复杂加权供应链网络攻击策略和鲁棒性研究

赵志刚[1,3] 周根贵[2] 李虎雄[3]
(浙江工业大学计算机科学与技术学院 杭州 310014)[1] (浙江工业大学经贸管理学院 杭州 310014)[2]
(浙江传媒学院 杭州 310018)[3]

摘 要 文中研究在不同攻击策略下,如何提高复杂供应链网络的鲁棒性。首先,调整复杂加权供应链网络的优先连接参数,模拟实际网络的演化过程,分析供应链网络的度分布函数和介数分布函数,证实其具有无标度特征。随后,研究了加权供应链网络的多种攻击策略,统计了供应链网络的最大连通子图的相对规模和网络传输效率指标,并分析了网络的鲁棒性。仿真结果表明,对节点攻击策略而言,节点度攻击和混合攻击破坏性较大;对边攻击策略而言,双点介数攻击破坏性较大。改变网络的演化机制可以提高网络的鲁棒性,这为在实际工作中优化网络设计、保护网络中的少数重要节点和边、提高网络抗毁性能提供了一定的研究思路。

关键词 复杂加权网络,鲁棒性,节点强度,介数,攻击,K-核
中图法分类号 TP311 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.08.023

Study on Attack Strategy and Robustness of Complex Weighted Supply Chain Network

ZHAO Zhi-gang[1,3] ZHOU Gen-gui[2] LI Hu-xiong[3]
(College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China)[1]
(College of Economics and Management, Zhejiang University of Technology, Hangzhou 310014, China)[2]
(Communication University of Zhejiang, Hangzhou 310018, China)[3]

Abstract This paper studied how to improve the robustness of complex supply chain network under different attack strategies. First of all, the priority connection parameters of the complex weighted supply chain network were adjusted, the evolutionary process of the actual network was simulated, supply chain network's degree distribution function and betweenness distribution function were analyzed, and its scale-free characteristics were verified. Then, various attack strategies of weighted supply chain network were studied. The statistics on relative size of maximal connected subgraph and network efficiency index of supply chain network were conducted, and the robustness of network was analyzed. The simulation results show that the node degree attack and the blend attack are more destructive for node attack strategy, and double-point betweenness attack is more destructive for edge attack strategy. The robustness of network can be improved by changing network's evolution mechanism, which provides certain research thoughts on how to optimize network design, protect few important nodes and edges in the network and improve network invulnerability in practical works.

Keywords Complex weighted network, Robustness, Node strength, Betweenness, Attack, K-core

1 引言

供应链系统运行过程中存在着不确定性,如内部的交易关系中断及外部的交通事故等因素会破坏供应链网络的结构,影响网络的性能。在不确定因素的作用下,鲁棒性成为供应链持续稳定运行的重要因素。现实世界中的许多复杂系统都具有鲁棒性,即对故障呈现出抗毁能力[1]。发现和保护复杂供应链网络中的重要节点和边,可帮助提高网络的安全性能,对提高网络的结构稳定性和抗毁性具有重要作用[2]。

复杂供应链网络的早期研究主要集中在无权网络,无权网络仅体现出节点间有无连接的概况。但在很多实际网络中,各个节点间具有不同的权值,或者说耦合的强度不同:如在科研合作网络中,各个研究者(节点)间合作的论文数量(连接权值)不同;在航空、铁路、公路网络中,各个节点间的客流量不同;在社交网络中,人与人的关系紧密程度也不同。而在供应链网络中,既要考虑网络拓扑结构又要考虑节点间的相互贸易关系。因此,加权网络更能描述节点间的紧密程度,能更真实地表达网络的结构[3]。

到稿日期:2018-06-04 返修日期:2018-10-29 本文受国家自然科学基金(U1509220),"计算机科学与技术"一流学科(Z511B17503),浙江省基础公益研究计划项目(LGG18F030003),浙江传媒学院第14批教学改革项目(jgxm201929)资助。
赵志刚(1976-),男,博士生,副教授,CCF会员,主要研究方向为复杂网络系统,E-mail:zhaozhig2006@126.com;**周根贵**(1958-),男,博士,教授,博士生导师,主要研究方向为人工智能、供应链网络分析,E-mail:ggzhou@zjut.edu.cn(通信作者);**李虎雄**(1971-),男,博士,教授,主要研究方向为模式识别。

近年来，科研人员已广泛研究了复杂供应链网络的鲁棒性和抗毁性。Monostori[4] 分析了供应链系统的静态鲁棒性和动态鲁棒性，提出了一些缓解风险的策略及衡量供应链网络鲁棒性优劣的框架，但它们仅仅停留在理论层面上。柳虹等[5] 把供应链网络节点的介数作为攻击的测度，研究节点失效的传递攻击策略，分析攻击发生时网络性能的变化情况，并给出了一些解决的建议，但没进行详细的仿真实验来验证解决方案。Nie 等[6] 使用 4 种策略对小世界网络和无标度网络进行攻击，研究度与介数在攻击过程中的动态关系，发现在无标度网络中二者之间遵守幂率分布关系直到网络崩溃，但未对网络进行加权。张怡等[7] 基于度和距离因素构建了复杂供应链网络，并根据参数的变化讨论了反映鲁棒性指标的网络效率和最大连通子图的相对大小，并指出改变网络拓扑结构可提高网络的鲁棒性，但对鲁棒性进行研究时，仅进行供应节点的破坏，没有考虑边的断裂因素。Fu 等[8] 在不完全信息情况下，结合级联失效的理论，研究了对多个节点的攻击策略。发现被攻击节点之间的距离对攻击效果有较大的影响，但是没有涉及到对网络结构的调整。

常见的加权模型有 BBV 模型，其新节点按照已有节点的点强度强弱优先连接老节点。而在 DM 模型中，其新节点按照网络中已有连边的边权选择优先连接老节点[9]。以上两种模型都是受到 BA 网络的启发设计的。在实际供应链网络的运行过程中，新企业加入供应链寻求合作伙伴时，往往倾向于选择实力较强的企业。因此，可以在 BA 网络的基础上，考虑选择节点能力强的企业（可综合交易数目多的、交易量大的和位置近的节点）进行优先连接。网络中有增加连接的情况，也有删除联系的情况。企业某个时期因为生产停滞、倒闭等原因也可能退出网络，与之有供需关系的节点将不再与之连接，或者企业在一段时间内没有迫切的交易需求，都会删除与这些企业节点间的连接关系。此外，新节点和老节点间的交易量也应随着网络规模的增加而动态变化，这才能符合实际供应链的运营情况。

然而，在以上复杂供应链网络鲁棒性的研究中，构建的网络模型多以随机网络和单纯的 BA 网络为主。构建的网络的过程也没有反映出现实加权供应链网络的节点间交易、节点退出和边断裂等动态演化过程，对复杂加权供应链网络的攻击策略和网络结构鲁棒性研究得不够深入。本文将节点度（所有与节点直接相连的边数）、节点强度（节点的所有连边的权值的和）作为节点优先连接概率，同时还考虑了节点之间的空间距离，构建成供应链网络。通过调整模型中的参数，改变模型的演化机制，构建更加贴近现实供应链运行情况且有交易量的加权供应链网络，并在此基础上研究了攻击策略和鲁棒性，这对合理设计供应链网络，提高其抗毁性有重要的理论价值和现实意义。

2　复杂网络的统计特征及鲁棒性标准

从复杂网络中删除一定的节点或边可以等效为网络遭受到攻击，因此可以用攻击后最大连通分支节点数与网络总结点数之比来度量网络的鲁棒性。网络的平均路径长度与移除节点（或移除边）的关系能够反映网络遭受攻击后网络的运营效率，同样能度量网络的鲁棒性。因此，可用以下指标进行复杂网络的鲁棒性研究和度量。

2.1　统计特征

节点的度指与该节点连接的边的条数。

平均路径长度：加权网络中两个节点间的距离即为两个节点间的最短路径上的边权值之和。任意两个不同节点之间距离的平均值则为加权网络的平均路径长度。

介数体现的是节点或边的重要程度。节点 u 的介数是网络中经过节点 u 的最短路径占所有最短路径的比重。记 (i,j) 之间的最短路径的集合为 g_{ij}，则节点 u 的介数定义为：

$$B_u=\sum_{(i,j)}\frac{g_{iuj}}{g_{ij}},i,j\neq u,i\neq j \tag{1}$$

边 l_{mn} 的介数的计算公式为：

$$Bmn=\sum_{(i,j)}\frac{g_{imnj}}{g_{ij}},i,j\neq m,i,j\neq n,i\neq j \tag{2}$$

其中，g_{imnj} 为经过边 l_{mn} 的节点 i 与节点 j 之间的最短路径的数目。

2.2　鲁棒性衡量标准

（1）最大连通子图的相对大小 R

当对网络的节点和边进行攻击后，网络的结构和运输效率会发生改变，因此可使用网络效率和最大连通子图的相对规模反映网络发生意外时的鲁棒性[10]：

$$R=\frac{s}{S} \tag{3}$$

其中，s 是网络遭受攻击后网络的最大连通子图的节点数目，S 指原始网络的节点数目。

（2）网络效率

网络效率是网络在某时段内能够正常运转并发挥功效的程度，可刻画出网络传递信息的效率。计算全网效率的方法如下：

$$\eta_E=\frac{1}{n(n-1)}\sum_{j\neq i\in G}\frac{1}{d_{ij}} \tag{4}$$

由式(4)可知，信息传递的路程越长，传输距离 d_{ij} 越大，传播过程消耗的时间越长，网络的传输效率越低；反之，网络传输效率越高。

3　复杂供应链网络模型

供应链在正常运行过程中通常会受到干扰，之后一般会出现两种情况：1）节点企业因为生产停滞和企业倒闭等原因无法适应供应链运作，会断开与其他节点的连接，在网络中体现为去点；2）因运输路线中断和无交易要求等原因无法与其他节点发生联系，在网络中体现为去边。为反映复杂供应链网络的动态变化过程，本文设计和使用了相应的模型和演化规则。

复杂供应链网络可抽象为由点集 V 和边集 E 组成的图 $G=(V,E)$。为每条边都赋予相应的权值，该网络即为加权网络。一个具有 N 个点的网络可用一个 $N\times N$ 阶矩阵 $\boldsymbol{A}(G)$ 表示。加权网络 $\boldsymbol{A}$ 的矩阵元素 A_{ij} 代表企业 i 和企业 j 之间的贸易情况。网络演化算法的步骤如下[11-12]：

步骤 1（供应链网络初始化）　在初始状态下 $t=0$，生成 m_0 个初始节点，节点企业之间的边连接即交易量 $A_{ij}\in[0,1]$ 随机生成。预先设定边断裂阈值 P_0，若 $A_{ij}<P_0$，则节点 i 与节点 j 之间失去了联系，此时度为 0 的节点退出供应链网络。

步骤 2（择优增长）　在时刻 t，新增一个节点 j。新节点 j

选择原网络中 M 个空间距离与之较近的不同老节点作为其局域世界，然后再从局域世界中选择 m 个节点进行优先连接，从而生成边。优先连接的概率为：

$$\Pi(j->i)=a*k_i/\sum k_j+b*s_i/\sum s_j \quad (5)$$

其中，k_i 为节点 i 的度，s_i 为节点 i 的强度，$s_i=\sum A_{ij}$，此概率体现了网络中的节点的重要程度。$b=1-a$，且 $a>0$，$b>0$。对新加入网络的具有交易关系的节点，随机生成节点间的新的交易量边 $A_{ij}\in[0,1]$。

步骤 3(去点) 供应链网络更新后，度为 0 的节点因缺乏交易伙伴将退出供应链网络。

步骤 4(断边) 对加入新节点和边后的网络，如节点 i 与节点 j 间的交易量值 $A_{ij}<P_0$，则节点 i 与节点 j 之间联系中断。

步骤 5(循环) 返回步骤 2，直至供应链网络到达预期的节点规模 N 为止。以上过程中可先设定 m_0，m，P_0，M 和 N 的值。

4 实验仿真及分析

本文根据对演化模型的仿真发现了实际供应链网络的特性，通过研究仿真网络的鲁棒性对重要节点和重要边进行识别，并对其加以保护，以提高复杂供应链网络的抗毁性。

4.1 分布函数

本文在 Matlab2014b 的环境下进行仿真。$P(K)$ 表示节点度的概率分布函数，其指度为 k 的节点在网络中存在的概率。本文模型中，取初始节点数 $m_0=10$，每次进入网络的新节点与原有网络中的两个老节点连边，即连边数 $m=2$，边断裂门限值 $P_0=0.1$，网络规模 $N=1000$，模型参数暂取均衡值 $a=b=0.5$。经过仿真可得到如图 1 所示的节点度的分布图。

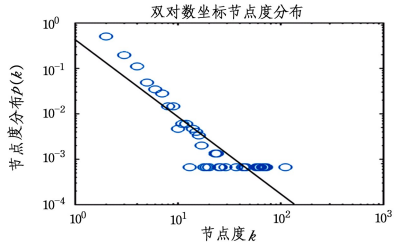

图 1 模型节点度的分布图

Fig. 1 Distribution diagram of model node degree

由图 1 可知，本模型的度分布呈现出较为明显的幂率分布。绝大多数节点的度较低，只有少数节点的度较高。图 2 为节点介数的分布情况，由图 2 可知，模型的介数分布大致也呈现幂率分布趋势，介数大的节点的数目也不多。

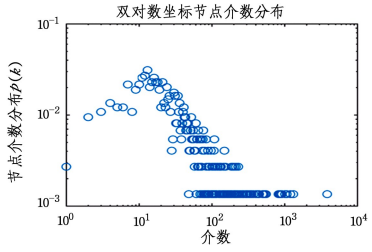

图 2 模型节点介数的分布图

Fig. 2 Distribution diagram of model node betweenness

4.2 鲁棒性分析

4.2.1 节点攻击策略

为研究加权供应链网络的鲁棒性，可从节点攻击和边攻击两个方面进行研究[13-14]。对节点的攻击按照以下几种方式进行，攻击算法的思想分别为：

(1)随机删除节点；

(2)按节点度从大到小排序，删除节点；

(3)按节点介数从大到小排序，删除节点；

(4)按节点度数 50%和介数 50%的值加权后，从大到小排序，删除节点；

(5)按节点强度从大到小排序，删除节点；

(6)按 K-核强度从大到小排序，删除节点。

本文以节点的混合攻击为例来阐述的算法的步骤，其他节点攻击策略的思路与之类似，只是会因统计节点的参数的不同而不同：

步骤 1 根据本文的复杂供应链网络演化机制，得到初始网络 $G=(V,E)$；

步骤 2 计算网络 $G=(V,E)$ 的各个节点的介数 $B_i(i=1,2,\cdots,n)$ 和度数 K_i，以及网络中所有节点的混合攻击参数 $H_i=B_i*0.5+K_i*0.5$；

步骤 3 将 H_i 按降序排列后，将混合攻击参数值对应的最大值的节点去掉，如果此时有多个节点的 H_i 值相同，则删除所有值最大的节点；

步骤 4 计算最大连通子图的相对大小和网络效率两个指标的值，如果其中一个指标的值为零，则结束算法，否则跳转步骤 2。

经编程计算得到的图 3 是最大连通子图的相对大小(子图规模)与节点删除比例的关系图，图 4 是网络效率与节点删除比例的关系图。由图 3 与图 4 可知，随着网络节点删除数目的增加，随机攻击和点强度攻击对网络的破坏性较弱，而节点度攻击和混合攻击对网络的破坏力较强。

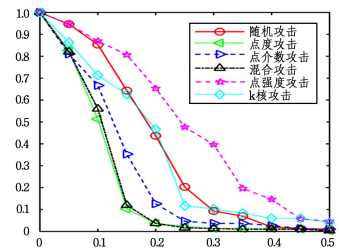

图 3 不同攻击下最大连通子图的相对大小与节点删除比例的关系

Fig. 3 Relation between maximal connected subgraph relative size and node deletion ratio under different attack

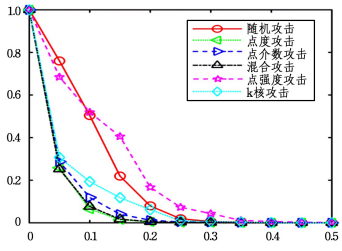

图 4 不同攻击下网络效率与节点删除比例的关系

Fig. 4 Relation between network efficiency and node deletion ratio under different attack

图 5 和图 6 是在不同优先连接概率参数 a，b 下，随机攻击在节点按比例删除的情况下网络的鲁棒性关系图。从图中可以看出，在大多数情况下，$a=1$，$b=0$ 时网络对攻击的鲁棒性较强。且 a 值越大，即优先连接概率中节点度的占比越大，网络对随机攻击的鲁棒性越强，体现出典型 BA 无标度网络对随机攻击较强的鲁棒性。

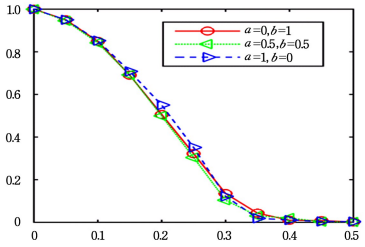

图 5　随机攻击下不同参数网络的最大连通子图的相对大小

Fig. 5　Relative size of maximal connected subgraph of different parameter network under random attack

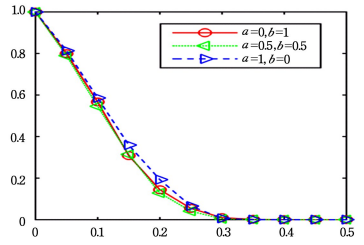

图 6　随机攻击下不同参数网络的网络效率

Fig. 6　Network efficiency of different parameter network under random attack

图 7 与图 8 为度攻击下不同参数网络的最大连通子图相对大小和网络效率。从图中可以看出，$a=1$，$b=0$ 时攻击对网络的破坏力较强，因为此时优先连接概率完全由节点的度决定，其网络效率较低。相比而言，$a=0.5$，$b=0.5$ 时对应的网络的鲁棒性较好。

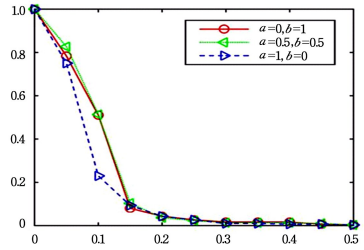

图 7　度攻击下不同参数网络的最大连通子图的相对大小

Fig. 7　Relative size of maximal connected subgraph of different parameter network under degree attack

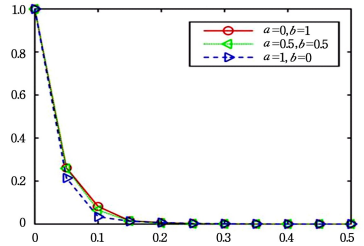

图 8　度攻击下不同参数网络的网络效率

Fig. 8　Network efficiency of different parameter network under degree attack

图 9 与图 10 为介数攻击下不同参数网络的最大连通子图的相对大小和网络效率。从图中可以看出，$a=1$ 与 $b=0$ 时攻击对网络的破坏力较强，网络效率较低。相比而言，$a=0.5$，$b=0.5$ 时对应的网络的鲁棒性较好。

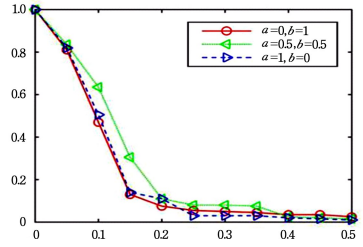

图 9　介数攻击下不同参数网络的最大连通子图的相对大小

Fig. 9　Relative size of maximal connected subgraph of different parameter network under betweenness attack

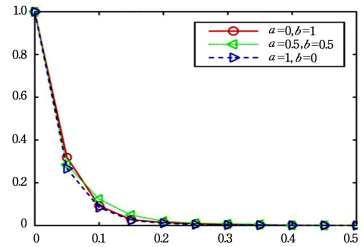

图 10　介数攻击下不同参数网络的网络效率

Fig. 10　Network efficiency of different parameter network under betweenness attack

图 11 与图 12 是混合攻击下不同参数网络的最大连通子图的相对大小和网络效率。从图中可以看出，$a=1$，$b=0$ 时攻击对网络的破坏力较强，网络效率也较低。相比而言，$a=0.5$，$b=0.5$ 时对应的网络的鲁棒性较好。但由图 3 和图 4 可知，本文提出的融合了节点度和节点介数的混合攻击策略对网络的破坏程度还是相当大的。

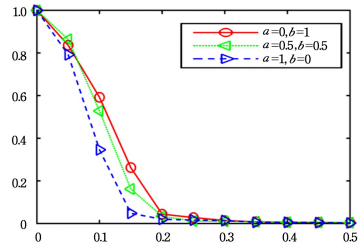

图 11　混合攻击下不同参数网络最大连通子图相对大小

Fig. 11　Relative size of maximal connected subgraph of different parameter network under blend attack

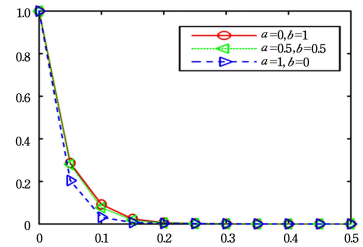

图 12　混合攻击下不同参数网络的网络效率

Fig. 12　Network efficiency of different parameter network under blend attack

实验仿真中，节点攻击算法的思想是基于节点的度和介数这两种中心性度量的，其中节点度攻击是基于网络局域属性的指标，节点介数攻击是基于网络全局属性的指标。由于各种复杂加权网络模型的演化机制和参数不尽相同，因此本文在此比较同一演化机制下两种不同参数网络结构的鲁棒性。在图 7－图 12 中，当 $a=1,b=0$ 时，节点优先连接概率完全由度指标衡量，网络即为相同演化机制下，在 BA 网络的基础上进行加权的网络结构。从这 6 个图中可以看出，本文的加权网络结构（$a=0.5,b=0.5$）在大多数情况下无论是从最大连通子图的相对大小还是从网络效率方面，都要好于相同演化机制下在 BA 网络基础上进行加权的网络结构（$a=1,b=0$）。这种现象也在下文各种节点攻击策略中得到了体现。图 13 与图 14 是点强度攻击下不同参数网络的最大连通子图的相对大小和网络效率。从图中可以看出，大多数情况下参数组合为 $a=0,b=1$ 时，攻击对网络的破坏力较强，因为此时优先连接概率完全由节点强度决定，其网络效率也较低。相比而言，$a=0.5,b=0.5$ 的参数组合以及 $a=1,b=0$ 的参数组合所对应的网络鲁棒性差别不大，但都比 $a=0,b=1$ 的参数组合好。

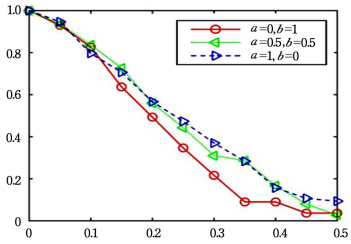

图 13 点强度攻击下不同参数网络的最大连通子图的相对大小

Fig. 13 Relative size of maximal connected subgraph of different parameter network under node strength attack

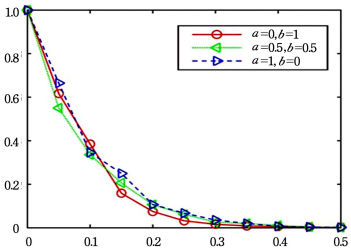

图 14 点强度攻击下不同参数网络的网络效率

Fig. 14 Network efficiency of different parameter network under node strength attack

图 15 与图 16 为 K-核攻击下不同参数网络的最大连通子图的相对大小和网络效率。

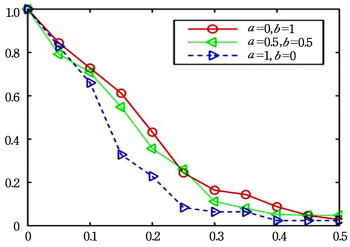

图 15 K-核攻击下不同参数网络最大连通子图相对大小

Fig. 15 Relative size of maximal connected subgraph of different parameter network under K-core attack

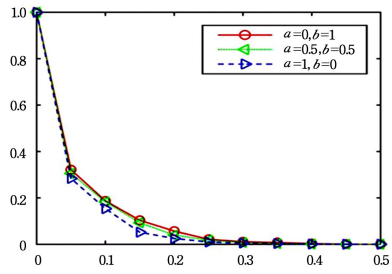

图 16 K-核攻击下不同参数网络的网络效率

Fig. 16 Network efficiency of different parameter network under K-core attack

从图中可以看出，大多数情况下，$a=1,b=0$ 的参数组合下攻击对网络的破坏力较强。相比而言，$a=0.5,b=0.5$ 的参数组合以及 $a=0,b=1$ 的参数组合对应的网络的鲁棒性能差别不大，但都比 $a=1,b=0$ 参数组合的情况好。

4.2.2 边攻击策略

本文从以下几种形式来研究复杂供应链网络的边攻击策略[15-16]，攻击方式的思想分别是：

（1）边介数攻击边，对边介数从大到小排序后，然后按序删除边；

（2）双点介数攻击边，对边的两个端点的介数的乘积从大到小排序，然后按序删除边；

（3）边度攻击边，对边的两个端点的度的乘积从大到小排序，然后按序删除边；

（4）双点 K-核强度攻击边，对边的两个端点对应的 K-核强度的乘积从大到小排序，然后按序删除边。

本文以双点介数攻击为例来阐述算法的步骤，其他边攻击策略的思路与之类似，它们只会因统计边的两个端节点的参数的不同而不同。

步骤 1 根据本文的复杂供应链网络演化机制得到初始网络 $G=(V,E)$；

步骤 2 计算网络 $G=(V,E)$ 中各个节点的介数 B_u（$u=1,2,\cdots,n$），以及网络中所有有直接连边的双点介数乘积 $B_{ij}=B_i * B_j$；

步骤 3 将 B_{ij} 降序排列后，将双点介数乘积值对应的最大值的边去掉，如果此时有多条边的 B_{ij} 值相同且有多个时，删除所有的值最大的边；

步骤 4 计算最大连通子图的相对大小和网络效率两个指标的值，如果其中一个指标的值为零，则结束算法，否则跳转步骤 2。

经编程计算得到的图 17 是最大连通子图的相对大小（子图规模）与边删除比例的关系图；图 18 是网络效率与边删除比例的关系图。由图 17 与图 18 可知，随着网络边删除数目的增加，双点介数攻击对网络的破坏力较强。相比图 3 和图 4，从破坏性的强度方面进行对比发现，节点攻击对网络的破坏程度要大于边攻击对网络的破坏程度。按节点的度数进行攻击时，当攻击到 15％左右的节点时，网络传输效率就基本瘫痪；按双点介数攻击时，当攻击到 50％左右的边时，网络传输效率才瘫痪至 28％左右。这是因为当在网络中删除一个节点时，与这个节点相连的所有边都将被破坏；而在网络中

删除一条边时，与这条边相关联的节点并不会被同时删除。只有当与某个节点相连的所有边都删除时，这个节点才算真正删除。

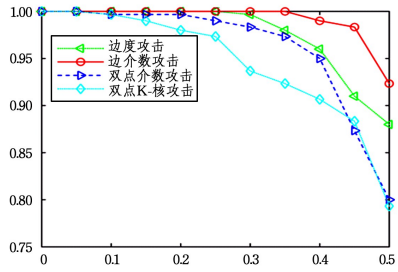

图 17　不同攻击下最大连通子图的相对大小与边删除比例的关系

Fig. 17　Relation between maximal connected subgraph relative size and edge deletion ratio under different attack

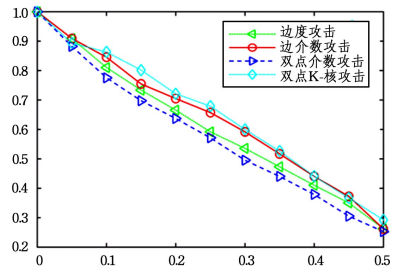

图 18　不同攻击下网络效率与边删除比例的关系

Fig. 18　Relation between network efficiency and edge deletion ratio under different attack

图 19 与图 20 是边介数攻击下不同参数网络的最大连通子图的相对大小和网络效率。从图中可以看出，大多数情况下，$a=0$，$b=1$ 的参数组合下攻击对网络的破坏力较强。相比较而言，$a=0.5$，$b=0.5$ 的参数组合的网络效率更优。

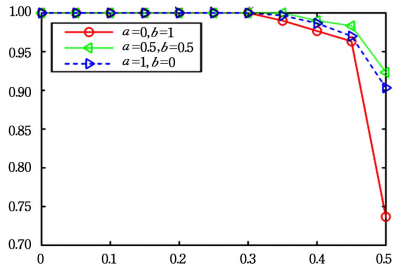

图 19　边介数攻击下不同参数网络最大连通子图的相对大小

Fig. 19　Relative size of maximal connected subgraph of different parameter network under edge-betweenness attack

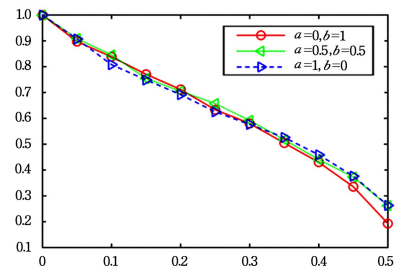

图 20　边介数攻击下不同参数网络的网络效率

Fig. 20　Network efficiency of different parameter network under edge-betweenness attack

与此类似，通过编程发现，对于边的其他攻击方式，如双点介数攻击、边度攻击和双点 K-核攻击的网络鲁棒性也有相似的规律。即大多数情况下，当 $a=0.5$，$b=0.5$ 时，网络效率更好。

结束语　本文研究了加权供应链网络的演化模型，从而改进了 BA 模型的连接机制，把节点度和节点强度共同作为新加入供应链网络节点的优先选择概率，发现该参数可变模型具有无标度网络的特征。基于复杂网络理论中的几个重要鲁棒性能指标对该模型的复杂供应链网络进行了攻击策略方面的研究。通过基于节点删除的随机攻击、度攻击、介数攻击、混合攻击和 K-核攻击，以及对基于边删除的边介数攻击、双点介数攻击、边度攻击和双点 K-核攻击等多种方式进行仿真分析，从最大连通子图的相对大小（子图规模）和网络效率两个测度研究了网络的鲁棒性。

由实验结果可得出以下结论：1）该模型的度分布和介数分布呈现出较为明显的幂率分布形式，体现出无标度网络特征；2）当参数 a 和 b 的值确定时，例如 $a=b=0.5$ 时，网络在随机攻击下表现出较强的鲁棒性，对于蓄意攻击（特别是针对点破坏性较强的节点度攻击及混合攻击和针对边破坏性较强的双点介数攻击），网络的鲁棒性较差，这是由网络拓扑结构对网络负荷分配的异质性引起的；3）从破坏性最强方面对比，发现节点攻击对网络的破坏程度要大于边攻击对网络的破坏程度，按点度攻击时，当攻击到 15%左右的节点时，网络传输效率基本全部瘫痪，按双点介数攻击时，当攻击到 50%左右的边时，网络传输效率仅部分瘫痪；4）对于不确定的优先概率，选择参数 a、b 不同组合下的值，发现多数攻击情况下，当 $a=1$，$b=0$ 时，攻击对供应链网络的破坏力较强，因此仅以度为优先连接概率构建的 BA 模型的鲁棒性不佳，应改变其优先连接概率。本文综合考虑节点度比重 a 和节点强度的比重 b 作为节点的复合优先连接概率是合理的，可以提高网络的鲁棒性，通过实验发现大多数情况下当 $a=0.5$，$b=0.5$ 时，网络的鲁棒性较好。

通过对网络攻击策略的研究可识别出复杂供应链网络中的重要节点和关键供应关系，可考虑通过增加网络中重要节点的冗余备份以保护关键节点，而节点之间可以通过增加边的方式结成区域联盟以保护关键边的手段，来提高网络的鲁棒性，以便更好地保护网络。

下一步将重点研究复杂供应链网络在动态变化过程中的重要节点的优先识别、级联失效的负载均衡和牵制控制等问题。

参 考 文 献

[1]　JI X P, WANG B, LIU D C, et al. Improving interdependent networks robustness by adding connectivity links[J]. Physica A: Statistical Mechanics and its Applications, 2016, 444: 9-19.

[2]　RUAN Y R, LAO S Y, WANG J D, et al. Algorithm of Significance Evaluation of Complex Network Nodes Based on Neighborhood Similarity[J]. Chinese Journal of Physics, 2017, 66(3): 365-373. (in Chinese)

阮逸润,老松杨,王竣德,等.基于邻域相似度的复杂网络节点重要度评估算法[J].物理学报,2017,66(3):365-373.

[3] ZHOU J,PAN J X,CHENG K Q. Research on BBV Network Model Evolution Based on New Local World[J]. Computer Engineering,2010,36(19):266-268. (in Chinese)
周健,潘家鑫,程克勤.基于新局域世界的 BBV 网络模型演化研究[J].计算机工程,2010,36(19):266-268.

[4] MONOSTORI J. Supply Chains' Robustness:Challenges and Opportunities[J]. Procedia CIRP,2018,67:110-115.

[5] LIU H,ZHOU G G,FU P H,et al. Research on Delivery Attack Strategy Based on Supply Chain Network[J]. Computer Science,2013,40(7):98-101. (in Chinese)
柳虹,周根贵,傅培华,等.基于供应链网络的传递攻击策略研究[J].计算机科学,2013,40(7):98-101.

[6] NIE T Y,GUO Z,ZHAO K,et al. The dynamic correlation between degree and betweenness of complex network under attack[J]. Physica A:Statistical Mechanics and its Applications,2016,457:129-137.

[7] ZHANG Y,XIONG J,FENG C. Analysis on Robustness of Supply Chain NetworkBased on Complex Network[J]. Computer Simulation,2012,29(11):370-373. (in Chinese)
张怡,熊杰,冯春.基于复杂网络的供应链网络鲁棒性分析[J].计算机仿真,2012,29(11):370-373.

[8] FU C Q,WANG Y,WANG X Y,et al. Multi-node attack strategy of complex networks due to cascading breakdown[J]. Chaos,Solitons and Fractals,2018,106:61-66.

[9] WANG X. Research on Agri-food Supply Chain Modeling and Network Risk Propagation Based on Complex Network [D]. Changchun:Jilin University,2017. (in Chinese)
王杏.基于复杂网络的农产品供应链建模与网络风险传播研究[D].长春:吉林大学,2017.

[10] MAO K. Research on Stability and Robustness of Complex Network Structure[J]. Computer Science,2015,42(4):85-88. (in Chinese)
毛凯.复杂网络结构的稳定性与鲁棒性研究[J].计算机科学,2015,42(4):85-88.

[11] CAO W B,XIONG X. Local Evolution Mechanism of Complex Supply Chain Network Based on Edge Benefit [J]. Computer Application Research,2016,33(1):75-77. (in Chinese)
曹文彬,熊曦.边效益因素下复杂供应链网络局域演化机制[J].计算机应用研究,2016,33(1):75-77.

[12] LIU H,ZHOU G G,FU P H. Local Evolution Model Research of Layered Supply Chains Complex Networks [J]. Computer Science,2013,40(2):270-273. (in Chinese)
柳虹,周根贵,傅培华.分层供应链复杂网络局部演化模型研究[J].计算机科学,2013,40(2):270-273.

[13] BELLINGERI M,CASSI D. Robustness of weighted networks[J]. Physica A:Statistical Mechanics and its Applications,2018,489:47-55.

[14] LIN J H,GUO Q,DONG W Z,et al. Identifying the Node Spreading Influence with Largest K-core Values[J]. Physics Letters A,2014,378(45):3279-3284.

[15] SAITO K,KIMURA M,OHARA K,et al. Super mediator-A New Centrality Measure of Node Importance for Information Diffusion Over Social Network[J]. Information Sciences,2016,329(C):985-1000.

[16] SUN L S,HUANG Y C,CHEN Y Y,et al. Vulnerability Assessment of Urban Railtransit Based on Multi-static Weighted Method in Beijing [J]. Transportation Research Part A:Policy and Practice,2018,108:12-24.