有向加权供应链网络级联失效的抗毁性研究

崔慧霞[1,2], 邱建龙[1†], 郭 明[1], 张润发[1,2]

(1. 临沂大学 自动化与电气工程学院, 山东 临沂 276005; 2. 曲阜师范大学 工学院, 山东 日照 276800)

摘要: 供应链网络是一个高度复杂的有向加权网络, 研究供应链网络本身的抗毁性对改良供应链网络拓扑结构, 提高网络稳定性和鲁棒性有着至关重要的意义. 因此本文依据复杂供应链网络中不同的网络攻击方式导致的节点或者连边级联失效现象, 提出了一项在有向加权供应链网络下的抗毁性标准. 在提出的抗毁性准则中, 本文引入了“网络运营度”的概念, 并针对有向加权网络的几种级联失效现象下的“网络运营度”的理论机理进行阐述, 最后通过实验证明该抗毁性准则相对于其他文章所提出的抗毁性准则有着相对较好的表现, 证实了本文提出的抗毁性测度的有效性.

关键词: 有向加权网络; 级联失效; 抗毁性; 供应链网络

引用格式: 崔慧霞, 邱建龙, 郭明, 等. 有向加权供应链网络级联失效的抗毁性研究. 控制理论与应用, 2021, 38(11): 1828 – 1834

DOI: 10.7641/CTA.2021.10792

Research on invulnerability of cascading failures in directed weighted supply chain networks

CUI Hui-xia[1,2], QIU Jian-long[1†], GUO Ming[1], ZHANG Run-fa[1,2]

(1. School of Automation and Electrical Engineering, Linyi University, Linyi Shandong 276005, China;
2. School of engineering, Qufu Normal University, Rizhao Shandong 276800, China)

Abstract: Supply chain network is a highly complex directed weighted network. Studying the invulnerability of supply chain network is of great significance to improve the topology of supply chain network and the stability and robustness of the network. Therefore, based on the phenomenon of node or edge cascading failure caused by different network attack modes in complex supply chain networks, this paper proposes a criterion of invulnerability in directed weighted supply chain networks. In the proposed invulnerability criterion, we introduce the concept of “network operation degree”, and elaborate the theoretical mechanism of “network operability” under several cascading failures of directed weighted networks. Finally, experiments show that the invulnerability criterion has a relatively good performance compared with the invulnerability criteria proposed in other papers, which proves the effectiveness of the invulnerability measure proposed in this paper.

Key words: directed weighted network; cascading failure; invulnerability; supply chain network

Citation: CUI Huixia, QIU Jianlong, GUO Ming, et al. Research on survivability of cascading failures in directed weighted supply chain networks. *Control Theory & Applications*, 2021, 38(11): 1828 – 1834

1 引言

随着现代生活水平的提高, 人们对货物的需求已经不单单局限于本区域, 而是全中国区域、甚至是全世界, 这也就促生了物流行业的产生. 货物运转以物流网络为支撑, 形成了一个庞大的物流供应链网络, 该网络属于复杂网络的一种. 物流网络承担着运输需求货物的任务, 且建设费用巨大, 一旦道路发生故障或者是运输站点出现故障, 则会对供应链网络的正常运作造成影响. 这会导致局部物流网络的瘫痪, 甚至是威胁到整个物流网络的连通性和能控性, 造成物流网络大规模瘫痪, 因此提高物流供应链网络的抗毁性能成为广大学者研究的热点话题. 随着复杂网络科

收稿日期: 2021−08−25; 录用日期: 2021−10−28.

†通信作者. E-mail: qiujianlong@lyu.edu.cn; Tel.: +86 15653971177.

本文责任编委: 洪奕光.

国家自然科学基金项目(61877033, 61833005, 61903170, 62173175), 山东省自然科学基金项目(ZR2019BF045, ZR2019MF021, ZR2019QF004), 山东省高等学校青年创新团队发展计划项目资助.

Supported by the National Natural Science Foundation of China (61877033, 61833005, 61903170, 62173175), the Natural Science Foundation of Shandong Province (ZR2019BF045, ZR2019MF021, ZR2019QF004) and the Youth Innovation Team Development Program of colleges and universities in Shandong Province.

学[1]的发展, 人们对于物流网络结构认知也越来越深刻, 复杂网络理论成为研究物流网络稳定性、能控性、鲁棒性的重要手段之一.

复杂网络本身都有一定的容错性[2]、抗毁性[3]、鲁棒性, 物流网络结构也有相应的抗毁性[4]. 这表示物流网络的结构在面对未知的攻击时(该攻击可以体现为某条路线突发事故导致的线路不通, 或者是某物流节点遭受破坏无法承担职责)也能保持良好的连通性[5]和能控性[6]. 连通性是指的是即使物流网络上的某些线路不通顺, 也可以通过其他线路到达原定节点, 这就是连通鲁棒性. 而能控性则是表现在物流网路中的某些节点或者是某些线路遭受到破坏, 其余网络部分依旧通过可连通线路和节点在控制节点的控制之下. 延迟物流网络的瘫痪, 为后续补救建设争取时间, 这就是能控性鲁棒性.

近几年基于复杂网络理论对物流网络的分析的研究越来越多, 例如: 杨等人[7]基于复杂网络理论知识, 对城市轨道交通网络特性进行研究, 构建URTN拓扑结构, 并建立了级联失效模型, 使用网络效率和最大连通子图的比例作为鲁棒性评价指标进行分析. Wang等人[8]研究了在不同复杂网络模型和不同的鲁棒性能评价指标下, 考虑攻击代价的网络鲁棒性问题, 并对鲁棒性能变化过程进行分析. Shi等人[9]针对无向供应链网络进行混合级联故障的分析, 并提出一个可调参数的供应链网络, 分析了网络模型中可调参数对随机和蓄意攻击的鲁棒性能. Yang等人[10]从网络蓄意攻击的角度上研究了网络的可控性鲁棒性, 提出了一种分层攻击框架, 并设计了相应实验, 在实验的结构上提出有利于网络可控性鲁棒性的建议.

通过上述文献, 可得看出研究者在研究物流网络的时候都会考虑物流网络模型的鲁棒性能. 而鲁棒性能的研究必须要考虑网络的抗毁性能, 所以本文针对有向加权的供应链的抗毁性测度展开了研究. 物流供应链网络是一个开放的复杂巨系统, 不单单是节点性质不同, 网络中的连边的权重也是不同的, 该网络本身是一个有向网络. 总的来说物流供应链网络是一个有向加权网络, 本文需要对供应链网络的拓扑结构研究. 通过对节点之间的有向连边关系的研究, 通过不同的网络攻击方式对其进行攻击, 通过考虑攻击节点和连边级联失效效应[11], 从相应的抗毁性曲线结果上得出相应的结构优化结论.

本文根据供应链网络攻击, 网络中节点和连边的级联失效的演化过程, 提出了一个新的抗毁性标准, 该标准考虑到连边的有效性.

2　复杂物流网络鲁棒性分析

2.1　物流供应链网络拓扑结构

物流供应链网络是将供应商、多级配送中心和需求点看作是网络节点, 这些节点不能以单一的节点形式表示, 必须给与区分, 在本文由于研究的是网络拓扑结构的抗毁性测度, 节点的类型大体可以从节点的出度和入度进行判断, 因此可以将节点看作是相同的类别. 将供应链中的货物流、信息流等看作是网络的连边(本文中只考虑货物流), 节点没有自环, 且连边的权重也是不同的, 本文的权重取决于连边两边的节点的度值, 由文献[12]可知, 加权网络连边的权值可以表示为$W_{ij} = a_{ij} * (k_i * k_j)^{\theta}$, 其中$a_{ij}$代表的是节点$i$和$j$之间是否有连边, 节点$i$和$j$之间有连边, $a_{ij} = 1$, 否则, $a_{ij} = 0$. k_i代表的则是节点i的度值.

典型的供应链网络结构模型如图1, 网络拓扑结构如图2所示.

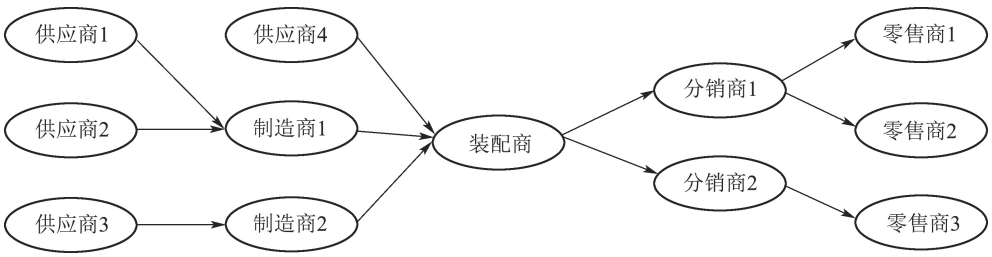

图 1　供应链网络结构模型图

Fig. 1　Supply chain network structure model diagram

从图1可以看出, 物流供应链网络节点有的只有输出连边, 有的节点既有输出连边, 也有输入连边. 只有输出连边的节点是供应商节点, 既有输入连边也有输出连边的是非供应商节点. 由文献[13]可知, 供应链网络符合的区域无标度特性, 无标度网络由Barabási于1999年在Science杂志上发表了该无标度网络的概念的文章.

2.1.1　节点度

由于物流供应链网络是有向加权网络, 所以该网络的节点v_i的度包含出度k_i^{out}和入度k_i^{in}. 节点i的度$k_i = k_i^{\text{out}} + k_i^{\text{in}}$.

$$k_i^{\text{out}} = \sum_{j=1}^{m} l_{ij},\ k_i^{\text{in}} = \sum_{j=1}^{m} l_{ji},$$

l_{ij}表示节点i和节点j之间有节点i指向节点j的有向连

边, 整个网络不同的节点的度值可以根据节点之间的邻接矩阵进行计算, 且供应链网络节点的度值分布符合幂律分布.

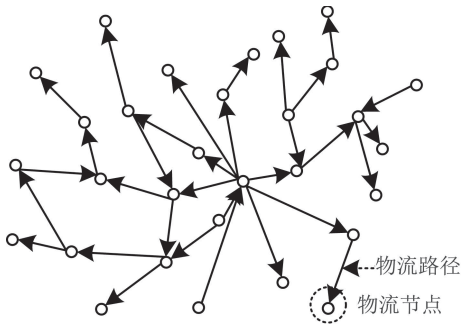

图 2 供应链网络拓扑结构图

Fig. 2 Supply chain network topology

2.1.2 介数

点介数能够表示该节点在整个物流网络中的影响力, 对于维持网络连通性和可控性有着非常重要的意义. 一个节点或者连边的介数越大, 就表示该网络的最短路径路过该节点或者连边次数就越多.

$$D_o = \sum_{i\neq o\neq j} \frac{d_{ioj}}{d_{ij}},$$

d_{ioj}表示的是物流节点i和物流节点j之间的最短路径经过节点o的数目, d_{ij}表示的是物流节点i到物流节j之间的最短路径总数.

边介数表示的是节点m与节点n之间的连边l_{mn}在整个物流网络的重要程度.

$$B_{mn} = \sum_{i\neq m\neq n\neq j} \frac{b_{imnj}}{b_{ij}},$$

b_{imnj}表示的是物流节点i和物流节点j之间的最短路径经过连边mn的数目, d_{ij}表示的是物流节点i到物流节j之间的最短路径总数.

2.2 供应链网络抗毁性测度

物流供应链网络需要保持良好的连通鲁棒性和能控鲁棒性, 运行状态最良好的情况就是由最少的控制输出节点来控制整个供应链网络. 因此在本文中检验供应链网络鲁棒性的标准有两个: 网络运营度和能控性曲线.

2.2.1 网络运营度

网络可用性指标是由孙昱等人[14]提出的新的抗毁性测度, 该测度是在无向网络的基础上提出的, 设原始网络有m个连通分量, 那么该网络的可用性指标U可以用以下公式进行表示:

$$U = \frac{\sum\limits_{i=1}^{m} n_i(n_i-1)/2}{n(n-1)/2},$$

其中: n_i代表的是第i个连通分量里面所含有的节点的数目, n代表的是m个连通分量里一共含有的节点数目.

本文根据供应链网络的特点在此基础上提出了“网络运营度”的概念, “运营”一词指的是网络能够正常运作, 被控制. 为了能够更好的理解这“网络运营度”这一概念, 在此对节点的控制输入或者输出重新定义. 节点的控制输入或者输出是相对而言的, 例如一个节点a接收节点b的货物, 此时a为控制输入节点, b为控制输入节点. 然后b通过加工或者是分销输送货物到c, 此时为b控制输出节点, c为控制输入节点.

在供应链系统没有遭受到网络攻击时, 整个系统是处于全面“运营”的状态, 也就是说各个节点都与整个系统有连接, 且节点皆处于被控状态. 供应链网络里节点之间能够进行正常的货物来往–节点之间的有向连边正常运作, 此时的网络运营度为1. 当供应链网络遭受到网络攻击时, 由于有向网络的级联失效效应造成有的节点或者是连边失效, 进而使节点之间的货物来往遭到破坏. “网络运营度”在遭受攻击之后的变化与网络的攻击级联失效效应密切相关. 因此针对不同的攻击方式(连边攻击、节点攻击)造成的级联失效效应的情况进行举例讨论. 图3为某供应链网络局部遭受到网络攻击之后的网络拓扑结构级联失效变化示意图.

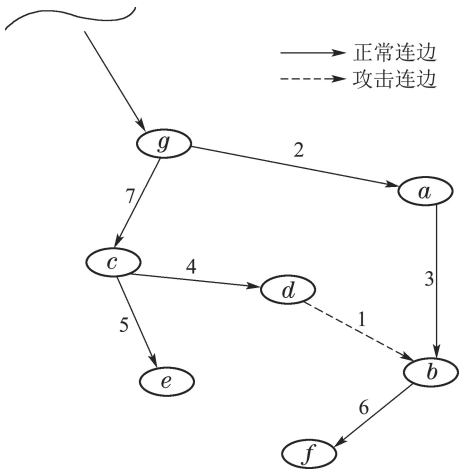

图 3 攻击模式1

Fig. 3 Attack mode 1

从图3可以看出, 当网络只攻击连边1时, 该网络之间的节点依旧能够处于被控制状态, 网络并没有因为遭受攻击而断开与网络之间的连接与被控制状态. 也就是说系统网络中的节点不需要额外的控制输入节点来对其进行控制, 控制输入节点的总数目没有发生改变. 该局域系统中没有发生故障级联失效现象, 这启示在供应链网络中应增加货物来源途径, 减少因某一条供货线路中断造成大规模的货运瘫痪的几率. 但是此时网络的平均度值发生了改变, 系统的连通性发生了改变, 边介数可能也会发生变化. 还有其他的一些网络的一些基本性质特征可能会发生相应的变化,

这需要具体网络进行具体的分析.

从图4可以看出, 当网络攻击连边2时, 由于节点a只有一个输入连边, 当遭受攻击时, 缺少控制输入, 即供应链网络中缺少货物来源. 后续的货物运输无法进行, 连边3遭受级联失效. 节点b除连边3的输入还有连边1的输入, 即节点b在系统中依旧可控. 连边2和3从系统中移除, 系统的网络运营度遭受破坏, 系统的可控性能也会受到影响.

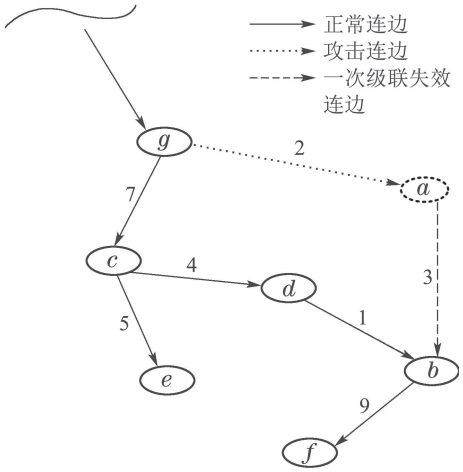

图 4 攻击模式2

Fig. 4 Attack mode 2

从图5可以看出, 当网络攻击节点b时, 与节点b有直接连接关系的连边被移除网络, 因为节点b不涉及出度连边的2次级联, 所以没有级联连边被移除的情况. 针对图3和图5的攻击示意图进行对比, 不难发现同样是没有级联失效现象的攻击过程, 攻击节点比攻击单条连边造成的系统破坏程度大. 因此在供应链网络末端应该加强节点的维护, 此节点承担着货物的分配.

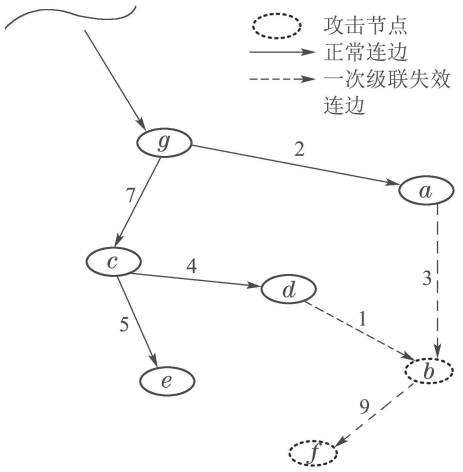

图 5 攻击模式3

Fig. 5 Attack mode 3

从图6可以看出, 当网络攻击节点c时, 与节点c有直接连接关系的连边被移除网络. 但是节点c的出度连边4与节点d相连, 所以节点d因失去控制输入节点而失效, 进而节点d的出度连边1级联失效, 但节点b接收节点d的控制输入, 所以节点b依旧可控.

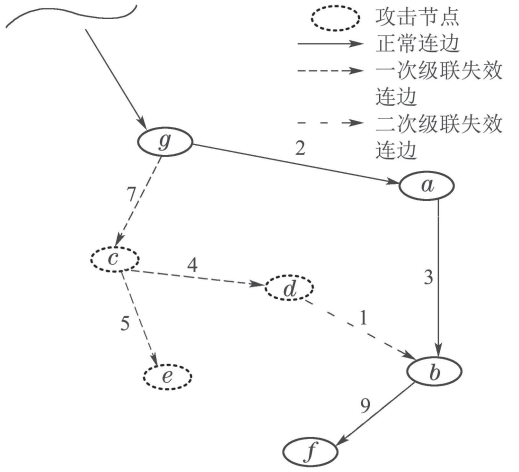

图 6 攻击模式4

Fig. 6 Attack mode 4

网络运营度的计算必须要对所研究的供应链网络有足够的认识, 才能得到精准的计算. 因此在对供应链网络足够认识的基础上, 网络运营度G为现存能够正常运作的有向连边数目占原供应链网络未遭受到攻击时的连边总数的比值, 转化为相应的数学模型如下所示:

$$G=\frac{\sum_{i=1}^{m} n_{yi}}{N},$$

其中: n_{yi}代表的当前系统里第i个连通分量里面能够正常被系统控制的连边数目; 而n_i代表的是原始系统连边总数.

2.2.2　能控性曲线

物流供应链网络最重要的就是在网络遭受攻击后, 整个网络的可控性鲁棒性, 点的能控性鲁棒性的定义如下[15]:

$$N^d(i)\equiv\frac{n_d(i)}{n-i},\ i=0,1,\cdots,n-1,$$

其中: $n_d(i)$是当供应链中i个节点遭受攻击后, 系统所需要控制的节点数目, 也就是系统中没有控制输入的节点数目; $n-i$为供应链网络在遭受i个节点攻击之后的网络剩余节点数.

供应链网络遭受到连边攻击之后, 可能会形成没有控制输入的节点, 在连边攻击下能控性鲁棒性定义如下:

$$N^l(i)\equiv\frac{n_l(i)}{n},\ i=0,1,\cdots,n-1,$$

其中: $n_l(i)$表示的是当供应链网络中某些连边遭受到攻击时, 网络所需要控制的节点数; n表示的未遭受攻击的原始节点数目. 无论是节点攻击还是连边攻击,

当$i=0$时代表的是供应链系统未遭受攻击时的状态.

3 供应链网络攻击

供应链网络并不是一直处于稳定状态的, 而是会不定期的遭受攻击, 而攻击方式则可以分为随机攻击和蓄意攻击. 随机的攻击供应链网络中的节点或者是连边称为随机攻击. 而蓄意攻击就是优先攻击在供应链里面被认为重要的节点或者连边, 可以是攻击节点度最大的节点, 也可以是攻击权重最大的连边. 例如, 在实际应用中, 由于自然原因造成的道路损坏(供应链连边的损坏)或者是建设设施的损坏(供应链中的节点损坏). 这种攻击方式是无差别攻击, 对应的是供应链随机网络攻击. 而恶性的蓄意攻击不同于随机的无差别攻击方式, 例如竞争对抢占货物资源而导致供应链中节点(供应商)的消失, 直接造成了与节点有联系的连边消失.

本文重点讲述几种蓄意网络攻击方式.

1) 基于节点度值进行的蓄意攻击[16–17], 节点度值的计算方法见2.1.1. 可以尽可能快的破坏网络中连边多的节点, 当攻击策略遇到多个节点度值一样的点, 优先攻击级联失效作用更强的节点, 能够更好的破坏节点之间的连通性.

2) 基于连边权重进行的蓄意攻击. 连边的权重越大说明该连边两边的节点业务来往越多, 破坏该连边对于网络的连通性也会有影响. 当攻击策略遇到多个连边的权重一样时, 优先攻击级联失效作用更强的连边.

3) 优先攻击网络中的关键节点和关键连边的蓄意攻击. 关键节点的蓄意攻击指的是物流供应链网络的某些节点, 在遭受到攻击时能导致系统大范围瘫痪. 而关键连边依然, 在系统攻某些连边时, 导致了系统的大范围瘫痪.

4 供应链网络恢复机制

物流供应链网络是有向的网络, 所以在遭受到攻击的时候, 节点之间根据出度和入度的关系并不是简单的散落成单个的节点, 节点间的连边并不是全部消失. 这就是实际供应链网络与单纯的数学上的复杂网络结构相异的地方.

本文所述的供应链网络只考虑货物的流通, 箭头的方向代表了货物流通的方向, 当供应链网络遭受到连边攻击的时后, 局部供应链网络可能出现的情况如图7所示.

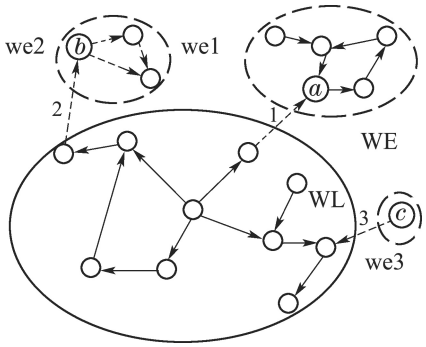

图 7 供应链网络遭受连边攻击

Fig. 7 Supply chain network suffers edge attack

图7所标识的WL领域是遭受到连边网络攻击之后的剩余的主网络, 而WE则是在遭受到连边攻击后被“抛弃”的网络. 当网络中因攻击策略删除掉一个连边时, 如果在WE中被抛弃的网络, 节点a在删除与WL网络之间的连边1之后, we1局部网络中仍有一个控制输入节点. 该部分局部网络并没有因为连边攻击而增加额外所需控制输入节点, 可以由该网络中的控制输出节点进行正常的局部的供应链系统运行, 这类型网络称之为“主动”局域网络. 当网络因攻击策略删除掉一个连边2时, 在WE中被抛弃的网络we2因没有额外的控制输出而导致了其他连边的级联失效, 这类型网络称之为“被动”局域网络. 网络中还存在一种状态就是被攻击的节点只是一个单纯的控制输出节点we3. 该节点对应在供应链网络里面就是供应商节点, 该节点的恢复会增加供应链网络中货物的运输总量或者是货物种类. 如果存在另外一个单独的输入型节点, 那么本文应该优先考虑恢复单独的控制输出节点.

5 供应链网络攻击实验

先设计一个简单的供应链网络作为实验主体, 进行网络攻击实验, 通过下面几种不同的攻击方式进行网络抗毁性的测试. 设计的加权有向供应链网络如图2, 有30个节点, 节点的度分布符合幂律分布, 即少数节点有较大的度值, 大多数节点有较小的度值.

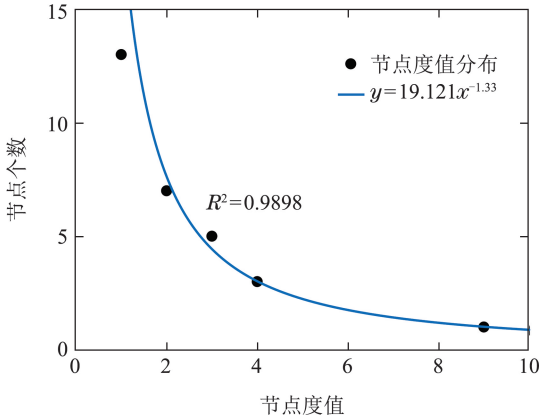

图 8 供应链节点度分布拟合曲线

Fig. 8 Fitting curve of supply chain node degree distribution

图8所示为的实验网络度值的分布特征, 可以通过数据拟合得出该网络的节点度值分布符合幂律分布, 当趋势线的R^2等于或近似于1时, 趋势线最可靠. 由此可见该数据可靠.

5.1　基于节点度值的蓄意攻击

对供应链网络中节点的度值进行分析、统计, 依照度值从大到小进行排列, 得到序列D. 假设网络攻击每次只攻击一个节点, 攻击的节点顺序按照序列D进行. 网络遭受到攻击之后需要重新计算节点的度值, 按照新的度值从大到小排列, 更新序列D. 依次类推, 直到网络中没有节点存在, 系统的网络运营度曲线和能控性曲线随着网络攻击进程的变化如图9所示.

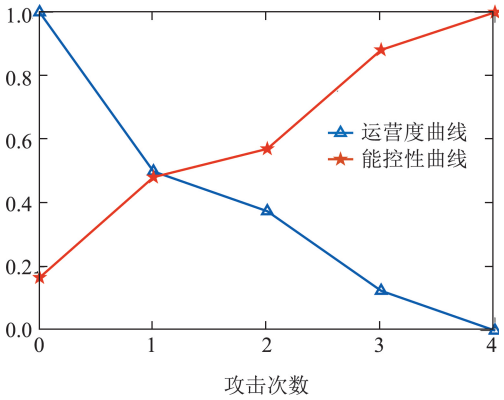

图 9　基于节点度值攻击网络性能曲线

Fig. 9　Attack network performance curve based on node degree value

通过对网络攻击后的抗毁性测度图进行分析, 得出结论: 根据节点度值的网络攻击方式, 对于该网络来说不管是能控性曲线还是网络运营度曲线来说, 结果都可以表示出网络的抗毁性能. 能控性曲线数值越大, 代表的是供应链网络的连通性和可控性越差. 而网络运营度曲线则正好相反, 数值越小代表的是网络的连通性和可控性越差.

5.2　基于连边权重的蓄意攻击

加权网络的连边权重由1.1内容可知, 根据连边的权值大小依次降序排列, 每次根据序列攻击一条连边, 每攻击完一条连边, 对网络中连边的权值进行重新分析, 统计. 更新排序列表, 直到网络中没有连边的存在.

从图10可以看出, 能控性曲线在第1次和第2次、第4和第5次、第7和第8次、第15和第16次网络攻击时, 网络中所需要的的控制节点并没有发生变化. 根据网络运营度曲线可知, 网络的连通性发生改变. 由此可见网络运营度曲线更能够体现网络连通性的变化, 而能控性曲线则更能够体现网络能控性的变化. 通过该变化曲线得出结论, 在设计网络拓扑结构时, 多增加控制节点, 对应的就是增加供应链网络里的供应商来源多样性. 即使有供应商受到攻击, 其他供应商可以继续控制网络运行, 提高网络的抗毁性.

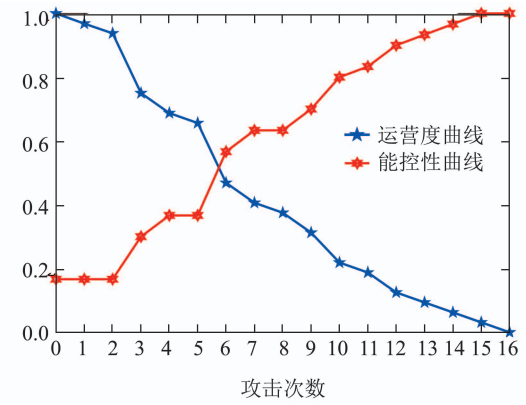

图 10　基于连边权重攻击网络性能曲线

Fig. 10　Network performance curve based on edge weight attack

供应链网络的攻击与恢复是相辅相成的, 网络遭受攻击就需要对网络进行修复, 修复的方法有很多种. 针对于本文供应链网络在遭受攻击之后, 会产生级联失效现象, 所以在实行网络恢复机制时候应该优先考虑恢复使网络运营度增加大的节点或者是连边.

6　结论与展望

本文针对有向加权供应链网络进行抗毁性研究, 通过不同的网络攻击方式, 对网络的节点或者是连边进行攻击. 为了能够更好的体现出在网络攻击模式下网络的的连通性和可控性能, 本文设计了“网络运营度”的概念, 通过列举相应的例子对其展开描述. 然后通过供应链网络攻击例子得出相应的能控性曲线和网络运营度曲线, 并对其变化趋势进行分析, 得出网络运营度策略可以运用于加权有向网络的抗毁性性能分析的结论. 本文在实验后提出网络拓扑结构的改良方法以及网络恢复机制方法. 通过本文的研究, 对于供应链网络的鲁棒性有一定的了解, 后期会针对复杂供应链网络的其他攻击方式的系统鲁棒性进行研究.

参考文献:

[1] WANG Xiaofan, LI Xiang, CHEN Guanrong. *Complex Network Theory and Its Application*. Beijing: Tsinghua University Press, 2006.
(汪小帆, 李翔, 陈关荣. 复杂网络理论及其应用. 北京: 清华大学出版社, 2006.)

[2] ALBERT R, JEONG H, BARABÁSI A L. Error and attack tolerance of complex networks. *Nature*, 2000, 406: 378 – 382.

[3] LIU Haoran, WANG Xingqi, QIN Yuhua, et al. A directed topology model for wireless sensor networks with destructiveness. *Control Theory and Applications*, 2020, 37(6): 1225 – 1231.
(刘浩然, 王星淇, 覃玉华, 等. 具有抗毁性的无线传感器网络有向拓扑模型. 控制理论与应用, 2020, 37(6): 1225 – 1231.)

[4] HU Yihong, WU Qinmin, ZHU Daoli. Topological properties and vulnerability analysis of urban road network. *Complex Systems and Complexity Science*, 2009, 6(3): 69 – 76.
(胡一竑, 吴勤旻, 朱道立. 城市道路网络的拓扑性质和脆弱性分析. 复杂系统与复杂性科学, 2009, 6(3): 69 – 76.)

[5] WU Jun, TAN Yuejin. Research on survivability measurement of complex networks. *Journal of Systems Engineering*, 2005, 20(2): 128 – 131.
(吴俊, 谭跃进. 复杂网络抗毁性测度研究. 系统工程学报, 2005, 20(2): 128 – 131.)

[6] LIU Y Y, SLOTINE J J, BARABÁSI A L. Controllability of complex networks. *Nature*, 2011, 473(7346): 167 – 173.

[7] YANG Jingfeng, ZHU Dapeng, ZHAO Ruilin. Characteristics of urban rail transit network and robustness analysis of cascading failure. *Computer Engineering and Application*, 2021: 1 – 12.
(杨景峰, 朱大鹏, 赵瑞琳. 城市轨道交通网络特性与级联失效鲁棒性分析. 计算机工程与应用, 2021: 1 – 12.)

[8] WANG C, XIA Y. Robustness of complex networks considering attack cost. *IEEE Access*, 2020, 8: 172398 – 172404.

[9] SHI X Q, DENG D S, LONG W, et al. Research on the robustness of interdependent supply networks with tunable parameters. *Computers and Industrial Engineering*, 2021, 158: 107431.

[10] LOU Y, WANG L, CHEN G R. A framework of hierarchical attacks to network controllability. *Communications in Nonlinear Science and Numerical Simulation*, 2021, 98: 105780.

[11] XIE Feng, CHENG Suqi, CHEN Dongqing, et al. Survivability of complex networks based on cascading failure. *Journal of Tsinghua University (Natural Science Edition)*, 2011, 51(10): 1252 – 1257.
(谢丰, 程苏琦, 陈冬青, 等. 基于级联失效的复杂网络抗毁性. 清华大学学报(自然科学版), 2011, 51(10): 1252 – 1257.)

[12] ZHANG Y, ZHOU S, ZHANG Z, et al. Traffic fluctuations on weighted networks. *IEEE Circuits and Systems Magazine*, 2012, 12(1): 33 – 44.

[13] LI Guang, ZHAO Daozhi. Research on scale-free characteristics of supply chain networks. *Industrial Engineering*, 2012, 15(1): 28 – 32.
(李广, 赵道致. 供应链网络的无标度特性研究. 工业工程, 2012, 15(1): 28 – 32.)

[14] SUN Yu, YAO Peiyang, ZHANG Jieyong, et al. Complex network node attack strategy based on optimization theory. *Journal of Electronics and Information*, 2017, 39(3): 518 – 524.
(孙昱, 姚佩阳, 张杰勇, 等. 基于优化理论的复杂网络节点攻击策略. 电子与信息学报, 2017, 39(3): 518 – 524.)

[15] LOU Yang, LI Junli, LI Sheng, et al. Research progress on controllability and robustness of complex networks. *Acta Automatica Sinica*, 2021, DOI: 10.16383/j.aas.c200916.
(楼洋, 李均利, 李升, 等. 复杂网络能控性鲁棒性研究进展. 自动化学报, 2021, DOI: 10.16383/j.aas.c200916.)

[16] HOLME P, KIM B J, YOON C N, et al. Attack vulnerability of complex networks. *Physical Review E*, 2002, 65(5): 056109.

[17] LIU Y Y, SLOTINE J J, BARABÁSI A L. Controllability of complex networks. *Nature*, 2011, 473: 167 – 173.

作者简介:

崔慧霞 硕士研究生, 目前研究方向为物流网络优化、复杂供应链网络鲁棒性分析, E-mail: 15563378105@163.com;

邱建龙 博士, 教授, 博士生导师, 中国自动化学会TCCT物流系统智能优化与控制学组主任, 目前研究方向为复杂系统与复杂网络的理论与应用、物流系统智能优化与控制, E-mail: qiujianlong@lyu.edu.cn;

郭 明 博士, 教授, 硕士生导师, 目前研究方向机器学习与系统控制、模式识别等, E-mail: guoming0537@126.com;

张润发 硕士研究生, 目前研究方向为智能算法的改进, E-mail: zrf20210510@163.com.