho = 0.75$ 。

## B、不同类型网络抗毁性仿真分析

如果仿真初始条件如前面所述。分别对 BA 网络和随机网络各自进行 10 次半毁伤和全毁伤抗毁性仿真，在每次仿真过程中，网络拓扑结构保持不变。10 次仿真的仿真结果及平均所需半毁伤和全毁伤时间如下表 1 所示：

表 1：不同结构类型的复杂网络半、全毁伤仿真结果

编号	NO1	NO2	NO 3	NO 4	NO 5	NO 6	NO 7	NO 8	NO 9	NO 10	平均值
BA 网络半毁伤所需时间	181	130	236	290	189	218	282	225	319	268	233.8
随机网络半毁伤所需时间	377	376	339	281	383	347	418	273	296	431	352.1
BA 网络全毁伤所需时间	2351	1916	1517	2917	1265	1255	1958	1910	1208	1306	1760.3
随机网络全毁伤所需时间	683	746	740	803	573	514	736	500	788	918	700.1

从上面表 1 的仿真结果可以看出，BA 网络半毁伤所需要的打击时间平均为 233.8 个仿真周期，小于随机连接网络的平均值 352.1 个仿真结果。这个结果与前面解析分析的结论：BA 网络抗毁性能要比随机网络的抗毁性能差的结果吻合。

但是 BA 网络全毁伤所需要的打击时间平均为 1760.3 个仿真周期，远大于随机连接网络的平均值 700.1 个仿真结果。这个结果与解析前面解析分析的结果：两种网络的全毁伤概率相等不相符。

出现解析分析与仿真分析结果不相符的原因是什么呢？通过分析，我们发现，在解析分析过程中，复杂网络系统的抗毁性是对每个节点个体抗毁性的一种线性综合。每个节点 Agent 的抗毁性只与它的连接边数量相关联，与它所连接的节点无关。但在仿真过程中我们可以看到，当复杂网络为 BA 网络时，网络节点度分

布极不均匀，最大的度为 43，最小的只有 2。这样，在进行半毁伤仿真中，被毁伤的绝大部分是连接边数量较少的网络节点。去掉网络中一半节点所需要时间较短。但是由于 BA 网络中存在极少数度很大的节点，例如最大度为 43 的节点，其毁伤概率为：

$$p_{\min} = a\rho^{d^{\max}} = 0.8 \times (0.75)^{43} = 3.3941e^{-6} \quad (26)$$

这说明要将单个节点毁伤是极其困难的。正由于 BA 网络中存在少数极难毁伤的节点，所以，BA 网络的全毁伤时间要远大于随机网络。

在复杂网络抗毁性全毁伤仿真中，所采用的打击模式是一种随机打击，抗毁性评价目标是一种完全抗毁性。它的仿真结果“BA 网络相比于随机网络抗毁性较强”与在无标度网络经常提到的“无标度网络对于随机打击具有较强的抗毁性”的结论一致。

### C、网络微观结构对复杂网络系统抗毁性影响的仿真分析

从前面复杂网络系统抗毁性毁伤的解析分析时可知，如果两个网络具有相同的度分布，则不管网络内部节点相互之间是如何相连接的，其半毁伤和全毁伤的概率都是一样的。即只要网络的度分布一样，其半毁伤和全毁伤的抗毁性能就是一样的。但是，从直观上讲，采用“富—富”相联策略的网络和采用“富—贫”相联策略网络的全毁伤抗毁性应该不同，同配网络比非同配网络的全毁伤抗毁性能要强。

对此，我们设计了一个仿真，分别对两个具有相同节点数，总边数和度分布序列的同配网络和非同配网络的半毁伤和全毁伤抗毁性能进行了仿真，仿真结果如下表 2 所示：

表 2：同配与非同配 BA 网络半、全毁伤仿真结果

编号	NO1	NO2	NO 3	NO 4	NO 5	NO 6	NO 7	NO 8	NO 9	NO 10	平均值
同配网络半毁伤所需时间	181	130	236	290	189	218	282	225	319	268	233.8
非同配网络半毁伤所需时间	153	187	237	393	256	247	203	163	241	161	224.1
同配网络全毁伤所需时间	2351	1916	1517	2917	1265	1255	1958	1910	1208	1306	1760.3
非同配网络全毁伤所需时间	1187	1217	1165	972	1410	1518	1112	1012	1061	1165	1181.9

从上述仿真结果可以看出，同配网络与非同配网络的半毁伤时间分别为 233.8 和 224.1，两者相差无几。说明同配网络和非同配网络的半毁伤抗毁性能差不多。但是同配网络与非同配网络的全毁伤时间相差较大，分别是 1760.3 和 1181.9。非同配网络全毁伤时间只有同配网络的 2/3。这说明同配网络的全毁伤抗毁性要强于非同配网络。这一仿真结果与解析结果不一致，其不一致的原因是什么？

通过对同配网络和非同配网络全毁伤仿真过程的单步分析，我们发现，造成非同配网络的全毁伤抗毁性要弱于同配网络原因是：当网络内部采用“富—贫”相联策略时，由于“贫”节点的度较少，其节点抗毁性较差，仿真不久就被较毁伤，它所连接的边很早就被删除，导致与它相联的“富”节点的连接边数量跟着动态下降，度降低，毁伤概率增大，抗毁性能变差。最终由于“贫—富”相联中，贫对富的“诛连”作用，使



“富”得被拖“贫”，“贫”的被拖毁。使得“富”节点不能长久地坚持下去，导致了网络系统整体全毁伤抗毁性的降低。而“富—富”相联的同配网络，所有“富”节点的高抗毁性保证了整个网络系统的高抗毁性。

事实上，当我们保持网络节点数量不变，将网络系统的总边数由 250 降低到 50，即每个节点平均连接边数量为 2 时，也可得到类似的结果。仿真结果如下表 3 所示：

表 3：总边数为 50 的同配与非同配 BA 网络半、全毁伤仿真结果

编号	NO1	NO2	NO 3	NO 4	NO 5	NO 6	NO 7	NO 8	NO 9	NO 10	平均值
同配网络半毁伤所需时间	51	42	51	46	49	38	53	41	56	46	47.3
非同配网络半毁伤所需时间	60	78	59	51	67	43	57	53	42	56.9	60
同配网络全毁伤所需时间	110	210	219	102	164	175	272	307	138	147	184.4
非同配网络全毁伤所需时间	213	162	212	166	159	165	128	136	182	147	167

从上表仿真结果看出，当网络系统的总边数减少时，由于总边数太少，以至于“富”节点与“贫”节点相差不大，“富—富”相联和“富—贫”相联的差别也不大，所以同配网络和非同配网络全毁伤抗毁性差不多，同配网络全毁伤抗毁性只稍强于非同配网络的全毁伤抗毁性。

从上述仿真分析可知：网络内部的微观结果对网络系统的抗毁性也有很大的影响，采用解析分析的方法无法描述毁伤过程中节点间的动态关联关系，较难分析和计算出这种毁伤过程中的影响作用的大小，而仿真分析的方法却能较好地解决这一问题。

#### D、节点动态网络系统抗毁性影响的仿真分析

在疾病传染网络中，复杂网络节点的移动肯定会影响节点被传染和传染他人的概率。在通讯网络中，网络节点可能是会移动的雷通讯电台，电台的快速移动可能会提高它抗毁性，降低它被毁伤的概率。这种网络节点移动行为对网络系统抗毁性的影响是很难用解析分析的方法来进行研究的。而用仿真的方法则可以定性、定量地分析出各种网络节点行为对网络系统抗毁性的影响大小。

设其它仿真条件与前面一样，保持复杂网络系统节点数、总边数和拓扑结构及微观连接方法不变，我们来分析网络节点移动行为对网络抗毁性的影响。

在仿真中，每个节点新增一个属性值  $r$ ，表示节点的移动半径。网络节点的移动半径大小随机分布于区间  $[1, 4]$  内。不同的节点，其移动半径可能不同。

网络系统新增一个参数  $L$ ，表示打击半径。我们设  $L=10$ 。

我们设定网络节点的随机移动规则为：每个仿真周期，每个“存活”的节点 Agent，随机选择一个离它在位置距离不超过  $r$  的新位置，然后移动到新位置。如果新位置处于系统环境之外，则 Agent 原地不动。

由于节点的随机移动，其毁伤概率将发生变化，所以我们将打击模式修改如下：

- 1、 每个仿真周期，按 Agent 的编号，依次选择一个 Agent，作为本周期的打击选中对象。如果 Agent 总数为 N，则经过 N 个仿真周期，每个 Agent 都被选中一次。
- 2、 如果经过 T 个仿真周期的延迟后，如果节点 Agent 仍在以被选中时的位置为圆心，半径为 L 的圆内，即仍处于打击范围内。则节点 Agent 将以概率 P 毁伤。P 越大，Agent 被毁伤的越大。当 P 很小时，Agent 即使多次遭受打击，也不会有任何损伤。如果不在打击范围内，则不执行打击。
- 3、 每个被毁伤的 Agent，生命状态将由“存活”变成“死亡”，并删除它与其它节点 Agent 间的所有连接。
- 4、 进入下一仿真周期。

从常理上讲，基于前面网络节点行为的设计，新的具有随机移动行为的复杂网络的抗毁性应该要比静态随机网络的抗毁性要好。因为节点的移动，可能会降低节点的毁伤机率，提高节点的抗毁性，而不可能降低节点的抗毁性。所以从解析分析的结果可知：复杂动态网络的抗毁性要比静态网络的抗毁性好。对此我们可以进行解析分析。

### 1、复杂动态网络全毁伤概率分析

在网络节点没有移动行为时，每个节点的毁伤概率为： $p_{vi} = a\rho^{di}$ 。当节点有移动行为时，从前面的打击模式可以看出，移动可能会使节点运动到打击范围之外，降低节点毁伤概率。假设节点运动到打击范围外的概率为  $b$  ( $0 \leq b \leq 1$ )，则：

$$\begin{aligned}
 p_{vi-move} &= (1-b)(a\rho^{di}) \leq p_{vi} = a\rho^{di} \quad (0 \leq b \leq 1) \\
 \Rightarrow P_{total-move} &= P_{v_1-move} \times P_{v_2-move} \times \cdots \times P_{v_N-move} \\
 &\leq p_{v_1} \times p_{v_2} \times \cdots \times p_{v_N} = P_{total-static}
 \end{aligned}
 \tag{27}$$

由上面的解析分析可知，节点随机移动网络的全毁伤抗毁性要比静态随机网络的全毁伤抗毁性要好。同样可推导出节点随机移动网络的半毁伤抗毁性要比静态随机网络的半毁伤抗毁性要好。

同时，我们对节点随机移动网络和静态随机网络的抗毁性分别进行了仿真，看仿真结果与解析结果是否一致。节点随机移动网络、静态随机网络抗毁性仿真结果如下表 4 所示：

表 4：节点随机移动网络、静态随机网络半、全毁伤仿真结果

编号	NO1	NO2	NO 3	NO 4	NO 5	NO 6	NO 7	NO 8	NO 9	NO 10	平均值
节点随机移动网络半毁伤时间	192	241	192	430	380	226	395	191	243	191	268.1
静态随机网络半毁伤时间	181	130	236	290	189	218	282	225	319	268	233.8
节点随机移动网络全毁伤时间	2005	1464	1563	1805	1918	1113	1207	1458	1663	1604	1580
静态随机网络全毁伤时间	2351	1916	1517	2917	1265	1255	1958	1910	1208	1306	1760.3

从上面表 4 可知：节点随机移动网络平均半毁伤时间为 268.1，比静态随机网络的 233.8 要稍长，说明节

点随机移动网络在半毁伤评价标准下，其抗毁性要略优于静态随机网络的抗毁性，或者相一致。这一结果与解析分析的结果一致。

从上面表 4 也可知：节点随机移动网络平均全毁伤时间为 1580，与静态随机网络的 1760.3 相差不大，稍小一点。说明节点随机移动网络在全毁伤评价标准下，其抗毁性要劣于静态随机网络的抗毁性。节点的随机移动不但没有提高其抗毁性，反而降低了其抗毁性。这一结果与常理不符，也与解析分析的结果不一致。甚至相反。通过对节点移动规则，打击模式的深入分析，我们认为，当网络节点具有随机移动行为时，其移出打击范围的概率不大，节点随机移动网络的抗毁性与静态网络的抗毁性相差不多。仿真结果中出现 1580 小于 1760 的现象，是由于仿真试验的次数不够，没能完全消除随机因素对结果的干扰。当随机机动的效果不明显时，随机因素带来的干扰影响大于随机移动所带来的影响。所以在仿真结果中，节点随机移动网络全毁伤抗毁性和静态随机网络全毁伤抗毁性相差不多。

当节点机动半径大幅增加。或者是节点采用的是较规则的战术机动行为时，节点随机移动网络全毁伤抗毁性要比静态随机网络全毁伤抗毁性高不少。

所以，网络节点的机动行为会在一定程度上提高节点随机移动网络的抗毁性能。但不是所有类型的节点移动行为都是提高抗毁性的有效手段。必须针对外界打击的模式，设计特定的“适应性机动行为”，才能真正有效地提高动态网络系统的抗毁性。至于如何发现、设计、选择出较优的“适应性机动行为”则是复杂动态网络抗毁性优化所需要研究的一个问题。

## E、结构动态变化网络抗毁性影响的仿真分析

在前面复杂网络节点移动行为对网络系统抗毁性影响的研究中，网络节点采取了随机移动行为，这种移动行为只影响到网络节点本身的抗毁性，并没有影响到网络的拓扑结构，他对网络系统抗毁性的影响是间接的，影响力不大。如果其行为还影响到网络的拓扑结构，使得这种网络成为名符其实的动态网络后，其抗毁性受影响的程序又将如何呢？

在军事系统中，战术机动网络就是这样的典型网络，由于战术电台体积、功率、保密等因素的约束和限制，战术电台只有与它有限距离内的其它电台相连接。随着战争的推进，部队的机动，战术电台也处于不断地移动过程中，它所能连接上的其它电台也在不断地变化，整个军事系统的通讯网络结构也随之发生变化。在这种情况下，结构动态变化网络的抗毁性不但与节点的行为、节点的抗毁性有关，也与网络结构的动态变化相关联。

对于这种结构动态变化网络，因为网络节点 Agent 是随机移动的，其连接对象也是随机变化的。任何时刻，网络的拓扑结构是随机变化、无法确定的。它的抗毁性能不能用解析分析的方法明确地求解出来。但我们可以采用仿真的方法来定性、定量地分析这种复杂网络节点行为、动态结构变化对网络系统抗毁性的影响。

设外界打击策略不变，网络节点随机移动行为不变，但节点连接关系发生了变化，在每个仿真周期，每个节点都要重新选择、连接离它较近的邻居节点 Agent，组成一个新的网络。网络节点 Agent 的动态重联规则如下：

**网络节点 Agent 的动态重联规则：**每个仿真周期，每个“存活”的 Agent 搜索距离它不超过其探测距离  $L_i$  的所有其它处于“存活”状态的 Agent 编号，建立于它们的连接关系。

为了提高结构动态变化网络与其它网络，特别是静态随机网络的可比性，我们要尽量使得动态、静态网络的总边数一致。在前面网络设计中，静态随机网络节点的平均连接边数量为 10。则在结构动态变化网络中，我们要基本保证每个网络节点在其可连接范围内，平均节点数为 11（包括它自身）。因为网络外界环境总面积为  $600 \times 600$ ，节点总数为 50。因此

$$\frac{\pi L_i^2}{600 \times 600} = \frac{11}{50} \quad (28)$$

$$\Rightarrow L_i \approx 158.78$$

所以，我们设每个节点Agent的探测距离  $L_i = 159$ 。

### 1、结构动态变化网络半、全毁伤概率分析

因为仿真一开始，所有 50 个节点都是均匀随机分布在环境之中的，而仿真过程中所有节点的移动方向和距离都是一个随机值，所以仿真过程中的节点也都是随机均匀分布的。根据前面推导的节点的探测距离  $L_i$  的大小可知，在任何时刻，每个节点探测范围内的节点数量平均值应该为 10。所以每个节点连接边数量的平均值为 10，单个节点的抗毁性为  $p_{vi} \approx a\rho^{10}$ 。这种情况与前面静态随机网络中节点的毁伤概率一样。这样结构动态变化网络的半毁伤和全毁伤概率也应该与前面静态随机网络的半毁伤、全毁伤概率一样，分别是：

$$p_{half-dynamic} \approx C_N^{N/2} \times a^{N/2} \rho^{M/2} \quad (29)$$

$$p_{total-dynamic} \approx a^N \rho^M$$

### 2、结构动态变化网络半、全毁伤抗毁性仿真分析

我们对结构动态变化网络的半毁伤和全毁伤抗毁性分别进行仿真，看仿真结果与解析结果是否一致，并比较它与节点随机移动网络及静态随机网络的抗毁性水平。

其中，一次结构动态变化网络抗毁性仿真的过程截图如下图 4 所示：

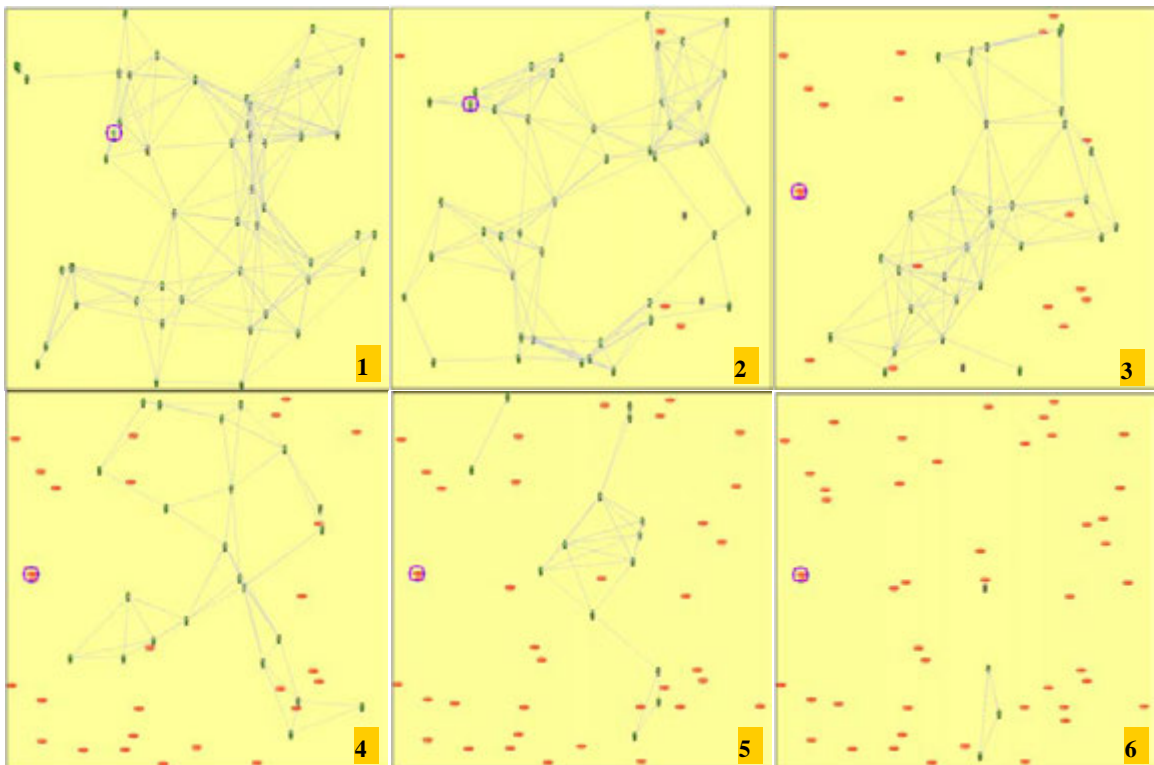


图 4：结构动态变化网络抗毁性仿真的过程截图

结构动态变化网络抗毁性仿真过程中“存活”节点数量变化曲线如下图 5 所示：

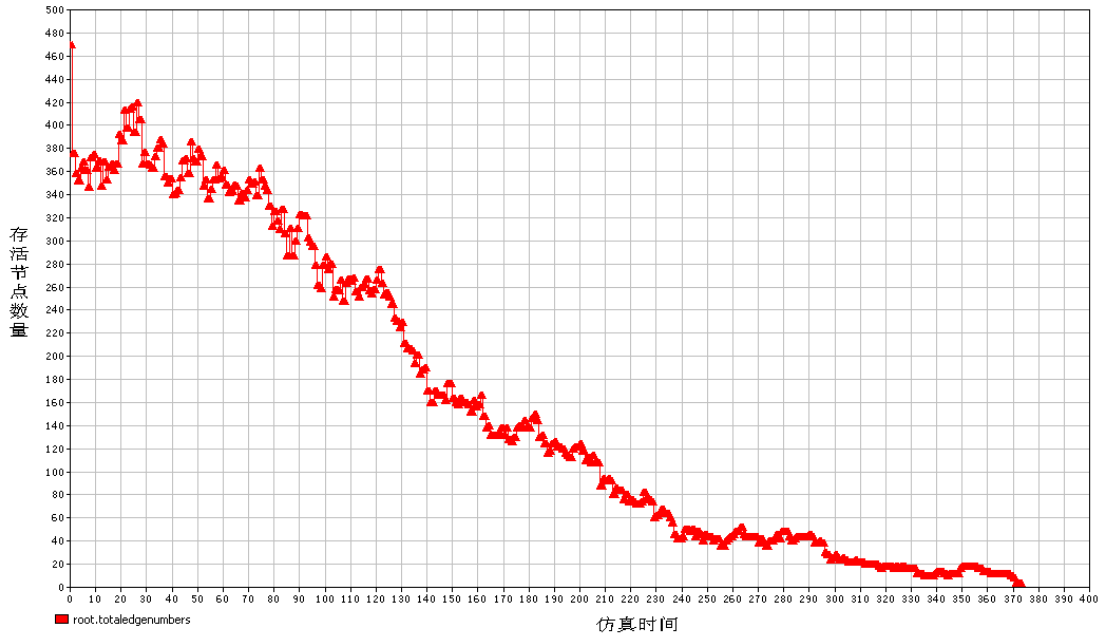


图 5：“存活”节点数量变化曲线

结构动态变化网络、节点随机移动网络和静态随机网络的半、全毁伤仿真结果如下表 5 所示：

表 5：节点动态网络、结构动态网络和静态随机网络半、全毁伤仿真结果

编号	NO1	NO2	NO 3	NO 4	NO 5	NO 6	NO 7	NO 8	NO 9	NO 10	平均值
结构动态变化网络半毁伤时间	103	165	166	112	164	149	190	182	184	141	155.6
节点随机移动网络半毁伤时间	192	241	192	430	380	226	395	191	243	191	268.1
静态随机网络半毁伤时间	377	376	339	281	383	347	418	273	296	431	352.1
结构动态变化网络全毁伤时间	339	320	328	327	235	325	262	333	406	395	327

节点随机移动网络全毁伤时间	2005	1464	1563	1805	1918	1113	1207	1458	1663	1604	1580
静态随机网络全毁伤时间	683	746	740	803	573	514	736	500	788	918	700.1

从上述表 5 结果中可知：结构动态变化网络、节点随机移动网络和静态随机网络的平均半毁伤时间分别为 155.6, 268.1: :352.1。而三种网络的平均全毁伤时间分别为 327: 1580: 700。说明静态随机网络的半毁伤抗毁性优于节点动态变化网络，而节点随机移动网络又优于结构动态变化网络。全毁伤抗毁性的排序列情况不同于半毁伤抗毁性排序，节点随机移动网络的全毁伤抗毁性优于静态随机网络，而静态随机网络又优于结构动态变化网络。但不管按哪个评价标准，结构动态变化网络的抗毁性都是最差的。这一仿真结果与解析推导结果（结构动态变化网络半、全毁伤概率与静态随机网络相等）不相符。

通过对解析推导过程及仿真过程的分析研究，及仿真结果与解析结果的对比分析可知：结构动态变化网络虽然在理论上，每个节点的抗毁性与其它两种网络一样，但由于节点的随机移动，使得每个节点都有可能远离整个节点 Agent 群体，导致其连接边数量降低，毁伤概率提高，抗毁性降低情况的出现。由于毁伤概率与连接边数量成指数关系，当一个节点的连接边数量从 10 降低到 1 时，其毁伤概率提高了约 13.4 倍，处在这一危险情况时，其被毁伤的可能性大大提高。而在整个仿真过程中，对于每一个节点 Agent，出现这种危险情况的机会都还不少，所以整个网络系统这种危险情况出现较频率，导致整个结构动态变化网络系统的抗毁性大大降低。

## IX、总结

复杂网络的抗毁性研究是复杂网络理论方法研究中的一个研究重点，它对复杂网络理论的研究具有重要的理论意义，也具有现实的应用价值。传统的研究方法偏重于研究静态随机网络拓扑结构的抗毁性，在复杂动态网络抗毁性研究上还存在不少不足之处。传统的基于图论的和解析分析的抗毁性研究方法在复杂动态网络抗毁性研究上仍然具有一定的价值，但已经远远满足不了复杂动态网络抗毁性研究的需要。为此，我们提出了一个基于多 Agent 的复杂动态网络抗毁性仿真分析方法，并用它研究了在考虑节点抗毁性情况下，复杂网络拓扑结构对复杂网络抗毁性的影响，网络微观连接结构对复杂网络抗毁性的影响。研究了网络节点随机移动行为及结构动态变化对复杂网络系统抗毁性的影响。并把仿真结果与解析分析的结果进行了对比分析。研究了两种方法产生不一致，甚至出现矛盾的原因。通过对上述问题的对比研究也说明解析方法在复杂动态网络抗毁性研究上的不足，及基于多 Agent 的复杂动态网络抗毁性仿真分析方法在复杂动态网络抗毁性研究上有效性和正确性。

事实上，我们的研究也还有不少考虑不充分之处。例如因计算机速度的原因，网络节点数量太少，离复杂网络的规模较远，仿真次数较少，有些结果还存在一定误差。复杂网络动态性对其抗毁性的影响还不够，这都是我们下一步需要改进和进一步研究的内容与方向。

参考文献

- [1] Frank H, Frisch I T. Analysis and design of survivable network. IEEE Transaction on Communication Technology, 1970, COM-18 (5): 567-662
- [2] Cohen R, Erez K, ben-Avraham D, et al. Resilience of the Internet to random breakdowns. Phys. Rev. Lett., 2000, 85 (21): 4626-4628
- [3] Newman M E J, Strogatz S H, Watts D J. Random graphs with arbitrary degree distributions and their applications. Phys. Rev. E, 2001, 64 (2): 26118
- [4] Broadbent S R, Hammersley J M. Percolation processes: I. Crystals and mazes. Proc Cambridge Philos Soc, 1957, 53: 629-641
- [5] Hammersley J M. Percolation processes: II. The connective constant. Proc. Cambridge Philos. Soc., 1957, 53: 642-645
- [6] Cohen R, Erez K, ben-Avraham D. Breakdown of the Internet under Intentional Attack. Phys. Rev. Lett., 2001, 86 (16): 3682-3685
- [7] Dorogovtsev S N, Mendes J F F. Comment on "Breakdown of the Internet under intentional attack". Phys. Rev. Lett. , 2001, 87 (21): 219801
- [8] Callaway D S, Newman M E J, Strogatz S H, et al. Network robustness and fragility: percolation on random graphs. Phys. Rev. Lett., 2000, 85 (25): 5468-5471
- [9] Broder A, Kumar R, Maghoul F, et al. Graph structure in the Web. Comput. Netw., 2000, 33 (1): 309-320
- [10] Amaral L A N, Scala A, Barthélémy M, et al. Classes of behavior of small-world networks. Proc. Natl. Acad. Sci. U.S.A, 2000, 97: 11149-11152
- [11] Schwarte N, Cohen R, Ben-Avraham D, et al. Percolation in directed scale-free networks. Phys. Rev. E, 2002, 66 (1): 015104
- [12] Gallos L K, Cohen R, Argyrakis P, et al. Stability and topology of scale-free networks under attack and defense strategies. Phys. Rev. Lett., 2005, 94 (18): 188701
- [13] Vázquez A, Moreno Y. Resilience to damage of graphs with degree correlations. Phys. Rev. E, 2003, 67: 015101
- [14] Warren C P, Sander L M, Sokolov I. Geography in a scale-free network model. Phys. Rev. E, 2002, 66: 056105
- [15] Rozenfeld A F, Cohen R, ben Avraham D, et al. Scale-free networks on lattices. Phys. Rev. Lett. , 2002, 89: 218701
- [16] Jeong H, Mason S, Barabási A-L, et al. Lethality and centrality in protein networks. Nature, 2001, 411: 41-42
- [17] Dunne J A, Williams R J, Martinez N D. Network structure and biodiversity loss in food webs:Robustness increases with connectance. Ecology Letters, 2002, 5: 558-567
- [18] Newman M E J, Forrest S, Balthrop J. Email networks and the spread of computer viruses. Phys. Rev. E, 2002, 66 (3): 035101
- [19] Magoni D. Tearing down the Internet. IEEE J. Sel. Areas Commun., 2003, 21 (6): 949-960

- [20] Samant K, Bhattacharyya S. Topology, search, and fault tolerance in unstructured P2P networks. In: Proceedings of the Hawaii International Conference on System Sciences. Piscataway: IEEE Computer Society, 2004. 4607-4612
- [21] Holme P, Kim B J, Yoon C N, et al. Attack vulnerability of complex networks. Phys. Rev. E, 2002, 65 (5): 056109
- [22] Barthelemy M. Betweenness centrality in large complex networks. Euro. Phys. J. B, 2004, 38 (2): 163-168
- [23] Freeman L C. A set of measures of centrality based upon betweenness. Sociometry, 1997, 40: 35-41
- [24] Goh K-I, Oh E, Jeong H, et al. Classification of scale-free networks. Proc. Natl. Acad.Sci. USA, 2002, 99: 12583-12588