复杂网络抗毁性研究及其军事应用

谭跃进， 吕欣
（国防科技大学 信息系统与管理学院， 长沙 410073）

摘要：自从小世界效应和无标度特性发现以来，复杂网络的研究在过去几年得到了迅速发展，其中复杂网络的抗毁性是研究焦点之一。本文简介了无标度网络的发现及其特性，在提出了网络抗毁性的定义的基础上，介绍了复杂网络抗毁性理论的研究内容，并对复杂网络抗毁性研究的军事应用进行了阐述。最后，对复杂网络抗毁性研究进行了总结和展望。

关键词： 复杂网络，军事网络，抗毁性，无标度网络

Review on the Invulnerability of Complex Networks and Its Military Application

TAN Yue-jin, LV Xin
（School of information systems and management, National University of Defense Technology, Changsha 410073, China）

Abstract: In the past few years, the discovery of small-world and scale-free properties has stimulated a great deal of interest in studying the underlying organizing principles of various complex networks. As a focus, the study on invulnerability of complex networks has made quick progress along with the development of complex network theory. In this paper, the discovery of scale-free networks and their properties is introduced briefly firstly. And then the content of complex networks invulnerability research is concluded, as well as its military applications. Finally, the open questions and development trend are summarized and discussed.

Keywords: complex networks, military networks, invulnerability, scale-free network

1 引言

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，其中许多研究成果很大程度上改变和拓展了我们对于现实网络的认识。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。

2 网络抗毁性

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。如在通信领域，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[5, 6]等作为抗毁性的测度指标。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[7]。

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

*收稿日期：
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综合集成。

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。

3 复杂网络抗毁性理论研究内容

Albert 等[8]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；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。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”。

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[9-12]，总体来说，复杂网络抗毁性理论研究内容可以归纳为如下四个方面：

3.1 复杂网络抗毁性评价指标研究

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[8]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。此外，网络抗毁性评价的常用指标还有粘聚度和连通度等[13]。

Vito Latora 等[14]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。

3.2 复杂网络的抗毁性建模方法研究

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。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[8, 15]，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[15, 16]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”）[17-19]。

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[20]。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研究

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[8]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[21]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）。

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。

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军事应用

在军事系统中，复杂网络抗毁性研究具有特殊的重要意义。40 多年以来，军事指挥控制系统的体系结构发生了很大的变化，已从原先的以指挥控制为中心，依次演变为以通信、平台（战车、飞机、舰艇等）、网络为中心，交战双方不仅是武器装备的较量，更是各种网络系统之间的对抗。

4.1 军事综合电子信息系统

随着科学技术的进步，军事综合电子信息系统的功能逐渐增强，结构也越来越复杂，发生故障的可能性也越来越大。作为作战体系的神经中枢，军事综合电子信息系统在信息化战争中发挥着兵力倍增器的作用——前提是系统能够在复杂多变的战场环境下保持高抗毁性。战场上的军事综合电子信息

系统发生故障时，往往会严重地降低部队的整体战斗力，使部队处于被动挨打的境地。因此，军事综合电子信息系统的抗毁性是一项基本要求。

4.2 指挥通信网

目前，指挥通信网络逐步形成了以太空、空基、地面、水上、水下、地下等指挥设施、机构为节点，以有线通信、无线通信、数据链等各种通信方式为联系的复杂网络。特别是太空被视为下一个“战略制高点”，它将决定空中、陆地和海洋的控制权。这些网络系统中的一些“关键”节点,如军事卫星或一根光纤的失效或被毁，都可能产生连锁发应，导致整个军事指挥通信网络系统功能瘫痪，从而影响战争的成败。因此，研究军事网络及其“关键”节点的抗毁性具有重要的现实意义。

4.3 传感器网络

网络中心的提出与实施使得战争观念发生了重大转变，并产生了新的作战能力，即协同交战能力(CEC)。CEC 的实质就是把高性能传感器网络与高性能交战网络有机地结合起来。高效的传感器网络能快速生成交战质量的态势信息，交战网络则可把这一态势信息转化成更高的作战能力。传感器网络是网络中心战实现的技术关键，它融合来自多传感器的数据，产生具有交战质量的合成信息，该信息所产生的对作战空间的了解超过任何单独传感器所能获得的对作战空间的了解。

我们必须认真对待发展一种高度依赖于单项资源（如一个超级网络）的作战学说所带来的风险。历史表明，在所依赖的主要技术系统失效之后要维持作战能力是十分困难的。换句话说，一个不可靠的网络比没有网络更糟糕。传感器网络中传感器节点数量巨大、分布广泛，整个网络中包含了大量的精密设备以及为了使系统协调工作所必须的无数网络接口，而且整个网络是不断扩展和动态变化的。因此如何保证传感器网络的可靠性是一个不容忽视的问题，它直接关系到协同交战能力的发挥。

4.4 野战地域通信网

野战地域通信网是一种满足战争需要的特殊的通信网，它通常在一个进攻和防御方向适应一个集团军内外通信的需要，覆盖大约一个集团军的展开区域。它充分的利用了现代通信的量新技术，并行成了自己的特点。现代战争是多兵种的协同行动，在一定的区域内集中了大量的人力和物资，强度大大增加，战场形势瞬息万变。先进的计算机技术，自动控制技术的应用，已使现代战场完全数字化了。如何把各种数字信息快速、安全地传送到需要的地方，成了是否能量大限度的利用各种资源打败敌人的决定因素之一。各个国家根据各自战略要求纷纷建立了野战地域通信网。如英国的“松鸡”系统，法国的“里达”系统. 美国的 MSE 系统(移动用户设备)。它们都具有移动性强、全数字化、可自动交换、保密性能高，具有抗破坏性等待点。可以支持保密话、数据交换、传真等多种业务，特别是美国的 MSE 系统量具有代表性，在“沙漠风暴”行动中经受住了考验。对野战地域通信网的干扰是目前通信对抗领域研究的热点及难点之一，而准确分析野战地域通信网的抗毁性能是探讨对其进行干扰的前提条件。

4.5 其他网络系统

此外，对于交通运输网络、电力网络、信息网络等，这些网络不仅是关系国计民生的国家基础设施网络，也是军事网络系统的重要组成部分，如，综合保障网络中基地、兵站、仓库、供应站等保障实体之间就必然依托交通运输网络（铁路、公路等）来进行资源的合理调配和部署。

即使在平时，这些网络的抗毁性能也是也是一个关键的问题，不论对保障人民正常的生产生活还是保障军事任务的准确、及时执行，都具有重要意义。

各种各样的自然灾害（地震、冰雪）对这些基础网络设施的破坏，严重考验网络的抗毁能力，典型的如 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 年初发生在我国南方的重大冰灾造成的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？在意外事故发生后，如何采取相应的应急措施以最大限度地降低（避免）损失？这些都是复杂网络抗毁性研究需要回答的问题。

5 结束语

目前我国复杂网络抗毁性研究还处于起步阶段，具体表现在原创性工作较少，研究面宽泛而不够深入，没有形成一套完整的理论体系，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。

在军事领域，应用复杂网络理论来研究军事网络抗毁性的成果还很少，这一方面是由于我们对各种军事网络的结构、功能、复杂性程度了解的不够全面、深入，另一方面是由于我们对网络抗毁能力重要性的认识不够。

在 2008 年的冰雪灾害和汶川大地震的灾难中，自然灾害一再考验我国电力、交通、通信网络的抗毁性能，灾区补给、救援工作因网络设施破坏而严重受阻的现实不得不引起我们的深思：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。

主要参考文献:

1. Barabási, A.-L. and R. Albert, *Emergence of scaling in random networks.* Science, 1999. **286**(5439): p. 509-512.
2. Vázquez, A., R. Pastor-Satorras, and A. Vespignani, *Large-scale topological and dynamical properties of the Internet.* Phys. Rev. E, 2002. **65**(6): p. 066130.
3. Amaral, L.A.N., et al., *Classes of behavior of small-world networks.* Proc. Natl. Acad. Sci. U.S.A, 2000. **97**: p. 11149-11152.
4. Sporns, O., *Network analysis, complexity, and brain function.* Complexity, 2002. **8**(1): p. 56-60.
5. 罗鹏程, *通信网可靠性研究综述.* 小型微型计算机系统, 2000. **21**(10): p. 73-77.
6. 刘啸林, *网络抗毁性研究介绍.* 计算机应用与软件, 2007. **24**(6): p. 135-136.
7. 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. **3**(3): p. 23-27.
8. Albert, R., H. Jeong, and A.-L. Barabási, *Error and attack tolerance of complex networks* Nature, 2000. **406**(6794): p. 378-382.
9. Magoni, D., *Tearing down the Internet.* IEEE J. Sel. Areas Commun., 2003. **21**(6): p. 949-960.
10. Jeong, H., et al., *Lethality and centrality in protein networks.* Nature, 2001. **411**: p. 41-42.
11. Dunne, J.A., R.J. Williams, and N.D. Martinez, *Network structure and biodiversity loss in food webs:Robustness increases with connectance.* Ecology Letters, 2002. **5**: p. 558-567.
12. Newman, M.E.J., S. Forrest, and J. Balthrop, *Email networks and the spread of computer viruses.* Phys. Rev. E, 2002. **66**(3): p. 035101.
13. Frank, H. and I.T. Frisch, *Analysis and design of survivable network.* IEEE Transaction on Communication Technology, 1970. **COM-18**(5): p. 567-662.
14. Latora, V. and M. Marchiori, *Vulnerability and protection of infrastructure networks.* Phys. Rev. E 2005. **71**: p. 015103(R).
15. Holme, P., et al., *Attack vulnerability of complex networks.* Phys. Rev. E, 2002. **65**(5): p. 056109.
16. Barthelemy, M., *Betweenness centrality in large complex networks.* Euro. Phys. J. B, 2004. **38**(2): p. 163-168.
17. J, W., et al., *Attack vulnerability of complex networks based on local information.* MODERN PHYSICS LETTERS B, 2007. **21**(16): p. 1007-1014.
18. J, W., et al., *Vulnerability of complex networks under intentional attack with incomplete information.* Journal of Physics A-Mathematical and Thoretical 2007. **40**(11): p. 2665-2671.
19. J, W., et al., *A robustness model of complex networks with tunable attack information parameter.* Chinese Physics Letter, 2007. **24**(7): p. 2138-2141.
20. Gallos, L.K., et al., *Stability and topology of scale-free networks under attack and defense srategies.* Phys. Rev. Lett., 2005. **94**(18): p. 188701.
21. Valente, A.X.C.N., A. Sarkar, and H.A. Stone, *Two-peak and three-peak optimal complex networks.* Phys. Rev. Lett., 2004. **92**(11): p. 118702.