

编号: 1000-6788(2008)S0-0116-05

复杂网络抗毁性研究若干问题的思考

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: 通过对复杂网络抗毁性研究的应用背景描述和对学科领域间网络抗毁性的理解差异分析, 给出了网络抗毁性的一般性定义——网络抗毁性是指在网络中的节点(或边)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。文章进一步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; 框架; 一般性定义

中图分类号: N949

文献标志码: A

On 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: Based on the analysis of application backgrounds and different understandings of network invulnerability among research fields, a general definition of network invulnerability is proposed—which denotes the ability of maintaining the network function under conditions of suffering random failures or intentional attacks. Furthermore, main scientific problems for the research of network invulnerability are discussed and a general research framework is constructed.

Key words: complex networks; invulnerability; scale-free networks; framework; general definition

1 无标度网络与阿喀琉斯之踵

我们被网络包围着, 几乎所有的复杂系统都可以抽象成网络, 这些网络往往有着大量的节点, 节点之间有着复杂多变的连接关系。例如, 人类社会是人通过各种社会关系连成的网络, 军事系统是由人和装备组成的一个网络, 因特网是由路由器和计算机连成的网络, 万维网是由大量页面通过超链接组成的网络, 神经系统可以看作大量神经细胞通过神经纤维相互连接形成的网络, 甚至世界贸易、城市经济都可以描述成一个网络。

1999年, Barabási等^[1]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。其度分布并不是预期的那样服从属于随机图的钟形曲线, 而是服从幂法则($P(k) \sim k^{-\lambda}$), 在这种分布下, 网络中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^[2]、社会网络^[3]和生物网络^[4]等都具有无标度特性。

随着复杂网络无标度性的发现和无标度网络模型的提出, 复杂网络理论的研究进入了无标度网络时代。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论意义和应用价值也日益凸现出来。

Albert等^[5]在2000年发表于《Nature》上的一篇文章中分别把ER随机网络和BA无标度网络置于两种

收稿日期: 2007-10-19

资助项目: 国家自然科学基金(70501032, 70771111)

作者简介: 谭跃进(1958-), 男, 国防科技大学信息系统与管理学院教授, 博士生导师, 主要研究方向为系统理论与系统集成。

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(相当于网络节点的随机失效);在另外一种打击中,则按照节点连接度从大到小的顺序移除节点(相当于网节点的故意攻击)。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“关键节点”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。无标度网络这种双重特性(robust-yet-fragile)被形象地称为“Achilles' heel”。

2 我们的网络到底有多可靠?

Albert 等的研究激起了大量研究人员研究网络抗毁性的兴趣。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,总体研究结果几乎都与 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^[6-9]。

现实网络的无标度特性导致网络中存在一些具有大量连接的“关键节点”,虽然只占整个网络中节点的极少部分,但却对网络发挥其功能具有重要作用。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的停电事故,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^[10]。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,只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。

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

3 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^[11]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^[12]。该定义强调了敌方的主动攻击性,即网络节点(或边)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(或边)发生随机失效或遭受故意攻击的条件下,网络维持其功能的能力。

上述定义表示,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。我们已经知道,网络部件的失效,既可以是各种随机因素引起的,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。

4 复杂网络抗毁性研究的主要科学问题

4.1 复杂网络抗毁性研究的科学问题

复杂网络抗毁性研究的目的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。

4.1.1 如何度量复杂网络的抗毁性?

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。如在物流配送网络中,平均最短路径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径距离的增加值来衡量。显然,平均最短路径距离增加的越多,说明网络性能下降的越快,网络抗毁性越差。在2000年Albert等的开创性研究中,他们则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。

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,才能进一步建立复杂网络抗毁性评价指标,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^[13,14]。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)与网络上的负载、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。

4.1.2 怎样研究复杂网络的抗毁性？

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,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.对于存在流量和负载的复杂网络,使用介数可能更加符合实际.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”).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.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.

4.1.3 什么样的复杂网络抗毁性好？

拓扑结构是影响复杂网络抗毁性的重要因素,Albert 等的研究表明,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^[15]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 $k_{\min} < k^* < k_{\max}$.

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.

4.1.4 怎样得到抗毁性好的复杂网络？

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:拓扑结构的优化设计,链路容量的优化设计,路由策略的优化设计.目前的抗毁性优化设计模型集中于拓扑结构的优化,主要讨论了两个方面的问题:一是在满足网络连通性的要求下,使得总费用最少;二是在给定费用的前提下,使得网络的连通性最大.仿真方法在复杂网络抗毁性优化设计中具有重要作用.此外,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.

4.2 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:一、结合网络功能,对实际复杂网络进行实证研究;二、复杂网络抗毁性评价指标研究;三、复杂网络抗毁性建模;四、复杂网络抗毁性评价与优化.

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攻击和修复策略,建立复杂网络抗毁性模型,根据模型的解析和仿真分

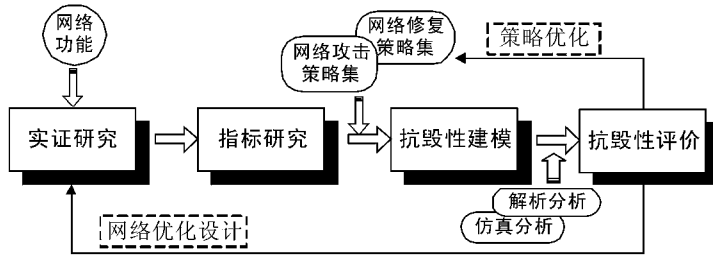


图1 复杂网络抗毁性研究框架

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.

5 结束语

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引起更多的注意力,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] Barabási A-L, Albert R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509 - 512.
- [2] Vázquez A, Pastor-Satorras R, Vespignani A. Large-scale topological and dynamical properties of the Internet[J]. Phys Rev E, 2002, 65(6): 066130.
- [3] Amaral L A N, Scala A, Barthélémy M, et al. Classes of behavior of small-world networks[J]. Proc Natl Acad Sci U. S. A, 2000, 97 11149 - 11152.
- [4] Sporns O. Network analysis, complexity, and brain function[J]. Complexity, 2002, 8(1): 56 - 60.
- [5] Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(6794): 378 - 382.
- [6] Magoni D. Tearing down the internet[J]. IEEE J Sel Areas Commun, 2003, 21(6): 949 - 960.
- [7] Jeong H, Mason S, Barabási A-L, et al. Lethality and centrality in protein networks[J]. Nature, 2001, 411 41 - 42.
- [8] Dunne J A, Williams R J, Martinez N D. Network structure and biodiversity loss in food webs: Robustness increases with connectance[J]. Ecology Letters, 2002, 5 558 - 567.
- [9] Newman M E J, Forrest S, Balthrop J. Email networks and the spread of computer viruses[J]. Phys Rev E, 2002, 66(3): 035101.
- [10] 孙可, 韩祯祥, 曹一家. 复杂电网连锁故障模型评述[J]. 电网技术, 2005, 29(13): 1 - 9.
- [11] 罗鹏程, 金光, 周经纶, 等. 通信网可靠性研究综述[J]. 小型微型计算机系统, 2000, 21(10): 73 - 77.
- [12] 李德毅, 于全, 江光杰. C³I系统可靠性、抗毁性和抗干扰的统一评测[J]. 系统工程理论与实践, 1997, 17(3): 23 - 27.
- [13] 谭跃进, 吴俊, 邓宏钟. 复杂网络中节点重要度评估的节点收缩方法[J]. 系统工程理论与实践, 2006, 26(11): 79 - 83.
- [14] 吴俊, 谭跃进, 邓宏钟, 等. 考虑级联失效的复杂负载网络节点重要性评估[J]. 小型微型计算机系统, 2007, 28(4): 627 - 630.
- [15] Valente A X C N, Sarkar A, Stone H A. Two-peak and three-peak optimal complex networks[J]. Phys Rev Lett, 2004, 92(11): 118702.