DOI: 10.13718/j.cnki.xdzk.2017.02.021

相互作用网络的攻击模型与渗流研究①

陈垂波[1]，　杨　春[1]，　付传技[2]，　杨程成[1]，　陈小龙[1]

1. 电子科技大学 数学科学学院，成都 611731；2. 电子科技大学 物理电子学院，成都 610054

摘要：针对相互作用网络的蓄意攻击问题，本文提出了一种一般性的蓄意攻击模型，将该模型应用于 2 个完全随机耦合的 ER 网络与 SF 网络，并对渗流现象进行数值模拟与理论分析. 本文主要结论为：相互作用网络较为脆弱，但对度大的和具有度大依赖顶点的顶点进行保护可以有效地提高整个相互作用网络的鲁棒性. 具体表现为：① 在耦合 ER 网络中，降低对度大顶点的攻击概率，对网络的破坏程度会降低，但攻击概率降低到一定程度后不再起作用；② 在耦合 SF 网络中，发现需要同时保护 2 个网络的度大顶点，才能提高整个网络的鲁棒性；③ 对上面 2 种网络，即使同时保护 2 个网络的度大顶点，整个网络依然存在级联失效风险；④ 对混合 ER-SF 网络，需要同时保护 2 个网络的度大顶点，但保护 ER 网络的度大顶点更为有效. 本文提出的蓄意攻击模型更符合实际相互作用网络的受攻击情况，对评估和研究相互作用网络具有重要的指导意义；同时，本文的研究结果在耦合网络的构建和维护等方面有着潜在的应用前景.

关　键　词：相互作用网络；蓄意攻击；渗流；鲁棒性

中图分类号：N94　　**文献标志码**：A　　**文章编号**：1673－9868(2017)02－0135－07

近年来，相互作用网络得到了广泛研究[1－3]. Buldyrev[4]使用随机图论中的度分布理论与生成函数方法，首次提出了研究 2 个相互作用网络级联失效的数学框架，发现在随机攻击下相互作用网络比单网络更加脆弱. Parshani 等人[5]研究部分耦合网络发现，在随机攻击下，降低网络之间的耦合强度会使网络渗流从一阶相变转为二阶相变. Huang 等人[6]研究了全耦合相互作用网络在蓄意攻击模型下的鲁棒性问题，提出了将蓄意攻击模型转化为随机攻击模型的研究方法，发现在完全随机耦合的 SF 网络中，即便降低对其中一个网络度大顶点攻击的概率，网络依然很脆弱，说明保护完全随机耦合的 SF 网络是极其困难的. Dong 等人[7]研究了蓄意攻击模型下部分耦合相互作用网络的鲁棒性问题，发现随着耦合强度的降低，网络渗流由一阶相变跳到二阶相变，并且一阶相变与二阶相变之间的交界线随着保留顶点比例 p 的减少而递减，随着度大顶点被攻击概率的增大而增加. 2013 年，Dong 等人[8]在对蓄意攻击模型下 NON 网络[9]的鲁棒性研究中发现，当网络平均度小于某个临界值时，即使只移除一个顶点也会导致网络破碎.

上述蓄意攻击模型均假设顶点被攻击的概率只正比于顶点自身度数，我们认为在相互作用网络中，顶点被攻击的概率还应该正比于其依赖的顶点度数. 例如在相互作用的计算机—电力网中，黑客要破坏重要的电力站，他就要攻击控制着重要电力站的计算机，也就说计算机被攻击的概率与其控制的电力站的度成正比. 基于此，本文提出了一种对耦合网络更一般化的蓄意攻击模型，该模型定义对顶点的攻击概率正比于顶点度数及其依赖的顶点度数，同时设置控制参数 α 与 β 调节对顶点的攻击概率. 通过对完

① 收稿日期：2015－03－23
基金项目：国家自然科学基金项目(61172115，60872029)；9140A06030614DZ02083 项目资助；CEMEE 国家实验室开放课题基金项目(CEMEE2014K0209B).
作者简介：陈垂波(1989－)，男，广西玉林人，硕士研究生，主要从事复杂网络的研究.

全随机耦合的ER与SF网络的数值实验与理论分析发现：即便是2个相互作用网络的高度数顶点都得到保护，其渗流阈值仍然大于0，说明相互作用网络极其脆弱. 在耦合ER网络中，降低度大顶点被攻击的概率可以有效增加其鲁棒性，但是降低到一定程度后渗流阈值不再减少，网络的鲁棒性没有再提升. 在2个相互作用并且完全耦合的SF网络中，还发现需要同时保护2个网络的度大顶点，才能提高整个相互作用网络的鲁棒性.

1 模型描述

本文研究的相互作用网络由网络A与网络B组成，它们的顶点数都为N. $P_A(k)$，$P_B(k)$分别表示它们的度分布函数. 与文献[4]中的网络构造相同，设定2个网络顶点之间的依赖关系是完全随机的一一依赖关系，即若顶点a_i依赖顶点b_m，且b_m依赖顶点a_k，则有$i=k$. 当网络受到攻击时，若顶点a_i失效，则其依赖顶点b_m也失效，同时假定没有连接到最大连通分支的顶点也被视为失效顶点，于是产生级联失效现象. 在现实相互作用网络中，顶点被攻击的概率不仅取决于自身度数大小，同时与其依赖顶点的度数有关. 基于此，我们构建对初始顶点的蓄意攻击模型，如下所示：

$$W_{\alpha,\beta}(i)=\frac{k_i^{\alpha}\times k_j^{\beta}}{\sum\limits_{i\leftrightarrow j}k_i^{\alpha}\times k_j^{\beta}} \tag{1}$$

模型中$W_{\alpha,\beta}(i)$表示网络A中顶点i被攻击的概率，$i\leftrightarrow j$表示网络A中顶点i与网络B中顶点j相互依赖，k_i表示顶点i的度数，k_j表示顶点j的度数，α与β为设定的攻击概率控制参数，取值范围是$-\infty<\alpha,\beta<+\infty$. 对于模型(1)我们可以将2个网络推广到$N(N>=2)$个网络，则模型的表达式为：

$$W_{\alpha}(i)=\frac{k_i^{\alpha_i}\times\sum\limits_{j}k_j^{\alpha_j}}{\sum\limits_{i\leftrightarrow j}(k_i^{\alpha_i}\times\sum\limits_{j}k_j^{\alpha_j})} \tag{2}$$

其中，α为N维的参数向量，表示N个网络中顶点度的权重. 为方便分析，本文仅考虑由2个随机一对一依赖的网络构成的相互作用网络. 模型(1)具有如下6种情形：

1) 当$\alpha=0$，$\beta=0$时，$W(i)=\frac{1}{N}$，模型(1)退化为文献[4]在相互作用网络中使用的随机攻击模型；

2) 当$\beta=0$时，$W_{\alpha}(i)=\frac{k_i^{\alpha}}{\sum\limits_{i}k_i^{\alpha}}$，这是文献[10]在单一网络中提出的蓄意攻击模型，也是文献[6]在相互作用网络中使用的蓄意攻击模型，该蓄意攻击模型通过调节α参数控制顶点被攻击的概率，当$\alpha>0$时，度大顶点优先被攻击；当$\alpha<0$时，度大顶点被攻击的概率变小；

3) 当$\alpha<0$，$\beta<0$时，如果网络A中的顶点度数及其依赖点的度数越大，则该顶点被攻击的概率越小；

4) 当$\alpha>0$，$\beta>0$时，如果网络A中的顶点度数及其依赖点的度数越大，则该顶点被攻击的概率越大；

5) 当$\alpha<0$，$\beta>0$时，如果网络A中的度小顶点越依赖于网络B中的度大顶点，则该顶点被攻击的概率越大；

6) 当$\alpha>0$，$\beta<0$时，如果网络A中的度大顶点越依赖于网络B中的度小顶点，则该顶点被攻击的概率越大.

假设网络A中的初始失效顶点比例为$(1-p)$，同时设网络级联失效达到稳定时最大相互连通分支在整个网络中所占的比值为p_{∞}. 针对由2个ER网络(ER-ER)和2个SF(SF-SF)网络构成的一对一全耦合的相互作用网络，图1中的(a)与(b)分别展示了ER-ER网络与SF-SF网络在上述几种不同情形下，p_{∞}的模拟值随p的变化关系，其中，顶点数$N=10\ 000$. 图1(a)取平均度$\langle k\rangle=4$的ER-ER网络与$\lambda=2.8$，$m=2$的

SF-SF 网络，图 1(b) 是在不同 α,β 取值下模拟级联失效中 p_∞ 随 p 的变化关系. 从图 1(b) 可看出，随着 α，β 取值的变化，阈值 p_c 也在变化，说明对顶点度数与依赖的顶点度数赋予不同权重会影响网络的鲁棒性. 接下来本文使用度分布理论与渗流理论分析相互作用网络在蓄意攻击模型(1) 下的网络级联失效过程，即求解出理论值 p_∞ 与渗流阈值 p_c，然后通过数值实验进行理论结果的验证与分析.

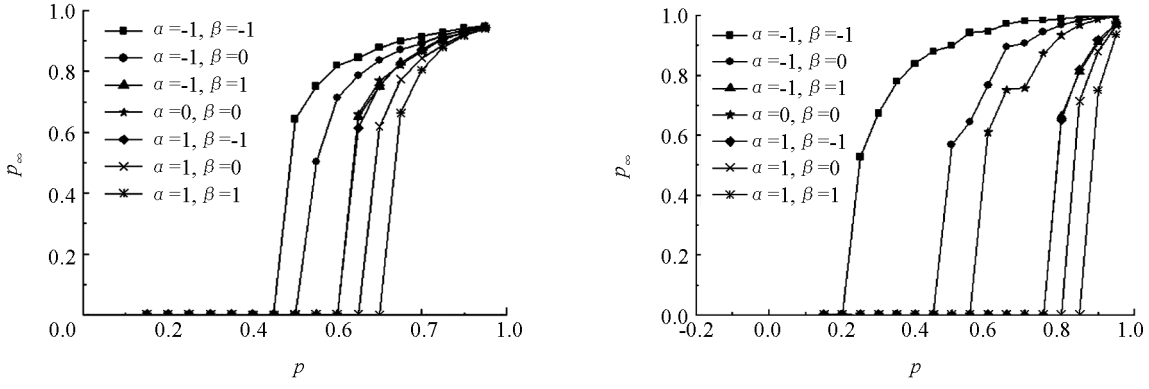

图 1　模拟级联失效中 p_∞ 随 p 的变化关系

2　求解 p_c 与 p_∞

对于度分布为 $P_A(k)$ 的网络 A，我们定义其生成函数为

$$G_{A0}(x)=\sum_k P_A(k)x^k \tag{2}$$

则网络 A 分支过程的生成函数为

$$G_{A1}(x)=\frac{G'_{A0}(x)}{G_{A0}(1)}$$

平均度为

$$\langle k^A\rangle=\sum_k P_A(k)k$$

同理 B 网络也有类似结果.

我们使用文献[6] 中提出的方法框架，并参照文献[11] 的方法，将蓄意攻击模型映射到随机攻击模型中，进而分析一般化的蓄意攻击下的渗流结果. 首先我们根据模型(1)，从网络 A 中移除 $(1-p)$ 比例的顶点，但不移除那些剩下的顶点与被移除顶点之间的连边(这样的边属于只有一个顶点的悬挂边，相当于从一个顶点引出的残端)，那么剩下顶点的度分布 $P_p(k)$ 为

$$P_p(k)=\frac{A_p(k)}{pN} \tag{3}$$

其中 $A_p(k)$ 表示在网络 A 中移除部分顶点后度为 k 的顶点个数.

令 $\varphi(k_i)=k_i^\alpha$(对于网络 B：$\varphi(k_i)=k_i^\beta$)，则选中度为 k_i 的顶点概率为

$$W(k_i)=\frac{\varphi(k_i)}{\sum_{k_i}\varphi(k_i)}$$

由文献[6] 可知，当网络再移除一个顶点时，$A_p(k)$ 变为

$$A_{p-1/N}(k)=A_p(k)-\frac{P_p(k)\varphi(k)}{\sum_k P_p(k)\varphi(k)} \tag{4}$$

当 $N\to\infty$ 时，$A_p(k)$ 对 p 进行求导，再结合公式(3) 得

$$-P\frac{\mathrm{d}P_P(k)}{\mathrm{d}P}=P_p(k)-\frac{P_p(k)\varphi(k)}{\sum_k P_p(k)\varphi(k)} \tag{5}$$

为了求解等式(5),定义

$$G_{\varphi}(x)=\sum_{k}P(k)x^{\varphi(k)} \qquad t\equiv G_{\varphi}^{-1}(p)$$

得到如下解

$$P_{p}(k)=\frac{P(k)t^{\varphi(k)}}{p} \tag{6}$$

$$\sum_{k}P_{p}(k)\varphi(k)=\frac{tG'_{\varphi}(t)}{G_{\varphi}(t)} \tag{7}$$

等式(6)与(7)满足等式(5). 于是 $P_{p}(k)$ 的生成函数可表示为

$$G_{Ab}(x)=\sum_{k}P_{p}(k)x^{k}=\frac{1}{p}\sum_{k}P(k)t^{\varphi(k)}x^{k} \tag{8}$$

当移除剩下顶点与已被移除顶点间的连边后,网络 A 中剩下的顶点的生成函数为[12-14]

$$G_{Ac}(x)=G_{Ab}(1-p_{A}+p_{A}x) \tag{9}$$

其中 p_{A} 表示剩下顶点之间的连边数与原图连边数的比值,即

$$p_{A}=\frac{pN\langle k(p)\rangle}{N\langle k(p)\rangle}=\frac{\sum_{k}p(k)kt^{\varphi(k)}}{\sum_{k}p(k)k} \tag{10}$$

$\langle k(p)\rangle=\sum_{k}P_{p}(k)k$ 表示网络 A 中剩余顶点的平均度.

如果我们找到一个生成函数为 $G'_{A0}(x)$ 的网络 $\widetilde{A}$,在随机移除$(1-p)$比例的顶点数之后,$\widetilde{A}$ 的生成函数正好是 $G_{Ac}(x)$,那么蓄意攻击模型就可以映射到随机攻击模型中来求解. 令

$$G'_{A0}(1-p+px)=G_{AC}(x)$$

再结合等式(9)可得

$$G'_{A0}(x)=G_{Ab}\left(1+\frac{p_{A}}{p}(x-1)\right) \tag{11}$$

那么该生成函数下的分支过程的生成函数为

$$G'_{A1}(x)=\frac{G'_{A0}(x)}{G'_{A0}(1)}$$

当网络 A 被移除掉$(1-p)$比例的顶点后,最大连通分支比值为

$$g_{A}(p)=1-G'_{A0}(1-p(1-f_{A}))$$

其中

$$f_{A}\equiv f_{A}(p)=G'_{A1}[1-p(1-f_{A})]$$

应用文献[4]的理论框架,在移除$(1-p)$比例的顶点后,相互作用网络中最大的相互连通分支 $p_{\infty}=xg_{B}(x)=yg_{A}(y)$,其中 $x=pg_{A}(y)$,$y=pg_{B}(x)$;x,y 为未知变量. 将 x 代替后得到 x 的迭代公式为

$$x=pg_{A}[pg_{B}(x)] \tag{12}$$

对等式(12)求导可得

$$1=p^{2}\frac{\mathrm{d}g_{A}}{\mathrm{d}x}[pg_{B}(x)]\frac{\mathrm{d}g_{B}}{\mathrm{d}x}(x)\mid_{x=x_{c},\ p=p_{c}} \tag{13}$$

结合等式(12)、(13)即可求解得到渗流阈值 p_{c} 与 $p_{\infty}=x_{c}g_{B}(x_{c})$.

3 实验结果与分析

我们对 ER-ER 和 SF-SF 网络作数值实验分析,研究渗流阈值 p_{c} 随 α,β 的变化关系,见图2. 其中网络规模 $N=10\ 000$,ER 网络的平均度 $\langle k\rangle=4$,SF 网络的 $\lambda=2.8$,$m=2$. 这2个网络的耦合关系均为一对一随机耦合. 图2(a)与图2(b)分别展示了 ER-ER 网络与 SF-SF 网络在 β 的3种取值下理论阈值

与模拟阈值的对比，图中点代表模拟值，实线代表理论值. 首先根据公式(12)～(13)迭代计算得到的理论解(由图 2 中的实线表示)；然后模拟相互作用网络级联失效过程得出数值解(由图 2 中实线上的实点表示). 图 2 的结果验证了在 ER-ER 与 SF-SF 网络中渗流阈值理论解与数值解是吻合的，特别地，当 $\beta=0$ 时，图 2(b) 中的结果与文献[6]中的实验结果一致. 因而在实际的 ER-ER 或 SF-SF 网络中，可以先使用统计方法得到度分布函数，再通过公式(12) 和(13) 计算不同攻击方式下的渗流阈值 p_c，使其作为评估实际网络的鲁棒性的一个指标.

图 2(c) 与图 2(d) 分别展示了 ER-ER 网络与 SF-SF 网络在 $-5\leqslant\alpha\leqslant5$，$-5\leqslant\beta\leqslant5$ 范围时模拟阈值 p_c 的灰度图. 在图 2(c) 中，ER-ER 网络的阈值在各个区域中所占面积几乎相等，p_c 与 α，β 呈近似线性关系，随着 α，β 的减小，度大顶点被攻击的概率降低，渗流阈值也随之减小，网络不容易被破坏，但当 $\alpha\leqslant-2$，$\beta\leqslant-2$ 时，渗流阈值不再随着 α，β 的减小而减小. 在图 2(d) 中，深灰色区域表示 SF-SF 网络的渗流阈值处于最大范围，说明在 $\alpha\geqslant1$ 或 $\beta\geqslant1$ 的蓄意攻击方式下，SF-SF 网络迅速受到破坏. 因此可以取 $\alpha=\beta=1$ 近似作为最优攻击方式快速破坏 SF-SF 网络. 此外，图 2(d) 中 $\alpha\leqslant-2$，$\beta\leqslant-2$ 对应的浅灰色区域表示渗流阈值处于最小范围，此时 SF-SF 网络对于 $\alpha\leqslant-2$，$\beta\leqslant-2$ 的蓄意攻击方式的鲁棒性是最高的，说明需要同时保护 2 个 SF-SF 网络的度大顶点，才能提高整个相互作用网络的鲁棒性. 从保护网络角度来看，可以取 $\alpha=\beta=-2$ 近似作为最优顶点保护方式，从而使得 SF-SF 网络受到最小程度破坏. 同时，在图 2(c) 与图 2(d) 中，当 $\alpha\leqslant-2$，$\beta\leqslant-2$ 时，ER-ER 网络的 p_c 达到最小值范围(0.4 附近)，SF-SF 网络的 p_c 达到最小值范围(0.2 附近)，说明这 2 个网络的度大顶点被攻击的概率在很小的情况下，网络渗流阈值仍然大于 0，说明了完全随机耦合的 ER 和 SF 网络都是相当脆弱的.

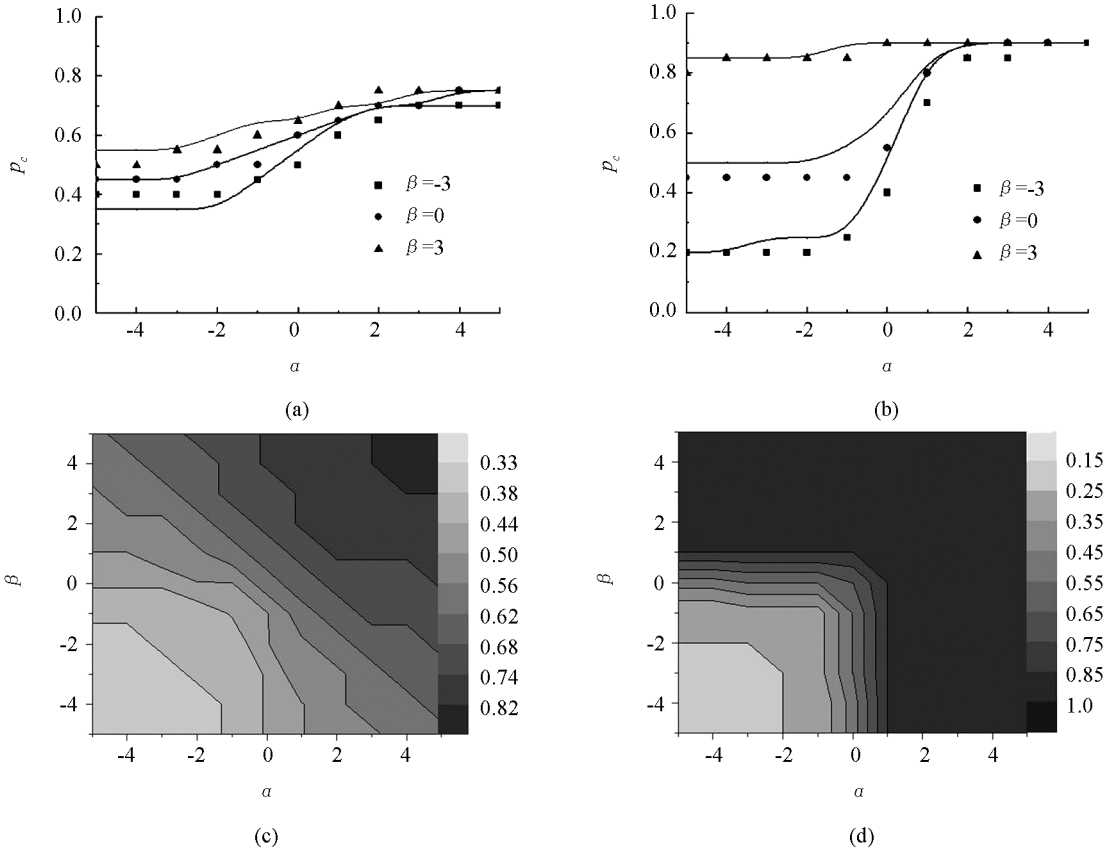

图 2　渗流阈值 p_c 随 α,β 的变化关系

在实际生活中，混合 ER-SF 结构的相互作用网络普遍存在，因此本文还对混合 ER-SF 的相互作用网络作了数值模拟实验(见图 3). 设 ER 网络为 A 网络，SF 网络为 B 网络，2 个网络的规模均取 $N=10\,000$，ER

网络的平均度$\langle k\rangle=4$，SF网络的$\lambda=2.8$，$m=2$，2个网络的耦合关系为一对一随机耦合. 这2个网络顶点之间的依赖关系以及攻击方式同上述ER-ER，SF-SF一样. 在实验结果图3中，深灰色区域(>=0.6)形状趋势较陡，说明$\alpha\geqslant 1$时，β取任何值的蓄意攻击方式都会对ER-SF网络轻易造成网络破坏. 此外，$\alpha<0$，$\beta<0$对应的浅灰色区域表示渗流阈值处于最小范围，说明对于ER-SF网络也需要同时保护2个网络的度大顶点，才能提高整个相互作用网络的鲁棒性. 从图3中还能看出，保护ER网络中的度大顶点比保护SF网络中的度大顶点更能有效地提高网络的鲁棒性. 从上述分析可知，模型(1)能够结合顶点度数权重以及依赖顶点度数权重2个因素，从更一般的角度了解相互作用网络在不同攻击下的渗流现象及其鲁棒性.

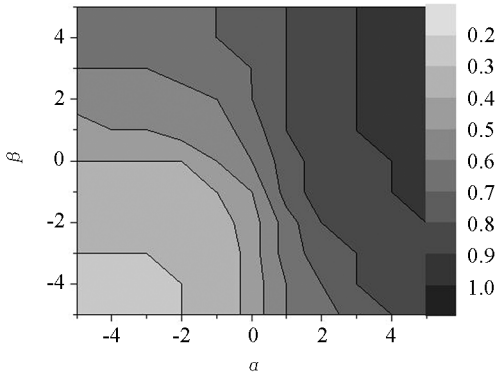

图3 ER网络与SF网络组成的耦合网络在不同α,β取值下，模拟阈值p_c的灰度图

4 结束语

本文通过引入依赖顶点的度数权重，提出了一个在相互作用网络中基于顶点度与依赖顶点度的蓄意攻击模型，从一般的角度研究了2个相互作用网络在不同的攻击方式下的渗流现象以及鲁棒性问题. 当$\alpha<0$，$\beta<0$时，2个网络都得到保护但渗流阈值p_c依然大于0，说明相互作用网络是相当脆弱的. 对于ER-ER网络，降低对度大顶点的攻击概率，对网络的破坏程度会降低，但攻击概率降低到一定程度后，对网络的破坏程度不会再下降. 除此之外，对于SF-SF网络，需要同时保护2个网络的度大顶点，才能提高整个相互作用网络的鲁棒性. 在现实网络中，SF网络非常广泛，因而这个结果对现实中的耦合网络构造与维护有着潜在的应用. 此外，本文仅对完全随机耦合网络进行了研究，我们可以根据实际情况，将模型(1)扩展应用到部分耦合或者NON网络中.

参考文献：

[1] RINALDI S M, PEERENBOOM J P, KELLY T K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies [J]. IEEE Control Systems Magazine, 2001, 21(6): 11-25.

[2] LAPRIE J C, KANOUN K, KAÂNICHE M. Modelling Interdependencies Between the Electricity and Information Infrastructures [J]. Lecture Notes in Computer Science, 2007(4680): 54-67.

[3] PANZIERI S, SETOLA R. Failures Propagation in Critical Interdependent Infrastructures [J]. International Journal of Modelling, Identification and Control, 2008, 3(1): 69.

[4] BULDYREV S V, PARSHANI R, PAUL G, et al. Catastrophic Cascade of Failures in Interdependent Networks [J]. Nature, 2010, 464(7291): 1025-1028.

[5] PARSHANI R, BULDYREV S V, HAVLIN S. Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition [J]. Phys Rev Lett, 2010, 105(4): 048701.

[6] HUANG X, GAO J, BULDYREV S V, et al. Robustness of Interdependent Networks Under Targeted Attack [J]. Phys Rev E Stat Nonlin Soft Matter Phys, 2011, 83(6 Pt 2): 065101.

[7] DONG G, GAO J, TIAN L, et al. Percolation of Partially Interdependent Networks Under Targeted Attack [J]. Phys Rev E Stat Nonlin Soft Matter Phys, 2012, 85(1 Pt 2): 016112.

[8] DONG G, GAO J, DU R, et al. Robustness of Network of Networks Under Targeted Attack [J]. Phys Rev E Stat Nonlin Soft Matter Phys, 2013, 87(5): 052804.

[9] GAO J, BULDYREV SV, HAVLIN S, et al. Robustness of a Network of Networks [J]. Phys Rev Lett, 2011,

107(19)：195701.

[10] GALLOS L K，COHEN R，ARGYRAKIS P，et al. Stability and Topology of Scale-Free Networks Under Attack and Defense Strategies [J]. Phys Rev Lett，2005，94(18)：188701.

[11] 杨程成，杨春. 相互作用网络耦合关系对其鲁棒性的影响 [J]. 西南大学学报(自然科学版)，2015，37(9)：145－149.

[12] NEWMAN M E. Spread of Epidemic Disease on Networks [J]. Phys Rev E Stat Nonlin Soft Matter Phys，2002，66(1 Pt 2)：016128.

[13] SHAO J，BULDYREV S V，HAVLIN S，et al. Cascade of Failures in Coupled Network Systems with Multiple Support-Dependence Relations [J]. Phys Rev E Stat Nonlin Soft Matter Phys，2011，83(3 Pt 2)：036116.

[14] SHAO J，BULDYREV S V，BRAUNSTEIN L A，et al. Structure of Shells in Complex Networks [J]. Phys Rev E Stat Nonlin Soft Matter Phys，2009，80(3 Pt 2)：036105.

Investigation of an Attack Model and Percolation of Interdependent Networks

CHEN Chui-bo[1]，　YANG　Chun[1]，　FU Chuan-ji[2]，
YANG Cheng-cheng[1]，　CHEN Xiao-long[1]

1. *School of Mathematical Sciences，University of Electronic Science and Technology of China，Chengdu 611731，China*；
2. *School of Physical Electronics，University of Electronic Science and Technology of China，Chengdu 610054，China*

Abstract：To study the targeted-attack problem in independent networks，we propose a general targeted-attack model. Based on the oretical analysis and numerical simulations for two completely and randomly coupled ER networks in an investigation reported herein，we found that the independent networks were quite vulnerable，but their robustness could be improved by protecting the nodes with high degrees，or with high-degree independent nodes. Specifically，the results were：① In the coupled ER networks，decreasing the attacking probability of high degree nodes would reduce the damage to the networks，yet no effect was observed when the attacking probability declined to a certain value. ② For the coupled SF networks，the robustness of the independent networks could be improved only by protecting the nodes with high degree simultaneously in the two networks. ③ The above methods could not completely resolve the failure cascading，indicating the vulnerability of the independent networks. ④ For the coupled ER-SF networks，the high-degree nodes of both networks should be simultaneously protected，though the low attacking probability of the nodes in ER networks was more efficient to improve the robustness. The targeted-attack model described in this paper is more close to real attacking situations，thus can provide a valuable guide for the study of the robustness of actual independent networks. Moreover，the results are expected to be helpful for the construction and maintenance of independent networks.

Key words：interdependent networks；targeted-attack；percolation；robustness

责任编辑　崔玉洁