

文章编号:1001-9081(2015)05-1224-06

doi:10.11772/j.issn.1001-9081.2015.05.1224

## 信息缺失条件下的相互依存网络抗毁性分析

蒋宇翔\*, 吕晨, 虞红芳

(光纤传感与通信教育部重点实验室(电子科技大学), 成都 611731)

(\* 通信作者电子邮箱 jyxjyx27@163.com)

**摘要:**提出了信息缺失条件下的相互依存网络抗毁性分析方法。首先,提出了结构信息和攻击信息,在结构信息已知的情况下利用信息广度参数和信息精度参数将攻击信息的获取抽象成无放回不等概率抽样问题,以此建立攻击信息缺失模型;然后,借助生成函数和渗流理论的思想提出了在随机信息缺失和优先信息缺失条件下的相互依存网络的抗毁性分析模型。根据此模型可以得到不同情况下的渗流阈值。通过以无标度网络作为实例进行进一步的实验发现信息广度参数和信息精度参数对相互依存网络的渗流阈值影响巨大,并且信息精度比信息广度影响更大,少量的高精度节点信息等价于大量低精度节点信息;已知少量最重要的节点就可以很大程度上降低相互依存网络的抗毁性;即使是在信息缺失的条件下,相互依存网络的抗毁性依旧远低于单层网络。

**关键词:**信息缺失;相互依存网络;抗毁性;渗流理论;信息精度;信息广度

中图分类号:TP393.0 文献标志码:A

### Survivability analysis of interdependent network with incomplete information

JIANG Yuxiang\*, LYU Chen, YU Hongfang

(Key Laboratory of Optical Fiber Sensing and Communications, Ministry of Education  
(University of Electronic Science and Technology of China), Chengdu Sichuan 611731, China)

**Abstract:** This paper proposed a method for analyzing the survivability of interdependent networks with incomplete information. Firstly, the definition of the structure information and the attack information were proposed. A novel model of interdependent network with incomplete attack information was proposed by considering the process of acquiring attack information as the unequal probability sampling by using information breadth parameter and information accuracy parameter in the condition of structure information was known. Secondly, with the help of generating function and the percolation theory, the interdependent network survivability analysis models with random incomplete information and preferential incomplete information were derived. Finally, the scale-free network was taken as an example for further simulations. The research result shows that both information breadth and information accuracy parameters have tremendous impacts on the percolation threshold of interdependent network, and information accuracy parameter has more impact than information breadth parameter. A small number of high accuracy nodes information has the same survivability performance as a large number of low accuracy nodes information. Knowing a small number of the most important nodes can reduce the interdependent network survivability to a large extent. The interdependent network has far lower survivability performance than the single network even in the condition of incomplete attack information.

**Key words:** incomplete information; interdependent network; survivability; percolation theory; accuracy of information; breadth of information

### 0 引言

近年来,复杂网络的研究虽然取得了巨大的进步<sup>[1-4]</sup>,但大多集中在不依赖其他网络的单一网络中<sup>[5-8]</sup>。随着信息技术的飞速发展,复杂网络之间的联系和依赖越来越强,网络系统的正常运行需要各部件之间相互地提供一定的支持功能<sup>[9-12]</sup>。因此人们对复杂网络的研究重心开始从单一网络组成的系统转到多个网络组成的相互依存系统中<sup>[13-15]</sup>。相互依存网络就是具有相互作用关系的两个或多个网络所组成

的一个网络系统。两个网络组成的相互依存网络示意图如图1所示,其中,实线代表了各网络中的实际连接关系,虚线代表两个网络间的依存关系。

目前,大部分的相互依存网络抗毁性研究都是在随机失效或者蓄意攻击条件下进行的,而这只是两种极端情况。在相互依存网络构成的复杂系统中,节点的数量往往都是非常巨大的,结构也是极其复杂的,虽然大多数时候我们能通过流量监控等手段获取网络全部的结构信息,但只能通过探测器等手段探测网络以获取尽可能多的攻击信息。本文定义结构

收稿日期:2014-12-24;修回日期:2015-03-09。

基金项目:国家自然科学基金资助项目(61271171);国家973计划项目(2013CB329103)。

作者简介:蒋宇翔(1991-),男,四川广元人,硕士研究生,主要研究方向:绿色网络、复杂网络;吕晨(1991-),女,四川乐山人,硕士研究生,主要研究方向:网络虚拟化、复杂网络;虞红芳(1975-),女,浙江萧山人,教授,博士,主要研究方向:网络虚拟化、软件定义网络、绿色网络、复杂网络。

信息是指网络的度分布、各节点的连接情况等拓扑信息。结构信息只能够代表对网络拓扑的了解情况,只掌握结构信息并不代表具备蓄意攻击的条件;攻击信息是指那些具备可蓄意攻击条件的信息,例如详细的地理位置等。攻击信息已知的节点可进行蓄意攻击,而攻击信息未知的节点只能尝试随机攻击。为了填补相互依存网络在随机失效和蓄意攻击之间的抗毁性分析模型的空白,本文提出了信息缺失条件下的相互依存网络抗毁性的理论分析方法,其中,信息缺失即为掌握全网的结构信息但不完全掌握全网的攻击信息。

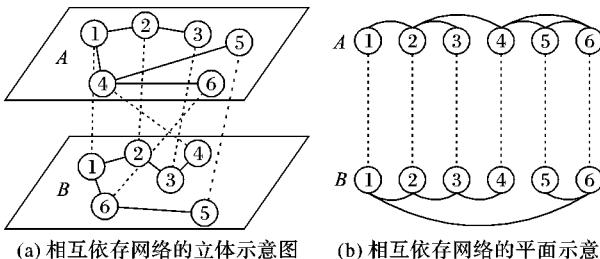


图1 相互依存网络示意图

本文首先利用信息广度参数和信息精度参数将攻击信息的获取抽象成无放回不等概率抽样问题,以此建立信息缺失条件下的相互依存网络分析模型;其次借助渗流理论以及相互依存网络的级联失效过程分别提出了随机信息条件缺失下和优先信息条件缺失下的完全相互依存网络的抗毁性分析方法,利用此方法可以准确得到渗流阈值  $P_c$  的表达式;再次,以无标度网络作为实例通过数值求解的方法求解出理论渗流阈值  $P_c$ ,并以模拟真实网络的仿真方法对本文提出的抗毁性分析理论模型进行了详细验证;最后,在仿真验证的过程中分析得到了在信息缺失条件下相互依存网络的一系列结论与性质。发现:1)信息广度  $\alpha$  和信息精度  $\beta$  ( $\alpha$  和  $\beta$  的具体定义见1.1节)对相互依存网络的渗流阈值影响巨大,并且信息精度比信息广度影响更大,少量的高精度节点信息等价于大量低精度节点信息。若只想攻击 20% 的节点就想摧毁整个网络,在  $\beta = \infty$  时只需要掌握 1.4% 的节点信息即可,而在  $\beta = 0$  时需要掌握 62% 的节点信息才行。2)已知少量最重要的节点就可以很大程度上降低相互依存网络的抗毁性。在  $\beta = \infty$  条件下,  $\alpha = 0$  时渗流阈值  $P_c = 0.74$ ,之后  $P_c$  便急剧上升,在信息广度  $\alpha = 0.105$  时就已经达到上界。3)即使是在信息缺失的条件下,相互依存网络的抗毁性依旧远低于单层网络,在  $\beta = 0, \alpha = 0.8$  时,攻击相互依存网络中 16% 的节点就可以摧毁整个网络,而同样攻击单层网络中 16% 的节点后仍会剩余 70% 的节点未受到影响。

信息缺失是现实世界中尤其是军事场合中探测手段有限等情况下所面临的最普遍的问题,所以在信息缺失条件下相互依存网络的抗毁性分析变得异常重要,它填补了相互依存网络在随机失效和蓄意攻击之间的抗毁性分析模型的空白,结合得到的结论和性质可对攻击策略的制定提供有效参考。

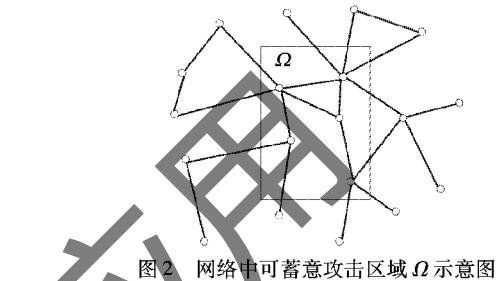
## 1 模型与分析

### 1.1 模型与攻击策略简介

在复杂网络中,可以用  $G = (V, E)$  来表示一个图,其中  $V = \{v_1, v_2, \dots, v_N\}$  是一个非空集合,称为顶点集,  $N = |V|$  表示全网顶点数。本文的模型是由两个网络( $A$  网络和  $B$  网

络)组成的完全相互依赖网络。不失一般性地,对  $A$  网络进行探测,以此获取攻击信息,并尝试攻击  $A$  网络。

给定信息广度  $\alpha$  和信息精度  $\beta$  就能依概率探测出攻击信息已完全知晓的节点,这些节点可被蓄意攻击。定义这些攻击信息已完全知晓的节点组成的集合为可蓄意攻击区域  $\Omega$ (如图2所示)。本文将把可蓄意攻击区域  $\Omega$  的选取建模成无放回不等概率抽样问题<sup>[16]</sup>。不等概率抽样问题简单来说就是由于样本空间中每个个体的重要性不同,为了提高估算精度,减少抽样误差,故使每个个体的入样概率  $\varphi$  不再相等,其入样概率和它的某一辅助变量成正比。无放回不等概率抽样是不等概率抽样中的一种,由于样本的无放回性并且各次抽取相互不独立,需要对每一次抽取的概率进行精心的设计。

图2 网络中可蓄意攻击区域  $\Omega$  示意图

在此模型中:

1)信息广度  $\alpha$  表示  $\Omega$  中包含的节点数占全网节点数的比例,  $N\alpha$  表示可蓄意攻击区域  $\Omega$  中的节点数量,  $\alpha \in [0, 1]$ 。 $\alpha$  越大表示在整个网络中攻击信息完全知晓的节点越多。其中两种极端的情况为:

a)当  $\alpha = 0$  时,  $n = N\alpha = 0$ , 表示不知道整个网络的任何攻击信息;

b)当  $\alpha = 1$  时,  $n = N\alpha = N$ , 表示整个网络的攻击信息完全知晓。

2)信息精度  $\beta$  表示  $\Omega$  中包含节点的重要程度,  $\beta$  取值越大,更重要的节点更加容易被探测到。两种极端的情况为:

a)当  $\beta = 0$  时,各节点被探测到的概率相等且都为  $1/N$ ,称此情况为随机信息缺失;

b)当  $\beta = \infty$  时,每次探测都能探测到当前最重要的节点,称此情况为优先信息缺失。

值得注意的是,这里的可蓄意攻击区域  $\Omega$  是根据同一组  $(\alpha, \beta)$  依概率抽样出来的一个样本,多次探测获得的可蓄意攻击区域  $\Omega$  可能不同。另外,节点的重要性有很多评估指标,例如:度数中心性、紧密度中心性、介数中心性、信息中心性等<sup>[17]</sup>,由于各个评估指标的侧重点不同,故在不同的应用场景中可选取其适合的评估指标,除此以外,不同的评估标准并不会对分析步骤上产生差异。为方便说明,在本文中均统一采用度数中心性作为节点的重要性评估指标。

下面详细介绍可蓄意攻击区域  $\Omega$  的建模过程。

首先在产生的网络中将节点按照重要性降序排序,令  $r_i$  为排好序后节点  $v_i$  的编号,其中,最重要的节点编号为 1,最次要的节点编号为  $N$ 。构造节点  $v_i$  的辅助变量  $\Pi_i$  为:

$$\Pi_i = r_i^{-\beta} \quad (1)$$

其中  $\beta \in [0, \infty]$  为信息精度参数,则节点  $v_i$  的入样概率  $\varphi_i$  为:

$$\varphi_i = \Pi_i / \left( \sum_{j=1}^N \Pi_j \right) \quad (2)$$

由表达式可知,  $\beta$  取值越大, 更重要的节点更加容易被选取到。当  $\beta = 0$  时,  $\varphi_i = 1/N$ , 即各节点被取到的概率相等且都为  $1/N$ , 此时为上文中提到的随机信息缺失情况; 当  $\beta = \infty$  时, 最重要节点  $v_i^*$  的辅助变量  $H_{i*} = 1$ , 其余为 0, 则可知最重要节点被选取的概率为 1, 其余节点被选取的概率为 0, 由于每抽取 1 个样本后需要重新计算剩余节点的入样概率, 这样每次选取都能选到当前最重要的节点, 此时为上文中提到的优先信息缺失情况。

按照式(2)中的入样概率抽取样本, 每抽取 1 个样本后需要重新计算剩余节点的入样概率。重复这个过程直到抽取出  $N\alpha$  个节点, 这  $N\alpha$  个节点构成了可蓄意攻击区域  $\Omega$ 。

本文进行的抗毁性分析都是在具有任意度分布的广义随机网络条件下进行的。假设需要攻击网络中的  $N(1 - P)$  个节点 ( $P$  为未被攻击节点比例), 被攻击后的节点可视为失效, 与其相连的边也失效。具体的攻击步骤为, 首先从已掌握节点信息的可蓄意攻击区域  $\Omega$  中按照节点重要性大小依次进行蓄意攻击, 若  $(1 - P) > \alpha$ , 则当可蓄意攻击区域  $\Omega$  中的节点被攻击完后, 还需要对未知区域中的节点进行攻击, 直到完成对整个网络中  $(1 - P)$  比例节点的攻击。值得注意的是, 由于  $\Omega$  区域以外的节点信息未知, 这部分的攻击只能是随机攻击。由此可将攻击步骤分为两类:

1) 若  $(1 - P) \leq \alpha$ , 直接在可蓄意攻击区域  $\Omega$  中按照节点的重要度从大到小进行蓄意攻击即可, 如图 3(a) 所示。

2) 若  $(1 - P) > \alpha$ , 先蓄意攻击可蓄意攻击区域  $\Omega$  中的所有节点, 之后再随机攻击  $\Omega$  区域以外的  $N((1 - P) - \alpha)$  个节点, 如图 3(b) 所示。

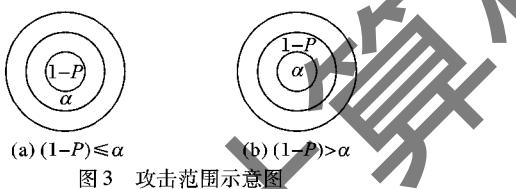


图 3 攻击范围示意图

## 1.2 随机信息缺失条件下的抗毁性分析

首先在  $\beta = 0$  的情况下建立网络分析模型, 即在随机掌握网络中  $N\alpha$  个节点的攻击信息的条件下对网络进行分析。令  $P_c$  为非完备信息条件下的渗流阈值, 表示按照 1.1 节中的攻击步骤攻击  $(1 - P_c)$  比例的节点可以使得整个网络崩溃。

由于已知区域  $\Omega$  中的节点是随机选取的, 所以对于  $(1 - P) > \alpha$  的情况可以等价为先随机攻击网络中的  $N\alpha$  个节点, 再随机攻击  $N((1 - P) - \alpha)$  个节点, 则整个攻击过程可视为随机攻击。设随机攻击渗流阈值为  $P_c^{RF}$ , 若满足  $(1 - P_c^{RF}) > \alpha$ , 则使已知区域  $\Omega$  内的  $N\alpha$  个节点全部移除, 都不能使网络崩溃, 即  $(1 - P_c) > \alpha$ , 此时等效于上述的全网随机攻击, 则有  $P_c = P_c^{RF}$ , 表示非完备信息条件下的渗流阈值  $P_c$  与随机攻击的渗流阈值  $P_c^{RF}$  相等, 此时视为情况 1, 情况 1 的攻击示意图如图 3(b) 所示。若渗流阈值  $P_c^{RF}$  满足  $(1 - P_c^{RF}) \leq \alpha$ , 表示随机攻击已知区域  $\Omega$  内的  $(1 - P_c^{RF})$  比例节点就可以使网络崩溃, 则可知  $(1 - P_c) \leq (1 - P_c^{RF}) \leq \alpha$ , 此时是对已知区域  $\Omega$  中的蓄意攻击, 即在已知区域  $\Omega$  中按照节点的重要度从大到小进行蓄意攻击, 并且蓄意攻击范围不会超出已知区域  $\Omega$ , 此时视为情况 2。情况 2 的攻击范围如图 3(a) 所示。

由于情况 1 有:  $P_c = P_c^{RF}$ , 此时仅为随机攻击, 故不再赘

述。下面利用生成函数对第 2 种情况时的相互依存网络进行分析<sup>[18-19]</sup>。在本文的模型中, 用  $G_{A0}(x)$  表示  $A$  网络中节点度分布为  $p_A(k)$  的生成函数。生成函数可以提供度分布的统计信息, 其含义为度数为  $k$  的节点的概率分布, 以此为基础可推导出网络中最大聚类的大小并最终得到渗流阈值  $P_c \circ G_{A0}(x)$  的表达式为:

$$G_{A0}(x) = \sum_k p_A(k)x^k \quad (3)$$

同理,  $B$  网络中的节点度分布为  $p_B(k)$ , 则其度分布的生成函数  $G_{B0}(x)$  为:

$$G_{B0}(x) = \sum_k p_B(k)x^k \quad (4)$$

当网络中的节点数目很大时, 随机连边的过程可以被建模成分支过程。网络中某个节点与一个度为  $k$  的节点相连的概率  $p_E(k)$  其不仅与  $k$  本身成正比, 还与度为  $k$  的节点数量成正比<sup>[18,20]</sup>, 则有:

$$p_E(k) = \frac{kp(k)}{\sum_k p(k)k} \quad (5)$$

令  $\bar{k} = \sum_k p(k)k$  为节点平均度, 因此, 随机选择一条边到达剩余度为  $k$  的概率  $p_l(k)$ <sup>[21]</sup> 为:

$$p_l(k) = p_E(k+1) = [(k+1)p(k+1)]/\bar{k} \quad (6)$$

则分支过程的生成函数<sup>[15,18,20,22]</sup>  $G_1(x)$  为:

$$G_1(x) = \sum_k p_l(k)x^k = \frac{G_0'(x)}{G_0'(1)} \quad (7)$$

所以  $A$  网络和  $B$  网络分支过程的生成函数  $G_{A1}(x)$ 、 $G_{B1}(x)$  分别为:

$$G_{A1}(x) = \frac{G_{A0}'(x)}{G_{A0}'(1)} \quad (8)$$

$$G_{B1}(x) = \frac{G_{B0}'(x)}{G_{B0}'(1)} \quad (9)$$

令  $R(k)$  表示在  $A$  网络中已知区域  $\Omega$  中度为  $k$  的节点的序号<sup>[23]</sup>, 度数越大的节点越重要, 排序越靠前, 故可得:

$$R(k) = N\alpha \sum_{m=k}^K p(m) \quad (10)$$

其中  $K$  表示节点的最大度。令  $\bar{K}$  表示蓄意攻击完成后在已知区域  $\Omega$  中未失效节点的最大度, 则可得到:

$$R(\bar{K}) = N\alpha \sum_{m=\bar{K}}^K p(m) = N(1 - P) \quad (11)$$

通过解此方程式, 可以得到  $\bar{K}(\alpha, P)$ 。

下面描述对  $A$  网络攻击的过程。设  $q(k)$  表示整个  $A$  网络中度为  $k$  的节点未被攻击的概率, 则可得:

$$q(k) = \begin{cases} 1, & k \leq \bar{K} \\ 1 - \alpha, & k > \bar{K} \end{cases} \quad (12)$$

不失一般性地假设若某个节点  $a$  与节点  $b$  相连, 可以得到节点  $b$  未被攻击的概率  $Q(\bar{K})$  为:

$$Q(\bar{K}) = \sum_{k=0}^{\bar{K}} p(k) * 1 + \sum_{k=\bar{K}+1}^{\infty} p(k)(1 - \alpha) \quad (13)$$

攻击完成后整个  $A$  网络剩余节点的度分布  $p_{AR}(m)$  为:

$$p_{AR}(m) = \sum_{k=m}^{\infty} p_A(k) \binom{k}{m} Q(\bar{K})^m (1 - Q(\bar{K}))^{k-m} \quad (14)$$

所以, 攻击完成后  $A$  网络剩余节点度分布的生成函数  $G_{A0}(x, Q(\bar{K}))$  为:

$$G_{A0}(x, Q(\bar{K})) = \sum_{m=0}^{\infty} p_{AR}(m) x^m \quad (15)$$

化简得到:

$$G_{A0}(x, Q(\bar{K})) = G_{A0}(1 - Q(\bar{K}) + Q(\bar{K})x) \quad (16)$$

同时可得攻击完成后分支过程的生成函数  $G_{A1}(x, Q(\bar{K}))$  为:

$$\begin{aligned} G_{A1}(x, Q(\bar{K})) &= \frac{G_{A0}'(x, Q(\bar{K}))}{G_{A0}'(1, Q(\bar{K}))} = \\ &G_{A1}(1 - Q(\bar{K}) + Q(\bar{K})x) \end{aligned} \quad (17)$$

由于攻击完成之后相互依存网络会进行级联失效步骤,所以现在将此蓄意攻击映射到随机失效中。设有网络  $A'$ ,其生成函数为  $\tilde{G}_{A0}(x)$ ,分支过程的生成函数为  $\tilde{G}_{A1}(x)$ 。随机令其中  $(1 - P)$  比例的节点失效,之后若剩余节点的生成函数满足  $\tilde{G}_{A0}(x, P) = G_{A0}(x, Q(\bar{K}))$ ,则可将上述蓄意攻击过程等价成对网络  $A'$  的随机攻击。又因为对网络  $A'$  随机攻击后,剩余节点的生成函数满足  $\tilde{G}_{A0}(x, P) = \tilde{G}_{A0}(1 - P + Px)^{[15]}$ 。可以得到网络  $A'$  的生成函数  $\tilde{G}_{A0}(x)$  和分支过程的生成函数  $\tilde{G}_{A1}(x)$  为:

$$\tilde{G}_{A0}(x) = G_{A0}\left(1 - \frac{Q(\bar{K})}{P} + \frac{Q(\bar{K})}{P}x\right) \quad (18)$$

$$\tilde{G}_{A1}(x) = G_{A1}\left(1 - \frac{Q(\bar{K})}{P} + \frac{Q(\bar{K})}{P}x\right) \quad (19)$$

根据生成函数理论,定义  $f_A$  为随机的选择一个向外伸出的边,而且这个边没有连向最大聚类的概率,它满足递推关系:

$$\begin{aligned} f_A &= \tilde{G}_{A1}(f_A, P) = G_{A1}(f_A, Q(\bar{K})) = \\ &G_{A1}(1 - Q(\bar{K}) + Q(\bar{K})f_A) \end{aligned} \quad (20)$$

定义  $z_A = 1 - Q(\bar{K}) + Q(\bar{K})f_A$ , 则有:

$$1 - \frac{1}{Q(\bar{K})} + \frac{z_A}{Q(\bar{K})} = G_{A1}(z_A) \quad (21)$$

在攻击完成之后,  $A'$  网络中有  $(1 - P)$  比例的节点被随机移除,则在剩余  $P$  比例的节点中属于最大聚类的比例  $\tilde{g}_A(P)^{[15,19,24]}$  为:

$$\tilde{g}_A(P) = 1 - \tilde{G}_{A0}(f_A, P) \quad (22)$$

根据式(20)、(21),可以得到:

$$\tilde{g}_A(P) = 1 - G_{A0}(z_A) \quad (23)$$

对  $A'$  网络的等效随机攻击完成后,由于  $A'$ 、 $B$  网络是相互依存的, $B$  网络中相应的节点也会失效。由于  $A'$ 、 $B$  网络的连接是随机的。此时  $B$  网络相应地有  $(1 - P)$  比例的节点随机失效,则  $B$  网络剩余节点度分布的生成函数  $G_{B0}(x, P)$  和分支过程的生成函数  $G_{B1}(x, P)^{[15]}$  分别为:

$$G_{B0}(x, P) = G_{B0}(1 - P(1 - x)) \quad (24)$$

$$G_{B1}(x, P) = G_{B1}(1 - P(1 - x)) \quad (25)$$

在剩余  $P$  比例的节点中属于最大聚类的比例  $g_B(P)$  为:

$$g_B(P) = 1 - G_{B0}(f_B, P) \quad (26)$$

其中:

$$f_B = G_{B1}(f_B, P) \quad (27)$$

令  $z_B = 1 - P(1 - f_B)$ , 则有:

$$g_B(P) = 1 - G_{B0}(z_B) \quad (28)$$

令  $x$  为第  $2m+1$  次级联失效后  $A$  网络的剩余节点比例,其中  $m$  为任意正整数,  $y$  为第  $2m$  次级联失效后  $B$  网络的剩余节点比例。由于文献[15] 中推导出  $x$  和  $y$  的表达式为:

$$\begin{cases} x = g_A(y)P \\ y = g_B(x)P \end{cases} \quad (29)$$

由式(29)推导得到:

$$x = g_A(g_B(x)P)P \quad (30)$$

则此迭代式稳定的  $x$  为级联失效过程后相互依存网络剩余节点比例。将式(23)、(28)代入式(30)可以得到级联失效过程后相互依存网络的最大聚类的大小以及渗流阈值  $P_c$ 。

### 1.3 优先信息缺失条件下的抗毁性分析

下面将在  $\beta = \infty$  的情况下建立网络分析模型,即在优先掌握网络中最重要的  $N\alpha$  个节点信息的条件下对网络进行分析。在优先信息缺失的条件下,每次选取都能选到当前最重要的节点。由于按照节点度的大小来判定节点的重要性,所以在已知区域  $\Omega$  中节点的度都比已知区域  $\Omega$  外节点的度大。

1) 当攻击比例  $(1 - P) \leq \alpha$  时,攻击范围如图 3(a) 所示,此时可以等效为对整个网络蓄意攻击  $(1 - P)$  比例的节点。令  $\bar{K}$  表示蓄意攻击完成后在已知区域  $\Omega$  中未失效节点的最大度,  $\bar{K}$  满足等式:

$$N \sum_{k=\bar{K}}^K p(k) = N(1 - P) \quad (31)$$

其中  $K$  表示节点的最大度。通过解此方程式,可以得到  $\bar{K}(P)$ , 则整个网络中任意一个度为  $k$  的节点未受到攻击的概率  $q(k)$  为:

$$q(k) = \begin{cases} 1, & k \leq \bar{K} \\ 0, & k > \bar{K} \end{cases} \quad (32)$$

所以和 1.2 节的原理相同,不失一般性地假设若某个节点  $a$  与节点  $b$  相连,可以得到节点  $b$  未被攻击的概率  $Q(\bar{K})$  为:

$$Q(\bar{K}) = \sum_{k=0}^{\bar{K}} p(k) * 1 + \sum_{k=\bar{K}+1}^{\infty} p(k) * 0 = \sum_{k=0}^{\bar{K}} p(k) \quad (33)$$

将式(33)代入式(14),可得到攻击完成后整个  $A$  网络剩余节点的度分布  $p_{AR}(m)$ 。之后按照 1.2 节的分析方法可以求出  $(1 - P) \leq \alpha$  条件下的  $P_c^{IA}$ , 令作  $P_c^{IA(1)}$ 。若  $P_c^{IA(1)}$  满足  $(1 - P_c^{IA(1)}) \leq \alpha$ , 则表示仅需要移除不超过  $\alpha$  比例的节点就可以使得整个相互依存网络崩溃,所以此时有  $P_c = P_c^{IA(1)}$ 。

2) 若  $P_c^{IA(1)}$  不满足  $(1 - P_c^{IA(1)}) \leq \alpha$ , 则可知若要使网络崩溃不仅要移除已知区域  $\Omega$  中的所有节点,还要随机移除已知区域外的一部分节点,即攻击比例  $(1 - P) > \alpha$ , 此时攻击示意图如图 3(b) 所示。

令  $\tilde{m}$  表示已知区域  $\Omega$  中节点的最小度,可以得到  $\tilde{m}$  满足等式:

$$N\alpha = N \sum_{k=\tilde{m}}^K p(k) \quad (34)$$

通过解此方程式,可以得到  $\tilde{m}(\alpha)$ , 则整个网络中任意一个度为  $k$  的节点未受到攻击的概率  $q(k)$  为:

$$q(k) = \begin{cases} \frac{P}{1 - \alpha}, & k < \tilde{m} \\ 0, & k \geq \tilde{m} \end{cases} \quad (35)$$

所以,和 1.2 节的原理相同,不失一般性地假设若某个节点  $a$  与节点  $b$  相连,可以得到节点  $b$  未被攻击的概率  $Q(\bar{K})$  为:

$$Q(\bar{K}) = \sum_{k=0}^{\tilde{m}-1} p(k) * \frac{P}{1 - \alpha} + \sum_{k=\tilde{m}}^{\infty} p(k) * 0 =$$

$$\frac{P}{1-\alpha} \sum_{k=0}^{\bar{m}-1} p(k) \quad (36)$$

将式(36)代入式(14),可得到攻击完成后整个 A 网络剩余节点的度分布  $p_{AR}(m)$ 。之后按照 1.2 节的分析方法就可以求出  $(1-P) > \alpha$  条件下的  $P_c^{IA}$ ,令作  $P_c^{IA(2)}$ 。此时有  $P_c = P_c^{IA(2)}$ 。

## 2 实例分析与仿真实验

在上一章中,主要研究了两种情况(随机信息缺失和优先信息缺失)下相互依存网络的抗毁性,提出了信息缺失条件下的相互依存网络抗毁性分析方法。下面将以无标度网络为例通过 Matlab 进行数值求解并通过模拟真实网络的仿真方法对提出的理论进行详细的验证。其中,模拟真实网络的仿真方法是借助文献[25~26]中提出的方法产生一个度分布为  $p(k) = Ck^{-\lambda}$  的无标度网络来进行仿真,同时为了与已有文献的数据进行对比验证,本文将无标度网络参数设置为:  $N = 10000, \lambda = 3, m = 1$ 。由于无标度网络的生成和蓄意攻击区域  $\Omega$  的选取过程都具有随机性,需要通过多次(同样为了与已有文献的数据进行对比验证,本文中取 10 次,与文献[23]相同)仿真求平均值的方式尽可能地消除偶然性。

图 4 给出了无标度网络在随机信息缺失(即  $\beta = 0$ )条件下  $x$  与  $g_A(g_B(x)P)P$  的关系。根据上一章的理论分析可知,迭代式  $x = g_A(g_B(x)P)P$  中的  $x$  为级联失效过程后相互依存网络剩余节点比例,所以当曲线与  $x = g_A(g_B(x)P)P$  相切时,此曲线对应的  $P$  值即为渗流阈值  $P_c$ 。在图 4(a) 中,当  $\alpha = 0.8, \beta = 0$  时,得到  $P_c = 0.8411$ ,满足  $(1 - P_c) < \alpha$ 。在图 4(b) 中,当  $\alpha = 0, \beta = 0$  时,得到  $P_c = 0.7401$ ,满足  $(1 - P_c) > \alpha$ 。值得注意的是:  $(1 - P_c) > \alpha$  (即图 4(b)) 的情况即与全网随机失效时等价,此时为文献[15]中的情况,通过本文方法求解得到的渗流阈值  $P_c$  与文献[15]中的结果一致,这也间接验证了理论的正确性。

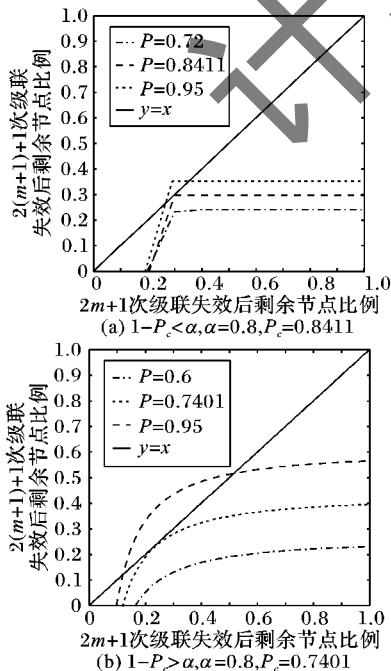


图 4 无标度网络在随机信息缺失(即  $\beta = 0$ )条件下  $x$  与  $g_A(g_B(x)P)P$  的关系

图 5 给出了无标度网络在优先信息缺失(即  $\beta = \infty$ )条

件下  $x$  与  $g_A(g_B(x)P)P$  的关系。同上,当曲线与  $x = g_A(g_B(x)P)P$  相切时,此曲线对应的  $P$  值即为阈值。在图 5(a) 中,当  $\alpha = 0.8, \beta = \infty$  时,得到阈值  $P_c = 0.8949$ ,满足  $(1 - P_c) < \alpha$ 。在图 5(b) 中,当  $\alpha = 0.8, \beta = \infty$  时,得到阈值  $P_c = 0.8864$ ,满足  $(1 - P_c) > \alpha$ 。值得注意的是:  $(1 - P_c) < \alpha$ (即图 5(a))的情况即与全网蓄意攻击时等价,此时为文献[23]中的情况,通过本文方法求解得到的渗流阈值  $P_c$  与文献[23]中的一致,同样间接验证了理论的正确性。

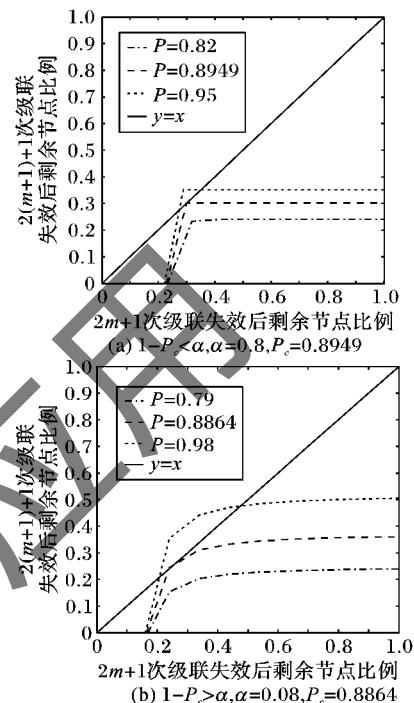


图 5 无标度网络在优先信息缺失(即  $\beta = \infty$ )条件下  $x$  与  $g_A(g_B(x)P)P$  的关系

图 6 完整地展现了无标度网络中信息广度  $\alpha$  和信息精度  $\beta$  与  $P_c$  的关系,实线为数值解,符号为模拟真实网络的结果,两者基本一致,说明理论分析方法正确。可以看出信息广度参数  $\alpha$  和信息精度参数  $\beta$  对相互依存网络的渗流阈值影响巨大,并且信息精度比信息广度影响更大,少量的高精度节点信息就等价于大量的低精度节点信息。例如,若只想攻击 20% 的节点就想摧毁整个网络(即  $P_c = 0.8$ ),在  $\beta = \infty$  时只需要掌握 1.4% 的节点信息(即  $\alpha = 0.014$ )即可,而在  $\beta = 0$  时需要掌握 62% 的节点信息(即  $\alpha = 0.62$ )才行。同时可以看到,隐藏少量节点的信息即可很大程度上增加网络的抗毁性。已知少量最重要的节点可以很大程度上降低网络的抗毁性。例如,在  $\beta = \infty$  条件下,  $\alpha = 0$  时渗流阈值  $P_c = 0.74$ ,之后  $P_c$  便急剧上升,在  $\alpha = 0.105$  时就已经达到上界。由于目前理论研究的局限性,在  $\beta = 1$  和  $\beta = 2$  时只是通过模拟真实网络得到的仿真解,本文尚未作理论值分析。从中可以得出  $\beta$  越大,越重要的节点的攻击信息更容易被获取,即更容易被蓄意攻击,此时渗流阈值就会相应升高,即网络的抗毁性就会下降。

图 7 分别给出了在  $\beta = 0, \beta = \infty$  下无标度网络中未被攻击的节点比例  $P$  与级联失效后剩余节点比例  $P_c$  的关系,实线为相互依存网络下的数值解,符号为仿真结果,两者基本符合。从图中可以看出,相互依存网络的抗毁性明显弱于单层网络,这是因为,在 A 网络中度比较小的节点失效可能会导

致B网络中一个大度节点失效,这样就使得相互依存的无标度网络变得很难被保护,因此更加脆弱。虽然增加相互依存网络度的相关性可以提高系统的抗毁性<sup>[27]</sup>,但相互依存网络的抗毁性依然显著低于单层网络。

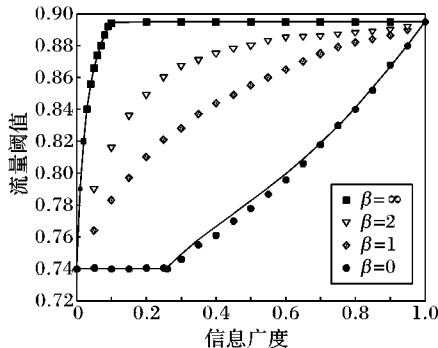
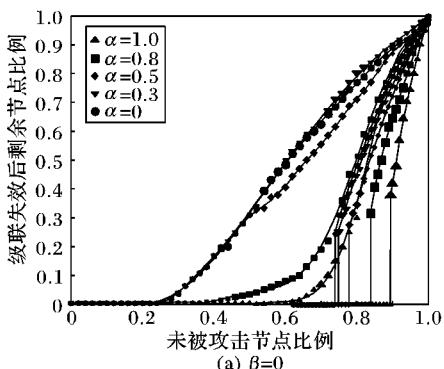


图6 无标度网络中信息广度 $\alpha$ 和信息精度 $\beta$ 与 $P_c$ 的关系



(a)  $\beta=0$

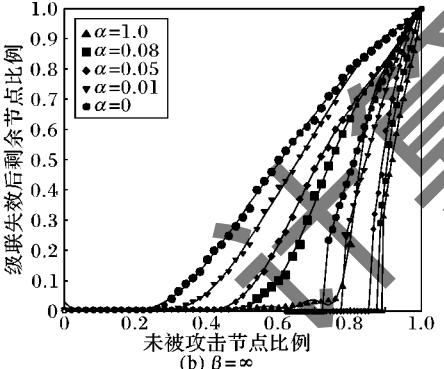


图7 无标度网络中 $P$ 与 $P_\infty$ 的关系

图8给出了无标度网络中节点个数 $N$ 与渗流阈值 $P_c$ 的关系。实线为数值解,符号为仿真结果。可以看出,虽然经过多次求解取平均的方式,在节点数量 $N$ 较少的情况下仿真结果与数值解之间还是存在较大差异,而随着 $N$ 的增加,仿真结果与数值解之间的差异逐渐缩小,最终和数值解基本吻合。从图中还可以得出,随着 $N$ 的增加,相互依存网络的渗流阈值逐渐下降,并且下降的趋势逐渐趋于平缓。

### 3 结语

本文首先将网络信息具体地分为结构信息和攻击信息,利用无放回不等概率抽样的方法建立了信息缺失模型;在此模型的基础上借助生成函数和渗流理论的思想创新地提出了信息缺失条件下的相互依存网络抗毁性的理论分析方法。在以无标度网络作为实例进行进一步的仿真实验后发现,信息广度 $\alpha$ 和信息精度 $\beta$ 对相互依存网络的渗流阈值影响巨

大,并且信息精度比信息广度影响更大,少量的高精度节点信息就等价于大量低精度节点信息;隐藏少量节点的信息即可很大程度上增加网络的抗毁性,已知少量最重要的节点可以很大程度上降低网络的抗毁性;同时,本文还发现即使在信息缺失条件下相互依存网络仍然比单层的网络更脆弱。信息缺失条件下相互依存网络的抗毁性分析填补了相互依存网络在随机失效和蓄意攻击之间的抗毁性分析模型的空白,结合得到的结论和性质可对攻击策略的制定提供有效的参考。本文仅仅考虑了无反馈且完全相互依赖的相互依存网络抗毁性,并且假设节点被攻击后与之相连的边会被全部移除。实际上,大多数时候相互依存网络的依赖结构比较复杂,而且节点是很难被完全移除的。因此,有反馈、部分相互依赖和基于边的非完备信息条件下的网络抗毁性分析将是下一步工作的重点。

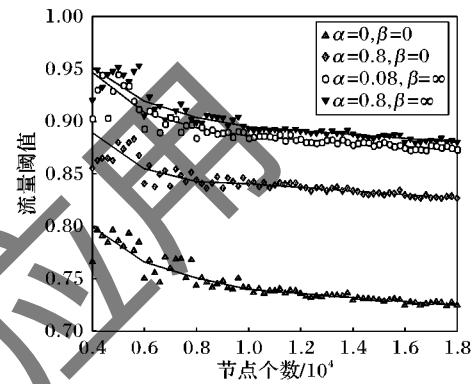


图8 无标度网络中 $N$ 与 $P_c$ 的关系( $\lambda = 3, m = 1$ )

### 参考文献:

- [1] WATTS D J, STROGATZ S H. Collective dynamics of "small-world" networks [J]. Nature, 1998, 393(6684): 440–442.
- [2] ALBERT R, JEONG H, BARABÁSI A L. Error and attack tolerance of complex networks [J]. Nature, 2000, 406(6794): 378–382.
- [3] COHEN R, EREZ K, BEN-AVRAHAM D, et al. Resilience of the Internet to random breakdowns [J]. Physical Review Letters, 2000, 85(21): 4626.
- [4] CALLAWAY D S, NEWMAN M E J, STROGATZ S H, et al. Network robustness and fragility: percolation on random graphs [J]. Physical Review Letters, 2000, 85(25): 5468.
- [5] ALBERT R, BARABÁSI A L. Statistical mechanics of complex networks[J]. Reviews of Modern Physics, 2002, 74(1): 47.
- [6] NEWMAN M E J. The structure and function of complex networks [J]. SIAM Review, 2003, 45(2): 167–256.
- [7] DOROGOVTCSE S N, MENDES J F F. Evolution of networks: from biological nets to the Internet and WWW [M]. Oxford: Oxford University Press, 2013: 6–220.
- [8] SONG C, HAVLIN S, MAKSE H A. Self-similarity of complex networks [J]. Nature, 2005, 433(7024): 392–395.
- [9] PASTOR-SATORRAS R, VESPIGNANI A. Evolution and structure of the Internet: a statistical physics approach [M]. Cambridge: Cambridge University Press, 2007: 5–268.
- [10] NEWMAN M E J, BARABÁSI A L, WATTS D J. The structure and dynamics of networks [M]. Princeton: Princeton University Press, 2006: 9–415.
- [11] CALDARELLI G, VESPIGNANI A. Large scale structure and dynamics of complex Webs [M]. Singapore: World Scientific, 2007: 4–168.

(下转第1254页)

- sponse digital filter based on free search algorithm [J]. Computer Engineering, 2014, 40(8): 318–321. (任伟, 曾以成, 陈莉, 等. 基于自由搜索算法的 IIR 数字滤波器设计[J]. 计算机工程, 2014, 40(8): 318–321.)
- [2] YANG Y, YU X. Cooperative coevolutionary genetic algorithm for digital IIR filter design [J]. IEEE Transactions on Industrial Electronics, 2007, 54(3): 1131–1318.
- [3] LISERRE M, DELL A, BLAABJERG F. Genetic algorithm-based design of the active damping for an LCL-filter three-phase active rectifier [J]. IEEE Transactions on Power Electronics, 2004, 19(1): 76–86.
- [4] WU Y. FIR filter design based on genetic algorithms [J]. Communications Technology, 2012, 45(3): 108–110. (吴艳君. 基于遗传算法的 FIR 滤波器设计[J]. 通信技术, 2012, 45(3): 108–110.)
- [5] SEMWAL G, RASTOGI V. Design of LPWG broad band filter with genetic algorithm optimization [J]. Journal of Optics, 2014, 43(3): 165–168.
- [6] SONG D. Digital filter optimization based on momentum crossover particle swarm optimization algorithm [J]. Computer Simulation, 2013, 30(8): 356–375. (宋定宇. 基于粒子群算法的数字滤波器优化与仿真[J]. 计算机仿真, 2013, 30(8): 356–375.)
- [7] ZHANG X, MA H, XUE P. IIR digital filter design based on improved PSO algorithm [J]. Computer Engineering and Design, 2011, 32(8): 2853–2856. (张旭针, 马红梅, 薛鹏骞. 基于改进粒子群优化算法的 IIR 数字滤波器设计. 计算机工程与设计, 2011, 32(8): 2853–2856.)
- [8] CHEN S, LUK B. Digital IIR filter design using particle swarm optimization [J]. International Journal of Modelling, Identification and Control, 2010, 9(4): 327–335.
- [9] WANG L, LIU D. Soft morphological filter based on particle swarm algorithm [J]. Journal of Computer Applications, 2010, 30(10): 2811–2814. (王利朋, 刘东权. 基于粒子群算法的柔性形态学滤波器 [J], 计算机应用, 2010, 30(10): 2811–2814.)
- [10] ZHONG J, FUNG Y, DAI M. A biologically inspired improvement strategy for particle filter: ant colony optimization assisted particle filter [J]. International Journal of Control, Automation and Systems, 2010, 8(3): 519–526.
- [11] SHUNTARO T, KENJI S. Design of FIR filters with discrete coefficients using ant colony optimization [J]. IEEE Transactions on Electronics, Information and Systems, 2012, 132(7): 1066–1071.
- [12] LAN C, GAO H, LI S. FIR digital filters design based on differential cultural algorithm [J]. Techniques of Automation and Application, 2010, 29(6): 65–73. (兰成章, 高洪远, 李诗桓. 基于差分文化算法的 FIR 数字滤波器设计[J]. 自动化技术与应用, 2010, 29(6): 65–73.)
- [13] JIN Y, CAI Z, LIANG D. Adaptive unscented Kalman filter based on differential evolution algorithm [J]. Journal of Electronics and Information Technology, 2013, 35(4): 838–843. (金璐, 蔡之华, 梁丁文. 基于差分演化算法的自适应无迹卡尔曼滤波[J]. 电子与信息学报, 2013, 35(4): 838–843.)
- [14] CHANDRA A, CHATTOPADHYAY S. A novel approach for coefficient quantization of low-pass finite impulse response filter using differential evolution algorithm [J]. Signal, Image and Video Processing, 2012, 8(7): 1307–1321.
- [15] CHAUHAN R, ARYA S. Determine optimal coefficients of IIR digital filters using simulated annealing [J]. International Journal of Computer Applications, 2012, 43(10): 36–40.

(上接第 1229 页)

- [12] BARRAT A, BARTHELEMY M, VESPIGNANI A. Dynamical processes on complex networks [M]. Cambridge: Cambridge University Press, 2008: 8–145.
- [13] COHEN R, HAVLIN S. Complex networks: structure, robustness and function [M]. Cambridge: Cambridge University Press, 2010: 9–144.
- [14] NEWMAN M. Networks: an introduction [M]. Oxford: Oxford University Press, 2010: 5–129.
- [15] BULDYREV S V, PARSHANI R, PAUL G, et al. Catastrophic cascade of failures in interdependent networks [J]. Nature, 2010, 464(7291): 1025–1028.
- [16] RAO J N K, HARTLEY H O, COCHRAN W G. On a simple procedure of unequal probability sampling without replacement [J]. Journal of the Royal Statistical Society: Methodological, 1962, B24: 482–491.
- [17] ZHUGE H, ZHANG J. Topological centrality and its e-science applications [J]. Journal of the American Society for Information Science and Technology, 2010, 61(9): 1824–1841.
- [18] NEWMAN M E J. Spread of epidemic disease on networks [J]. Physical Review E, 2002, 66(1): 016128.
- [19] SHAO J, BULDYREV S V, COHEN R, et al. Fractal boundaries of complex networks [J]. Europhysics Letters, 2008, 84(4): 48004.
- [20] 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.
- [21] SHAO J, BULDYREV S V, BRAUNSTEIN L A, et al. Structure of shells in complex networks [J]. Physical Review E, 2009, 80(3): 036105.
- [22] 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]. Physical Review Letters, 2010, 105(4): 048701.
- [23] WU J, DENG H, TAN Y, et al. Vulnerability of complex networks under intentional attack with incomplete information [J]. Journal of Physics A: Mathematical and Theoretical, 2007, 40(11): 2665.
- [24] HUANG X, GAO J, BULDYREV S V, et al. Robustness of interdependent networks under targeted attack [J]. Physical Review E, 2011, 83(6): 065101.
- [25] MOLLOY M, REED B. A critical point for random graphs with a given degree sequence [J]. Random Structures and Algorithms, 1995, 6(2/3): 161–180.
- [26] MOLLOY M, REED B. The size of the giant component of a random graph with a given degree sequence [J]. Combinatorics, Probability and Computing, 1998, 7(3): 295–305.
- [27] BULDYREV S V, SHERE N W, CWILICH G A. Interdependent networks with identical degrees of mutually dependent nodes [J]. Physical Review E, 2011, 83(1): 016112.