

基于多局域的恐怖组织网络择优增长演化模型

何晶¹ 李本先¹

摘要 恐怖组织网络是一种特殊的复杂网络, 其时空演化规律反映出恐怖组织活动的特征. 为更准确地理解恐怖组织网络的动态演化规律, 提出一种基于多局域的恐怖组织网络择优增长演化模型, 并对此模型进行了仿真与模拟. 该模型能准确地描述在局部信息条件下, 新节点的择优和网络的生长过程及其规律; 并且利用网络信息中心度来衡量恐怖组织网络节点的信念水平, 动态地刻画了恐怖组织网络的生长过程. 实验结果表明: 恐怖组织网络的局域度分布仍服从幂律分布, 网络信息中心度具有集中与分散性的特征; 最后, 对多个恐怖组织网络按该模型进行仿真演化, 验证了该模型的准确性与科学性.

关键词 恐怖组织网络, 择优增长, 多局域, 信息中心度, 幂律分布

引用格式 何晶, 李本先. 基于多局域的恐怖组织网络择优增长演化模型. 自动化学报, 2019, 45(11): 2137–2147

DOI 10.16383/j.aas.c170711

A Preferential Growing Evolution-model of Terrorist Networks Based on Multi-local Network

HE Jing¹ LI Ben-Xian¹

Abstract The network of terrorist organizations is a special complex network, and its spatiotemporal evolution process reflects the characteristics of terrorist organization activities. To more accurately depict the dynamic evolution process of terrorist network, this paper puts forward a preferential-growing evolution model of terrorist networks based on the multi-local network, and the model is simulated. The model can accurately describe the growth of new nodes and the growth process of network under the condition of local information. We use the node network information center degree to measure the level of terrorist beliefs, dynamic characterization of a terrorist network growth process. The experimental results show: in the terrorist networks, the degree distribution of local network follows the power-law distribution, the network information center degree of the nodes of local network has the characteristics of centralized and decentralized. Finally, the model is verified with the data of terrorist networks. The verification results show that the model is accurate.

Key words Terrorist networks, preferential-growth, multi-local network, information center degree, power law distribution

Citation He Jing, Li Ben-Xian. A preferential growing evolution-model of terrorist networks based on multi-local network. *Acta Automatica Sinica*, 2019, 45(11): 2137–2147

目前全球恐怖主义泛滥, 恐怖袭击事件时有发生, 袭击方式呈现出多样化、网络化的特点, 网络已成为恐怖组织活动的主要平台之一. 人们越来越意识到反恐的重要性, 紧迫性. 分析全球发生的主要恐怖事件, 除部分独狼式恐怖袭击事件外, 大多数恐怖组织都具有自组织性, 规律性. 分析这些事件, 人们会发现其背后都有一张无形的网络, 并呈现出一些规律与特征, 整个网络的构建与编制, 都具有一定的

规律. 掌握这些规律与特征, 对制定反恐策略, 预防恐怖袭击, 实现源头反恐, 打击恐怖组织具有重要的理论与实践意义^[1]. 针对恐怖组织网络的时空演化问题, 国内外不少学者展开了相关研究. Stripling^[2]对多个恐怖组织网络进行了实证研究, 发现其具有无标度特性, 幂律分布服从 $p(k) \sim k^{-\gamma}$. Moon 等^[3]从多元关系出发, 绘制了 2002 年中东恐怖组织网络的动态演化过程; Krebs^[4–5]利用开源情报, 从恐怖组织网络个体间的关系出发, 构建了“9·11”恐怖组织网络. 在此基础上, Memon 等^[6–9]发现恐怖组织网络具有小世界, 无标度等特性, 其子群具有同质性. Walter^[10], Carly^[11–12]等学者在对“9·11”恐怖组织网络演化规律研究时发现, 复杂网络的生长与择优机制同样适用于恐怖组织网络, 网络度分布具有幂律特性. 毕震坤等^[13]利用“9·11”恐怖组织网络数据, 验证了基于割集和 BP (Back propagation) 神经网络的方法, 能更好识别网络关键节点. 张海

收稿日期 2017-12-19 录用日期 2018-07-05

Manuscript received December 19, 2017; accepted July 5, 2018
国家重点研发计划 (2017YFC0820104), 国家社科基金重大项目 (15ZDA034) 资助

Supported by National Key R&D Program of China (2017YFC0820104) and Major Projects of the National Philosophy and Social Science Foundation (15ZDA034)

本文责任编辑 赵铁军

Recommended by Associate Editor ZHAO Tie-Jun

1. 武警警官学院部队管理系 成都 610213

1. Department of Military Management, Officers College of PAP, Chengdu 610213

等^[14] 利用社会网络分析方法对美国大使馆爆炸案进行研究, 有效识别出恐怖组织网络中隐蔽的核心成员. 李本先等^[15-18] 从心理学和系统动力学角度出发, 认为恐怖组织网络增长的动力来源于恐怖主义信念, 并对“9·11”恐怖组织网络增长到 100 个节点的过程进行了仿真, 验证了恐怖组织网络具有小世界和无标度两大特性. 许晴等^[19] 利用复杂网络择优增长机制, 对多个恐怖组织网络动态演化到 450 个节点进行仿真, 发现网络度分布的幂律指数 $\gamma \approx 2.7$. 孙多勇等^[20] 在基于局域优先原则上, 对 200 个新节点进入恐怖组织网络的过程进行仿真, 发现节点恐怖主义信念的变化是恐怖组织发动恐怖袭击的重要因素.

上述文献均是在已知恐怖组织网络全局信息条件下, 对恐怖组织网络结构, 演化规律进行的研究, 这些研究成果对指导反恐具有重要的理论与现实意义. 但是, 考虑到恐怖组织网络的隐蔽性与自我保护性, 其新节点在只拥有网络局部信息情况下, 网络择优与增长的规律仍然需要进一步研究. 特别是在局域网络动态演化背景下, 恐怖组织网络是否仍具有复杂网络特征, 局域演化过程又有哪些规律, 局域反映的特征与规律是否与整体一致, 都是值得研究与探讨的问题.

本文从恐怖组织与个体交互选择过程研究出发, 在分析边缘或底层恐怖分子发展新成员的作用时发现, 恐怖组织网络的择优与增长不同于 BA (Barabasi-Albert)^[21-22] 网络, 具有局域世界网络的演化特征; 构建了基于多局域的恐怖组织网络择优增长演化模型, 并通过实验验证了模型各局域度分布仍服从幂律分布. 其次, 选取网络信息中心度衡量节点恐怖主义信念水平, 发现数量较多, 信息传递能力较弱的边缘或底层节点, 在恐怖组织网络择优增长演化过程中具近似且较小的网络信息中心度. 最后对“9·11”等多个恐怖组织网络按基于多局域的恐怖组织网络择优增长演化模型进行仿真, 验证了该模型的有效性和准确性.

1 恐怖组织与个体交互选择过程

恐怖组织网络不是天生的, 其成长具有一个演化过程. 将恐怖组织中的恐怖分子或资源视为网络中的节点, 节点间的信息传输, 资源分配视为连线, 那么实体的恐怖组织可以构建成恐怖组织网络, 其具有复杂网络的基本特征. 并且, 恐怖组织网络是一个根据外部环境变化而不断调整网络结构的动态网络, 具有时空演化特性, 如图 1 所示.

1.1 个体到恐怖组织

没有人天生就是恐怖分子, 一个人转变为恐怖

分子, 是一个渐进的过程^[15]. 在编制网络过程中, 个体由于受多种环境因素的影响, 不断更改, 累积, 变迁自我世界观, 人生观, 价值观, 并将恐怖主义视为人生价值的过程. 将个体对恐怖主义的认同感, 归属感视为恐怖主义信念. 那么这个信念水平的增长, 受恐怖组织中信息传递能力较强的核心成员影响最大. 另一方面, 由于恐怖组织的脆弱性, 隐蔽性及自我保护性, 个体在成为恐怖分子之前, 几乎很难与核心成员产生联系, 甚至个体从加入恐怖组织, 到遭受打击乃至消亡, 都可能没有接触过核心成员. 与个体接触较多的是恐怖组织的边缘或底层分子, 称之为“守门人”或“边缘人”. 这些“守门人”或“边缘人”虽然在增加个体恐怖主义信念水平的作用有限, 甚至还可能降低其信念水平. 但由于“守门人”或“边缘人”在恐怖组织结构中地位的原因, 使得其即使被发现遭受打击, 也不会对恐怖组织产生较大影响.

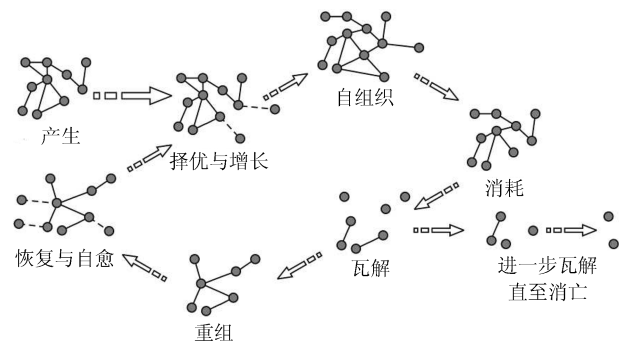


图 1 恐怖组织网络时空演化过程

Fig. 1 Spatiotemporal evolution of the terrorism organization network

1.2 恐怖组织选择个体

恐怖组织在与个体产生联系时, 主要依靠“守门人”或“边缘人”为中介, 向个体传递恐怖主义思想. 这个联系是一个弱连接到强连接的过程, 具有一定的传染效应, 需要时间的累积, 很可能导致个体的恐怖主义信念水平发生变化. 若个体恐怖主义信念水平下降, 说明个体抵触恐怖主义, 恐怖组织将减少或停止与其产生联系; 若个体的恐怖主义信念水平增加, 说明感染成功, 将加大与其联系的频率. 当个体的恐怖组织信念水平达到要求, 个体将被恐怖组织选中, 纳入其中. 若在这个联系中, 个体恐怖主义信念水平没有变化, 恐怖组织仍将以原有策略与其产生联系, 观察其信念水平的变化而调整策略.

2 多局域择优增长演化模型

Barabási 和 Albert^[21-22] 在研究万维网的度分布时发现, 新节点不是随机与网络中节点连接, 其连接概率与网络中节点的度值成正比, 并提出 BA 网

络模型. 在 BA 网络模型中, 新节点在拥有网络全局信息基础上, 总是倾向于与网络中具有较多边的节点连接. 恐怖组织网络的增长过程也遵循 BA 网络模型的择优与增长规律^[12], 但出于保护核心成员的目的, 其时空演化过程具有脆弱性, 隐蔽性及自我保护性等特点^[18]. 这导致新节点是在不知道恐怖组织网络全局信息和所有节点度分布条件下进行择优的. 这与基于全局信息的 BA 网络演化模型是不一样的.

Li 等^[23-24] 在研究世界贸易网, 手机通信网时发现, 在只知道网络局部信息时, BA 网络的择优连接机制并不适合. 将所有已知节点视为一个局域网络, 那么新节点加入时, 只能按照局域节点度状态来进行择优. 除独狼式等较为特殊的恐怖组织, 恐怖组织网络在演化过程中, 一般存在多个呈竞争关系的子群. 将每个子群视为一个局域网络, 那么新节点首先在多个局域网络中选出一个, 再在选出的局域内按 BA 网络模型进行择优连接.

图 2, m 为新节点. 图 2(a) 中, 在拥有全局信息基础上, m 按 BA 网络模型进行择优连接. 图 2(b) 中, m 在网络局域 M 中进行择优连接. 图 2(c) 中, 网络划分出 2 个局域 (M_1, M_2), m 首先确定连接局域 M_2 , 再在 M_2 内进行择优连接. 多局域择优增长网络演化模型如下:

开始于较少节点数量 m_0 , 按 BA 网络演化模型增长. 在 t_1 时刻, 网络出现局域. 此时所有局域包含 $M (M \leq m_0 + t_1)$ 个节点.

在 $t (t_1 \leq t)$ 时刻网络有 N 个局域, $L_j(t)$ 为各局域内节点数量, $j \in N$. 每个时间步增添 $m (m \leq \min L_j(t))$ 条边的新节点 v , 按概率 δ 选出局域 $L_j(t)$. 概率 δ 按式 (1) 计算:

$$\delta = \frac{L_j(t)}{\sum_N L_l(t)}, l = 1, 2, \dots, N \quad (1)$$

v 与 $L_j(t)$ 内节点的连接概率 π_{local} , 按式 (2) 计算:

$$\pi_{local}(k_i) = \frac{\delta M}{m_0 + t} \frac{k_i}{\sum_j k_j} \quad (2)$$

其中, k_i 为局域内节点 $i (i \leq L_j(t))$ 的度, $m_0 + t$ 为

$L_j(t)$ 中节点的个数. 假定 k_i 是实值连续变量^[25], 由于 k_i 的变化率正比于概率 $\pi_{local}(k_i)$, 所以 k_i 满足动态方程:

$$\frac{\partial k_i}{\partial t} = m \frac{\delta M}{m_0 + t} \frac{k_i}{\sum_j k_j} \quad (3)$$

引入 t 时刻局域网络节点的平均度^[24] $\langle k_i \rangle = (2mt + 2e_0)/(m_0 + t)$, 则 $\sum_j k_j = M \langle k_j \rangle$. e_0 为 t_1 时刻连接到 m_0 的度, 则:

$$\frac{\partial k_i}{\partial t} = m \frac{\delta M}{m_0 + t} \frac{k_i}{M (2mt + 2e_0)/(m_0 + t)} = \frac{m \delta k_i}{2 (mt + e_0)} \approx \frac{\delta k_i}{2t} \quad (4)$$

因 $k_i(t_1) = m$, 解得:

$$k_i(t) = \frac{(2 - \delta) m}{\delta} \left(\frac{t}{t_1} \right)^{\delta/2} \quad (5)$$

$$k_i(t) \sim t^{\delta/2} \quad (6)$$

所以, 在多局域择优增长模型中, 各个局域也具有无标度特性, 度分布服从幂律分布. 初始于较少 m_0 节点按 BA 模型择优增长, 在出现局域 ($M = 20, 25, 30, \delta = 0.2, 0.1, 0.05$) 后, 网络按多局域择优增长到 10 000 个节点, 局域度分布如图 3 所示.

图 3 仿真结果反映出, 不同初始条件下, 网络增长到较多节点数量时, 相同 δ 的局域具有近似的幂律分布, δ 越大的局域其指数 γ 越大, 说明其“竞争力”较强, 无尺度特性更明显.

3 恐怖主义信念水平

决定个体是否成为恐怖分子的关键因素是其自身的恐怖主义信念水平. 通过与个体产生联系, 传递恐怖主义思想是恐怖组织最直接, 最常用的增加个体恐怖主义信念水平的手段. 所以, 计量恐怖组织网络中节点信息传递能力是研究恐怖组织网络择优增长的重要内容.

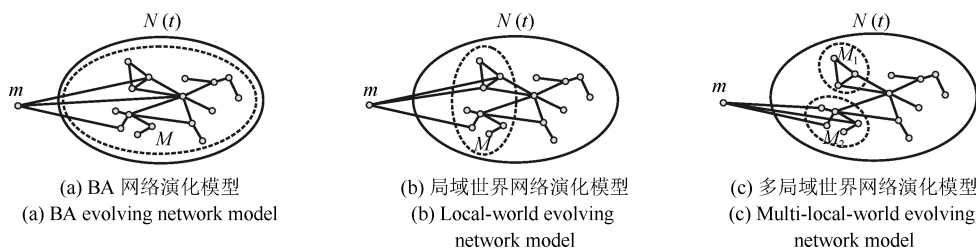


图 2 三种网络演化模型
Fig. 2 Three types of evolving network model

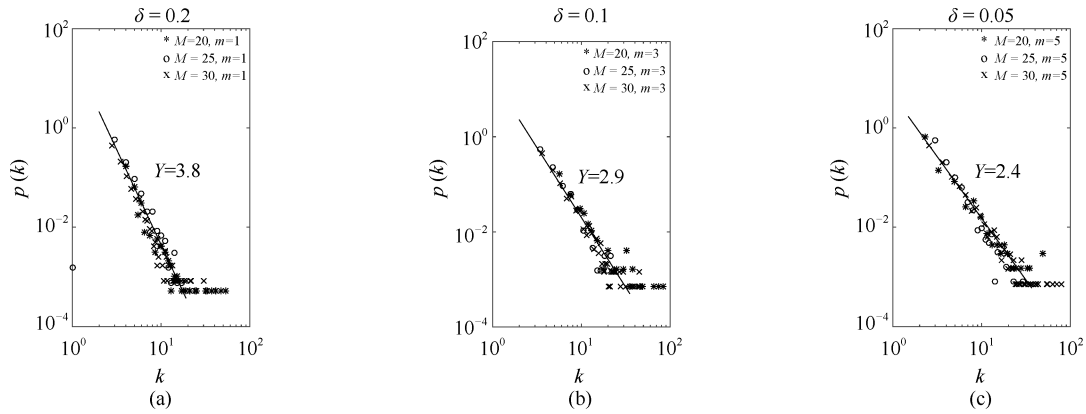


图 3 $N(t) = 10\,000$, $M = 20, 25, 30$, $m = 1, 3, 5$, 在双对数坐标下, $\delta = 0.2, 0.1, 0.05$ 的局域网络度分布比较图
 Fig. 3 The comparison of degree distribution at $\delta = 0.2, 0.1, 0.05$ of the local network, in the log-log scale, for the case that $N(t) = 10\,000$, $M = 20, 25, 30$ and $m = 1, 3, 5$

3.1 社会网络分析方法

自“9·11”事件后,许多学者利用 SNA (Social network analysis) 方法来研究恐怖组织网络,通过网络度中心度,接近中间度,中介中间度等指标来识别网络核心人物,挖掘隐藏关系,衡量节点信息传递能力,评估网络抗毁性等^[4-5, 11-12, 26-27]. 但这些指标是建立在已知网络全局信息前提下,描述节点的网络位置,重要性及信息传递能力. 对存在多个局域,且只拥有局域网络信息情况,这些指标一是不能准确反映局域中节点传递信息能力大小,传递信息多少;二是难以对不同局域中节点信息传递能力进行比较;三是随着节点数量增加,度值较小的节点增加或减少一条边,对网络拓扑变化影响微弱. 但这些节点在特殊网络中,如恐怖组织网络,往往对信息传递又起到较大作用.

3.2 网络信息中心度

在统计学,经济学和社会学中,信息被广泛运用于估算理论和数据挖掘. Stephenson 等和 Wasserman 等^[28-29] 将信息估算运用到社会网络分析中,提出信息中心度概念,认为测量一个节点传递信息的能力,是流出该节点所有路径信息的函数,并采取关联矩阵计算节点信息中心度. 与其他几个基于中介的度指标相比,信息中心度具有更加连续,对节点度变化更加敏感的特征. Morris^[30] 运用信息中心度研究网络群组级信息时,得出信息中心度更适用于反映子群或局域间信息传递能力的差异,不同子群或局域在网络中传递信息的多少应是信息中心度的函数.

在由 g 个节点组成的无向不完全图 (不含孤立点) 中,建立 $g \times g$ 的关联矩阵 A , 它的对角线元素为:

$$a_{ij} = 1 + n_i \tag{7}$$

不在对角线的元素为:

$$a_{ij} = \begin{cases} 1, & n_i \text{ 与 } n_j \text{ 相邻} \\ 0, & n_i \text{ 与 } n_j \text{ 不相邻} \end{cases} \quad (i \neq j) \tag{8}$$

那么,节点 i 的信息中心度为:

$$C(n_i) = \frac{1}{c_{ii} + (T - 2R)/g} \tag{9}$$

其中, c_{ii} 为 A^{-1} 的对角线元素, $T = \sum_{i=1}^g c_{ii}$, $R = \sum_{j=1}^g c_{ij}$. $C(n_i)$ 度量了每个节点包含信息的大小. 采取相对信息指标,将节点的信息中心度限制在 0 和 1 之间,并且和为 1.

$$C'(n_i) = \frac{C(n_i)}{\sum_i C(n_i)} \tag{10}$$

相对信息指标 $C'(n_i)$ 为节点 n_i 所控制图的整个信息流的比例. 如果某一节点的信息中心度值较大,那么其他节点就具有较小的信息中心度. 度值较大的节点,具有较强的信息传递能力.

每个时间步增添 m 条边的新节点 v , 网络 ($M = 25$) 按多局域择优增长到 10000 个节点时,局域内节点 $C'(n_i)$ 值的比较结果如图 4 所示.

从图 4 中可以得出,初始局域规模相同,较小的 m 使得局域节点的信息中心度更为集中,大量节点具有相近且较小的网络信息中心度,而少量节点的网络信息中心度较大.

对图 4 仿真结果的 $C'(n_i)$ 进行统计,如图 5 所示. x 坐标轴代表数量, y 坐标轴为 $C'(n_i)$ 值. 通过统计进一步说明局域内节点的网络信息中心度的集中与分散特征,具有较大网络信息中心度的少量节点是此局域中的核心节点. 这些少量的核心节点拥

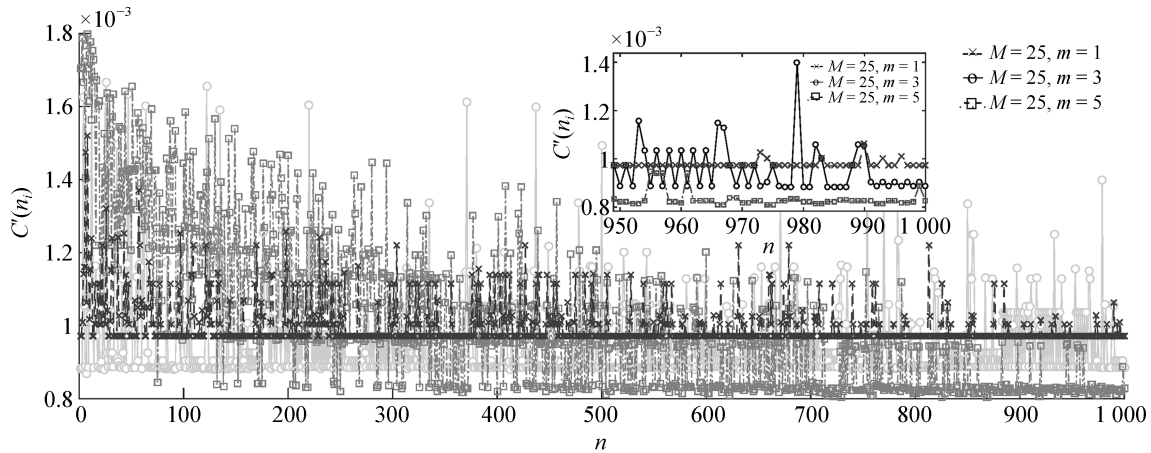


图 4 网络 ($M = 25$) 增长到 10 000 个节点时, 在 $m = 1, 3, 5$ 条件下, 局域内节点的 $C'(n_i)$ 值比较图
 Fig. 4 The comparison of $C'(n_i)$ of local network, at network ($M = 25$) growing to 10 000 nodes with $m = 1, 3, 5$

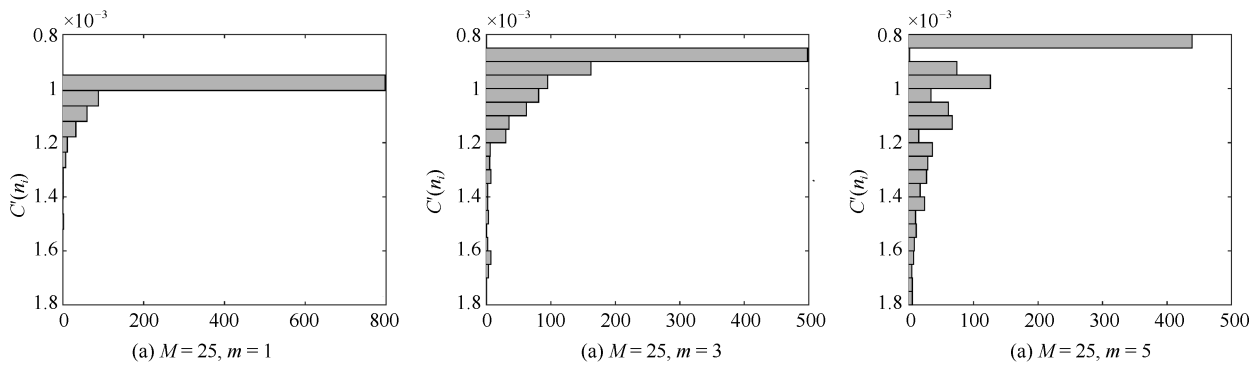


图 5 图 4 中局域在 $m = 1, 3, 5$ 条件下, $C'(n_i)$ 的仿真结果统计图
 Fig. 5 Statistical on $C'(n_i)$ in the simulation results of local network in Fig. 4, with $m = 1, 3, 5$

有较强信息传递能力, 位于局域网络的“重心”. 而大量节点具有较弱的信息传递能力, 位于网络边缘或底层.

4 基于多局域的恐怖组织网络择优增长演化模型

将新成员视为恐怖组织网络中新到达节点. 每个时间步增添 m 条边的新节点 v , 其初始恐怖主义信念水平为 A . 在时刻 t_i , v 的恐怖主义信念水平为 $A + \sum_i \Delta A$. 当 $A + \sum_i \Delta A$ 达到阈值 ρ 时, v 与网络停止连接, v 进入恐怖组织网络. 恐怖组织网络完成吸收一名新成员过程.

4.1 算法设计

步骤 1. 初始. 开始于较少节点数量 m_0 的恐怖组织网络, 按 BA 网络模型增长. 在 t_1 时刻, 网络出现子群, 将每个子群视为一个局域, 如有孤立点, 去掉孤立点. 此时所有局域共包含 M ($M \leq m_0 + t_1$) 个节点.

步骤 2. 选择局域. 按式 (1) 选择出一个局域 $L_j(t)$.

步骤 3. 按多局域择优增长. 在每个时间步, 新到来节点 v 与 $L_j(t)$ 中 m 个节点进行连接.

步骤 4. 择优. 节点 v 与 $L_j(t)$ 中节点的连接概率 π_{local} 按式 (2) 计算.

步骤 5. 计算恐怖主义信念. $\Delta A = \sum_i \alpha C'_i$ ($-1 \leq \alpha \leq 1, i \in L_j(t)$). C'_i 按式 (10) 计算.

步骤 6. 判断 α 值.

1) $-1 \leq \alpha < 0$, 局域节点 i 对 v 的感染不成功, v 的恐怖主义信念水平下降, i 与 v 断开连接, 转到步骤 7.

2) $\alpha = 0$, i 与 v 连接后其恐怖主义信念水平 A 不变. i 与 v 断开连接, 返回步骤 3.

3) $0 < \alpha \leq 1$, 局域节点 i 对 v 的感染成功, v 的恐怖主义信念增加, i 与 v 断开连接, 转到步骤 8.

步骤 7. 重新择优. 连接概率 π_{local} 受控制系数 p_f ($0 < p_f < 0.5$) 影响. v 以较小概率 $p_f \pi_{local}$ 与 i

产生连接, 与其他节点以概率 $(1 - p_f)\pi_{local}$ 连接, 返回步骤 5. 若在时间 τ , $A < \rho$, 恐怖组织网络放弃新节点 v , 认为其很难发展成为恐怖分子, 不再与 v 产生联系.

步骤 8. 强化择优. 在 t_{i+1} , v 以较大概率 $(1 - p_f)\pi_{local}$ 与 i 产生连接, 与其他节点以概率 $p_f\pi_{local}$ 连接. 若在时间 τ , $A \geq \rho$, 视 v 的恐怖主义信念达到要求, v 被吸收进恐怖组织网络, 成为恐怖分子, 并与恐怖组织网络建立牢固连接. 恐怖组织网络完成一次增长.

4.2 实例仿真

对 Krebs^[4], Memon 等^[7] 收集并绘制的“9·11”劫机事件, 马德里火车站连环爆炸案, 伦敦地铁爆炸案的恐怖组织网络数据进行仿真. 各恐怖组织网络局域划分如表 1~3 所示.

表 1 “9·11” 恐怖组织网络局域划分
Table 1 The division on local network of “9·11” Terrorist Network

$L_j(t)$	δ
5	0.263
4	0.211
5	0.263
5	0.263

进行演化. 根据节点的网络信息中心度值大小, 并剔除孤立节点后, 其择优增长演化过程如图 6~8 所示.

表 2 伦敦爆炸案恐怖组织网络局域划分
Table 2 The division on local network of London bombing terrorist network

$L_j(t)$	δ
5	0.106
7	0.149
7	0.149
10	0.213
18	0.383

表 3 马德里火车站爆炸案恐怖组织网络局域划分
Table 3 The division on local network of Madrid train bombings terrorist network

$L_j(t)$	δ
4	0.06
4	0.06
6	0.09
10	0.149
11	0.164
13	0.193
19	0.284

各恐怖组织网络按基于多局域的择优增长模型

恐怖组织网络中信息中心度值较大节点接近网

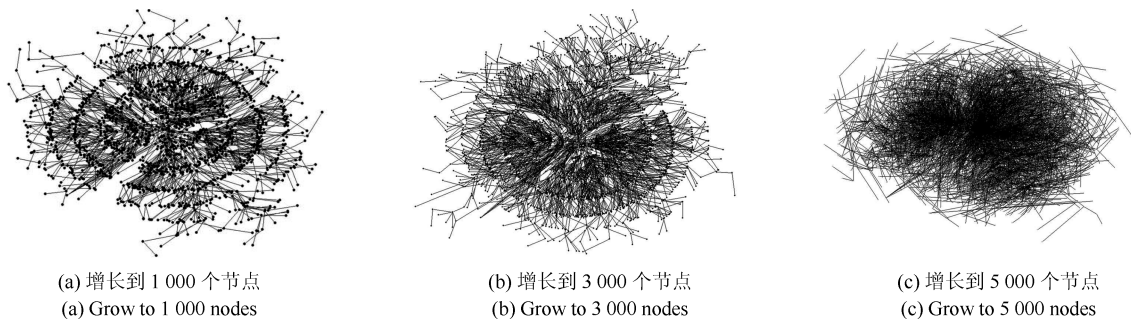


图 6 “9·11” 恐怖组织网络择优增长演化过程

Fig. 6 Preferential-growing evolution of “9·11” terrorist network

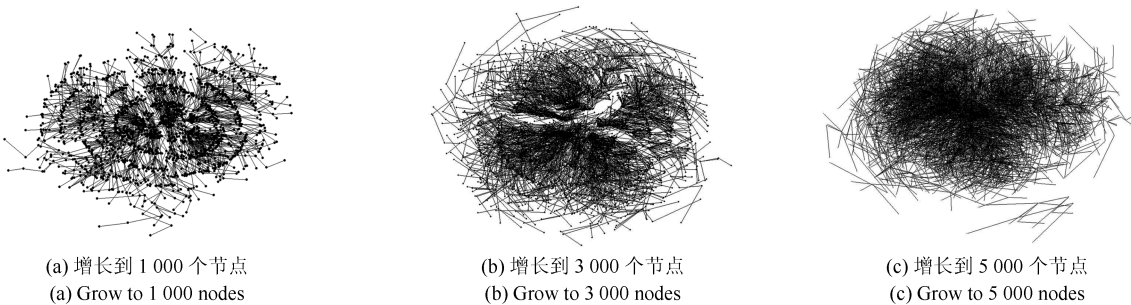


图 7 伦敦爆炸案恐怖组织网络择优增长演化过程

Fig. 7 Preferential-growing evolution of London bombing terrorist network

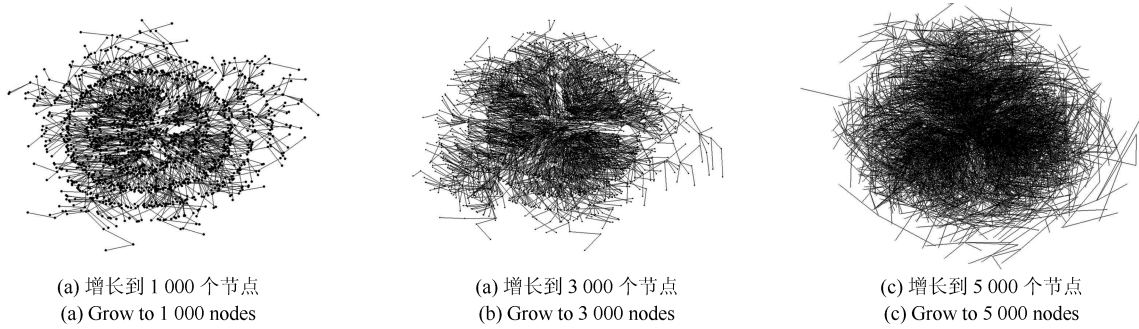


图 8 马德里火车站爆炸案恐怖组织网络择优增长演化过程

Fig. 8 Preferential-growing evolution of Madrid train bombings terrorist network

络中心, 度值较小节点靠近网络边缘. 图 6(a), 图 7(a), 图 8(a) 为网络增长到 1 000 个节点, 此时网络呈现较为明显的 3 层环状布局; 图 6(b), 图 7(b), 图 8(b) 为网络增长到 3 000 个节点, 大量节点聚集在网络信息中心度值大的节点周围; 图 6(c), 图 7(c), 图 8(c) 为网络增长到 5 000 个节点, 聚集在信息中心度值大的节点周围趋势更为明显. 通过实验可以得出信息中心度值大的节点被识别为恐怖组织的核心成员, 而大量度值较小的节点, 即“守门人”或新进节点, 位于恐怖组织的底层或边缘.

从图 9~11 可以得出, 恐怖组织网络在择优增长过程中, 各局域网络的度分布仍服从幂律分布, 其幂律指数 γ 随局域规模增长而增长. 通过对比 γ 值可以得出, 较大 δ 的局域随时间推移拥有较大的累积优势, 即较大 δ 的局域具有较强的增长能力, 其“竞争力”较强, 网络无尺度特性更明显, 局域内节点间关系也更为紧密.

图 12~14 为基于多局域择优增长模型中, 三个恐怖组织网络节点的 $C'_i(n_i)$ 值在网络增长到不同时刻的统计对比图. x 轴为节点数量, y 轴为节点

$C'_i(n_i)$ 值.

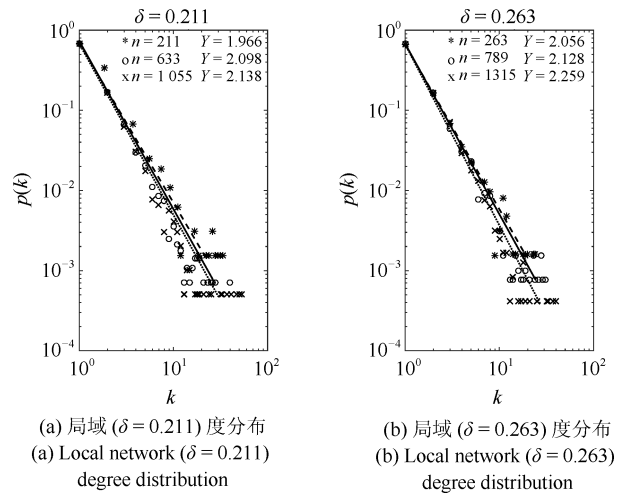


图 9 在双对数坐标下, 基于多局域的“9-11”恐怖组织网络择优增长模型中局域度分布对比图

Fig. 9 In the log-log scale, the comparison of local network degree distribution of “9-11” terrorist network based on multi-local-network preferential-growing model

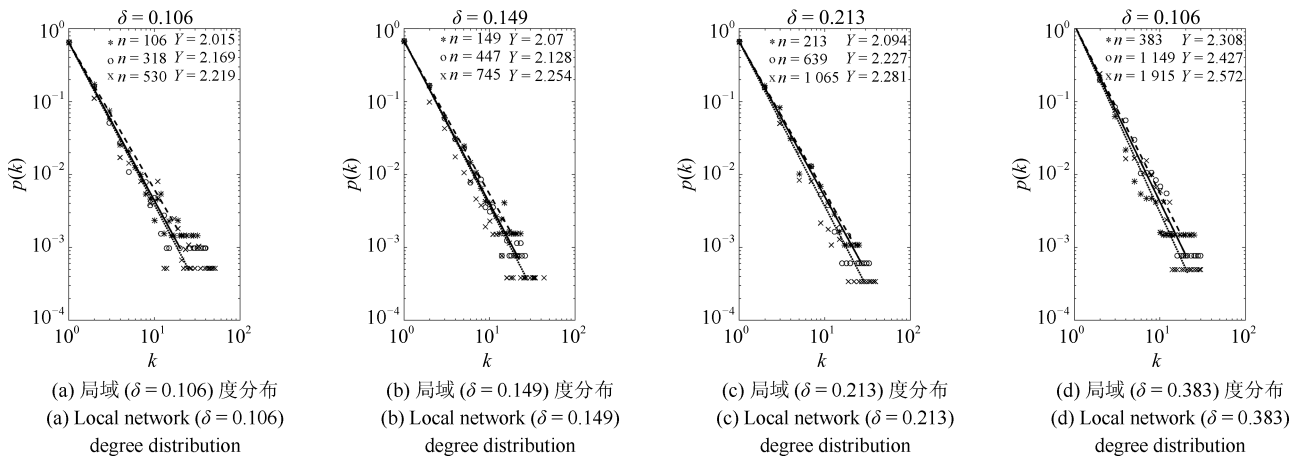


图 10 在双对数坐标下, 基于多局域的伦敦爆炸案恐怖组织网络择优增长模型中局域度分布对比图

Fig. 10 In the log-log scale, the comparison of local network degree distribution of London bombing terrorist network based on multi-local-network preferential-growing model

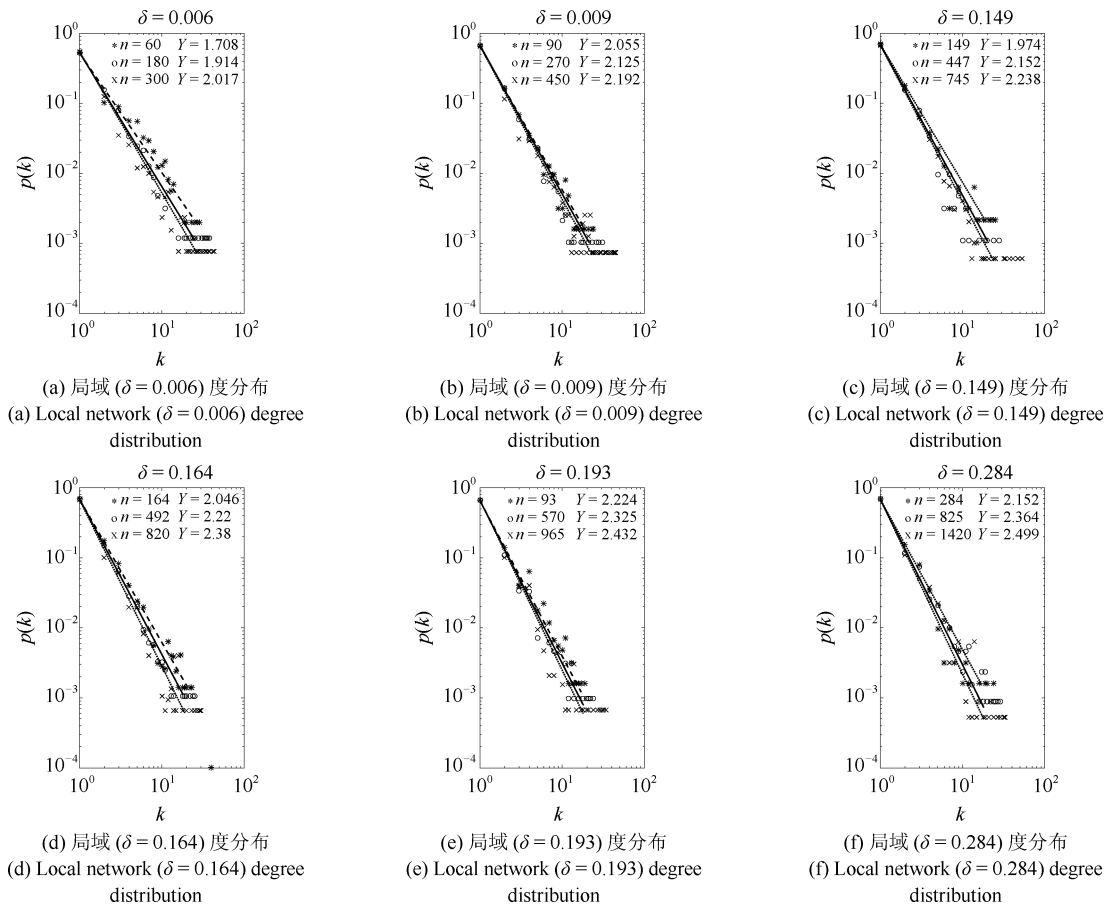


图 11 在双对数坐标下, 基于多局域的马德里火车站爆炸案恐怖组织网络择优增长模型中局域度分布对比图
Fig. 11 In the log-log scale, the comparison of local network degree distribution of Madrid train bombings terrorist network based on multi-local-network preferential-growing model

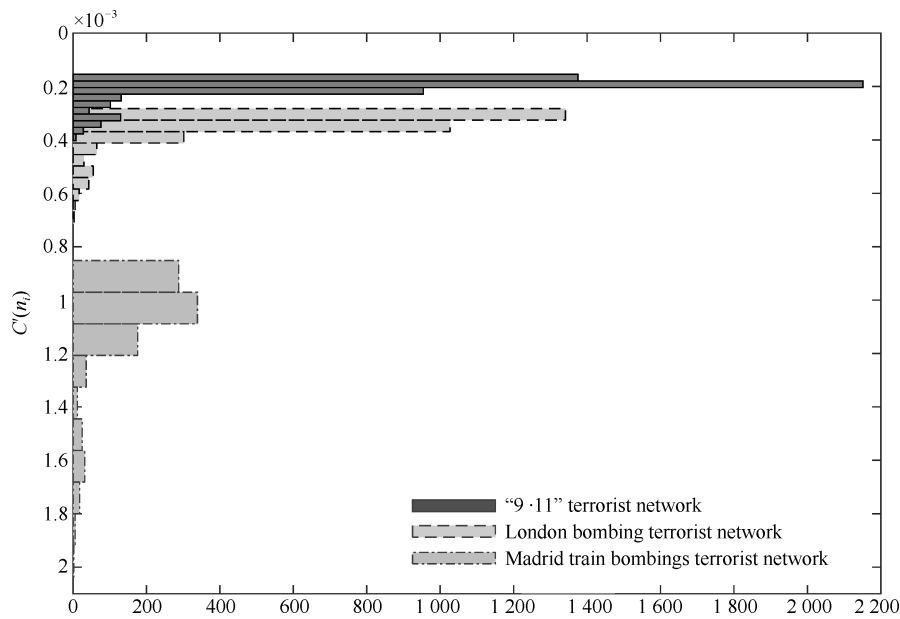


图 12 三个恐怖组织网络演化到 1000 个节点时, $C'_i(n_i)$ 统计对比图
Fig. 12 The statistical comparison of $C'_i(n_i)$, with the three terrorist networks having grown to 1000 nodes

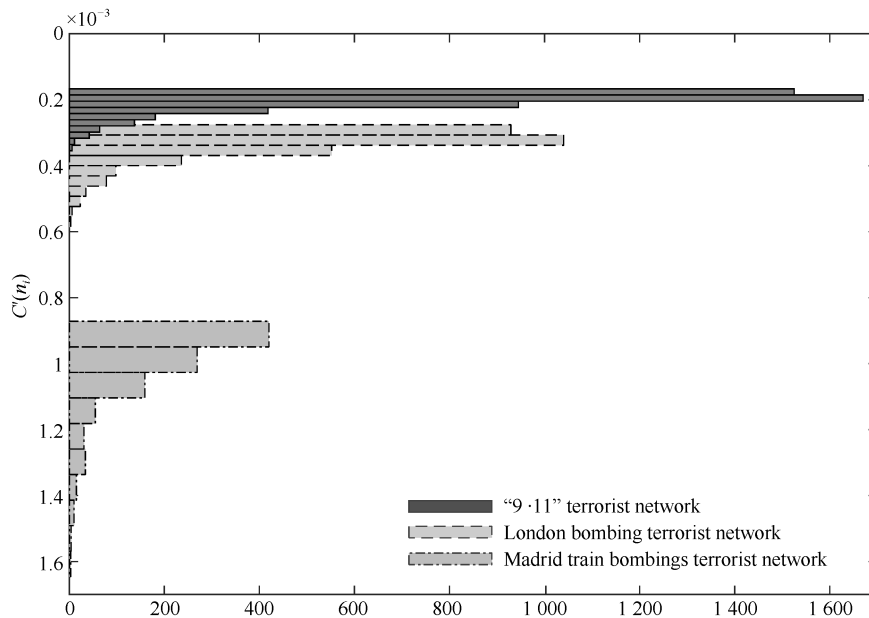


图 13 三个恐怖组织网络演化到 3000 个节点时, $C_i'(n_i)$ 统计对比图

Fig. 13 The statistical comparison of $C_i'(n_i)$, with the three terrorist networks having grown to 3000 nodes

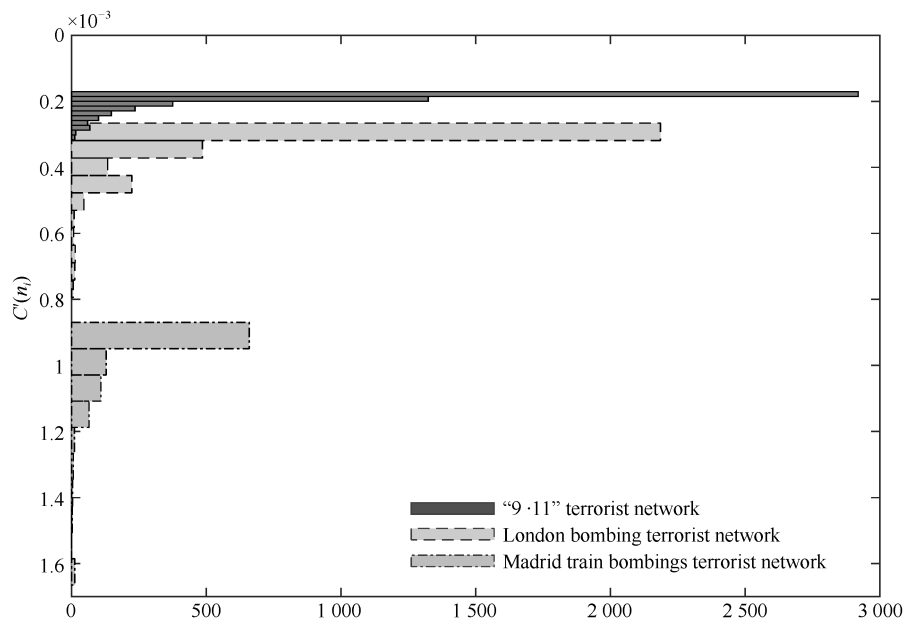


图 14 三个恐怖组织网络演化到 5000 个节点时, $C_i'(n_i)$ 统计对比图

Fig. 14 The statistical comparison of $C_i'(n_i)$, with the three terrorist networks having grown to 5000 nodes

从图 12~14 结果可以得出随着时间的推移, 虽然有更多的新节点进入恐怖组织网络, 但大量节点的网络信息中心度分散在较小的值, 这些节点在模型演化结果中位于网络的底层或边缘. 而具有少量的节点的信息中心度集中在较大的值, 这些少量节点是恐怖组织网络的核心成员, 位于网络的“重心”. 说明恐怖组织网络节点的信息中心度具有集中与分散的特征. 并且随着网络不断增长, 拥有远高于平均

信息中心度值的少量节点数量也在缓慢增加, 说明恐怖组织网络核心成员数量也是随网络规模增长而不断增加的.

5 结论

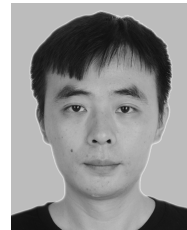
恐怖组织网络时空演化规律是当前反恐领域研究的热点与难点问题. 预防与打击恐怖活动并不能从根本上消亡恐怖组织, 而遏制恐怖组织增长, 找寻

网络增长的动力, 才是瓦解恐怖组织的重要途径. 本文从复杂网络研究出发, 发现新节点进入恐怖组织网络是在拥有网络局部信息条件下进行的择优, 提出了基于多局域的恐怖组织网络择优增长演化模型. 通过实验验证了模型各局域的度分布仍服从幂律分布. 其次, 利用节点网络信息中心度指标衡量个体恐怖主义信念水平, 动态描述了新节点进入网络的过程, 并发现网络演化过程中节点的网络信息中心度具有集中与分散特征. 最后, 对“9·11”等恐怖组织网络按模型进行仿真, 验证了该模型的有效性与准确性. 本文研究结果对遏制恐怖组织发展, 预防恐怖事件发生, 消除恐怖组织具有一定的指导意义和参考价值.

References

- Cheng Cong-Hui, Guo Jun-Hua. Challenges and prevention of cyberterrorism. *Journal of Intelligence*, 2015, **34**(3): 10–15, 20
(程聪慧, 郭俊华. 网络恐怖主义的挑战及其防范. 情报杂志, 2015, **34**(3): 10–15, 20)
- Stripling M. Embodying terror networks: How direction creates structure [Online], available: <http://www.crisisville.com/files/Terrorism-DirectedNetworks.pdf>, January 8, 2013.
- Moon I C, Carley K M. Modeling and simulating terrorist networks in social and geospatial dimensions. *IEEE Intelligent Systems*, 2007, **22**(5): 40–49
- Krebs V E. Mapping networks of terrorist cells. *Connections*, 2002, **24**(3): 43–52
- Krebs V E. Uncloaking terrorist networks. *First Monday*, 2002, **7**(4): 1–4
- Memon N, Hicks D L, Harkiolakis N, Rajput A Q K. Retracted: Small world terrorist networks: a preliminary investigation. *Applications and Innovations in Intelligent Systems XV*. London: Springer, 2008. 339–344
- Memon N, Larsen H L, Hicks D L, Harkiolakis N. Retracted: detecting hidden hierarchy in terrorist networks: some case studies. In: *Proceedings of the 2008 International Conference on Intelligence and Security Informatics*. Taipei, China: Springer-Verlag, 2008. 477–489
- Memon N, Larsen H L. Practical Approaches for analysis, visualization and destabilizing terrorist networks. In: *Proceedings of the First International Conference on Availability, Reliability and Security*. Vienna, Austria: IEEE, 2006. 435–448
- Will U K, Memon N, Karampelas P. Detecting new trends in terrorist networks. In: *Proceedings of the 2010 International Conference on Social Networks Analysis and Mining*. Odense, Denmark: IEEE, 2010. 435–440
- Enders W, Su X J. Rational terrorists and optimal network structure. *Journal of Conflict Resolution*, 2007, **52**(1): 33–57
- Carly K M. Dynamic network analysis for counter-terrorism [Online], available: https://www.researchgate.net/publication/228770516_Dynamic_network_analysis_for_counter-terrorism, January 7, 2017.
- Carly K M. Destabilization of covert networks. *Computational and Mathematical Organization Theory*, 2006, **12**(1): 51–56
- Bi Zhen-Kun, Zhang Wei, Yu Hao-Miao, Chen Yun-Fang. Organizational structure discovery in terrorist networks based on cut Set and hierarchical method. *Journal of Nanjing University of Posts and Telecommunications (Nature Science)*, 2014, **34**(5): 111–118
(毕震坤, 张伟, 余浩淼, 陈云芳. 恐怖网络中基于节点割集分层的组织结构发现方法. 南京邮电大学学报(自然科学版), 2014, **34**(5): 111–118)
- Zhang Hai, Sun Duo-Yong. Study on the terrorist covert networks from the perspective of social network analysis. *Journal of Safety and Environment*, 2011, **11**(3): 259–264
(张海, 孙多勇. 基于社会网络理论的恐怖组织隐蔽网络分析方法. 安全与环境学报, 2011, **11**(3): 259–264)
- Li Ben-Xian, Ling Yun-Xiang, Fang Jin-Qing, Mei Jian-Ming. How to map the network of terrorism group. *Complex Systems and Complexity Science*, 2016, **13**(1): 68–73
(李本先, 凌云翔, 方锦清, 梅建明. 恐怖组织如何编制网络. 复杂系统与复杂性科学, 2016, **13**(1): 68–73)
- Li Ben-Xian, Li Meng-Jun, Fang Jin-Qing, Yang Jin-Xin. Empirical study on spatiotemporal evolution of terrorism organization network. *Acta Automatica Sinica*, 2013, **39**(6): 772–779
(李本先, 李孟军, 方锦清, 仰璉歆. 恐怖组织网络的时空演化规律. 自动化学报, 2013, **39**(6): 772–779)
- Li Ben-Xian, Jiang Cheng-Jun, Fang Jin-Qing. Network science's challenges and opportunities in counter-terrorism research. *Complex Systems and Complexity Science*, 2014, **11**(1): 60–66
(李本先, 江成俊, 方锦清. 网络科学在反恐研究中面临的挑战和机遇. 复杂系统与复杂性科学, 2014, **11**(1): 60–66)
- Li Ben-Xian, Fang Jin-Qing, Jiang Cheng-Jun, Mei Jian-Ming, Chi Yan. Psychology and dynamical analysis of terrorism organization: from individual to group. *Complex Systems and Complexity Science*, 2014, **11**(2): 87–94
(李本先, 方锦清, 江成俊, 梅建明, 迟妍. 恐怖组织网络的心理学与动力学分析: 从个体到群体. 复杂系统与复杂性科学, 2014, **11**(2): 87–94)
- Xu Qing, Zu Zheng-Hu, Zheng Tao. Empirical study of terrorist organizations network. *Journal of Hefei University of Technology (Natural Science)*, 2010, **33**(2): 242–244, 292
(许晴, 祖正虎, 郑涛. 恐怖组织网络的实证研究. 合肥工业大学学报(自然科学版), 2010, **33**(2): 242–244, 292)
- Sun Duo-Yong, Li Wen-Ju, Fu Ju-Lei, Li Bo. On the factors leading to terror attacks based on the agent simulation analysis approach. *Journal of Safety and Environment*, 2013, **13**(5): 259–264
(孙多勇, 李文举, 付举磊, 李博. 基于 Agent 建模的恐怖袭击影响因素仿真分析. 安全与环境学报, 2013, **13**(5): 259–264)
- Lange S, Donges J F, Volkholz J, Kurths J. Local difference measures between complex networks for dynamical system model evaluation. *PLoS One*, 2015, **10**(4): Article No. e0129413

- 22 Li B, Sun D Y, Zhu R Q, Li Z. Agent based modeling on organizational dynamics of terrorist network. *Discrete Dynamics in Nature and Society*, 2015, **2015**: Article No. 237809
- 23 Gaharwar R D, Shah D B. Application of centrality principles for terrorist network role analysis. *International Journal of Scientific Research in Science and Technology*, 2018, **4**(2): 1216–1221
- 24 Barabási A L, Albert R. Emergence of scaling in random networks. *Science*, 1999, **286**(5439): 509–512
- 25 Barabasi A L. *Linked: The New Science of Networks*. Cambridge, MA: Perseus, 2002.
- 26 Michalak T P, Rahwan T, Skibski O, Wooldridge M. Defeating terrorist networks with game theory. *IEEE Intelligent Systems*, 2015, **30**(1): 53–61
- 27 Husslage B, Borm P, Burg T, Hamers H, Lindelauf R. Ranking terrorists in networks: a sensitivity analysis of Al Qaeda's 9/11 attack. *Social Networks*, 2015, **42**: 1–7
- 28 Aitkin M, Vu D, Francis B. Statistical modelling of a terrorist network. *Journal of the Royal Statistical Society*, 2017, **180**(3): 751–768
- 29 Penzar D, Srbljinovic A. About modeling of complex networks with applications to terrorist group modeling. *Interdisciplinary Description of Complex Systems*, 2005, **3**(1): 27–43
- 30 Li X, Chen G R. A local-world evolving network model. *Physica A: Statistical Mechanics and its Applications*, 2003, **328**(1–2): 274–286
- 31 Qin S, Dai G Z. A new local-world evolving network model. *Chinese Physics B*, 2009, **18**(2): 383–390
- 32 Arquilla J, Ronfeldt D F. *Networks and Netwars: the Future of Terror, Crime, and Militancy*. California: Santa Monica, 2001. 20–24
- 33 Bohannon J. Counter terrorism's new tool: "metanetwork" analysis. *Science*, 2009, **325**(5939): 409–411
- 34 Wasserman S, Faust K. *Social Network Analysis: Methods and Applications*. London: Cambridge University Press, 1994. 125–245
- 35 Stephenson K, Zelen M. Rethinking centrality: methods and examples. *Social Networks*, 1989, **11**(1): 1–37
- 36 Morris M. *Networks and Diffusion: An Application of Loglinear Models to the Population Dynamics of Disease*. Chicago: Dissertation Department of Sociology, 1989. 110–126
- 37 Gill P, Corner E, Conway M, Thornton A, Bloom M, Horgan J. Terrorist use of the internet by the numbers. *Criminology & Public Policy*, 2017, **16**(1): 99–117
- 38 Gaharwar R D, Shah D B, Gaharwar G K S. Terrorist network mining: issues and challenges. *International Journal of Advance Research in Science and Engineering*, 2015, **4**(1): 33–37
- 39 Zhang Jiang-Xing. An analysis of the features of global terrorist activities from 1970 to 2013 — a comparison of those before and after Sept. 11. *Journal of Tongji University (Social Science Section)*, 2016, **27**(2): 48–57
(张将星. 1970–2013 年全球恐怖主义活动的特征分析 — 兼论“9·11”事件前后时段比较. 同济大学学报(社会科学版), 2016, **27**(2): 48–57)



何晶 武警警官学院部队管理系讲师。主要研究方向为复杂网络与复杂系统, 反恐怖。本文通信作者。

E-mail: maxhe_PAP@163.com

(HE Jing Lecturer in the Department of Military Management, Officers College of PAP. His research interest covers complex networks and complex systems and counter-terrorism. Corresponding author of this paper.)



李本先 武警警官学院部队管理系副教授。主要研究方向为社会网络分析, 反恐怖。E-mail: libenxianxian@163.com

(LI Ben-Xian Associate professor in the Department of Military Management, Officers College of PAP. His research interest covers social network analysis (SNA) and counter-terrorism.)