复杂网络抗毁性研究的主要科学问题*

谭跃进，吕　欣，吴　俊，邓宏钟
（国防科技大学 信息系统与管理学院，长沙 410073）

摘要： 网络抗毁性是指在网络中的节点(边)发生自然失效或遭受故意攻击的条件下，网络维持其功能的能力．文章简要介绍了复杂网络抗毁性理论的发展，结合北美大停电、台湾地震、我国南方冰雪灾害等导致的网络事故，分析了复杂网络抗毁性研究的主要科学问题，并提出了复杂网络抗毁性研究的一般框架．

关键词： 复杂网络；抗毁性；无标度网络；研究框架

Main Scientific Problems for the Invulnerability Research of Complex Networks

TAN Yue-jin, LV Xin, WU Jun, DENG Hong-zhong
(School of Information Systems and Management, National University of Defense Technology, Changsha 410073, China)

Abstract: Network invulnerability is defined as the network's ability of maintaining its function under suffering natural failures or intentional attacks. Together with the network accidents caused by North America electricity blackout, Taiwan earthquake and Chinese southern ice-snow disaster, a brief description for the progress of complex networks invulnerability research is presented. Furthermore, main scientific problems for the invulnerability research of complex networks are discussed and a general research framework is constructed.

Key words: complex networks; invulnerability; scale-free network; research framework

1 引言

21 世纪以来，以信息技术的飞速发展为基础，人类社会加快了网络化进程，从交通运输网络到电力供应网络，从 Internet 到 WWW，从科研合作网络到各种经济、政治、社会关系网络等，无不与人们的生活息息相关，可以说，人们已经生活在一个充满着各种各样的复杂网络的世界中．

在过去的 40 多年里，科学家们惯于将复杂网络看作是随机网络[1]，在随机网络模型中，各个节点之间的连接是随机的，整个网络是均匀的，连接度分布服从泊松分布，其分布图是一条钟型的曲线．很显然，现实世界中的网络不可能是完全随机的，复杂网络背后一定隐藏了很多潜在的一般属性．1999 年，印第安纳州圣母大学物理学教授 Barabàsi 等[2]在对万维网拓扑结构进行研究时发现，万维网基本上是由少数高连通性的页面串连起来的，80% 以上页面的连接数不到 4 个，而占节点总数不到万分之一的极少数节点，却和 1000 个以上的节点连接，即网络中

* **资助项目** 国家自然科学基金(70501032；70771111)

大部分的节点只有少数连接,而少数节点则拥有大量的连接,他们把这种网络称为"无标度网络". 科学家们通过大量的实证研究发现,现实生活中的大部分网络,包括信息网络[3]、社会网络[4]和生物网络[5]等都具有无标度特性.

现实网络的无标度特性表明,网络中存在一些具有大量连接的"关键节点",虽然这些节点只占整个网络中节点的极少比例,但却对网络发挥功能具有重要作用. 一旦这些关键节点出现故障或遭到故意攻击,将会严重影响整个网络的性能. 此外,现实中的电力网络、通信网络、计算机网络、物流网络、金融网络等网络中节点和节点之间的联系错综复杂,除了那些连接数量众多,显然处于核心地位的关键节点外,网络中往往还存在一些不引人注目的、难以发现却又能对网络性能产生重要影响的节点,一旦这些节点发生故障,可能引发级联效应,导致大规模网络故障或导致整个网络系统瘫痪. 现实生活中不乏这样的例子.

在电力网络中,2003 年 8 月,美国俄亥俄州的三条超高压输电线路发生故障,随即导致该地区一个发电厂关闭,由于该发电厂所处的北美电力网使用的是同步交流电网,该电厂发生事故的频率异动瞬间波及全网,产生级联崩溃效应,导致美国的 8 个州和加拿大的 2 个省发生大规模停电,约 5000 万居民受到影响,损失负荷量 61800MW,经济损失约 300 亿美元. 同年 8 月 28 日,英国首都伦敦发生了两个多小时的重大停电事故,导致伦敦三分之二的地铁停运,一度有 25 万余人被困在地铁中;9 月 23 日,丹麦首都哥本哈根及其邻国瑞典部分地区发生大面积停电事故,近 400 万用户受到影响;9 月 28 日,意大利发生历史上首次全国性大停电,境内仅有撒丁岛幸免,引起了全国性的混乱[6]. 大停电事故的频频发生,引起了科学界和工程界的高度重视:为什么与人们生活密切相关的电力网络却如此脆弱? 其他国家网络基础设施是否也同样脆弱?

2006 年 12 月,南海台湾附近发生地震,导致台湾地区的 6 条主要的国际海底电缆遭受破坏,仅剩下两条部分可以运作,其它全部中断,这一事故导致整个亚太地区的互联网服务几近瘫痪,远至欧美澳洲均大受影响,至少 19 个国家及地区的通信受影响,大量海外客户的金融、商贸无法交易,许多业务一个多月后才恢复正常.

2008 年 1 月 25 日,在持续了十多天的冰雪天气后,湖南郴州一架巨大输电塔轰然倒下,一条 10 万伏的高压线搭在了其下 2.5 万伏的铁路接触网上,导致配电所跳闸断电,N582 次列车行驶至湖南耒阳时失去电力,拉开了湖南地区电网崩溃,交通瘫痪,人员滞留的序幕. 25 日晚,连锁反应使数十辆列车被迫停在铁路线上,仅到 1 月 26 日凌晨,京广线上就有 136 列客车晚点,20 万人滞留广州火车站. 与此同时,由于冰冻难行,京珠高速公路也陷入半瘫痪状态,在湖南段滞留的车辆和旅客、司机一度达到 2.7 万辆、8 万人,堵塞距离长达 190 公里. 在湖南省,输电塔倒塌和主干输电线路受灾停运导致除湘西北张家界与常德之外的怀化、湘西、邵阳、娄底、湘潭、衡阳、郴州、永州等地区的电网与华中电网断开,解网运行,造成郴州、衡阳、永州、怀化四市大面积停电. 冰雪灾害期间,江西电网先后 5 次与华中主网解裂,500kV 网架基本瘫痪,省内电网一度解裂成 3 片运行,全省 80%的城乡地区相继出现大面积停电,其中 45 个县城和 806 个乡镇遭遇全部停电,220kV 电网一度面临瓦解. 浙江、安徽、江苏、福建、湖北、四川、重庆、贵州、云南、广西、广东等电网的电力设施均遭到不同程度破坏,局部地区由于电力设施毁坏严重使电力供应中断达 10 余天之久. 电网和交通的瘫痪使一些县城、乡镇成了孤岛,交通瘫痪、电力中断、供水停止、燃料告急、食物紧张……

越来越频繁发生的事故将一个严峻的问题摆在我们面前:我们的网络到底有多可靠? 一

些微不足道的事故隐患是否会导致整个网络系统的级联崩溃？在面对敌对势力蓄意破坏的情况下，我们的网络是否还能正常发挥作用？这些都是复杂网络抗毁性研究需要回答的问题.

2 网络抗毁性的定义

现实网络是复杂多样的，不同类型网络的结构和功能存在很大差异，因此，在不同领域中，网络抗毁性的定义也不尽一致，并常常与网络可靠性(reliability)、鲁棒性(robustness)生存性(survivability)、有效性(availability)等指标混用，不加区分.

在通信领域，一般认为抗毁性是指网络拓扑结构的可靠性，即为了中断部分节点之间的通信需要破坏的最少节点数或链路数，常用连通度、粘聚度、端端可靠度.[7, 8]等作为抗毁性的测度指标. 这一定义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，它衡量的是破坏一个系统的难度.

在军事领域，抗毁性通常指系统在受到敌方物理破坏或火力攻击环境下，在规定的时间内，完成规定功能的能力.[9]. 该定义强调了敌方的主动攻击性，即网络节点(边)发生故障的原因来源于外部故意攻击，对于一个军事网络系统来说，这种攻击可以是电磁信号干扰而导致网络通讯中断或破坏保障网络的重要枢纽以切断物资供应等.

由此可见，尽管研究领域不同，网络抗毁性考虑的都是在一定破坏策略下，网络在若干部件出现故障后持续作用的能力. 这种破坏可以是源自于网络系统内部发生的随机故障，也可以是来自网络系统外界的有目的的攻击. 为此，不失一般性，我们给出网络抗毁性的如下定义：

网络抗毁性是指在网络中的节点(边)发生自然失效或遭受故意攻击的条件下，网络维持其功能的能力.

上述定义表明，要开展网络抗毁性研究，至少应该完成下面三个方面的工作：

(1) 网络失效模式的选择. 我们知道，网络部件的失效，既可以是各种自然因素引起的，也可以是人为故意攻击导致的. 那么，如何能更全面地考虑各种可能对网络产生影响的破坏？是否存在某种最优攻击策略？只有在充分考虑了各种攻击策略的情况下，才能对网络的抗毁性具有充分的认识，进而有效地采取措施来提高网络的抗毁生存能力.

(2) 网络功能的度量. 不同网络实现的功能是不同的，物流网络希望节点之间能以最短的距离运输物资，通信网络希望节点之间能保持连通以交流信息，这导致在开展抗毁性研究时，随着研究对象的不同，对网络功能的度量也不相同. 科学合理地选择网络功能的度量指标，是有效地进行网络抗毁性评价的前提条件.

(3) 网络维护策略. 在对网络抗毁性进行科学系统的分析之后，有必要制定不同失效模式下的网络维护策略，包括网络监控、网络保护、网络修复、网络应急措施等，从而有效地提高网络抗毁性.

3 复杂网络抗毁性研究的主要科学问题

复杂网络抗毁性研究的目的就是为了正确地分析评价复杂网络的抗毁性，发现网络中的安全隐患和薄弱环节，从而采取有效的优化措施，提高网络的抗毁性. 前面我们给出了网络抗

毁性的定义,提出了三个需要完成的工作,实际上,这些正是复杂网络抗毁性研究需要解决的科学问题.

3.1 复杂网络抗毁性评价指标

复杂网络的抗毁性指网络功能在各种失效模式下持续作用的能力,往往被定义为网络在发生失效后网络整体性能的下降值. 因此,为了评价复杂网络抗毁性,首先必须对网络功能进行合理的度量. 如在物资配送网络中,平均最短路距离就可作为一个有效的网络功能度量指标. 在道路或仓储节点发生故障后,网络抗毁性就可以由平均最短路距离的增加值来衡量. 显然,平均最短路距离增加的越多,说明网络性能下降的越快,网络抗毁性越差. 在2000年Albert等.[10]的开创性研究中,他们同时选择了极大连通片尺寸与网络规模之比和极大连通片平均最短路径作为网络功能度量指标. Vito Latora等[11]在对美国光纤网、波士顿地铁网等几种实际网络中进行实证分析过程中,定义了网络的易毁性(Vulnerability)

$$V[S,D] = \frac{\Phi[S] - W[S,D]}{\Phi[S]}$$

为区间[0,1]上的函数,其中$\Phi[S]$为某网络功能度量指标下没有受到攻击时的值,$W[S,D]$为在各种可能的攻击情况下,该指标的最小值. 类似地,定义网络的恢复性(Improvability)

$$IM[S,I] = \frac{B[S,I] - \Phi[S]}{\Phi[S]}$$

$B[S,I]$为在各种可能的恢复情况下,网络功能度量指标的最大值.

可见,只有在充分了解特定复杂网络的性质和功能的基础上,制定合理的网络功能度量指标,才能进一步进行复杂网络抗毁性评价,在对各项抗毁性指标研究的基础上,分析指标之间的相互关系,构建规范、系统的复杂网络抗毁性评价指标体系. 分析验证其完备性、系统性及各指标之间的独立性. 根据确定的抗毁性评价指标体系,尤其是针对一些NP难的度量参数,设计快速有效的算法.

构建复杂网络抗毁性评价指标体系的一个重要方面,就是对复杂网络中关键节点的识别和标识. 复杂网络节点的"关键性"和"重要性"是一个动态的、发展的概念. 它与以下多方面的因素密切相关:1)与网络节点、边的属性、性能和价值相关;2)与节点、边在网络拓扑结构中所处的位置相关;3)与往络上的负载、流(物资、信息等)相关;4)与网络系统的演化方向、规律及动态变化情况相关;5)与网络系统的设计目标,所要完成的任务,实现的功能相关. 在不同的网络中,这些关键节点可以是重要的网络服务器,可以是整个网络流的交通枢纽,可以是重要的作战指挥部,此外,还可能是一些不易发现、却极容易引起网络级联故障的隐蔽节点. 这些关键节点对维持整个网络的功能起着十分重要的作用. 因此,在网络系统不断演化发展情况下,使用复杂网络抗毁性评价指标,从大量的节点中识别出影响网络抗毁性的"关键"节点,综合评价、度量其抗毁性,进而采取有效的防护措施,防止其出现故障,对于提高整个网络的抗毁性具有重要的实际意义.

3.2 复杂网络的抗毁性研究建模方法

总的来说,可以采用解析和仿真的方法来研究复杂网络抗毁性. 前者需要综合利用图论、

概率论、复杂性理论、统计物理等理论和方法建立复杂网络抗毁性的解析模型，包括静态结构抗毁性模型、动态级联失效模型等. 使用解析法时，通过分析模型的解或研究模型的解的形态，可以比较准确地获得系统状态变化信息. 缺点是考虑因素少，要进行假设和简化，除了一些理想的和相对简单的情况，只在严格限定的假设条件下才有效. 对于大型复杂网络抗毁性研究，有时难以建立解析模型. 而后者可以采用基于 Agent 建模仿真方法，建立复杂网络抗毁性的仿真模型，研究网络的个体行为是如何涌现出整体行为的，因此，在复杂网络系统抗毁性研究领域具有十分重要的应用前景.

然而，无论是建立解析或仿真模型，都必须考虑如下的问题：

首先是攻击策略的设计或选择. 在研究复杂网络抗毁性的建模过程中，一般情况下是以一定的规则将节点或边移除作为攻击策略来观察网络性能的变化. 使用最广泛也是最简单的攻击规则就是将节点按照度的大小顺序移除[10,12]，然而，按照度来移除节点并不一定是最优的攻击策略，度并不总是代表节点的重要程度. 比如对于存在流量和负载的复杂网络，使用介数[12, 13]的就可能更加符合实际.

其次是对所攻击网络认识水平的假设，目前的研究大多都是基于完美的信息，即假设攻击者了解网络的所有信息，然而在实际网络对抗中，攻击者对网络的整体知识是很难全面掌握的，往往只能得到一部分网络的信息(称为“不完全信息”)，而对于网络中的其他部分信息只具有不确定的认识(称为“不确定信息”)[14-16].

此外，攻击者还需要了解网络面临攻击时采取的应急措施，比如修复，隐蔽，加强保护等[17]. 因为实际网络中对关键节点的保护要远远高于一般节点，这导致如果攻击这些关键节点，攻击这自身也将付出较高的代价. 这种考虑网络节点保护和攻击代价、基于不完全信息和不确定信息建立的复杂网络抗毁性模型，将是复杂网络抗毁性研究从理论走向实践的必由之路.

3.3 复杂网络抗毁性的影响因素

影响复杂网络抗毁性有很多，其中拓扑结构是影响复杂网络抗毁性的重要因素. Albert 等.[10]的研究表明，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，在故意攻击下，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，表明无标度网络面对故意攻击显得异常脆弱. Valente 等[18]在广义随机网上的抗毁性研究表明，当单独考虑随机失效或选择性攻击时，最优度分布为双峰分布(two-peak distribution，bimodal)，但当同时综合考虑随机失效和选择性攻击时，最优度分布为三峰分布(three - peak distribution)，即 $p(k_{min}) + p(k^*) + p(k_{max}) = 1$，其中 $k_{min} < k^* < k_{max}$.

从网络拓扑结构出发主要关注的是网络的静态抗毁性，不考虑节点(边)失效的动态关联，即总是假设一个节点(边)的失效不会导致其它节点(边)的失效. 在这种假设下，少数几个节点的失效不会导致整个网络的崩溃，而实际上大多数网络上是有负载的，这些负载可以是物质、信息或能量，可以是具体的，也可以是抽象的. 一般来说，网络中节点承受负载的能力是有限的，即节点的负载容量是有限的，同时，网络上的负载是动态变化的，特别是当网络结构发生改变，如节点的加入、移除，网络上的负载将重新分配. 有限的负载容量和负载的重新分配使得负载网络的抗毁性问题变得更加复杂：一个节点的失效导致网络负载的重分配，负载的重分配使得某些节点上的负载超过其负载容量而失效，这些节点的失效又可能导致其他节点的“级

联失效"(cascading failure). 因此,不同失效模式下网络中节点的动态行为、网络流的路由策略等同样是影响复杂网络抗毁性的重要因素. 我们建立复杂网络抗毁性模型,进行解析和仿真分析,其目的就是要通过对复杂网络宏观与微观属性、静态与动态行为的定性、定量刻画,分析这些属性与行为之间的相互关联特征,探索研究复杂网络各种属性与行为对抗毁性的影响,明确抗毁性好的网络应该具有的要素,为复杂网络抗毁性的设计、优化、控制提供理论依据.

3.4 复杂网络抗毁性优化策略

研究复杂网络抗毁性的最终目的,就是得到一个抗毁性好的复杂网络. 复杂网络抗毁性优化设计主要包括三个层次:

网络拓扑结构的优化设计. 一般情况下,增加网络中节点或边的数量,能缩短网络节点之间的最短路距离,提高网络连通性,从而当面临打击时,网络可以通过其他节点和边保持工作能力. 若给定网络节点的数量、节点间的连接链路和成本,网络抗毁性拓扑结构优化的目标就是如何以最少的成本,建设一个满足一定度量指标要求的网络.

网络容量的优化设计. 网络容量是影响网络性能的重要因素,在网络流的传递过程中,极有可能因为某些关键节点或边的容量限制而导致网络阻塞,进而引发导致全网崩溃的"级联失效". 如何在有限成本下增加网络中部分节点或边的容量以最大限度地提高网络抗毁性能,就是网络容量优化设计的目标.

路由策略的优化设计. 好的路由策略是网络持续发挥作用的基础,包括静态路由策略和动态路由策略.

很多网络优化问题被证明是 NP 难的,因此,神经网络、遗传算法、禁忌搜索等启发式算法被广泛应用于研究这类问题.

在复杂网络抗毁性研究的实际应用中,往往不是重新设计、构建一个网络,而是在已有网络的基础上,提出具体的抗毁性优化策略. 以交通运输网络为例,抗毁性优化策略涉及如何新建一些道路以增加网络流量,如何采取一定的收费或法规手段合理疏导交通,如何在道路损毁、交通堵塞的情况下采取相应的应急措施(应急预案)等. 此外,在对网络安全性有较高要求的国家基础设施网络、军事指挥通信网络中,复杂网络抗毁性的优化设计还包括网络的最优防御策略研究,最优故障修复策略研究等. 从网络防御研究出发,进一步可以研究复杂网络的最优攻击策略.

4 复杂网络抗毁性研究的一般框架

从对上述科学问题的讨论可以发现,复杂网络抗毁性研究的主要内容集中在下述四个方面:(1) 结合网络功能,对实际复杂网络进行实证研究;(2) 复杂网络抗毁性指标研究;(3) 复杂网络抗毁性建模研究;(4) 复杂网络抗毁性评价与优化研究.

图 1 给出了复杂网络抗毁性研究的一般框架:首先根据所研究复杂网络的功能特点,制定合适的抗毁性度量指标,继而采用不同的网络失效模式和修复策略,建立复杂网络抗毁性模型,根据模型的解析和仿真分析结果对复杂网络抗毁性进行评价. 重复进行建模到评价这一过程即可找到适合该复杂网络的有效攻击策略或修复策略. 抗毁性评价的结果用于指导所研究网络的抗毁性优化设计.

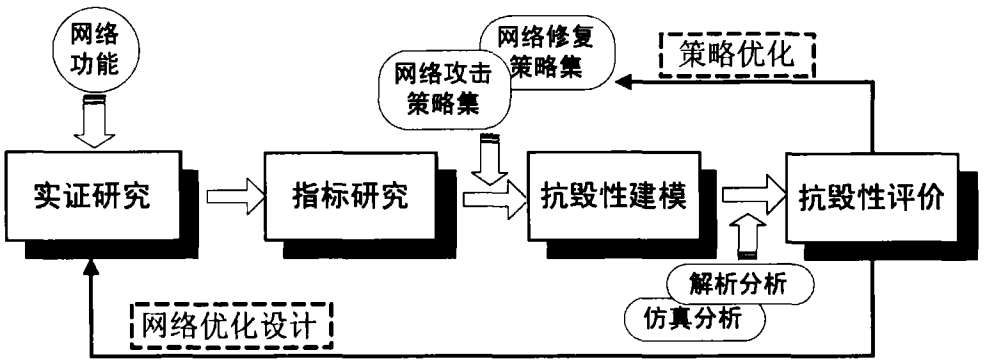

图 1　复杂网络抗毁性研究框架

5　结束语

目前我国复杂网络抗毁性研究水平与国外相比还有很大差距，具体表现在原创性工作较少，研究面宽泛而不够深入，没有形成一个完整的理论体系，此外，关于考虑成本的网络攻击、网络在面临打击时的最优应急策略等还很少有人研究.

频频爆发的网络事故给我们敲响了警钟：如何规划电网、交通网、通信网等国家基础设施网络，使其在面临自然灾害时也能正常工作？如何在网络发生故障时采取合理的应急预案，避免造成整个网络的级联崩溃？如何通过抗毁性分析识别网络中的薄弱环节或关键单元，从而采取保护或优化措施以提高整个网络的抗毁性？这些将是未来复杂网络抗毁性研究的重要方向.

复杂网络理论的研究目前已经发展成物理学、控制科学、生物学、管理学等几乎所有学科的前沿热点问题，复杂网络抗毁性研究也日益吸引了更多研究者的注意力，其研究成果（尤其是在无标度网络上）已经在很大程度上改变和拓展了我们对网络抗毁性的认识. 由于复杂网络不仅仅是一种常见的复杂系统的结构形态，它还可以作为复杂系统结构拓扑特性的模型，因而复杂网络抗毁性研究必将对复杂系统的抗毁性研究产生重大的推动作用，成为系统科学的一个重要研究内容.

参考文献：

[1] Erdö P, Rényi A. On random graphs. Publ. Math., 1959, 6: 290 - 297.

[2] Barabási A - L, Albert R. Emergence of scaling in random networks. Science, 1999, 286 (5439): 509 - 512.

[3] Vóquez A, Pastor-Satorras R, Vespignani A. Large-scale topological and dynamical properties of the internet. Phys. Rev. E, 2002, 65 (6): 066130.

[4] Amaral L A N, Scala A, Barthélémy M, Stanley H E. Classes of behavior of small-world networks. Proc. Natl. Acad. Sci. U.S.A, 2000, 97: 11149 - 11152.

[5] Sporns O. Network analysis, complexity, and brain function. Complexity, 2002, 8 (1): 56 - 60.

[6] 孙可，韩祯祥，曹一家. 复杂电网连锁故障模型评述. 电网技术，2005，29 (13)：1 - 9.

[7] 罗鹏程，金光，周经纶，刘琦. 通信网可靠性研究综述. 小型微型计算机系统，2000，21 (10)：73 - 77.

[8] 刘啸林. 网络抗毁性研究介绍. 计算机应用与软件，2007，24 (6)：135 - 136.

[9] 李德毅，于全，江光杰. C^3I 系统可靠性、抗毁性和抗干扰的统一评测. 系统工程理论与实践，1997，17

(3): 23 - 27.

[10] Albert R, Jeong H, Barabási A -L. Error and attack tolerance of complex networks. Nature, 2000, 406 (6794): 378 - 382.

[11] Vito Latora, Massimo Marchiori. Vulnerability and protection of infrastructure networks. Phys. Rev. E, 2005, 71: 015103(R).

[12] Petter Holme, Beom Jun Kim, Chang No Yoon, Seung Kee Han. Attack vulnerability of complex networks. Phys. Rev. E, 2002, 65 (5): 056109.

[13] Barthelemy M. Betweenness centrality in large complex networks. Euro. Phys. J. B, 2004, 38 (2): 163 - 168.

[14] Wu J, Deng HZ, Tan YJ, LI Y, Zhu DZ. Attack vulnerability of complex networks based on local information. MODERN PHYSICS LETTERS B, 2007, 21 (16): 1007 - 1014.

[15] Wu J, Deng HZ, Tan YJ, Zhu DZ. Vulnerability of complex networks under intentional attack with incomplete information. Journal of Physics A - Mathematical and Thoretical, 2007, 40 (11): 2665 - 2671.

[16] Wu J, Tan YJ, Deng HZ, LI Yong. A robustness model of complex networks with tunable attack information parameter. Chinese Physics Letter, 2007, 24 (7): 2138 - 2141.

[17] Lazaros K Gallos, Reuven Cohen, Panos Argyrakis, Armin Bunde, Shlomo Havlin. Stability and topology of scale-free networks under attack and defense srategies. Phys. Rev. Lett., 2005, 94 (18): 188701.

[18] Andre X. C. N. Valente, Abhijit Sarkar, Howard A. Stone. Two-peak and three-peak optimal complex networks. Phys. Rev. Lett., 2004, 92 (11): 118702.