

基于社会网络与事件关联的恐怖事件监测与识别

李泽, 孙多勇, 李博

国防科技大学信息系统与管理学院, 长沙 410073

摘要 恐怖组织的社会网络结构变化与恐怖事件的发生具有一定的关联性。基于此关联,通过监测恐怖组织社会网络的变化,可以实时、有效地识别恐怖事件。将基于社会网络变化检测的恐怖事件监测与识别问题视为分类问题,并通过神经网络模型进行分类研究。以某一时刻是否发生恐怖事件为标准,对恐怖组织社会网络进行分类;通过网络分析技术,得出网络的参数指标,建立混合算法改进的神经网络模型;将网络的参数指标与恐怖事件发生情况分别作为输入和输出,对神经网络进行训练与测试。案例分析和对比结果表明,基于神经网络模型的社会网络变化检测方法具备较好的恐怖事件监测与识别能力;该方法可在一定程度上弥补现有方法正确率不高、通用性不强、检测结果与恐怖事件实际发生的相关性不高等不足。

关键词 恐怖组织网络;变化检测;恐怖事件;监测与识别;神经网络

恐怖主义是信息时代世界各国面临的重大挑战,已成为国家、社会和民众安全的重大威胁之一。近年来,发生在欧洲的系列恐怖袭击事件让人们愈加关注恐怖主义的发展,也让研究者们更加重视恐怖事件预警的研究。尽管存在许多恐怖袭击的“独狼”行动,恐怖组织仍然是谋划和实施恐怖袭击的主要力量来源,因而恐怖组织及其内部结构是反恐研究的重要领域。通过数据挖掘和社会网络分析,国内外研究学者在分析恐怖组织领域取得了许多研究成果^[1-5]。现有研究表明:不同于层次化的传统组织,恐怖组织具有松散的网络化结构^[2-3];其网络结构受内部和外部因素的影响而不断发生变化^[4];同时,网络结构的变化与恐怖事件的发生又具有一定的关联性^[5]。

恐怖事件监测与识别是恐怖事件预警的重要组成部分,是有效实现恐怖事件预警的前提条件之一。基于社会网络变化检测的恐怖事件监测与识别是反恐领域研究的一个热点兼难点,其核心思想是:在对恐怖组织构建时序社会网络的基础上,通过相关技术手段对时序社会网络进行变化检测。社会网络变化检测中的“变化”指的是异常变化,所以社会网络变化检测又称社会网络异常变化检测。一部分网络的异常变化可以通过动态社会网络建模的方法进行检测。现有的动态社会网络建模方法有连续马尔可夫链模型、动态环境友谊模型、隐空间模型、多agent仿真模型等^[6]。但当网络异常变化是由无法预知的、外部的、随机的因素引起时,则无

法通过建模方法进行研究,而需要采用变化检测机制去分析。现有方法中,McCulloh和Carley提出了基于统计过程控制(SPC)的网络动态行为变化检测方法,并探讨了其在不同类型网络中的应用可行性^[5];Priebe运用扫描统计(滑动窗口)和时间序列异常检验相结合的方法对Enron邮件社会网络进行了变化检测^[7]。Sun等通过GraphScope,并基于最小描述长度检验了演化网络中的社区变化^[8]。Peel和Clauset基于概率框架模型识别网络变化时间点,通过广义层次随机图模型进行网络建模,并根据广义似然比检验识别异常变化^[9]。Li通过对点过程的相似比检验,并基于EM算法检验网络中事件的微弱变化^[10]。此外该领域还存在图形相似度比较、图形模式识别、链路预测等分析方法^[6,11]。与此同时,以社会网络变化检测方法为核心的社会组织智能监测系统也在不断发展,例如,美国国防高级研究计划局(DARPA)于2001年“9·11”事件之后,开发了恐怖信息感知系统,帮助情报分析人员及时识别恐怖威胁,预测可能的恐怖活动并提供及时的应对策略^[12]。

现有的研究证明社会网络结构变化与恐怖事件之间的关联性,同时也验证了针对社会网络模型的变化检测技术在恐怖事件监测与识别方面操作的可行性。然而,由于恐怖组织自身具有隐蔽性和非常规性,恐怖事件具有突发性和难以预测性,加上该领域的研究尚处于起步阶段,目前的研究存在以下3点不足:1) 现有方法需要考虑恐怖组织社会网络的

收稿日期:2016-08-22;修回日期:2016-10-12

基金项目:国家自然科学基金项目(71473263);高等学校博士学科专项科研基金项目(20134307110020)

作者简介:李泽,博士研究生,研究方向为国家安全与危机管理,电子信箱:plalize@nudt.edu.cn;孙多勇(通信作者),教授,研究方向为国家安全与危机管理,电子信箱:sunduoyong@nudt.edu.cn

引用格式:李泽,孙多勇,李博.基于社会网络与事件关联的恐怖事件监测与识别[J].科技导报,2017,35(9):87-94;doi:10.3981/j.issn.1000-7857.2017.09.011

结构特征,在此基础上采取特定的模型和方法进行分析,因而通用性不高。2) 现有方法仅考虑某一特定的网络结构参数,而遗失了网络本身的一些重要信息,使得所检测到的网络异常变化具有较高的虚报率和漏报率。对于恐怖组织网络而言,较高的虚报率和漏报率使得恐怖事件的监测、识别和预警变得困难。3) 现有方法侧重于社会网络变化检测技术,对社会网络结构变化与恐怖事件之间的关联性重视不够,因而造成最终检测的结果与实际发生恐怖事件的相关性不高。

本文提出了一种新的研究思路——引入神经网络作为社会网络变化检测和恐怖事件监测与识别的模型和方法。将网络变化检测视为一种分类问题——网络存在“变化”和“正常”2种类型,分别对应于相应时刻恐怖组织“发动恐怖袭击”和“未发动恐怖袭击”;并根据研究对象的特性构建了基于混合智能优化算法的BP神经网络模型,以神经网络分类的结果作为恐怖事件监测识别的参考。神经网络模型充分考虑了社会网络与恐怖事件关联性,又具有通用性强、准确率高的优点。

1 神经网络模型

人工神经网络是一种模仿动物神经网络行为特征,进行分布式并行信息处理的数学模型。目前神经网络已经成熟应用于模式识别、信号处理、知识工程、专家系统、优化组合和机器人控制等领域。人工神经网络从复杂的社会系统中进行模式匹配,从而较好地处理分类和回归问题。相较于传统的多元线性回归方法,基于非线性映射关系的神经网络在拟合优度、对初始数据的仿真与模拟能力及对新数据的预测能力方面有较明显的优势^[13]。

1.1 BP神经网络

BP神经网络,即多层前馈式误差反向传播神经网络,是人工神经网络中最具代表性和广泛应用的一种。其结构简单,可操作性强,能模拟任意的非线性输入输出关系^[14]。BP神经网络通常由输入层、输出层和若干隐含层构成。每层又由若干个结点组成,每1个结点表示1个神经元,上层结点与下层结点之间通过权联接,同一层结点之间没有联系。图1为典型的BP神经网络拓扑结构^[15]。BP神经网络有2个阶段:

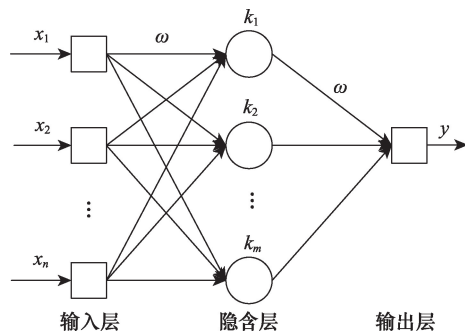


图1 典型的BP神经网络拓扑结构

Fig. 1 A typical topology of BP neural network

第1阶段,信息的正向传播,信息从输入层输入,通过隐含层,在输出层计算实际输出值,如果在输出层没有得到预期的输出,即开始第2阶段,误差的反向传播过程。如此反复迭代,直到误差小于给定的值为止^[16]。

BP神经网络的优点是寻优具有精确性,但同时也存在许多弊端,如对网络初始权值设置敏感、容易陷入局部极小点、收敛速度慢、易引起震荡效应等。当应用于恐怖组织网络变化检测时,必须输入大量的网络参数来消除恐怖网络信息的不确定性和不完整性。然而,随着输入层维度的升高,BP神经网络的拟合精度随之变差,而且由于各参数之间的相关性,很难保证拟合算法收敛到整体最优,从而影响全局最优权重和阈值的寻找。

1.2 BP神经网络的改进

针对BP神经网络的缺点,现有研究通过引入智能优化算法对BP神经网络进行改进,有效地弥补了BP神经网络的不足。如将遗传算法引入BP神经网络的GABP(Genetic Algorithm Back-propagation)神经网络模型^[16],粒子群算法与BP神经网络相结合的PSOBP神经网络模型^[17],混合的遗传算法和粒子群算法与BP神经网络相结合的GAPSOBP神经网络模型等^[18-20]。这些改进的BP神经网络的优势已得到相关研究者的验证,并得到广泛应用。

如前所述,在恐怖组织社会网络变化检测中,为能充分利用恐怖网络的信息,需要将大量的网络参数作为输入。遗传算法虽然具有鲁棒性,在全局性最优解的搜索上非常高效,但种群较大、维数较多时,它容易早熟收敛从而陷入局部最优。针对遗传算法的这个缺点,将遗传算法与粒子群算法相结合的BP神经网络,既可以提高遗传算法的求解质量和运行效率,又能在保持算法通用性的基础上提高效率^[18]。由于GAPSOBP神经网络具备这些优点,本文以GAPSOBP神经网络为社会网络变化检测的模型,并将其与GABP和BP神经网络的结果进行对比。GAPSOBP神经网络的流程如图2所示。

2 研究方法

2.1 研究思路

恐怖组织在发动恐怖袭击之前,有较长时间的潜伏期用来进行准备活动,如招募成员、募集资金、购置武器、交流任务等。这一系列活动反映在恐怖组织社会网络中,是网络中节点、连接属性及拓扑结构的变化。图3是恐怖组织社会网络变化过程的示例。如果研究者能及时识别出这些变化,并找出其中的规律性,则可在其造成更大影响之前合理控制。

现有研究的中心任务是选择一个“模式”来代表网络,以及一种可以有效检测“模式”变化的数学方法^[9]。然而对于社会组织而言,很难找到一个可以充分代表网络的“模式”;同时对于恐怖组织而言,值得关注的是恐怖袭击这一特定的外部行为。所以本文根据研究对象的特征给出网络“变化”的定义,即以对应时刻恐怖组织是否发动恐怖袭击为标准,当发生恐怖袭击时,其对应的社会网络的状态为“变化”的,否

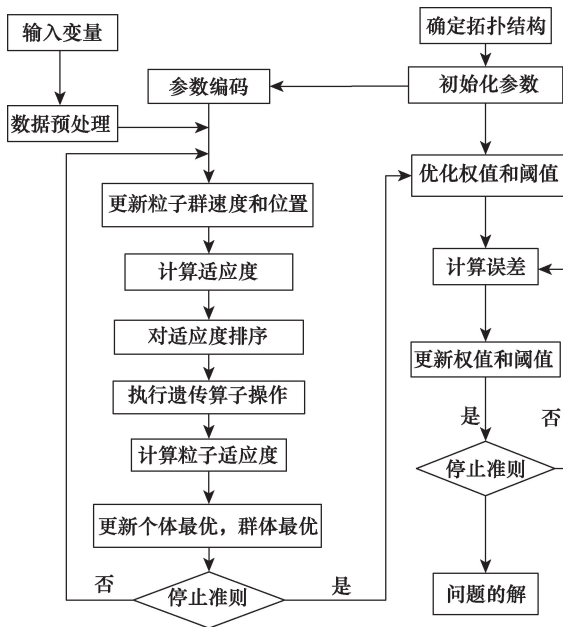


图2 GAPSOPB神经网络流程
Fig. 2 Flowchart of GAPSOPB neural network

则为“正常”。

研究思路是:首先,从恐怖组织数据库中提取出恐怖组织人员及关系信息、时间和恐怖事件信息,通过这些信息构建恐怖组织的动态社会网络,并通过社会网络分析得出各时间点网络的结构参数。其次,以对应时刻组织是否发动恐怖

袭击为标准,对时间序列进行分类——当某一时刻发生恐怖袭击时,编码为1;当没有发动袭击时,编码为0。再次,根据时间序列的分类结果,将对应时刻的网络结构参数分为2类。最后,构建GAPSOPB神经网络,并将分类后的网络参数和0、1序列分别输入至神经网络的输入层和输出层;经过神经网络一系列的训练和测试后,最终实现根据网络参数来检测网络变化,从而实现恐怖事件的监测与识别。研究框架如图4所示。

2.2 神经网络的模型参数

1) 神经网络的输入层选择。神经网络的输入层是每个时间点恐怖组织社会网络的参数。社会网络参数是社会网络某一方面特性的数字化表达,如中心度体现的是网络中节点之间的连接情况;社区体现的是网络中子群的凝聚状态;密度体现的是网络的疏密程度。一般而言,网络的参数可以分为3个层面,即节点层面(node level)、子图层面(sub-graph level)和网络整体层面(graph level)。社会网络变化检测的对象是网络整体层面的参数^[5],因为这些网络参数可以有效表征网络整体的属性。节点层面和子图层面的参数变化反映的是网络局部特性的变化,对于这些参数可以通过求均值等方法转化为网络整体参数^[4-5]。

现存社会网络的参数有几十种^[21],但是并不是所有的参数都需要拿来作为神经网络的输入,而是需要对其进行筛选。本文筛选具有代表性、变化具有显著性、与输出层具有较高相关性、对结果具有较好解释性的网络参数。为了提高

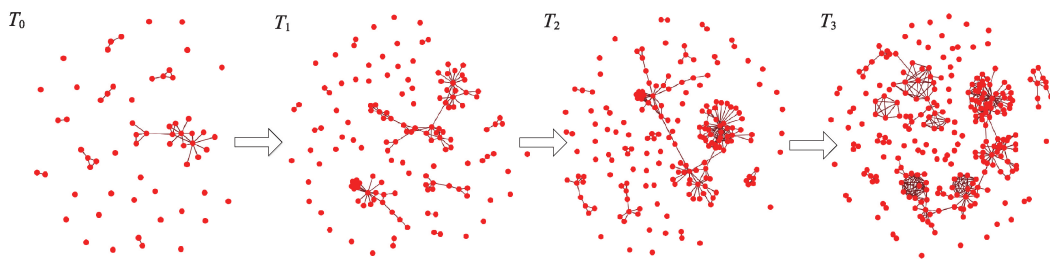


图3 恐怖组织社会网络的动态过程
Fig. 3 Dynamic process of terrorist social networks



图4 基于神经网络的社会网络变化检测框架
Fig. 4 Framework of social network change detection based on neural network

准确率,对选择的每个网络参数 X 进行如下归一化处理^[22],表达式为

$$X = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (1)$$

式中, X_{\max} 和 X_{\min} 分别为各参数的最大值和最小值。

2) 神经网络的隐含层选择。为了提高神经网络运行的准确性,需要根据神经网络输入层和输出层的神经元个数选择合理的隐含层神经元的个数。本文构建的是具有单层隐含层神经网络,隐含层的神经元的个数可由式(2)决定^[23]

$$N_{\text{hidden}} = \left\lfloor \sqrt{N_{\text{in}} + N_{\text{out}}} + a \right\rfloor \quad (2)$$

式中, N_{hidden} 、 N_{in} 、 N_{out} 分别为隐含层、输入层和输出层神经元的个数;参数 a 为[1, 10]范围内的整数,不同的模型和数据需要通过不断尝试,得出最优取值。

2.3 结果的评价指标

本文使用 ROC 曲线(受试者工作特征曲线)对不同神经网络进行分析。ROC 曲线以负正类率(false positive rate, FPR)为横轴,以真正类率(true positive rate, TPR)为纵轴。ROC 曲线的理想目标是 $FPR=0$, $TPR=1$,故 ROC 曲线越靠坐标(0,1)点效果越好。通常 ROC 曲线下方面积 AUC 与 ROC 曲线一起对模型平均性能进行评价。对于 AUC 而言,在 $AUC>0.5$ 的情况下, AUC 越接近于 1,说明效果越好。

此外,用一些现有分析手段来与本文的方法进行对比分析。选取统计过程控制(SPC)、局部异常因子(LOF)检测及逻辑回归(LR)方法对数据集进行分析,并选取准确率 p (precision)、召回率 r (recall)和综合评价指标 F (F -score)对结果进行评价。准确率和召回率越高,说明分析结果的精度越高,与实际越符合。同时,为了消除二者“此消彼长”的矛盾,引入 F -score 进行综合考虑, F -score 越高则说明该方法越好,其计算式为

$$F = 2 \times \frac{pr}{p+r} \quad (3)$$

3 案例应用

3.1 基地组织及数据

本文以基地组织(Al-Qaeda)为例进行分析。基地组织是近 20 年以来全球最具有代表性的、危害性最高的恐怖组织,是被联合国安全理事会认定的世界恐怖组织之一^[24]。基地组织数据来源于美国空军科研办公室的 JJATT(John Jay & ARTIS Transnational Terrorism)数据^[25]。该数据来源于公开数据的挖掘和整理,包括互联网新闻、在线刊出的报纸、书籍和杂志等,同时也参考了一些专家和非政府组织的情报。尽管该数据库的内容已经非常丰富,但是由于恐怖数据难以获取性的特征,单一数据库无法包含足够正确的数据。为了更好地消除数据质量带来的影响,同时参考了卡内基·梅隆大学 CASOS(Center for Computational Analysis of Social and Organizational Systems)中心的基地组织数据^[4]。通过将两个数据库进行融合,使数据更为详实,也更能反映组织的实际情况。

整理之后的数据集包含基地组织人员、恐怖事件及时间等数据。其中组织人员主要包括 2 部分:一是组织的核心领导成员;二是直接参与恐怖事件或者事件策划的人员。已有研究表明,指挥控制人员和实际参与人员等核心成员的变化对组织外部行为的影响很大^[26]。该数据从 1989—2003 年共 15 年,覆盖了基地组织的成长和成熟阶段。恐怖事件数据包含基地组织发动的 21 件恐怖袭击。恐怖事件与对应时间见图 5。

3.2 基地组织社会网络分析

1) 社会网络的构建

按照时间顺序,以月为单位,构建从 1989—2003 年共 180 个基地组织社会网络,依次编号为 T_1, T_2, \dots, T_{180} ,图 6 为 T_1 和 T_{180} 时刻基地组织社会网络的示例。

这些社会网络是有向加权网络,其中节点是恐怖分子,边是恐怖分子之间的关系。这些关系包括亲属关系、朋友关

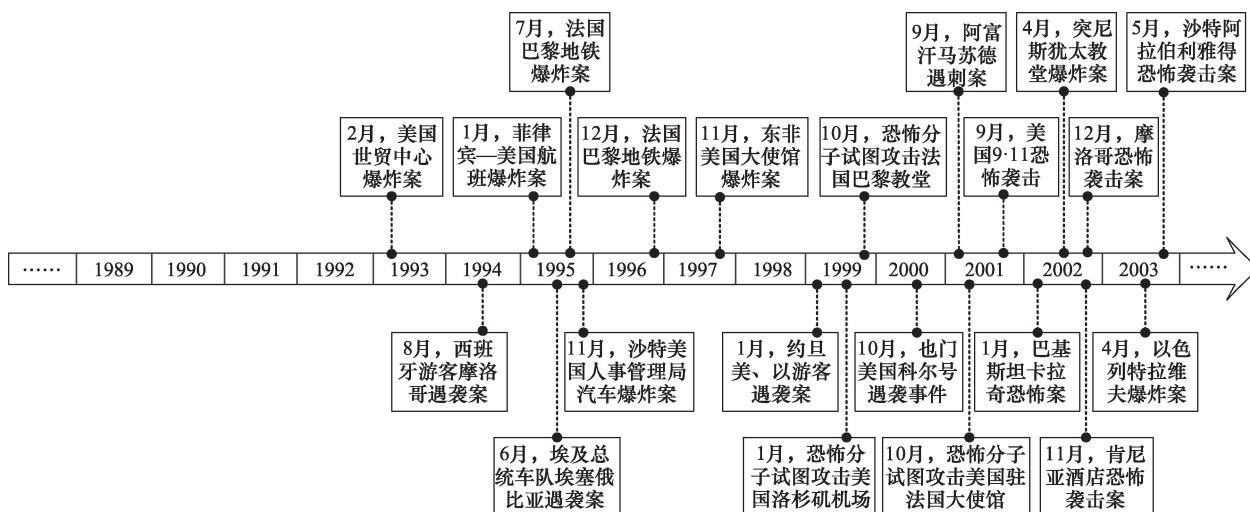


图5 基地组织恐怖袭击事件的时间轴

Fig. 5 Timeline of terrorist attacks launched by Al-Qaeda

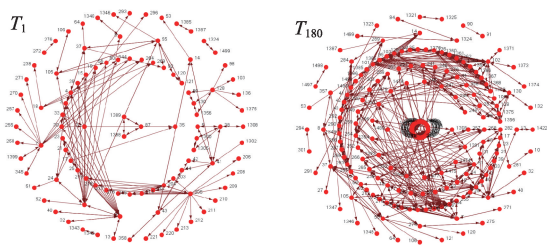


图6 基地组织社会网络快照

Fig. 6 Snapshots of social networks of Al-Qaeda

系、组织隶属关系以及任务合作关系等。随着时间的推移,网络中的节点和边都在发生着变化:对于节点而言,新成员的加入、旧成员的死亡或者脱离组织都会造成节点的变化;对于边而言,当成员加入或者离开组织时,边随之发生变化——对于组织隶属关系而言,当组织被瓦解之后关系随即结束;对于任务合作关系而言,当任务完成之后关系随即结束。

2) 社会网络参数求解与筛选。

通过社会网络分析软件ORA^[21]对网络进行分析,得到各时间节点网络的参数指标。然后根据图5中的恐怖事件数据对180个时间点和对应的网络进行分类:当时刻 t 发生恐怖袭击时,该时间节点 T 赋值为1,否则赋值为0。接着以分类后的0、1序列作为因变量,以对应网络的参数作为自变量,进行相关性分析,选取相关系数高且通过显著性检验的参数,最终选取了8个指标:4个网络整体参数(节点数、聚类系数、控制幅度、横截性)、3个网络子图参数(节点数/连通片、派系的个数、模块度 Q)及1个网络个体参数(接近中心度)。这些指标随时间变化的趋势如图7所示。

3.3 GAPSOPBP神经网络的构建与分析

1) GAPSOPBP神经网络的构建。通过Matlab构建具有单层的输入层、隐含层和输出层的GAPSOPBP神经网络。其中输入层的神经元有8个,对应于每个选取的网络参数;输出层的神经元有1个,为分类后的0、1序列;隐含层根据公式(2),经过不断尝试,选取 $a=9$,则对应的神经元的个数 $N_{\text{hidden}}=12$ 。

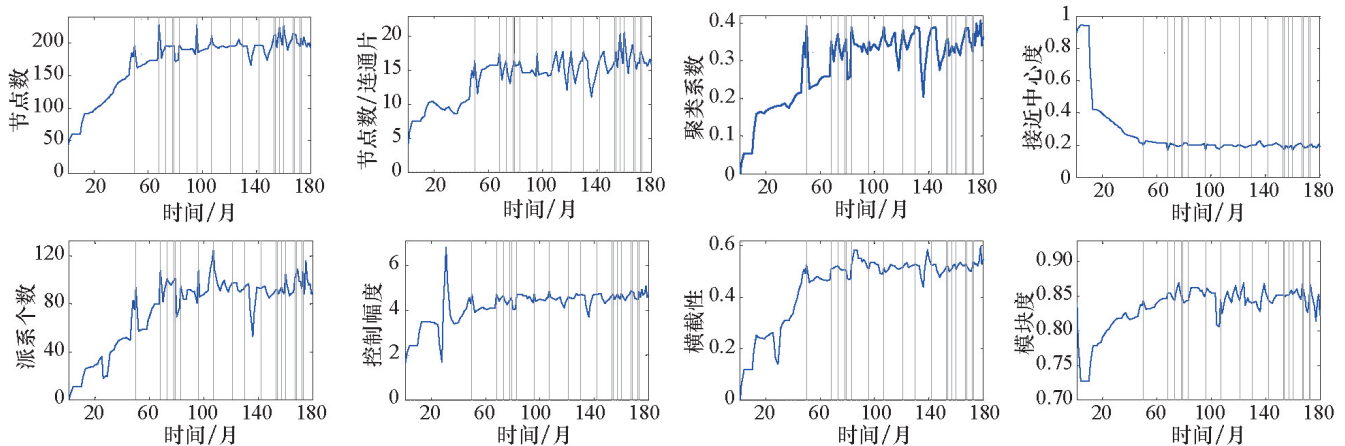


图7 选取的网络参数的变化趋势

Fig. 7 Changing trends of selected network measures

故构建的GAPSOPBP神经网络的结构为“8-12-1”结构。根据文献[19]的研究结果,粒子群的参数设置如表1所示。其中 c_1 和 c_2 为粒子在更新过程中的两个回事系数, w 表示惯性权重, v_{max} 、 v_{min} 分别表示粒子更新过程中的最大速度和最小速度。

表1 粒子群算法的参数设置

Table 1 Parameters of particles swarm optimization

粒子群维度	种群大小	c_1	c_2	w	v_{max}	v_{min}
121	100	1.49	1.49	0.729	1	-1

遗传算法保留前30%的个体(U_1);接下来的60%个体应用交叉算子,且交叉概率为0.6(U_2);最后10%个体应用变异算子,且变异概率为0.01(U_3),文献[20]表明,遗传算法在这样的设置下更有效。参数设置如表2所示。

表2 遗传算法的参数设置

Table 2 Parameters of genetic algorithm

U_1	U_2	U_3
0.3	0.6($P_{\text{crossover}}=0.6$)	0.1($P_{\text{mutation}}=0.01$)

2) 训练与测试样本选取。以180个时间点的前140个数数据作为训练样本,后40个数数据作为测试样本。其中训练样本中的输出层有130个“0”和10个“1”;测试样本的输出层中有31个“0”和9个“1”。本文对所构建的GAPSOPBP神经网络进行多次运行,并取平均值作为最终的分析结果。

3.4 结果与分析

为了评价GAPSOPBP神经网络分析结果的好坏,首先将结果与GABP神经网络及BP神经网络的分析结果进行对比。构建GABP和BP神经网络,使用ROC曲线结合AUC将三者结果进行对比(图8)。

从图8可以看出,GAPSOPBP神经网络的AUC为0.846,GABP神经网络的AUC为0.792,而BP神经网络的AUC为0.760。根据AUC的对比,GAPSOPBP的结果优于后两种方法。通过LR、SPC和LOF对相同数据进行分析,并对比它们

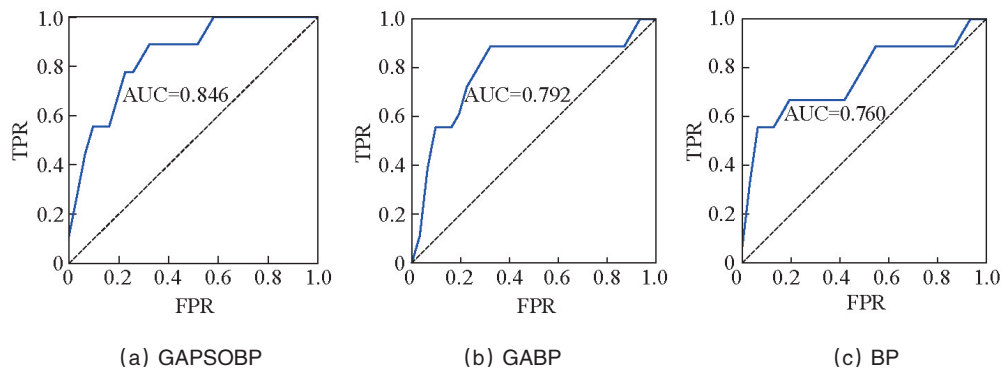


图8 不同神经网络分析结果的ROC和AUC

Fig. 8 ROC and AUC of different neural networks

与上述3种神经网络方法在准确率、召回率和综合评价指标方面的差别(表3)。

从表3可以看出,神经网络方法的准确率、召回率和综合评价指标值相较于其他方法普遍较高,尤其是通过粒子群和遗传算法优化的神经网络表现最好。异常检验方法SPC和LOF的准确率、召回率和综合评价指标值最低;虽然LR的准确率比GABP和BP高,但是其召回率较低,相比综合评价指标,仍不如后2种方法。通过对比可以发现本文构建的GAPSOBP神经网络不仅优于BP神经网络及GABP神经网络,同时比现有的一般异常检验和分类方法要好,说明通过粒子群和遗传算法优化的BP神经网络具有更好的处理这一类问题的能力。

表3 不同方法的结果对比

Table 3 Performance comparison of different methods

方法	准确率	召回率	综合评价指标
GAPSOBP	0.714	0.556	0.625
GABP	0.545	0.667	0.600
BP	0.556	0.556	0.556
LR	0.615	0.333	0.432
SPC	0.308	0.444	0.364
LOF	0.333	0.444	0.381

最后根据尤登指数(Youden's Index)计算公式,得出最优阈值为0.599。在该阈值下,对GAPSOBP的结果进行0、1化处理,结果与实际变化的0、1序列进行对比(表4)。

该实验结果即为基地组织社会网络变化检测和恐怖事件监测与识别的结果。从结果中可以看出,在 T_{157} 、 T_{160} 、 T_{167} 、 T_{168} 和 T_{173} 时刻网络发生异常变化,对应时刻有恐怖事件的发生。虽然在与实际变化的对比中, T_{169} 和 T_{175} 时刻发生虚报,而 T_{142} 、 T_{153} 、 T_{154} 和 T_{172} 时刻发生漏报,但是训练好的神经网络仍然具有很高的正确率,说明它已经具备通过实时监控网络结构变化实现对恐怖事件识别的能力。

表4 GAPSOBP神经网络的实验结果及与实际的对比

Table 4 Experiment results of GAPSOBP neural network and the comparison with actual results

时间	实验	实际	时间	实验	实际	时间	实验	实际	时间	实验	实际
T_{141}	0	0	T_{151}	0	0	T_{161}	0	0	T_{171}	0	0
T_{142}	0	1	T_{152}	0	0	T_{162}	0	0	T_{172}	0	1
T_{143}	0	0	T_{153}	0	1	T_{163}	0	0	T_{173}	1	1
T_{144}	0	0	T_{154}	0	1	T_{164}	0	0	T_{174}	0	0
T_{145}	0	0	T_{155}	0	0	T_{165}	0	0	T_{175}	1	0
T_{146}	0	0	T_{156}	0	0	T_{166}	0	0	T_{176}	0	0
T_{147}	0	0	T_{157}	1	1	T_{167}	1	1	T_{177}	0	0
T_{148}	0	0	T_{158}	0	0	T_{168}	1	1	T_{178}	0	0
T_{149}	0	0	T_{159}	0	0	T_{169}	1	0	T_{179}	0	0
T_{150}	0	0	T_{160}	1	1	T_{170}	0	0	T_{180}	0	0

4 结论

通过神经网络模型,并基于社会网络与事件的关联性,对恐怖事件的监测与识别问题进行了研究,得出以下结论。

1) 在考虑恐怖组织社会网络变化与恐怖事件关联性的前提下,通过实时检测社会网络结构参数的变化,可有效实现恐怖事件的监测与识别。

2) 神经网络将恐怖组织社会网络参数作为输入层,将恐怖事件发生情况作为输出层,通过不断学习,可以有效地掌握这一关联性。

3) 针对恐怖组织的特征,通过遗传算法和粒子群算法改进的BP神经网络在恐怖组织社会网络变化检测和恐怖事件监测与识别方面具备很好的能力。

通过社会网络变化检测实现对恐怖事件的监测与识别,是反恐领域的一个新兴领域,未来还需在以下3个方面进行改进。

1) 针对恐怖组织的特征与恐怖事件监测与识别的特性,设计更好的神经网络模型。

2) 寻找更好的网络参数来代表网络结构,作为神经网络的输入层。

3) 将恐怖事件的发生更好地用数量化的形式表现出来,使结果更接近于实际情况。

当然,作为一个“黑箱系统”,神经网络方法虽然可以检测出网络的异常变化,却只能有限地解释造成这一结果的原因。同时,神经网络从历史数据中得到训练,只能实现事件的监测与识别,但是要做到有效的预警,则需要对未来短期的网络数据进行预测和判断,并且要在更小的时间范围内构建社会网络(如每日或者每周)。然而,当前恐怖组织数据的获取仍然是一个短板,在网络数据的实时更新方面还有许多工作要做,这需要各相关领域加强合作,并加强国际交流。

参考文献 (References)

- [1] Chen H, Chung W, Qin J, et al. Uncovering the dark web: A case study of Jihad on the web[J]. *Journal of the American Society for Information Science and Technology*, 2008, 59(8): 1347-1359.
- [2] Carley Kathleen, Lee Ju-Sung, Krackhardt David. Destabilizing terrorist networks[J]. *Connections*, 2001, 24(3): 79-92.
- [3] Krebs V. Mapping networks of terrorist cells[J]. *Connections*, 2001, 24(3):43-52.
- [4] McCulloh I, Carley K, Webb M. Social network monitoring of Al-Qaeda [J]. *Network Science*, 2007(1): 25-30.
- [5] McCulloh I, Carley K M. Detecting change in longitudinal social networks[R]. New York: Military Academy West Point NY Network Science Center (NSC), 2011.
- [6] 刘棟, 罗军勇, 刘琰. 社会网络的动态建模与变化检测技术[J]. *计算机工程*, 2011, 37(19): 47-49.
Liu Lian, Luo Junyong, Liu Yan. Dynamic modeling and change detection technology of social network[J]. *Computer Engineering*, 2011, 37(19): 47-49.
- [7] Priebe C E, Conroy J M, Marchette D J, et al. Scan statistics on enron graphs[J]. *Computational and Mathematical Organization Theory*, 2005, 11(3): 229-247.
- [8] Sun J, Faloutsos C, Papadimitriou S, et al. Graphscope: Parameter-free mining of large time-evolving graphs[C]//Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2007: 687-696.
- [9] Peel L, Clauset A. Detecting change points in the large-scale structure of evolving networks[J]. *arXiv*, 2014: 1403.0989.
- [10] Li S, Xie Y, Farajtabar M, et al. Detecting weak changes in dynamic events over networks[J]. *arXiv*, 2016: 1603.08981.
- [11] 胡文斌, 彭超, 梁欢乐, 等. 基于链路预测的社会网络事件检测方法[J]. *软件学报*, 2015, 26(9): 2339-2355.
Hu Wenbin, Peng Chao, Liang HuanLe, et al. Event detection method based on link prediction for social network evolution[J]. *Journal of Software*, 2015, 26(9): 2339-2355.
- [12] Allanach J, Tu H, Singh S, et al. Detecting, tracking, and counteracting terrorist networks via hidden Markov models[C]//Aerospace Conference. Big Sky, MT: IEEE, 2004, 5: 3246-3257.
- [13] 张景阳, 潘光友. 多元线性回归与BP神经网络预测模型对比与运用研究[J]. *昆明理工大学学报(自然科学版)*, 2013, 6: 61-67.
Zhang Jingyang, Pan Guangyou. Comparison and application of multiple regression and BP neural network prediction model[J]. *Journal of Kunming University of Science and Technology (Natural Science Edition)*, 2013, 6: 61-67.
- [14] Zhang G, Patuwo B E, Hu M Y. Forecasting with artificial neural networks: The state of the art[J]. *International Journal of Forecasting*, 1998, 14(1): 35-62.
- [15] Deepa S N. An intelligent computing model for wind speed prediction in renewable energy systems[J]. *Procedia Engineering*, 2012, 30: 380-385.
- [16] 刘硕, 何永秀, 陶卫君, 等. 遗传BP神经网络的煤价预测与煤价风险规避策略[J]. *华北电力大学学报(自然科学版)*, 2009, 36(6): 75-80.
Liu Shuo, He Yongxiu, Tao Weijun, et al. Coal price forecasting based on GABP neural network and risk resistance strategy[J]. *Journal of North China Electric Power University (Natural Science Edition)*, 2009, 36(6): 75-80.
- [17] 张佳伟, 张自嘉. 基于PSO-BP神经网络的短期光伏系统发电预测[J]. *可再生能源*, 2012, 30(8): 28-32.
Zhang Jiawei, Zhang Zijia. Short-term photovoltaic system power forecasting based on PSO-BP neural network[J]. *Renewable Energy Resources*, 2012, 30(8): 28-32.
- [18] 江祥奎, 范永青, 王婉. 基于粒子群遗传算法的BP神经网络摄像机标定[J]. *计算机科学与探索*, 2014, 8(10): 1254-1262.
Jiang Xiangkui, Fan Yongqing, Wang Wan, et al. BP neural network camera calibration based on particle swarm optimization genetic algorithm[J]. *Journal of Frontiers of Computer Science and Technology*, 2014, 8(10): 1254-1262.
- [19] 潘勇, 郭晓东. 一种基于遗传算法改进的粒子群优化算法[J]. *计算机应用与软件*, 2011, 28(9): 222-224.
Pan Yong, Guo Xiaodong. An improved particle swarm optimisation algorithm based on genetic algorithm[J]. *Computer Applications and Software*, 2011, 28(9): 222-224.
- [20] 高玉明, 张仁津. 一种GA-PSO算法优化BP网络的网络流量预测[J]. *计算机应用与软件*, 2014, 31(4):106-110.
Gao Yuming, Zhang Renjin. A network traffic prediction based on BP neural network optimized by a GA-PSO algorithm[J]. *Computer Applications and Software*, 2014, 31(4): 106-110.
- [21] Carley K M, Pfeffer J, Reminga J, et al. ORA user's guide 2013[R]. Pittsburgh: Institute for Software Research, Carnegie Mellon University, 2013.
- [22] 范高锋, 王伟胜, 刘纯. 基于人工神经网络的风电功率短期预测系统[J]. *电网技术*, 2008, 32(22): 72-76.
Fan Gaofeng, Wang Weisheng, Liu Chun. Artificial neural network based wind power short term prediction system[J]. *Power System Technology*, 2008, 32(22): 72-76.
- [23] 沈花玉, 王兆霞, 高成耀, 等. BP神经网络隐含层单元数的确定[J]. *天津理工大学学报*, 2008, 24(5): 13-15.
Shen Huayu, Wang Zhaoxia, Gao Chengyao, et al. Determine the number of BP neural network hidden layer units[J]. *Journal of Tianjin University Technology*, 2008, 24(5): 13-15.
- [24] Zimmerman K. The Al Qaeda network: A new framework for defining the enemy [R/OL]. (2013-09-10) [2016-08-16]. <http://www.criticalthreats.org/al-qaeda/zimmerman-al-qaeda-network-new-framework-defining-enemy-september-10-2013>.
- [25] John Jay & ARTIS Transnational Terrorism Database[EB/OL]. [2016-08-20]. <http://doitapps.jjay.cuny.edu/jjatt/data.php>.
- [26] Moon I C. Destabilization of adversarial organizations with strategic interventions[D]. Pittsburgh: School of Computer Science, Carnegie Mellon University, 2008.

Terrorist events monitoring and identifying based on correlation between social networks and events

LI Ze, SUN Duoyong, LI Bo

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

Abstract The social networks of terrorist organization and terrorist events are changing correlatively. Based on the correlation between social networks and events, detecting changes in the networks may effectively help monitor and identify terrorist events. Terrorist attack early-warning is regarded as a classification problem, and neural network is used to solve this problem. The time when any terrorist attack happens is identified as a “change” point. Then the corresponding network is labeled as a changed one. Accordingly, the time sequence networks are classified into two sets: “changed” and “unchanged”. Measures of networks are obtained by social network analysis to represent networks. Hybrid heuristic algorithms are applied to optimizing the neural network. The classified network measures and the Boolean data of whether the terrorist events have happened are taken as the input and output, respectively. A real-world case study is given to show that detecting changes in terrorist networks based on neural network has the ability to monitor and identify terrorist events. Comparison results also show that the proposed approach can solve the problems such as versatility, accuracy and correlation encountered by the existing methods to some extent.

Keywords terrorist network; change detection; terrorist events; monitoring and identifying; neural network

(编辑 王志敏)