基于供应链网络的传递攻击策略研究

柳 虹[1,3] 周根贵[2] 傅培华[3] 毛国红[1]
(浙江工业大学信息学院 杭州 310014)[1] (浙江工业大学经贸管理学院 杭州 310014)[2]
(浙江工商大学计算机与信息工程学院 杭州 310018)[3]

摘 要 为了分析突发事件对供应链网络整体功能的影响,基于复杂网络理论,考虑节点失效性能的传递性,提出了传递攻击策略,用其模拟供应链系统中的供求失效,进而分析供应链网络在受到攻击时的脆弱性和鲁棒性。实验结果表明,传递攻击能够很好地模拟供应链网络中的供求失效,且供应链网络面对传递攻击时,网络结构表现得比较脆弱;同时也说明了该攻击策略是可行的,具有一定的现实意义。

关键词 复杂网络,供应链,节点失效,传递攻击,脆弱性,鲁棒性
中图法分类号 TP311 **文献标识码** A

Research of Transferring Attack Based on Supply Chain Network

LIU Hong[1,3] ZHOU Gen-gui[2] FU Pei-hua[3] MAO Guo-hong[1]
(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310014, China)[1]
(College of Business Administration, Zhejiang University of Technology, Hangzhou 310014, China)[2]
(Computer and Information Engineering College, Zhejiang Gongshang University, Hangzhou 310018, China)[3]

Abstract Unexpected events have negative impacts on the whole performance of supply chain network. Based on complex networks theory, and considering the transferring characteristic of nodes' invalidation performance, this paper put forward a transferring attack strategy to simulate supply disruption and demand disruption of supply chain system, and further analyse the frangibility and robust of supply chain network. A hypothetical supply chain network was constructed to illustrate the proposed attack strategy. The experiments' results show that such proposed attack strategy can well simulate supply disruption and demand disruption of supply chain system, and for suffering the transferring attack, supply chain network exhibits some frangible. And it also illuminates such strategy is feasible and has some realization significance.

Keywords Complex network, Supply chain, Node invalidation, Transferring attack, Frangibility, Robust

1 引言

供应链是一个由供应商、生产商、分销商、物流服务商、批发商和零售商等成员企业组成,实现将原材料转化为成品以满足顾客需求的复杂网络,网络内部存在着广泛的错综复杂的物质、信息和资金的交换,体现在节点企业之间具有高度的关联性。这样一个复杂自适应网络不可避免会受到各种不确定的内外部的干扰或攻击,而供应链网络结构和供应链实体关系的复杂性加剧了其网络运行情况的不确定性。面对竞争激烈的商业环境,网络上任何节点遭受突发事件(干扰或攻击)时,从危害角度来说,小则影响网络的运行和效率,大则攻击造成的影响会沿着整个供应链网络扩散,如很快影响到与被攻击节点相连接的上下游企业节点,进而沿着网络连接影响到网络上的所有企业,导致供应链系统部分供应中断或全部功能丧失(系统崩溃),从而急剧增加网络成本,降低服务水平。在经济全球化、信息化及大量不确定性问题背景下,供应链作为一个复杂网络,大多不能抵御不确定性甚至不能抵御风险。因此,分析不同攻击情况下供应链网络的脆弱性及鲁棒性的表现形式和特点,研究节点失效给供应链网络带来的冲击,研究如何采取有效措施提高供应链网络质量以应对各种攻击,对于提高供应链的运作绩效和鲁棒性都具有十分重要的意义。

国内外的学者在运用复杂网络研究供应链网络的脆弱性和鲁棒性方面取得了一定的进展。Christian Kuhnert[1]发现城市物资供应网络服从无尺度分布,即都有少数的核心节点发挥重要的物资调度和配送作用。DirkHelbing[2]研究发现好的供应链结构能够增加网络的稳定性和抗攻击性。在供应链网络中,任何一个环节上的细微变化都可能给另外的环节

到稿时间:2012-09-22 返修时间:2012-12-22 本文受国家自然科学基金项目(71071142,71171178),浙江省电子商务技术科技创新团队项目(2012R10041-20)资助。

柳 虹(1979—),女,博士生,副教授,主要研究方向为人工智能、系统集成与优化,E-mail:LLH@mail.zjgsu.edu.cn;周根贵(1958—),男,教授,博士生导师,主要研究方向为系统集成与优化、人工智能,E-mail:ggzhou@zjut.edu.cn(通信作者);傅培华(1966—),男,博士生,教授,主要方向为系统集成与优化、供应链管理;毛国红(1976—),女,博士生,讲师,主要研究方向为网络化制造与建模、计算机视觉。

带来变化，而这些变化和供应链网络本身的拓扑结构、宏观性质紧密相关。Albert[3]得出对随机故障的鲁棒性和对蓄意攻击的脆弱性是无标度网络的一个基本特性，并且指出其根源在于无标度网络中度分布的不均匀性。Barabasi 等[4]提出了复杂网络的 Scale-free 模型，并发现系统固有的结构特性对系统的脆弱性有着重要影响。Thadakamalla[5]通过复杂网络拓扑结构观点对供应链的存活性进行了分析。Latora 等[6]基于最短路径提出了网络效率参数，并通过比较系统故障前后功能变化来分析脆弱性。刘小峰[7]基于复杂网络理论分析供应链的鲁棒性，把鲁棒性分为稳定鲁棒性和性能鲁棒性；姜洪权等[8]提出了节点负荷与结构脆弱系数的概念，建立了基于最短路径长度和聚集系数的高度耦合工业生产系统脆弱性分析方法；闫妍等[9]将节点介数作为衡量企业负载的测度，通过计算级联失效后系统最大连通子图规模来衡量供应链网络的脆弱性。上述研究多将企业视为均质节点，忽略了企业间的差异性，并且考虑的节点攻击策略仅仅存在于拓扑意义上，没有考虑到网络上的动态性过程对网络脆弱性的影响，认为失效的节点对其他节点的变化与否没有任何影响，体现在复杂网络攻击策略上，当蓄意攻击时，每次选取的攻击节点之间没有必然的联系，只是根据节点的度(或介数)来选择攻击对象，忽略了失效节点会对其关联节点带来的传递影响。本文以供应链网络为背景，引入复杂网络理论研究其脆弱性，提出考虑节点失效性能传递特性的攻击策略，模拟供应链系统的供求失效，分析供应链网络遭受传递攻击时的结构变化情况。

2 问题描述

在供应链网络中存在各种不确定性，如客户需求变化，运输过程发生意外导致不能及时交货，生产设备发生故障等等。这些不确定性对客户需求、沿着供应链的供应交付、外部或者市场供应都会带来影响[10]，从而引发供应链系统中失效事件的发生。由于供应链是一种较为复杂的系统，表现为一个围绕核心企业的网状结构，同时连接供应商、制造商、分销商和顾客等，整个供应链环环相扣，因此任何一个环节产生的失效，都可能影响供应链的正常运作。从失效事件的影响后果角度可以把失效分为 3 类：供应失效(supply disruption)、内部运营失效(internal disruption)和需求失效(demand disruption)。本文研究供应失效和需求失效对网络造成的影响，其中供应失效指供应商、分销中心或零售商供应的失效，而需求失效指对产品或服务需求短时间内没有预测到的大规模下降。

在供应链网络系统中，供应失效发生在从供应链上游向下游传递的产品供应过程中，如一旦供应商出现问题或供应运输中断，若短时间不能及时找到替代的供应商，而当前供应网络中又普遍存在低库存的情况，该失效事件就很容易引发网络的中断而导致巨大的损失。而需求失效发生在从供应链下游向上游传递的需求过程中，是指需求信息在向上游传递的过程中所发生的需求偏差逐级放大，导致供应链中产品库存过高或者发生缺货，从而降低了供应链的绩效。对于供应链系统，不确定性通过一系列链式过程进行传递，即供应链上每一级的延迟交货都会造成延迟一级级向下传递，从而造成偏差与不确定性的叠加放大，具体过程如图 1 所示。若企业 1 供应中断，则会影响它的下游企业(3,4)，可能导致其下游企业(3,4)也发生业务中断，若 4 发生传递失效事件，则它又会影响自身的下游企业(8,10)，层层传递下去，结果会引起部分供应线路中断，严重的会引起整个供应系统中断。

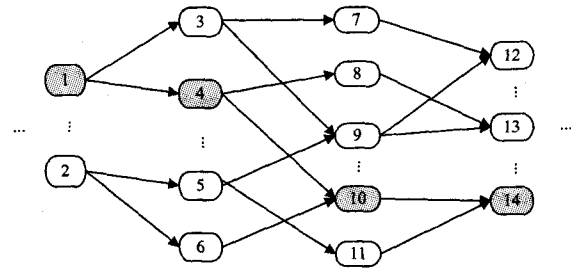

图 1 失效事件传递过程

3 供应链网络性能描述

供应链网络可以采用图型结构表示，形式为 $G^{w}=(V,E,W)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$ 代表供应链中企业节点的集合，类型包括：供应商、生产商、分销商、零售商、顾客等；$E=\{e_1,e_2,\cdots,e_m\}$ 表示所有供应弧的集合，弧 $e_{ij}=\langle v_i,v_j\rangle$ 代表从上游企业 v_i 到下游企业 v_j 的可行供应渠道，节点 v_i 的入向弧和出向弧分别记为 I_i 和 O_i。

本文用于评价供应链网络性能的网络特性有：

(1)节点介数(Betweenness)[11]：反映节点在整个网络中的作用和影响力，一个节点的介数越大，流经它的数据分组越多，意味着节点在网络中的作用性越大。表示为：

$$B_i=\frac{\sum_{v_i\neq v_j\neq v_k\in V}\frac{\sigma_{jk}(i)}{\sigma_{jk}}}{n*(n-1)} \tag{1}$$

式中，σ_{jk} 表示节点 v_j 与节点 v_k 之间所有的最短路径数目，$\sigma_{jk}(i)$ 表示节点 v_j 与节点 v_k 之间经过节点 v_i 的最短路径数目。

(2)最大连通子图(the Largest Connected Component)[3]：表示网络 G 受攻击后，节点 $v_1,\cdots,v_m(1\leqslant m\leqslant n)$ 与其他节点断开连接，使得网络 G 被拆分成多个独立的连通子图 $G_1,\cdots,G_t(1\leqslant t\leqslant n)$，其中最大连通子图 G_i 表示为：

$$C=size(G_i)=K_i=\max\{K_j,j=1,\cdots,t\} \tag{2}$$

式中，K_j 表示 G_j 的节点数目(即网络大小)。干扰后供应链网络的最大连通子图的大小实际上反映了供应链系统在受到内外部干扰(攻击)后，还有多少企业存在于其中，若该值较大，表明附着于网络的节点仍然很多，说明供应链结构稳定，反之说明结构比较脆弱。

(3)网络效率 $E(G)$[12]：用于描述网络中节点企业之间业务往来的效率，如企业间信息的传递效率、订单的处理效率等，反映了供应链网络的反应性及响应速度。表示为网络中任意两个节点之间距离倒数之和的平均值，即：

$$E(G)=\frac{1}{N(N-1)}\sum_{i\neq j\in G}\frac{1}{d_{ij}} \tag{3}$$

式中，$\frac{1}{d_{ij}}$ 表示节点 i 和 j 之间的最短路径长度的倒数，如果节点 i 和 j 之间不存在路径，则 d_{ij} 为 ∞，$\frac{1}{d_{ij}}=0$，显然 $E(G)\in[0,1]$。

(4)连接鲁棒性(Connnectiong Robustness)[13]:指网络中某些节点在遭受攻击破坏后,剩余的节点之间仍然能够继续保持连通的能力,表示为:

$$R=\frac{C}{(N-N_r(n))} \tag{4}$$

式中,N 表示初始网络规模,$N_r(n)$ 表示从网络中去除的节点个数。

4 传递攻击策略

在复杂网络抗毁性研究中,一般根据节点的度或介数的大小进行选择移除或随机移除,并以此作为攻击依据(即选择性攻击和随机性攻击)来研究网络性能的变化。考虑到供应链网络的流量和负载情况,本文以节点介数作为攻击的依据,提出了节点失效性能传递攻击策略 TA(Transferred Attack),其攻击原则为首先将节点介数进行降序排列,从中选择介数最大的节点作为攻击对象,如果一些节点恰巧具有相同的介数,将从中随机选择。进行第二次攻击时,攻击对象分为 3 种情况,如果失效事件为供应失效,则攻击对象为失效节点出向弧关联的节点;如果为需求失效,则攻击对象为失效节点入向弧关联的节点;否则,攻击对象为失效节点的所有关联节点。3 种情况下的攻击原则都为将关联节点的介数进行降序排列,从中选取介数最大的关联节点进行攻击。进行第三次攻击时,要同时考虑之前所有攻击产生的失效节点的关联节点集合,把它们作为优先攻击对象。当关联节点介数都为 0 时,对剩余节点根据 TA 重新进行攻击,以此类推,直到整个网络崩溃。

传递攻击策略的具体实验过程为:

(1)初始条件:网络 G,节点集合 V,弧集合 E,具有 n 个节点,m 条弧,定义攻击对象节点集合 A,介数集合 I,变量 ps,pd,随机变量 p。

(2)计算 n 个节点的介数,记录在 I 中,将 I 进行排序,选取具有最大介数值 I_i 的节点 v_i 作为攻击对象,将 v_i 从 V 中移除,即 $V=V-v_i$,$n=n-1$。确定传递攻击对象之后,再将 v_i 所有关联的弧一并删除,即 $E=E-e_i$,$e_i=\{\langle v_i,v_j\rangle,\langle v_k,v_i\rangle\in E|v_j,v_k\in V\}$。

(3)分情况确定失效传递攻击对象:

1)$0\leqslant p<ps$,产生供应失效传递,获得失效节点 v_i 的下游关联节点,即出向弧所关联的节点,将其记入在 A 中,即 $A=A\cup v_j,\langle v_i,v_j\rangle\in E$。

2)$ps\leqslant p<pd$,产生需求失效传递,获得失效节点 v_i 的上游关联节点,即入向弧所关联的节点,记入在 A 中,即 $A=A\cup v_j,\langle v_j,v_i\rangle\in E$。

3)$pd\leqslant p<1$,进行双向传递,获得失效节点 v_i 的所有关联节点,记入在 A 中,即 $A=A\cup v_j,\langle v_i,v_j\rangle\in E$ or $\langle v_j,v_i\rangle\in E$。

(4)将集合 A 中的节点作为攻击对象,计算其中的节点介数,记录在 I 中,将 I 进行排序,选取介数最大的节点作为攻击对象,然后重复(3)。若 I 中元素全为 0,则 $n=n-I$ 的元素个数,转(2)。

(5)模拟终止条件:网络不连通或剩余节点介数都为 0。

5 实验分析

本实验在 Matlab7.0 环境下进行,构建文献[7]中的供应链网络模型用于仿真分析,其中模型相关数值为 $N=1000$,$l:m:n=25:4:1$,$p=\frac{1}{2}$,$x=1$,$y=5$,$z=3$,$N_1=100$,$N_2=50$,$N_3=30$,传递攻击策略中相关数值为 $ps:pd=0.5:0.8$。实验结果图中横坐标为实验的步长(Step),该步长等同于攻击的次数以及移除的节点数,RA 表示点随机性攻击,SA 表示点选择性攻击,TA 表示传递攻击。实验过程中,按照攻击策略进行攻击时,每移除一个节点,计算网络性能。为了消除仿真过程中随机因素产生的影响,对于给定的网络配置参数,我们执行 10 次配置模型,再将结果取平均值。

由图 2 可见,当供应链网络遭到传递攻击时,整个网络在一个临界值(移除节点数和原有节点数的比例)之后全部解体,其中 TA 大致在 0.84 左右,介于 RA(0.96)和 SA(0.58)之间。对于网络效率和网络连接鲁棒性变化情况,TA 引起的变化趋势和 SA 的比较类似,即网络效率在一定范围内变化比较平缓,然后慢慢下降;而初始网络的连接性能比较好,大多节点之间都是连通的,接着网络连接性能慢慢下降,到一定程度后保持一个比较平稳的变化趋势,此时网络中尽管还有一些企业之间保持供应关系,但网络连接性能已经降到最低程度。

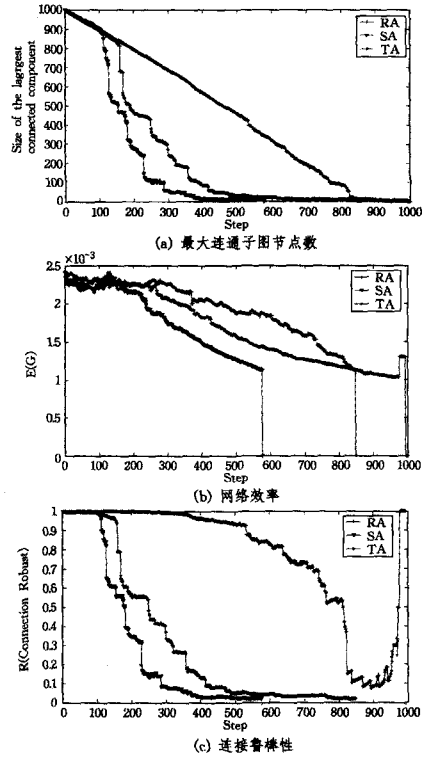

图 2 3 种攻击策略下网络性能的变化情况

总体来说,当供应链网络遭受传递攻击时,整个网络初始具有一定的响应能力和柔性,网络效率和连接性能也比较好,随着失效传递的发生,依附于供应链的节点企业越来越少,网络的反应性变得越来越差,网络的响应速度和柔性也跟着缓慢下降,在达到一个临界值后,整个网络完全坍塌。

供应链网络对传递攻击表现得比较脆弱,本文对不同比

例下的失效传递攻击情况进行了研究，仿真结果如图 3 所示。其中不同比例情况为，当 $ps:pd=1:1$ 时进行供应失效传递攻击，当 $ps:pd=0:1$ 时进行需求失效传递攻击，而 $ps:pd=0:0$ 时为供求失效双向传递攻击（即同时发生供应失效和需求失效）。

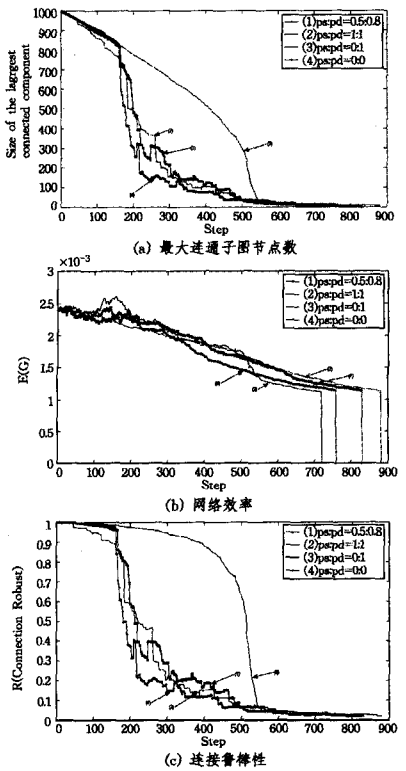

图 3　不同比例的传递攻击下网络性能的变化情况

由图 3 可见，供应链网络面对不同比例的传递攻击时，结构稳定性和连接鲁棒性的总体变化情况为：供求失效传递攻击＜供应失效传递攻击＜3 种类型都存在的传递攻击＜需求失效传递攻击，其中仅发生供应失效传递攻击时，网络效率最好。

结束语　本文从复杂网络的攻击策略角度描述供应链网络的脆弱性和鲁棒性，考虑失效事件的传递特性，提出传递攻击策略。由于供应链网络中只有少数的企业和供应关系为核心企业和核心供应关系，而大多数企业为非核心企业，因此面对传递攻击，网络结构表现得相对比较脆弱，但优于选择性攻击带来的影响。因此，在供应链管理中应该尽可能地采取一切措施保护好网络中的核心企业和关键供应关系，在供应链网络中，可以适度地增强网络的冗余度，如对于供应失效的情况，可以考虑执行多源供应商策略，这样当一个供应商不能按时提供下级所需产品的时候，多余的供应商可以保障供应链日常运行。

参 考 文 献

[1] Kuhnert C, Helbing D. Scaling laws in urban supply networks [J]. Physica A, 2006, 363(1): 89-95

[2] Helbing D. Information and material flows in complex networks [J]. Physica A, 2006, 363(1): xi-xvi

[3] Albert R, Jeong H, Barabhsi A L. The Internet's Achilles' Heel: Error and attack tolerance of complex networks[J]. Namre (London) (S0028-0836), 2000, 406: 378-382

[4] Barabasi A L, Albert R. Emergence of Scaling in Random Networks[J]. Science, 1999, 286(5439): 509-512

[5] Thadakamlla H P, Raghavan U N, Kumara S, et al. Survivability of multiagent-based supply networks: a topological perspective [J]. Intelligent Systems and Their Application, 2004, 19(5): 24-31

[6] Latora V, Marchiori M. Vulnerability and Protection of Infrastructure Networks[J]. Physical Review E, 2005, 71(1): 015103

[7] 刘小锋，陈国华. 基于复杂网络的供应链鲁棒性分析[J]. 东南大学学报：自然科学版，2007，26：147-150

[8] 姜洪权，高建民，陈富民，等. 基于网络特性的分布式复杂机电系统脆弱性分析[J]. 计算机集成制造系统，2009，15(4)：791-796

[9] 闫妍，刘晓，庄新田. 基于复杂网络理论的供应链级联效应检测方法[J]. 上海交通大学学报，2010，44(3)：322-325

[10] Petrovic D, Roy R, Petrovic R. supply chain modeling using fuzzy sets[J]. International Journal of Production Economics, 1999, 59 (1): 443-453

[11] Freeman L. A set of Measures of centrality based upon betweenness[J]. Sociometry, 1977, 40(1): 35-41

[12] Latora V A, Marchiori M. Efficient Behavior of Small-World Networks[J]. Phys. Rev. Lett., 2001, 87(19): 198701

[13] Motter A E, Lai Ying-cheng. Cascade-based attacks on complex networks [J]. Phys. Rev. E, 2002, 66(6)

(上接第 66 页)

[16] Kalil M A, Al-Mahdi H, Mitschele-Thiel A. Spectrum handoff reduction for cognitive radio ad hoc networks[C]// Wireless Communication Systems (ISWCS). York: IEEE, 2010: 1036-1040

[17] Aman M, Mahfooz S, Rehman W. Handoff delay in cognitive radios-A concept paper on utilization of guard channels[C]// Computer Networks and Information Technology. Abbottabad: IEEE, 2011: 211-215

[18] Chvatal V. A Greedy Heuristic for the Set-Covering Problem [J]. Mathematics of Operations Research, 1979, 4(3): 233-235

[19] Mohsenian-Rad A H, Wong V W S. Joint logical topology design, interface assignment, channel allocation, and routing for multi-channel wireless mesh networks[J]. Wireless Communications, 2007, 6(12): 4432-4440

[20] Cormen T H, Leiserson C E, Rivest R L. Clifford Stein. Introduction to Algorithms(Second Edition)[M]. Boston: MIT Press and McGraw-Hill, 2001

[21] Issariyakul T, Hossain E. Introduction to Network Simulator NS2[M]. New York: Springer Publishing Company, 2008