# 基于代价的复杂网络抗攻击性研究

吴泓润 覃 俊 郑波尽
(中南民族大学计算机科学学院 武汉 430074)

**摘 要** 目前的复杂网络抗攻击性研究大多基于"无代价"条件,而这一假设下的大多数复杂网络面对的选择性攻击都非常脆弱,这与现实网络相矛盾。针对这一矛盾,提出代价下影响复杂网络抗攻击性的关键指标——网络紧致系数、平均度;基于网络紧致系数、平均度建立了代价下面向节点的选择性攻击模型,定性分析了网络紧致系数、平均度与复杂网络抗攻击性间的关系。仿真结果证实了所提度量指标的有效性:网络紧致系数越大、平均度越大,则网络越鲁棒;相同平均度下,网络紧致系数越大,则网络越鲁棒。

**关键词** 复杂网络,网络紧致系数,平均度,代价
**中图法分类号** N949 **文献标识码** A

## Anti-attack Ability Based on Costs in Complex Networks

WU Hong-run QIN jun ZHENG Bo-jin
(College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China)

**Abstract** Current researches on anti-attack of complex networks are based on the hypothesis that all the attacks wouldn't spend any cost. However, most of the complex networks are fragile in confronting selective attack strategies without any cost, which is conflict with real-world networks. Aiming at the contradiction, this paper proposed key indexes, i. e. , the network compactness index and average degree, to measure the attack effects with costs. This paper developed the selective node attack strategies model based on the network compactness index, and qualitative analysis of the relation between network compactness index, average degree and anti-attack of complex networks. The detailed simulation results show that the key indexes proposed in the paper are effective: the more compact the network is, and the larger the average degree is, then the more robust the network is; in the same average degrees, the larger the network compactness index is, the more robust the network is.

**Keywords** Complex networks, Network compactness index, Average degrees, Cost

## 1 引言

现实世界充斥着各种各样的复杂网络,这些网络由许多节点与连接两节点的边所组成,其中节点用来代表组成真实系统中的个体,而节点间的边用来表示个体间的相互联系[1]。如由人与人之间的相互关系生成的社会关系网络[2],由路由器和计算机连接而成的因特网[3],由大量页面通过超链接组成的万维网[4],由大量神经细胞通过神经纤维相互连接形成的神经网络[5]等。随着人类社会日益网络化,人们对各种关乎国计民生的复杂网络的安全性和可靠性提出越来越高的要求,所以,复杂网络的抗攻击性研究的重大理论意义和应用价值也日益显示出来[6]。在理论上,此研究是复杂网络稳定性研究不可或缺的一部分;在应用上,此研究将得到保持复杂网络系统稳定、分裂复杂网络系统的理论和方法,同时该理论和方法对建立鲁棒的社会、生物和技术网络、瓦解犯罪集团等具有重要的指导意义。

当前,复杂网络抗攻击性研究方法主要有基于图论、基于解析和基于仿真的抗攻击性研究3种主要思路,这些研究方法主要基于"无代价"这一前提假设。"无代价"是指移除网络中节点或者边时不考虑攻击代价[7,8]。然而,这一假设下的大多数复杂网络面对选择性攻击都非常脆弱,如众所周知的无标度网络,其在选择性攻击下非常脆弱[9],这与现实世界中Internet无标度网络面对黑客的选择性攻击没有迅速崩溃相矛盾。本文的前期研究[10]已对此矛盾现象进行了论证,并指出"代价"下对复杂网络的研究更接近现实网络。"代价"下是指移除网络中节点或边时需要考虑攻击代价,虽然"代价"下研究复杂网络的抗攻击性更真实,但是并没有发现相关研究。为正确衡量复杂网络的抗攻击性,提出了度量复杂网络抗攻击性的关键指标,即网络紧致系数、平均度,针对主流的3种复杂网络模型[11]研究,定性分析了网络紧致系数、平均度与复杂网络抗攻击性间的关系,并通过仿真实验证明了网络紧致系数、平均度对复杂网络抗攻击性的重要影响。

## 2 代价下基于节点的选择性攻击模型

### 2.1 选择性攻击的定义

网络可定义为节点以及连接节点的边的集合,记为 $G$:

到稿日期:2011-10-14 返修日期:2012-02-23 本文受广西自然科学基金项目(2011GXNSFB018074)资助。
吴泓润(1989—),女,硕士生,主要研究方向为复杂网络、数据挖掘;覃 俊(1968—),女,博士,教授,主要研究方向为复杂网络,E-mail:wrj_qj@hotmail.com(通信作者);郑波尽(1975—),博士后,副教授,主要研究方向为复杂网络、智能优化。

$$G=(V,\{Edge\}) \tag{1}$$

式中，$V$ 为网络的节点集合，$\{Edge\}$ 为网络的边集合。

由网络的定义可知，网络由节点以及边组成。因此，选择性攻击可以是针对节点的，也可以是针对边的。本文只考虑针对节点的选择性攻击，针对边的选择性攻击将在后续工作中给出。

若基于节点攻击网络，则使用节点遭受攻击前、后网络的差异来定义攻击，即将节点攻击定义为移除节点集 $N$ 后对网络连通性的影响。

### 2.2 选择性攻击策略的定义

节点重要性度量指标有很多种，如节点度、介数、接近度、特征向量中心[12]等，攻击策略可以选择面对任意一种节点重要性度量指标的选择攻击。当前对选择性攻击策略的研究主要有：基于初始图面对节点度、介数、接近度重要性度量指标的选择攻击。为比较代价下选择攻击策略与无代价下选择攻击策略的差异性，本文同样采用“基于初始图面向节点度、介数、接近度”节点重要性度量指标作为选择性攻击策略。这 3 种选择性攻击策略定义如下：

1）基于初始图的面向度的选择性攻击策略：该攻击策略根据初始网络拓扑图，按照节点度从大到小的顺序，将节点逐个移除，简记为 ID(Initial-Degree)攻击策略。

2）基于初始图的面向介数的选择性攻击策略：该攻击策略根据初始网络拓扑图，按照节点介数从大到小的顺序，将节点移除，简记为 IB(Initial-Betweenness)攻击策略。

3）基于初始图的面向接近度的选择性攻击策略：该攻击策略根据初始网络拓扑图，按照节点接近度从大到小的顺序，将节点个逐移除，简记为 IC(Initial-Closeness)攻击策略。

### 2.3 攻击代价的定义

考虑到“度”是节点属性中最本质的度量，也为度量攻击代价，可以用基于度的函数来定义攻击的代价。

假设节点 $v\in V$，边 $e\in Edge$，在遭受一次攻击之后，即移走节点集 $N$ 之后，$G$ 变为 $G'=(V',\{Edge'\})$，则该次攻击的代价记为 $Cost(N)$：

$$Cost(N)=\sum_{v\in N} f(Degree(v)) \tag{2}$$

式中，$f(x)$ 的定义可以有很多种。如 $f(x)=x^2$，此时节点的攻击代价就为度的平方和，即移除一个度为 $a$ 的节点所花费的代价为 $a^2$；$f(x)$ 也可以定义为 $f(x)=\frac{1}{x}$，即移除一个度为 $a$ 的节点所花费的代价为 $\frac{1}{a}$。因此，为公平地定义攻击代价，本文以 $f(x)=x$ 来定义节点攻击代价（节点度与攻击代价成正线性比关系），即：

$$Cost(N)=\sum_{v\in N} Degree(v) \tag{3}$$

### 2.4 攻击效果的定义

攻击效果可以用网络遭受攻击前、后，其性能变化来度量。网络性能的度量有很多种，如最大连通子图规模、平均测量长度、反平均测量长度等[13,14]，本文以攻击后网络性能的变化来衡量攻击效果，而攻击后网络的性能由最大连通子图来度量。

网络 $G=(V,\{Edge\})$ 表示遭受攻击后的网络性能，用 $S(N)$ 表示当前最大连通子图的大小。为方便比较攻击前、后网络性能的变化，考虑将网络性能进行归一化，归一化的网络性能用 $E(N)$ 表示：

$$E(N)=\frac{S(N)}{|V|} \tag{4}$$

式中，$|V|$ 是初始网络包含的节点总数。

对于任意一个网络，必定存在攻击代价的上限。本文仅考虑节点攻击，因此攻击代价的上限称为节点总攻击代价。节点总攻击代价定义为在初始网络 $G$ 中，移走节点数目为 $|V|$，即移走全部节点数目所花费的代价，因此，$Cost(V)=\sum_{v\in V} Degree(v)$ 即为总攻击代价，$Cost(N)$ 表示移走节点集 $N$ 的攻击代价。为方便下文表示攻击效果和攻击代价间的关系，用 $C(N)$ 表示归一化后的攻击代价，因此将节点的攻击代价归一化公式定义为：

$$C(N)=\frac{Cost(N)}{Cost(V)} \tag{5}$$

## 3 网络紧致系数、平均度对网络抗攻击性的影响

### 3.1 网络紧致系数的定义

由 2.2 节攻击策略定义可知，复杂网络面对的攻击策略有很多种，复杂网络面对攻击策略 $A$ 可能具有良好的抗攻击性，却可能在攻击策略 $B$ 下很快就崩溃。如复杂网络 $G$ 面对不明攻击策略下，$G$ 中有些节点的度大，介数却很小，同时有些节点介数大，度却很小，若攻击者采取面向度的攻击策略时，攻击者会付出很高的攻击代价才使网络崩溃；若攻击者采取面对介数的攻击策略时，攻击者会以很低的攻击代价使网络快速崩溃。同样的情形也可以外推到其他节点重要性度量指标上。

综上分析可知，网络面对某一种攻击策略表现出较强的抗攻击性，却并不能表示该网络整体的抗攻击性较强，因此必须采取一种归一法来衡量网络的整体抗攻击性。若将所有的节点重要性度量指标“$a$、$b$、$c$ 度量指标”归约为其中一种重要性度量指标 $a$，即度量指标 $b$、$c$ 大时，度量指标 $a$ 也大；度量指标 $b$、$c$ 小时，度量指标 $a$ 也小，此时，网络面对度量指标 $b$、$c$ 所花费的攻击代价与面对度量指标 $a$ 所花费的攻击代价近似相同。因此，按照此方法对度量指标归一化后，可以从整体上衡量攻击网络所花费的攻击代价。

网络抗攻击性越强（弱），攻击网络所花费的攻击代价就越高（低），因此攻击网络所花费的攻击代价直接反映网络抗攻击性的强弱。由 2.3 节攻击代价的定义可知，攻击网络所花费的攻击代价与节点度密切相关，所以，本文将其他节点重要性度量指标（介数、接近度）规约到度，即其他节点重要性度量指标越大，则节点度越大，网络面对其攻击策略所花费的攻击代价就越高。

所以，为正确衡量网络的抗攻击性，本文提出衡量网络整体抗攻击性的重要度量指标——网络紧致系数。为方便表述网络紧致系数的定义，将介数、接近度重要性度量指标又称作其他节点重要性度量指标。在给出网络紧致系数定义之前，式(6)先给出节点度与其他节点重要性度量指标间的紧致系数。

皮尔逊相关系数公式是一种广为人知的计算公式，该公式通常用来测量两个定距变量（例如，年龄和身高）的关系强度。本文采用该公式来计算其他节点重要性度量指标（介数、接近度）紧致系数，公式如下：

$$\sigma=\frac{\sum XY-\frac{\sum X\sum Y}{N}}{\sqrt{(\sum X^2-\frac{(\sum X)^2}{N})(\sum Y^2-\frac{(\sum Y)^2}{N})}} \tag{6}$$

式中，$X$ 是网络节点的度序列，$Y$ 是其他节点重要性度量序列中的一种，$N$ 是网络节点总数。$\sigma$ 即为节点的度与其他某一种节点重要性度量指标的紧致系数，且 $\sigma\in[-1,1]$。若 $\sigma>0$，表明两个变量是正相关，即一个变量的值越大，另一个变量的值也会越大；若 $\sigma<0$，表明两个变量是负相关，即一个变量的值越大，另一个变量的值反而会越小。$\sigma$ 的绝对值越大，表明相关性越强；若 $\sigma=0$，则表明两个变量间不是线性相关。因此其他节点重要性度量指标的紧致系数即是：网络中节点度与其他重要性度量指标的相关程度。

度与其他节点重要性度量指标的紧致系数只可以度量网络面对某一攻击策略的抗攻击性，不可以度量整体网络的抗攻击性。为了度量整体网络抗攻击性，将网络紧致系数定义为各个其他重要性度量指标紧致系数的乘积。

### 3.2 网络紧致系数与网络抗攻击性相关关系分析

根据网络紧致系数的定义可知，若网络紧致系数越大，则节点度与其他节点重要性度量指标的紧致系数越大，此时面向其他节点重要性度量指标的攻击策略就可以规约为面向度的攻击策略，攻击代价会因为攻击度大的节点而上升得很快，则网络在面向其他节点重要性度量指标的攻击策略下，需要花费很高的攻击代价才能使网络崩溃；反之，攻击代价因为攻击度小的节点而上升得很慢，则网络在面向其他节点重要性度量指标的攻击策略下，只需花费很低的攻击代价就可以使网络崩溃。

综上分析可知，网络紧致系数比较大的网络在面对选择性攻击时，不会使攻击策略产生额外的攻击效率，因此攻击网络所花费的攻击代价比较高。所以，在相同其他条件下，网络紧致系数越大，网络的抗攻击性就越强。

### 3.3 平均度的定义

在网络 $G=(V,\{Edge\})$ 中，记网络 $G$ 的平均度为 $Avgdegree(V)$：

$$Avgdegree(V)=\frac{\sum_{v\in V}Degree(v)}{|V|} \tag{7}$$

式中，$|V|$ 是网络 $G$ 的节点数。

网络的平均度越大，平均每个节点所连接的边就越多。由 2.3 节攻击代价的定义可知，网络中攻击某一节点所花费的攻击代价等于该节点的度，所以，平均每个节点所连接的边越多，攻击网络所花费的代价越高。

### 3.4 平均度与网络抗攻击性相关关系分析

若网络 $G$ 平均度越大，则平均每个节点所连接的边就越多，在此情况下，若选择性攻击删除网络中度大的节点，其他节点仍有可能连接在一起，且攻击代价会因为攻击度大的节点上升得很快，但网络仍不会崩溃。所以，网络的平均度越大，则攻击网络所花费的攻击代价越高，网络崩溃速度越慢。

综上分析可知，相同其他条件下，网络的平均度越大，网络的抗攻击性就越强。

### 3.5 网络紧致系数、平均度与网络抗攻击性相关关系分析

由 2.3 节－3.4 节理论分析可得：在代价条件下，复杂网络在选择性节点攻击下可能是鲁棒的；进一步，网络紧致系数、平均度越大的复杂度网络在选择性攻击下的抗攻击性越强，而在同一平均度下，紧致系数越大，网络抗攻击性越强。

## 4 仿真实验结果及分析

为了实证网络紧致系数、平均度与复杂网络抗攻击性的密切关系，本文选择了当前主流的 3 类复杂网络模型进行研究，即无标度网络模型、规则网络模型、ER 网络模型。为了分析紧致系数、平均度对网络抗攻击性的影响，并避免其他因素对网络抗攻击性的影响，实验中模拟的 3 类复杂网络模型具有相同节点数目。对于如何模拟此 3 类复杂网络，本文的前期研究[11]已对此做了详细论述。3 类复杂网络节点数目、边数目如表 1 所列。

表 1 节点和边数目

| 网络 | 节点数目 | 度数目 |
|---|---|---|
| CSF 紧致无标度网络 | 100 | 554 |
| CSF 社区无标度网络 | 100 | 554 |
| Regular 网络 | 100 | 299 |
| ER 网络 | 100 | 295 |

对每一网络分别采用基于顶点的 ID、IB、IC 攻击策略进行选择性攻击，网络抗攻击性和攻击代价仿真实验如 4.2 节、4.3 节所示。

### 4.1 不同网络的网络紧致系数、平均度

紧致系数和平均度均与网络的抗攻击性有紧密的关系，为了定性地分析二者与网络抗攻击性的关系，我们将网络根据平均度大小分组，将相当平均度的网络归为一组。平均度超过 8 以上的网络归入“大度”组，平均度小于 4 的网络归入“小度”组。本文将 CSF 紧致无标度网络和 CSF 社区无标度网络归入“大度组”，将 ER 网络和 WS 网络归入“小度组”，如表 2 所列。

表 2 网络紧致系数和平均度

| 分组 | 网络 | 顶点度与介数紧致系数 | 顶点度与接近度紧致系数 | 网络紧致系数 | 平均度 |
|---|---|---|---|---|---|
| 大度组 | CSF 紧致无标度网络 | 0.94 | 0.58 | 0.545 | 11.9 |
| | CSF 社区无标度网络 | 0.45 | 0.62 | 0.279 | 8.4 |
| 小度组 | Regular 网络 | 0.32 | 0.12 | 0.038 | 2.99 |
| | ER 网络 | 0.95 | 0.88 | 0.836 | 2.95 |

### 4.2 代价下不同类型网络抗攻击性仿真结果及分析

在 ID、IB、IC 3 种攻击策略下，不同类型网络的抗攻击效果如图 1－图 4 所示。

图中，横轴 $|N|/|V|$ 表示移除节点的数目占初始图中总节点数目的比例；纵坐标 $E$ 表示移除 $|N|$ 个节点后归一化的网络性能，纵坐标 $C$ 表示移除 $|N|$ 个节点所需要的归一化攻击代价。$E$ 与 $|N|/|V|$ 间关系的意义：移除 $|N|$ 个节点后，网络性能下降的速度；$C$ 与 $|N|/|V|$ 间关系的意义：移除 $|N|$ 个节点，攻击代价的上升速度。因此，在某攻击策略下，若 $E$ 与 $|N|/|V|$ 的关系曲线下降趋势越陡，则表示在此攻击策略下，网络性能下降速度越快；若 $C$ 与 $|N|/|V|$ 的关系曲线上升趋势越陡，则表示在此攻击策略下，攻击该网络所需要的代价越大。

图 1－图 4 分别为不同网络在 ID、IB、IC 攻击策略下的攻击效果图。CSF 紧致无标度网络在 ID、IB、IC 攻击策略下，其归一化的网络性能 $E$ 均下降得很快，但其归一化攻击代价上升速度也很快；CSF 社区无标度网络在 ID 攻击策略下，其归一化的网络性能 $E$ 下降速度同 CSF 紧致无标度网络相当，在

IB 和 IC 攻击下，其归一化网络性能 $E$ 下降速度快于 ID，但其归一化攻击代价上升速度慢于 ID；Regular 网络在 IB 攻击策略下，其归一化网络性能下降速度比 ID、IC 快，但是其归一化攻击代价上升速度也比 ID、IC 快；ER 网络在 ID、IB、IC 攻击策略下，其归一化的网络性能 $E$ 下降速度慢于 Regular 网络，但其归一化攻击代价上升速度快于 Regular 网络。

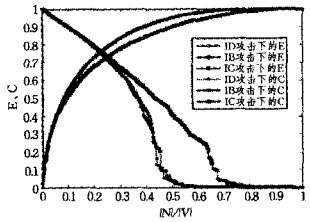

图 1　CSF 紧致无标度网络

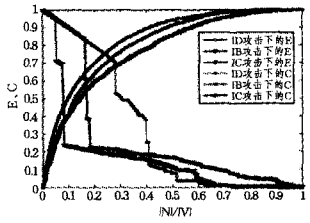

图 2　CSF 社区无标度网络

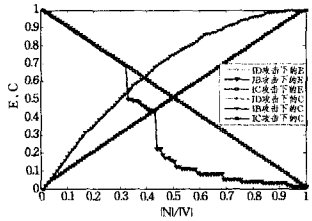

图 3　Regular 网络攻击图

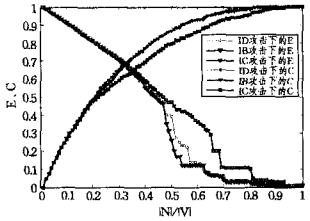

图 4　ER 网络攻击图

### 4.3　攻击代价与网络抗攻击性仿真结果及分析

为了分析代价下网络抗攻击性与所花费攻击代价间的关系，此部分给出 ID、IB、IC 攻击策略下，网络性能下降速度与攻击代价间的关系，如图 5－图 8 所示。

因为在不考虑攻击代价的情形下，全连通网络是最稳定的网络，所以，本文以代价下全连通网络在选择性攻击下 $E$-$C$ 关系线作为基准线。图中的 Baseline 表示基准线。

图中纵坐标 $E$ 表示归一化网络性能，横坐标 $C$ 表示归一化攻击代价。$E$-$C$ 关系线与 Baseline 间的意义为：在某一攻击策略下，若 $E$-$C$ 关系线大部分都在 Baseline 之上，则表示花费很大代价攻击网络，而其攻击效果却很差；若 $E$-$C$ 关系线大部分都在 Baseline 之下，则表示花费很小代价攻击网络，而其攻击效果却很好。

从图 5－图 8 可知，CSF 紧致无标度网络在 3 种攻击策略下的 $E$-$C$ 关系线 90%都在基准线之上，这表示：攻击 CSF 紧致无标度网络花费了较高的代价，却取得较差的攻击效果；CSF 社区无标度网络在 ID 下的 $E$-$C$ 关系线 90%在基准线之上，而在 IB 和 IC 的 $E$-$C$ 关系线 70%～80%都在基准线之下，这是因为该网络度与介数、度与接近度的紧致系数很小，导致出现了额外效率，使得 CSF 社区无标度网络面对介数、接近度的选择性攻击策略时，出现以较小代价使得网络快速崩溃的效果；Regular 网络在 3 种攻击策略的 $E$-$C$ 关系线均在基准线之下，这表示：攻击 Regular 网络花费较低的代价，却取得比较好的攻击效果；ER 网络在 3 种攻击策略的 $E$-$C$ 关系线有 85%在基准线之上，这表示：ER 网络花费较高攻击代价，却取得较差的攻击效果。

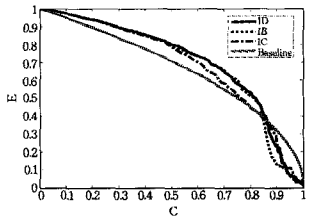

图 5　CSF 紧致无标度网络 $E$-$C$ 关系图

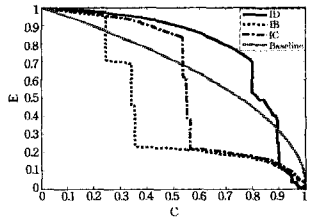

图 6　CSF 社区无标度网络 $E$-$C$ 关系图

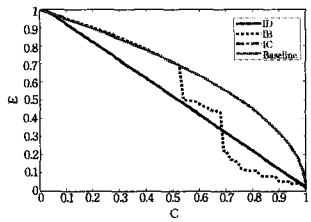

图 7　Regular 网络 $E$-$C$ 关系图

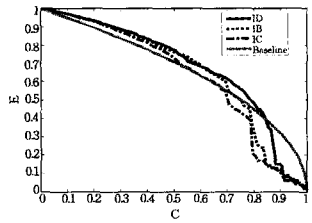

图 8　ER 网络 $E$-$C$ 关系图

为了更直观地分析网络抗攻击性与紧致系数、平均度之间的关系，根据仿真实验结果，列出网络性能和攻击的代价关系表（见表 3）。表 3 中 $E$ 表示归一化网络性能；$C$ 表示归一化攻击代价。表中左边第一列表示网络平均度分组，左边第二列表示网络类型，左边第三至五列表示：当网络性能下降到某一百分比时，3 种攻击策略分别需要花费的攻击代价。如表 3 中第二行 CSF 紧致无标度网络类型下的 $E$-$C$ 意义为：当归一化网络性能为 80%时，ID、IB、IC 攻击策略下的归一化攻击代价分别为 71.2%、70.7%、66.8%。

表 3　网络基于不同攻击策略下的 $E$-$C$ 关系

| 分组 | 网络 | E 为 80%时的 C | | | E 为 50%时的 C | | | E 为 30%时的 C | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | ID | IB | IC | ID | IB | IC | ID | IB | IC |
| 大度组 | CSF 紧致无标度网络 | 71.2% | 70.7% | 66.8% | 88.3% | 88.5% | 86.8% | 92.4% | 91.7% | 91.8% |
| | CSF 社区无标度网络 | 68.7% | 24.4% | 53.5% | 81.9% | 34.1% | 55.0% | 89.3% | 35.5% | 56.3% |
| 小度组 | ER 网络 | 50.5% | 49.5% | 48.5% | 82.0% | 83.4% | 76.7% | 87.1% | 85.8% | 89.8% |
| | Regular 网络 | 22% | 37.3% | 22% | 52% | 55.7% | 52% | 72% | 68% | 72% |

从表 3 可知：在“大度组”中，CSF 紧致无标度网络的 $E$ 为 80%时，其 $C$ 达到 66%～72%；当该网络下降到 30%时，其 $C$ 达到 90%以上。而 CSF 社区无标度网络的 $E$ 为 80%时，其在 ID 攻击下的 $C$ 达到 69%，而在 IB、IC 攻击下的 $C$ 却分别只有 25%、54%；当该网络下降到 30%时，其 ID 攻击下的 $C$ 达到 90%，而 IB、IC 攻击下的 $C$ 却分别只有 36%、57%。很明显，在 3 种攻击策略下，攻击 CSF 紧致无标度网络比 CSF 社区网络所需用的代价高很多，所以，CSF 紧致无标度网络比 CSF 社区网络的抗攻击性更强。

同理，在“小度组”中，ER 网络比 WS 网络的抗攻击性更强。

综上分析可知：CSF 紧致无标度网络的平均度与网络紧致系数均最大，所以，CSF 紧致无标度网络在 4 种网络中抗攻击性最强；Regular 网络的平均度与网络紧致系数均最小，所以，Regular 网络在 4 种网络中最脆弱。CSF 社区无标度网络的平均度较大，但其网络紧致系数却较小，因此其抗攻击性比 CSF 紧致无标度网络差；ER 网络平均度较小，但其网络紧致

（下转第 255 页）

[16] 顾亚祥,丁世飞. 支持向量机研究进展[J]. 计算机科学,2011,38(2):14-17

[17] Ren Y,Liu H,Xue C,et al. Classification study of skin sensitizers based on support vector machine and linear discriminant analysis[J]. Anal Chim Acta,2006,572(2):272-282

[18] Joachims T. Text categorization with support vector machines: learning with many relevant features[C]// Proceedings of the European conference on machine learning. Berlin:Springer,1998

[19] Nakashima H,Nishikawa K. Discrimination of intracellular and extracellular proteins using amino acid composition and residue-pair frequencies [J]. Journal of Molecular Biology,1994,238(1):54-61

[20] Chou K C, Maggiora G M. Domain structural class prediction [J]. Protein Engineering,1998,11(7):523-538

[21] Chou K C,Liu W M,Maggiora G M,et al. Prediction and classification of domain structural classes [J]. Proteins: Structure, Function and Bioinformatics,1998,31(1):97-103

[22] Baldi P,Brunak S,Chauvin Y,et al. Assessing the accuracy of prediction algorithms for classification: an overview [J]. Bioinformatics,2000,16(5):412-424

[23] 邹凌云,王正志,黄教民. 基于模糊支持向量机的膜蛋白折叠类型预测[J]. 生命科学研究,2007,11(4):306-310

[24] 李亚飞,吕强,苏伟峰,等. 一种小规模数据集下的贝叶斯网络学习方法及其应用[J]. 计算机科学,2011,38(7):181-184,234

(上接第 227 页)

系数比较大,因此其抗攻击性比 Regular 网络强。这与 3.5 节论述的平均度与紧致系数越大,则网络越鲁棒;同一平均度下网络紧致系数越大,则网络越鲁棒相符。

### 4.4 网络紧致系数、平均度与网络抗攻击性的关系

根据 3.1 节—3.5 节的理论性讨论和 4.2 节、4.3 节的仿真实验验证可知,针对不同类型网络,若平均度、网络紧致系数均比较大,则采用 ID、IB、IC 3 种攻击策略攻击网络均会花费比较高的攻击代价,且攻击效果较差;反之,则会有攻击策略以较低的攻击代价取得较好的攻击效果。其现实意义为:针对"安全系数低"的网络进行攻击,会达到事半功倍的效果。

本文在 3.2 节定性分析了网络紧致系数、平均度对网络抗攻击性的影响。图 1—图 4 表明,代价下网络面对选择性攻击时,网络性能迅速下降,且其攻击代价会迅速上升,这与现实网络遭受选择性攻击所表现的现象更为相符。图 5—图 8 和表 3 表明,代价下平均度、网络紧致系数越大,则网络越鲁棒;同一平均度下网络紧致系数越大,则网络越鲁棒。

综上所述,不同类型的网络,其平均度、网络紧致系数越大,则网络越鲁棒;同一平均度下,网络紧致系数越大,则网络越鲁棒。

**结束语** 本文在考虑攻击代价下,研究了主流的 3 类复杂网络模型——无标度网络、Regular 网络、ER 网络的抗攻击性。网络在面对多种攻击策略时,其抗攻击性可能在一种攻击策略下比较强,但是在其他攻击策略下却很弱。为了正确衡量网络整体抗攻击性,提出了度量网络鲁棒性的重要指标——网络紧致系数、平均度。进一步,为了实证网络紧致系数、平均度与网络抗攻击性间的关系,定性分析了前者与后者之间的相关关系,并通过实验实证了前者与后者间的紧密关系,进而得出结论:不同类型网络,平均度与紧致系数越大,则网络越鲁棒;同一平均度下网络紧致系数越大,则网络越鲁棒。该结论对如何提高网络的抗攻击性和防止黑客攻击有重要指导意义。

本文分别就 ID、IB、IC 3 种选择性攻击下的复杂网络抗攻击性进行了研究。然而,复杂网络面对的攻击策略众多,如 ID、IB、IC 任意两种攻击策略交替攻击复杂网络,或者 3 种攻击策略交替攻击复杂网络等,对以上攻击策略下复杂网络的抗攻击性仍需要进一步研究。我们将进一步从网络紧致系数、平均度出发,研究边攻击下网络的抗攻击性、边攻击下攻击策略的攻击强度等系列课题。

## 参 考 文 献

[1] Criado R,Garcia del Amo A. New results on computable efficiency and it's stability for complex networks[J]. Journal of Computational and Applied Mathematics,2006,192(1):59-74

[2] Wasserman S, Faust K. Social network analysis: methods and applications [D]. Cambridge University Press,1994

[3] Vazquez A, Pastor-Satorras R, Vespignani A. Large-scale topological and dynamical properties of the internet[J]. Phys. Rev. E,2002,65(6):066130

[4] Adamic L A, Huberman B A. Power-law distribution of the world wide web [J]. Science,2000,287(5461):2115

[5] Sporns O. Network analysis,complexity,and brain function[J]. Complexity,2002,8(1):56-60

[6] Lew I,Sexton,Thomas R. Network DEA: Efficiency analysis of organizations with complex internal structure[J]. Computersand Operations Research,2004,31(9):1365-1380

[7] Xia Yong-xiang. Attack Vulnerability of Complex Communication Networks[J]. IEEE Circuits and Systems,2008,55(1):65-69

[8] Schneider C M. The Robustness of Complex Networks[D]. 2011

[9] Matthew J F,Shweta B,Lauren A M. Network frailty and the geometry of herd immunity [J]. Proc Biol Sci,2006,273(1602):2743-2748

[10] Zheng Bo-jin,Huang Dan. Some scale-free networks could be robust under selective node attacks[J]. EPL,2011,94:28010-28015

[11] Wang Xiao-fan, Chen Guan-rong. Complex networks: small-world, scale-free and beyond[J]. IEEE Circuits and Systems Magazine,2003,3(1):6-20

[12] Wang Li,Yan Pei-zhou,Li Ying-hong,et al. Signal sub-control-area division of traffic complex network based on nodes importance assessment[C]// 2011 30th Control Conference. China,2011:5606-5609

[13] Holme P, Kim B J. Attack vulnerability of complex networks [J]. Phys. Rev. E,2002,65(5):1-14

[14] Repperger, Daniel W. New Results in Understanding Performance and Vulnerability in Complex Networks[C]// CIRA International Symposium. Jacksonville,Florida,U. S. A,2007