

# 基于级联效应的恐怖组织网络抗毁性研究

李本先, 李孟军, 孙多勇

国防科学技术大学信息系统与管理学院, 长沙 410073

**摘要** 应用动态社会网络方法分析了恐怖组织的网络结构及抗毁性, 并对其网络进行了选择性的攻击。首先对其人员网络进行攻击, 先从中间层进行打击, 再根据网络的中心性实施攻击; 其次应用图论中求最小割集的方法寻找其行动网络的脆弱性, 对其增广链实施攻击。与传统的打击方法相比, 该方法具有更强的优越性, 恐怖组织的整体网络更容易被破坏。

**关键词** 恐怖组织网络; 攻击策略; 扰动; 抗毁性; 中心性

**中图分类号** E87

**文献标志码** A

**doi** 10.3981/j.issn.1000-7857.2013.11.001

## Invulnerability of Terrorism Organization Network Based on Cascade Effect

LI Benxian, LI Mengjun, SUN Duoyong

School of Information System and Management, National University of Defense Technology, Changsha 410073, China

**Abstract** A dynamic society network analysis method is adapted to study terrorism organization structure and its invulnerability. Firstly, a selective attack method is proposed to destroy terrorism organization network. Secondly, the mesosphere is attacked, and then other segments are attacked according to the degree-distribution centralities of network. The minimal-cut set of graph theory is applied to scout the terrorism network of invulnerability and attack its augmentable chain. The experimental results show that these methods precede traditional attacking methods. It is easy to destroy the entire terrorism organization network.

**Keywords** terrorism organization network; attack strategy; dismantle; invulnerability; centrality

### 0 引言

网络的级联与抗毁性研究是复杂网络的一个重要课题<sup>[1]</sup>。在诸多的复杂网络中, 恐怖组织网络是一种特殊的网络, 其网络结构是一个复杂的自适应系统, 由许多单元组成, 系统中的各元素构成复杂网络, 是节点之间有着复杂连接关系的有组织犯罪网络<sup>[2]</sup>, 其网络结构既非完全规则也非完全随机, 但具有其内在的自组织规律。在各种外部因素的影响下, 网络节点之间不断进行着同步运动。对恐怖组织的网络结构及其抗毁性进行研究, 找到恐怖组织网络的脆弱点, 削弱其建立链接的力量, 具有重要意义。

针对恐怖主义网络的特点及抗毁性问题, Memon 等<sup>[3]</sup>对 9·11 事件中恐怖组织的网络结构进行了分析, 发现隐蔽的恐怖组织网络具有小世界特性, 并提出了扰动网络的方法。Stripling<sup>[4]</sup>对其他恐怖组织网络进行了研究, 发现恐怖组织的隐蔽网络具有无标度特性, 其幂律分布服从  $p(k) \sim k^{-\gamma}$ 。针对这

些特点, 研究人员通过查找网络中最具影响力的人物并设法消除他们, 使信息流动变慢, 致使其网络功能弱化, 从而破坏整个网络<sup>[5]</sup>。这一方法能对恐怖组织的网络造成干扰, 但也存在两个问题: 一是忽视了在网络中真正起关键作用的幕后人物; 二是设定网络是静态网络, 只有简单不变的隶属和交往关系。Carley 等<sup>[6]</sup>研究了如何有效打击暗藏的恐怖组织网络, 并开发了相关的动态仿真软件 ORA。研究过程中充分考虑恐怖组织网络的动态性, 弥补了许多静态网络方法分析中通过改变节点扰动网络的缺点<sup>[7,8]</sup>。Bohannon<sup>[9]</sup>也提出元网络分析法是研究恐怖组织网络的一个重要工具。

以上这些方法主要根据恐怖组织网络的中心度分布特点, 打击恐怖组织的首脑人物, 从而摧毁整个网络, 这一方法在短期内对恐怖组织的攻击具有明显的效果。但现实情况是恐怖组织具有自组织性、自适应性、耦合性、自适应性等, 恐怖组织网络能在较短的时间内迅速恢复, 新的领导人将会接

收稿日期: 2012-12-07; 修回日期: 2013-01-31

基金项目: 国家自然科学基金项目(70973138)

作者简介: 李本先, 博士研究生, 研究方向为系统优化与综合集成, 电子信箱: 13687314764@163.com; 李孟军(通信作者), 教授, 研究方向为系统优化与综合集成, 电子信箱: mjli1260744@sina.com

替旧的领导人,网络会自动修复<sup>[10]</sup>。另外,当把组织的人员结构网络摧毁后,某一个孤立的恐怖分子或群体得到足够的资源与信息,也可按照原定计划发动一定规模的恐怖事件。

本文构建恐怖组织的人员与行动网络模型,并对其人员及行动网络进行分析,对人员网络中的网络节点的重要性进行评估,对其网络的抗毁性进行研究。从恐怖组织网络的中间层选择多个中心节点同时进行打击,去除网络中足够多的中心节点,到达崩溃的临界点,从而破坏网络。根据网络的实际变化情况进行逐步消除,打击过程中不但考虑组织人员的变动关系,而且从整体网络出发,考虑其人员、资源、信息等因素,寻找恐怖组织整体网络中的最小割集,找到恐怖组织网络的脆弱点,采用选择性攻击法对其网络进行扰动,切断其资源,促使其发生内部级联故障,从而实现摧毁其网络。

## 1 相关理论

### 1.1 恐怖组织网络抗毁性

恐怖组织网络的抗毁性,是指恐怖组织网络抗打击、抗瓦解、维持生存、实施恐怖袭击的能力,其抗毁性可以从不同角度来理解。恐怖组织网络的抗毁性包括两个方面:一是其自身网络的生存机理、动力及结构;二是对其网络进行瓦解。许多专家应用复杂网络的抗毁性原理对恐怖组织网络的抗毁性进行了研究<sup>[11]</sup>。美军在反恐战争中的实践证明,应用复杂网络来研究恐怖组织的网络结构可以为反恐提供良好的决策支持,为查明和消灭恐怖组织的头目提供重要帮助<sup>[12,13]</sup>。

针对复杂网络的抗毁性问题,Albert 等<sup>[14,15]</sup>提出了对随机网络(ER 模型)和无标度(BA 模型)进行攻击的方法,选择的方式分为随机攻击和选择性攻击两种类型,分别称为网络的容错能力和抗攻击能力。在攻击策略方面,Holme 等<sup>[16]</sup>提出了4种不同的攻击策略:(1) 度值移除策略;(2) 介数移除策略;(3) 基于重新计算的度值移除策略;(4) 基于重新计算的介数移除策略。在恐怖组织网络的抗毁性研究方面,Carpenter 等<sup>[17]</sup>提出分析其中心性,试图发现恐怖分子网络的组织结构及核心人物。

### 1.2 恐怖组织网络抗毁性测度度量

#### 1.2.1 基于中心性的算法与抗毁性测度指标

网络的脆弱性和鲁棒性通常成对出现于网络模型之中,无论是脆弱性还是鲁棒性都离不开中心节点的参与,网络的中心节点支撑着整个系统的运行,除去这些中心节点,网络系统就会立即瘫痪<sup>[18]</sup>。在恐怖组织网络中,中心性是衡量恐怖组织网络结构中关键人物及抗毁性的一个重要指标,是一种权力和声望的量化,是衡量其网络抗毁性的重要指标,对其关键性人物的打击是有效瓦解恐怖组织网络的方法。关键人物是指在恐怖组织网络中能够影响资源流动的位置的人物,他们是组织的指挥人物,或是在组织中担当重要角色,这类人物的损失将严重影响恐怖组织的运行。其考查指标主要如下。

(1) 度中心性是指与此顶点相连接的边的数量,即通过

测量某一节点与其他节点的直接连接情况来衡量行动者的活跃程度。在恐怖网络中主要用来衡量谁在这个团体中是最主要的中心人物,中心性越高,在团体中的地位就越重要。

(2) 紧密中心性是一节点到其他节点的捷径长度总和的倒数<sup>[19]</sup>,主要反映恐怖组织网络中某人到达其他成员的容易程度。接近中心度高的行动者在信息传播上具有绝对优势,能以最快的速度在组织内部传达信息,但不一定处于网络的核心。

如果恐怖组织网络的群体是某一核心人物形成的星形结构网络(图 1(a)),其紧密中心度为 1;而在环形结构网络中,所有行动者的紧密中心度相等,均为 0.5(图 1(b))。

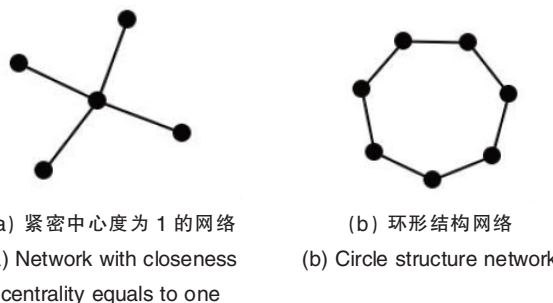


图 1 两种特殊的网络结构

Fig. 1 Two special network structures

(3) 介数中心性是衡量个体作为媒介者的能力。在恐怖组织网络中,某个指标的介数中心度越高,就有越多的人通过他进行联络,起这种角色作用的人物称为看门人或经纪人<sup>[8]</sup>。看门人在信息、资源交换等方面的作用尤其突出,作为打击的重要对象,除去看门人将使恐怖组织单元间失去联系,从而起到瓦解恐怖组织网络的作用。

(4) 效率是描述网络结构的特征参数之一,主要用来表征网络中信息的扩散和控制<sup>[16,20]</sup>。

(5) 特征向量中心性,主要用来衡量网络中一个节点的重要性,这既取决于其邻居节点的数量,也取决于其邻居节点的重要性。在恐怖组织网络中,特征向量反映了网络中的重要结点对邻居节点的影响力及信息传输能力。

通过上述指标来研究恐怖组织的恐怖特性,度中心性、紧密中心性、介数中心性、效率、特征向量中心性的度量公式分别为

$$C_d = \frac{d(n_i)}{n-1} \quad (1)$$

$$C_c = \frac{\sum_{i=1}^n (C_{\max} - C_{ci})}{(n-2)(n-1)} (2n-3) \quad (2)$$

$$C_b(x) = \frac{\sum_{j \neq i} g_{jk}(n_j)}{[(n-1)(n-2)/2]} \quad (3)$$

$$D_c = \frac{1}{n(n-1)} \sum_{i \neq j \in C} \frac{1}{d_j} \quad (4)$$

$$C_c(i) = \lambda^{-1} \sum_{j=1}^n a_{ij} x_j \quad (5)$$

其中,  $n$  为节点总数,  $n-1$  表示最大可能的节点数;  $C_{\max}$  为最大相对紧密中心度;  $C_{ci}$  为其他结点的中心度;  $g_{ik}$  为节点  $j$  和  $k$  之间存在的短程线数目,  $g_{ik}(n_j)$  为包含行动者  $n_i$  的两个行动者之间的短程线数目;  $d_{ij}$  为通过节点  $i$  到达节点  $j$  的最小边数;  $\lambda$  为特征值;  $a_{ij}$  为网络的邻接矩阵;  $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ 。

### 1.2.2 基于边割集的测度

在连通图  $G(V, E)$  中, 对于任意两个不相交的非空顶点子集  $P$  和  $Q$ , 用  $[P, Q]G$  表示  $G$  中所有两端分别在  $P$  和  $Q$  中的边的集合。特殊情况下, 对  $G$  的任一非空顶点真子集  $S \subset V$  及  $\bar{S} = V \setminus S$ , 称  $G$  的边子集  $[S, \bar{S}]$  为  $G$  的边割, 见图 2。

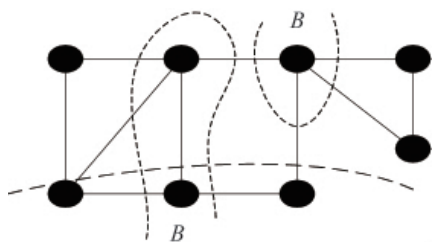


图 2 图  $G$  的边割

Fig. 2 Edge cut of graph  $G$

在图 2 中, 3 条连续的虚线分别对图进行了切割, 这时使  $\omega(G-B) = \omega(G) + 1$  成立的极小子集  $B$ , 称为  $G$  的割集。在这种情况下, 其完整度  $i(G) = \min\{|S| + \tau(G-S) : S \in C(G)\}^{[20]}$ , 其中  $\tau(G-S)$  为最大分支的边数,  $C(G)$  为  $G$  的所有边割集组成的集合,  $|S|$  为边割集  $S$  中边的个数。可以看出, 一个图的完整度越大, 则它所对应的网络抗破坏能力越强。

假设  $M_T$  是一个有  $n$  个成员的恐怖组织网络,  $C(M_T, k)$  为有序集  $M_T$  由  $k$  个成员组成的割集的数量,  $P(M_T, k)$  为当  $k$  个成员被逮捕时  $M_T$  被破坏的概率。则当  $k$  个成员被捕后, 恐怖组织网络  $M_T$  被破坏的概率为

$$P(M_T, k) = \frac{C(M_T, k)}{\binom{n}{k}} = \frac{\binom{n}{k-1}}{\binom{n}{k}} \quad (6)$$

其中, 对任意正整数  $k$  来说,  $k! = k(k-1)(k-2) \cdots 3 \cdot 2 \cdot 1$ 。

## 2 恐怖组织整体网络结构分析

恐怖组织的整体网络主要由两部分构成: 一部分是由组织内部成员构成的人员组织网络, 另一部分是由人员、资源等要素构成的行动网络。

### 2.1 组织网络结构

恐怖分子是恐怖主义研究的基本单位, 由恐怖分子组成的有机结合结构就是恐怖组织。恐怖组织实施袭击的有效性

很大程度上取决于组织的结构, 组织结构不是单个恐怖分子简单相加在一起的合成物, 其内部单元结构见图 3。

图 3 中, 处于最顶端的节点 ( $A, B, C$ ) 表示头目, 负责恐怖组织的指挥与控制; 一线恐怖分子用最底端的节点 ( $I, J, K$ ) 表示; 连接头目和一线恐怖分子的节点称为中间层节点, 他们是恐怖组织的骨干分子, 是恐怖头目与一线恐怖分子的联络人, 负责执行恐怖组织的各种任务。其中  $C, E, F, J$  形成一条极大链, 从最高等级到最低等级的序列为  $C, E, F, J$ 。

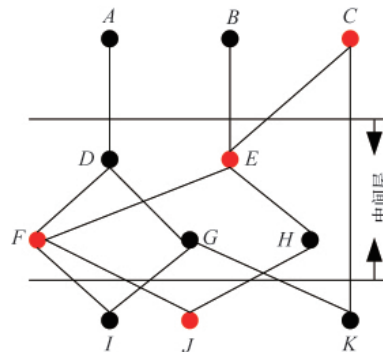


图 3 恐怖组织内部的一个结构单元

Fig. 3 One structural cell of terrorism organization inside network

恐怖组织的关系结构表示恐怖组织内部成员之间和恐怖组织内部与外部之间的关系结构。Penzar 等<sup>[21]</sup>对 9·11 事件后的恐怖组织网络进行了研究, 认为目前恐怖组织的网络结构主要有 3 种形式——指数分布式、全息等级结构式、均匀分布式, 见图 4。

图 4 是具有相同结点数, 密度不同的 3 种网络结构形式, 其中圆点表示恐怖分子, 边表示其连接关系。这 3 种结构几乎概括了当前大多数恐怖组织的网络结构特点。图 4(a) 为指数分布式随机网络。指数分布式是当前恐怖组织生存的主要结构, 整个组织结构由不同核心的领导人指挥, 每个领导人下面又分为不同的集团, 核心群体之间联系紧密, 单独的某一群体也可以构成一个微小的作战单元, 可以灵活地发动一定规模的恐怖行动。图 4(b) 为全息等级结构式网络模型。在恐怖组织网络中, 全息等级结构是最为传统的结构形式, 这种结构具有严格的等级制度, 高层领导人直接负责指挥与控制整个网络, 信息流动速度较快, 分工严密。图 4(c) 为均匀分布式网络模型。与全息结构及指数分布式相比, 均匀分布式的整个网络结构更为分散, 个体与个体之间的联系更加紧密, 核心群体较小, 自组织能力较强, 受到攻击时, 网络的受损面较小, 能在较短的时间内恢复; 但这种组织结构形式, 资源相对分散, 不容易发动大规模的恐怖袭击, 群体之间的作战能力远没有均匀分布式或指数分布式强, 缺乏较强的指挥与控制人物。

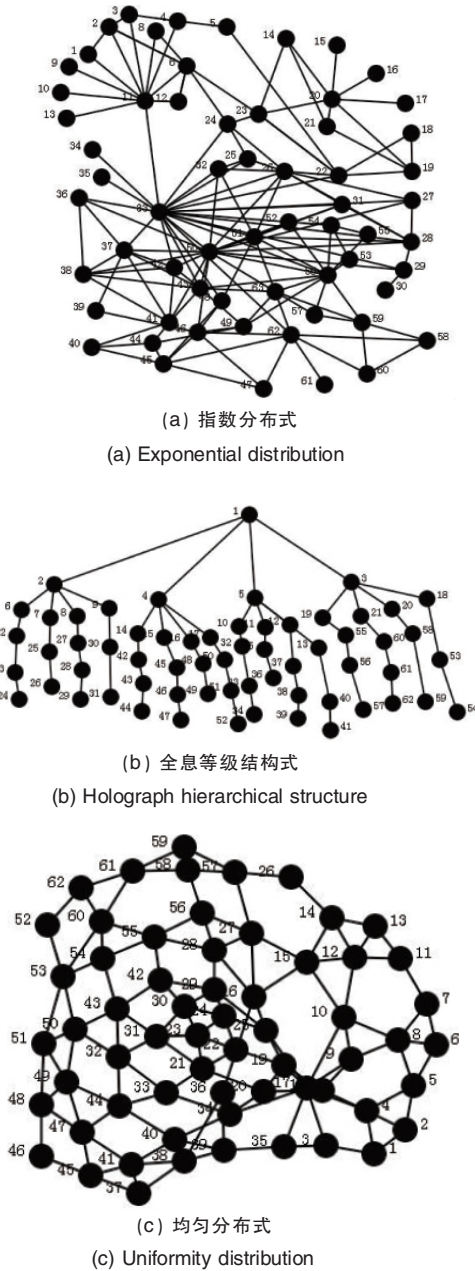


图 4 3 种类型的恐怖组织网络结构  
Fig. 4 Three-typed structures of terrorism organization

## 2.2 行动网络模型

### 2.2.1 行动结构分析

恐怖组织作为一种实体,有其独特的目标、结构、管理、资金筹集等内容,而这些内容超越恐怖分子个体之外。在策划一定规模的恐怖袭击时,群体间必须时常保持联系,筹集一定的资源(资金、武器等),交流计划,分配任务,分头执行。其行动可以抽象为恐怖主体(人)、知识、资源、任务。此模型可用一个二元组来描述—— $\langle \text{Agent}, \text{环境}(E) \rangle$ ,利用 Agent 网络来模拟恐怖组织中人员的学习、行动、参与事务、完成任务等行为,模拟组织和社会变化。采用多 Agent 模型组织中人员的行为建立恐怖组织的动态社会网络模型,他们之间的关系如图 5 所示。

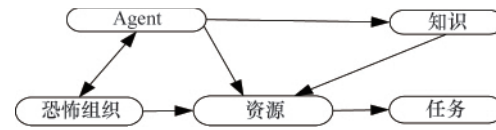


图 5 恐怖组织的语义网络  
Fig. 5 Semantics network of terrorism organization

#### (1) Agent。

图 5 中的 Agent 不仅限于内部结构的 Agent,更不是假设的单个 Agent,所有的 Agent 仅代表连接资源与任务的一个通信单元。Agent 通过交互达到交换信息的目的,交互动机影响着 Agent 选择交互对象。Agent 具有自主学习、改变信念、重新定位的能力,并通过这些过程在环境中进行调整。这一 Agent 组织模型设计主要是为了选择更适合的 Agent 模型。

恐怖组织群体是多个 Agent 的集合体,每个 Agent 只是 1 个或多个群体的一部分。在恐怖组织的基本组织内部,群体仅是紧随一系列 Agent 的一种方式,在更复杂的恐怖组织,其主要作用在于连接任务,也有可能代表更多的一般 Agent 系统,1 个 Agent 同时是  $n$  个群体中的一员,群体与个体之间可以交互,其交互关系见图 6。

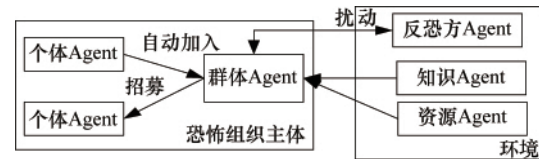


图 6 恐怖组织成员 Agent  
Fig. 6 Agent of terrorism organization members

图 6 描述了恐怖组织成员的变化过程。Agent 的状态有存活和死亡两种。恐怖组织通过招募或自动加入的方式使组织不断发展壮大,而环境对组织产生积极或消极影响。知识、资源的增加有助于恐怖组织招募到新成员,实施各种恐怖活动;另一方面,当反恐方对其进行打击时,扰动其生存网络,将会使组织中的成员死亡,甚至是被反恐方消灭。

#### (2) 环境。

环境指恐怖组织网络赖以生存的外界环境,是 Agent 的生存空间,节点 Agent 与节点 Agent 之间在环境中进行交互。本模型中的环境主要指资源、任务、知识。环境可用一个三维坐标和坐标上的  $k$  个函数值表示,即环境  $(E) = (x, y, z, f_1(x, y, z), f_2(x, y, z), \dots, f_k(x, y, z))$ ,  $x \in \mathbf{R}, y \in \mathbf{R}, z \in \mathbf{R}, k \in \mathbf{N}$ 。其中,任务为一个群体内知识 Agent、资源 Agent 的抽象表达,每个 Agent 能够充当多种角色,每个角色能够传到各个群体内。任务是支持恐怖组织网络中个体向群体不断演化的重要因素,任务的存在是恐怖组织演化的根本原因。在完成群体任务时,群体内的角色可以表示为一个代理的 Agent。资源在整个恐怖组织中起到了组织与任务的连接作用,通过与知识等因素交互,帮助恐怖分子完成任务。

(3) 各系统之间的关系。

在整个网络中,各 Agent 之间的互动过程描述见表 1。

表 1 组织各要素之间影响和作用模式

Table 1 Effect and function pattern for each elements of the organization

系统	范围	对其他主体的影响
人(Agent)	社会网络(人员之间的关系),组织的效忠程度;与谁联系,谁控制资源;谁去完成任务;	决定着任务的成 功与失败;决定资源 的分配
知识	知识网络(人员具有的 专长和技能)	影响人员的素质; 决定任务完成的 效果
资源	资源网络(人员占有或 能使用的资源);资金;信 息	连接人与任务的 中间因素
任务/目标/ 意图	任务网络(人员被指派 的任务或计划)	受到人、知识、资 源的影响

根据上述分析建立恐怖组织的多主体系统模型,见图 7。

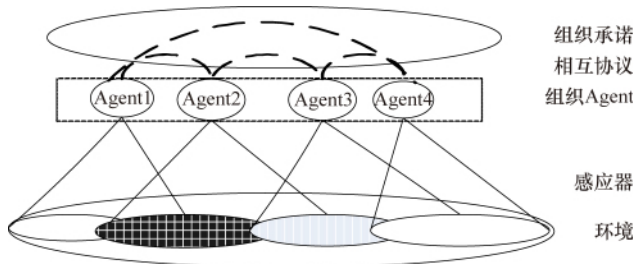


图 7 恐怖组织多主体系统框架

Fig. 7 Multi-agent system framework of terrorism organization

图 7 中较高的社会网络连通度能够帮助恐怖组织提高其合作、资源、任务、组织网络的效率;较高的环境连通度、较低的环境复杂度、环境因素的不确定性能帮助恐怖组织形成较高的连接网络;Agent 认识能力越精确越能提高组织的任务、合作、意图的效率。这些要素之间的连接更多的是依赖于信念来完成,外部环境因素的加入增加了群体对某一共同信念的刺激,环境使信息流动加快,进而增加群体的自发行为。

### 2.2.2 行动网络模型构建

在打击恐怖组织时,仅对其组织网络打击并不能完全根除恐怖主义。当恐怖组织的网络被打散后,虽然整体组织的威胁性大大降低,但在网络中存在一定的小群体或孤立点。如果他们掌握一定的资源及信息,仍然可以按原定计划在一定范围内发动一定规模的恐怖事件。反恐方在打击恐怖组织

的整体网络结构时,必须考虑费用,采用最少的费用达到最大的打击效果。从长远来看,对其行动网络的长期打击或监控会更好降低恐怖组织发动恐怖事件的概率。构建的恐怖组织行动网络见图 8。图 8 中  $x_{ij}$  为网络的容量,  $c_{ij}$  为费用。

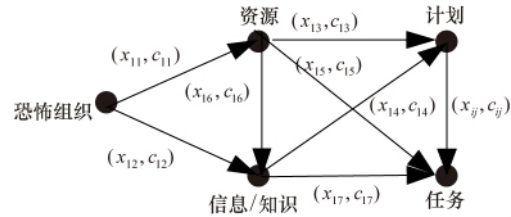


图 8 恐怖组织的行动网络

Fig. 8 Action network of terrorism organization

$$\min z = \sum_{(i,j) \in A} \sum c_{ij} x_{ij} \quad (7)$$

$$\text{s.t.} \sum_{(j,k) \in A} x_{jk} - \sum_{(i,j) \in A} x_{ij} = f_j \quad j \in N \quad (8)$$

$$l_{ij} \leq x_{ij} \leq u_{ij}, (i,j) \in A \quad (9)$$

则有如下定理<sup>[22]</sup>。

定理(1):设  $f$  是  $G$  上的可行流,  $\mu$  是  $v_s$  到  $v_t$  的一条链,若  $\mu$  满足条件  $[v_i, v_i] \in \mu^+$  时,  $f_{ij} < c_{ij}$ , 即  $\mu^+$  中每一弧是非饱和链;当  $[v_i, v_i] \in \mu^-$  时,  $f_{ij} > 0$ , 即  $\mu^-$  中每一弧是非零流弧, 则称  $\mu$  是一条增广链。

定理(2):设割集  $S, T \subset V, S \cap T = \emptyset, v_s \in S, v_t \in T$ , 则称  $(S, T) =$

$\{[v_i, v_j] | v_i \in S, v_j \in T\}$  为  $G$  的一个割集, 称  $C(S, T) = \sum_{[v_i, v_j] \in (S, T)} C([v_i, v_j])$  为割集  $(S, T)$  的容量。

定理(3):对任意的可行流  $f$  及任意割集  $(S, T)$  总有  $V(f) \leq C(S, T)$ , 则有某个可行流及某一割集  $(S^*, T^*)$  使得  $V(f^*) = C(S^*, T^*)$ , 则  $f^*$  为  $G$  的最大流,  $(S^*, T^*)$  为最小容量割集, 即最小割集。

在打击恐怖组织的行动网络时,主要通过寻找增广链求最小割集,从而实现对其网络的破坏,进而摧毁整个组织网络。

## 3 模拟实验及仿真结果

对恐怖组织网络进行攻击时,对其组织中的人员与行动分别进行攻击。当关键性指挥人物被消灭时,整个组织的力量将会被削弱,但威胁性仍然存在,必须对其资源进行瓦解,从而实现从整体上消灭其组织。

### 3.1 组织网络的脆弱性攻击

#### 3.1.1 对中心节点的选择性攻击

(1) 选择中心点。

实验时,选取最具有代表性的图 4 应用 ORA 软件对其中心性进行分析,排名前 10 的节点的中心性指标如表 2~表 4 所示。

表 2 图 4(a)的中心性指标  
Table 2 Centric index of Fig. 4(a)

节点	度中心性	节点	介数中心性	节点	紧密中心性
33	0.180	33	0.074	50	0.226
50	0.148	56	0.029	56	0.145
56	0.098	50	0.023	33	0.129
11	0.090	37	0.022	63	0.129
26	0.082	26	0.015	51	0.113
51	0.082	52	0.014	62	0.113
43	0.074	59	0.012	6	0.097
6	0.066	6	0.011	43	0.081
37	0.066	41	0.011	24	0.065
62	0.066	46	0.011	42	0.065

表 3 图 4(b)的中心性指标  
Table 3 Centric index of Fig. 4(b)

节点	度中心性	节点	介数中心性
2	0.041	4	0.004
3	0.041	2	0.004
4	0.041	3	0.004
5	0.041	5	0.004
1	0.033	6	0.002
6	0.016	8	0.002
7	0.016	10	0.002
8	0.016	12	0.002
9	0.016	14	0.002
10	0.016	15	0.002

表 4 图 4(c)的中心性指标  
Table 4 Centric index of Fig. 4(c)

节点	度中心性	节点	介数中心性
17	0.074	17	0.091
4	0.041	4	0.069
8	0.041	29	0.065
10	0.041	5	0.061
12	0.041	40	0.059
15	0.041	31	0.055
16	0.041	34	0.048
18	0.041	27	0.047
19	0.041	44	0.043
21	0.041	55	0.043

(2) 实施攻击。

从表 2~表 4 可以看出,各种类型的恐怖组织,由于结构形状不同,从而导致其中心性的选择有所不同。图 4 的中心指标排名最前的分别为:33,50,56;2,3,4,5;17,4,8。本文首先有选择性地对处于中间层的节点进行攻击,攻击时充分考虑恐怖组织的自组织性和快速耦合性,每一次攻击时同时攻击多个点。攻击后的效果见图 9 和图 10。从图 9 和图 10 可以看出,经过几次攻击后,恐怖组织的网络结构几乎被打散,达到了预期效果;特别是对具有全息结构的恐怖组织网络,同时攻击 2,3,4,5 节点,网络达到崩溃的临界点,与攻击其他节点相比或与传统的每一次攻击某一节点相比,攻击效率大大提高。

(3) 攻击效果对比分析。

传统的攻击在网络中选取节点中心性最高的某一节点进行打击,本文有选择性地同时打击多个节点,相比之下,本文方式的攻击效率和效果明显优于传统方式,如图 11 所示。

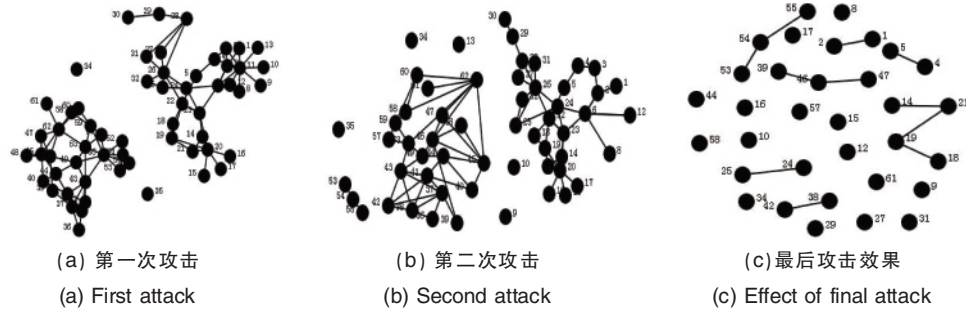


图 9 指数分布式网络经过攻击后的效果

Fig. 9 Effect of exponential distribution after the attack

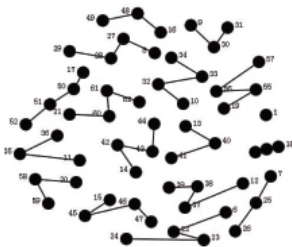


图 10 全息结构经过一次攻击后的效果

Fig. 10 Effect of holograph hierarchical structure after first attack

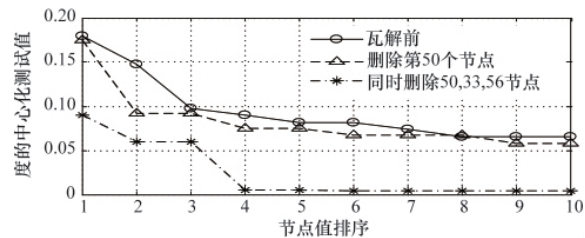


图 11 攻击效果对比

Fig. 11 Comparison of attack effects

从图 11 可以看出, 有选择性地攻击多个节点的效果明显优于每次只攻击某一节点的效果, 并且同时攻击多个节点可以有效防止恐怖组织的短期自组织性。

### 3.1.2 对边的选择性攻击

边的选择性攻击是指优先攻击重要的边<sup>[23]</sup>。边的重要性是依据边两端节点的重要性, 即一条边连接的两端节点的重

要性越高, 这条边的重要性就越高。图 12 和图 13 为攻击重要边的效果图, 与选择性攻击重要节点法相比, 此法效果明显较差。在指数分布式网络中, 同样经过 3 次攻击, 但整个网络的抗毁性依然很强, 网络的连通度较高。在全息等级结构网络中, 经过攻击后, 节点中的重要人物 1 被隔离, 但其他网络的抗毁性不但没有减弱, 反而分裂成更具威胁性的 4 个网络。

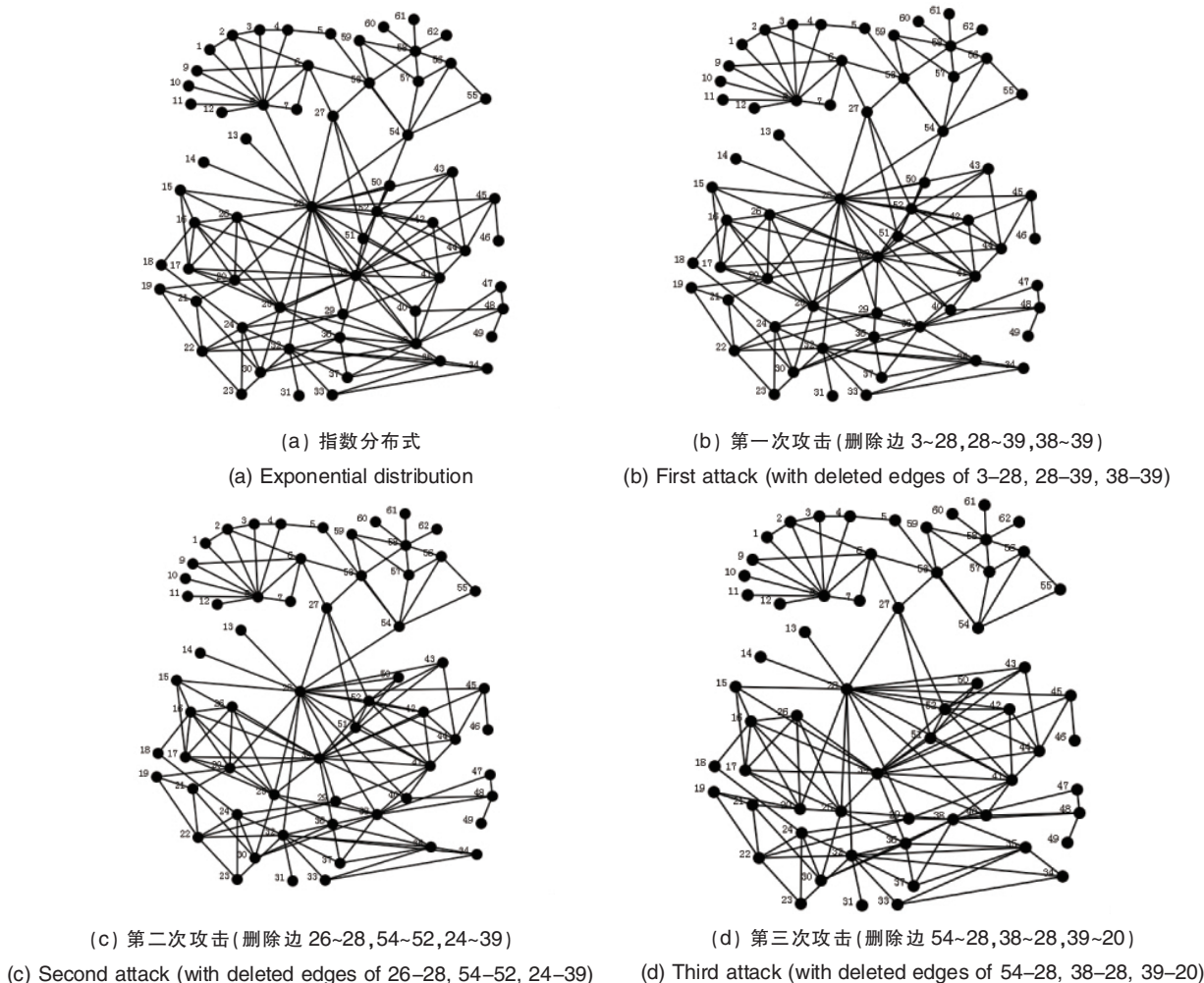


图 12 指数分布式删除边的攻击效果

Fig. 12 Attack effects of exponential distribution network with deleted edges

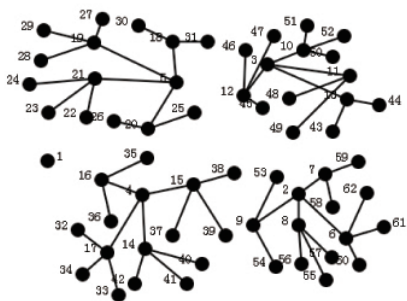


图 13 全息结构删除边的一次攻击效果  
(删除边 1~2, 1~3, 1~4, 1~5)

Fig. 13 First attack effect of holograph hierarchical structure with deleted edge (with deleted edge of 1~2, 1~3, 1~4, 1~5)

## 3.2 行动网络模型的攻击

### (1) 算法设计。

步骤 0: 取零流  $f$  作为初始可行流。

步骤 1: 构造剩余网络  $G(f)$ 。若  $G(f)$  中不存在  $(v_i, v_j)$  路, 结束, 则  $f$  为  $G$  中最小费用最大流; 否则, 在  $G(f)$  中找一条最小费用路  $P$ , 转步骤 0; 其中资源重要性度量公式为

$$R_i = \sum_{j=1}^T \text{TR}(i, j) \exp[1 - \text{sum}(\text{TR}(:, j))] \quad (10)$$

其中,  $\text{TR}(\text{Task Resource})$  表示元素  $(i, j)$  是智能体  $i$  占有资源  $j$  的度量,  $\text{sum}(\text{TR}(:, j))$  表示若人员  $i$  承担任务  $j$ , 则将所有承担任务  $j$  的人员数相加所得到的值。其综合能力的度量公式为

$$C = (x_{11} + x_{12} + \dots + x_{1n}) / n。$$

步骤 2:沿  $P$  对  $f$  进行增广得到新的可行流  $f$ , 转步骤 1。

(2) 行动网络攻击实验。

根据上述分析结合算法设计得到图 14 的各条增广链: 节点 1, 恐怖组织→资源→任务; 节点 2, 恐怖组织→资源→信息→任务; 节点 3, 恐怖组织→资源→信息→计划→任务。从发动恐怖事件的实际情况来看, 恐怖组织与资源是整个网络中最为重要的基础结点。在上文分析中已经对其组织网络进行了攻击, 当恐怖组织网络被攻击后, 对其行动网络中的一些节点进行有选择性地攻击, 根据增广链分别对其攻击, 首先对资源网络进行攻击, 攻击效果如图 14 所示。

从图 14(a) 可以看出, 反恐方对其行动网络中的资源增广链进行打击后, 恐怖组织发动恐怖袭击的概率大大降低。

原因在于当资源网络被切断后, 恐怖分子即使是掌握了一定的信息, 对计划进行周密部署, 也已经没有足够的资源去购买实施恐怖袭击的武器等; 但是仍然有部分资源掌握在恐怖组织手中, 仍然存在发动袭击的可能性。这说明在反恐过程中, 切断恐怖组织的资源网络对打击恐怖分子具有良好的效果。图 14(b) 是进行第二次攻击后的网络, 这次的攻击主要针对其信息/知识网络。该节点被破坏后, 恐怖组织仍然有能力去执行恐怖袭击, 并且与图 14(a) 相比, 其威胁性并没有得到明显降低; 但是这一次是针对其情报信息进行的攻击, 为反恐部门提供了一定的信息支持, 通过对信息的干预, 预防并打击可能的恐怖袭击。图 14(c) 是同时对资源及信息节点进行的攻击效果。如果同时对信息、资源网络节点进行打击, 整个网络陷入瘫痪状态, 效果比前两次更加明显。

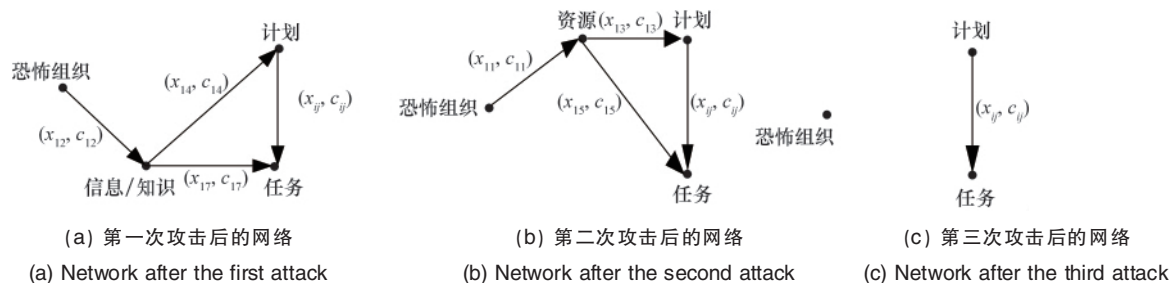


图 14 经过三次攻击后的行动网络  
Fig. 14 Action networks after three attacks

## 4 案例应用

### 4.1 9·11 事件网络分析与应用

9·11 恐怖事件震惊了全世界, 事件发生前, 恐怖组织作了充足准备, 对其资源、信息、任务、计划等进行了周密安排, 如图 15(a) 所示<sup>[24]</sup>。

图 15(a) 是根据事后调查的相关信息绘制的整体网络。恐怖组织在策划此次事件之前对整个行动进行了部署, 对人员进行了分工, 并对相关的行动资源、信息、任务进行了分配, 形成了一个等级全息结构。应用本文提出的方法, 对图

15(a) 中的资源与信息网络进行删除, 并得到图 15(b) 的网络结构。从图 15(b) 可以看出, 经过对资源与信息网络的打击, 整个恐怖组织的网络结构被破坏, 发动恐怖事件的概率大大降低。

以上主要分析了行动之前的网络, 在实际发动事件过程中, 恐怖组织的成员之间也进行了大量的准备工作。根据相关的情报及事后报道, Krebs 绘制了恐怖组织的网络图, 见图 16(a)<sup>[29]</sup>。应用中心性法对其网络进行分析 (表 5), 然后攻击, 其攻击效果见图 16(b)。

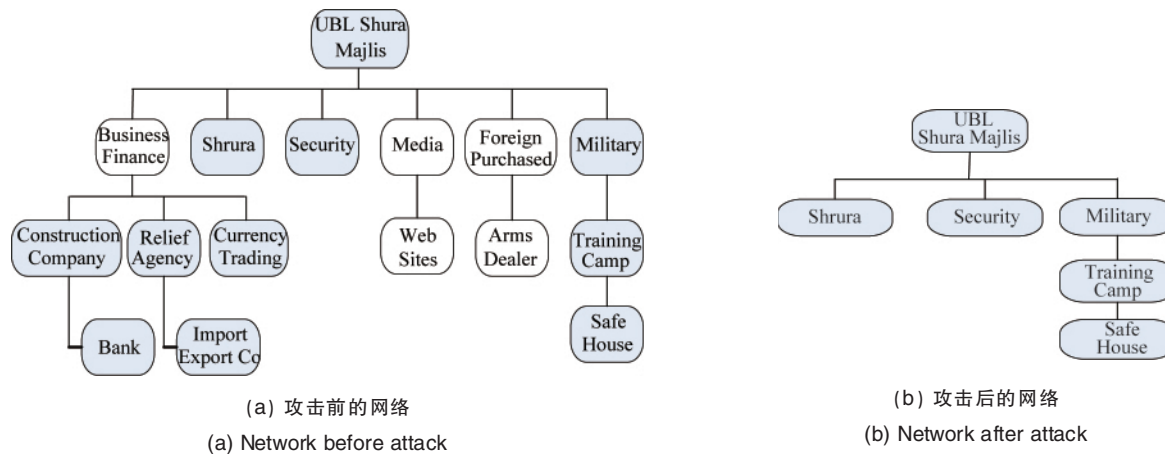
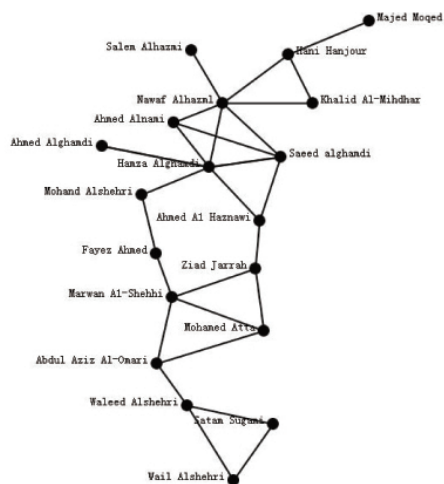
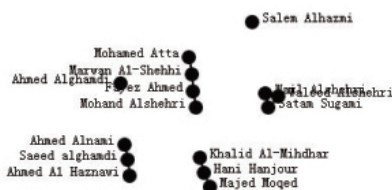


图 15 9·11 事件发生前的行动网络  
Fig. 15 Action network before 9/11 terrorist attacks



(a) 瓦解前的组织网络图

(a) Organization network before disintegration



(b) 经过两次攻击后的网络

(b) Network after two attack

图 16 直接参与 9·11 事件的恐怖组织主要成员关系网络  
Fig. 16 Relation network for the main member directly joining 9/11 terrorist attacks

表 5 9·11 事件中恐怖组织主要成员关系网络中心性分析  
Table 5 Centric analysis for the main members relation network of 9/11 terrorist attacks

节点	度中心性	节点	介数中心性
Hamza Alghamdi	0.222	Hamza Alghamdi	0.194
Nawaf Alhazml	0.167	Nawaf Alhazml	0.183
Saeed alghamdi	0.139	Ahmed Al Haznawi	0.172
Marwan Al-Shehhi	0.111	Ziad Jarrah	0.162
Waleed Alshehri	0.083	Abdul Aziz Al-Omari	0.147
Abdul Aziz Al-Omari	0.083	Marwan Al-Shehhi	0.117
Mohamed Atta	0.083	Waleed Alshehri	0.105
Ziad Jarrah	0.083	Saeed alghamdi	0.067
Ahmed Al Haznawi	0.083	Mohand Alshehri	0.064
Ahmed Alnami	0.083	Mohamed Atta	0.060

表 5 中, 首先选择度中心性较高的 Hamza Alghamdi 和 Nawaf Alhazml 进行同时攻击, 再选择 Abdul Aziz Al-Omari 和 Ziad Jarrah. 从图 16(b)可以看出, 经过两次攻击后, 恐怖组织网络的威胁性大大降低。

#### 4.2 伦敦地铁爆炸案

2005 年 7 月 7 日, 恐怖组织在伦敦上班高峰期制造了 7·7 伦敦地铁爆炸案。根据相关调查, 事后警方绘制了其网络, 如图 17 所示<sup>[20]</sup>。应用本文提出的方法对网络进行了攻击, 效果如图 18 所示。从图 18 可以看出, 只需经过一步攻击, 此网络几乎被摧毁, 整个恐怖组织网络的威胁性大大降低。

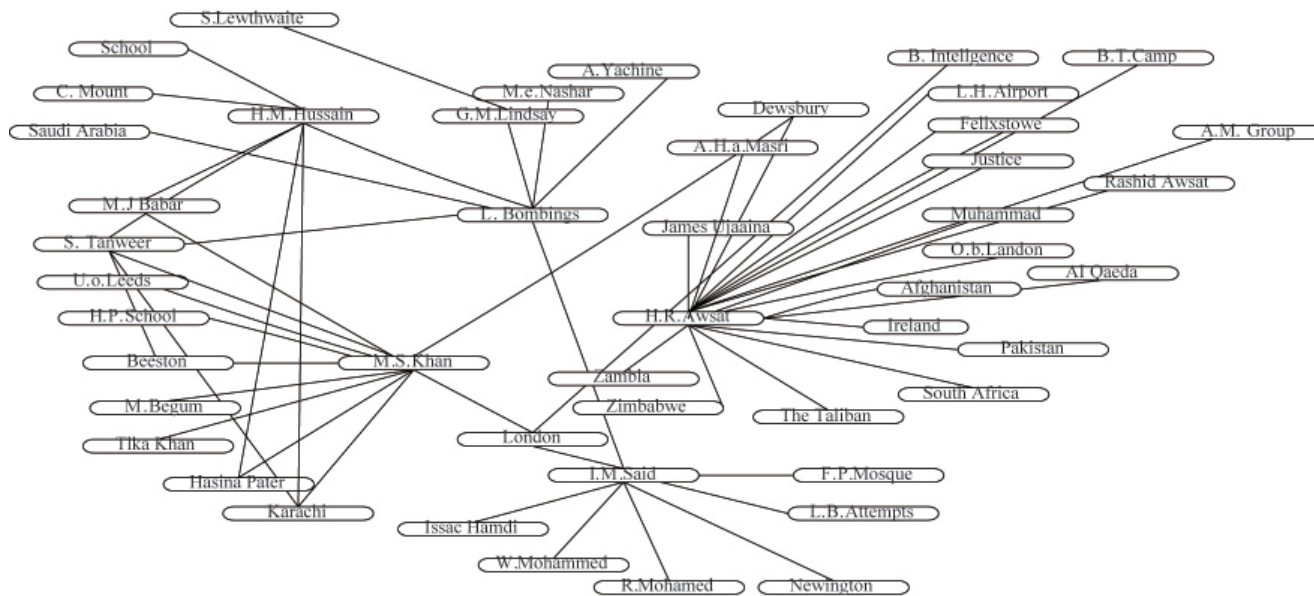


图 17 伦敦 7·7 地铁爆炸案恐怖组织网络

Fig. 17 Terrorism organization network of the 7/7 London bombings

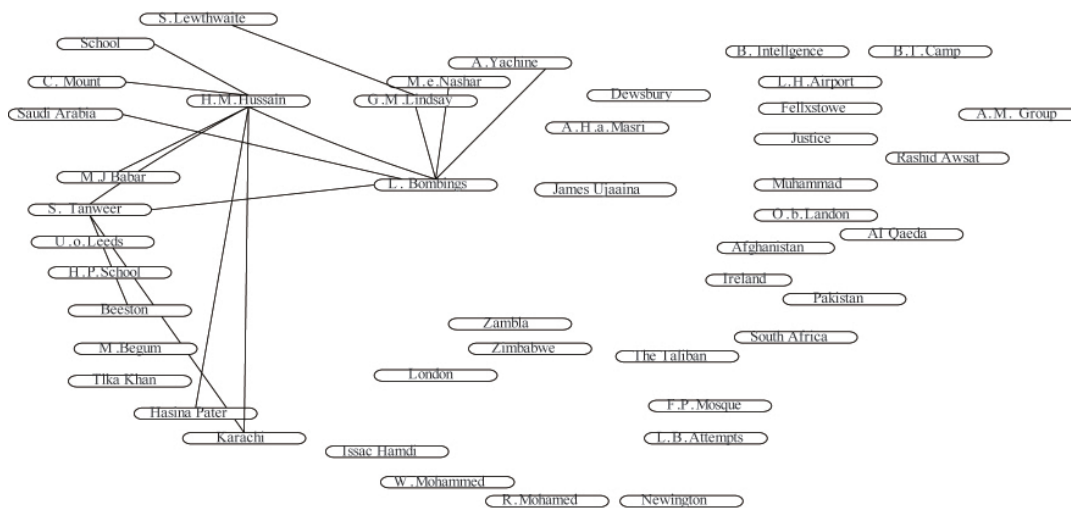


图 18 经过一步攻击后的网络  
Fig. 18 Network after first attack

5 结论

本文主要研究了恐怖组织网络的抗毁性。针对恐怖组织网络结构的特点,应用动态社会网络的方法分析了恐怖组织的网络结构及演化规律,构建了其行动网络模型。对恐怖组织网络进行了选择性攻击,攻击时从中间层进行突破,同时攻击多个节点。此方法对指数分布式、均匀分布式、全息结构的恐怖组织的网络结构均具有较好的应用,特别是全息结构,只需进行一步攻击,整个网络便被瓦解。在对其行动网络攻击时,考虑其流量及费用,通过寻找网络的增广链,优化攻击方案。通过抗毁性研究发现,指数分布式、均匀分布式组织网络需经多步攻击方能达到预期效果。在行动网络中,对恐怖组织的资源及信息进行打击,可以有效地破坏其整体网络,切断恐怖组织的资金网络;对其信息进行监视可以有效预防恐怖组织发动恐怖活动。

参考文献 (References)

[1] 汪秉宏, 周涛, 王文旭, 等. 当前复杂网络研究的几个方向 [J]. 复杂系统与复杂性科学, 2008, 5(4): 21-24.  
Wang Binghong, Zhou Tao, Wang Wenxu, et al. Complex System and Complexity Science, 2008, 5(4): 21-24.

[2] Sageman M. Understanding terror networks [M]. Philadelphia: University of Pennsylvania Press, 2005: 37-52.

[3] Memon N, Hicks D L, Harkiolakis N, et al. Small world terrorist networks: a preliminary investigation[M]. London: Springer-Verlag, 2008: 339-344.

[4] Stripling M. Embodying terror networks: How direction creates structure [EB/OL]. [2013-01-08]. <http://www.crisisville.com/files/Terrorism-Directed-Networks.pdf>.

[5] Ressler S. Social network analysis as an approach to combat terrorism: Past, present, and future research[J]. Homeland Security Affairs, 2006, 2(2): 1-10.

[6] Carley K M, Reminga J, Storrick J, et al. ORA user's guide 2009[EB/OL]. [2012-01-10]. <http://www.casos.cs.cum.edu>.

[7] Carley K M, Krackhardt J S. Destabilizing networks[J]. Connection, 2002, 24(3): 79-92.

[8] Carley K M. Dynamic network analysis for counter-terrorism [R]. Pittsburgh: Carnegie Mellon University, 2008: 1-24.

[9] Bohannon J. Counterterrorism's new tool: 'Metanetwork' analysis [J].

Science, 2009, 325(5939): 409-411.

[10] Carley K. M. Destabilizing dynamic covert networks [C]//Proceeding of the 8th international command and control research and technology symposium. Washington DC: the National Defense War College, 2003: 1-10.

[11] Carley K M. Estimating vulnerability in large covert networks [C]// Proceeding of the 9th international command and control research and technology symposium. Vienna: Loews Coron Do Resort, 2004: 1-4.

[12] Krebs V. Mapping networks of terrorist cells [J]. Connections, 2001, 24(3): 43-52.

[13] Borgatti S P, Mehra A, Brass D J, et al. Network analysis in the social sciences[J]. Science, 2009, 323(5912): 893-895.

[14] Albert R, Jeong H, Barabasi A L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(6794): 378-382.

[15] Albert R, Barabasi A L. Statistical mechanics of complex networks[J]. Review Modern Physical, 2002, 74(1): 47-97.

[16] Holme P, Kim B J. Attack vulnerability of complex networks[J]. Physical Review E, 2002, 65(5): 21-34.

[17] Carpenter T, Karakostas G, Shallcross D. Practical issues and algorithms for analyzing terrorist networks [EB/OL]. [2013-01-08]. <http://www.cas.memaster.ca/gk/papers/wmc2002.pdf>.

[18] Barabasi A L, Bonabeau E. Scale-free networks [J]. Science, 2003, 5(4): 50-58.

[19] Freeman L C. Centrality in social networks: conceptual clarification[J]. Social Networks, 1979, 22(1): 215-239.

[20] Vragovic I, Louis E, Diaz-Guilera A. Efficiency of informational transfer in regular and complex networks[J]. Physical Review, 2005, 71(3): 36-45.

[21] Penzar D, Srblijinovic A. About modeling of complex networks with applications to terrorist group modeling[J]. Interdisciplinary Description of Complex Systems, 2005, 3(1): 35-43.

[22] 运筹学编写组. 运筹学[M]. 北京: 清华大学出版社, 2005: 270-276.  
Operational Research Team. Operational research[M]. Beijing: Tsinghua University Press, 2005: 270-276.

[23] 谢丰, 程苏琦, 陈冬青, 等. 基于级联失效的复杂网络抗毁性[J]. 清华大学学报, 2011, 51(10): 1253-1254.  
Xie Feng, Cheng Suqi, Chen Dongqing, et al. Journal of Tsinghua University, 2011, 51(10): 1253-1254.

[24] Tucker D. Terrorist, networks, and strategy: Why the conventional wisdom is wrong[J]. Homeland Security Affairs, 2008, 5(2): 1-3.

[25] Krebs V E. Uncloaking terrorist networks [J]. First Monday-Peer Reviewed Journal on the Internet, 2002, 7(4): 4-5.

[26] Memon N, Larsen H L, Hicks D L, et al. Detecting hidden hierarchy in terrorist networks: Some case studies [M]. Berlin: Springer-Verlag, 2008: 477-489.

(责任编辑 吴晓丽, 安莹)