基于修复策略的舰艇编队复杂网络系统可靠性研究

刘中华[1] 胡 兵[2] 吴荣华[3]
(海军工程大学训练部 武汉 430033)[1] (海军工程大学管理工程系 武汉 430033)[2]
(海军工程大学电子工程学院 武汉 430033)[3]

摘 要 为了研究舰艇编队网络系统的可靠性,在建立舰艇编队网络系统组成模型的基础上,提出了一个舰艇编队复杂网络的修复模型。为了运用概率母函数对临界攻击比例和巨元组相对大小进行解析研究,在该模型的基础上引入了两个变量:攻击比例 f_a 和未受攻击节点的最大度 $\tilde{K}_a$。解析和数值计算表明,修复策略显著提高了无标度网络的可靠性,度指数较小的无标度网络其可靠性提高更大。仿真计算分析表明,所建模型可以应用于研究自我修复能力的复杂网络的可靠性。

关键词 可靠性,修复模型,复杂舰艇编队网络

Studying Reliability of Warship Fleet Complex Networks Based on Repair Tactical

LIU Zhong-hua[1] HU Bing[2] WU Rong-hua[3]
(Dept. of Training, Naval Univ. of Engineering, Wuhan 430033, China)[1]
(Dept. of Management Sci., Naval Univ. of Engineering, Wuhan 430033, China)[2]
(Dept. of Electronic Eng., Naval Univ. of Engineering, Wuhan 430033, China)[3]

Abstract To study the robustness of complex networks under attack and repair, we introduced a repair model of complex networks. Based on the model, we introduced two new quantities, i. e. attack fraction f_a and the maximum degree of the nodes that have never been attacked $\tilde{K}_a$, to study analytically the critical attack fraction and the relative size of the giant component of complex networks under attack and repair, using the method of generating function. We showed analytically and numerically that the repair strategy significantly enhances the robustness of the scale-free network and the effect of robustness improvement is better for the scale-free networks with smaller degree exponent. We discussed the application of our theory to the understanding of robustness of complex networks with reparability.

Keywords Reliability, Repairing model, Warship fleet complex networks

1 引言

随着信息和网络技术的飞速发展,先进的军事技术、超前的作战理念及高效的武器装备使由基于平台的作战向基于网络的作战转变。因此,研究舰艇编队复杂网络的相关技术是快速适应这种新的作战模式、打赢高技术条件下海战的关键。舰艇编队网络是编队实施一体化作战的基础。编队内的探测传感器和参与作战行动的预警机、岸基观通站雷达等探测传感器组成传感器网,编队内武器平台与参与作战的飞机、潜艇等组成作战网,所有指挥控制中心组成指控系统,探测器网、作战网和指控系统通过层次交换机组成整个信息网络,从而极大地提高了信息共享能力和部队行动速度[1-5]。故编队网络复杂性程度极高,舰艇编队复杂网络对于随机失效和故意攻击的可靠性是一个具有显著实际意义的主题,因为它直接影响网络上各过程的效率,它是复杂网络相关文献最先研究的对象之一[6,7]。

我们可以通过对舰艇编队复杂网络的拓扑结构进行优化从而提高复杂网络的可靠性[12-14],但这种方式对于网络可靠性的提高是有限的,而代价往往是网络效率的下降。一种更为有效的方式就是对复杂网络受到的损害进行修复。现实中的网络即使在遭受故意攻击时也不会轻易崩溃的重要原因是复杂网络的自我修复能力。在舰艇编队网络中,受过良好训练的舰员能够完成不太复杂的战时修理任务。一些受损的节点能够被修复,包括具有最大度的节点,如舰艇指挥控制中心。具有自我修复能力的舰艇编队网络使得舰艇编队在敌方的持续火力打击下仍能保持一定的战斗力。本文提出了一个基于修复策略的舰艇编队复杂网络的可靠性模型,且运用该模型研究编队网络的可靠性。

2 舰艇编队复杂网络系统及其修复模型

2.1 舰艇编队网络中心战系统结构组成

基于网络中心战的舰艇编队具有协同作战能力。这里假定:编队内有 n 条舰艇,且均具备网络中心战能力;在功能上,编队内的探测传感器和参与作战行动的预警机、岸基观通站雷达等探测传感器组成传感器网,编队内武器平台与参与作战的飞机、潜艇等组成作战网,所有指挥控制中心组成指控系

本文受海军工程大学基金课题资助。

刘中华(1963-),男,副教授,主要研究方向为装备管理及复杂系统建模。

统，探测器网、作战网和指控系统通过层次交换机组成整个信息网络，从而极大提高了信息共享能力和部队行动速度。舰艇编队复杂网络系统的网络组成如图1所示。

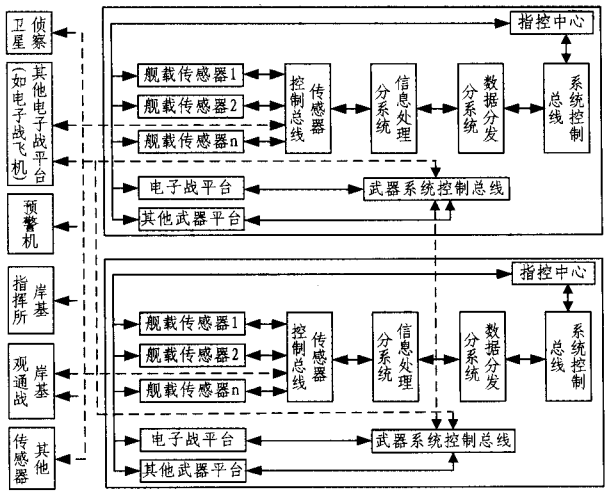

图1　舰艇编队复杂网络系统结构示意图

2.2　作战单元及作战过程抽象

为了更好地反映现代舰艇编队作战过程中的探测、决策、打击等行动，将单方的作战单元抽象为3类，其在网络模型中分别对应3类节点：(1)传感器S：表示侦察、监视类的系统，它包括所有提供作战空间感知的实元，负责接收目标的可测现象并传给决策器。舰艇编队中的传感器包括：舰艇上的雷达、声纳、光电传感器、参与作战行动的预警机、岸基观通站雷达和天基侦察卫星等。(2)决策器D：表示指挥控制的中心，它能接受从传感器或者影响器传来的信息，并对传感器和影响器进行控制协同。舰艇编队中的决策器主要是舰艇指挥控制中心。(3)影响器I：属于行动类武器装备，指直接进行任务行动的武器或装备系统。行动任务不仅包括直接火力的硬打击、降功能干扰的软打击，也包括支援保障行动等。行动类武器装备作为武器装备体系的执行终端，在指挥控制中心（决策器）的指挥下，完成预定的战略目标或作战任务。舰艇编队中的影响器包括：舰艇上的导弹、舰炮、鱼雷、水雷、各种干扰设备、参战飞机上的武器等。这样，舰艇编队的作战系统就可以抽象成由S、D、I 3类节点连接组成的网络。为了简化模型，假设舰艇编队由3类节点组成，并且节点之间能进行连边耦合，而舰艇编队的攻击目标则由孤立的目标节点T组成。因此整个作战模型表现为一个由S、D、I、T 4类节点组成的作战网络。

2.3　舰艇编队复杂网络的修复模型建立

舰艇编队网络的修复是一个动态过程。为了研究修复策略下遭袭网络的可靠性，需要将这个动态过程抽象为一个修复模型。修复模型如下：

(1) 构建一个复杂网络。这样的复杂网络包括：E-R随机网络、小世界网络、无标度网络等。一个复杂网络可表示为具有N个节点和E条边的图G。假设图G是无向的、简单连接的、无度相关分布的。设节点v_i的度为d_i。

(2) 故意攻击。用以下方式模拟故意攻击：找到度最大的节点，删除节点的所有边。如果一些节点恰好具有相同的最大度，则只从中随机选择一个节点进行攻击。

(3) 修复。用以下方式模拟修复：以修复概率p_r（$0\leqslant p_r<1$）将受到攻击节点原有的边重新连接。假设已修复的节点不再被攻击。

(4) 重复步骤(2)和(3)n_a（$0\leqslant n_a\leqslant N$）次。定义节点的攻击比例$f_a$为

$$f_a=\frac{n_a}{N} \tag{1}$$

修复模型的目标是模拟真实网络在遭受故意攻击时的修复过程。一般来说，我们无法修复所有受损的节点，因为一些损害太严重而无法修复，或者太复杂无法及时修复。尽管修复策略无法保持复杂网络完好无损，但是它能够一定程度地提高网络可靠性。在该模型的基础上，可以研究修复策略对复杂网络可靠性的具体影响。

设$p(k)$（$m\leqslant k\leqslant M$）为度分布，即在网络中任意选择一个节点的度为k的概率。网络节点的最小度为m，最大度为M。设$q(k)$是度为k的节点未被移除的概率。设$\widetilde{K}_a$是未被攻击的节点的最大度。运用$\widetilde{K}_a$，$q(k)$可表示为

$$\begin{aligned}q(k)&=\theta(\widetilde{K}_a-k)+(1-\theta(\widetilde{K}_a-k))\cdot p_r\\&=\begin{cases}1, & \text{if } k\leqslant\widetilde{K}_a\\ p_r, & \text{if } k>\widetilde{K}_a\end{cases}\end{aligned} \tag{2}$$

式中，θ是Heaviside阶跃函数。

在比例为f_a的最大度节点被攻击后，新的最大度$\widetilde{K}_a$可从下面的关系中推导。

$$\sum_{k=\widetilde{K}_a}^{M}p(k)=\sum_{k=\widetilde{K}_a}^{\infty}p(k)-\frac{1}{N}=f_a \tag{3}$$

特别地，对于具有幂指数度分布$p(k)=Ck^{-\gamma}$的无标度网络，在N很大的情况下，式(3)可表示为

$$\widetilde{K}_a=mf_a^{1/(1-\gamma)} \tag{4}$$

3　舰艇编队网络遭临界攻击比例和巨元组大小

设S是巨元组的大小。当临界攻击比例为f_{ac}时，S降为0，表明网络分解为独立的小连通片。f_{ac}和S是两个度量修复策略下遭袭网络崩溃程度的重要参数。运用概率母函数[10]，我们推导出了f_{ac}和S的解析解。

任意选择的节点的度为k且没有被移除的概率是$p(k)q(k)$，它的概率母函数是

$$F_0(x)=\sum_{k=m}^{M}p(k)q(k)x^k \tag{5}$$

任意选择一条边，沿着这条边所到达的点的度分布应为$kp(k)$，而不只是$p(k)$，这是因为这条任意选择的边更有可能到达度较大的节点。与式(5)类似，这样的点的概率母函数为[11]

$$F_1(x)=\frac{\sum_{k=m}^{M}kp(k)q(k)x^{k-1}}{\sum_{k=m}^{M}kp(k)}=\frac{F_0'(x)}{\langle k\rangle} \tag{6}$$

设$H_1(x)$是沿任意选择的一条边所到达的连通片大小的概率母函数。如果这条边所到达的节点均被移除，则该连通片包含0个节点，发生这种情况的概率为$1-F_1(1)$。沿这条边也可能到达一个剩余节点，该节点连接另外k条边，其分布函数为$F_1(1)$。这意味着$H_1(x)$满足一个递归形式，即

$$H_1(x)=1-F_1(1)+xF_1[H_1(x)] \tag{7}$$

任意选择的一个点所在的连通片大小的概率母函数为$H_0(x)$，其中

$$H_0(x)=1-F_0(1)+xF_0[H_1(x)] \tag{8}$$

可以从式(7)和式(8)推导出平均连通片大小和巨元组相对大小(巨元组与网络中所有节点的比例)的表达式,即

$$\langle s\rangle = H_0'(1) = F_0(1) + \frac{F_0'(1)F_1(1)}{1-F_1'(1)} \tag{9}$$

$$\frac{S}{N} = F_0(1) - F_0(u) \tag{10}$$

式中,u 是递归方程(11)的最小非负实数解。

$$u = 1 - F_1(1) + F_1(u) \tag{11}$$

当 $1-F_1'(1)=0$ 时,式(10)发散,也即

$$F'(1) = \frac{F_0''(1)}{\langle k\rangle} = \frac{\sum_{k=m}^{M} k(k-1)p(k)q(k)}{\sum_{k=m}^{M} kp(k)} = 1 \tag{12}$$

该临界点是系统的渗流临界值,在这个临界点相互连接的节点组成的巨元组首次形成。将式(2)代入式(12),可以得到

$$\sum_{k=m}^{K_a} k(k-1)p(k) + p_r \sum_{k=K_a+1}^{M} k(k-1)p(k) = \sum_{k=m}^{M} kp(k) \tag{13}$$

将式(4)代入式(13)并求解 f_a,可以得到临界攻击比例 f_{ac}。特别地,对于具有幂指数度分布 $p(k)=Ck^{-\gamma}$ 的无标度网络,对 $p(k)$ 进行连续性近似,式(13)可化为

$$\frac{(1-p_r)\widetilde{K}_a^{2-\gamma} - 2m^{2-\gamma} + (1+p_r)M^{2-\gamma}}{2-\gamma} = \frac{(1-p_r)\widetilde{K}_a^{3-\gamma} - m^{3-\gamma} + p_r M^{3-\gamma}}{3-\gamma} \tag{14}$$

式中,$M \approx mN^{1/(\lambda-1)}$。在 $p_r=0$ 的极端情况下,即在没有修复的故意攻击下,式(14)与文献[8]的结果一致。

4 模型的仿真与计算结果分析

根据前面提出的修复模型,对遭受攻击的复杂网络的修复过程进行仿真。按照文献[9]的方法构建了一个具有幂指数度分布 $p(k)=Ck^{-\gamma}$ 的无标度网络。每次对网络进行攻击和修复后,要判断网络是否崩溃[8]。选择 $\kappa \equiv \langle k^2\rangle/\langle k\rangle < 2$ 作为判断网络崩溃的标准。随着仿真的进行,κ 是不断递减的。当 $\kappa<2$ 时,记录下仿真次数 n_{ac} 和最大连接片的节点数 s_m。

对于特定的度分布,进行 10 次仿真产生 10 个网络;对于每个网络,按照修复模型对修复策略下遭袭网络的进行 20 次仿真。仿真得到的临界值 f_c 近似为 $\langle n_{ac}\rangle/N$,即 $f_c \approx \langle n_{ac}/N\rangle$;巨元组大小 S 近似为 $\langle s_m\rangle$,即 $S \approx \langle s_m\rangle$。

为了更好地研究修复策略对复杂网络可靠性的影响,可以借助于巨元组相对大小 S/N 与攻击比例 f_a 的关系图,如图 2 所示。图 2 表明修复策略显著提高了无标度网络的可靠性。当 $p_r=0$ 时,即无修复策略下的故意攻击,在网络中 21%的节点被攻击后网络崩溃。当 $p_r=0.2$ 时,在网络中 57%的节点被攻击后网络崩溃,这表明网络可靠性已经增大。当 $p_r=0.4$ 时,即使在网络中 100%的节点被攻击后巨元组仍然存在——网络将仍然具有很大的连通性,其巨元组的相对大小 $S/N=0.148$,这表明修复策略下的网络连通性对于故意攻击是非常健壮的。图 3 表示临界攻击比例 f_{ac} 与度指数 γ 的关系,包括仿真结果和精确的解析解。在相同的修复策略下,度指数 γ 较小的无标度网络的可靠性提高较大。当 $\gamma=2.7$ 时,临界攻击比例 f_{ac} 从 0.226($p_r=0$)提高到 0.371($p_r=0.04$)。当 $\gamma=3.5$ 时,临界攻击比例 f_{ac} 从 0.216 提升到 0.254。这是因为在度指数 γ 较小的无标度网络中,节点具有较大的度,对这些节点的修复能更大程度地提高网络连通度。尽管由于修复的随机性导致仿真结果具有一定的不确定性,但理论结果与仿真结果仍具有较好的一致性。

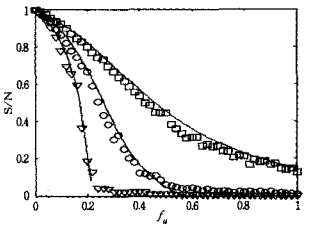

图 2 无标度网络中巨元组相对大小 S/N 与攻击比例 f_a 的关系图

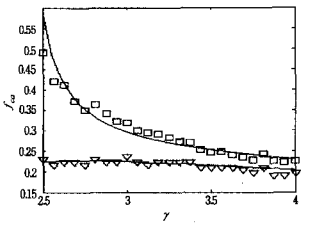

图 3 临界攻击比例 f_{ac} 与度指数 γ 的关系图

结束语 本文提出了舰艇编队复杂网络修复模型,基于该模型研究了修复策略下受攻击网络的可靠性。运用概率母函数方法,对网络崩溃时的临界攻击比例 f_{ac} 及巨元组相对大小 S/N 进行解析研究。通过解析和仿真计算表明:(1)修复策略能显著提高无标度网络的可靠性;(2)修复策略对于幂指数 γ 较小的无标度网络可靠性的提高效果较好。这些研究成果使我们能更好地理解具有自我修复能力的舰艇编队网络。

参 考 文 献

[1] Doyle J C, Alderson D L, Li L, et al. The "robust yet fragile" nature of the internet[J]. Proceedings of the National Academy of Sciences of the United States of America, 2005, 102(41): 14497-14502

[2] 陈晔,吴晓锋. 舰艇作战系统网络的鲁棒性分析[J]. 舰船电子工程, 2005, 25(6): 52-67

[3] Guimera R, Amaral L A N. Functional cartography of complex metabolic networks[J]. Nature, 2005, 433(7028): 895-900

[4] 胡斌,黎放,郑建华. 基于复杂网络的舰艇编队网络中心战模型研究[J]. 系统仿真学报, 22(8): 1960-1996

[5] 李敏勇,李陆冀. 网络中心战中舰艇编队的作战效能分析[J]. 火力与指挥控制, 2004, 29(5): 12-14

[6] Albert R, Jeong H, Barabasi A L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406: 378-382

[7] Holme P, Kim B J, Yoon C N, et al. Attack vulnerability of complex networks[J]. Phys. Rev. E, 2002, 65(5): 056109

[8] Cohen R, Erez K, ben-Avraham D, et al. Breakdown of the internet under intentional attack[J]. Physical Review Letters, 2001, 86(16): 3682-3685

[9] Molloy M, Reed B. A critical point for random graphs with a given degree sequence[J]. Random Structures and Algorithms, 1995, 6(2/3): 161-179

[10] Callaway D S, Newman M E J, Strogatez S H, et al. Network robustness and fragility: Percolation on random graphs[J]. Phys. Rev. Lett, 2000, 85(25): 5468-5471

[11] Newman M E J, Strogatz S H, Watts D J. Random graphs with arbitrary degree distributions and their applications[J]. Physical Review E, 2001, 64(2): 026118