基于社团重叠的电力通信相依网络建模及其抗毁性分析

龙覃飞[1],王 涛[1],顾雪平[1],王铁强[2]
(1. 华北电力大学 电气与电子工程学院,河北 保定 071003;2. 河北电力调度通信中心,河北 石家庄 050021)

摘要:为了更好地揭示电力通信网络系统特性,基于社团重叠理论与相依网络模型提出一种更符合实际的电力通信网络系统建模方法。分析了实际通信网的网架结构特点,利用点边图转换以及马尔科夫聚类算法对电力网进行社团划分,进而确定社团重叠节点。依据社团重叠节点和相依网络模型建立通信网模型,进而构建了电力通信相依网络系统层级拓扑结构与耦合关系。对IEEE标准算例搭建对应的电力通信网络,基于信息攻击建立电力通信网失效模型,并依据节点损失比例、负荷损失比例、网络相对效率指标进行抗毁性分析。结果表明随着攻击者攻击方式的改进,攻击对系统造成的破坏越大;网络规模的扩大,能够显著提高网络对随机攻击的耐受力;相对于传统建模方法,所建模型更能体现实际电力通信网的抗毁能力。

关键词:电力信息物理融合系统;混合系统模型;重叠社区;相依网络;抗毁性分析
中图分类号:TM 73 **文献标志码**:A DOI:10.16081/j.epae.201911021

0 引言

电力信息物理融合系统CPPS(Cyber-Physical Power System)是以信息物理融合技术为基础,将智能电网中电力网和通信网进行耦合所构成的一种新型网络[1-2]。一方面,CPPS能够使得传统电网适应新型业务的发展需要,如电网信息采集与监控、智能电力调度、新能源并网等;另一方面,CPPS中电力网与通信网的结合,也使电力网间接地由一个封闭网络变为开放网络,电力网络遭受信息攻击风险增大,这也给电力系统的安全稳定运行带来了新的挑战[3]。

CPPS建模作为基础性工作,对CPPS后续理论分析与研究开展具有重要意义[4],因此众多学者对于CPPS建模进行了多方面的研究。文献[5]从意大利电网大停电出发,分析了其耦合特性,提出相依网络模型对CPPS网络建模。文献[6]从通信网的角度,提出一种基于仲裁网络控制系统方法的CPPS建模架构。文献[7]运用细胞自动机,将CPPS中的节点建模为电力细胞与信息细胞,并研究影响它们状态转换的因素。文献[8]利用关联特性矩阵建立CPPS网络,定量地描述了CPPS各耦合部分间的逻辑关联。上述研究对提高CPPS建模的发展奠定了坚实的基础,但是部分研究[6-8]较少考虑通信网与电力网的实际拓扑结构,使得模型脱离实际,实用性较差;另外一些研究[5]直接采用某个实际CPPS拓扑探究CPPS的性能,但是过于具体的CPPS只能反映其本身的特性,可拓展性较低,缺少推广价值。

电力网与通信网深度融合势在必行,建立更接近实际的CPPS模型是电力信息物理系统研究的基础[9]。社团结构作为复杂网络的重要性质,通常指复杂网络由多个功能相近或性质相似的网络节点组成的现象,其实质是网络节点间物理、化学或社会作用关系的区域耦合[10]。针对我国电力网实行分层分区建设的现象,研究者引入社团结构以表征区域电网被划分为不同电力子网的结构特征[11]。文献[12]考虑实际通信网以及电力网的社团结构,探讨了不同耦合方式对其连锁故障鲁棒性的影响。文献[13]考虑网络的介观局域特征和社团结构划分通信网社团。而文献[14-15]通过比较我国省份实际通信网拓扑结构以及规划,表明我国通信网拓扑与电力网拓扑具有很强的社团重叠现象。通信网的重叠社团直接影响CPPS的拓扑模型,也会间接影响CPPS模型中的节点耦合关系。因此,在CPPS建模中充分考虑实际网络的社团重叠现象对于构建更加精确的具有一般性的CPPS模型具有很强的现实意义。

本文在分析“十二五”关于一级骨干通信网的技术规划[14]与“十三五”关于建设“坚强智能电网”[15]的要求的基础上,结合实际CPPS的规划需要,依据社团重叠理论和相依网络模型,从实际通信网与电力网拓扑结构出发,构建电力通信相依网络模型,并对其进行抗毁性分析研究。首先采用基于边图的改进马尔科夫聚类MCL(Markov CLuster algorithm)方法,通过将CPPS网络拓扑由点图转换为边图后,利用马尔科夫聚类与LHN(Leicht-Holme-Newman)相似度计算方法对边图进行分区,最后将分区后得到的边社团逆转换为点社团,从而找出重叠节点,再依据社团重叠构建通信网层级拓扑结构建立CPPS耦合网络,并利用信息攻击探究所建耦合网络的抗毁性。

收稿日期:2019-01-23;**修回日期**:2019-09-25
基金项目:国家自然科学基金资助项目(51677071);中央高校基本科研业务费专项资金资助项目(2016MS130)
Project supported by the National Natural Science Foundation of China(51677071) and the Fundamental Research Funds for the Central Universities(2016MS130)

1 实际电力通信网社团重叠特征

通信网是电力网的重要设施之一，如何布局新一代电力通信线路资源，完善电力骨干网整体架构，成为了“十三五”时期电力通信部门面临的任务。在文献[14-15]中，湖南、江苏两省分别从本省具体的通信网架结构出发，对现有网架结构进行规划建设，江苏省骨干网通信拓扑如附录中的图A1所示。由图A1可见，服务电力生产的通信网一般可划分为多个骨干环网结构，且通信环网内部节点间相较于其他通信节点连接更为紧密，因此通信网骨干环可被定义为通信网社团。通过分析实际通信网拓扑可发现，各骨干环之间存在交叉重叠区域，即为社团重叠区域，交叉重叠区域的节点，往往设置为省调度中心或区域调度中心。此外，相关研究表明[16]，对于下层由数据采集与监视控制（SCADA）系统组成的局部区域，为了增加可靠性，往往会连接到2个以上的骨干环节点，即表明单个骨干环节点至少会接收、传输2个局部区域信息，这表明其处于下层SCADA分区的重叠位置。

从有关通信网组网模式的研究[16-17]可知，智能变电站或调度中心的选址，既要考虑管理区域的分配与传输性能的优化，又要考虑网络结构的布置与成本经济性。按社团重叠区域布置选址能够较好地满足上述要求，一是因为社团重叠区域是以区域社团进行划分查找，能避免重叠区域的布置松散或紧凑，使网络结构布置与传输性能得到优化；二是因为上层站点可按照重叠社团分区结果分配其所管理的社团区域，有效减少管理区域冗余，降低了线路架设量，从而使管理区域分配与经济成本得到优化。因此为了满足这些选址要求，智能变电站与调度中心的选址都会存在一定的社团重叠的现象。

2 基于社团重叠的相依网络建模

电力通信相依网络主要由电力网与通信网耦合组成，本质是一个双层相依网络。本文将地区单个通信骨干环抽象为一个社团，通信骨干环的相交区域作为社团重叠区域，即可运用社团重叠理论对通信网拓扑进行解释与建模。

2.1 基于边图的社团重叠发现理论

2.1.1 点边图转换

CPPS通常抽象为点图，它以节点作为分析对象，节点间的联系用边描述。但本文所用社团重叠算法需要分析边的不同归属，即以边为分析对象，故将点图转换为边图。定义点图$G(V,E)$，其中V、E分别为复杂网络的节点集与边集，对其进行社区划分得到的是关于节点集合的划分，这里称为点社团C[18]。另外，定义边图$G_{\text{link}}(V_{\text{link}},E_{\text{link}})$，其中$V_{\text{link}}$、$E_{\text{link}}$分别为图$G$进行点-边转换后得到的新图$G_{\text{link}}$的节点集和边集，对$G_{\text{link}}$进行社区划分得到的社团，则是$G$中边集合的划分，因此称为边社团$C_{\text{link}}$[19]。需要指出的是，将点图$G$转换为边图$G_{\text{link}}$，即是将点图$G(V,E)$中的边集$E$作为边图$G_{\text{link}}$的点集合$V_{\text{link}}$，而点集$V$作为边图$G_{\text{link}}$的边集合$E_{\text{link}}$，得到边图$G_{\text{link}}(V_{\text{link}},E_{\text{link}})$。

2.1.2 LHN相似度矩阵

从边图G_{link}的邻接矩阵$\boldsymbol{A}_{\text{link}}$中，可得到边图点集$V_{\text{link}}$中各节点之间的联系。本文采用LHN相似度计算方法[20]得到边图G_{link}的相似度矩阵$\boldsymbol{S}_{\text{link}}$，以此衡量边图点集$V_{\text{link}}$中各个节点与其邻居节点之间的节点相似度。相似度矩阵$\boldsymbol{S}_{\text{link}}$中的对应元素可以通过以下公式求解。

$$S_{\text{link}}(i,j)=\begin{cases}\dfrac{2m_{\text{link}}\lambda_{\text{link}}}{k_{\text{link}}(i)k_{\text{link}}(j)}\dfrac{S_{\text{t}}(i,j)}{\max(\boldsymbol{S}_{\text{t}})} & i\neq j\\ 1 & i=j\end{cases}\tag{1}$$

$$\boldsymbol{S}_{\text{t}}=\left(\boldsymbol{I}-\frac{\alpha}{\lambda_{\text{link}}}\boldsymbol{A}_{\text{link}}\right)^{-1}\tag{2}$$

其中，m_{link}为边图G_{link}的边数；λ_{link}为边图邻接矩阵$\boldsymbol{A}_{\text{link}}$的最大特征值；$k_{\text{link}}(i)$为边图节点$i$的度；$\max(\boldsymbol{S}_{\text{t}})$为矩阵$\boldsymbol{S}_{\text{t}}$的最大元素；$\boldsymbol{I}$为与$\boldsymbol{A}_{\text{link}}$行列数相同的单位矩阵；$\alpha$为LHN相似度参数。

2.1.3 基于马尔科夫聚类的重叠社团查找

传统社团重叠算法一般从派系过滤出发，通过贪婪算法找出各派系重叠部分从而找出重叠节点[21]；但其要求派系必须为全耦合模式，这使得其应用于CPPS时会导致大量网络节点被忽略。另一种传统算法为局部社团发现方法，它通过随机选择网络中的种子节点，结合适应度函数扩展社团[22]；但其种子节点选择随机，易使社团重叠部分处于较边缘位置，与CPPS重叠部分即调度中心拓扑中心度较大的原则违背。而马尔科夫聚类算法能使划分社团不产生较大的重叠区域并弱化非社团全耦合结构的影响[23]。本文利用马尔科夫聚类算法对相似度矩阵$\boldsymbol{S}_{\text{link}}$进行社团聚类分析，具体步骤如下。

（1）扩展（expansion）：将相似度矩阵$\boldsymbol{S}_{\text{link}}$自乘$e$次，并使矩阵列归一化。

$$\begin{cases}\boldsymbol{M}=(\boldsymbol{S}_{\text{link}}^{(k)})^{e}\\ S_{\text{link}}^{(k+1)}(i,j)=\dfrac{M(i,j)}{\sum_{n=1}^{m}M(n,j)}\end{cases}\tag{3}$$

其中，k为迭代的次数；m为矩阵$\boldsymbol{M}$的行数。

（2）膨胀（inflation）：将相似度矩阵$\boldsymbol{S}_{\text{link}}$点乘$r$次，并进行列归一化处理。

$$S_{\text{link}}^{(k+1)}(i,j)=\frac{(S_{\text{link}}^{(k)}(i,j))^{r}}{\sum_{n=1}^{m}(S_{\text{link}}^{(k)}(n,j))^{r}}\tag{4}$$

（3）迭代步骤（1）、（2），直至满足式（5）。

$$S_{\text{link}}^{(k+1)}(i,j)=(S_{\text{link}}^{(k+1)}(i,j))^2 \tag{5}$$

2.1.4　点社团复原与过度相似社团处理

从 $\boldsymbol{S}_{\text{link}}$ 中可得到划分好的边社团 C_{link}。由于 V 中的节点可以与多条边相连，根据节点的多条边的不同归属可使节点从属于于不同的社团，利用该思想将边图 G_{link} 上划分好的边社团 C_{link} 转换为对应点图 G 上的点社团 C，找出 C 中从属于社团数大于 1 的节点即为所找的重叠节点。这样，通过 2.1.1 节的方法反向进行边图–点图转换，即可得到原网络的点社团划分以及社团重叠节点。

因为原网络中存在一些度大于 2 的节点，所以从边社团 C_{link} 转换为点社团 C 时，重叠社团节点可能存在冗余。为使区域划分边界的拓扑中心度与冗余度处在合理范围内，从节点冗余和社团冗余 2 个方面出发，对社团划分进行过度相似处理。

情况 1：节点从属社团数量超过其网络规模所限阈值，如式（6）所示。

$$D(V_{\text{p}}(i))>\theta \tag{6}$$

其中，$D(V_{\text{p}}(i))$ 为点图节点 i 所属的社团数；θ 为限定阈值。当满足情况 1 后，按照节点 i 所属社团规模从大到小依次剔除自身社团的节点 i，直到满足阈值 θ。

情况 2：社团间重合的节点相似度超过阈值，如如式（7）所示。

$$Y(C(i),C(j))>\zeta \tag{7}$$

其中，$C(i)$ 为划分后的社团 i；$Y(C(i),C(j))$ 为社团 i、j 的节点相似度；ζ 为所限定的阈值。当满足情况 2 后，对 2 个社团进行合并处理。

2.1.5　重叠节点筛选

从划分好的点社团 C 中，查找出网络的社团重叠节点，即将所属社团数大于 1 的节点，归入重叠节点集 V_{o}：

$$V_{\text{o}}=\left\{V_{\text{p}}\,\middle|\,D(V_{\text{p}})>1\right\} \tag{8}$$

2.2　电力通信相依网络建模

常规而言，电力通信网可由电力网和通信网构成。电力网（源、网、荷）具有相同的物理性质，都是电力能量流的传播，而通信网通过监控与采集电力网能量流的数据，生成信息流。通信网因其多层次、多业务的组网特点，通常分为接入层、骨干层和核心层[24]3层。接入层主要是由布置在各厂站与电力负荷的SCADA系统构成，其设备分布通常与电力网站点对应；骨干层主要由架设的光缆以及各地区变电站组成；核心层主要是由调度中心构成，往往配有备用调度中心。

由第 1 节可知，CPPS 中通信网各骨干环间存在交合重叠区域，运用社团重叠理论表示交合重叠区域，并根据实际电力网以及通信网 3 层组网特点，结合社团重叠对实际 CPPS 的描述，可构建更符合实际的 CPPS 模型。

2.2.1　电力网模型

基于复杂网络理论，从简化角度出发，将电力网拓扑中的电力设备抽象为电力节点 $V_{\text{p}}=\{1,2,\cdots,N\}$，表示电力网的节点集，将输电联络线抽象为电力网连接边 E_{p}，表示电力网的边集合，得到电力网拓扑图 $G_{\text{p}}(V_{\text{p}},E_{\text{p}})$，其邻接矩阵为 $\boldsymbol{A}_{\text{p-p}}$，$\boldsymbol{A}_{\text{p-p}}$ 中元素 $A_{\text{p-p}}(i,j)=1$ 表示节点 i 与节点 j 相连，$A_{\text{p-p}}(i,j)=0$ 表示节点 i 与节点 j 不相连。

2.2.2　通信网接入层模型

从实际电力通信耦合网中可知，通信网接入层设备通常安置于电力网站点中，两者分布对应，因此接入层的网架结构与电力网的网架结构具有很强的拓扑相似性。所以，令 $G_{\text{c1}}(V_{\text{c1}},E_{\text{c1}})$ 为通信网接入层拓扑结构，其节点个数、拓扑结构与电力网相同，即：

$$G_{\text{c1}}(V_{\text{c1}},E_{\text{c1}})=G_{\text{p}}(V_{\text{p}},E_{\text{p}}) \tag{9}$$

$$\boldsymbol{A}_{\text{c1-c1}}=\boldsymbol{A}_{\text{p-p}} \tag{10}$$

其中，$\boldsymbol{A}_{\text{c1-c1}}$ 为通信网接入层的邻接矩阵，且通信网接入层与电力网为一对一全耦合关系。

2.2.3　通信网骨干层模型

电力通信网骨干层网络主要是由各个网络区域的传输系统和控制系统组成，且节点主要位于电网社团分区中的重叠部分或者交叉部分[14-15]。电网社团分区，可以用社团理论来解释，而重叠部分，则属于多个社团间重叠的区域。

使用 2.1 节所述理论，对电力网或通信网接入层网络进行社团分区，找到各个社团之间相互重叠的节点，归入重叠节点集 V_{o}。在这些节点上设立骨干层节点，且耦合节点间通过一条主传输线连接，即映射为通信网骨干层网络的节点 V_{c2}：

$$V_{\text{c2}}=V_{\text{o}} \tag{11}$$

然后基于贪婪算法，找到边集 E_{c2}，使点集 V_{c2} 间的节点相连，组成环形缠绕结构且通过的最小路径最短，由此得到通信网骨干层拓扑结构为 $G_{\text{c2}}(V_{\text{c2}},E_{\text{c2}})$，其邻接矩阵为 $\boldsymbol{A}_{\text{c2-c2}}$。通信网骨干层与通信网接入层属于部分一对一耦合关系，耦合节点为重叠节点，与电力网节点无直接耦合关系。

2.2.4　通信网核心层模型

电力通信网核心层主要为大区域电力调度中心以及备用电力调度中心。从实际网架结构可看出，通信网核心层网络节点数较少，且主要位于与通信网骨干层各个环形骨干网的重叠节点处，并且每个核心层节点与骨干层网络所有重叠节点相连。由 2.1 节理论可求出通信网骨干层重叠节点。综上可得到通信网核心层拓扑结构为 $G_{\text{c3}}(V_{\text{c3}},E_{\text{c3}})$，邻接矩阵为 $\boldsymbol{A}_{\text{c3-c3}}$。其与通信网骨干层为部分多对多耦合关

系，耦合节点为通信网骨干层的重叠节点，但是与通信网接入层和电力网无直接耦合关系。

2.2.5 电力通信相依网络模型

考虑到电力网与通信网各层邻接矩阵以及上下层对应的耦合关系，可以得到改进的CPPS模型$G_{cpps}(V_{cpps},E_{cpps})$，其邻接矩阵$\boldsymbol{A}_{cpps}$为：

$$\boldsymbol{A}_{cpps}=\begin{bmatrix}\boldsymbol{A}_{p-p} & \boldsymbol{A}_{p-c1} & 0 & 0\\ \boldsymbol{A}_{c1-p} & \boldsymbol{A}_{c1-c1} & \boldsymbol{A}_{c1-c2} & 0\\ 0 & \boldsymbol{A}_{c2-c1} & \boldsymbol{A}_{c2-c2} & \boldsymbol{A}_{c2-c3}\\ 0 & 0 & \boldsymbol{A}_{c3-c2} & \boldsymbol{A}_{c3-c3}\end{bmatrix} \tag{12}$$

其中，$\boldsymbol{A}_{c1-p}$、$\boldsymbol{A}_{p-c1}$、$\boldsymbol{A}_{c2-c1}$、$\boldsymbol{A}_{c1-c2}$、$\boldsymbol{A}_{c3-c2}$、$\boldsymbol{A}_{c2-c3}$为异层耦合矩阵，例如$\boldsymbol{A}_{p-c1}$为电力层与接入层的耦合矩阵。

根据上述方法，得到电力通信相依网络模型示意图如附录中的图A2所示。

3 CPPS抗毁性分析

现有CPPS模型大多从复杂网络角度去衡量耦合网络的抗毁性，如利用网络的最大连通分支尺寸[12]。另外一些模型则从电力系统角度进行评估，如采用负荷故障概率[25]等指标。本文结合复杂网络以及电力系统因素，采用节点损失比例、负荷损失比例、网络相对效率来综合评估CPPS网络的抗毁性，并利用信息攻击搭建CPPS网络失效模型。

3.1 评估指标

本文所采用指标定义如下。

(1)节点损失比例I_n。

$$I_n=\frac{N_0-N_1}{N_0} \tag{13}$$

其中，N_0为初始CPPS网络节点数目；N_1为遭受信息攻击后CPPS网络剩余节点数目。

(2)负荷损失比例I_{load}。

$$I_{load}=\frac{\sum_{i=1}^{N_2}P_{load}(i)}{P_s} \tag{14}$$

其中，$P_{load}(i)$为遭受攻击后节点i的切负荷量；P_s为系统的总负荷；N_2为系统中电力节点数目。

(3)网络相对效率I_E。

$$\begin{cases}I_E=\dfrac{E_0-E_a}{E_0}\\ E=\dfrac{2}{N(N-1)}\displaystyle\sum_{1\leqslant i<j\leqslant N}\frac{1}{d_{ij}}\end{cases} \tag{15}$$

其中，E_0为CPPS网络的原始效率；E_a为信息攻击后CPPS网络的网络效率；d_{ij}为网络中节点i到节点j的最短距离；N为网络中节点的总数。

3.2 电力通信网失效模型

根据实际电力通信网拓扑耦合关系可知，CPPS节点的运行状态与其能否继续运行有关。例如当某个发电站受到恶意攻击致其停运时，将会导致依赖其提供电源的通信网站点失去供电，如果通信网站点无备用电源，将导致其失效，如果存在备用电源，通信网站点能继续维持一段时间，但是在备用电源耗尽后供电还未恢复时，站点也失效。反之，当通信网某个调度中心被外部电脑病毒植入能量管理系统(EMS)时，如果成功，则可获取操作权限下发调度命令使底层发电机或变电站控制服务器关机，或传播病毒进行大范围感染[26]。因此，这种故障在电力网与通信网中交替传播，最终导致大面积站点失效。

为了简化失效模型，参照文献[3,5,12,24]，本文做出如下假设。

(1)假设信息攻击最终可以实现对电力设备运行的完全控制，因此信息攻击下电力系统本身的运行控制机制不能维持系统自治运行。

(2)假设通信站点存在备用电源但其维持时间有限，失效模型中添加通信设备失效延后的机制，即电力节点被攻击退出运行后，与其耦合的通信节点会延迟几个时段以概率形式退出运行，电力节点退出运行越久，耦合通信节点退出运行的概率越大。

(3)模型不考虑信息攻击的具体细节，假设在单位仿真时间攻击者可以攻击被选择的节点直至失效。

(4)在判定电力因素造成电力节点失效时考虑分配与减载，但在判断通信因素所造成的电力节点失效时，不考虑潮流重新分配和减载策略。

(5)CPPS中1个社团分区因一系列信息攻击而失去与大系统的联系，若分区仍与该区调度中心连接，则可孤岛运行；若某分区调度中心退出运行，则会引发连锁故障，最终导致整个分区失效。

为了更清晰地说明电力通信网失效模型，结合社团重叠理论与相依网络模型，以图1为例，通过2次信息攻击说明CPPS网络失效过程。

第1次攻击：攻击电力节点A_1，导致A_1失效，使得电力社团1中与之相连的连接边失效；另外，通信社团1中的B_1与A_1存在依存边，依存边失效，从而令B_1失效，与B_1相连的连接边也相继失效，失效范围用三角符号与点线表示。

第2次攻击：攻击电力节点A_4，导致A_4失效，电力社团1与最大电网区域失去连接，并与该区调度节点A_4断开，则电力社团1失效；另外，A_4与通信节点B_3存在依存边，则B_3失效，导致通信社团1与最大通信分区失去连接而失效，且通信社团2中与B_3相连的连接边失效；另外，B_2与电力社团2中的A_7存在依存边，使得A_7失效，进一步导致A_6失效，失效范围用正方形符号与点划线表示。

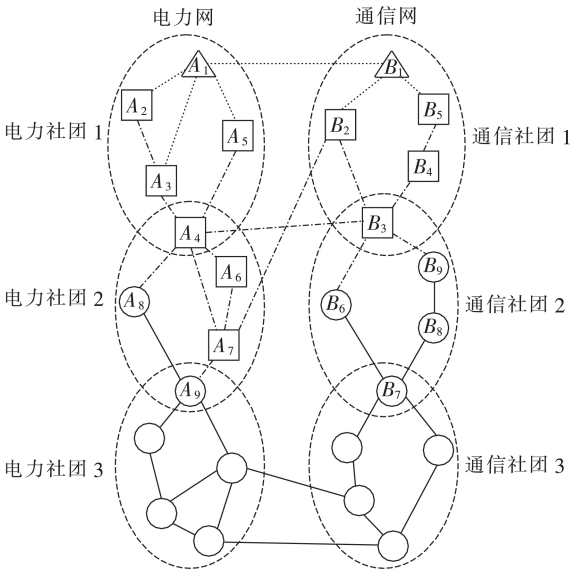

图 1　电力通信网失效模型示例

Fig.1　Example of power communication network failure model

4　算例分析

4.1　模型介绍

本文以 IEEE 39 节点系统为例，根据第 2 节 CPPS 建模规则，在 MATLAB 仿真软件上基于 MATPOWER 工具箱数据结构，构建电力通信相依网络模型，并探究其抗毁性。相关参数设置如下：LHN 相似度参数 $\alpha=0.3$，相似度矩阵 S_{link} 的扩展自乘指数 e、膨胀点乘指数 r 分别为 2 和 1.5，网络规模限定阈值 $\theta=2$，节点相似度限定阈值 $\xi=0.5$。

首先对 IEEE 39 节点的电力网拓扑进行社团分区，分区结果如表 1 所示。由表 1 可知：通信网接入层可被分为 5 个社团，一共包含 9 个重叠节点，这些重叠节点大多属于整个系统中心区域，节点拓扑中心度较大，能较好地体现出实际调度控制中心的设置区域。根据 9 个重叠节点依次构造通信网骨干层、核心层网络，最终可构建 CPPS 网络，其中包含 39 个电力节点、50 个通信节点，通信节点中包括 39 个接入节点、9 个骨干节点、2 个核心节点，具体 CPPS 网络模型如附录中的图 A3 所示。

表 1　IEEE 39 节点社团划分结果

Table 1　IEEE 39-bus community division results

社团	社团成员	重叠节点
1	1,2,4—9,11,30,31,39	4,6,11
2	4,6,10—15,32	4,6,11,15
3	3,15—21,24,27,33,34	15—17,21,24,27
4	16,21—24,35,36	16,21,24
5	17,25—29,37,38	17,27

4.2　抗毁性分析

为了更好地评估 CPPS 网络的抗毁性，本文依据第 3 节所述原理，在 MATLAB 软件上搭建电力通信网失效模型，以 CPPS 网络完全失效作为仿真运行结束标志。选择随机攻击、度数攻击、介数攻击 3 种攻击方式对所建 CPPS 模型进行抗毁性评估，仿真结果如图 2 所示。图中，“连续攻击次数”即为攻击直接造成的节点失效数量，例如，IEEE 39 节点系统中 15% 的节点受攻击，即约 6 个节点受到攻击，此时连续攻击次数为 6，后同。

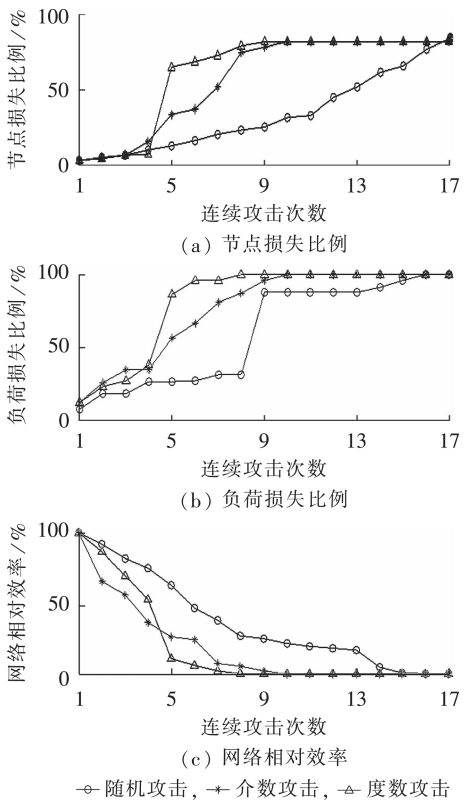

图 2　不同攻击下 IEEE 39 节点 CPPS 抗毁性对比

Fig.2　Invulnerability comparison of IEEE 39-bus CPPS among different attacks

在图 2(a)中，对于节点损失比例，度数攻击能较快地使 CPPS 网络系统的节点失效，体现出度数攻击存在更大的危害性。以 15% 的节点受攻击为例，受到随机攻击、介数攻击、度数攻击时的耦合网络故障节点损失比例分别约为 14.6%、36.0%、67.4%。从仿真攻击节点选择角度来看，度数攻击的对象节点中重叠区域的节点占比较高，其中包含重叠节点 6、11、16，被选择的重叠节点数高于其他攻击，体现出重叠节点的重要性。介数攻击也能使 CPPS 网络的节点快速失效，但相对于度数攻击而言，破坏网络所需的攻击次数相对较多，这主要是由于在 IEEE 39 节点系统中，拓扑结构复杂度不高，节点介数分布差异不大，介数攻击选择攻击节点部分处在系统边缘地区，导致造成的连锁故障危害程度较轻。随机攻击毁坏系统所需的攻击次数远高于介数攻击与度数

攻击。

由图2(b)、(c)可知，对于负荷损失比例与网络相对效率，在10%的节点受到攻击时，随机攻击下的负荷损失比例为26.5%、网络相对效率降低为74.6%；介数攻击下的负荷损失比例为34.6%、网络相对效率降低为35.9%；度数攻击下的负荷损失比例为37.9%、网络相对效率降低为52.1%。由此可知在攻击前期，介数攻击强于度数攻击，主要原因是部分高负荷节点位于重叠节点的邻接节点，而重叠节点的作用主要体现在能量传输上。另外介数攻击所选的节点介数都较高，易造成网络拓扑的毁坏，从而更容易降低网络相对效率。而若要造成CPPS网络完全失效，随机攻击需攻击近17次，介数攻击需攻击10次，度数攻击需攻击9次，即表明在信息攻击中后期，度数攻击造成的毁坏性更大，所需节点攻击次数更少。从图2中也可知，虽然网络中存在自制节点，但度数攻击可在不全使所有节点失效时，导致负荷损失比例为100%和网络相对效率降低为0，侧面体现现出度数攻击的强毁坏性，随机攻击造成同等破坏所需的攻击次数最多。

从3种评价指标可发现，在攻击前期，介数攻击对于CPPS网络的破坏较大，故障传播范围较广，而在攻击中后期时，度数攻击造成的毁坏性要大于介数攻击。总体而言，度数攻击在攻击次数上少于介数攻击。由此可知，攻击方式的毁坏性与重叠节点的选择有关，若某个攻击方式选择更多的重叠节点，则更可能造成较大的破坏；而攻击方式选择重叠节点的多少，与该攻击方式选择节点的判定标准、目标网络的拓扑结构有很大关系。随机攻击所需的攻击次数最多，但在时间允许的范围内，也能对CPPS网络系统造成较大的破坏性。

4.3 网络规模对抗毁性的影响

选取网络规模更大的IEEE 118节点系统，依据第2节所述理论搭建对应的CPPS模型，并对其进行抗毁性分析。本文的信息攻击方式选取随机攻击和度数攻击，对比IEEE 39节点与IEEE 118节点CPPS网络下模型的抗毁性，仿真结果如图3、4所示。

由图3可知，在随机攻击方式下，随着网络规模的增大，造成CPPS网络完全失效所需的攻击次数增加。在本文算例中，造成IEEE 39节点CPPS网络完全失效需连续攻击约17次，而造成IEEE 118节点CPPS网络需连续攻击约51次。在现实CPPS攻击中，采用随机攻击所需的代价最小，攻击者一般会先采取随机攻击策略对网络进行攻击，而仿真结果表明增加CPPS网络规模能够有效加强网络对随机攻击的抗毁性，防止危害发生。

由图4(a)和图4(b)可知，度数攻击下，当CPPS网络被连续攻击14次时，IEEE 39节点CPPS网络节

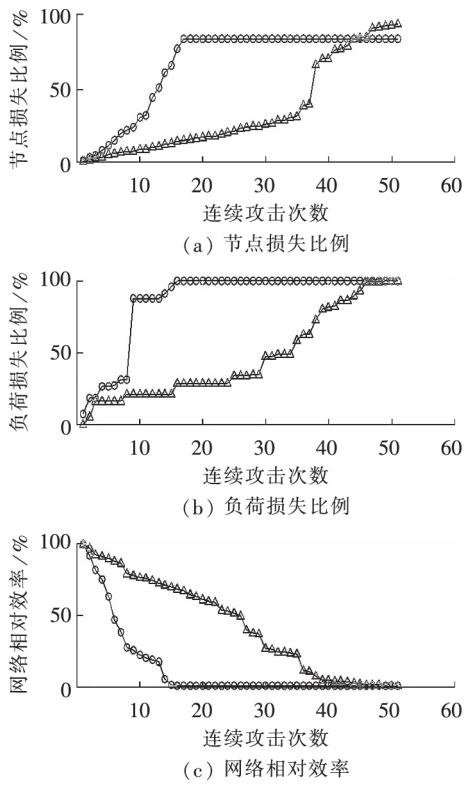

图3 随机攻击下各CPPS网络抗毁性对比

Fig.3 Invulnerability comparison under random attack between CPPS networks

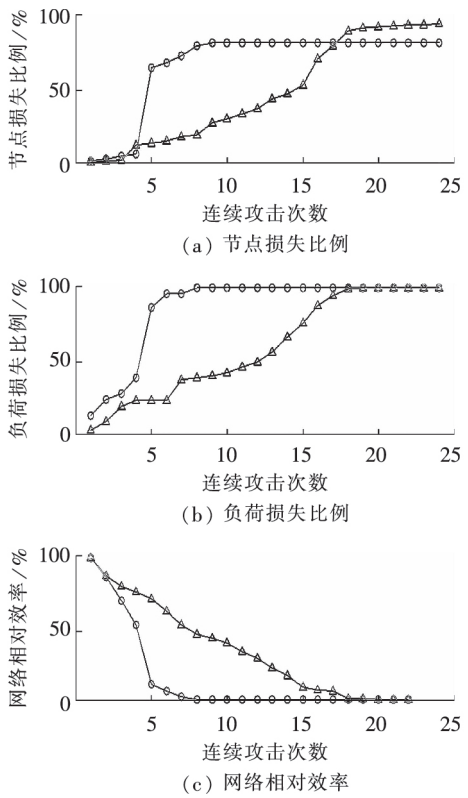

图4 度数攻击下各CPPS网络抗毁性对比

Fig.4 Invulnerability comparison under degree attack between CPPS networks

点损失比例和负荷损失比例已达上限，网络完全失效，而对于IEEE 118节点CPPS网络，其节点损失比例为46.6%，负荷损失比例为65.8%。这反映出网络规模的增大能够提高CPPS网络的攻击承受次数。

由图4(c)可知，度数攻击下，造成IEEE 39节点与IEEE 118节点网络相对效率降为0分别需要攻击约8、19次。从攻击次数占网络节点数比例来看，造成IEEE 39节点网络完全失效需攻击破坏网络中大约20.5% 的节点，而IEEE 118节点网络则需要攻击大约16.1% 的节点。由此可见，对于度数攻击，虽然提高网络规模可增加CPPS承受攻击的次数，但是瘫痪全网所需破坏的节点占全网络的比例降低，表明度数攻击在规模越大的网络下，单个攻击造成的连锁范围更广，这一方面是因为网络规模越大，故障传播的选择更多，另一方面是因为规模越大的网络负荷也相对越多，一旦引起连锁故障，则高负荷的转移对于网络会造成进一步破坏。

从2种CPPS网络抗毁性对比结果可知，在随机攻击下，网络规模的扩大能够显著提高网络承受攻击的能力。而在度数攻击下，网络规模的扩大可以提高网络承受攻击的次数，但规模越大瘫痪全网所需破坏节点占全网络的比例反而减小。现实中攻击者掌握的信息越多，越可能成功实施度数攻击，所以电网公司应在加强攻击识别及防御的同时做好相关信息保密工作。

4.4　CPPS建模方法对抗毁性的影响

传统CPPS建模方法一般采用双层一对一耦合方式[5]，并考虑电力层与通信层节点度、介数的排序，利用内在自相似性进行建模[27]。另一种CPPS建模方法则单方面考虑通信网分层设计原则，以网状结构对其进行拓扑建模[12,24]。分别选择传统一对一耦合CPPS模型、基于分层设计的CPPS模型，与本文提出的基于社团重叠的CPPS模型进行抗毁性比较。以IEEE 118节点系统为蓝本，运用3种建模方法，在MATLAB上搭建对应模型。表2给出了3种建模方法下CPPS模型的拓扑特征统计数据。

表2　IEEE 39节点社团划分结果

Table 2　IEEE 39-bus community division results

静态特征参数	参数值		
	基于社团重叠的CPPS模型	基于分层设计的CPPS模型	传统一对一耦合CPPS模型
电力层节点数	118	118	118
电力层支路数	179	179	179
通信层节点数	133	137	118
通信层支路数	213	301	179
节点平均度	4.0637	4.6902	4.0339
平均路径长度	6.4972	4.8125	6.7840
聚类系数	0.0827	0.1124	0.0732

从表中可知，传统一对一耦合CPPS模型的通信层节点数、支路数最少，其节点平均度和聚类系数较低，分别为4.0339、0.0732，表明其内部连接较稀疏。基于分层设计的CPPS模型，因其以环形辐射网进行拓扑连接，内部相对连接密度较大，节点平均度、聚类系数分别为4.6902、0.1124，节点间联系紧密，因此其平均路径长度较短，仅为4.8125。而基于社团重叠的CPPS模型，内部连接紧密程度介于传统一对一耦合CPPS模型、基于分层设计的CPPS模型之间。选取度数攻击，对以上3种CPPS模型进行抗毁性仿真，结果如图5所示。

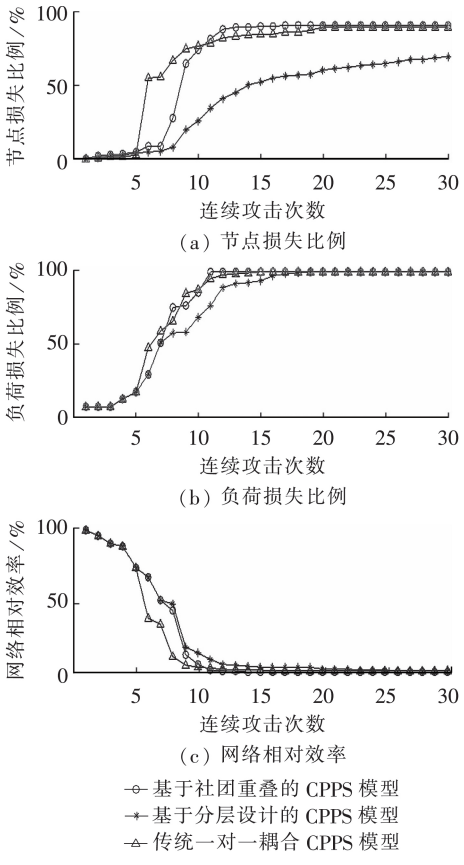

图5　基于3种建模方法的CPPS网络抗毁性对比

Fig.5　Comparison of invulnerability of CPPS networks based on three modeling methods

从图5(a)可知，传统一对一耦合CPPS模型易发生一阶相变，只需攻击较少的节点就能造成大范围的连锁故障，例如攻击约5.1% 的节点其节点损失比例就已达到56.8%，相同情况下基于分层设计和基于社团重叠的CPPS模型节点损失比例分别只有5.5% 和9.6%。这主要是由于传统一对一耦合CPPS模型内部连接稀疏，前期攻击时易导致整个网络断开为多个子网，破坏较大。而在后期攻击中，因子网间相互断开，抑制了连锁故障的传播，节点损失比例增长较小。

在图5(b)中，当攻击次数小于9时，传统一对一耦合CPPS模型因其故障传播范围大，负荷损失比例

较高，攻击约5.1%的节点时，其负荷损失比例为48.0%，而相同情况下基于分层设计和基于社团重叠的CPPS模型的负荷损失比例几乎相当，约为29.6%。随着攻击次数继续增加，基于社团重叠的CPPS模型的负荷损失比例超过其他模型。例如攻击次数超过9.3%的节点时，基于社团重叠的CPPS模型节点损失比例、负荷损失比例超过传统一对一耦合CPPS模型与基于分层设计的CPPS模型。结合图5(c)可知，当连续攻击次数小于10时，基于社团重叠的CPPS模型的网络相对效率与基于分层设计的CPPS模型的网络相对效率基本相同，都优于传统一对一耦合CPPS模型。

从实际CPPS遭遇攻击情况进行分析，攻击者在考虑攻击成本的情况下往往只能攻击网络中少量的节点，而且CPPS的保护与防御机制也能抑制大范围的攻击行为的开展，这使攻击者同时成功攻击网络中的大量节点几乎不可能实现。由相关文献[28-29]可知，一般将[5%，10%]作为最大攻击节点比例的合理范围，这里以最大攻击节点比例为7%为例进行分析。从图5中可看出，当攻击节点比例小于7%时，基于分层设计和基于社团重叠的CPPS模型，在节点损失比例、负荷损失比例、网络相对效率上都相差无几。这表明在现实合理的攻击强度下，两者的抗毁性几乎一致。但由表2可知，基于分层设计的CPPS模型中通信节点、支路分别有137个、301条，而同样的电力网规模下基于社团重叠的CPPS模型中通信节点、支路却分别只有133个、213条。本文模型的节点数少于基于分层设计的CPPS模型，支路数仅占70.76%，网络建设成本相差很大。在实际CPPS中，通信网节点、支路的造价费用直接影响了建设成本，上述结果表明基于社团重叠的CPPS拓扑更具经济性。

实际电力通信网结构需经过严谨规划设计，一对一耦合CPPS模型虽然因其构造简单而便于进行CPPS性质分析，但它只是根据假设规则构建CPPS的连接拓扑，考虑建模因素较少，不利于深入研究。基于分层设计的CPPS模型虽然考虑了通信网分层设计原则，但其拓扑结构以最优连接模式为准则，没有计及通信网络建设成本，虽然其抗毁性优良，但网络节点连接紧密，造价昂贵。本文基于社团重叠的CPPS模型是利用实际电力通信网的组网特征进行建模，因此借助了实际通信网规划综合考虑经济性与可靠性的优势，实验结果表明在实际攻击背景下其抗毁性能够充分反映出实际电力通信网的抗毁水平，这可为电网工作人员提供较为准确的评估数据。此外，在相同条件下本文CPPS模型的某些抗毁性指标计算结果与相关文献基本一致，尤其是与实际CPPS网络模型的指标计算结果基本相同，这说明文章所提模型构建方法是合理的。

5 结论

随着通信骨干网与电力网改造规划的深入，建立符合实际的电力通信相依模型越来越重要。本文参照实际通信网的拓扑结构，结合社团重叠理论以及相依网络模型，利用马尔科夫聚类算法与LHN相似度方法为辅助，构建了电力通信相依网络模型，所建模型能很好地反映出实际的组网特征。利用IEEE 39节点系统算例详细说明了CPPS建模方法流程，并利用信息攻击分析了所建模型的抗毁性。通过IEEE 118节点系统算例比较了不同网络规模以及不同建模方法对抗毁性的影响，结果表明网络规模的扩大能在一定程度上加强CPPS的抗毁性，并且本文方法所建模型更能体现实际电力通信网的抗毁能力。另外，本文抗毁性分析并未考虑信道传输与抗毁性间的联系、攻防博弈行为等情景。这些情景的引入将会对所建模型的准确性产生重要影响，而这需要在后续的工作中进行研究。

附录见本刊网络版(http://www.epae.cn)。

参考文献：

[1] 郭庆来，辛蜀骏，孙宏斌，等. 电力系统信息物理融合建模与综合安全评估：驱动力与研究构想[J]. 中国电机工程学报，2016，36(6)：1481-1489.
GUO Qinglai，XIN Shujun，SUN Hongbin，et al. Power system cyber-physical modelling and security assessment：motivation and ideas[J]. Proceedings of the CSEE，2016，36(6)：1481-1489.

[2] 刘汉宇，邱赟，牟龙华. 微电网CPS物理端融合模型设计[J]. 电力自动化设备，2014，34(10)：27-32.
LIU Hanyu，QIU Yun，MU Longhua. Conjunct model of physical side on microgrid CPS[J]. Electric Power Automation Equipment，2014，34(10)：27-32.

[3] 曹一家，张宇栋，包哲静. 电力系统和通信网络交互影响下的连锁故障分析[J]. 电力自动化设备，2013，33(1)：7-11.
CAO Yijia，ZHANG Yudong，BAO Zhejing. Analysis of cascading failures under interactions between power grid and communication network[J]. Electric Power Automation Equipment，2013，33(1)：7-11.

[4] DERLER P，LEE E A，VINCENTELLI A S. Modeling cyber-physical systems[J]. Proceedings of the IEEE，2012，100(1)：13-28.

[5] BULDYREV S V，PARSHANI R，PAUL G，et al. Catastrophic cascade of failures in interdependent networks[J]. Nature，2010，464(7291)：1025-1028.

[6] SOUDBAKHSH D，CHAKRABORTTY A，ANNASWAMY A M. A delay-aware cyber-physical architecture for wide-area control of power systems[J]. Control Engineering Practice，2017，60：171-182.

[7] 叶夏明，文福拴，尚金成. 电力系统中信息物理安全风险传播机制[J]. 电网技术，2015，39(11)：3072-3079.
YE Xiaming，WEN Fushuan，SHANG Jincheng. Propagation mechanism of cyber physical security risks in power systems[J]. Power System Technology，2015，39(11)：3072-3079.

[8] 薛禹胜，李满礼，罗剑波，等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化，2018，42(2)：

11-19.
XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11-19.
[9] 张文亮，刘壮志，王明俊，等. 智能电网的研究进展及发展趋势[J]. 电网技术，2009，33(13)：1-11.
ZHANG Wenliang, LIU Zhuangzhi, WANG Mingjun, et al. Research status and development trend of smart grid[J]. Power System Technology, 2009, 33(13): 1-11.
[10] ESTRADA E, HATANO N. Communicability in complex networks[J]. Physical Review E, 2008, 77(3): 1-20.
[11] 魏震波. 复杂网络社区结构及其在电网分析中的应用研究综述[J]. 中国电机工程学报，2015，35(7)：1567-1577.
WEI Zhenbo. Overview of complex networks community structure and its applications in electric power network analysis [J]. Proceedings of the CSEE, 2015, 35(7): 1567-1577.
[12] 汪勋婷，王波. 考虑信息物理融合的电网脆弱社团评估方法[J]. 电力自动化设备，2017，37(12)：43-51.
WANG Xunting, WANG Bo. Assessment method of vulnerable communities in power grid considering cyber-physical integration[J]. Electric Power Automation Equipment, 2017, 37(12): 43-51.
[13] TIAN M, WANG X, DONG Z, et al. Cascading failures of interdependent modular scale-free networks with different coupling preferences[J/OL]. [2018-10-30]. https://iopscience.iop.org/article/10.1209/0295-5075/111/18007.
[14] 王海勇，李伟. 江苏电网“省-市”骨干通信网第二平面建设[J]. 电力系统通信，2012，33(1)：6-9.
WANG Haiyong, LI Wei. The construction of the second plant of the “province to city” backbone communication network in Jiangsu grid[J]. Telecommunications for Electric Power System, 2012, 33(1): 6-9.
[15] 周静，胡紫巍，刘国军，等. 电力骨干通信网业务需求分析与拓扑规划[J]. 光通信研究，2016(2)：15-18.
ZHOU Jing, HU Ziwei, LIU Guojun, et al. Research on business requirement analysis and topology planning of backbone power communication network[J]. Study on Optical Communications, 2016(2): 15-18.
[16] 樊陈，倪益民，窦仁辉，等. 智能变电站过程层组网方案分析[J]. 电力系统自动化，2011，35(18)：67-71.
CHEN Fan, NI Yimin, DOU Renhui, et al. Analysis of network scheme for process layer in smart substation[J]. Automation of Electric Power Systems, 2011, 35(18): 67-71.
[17] 刘自发，张建华. 基于改进多组织粒子群体优化算法的配电网络变电站选址定容[J]. 中国电机工程学报，2007，27(1)：105-111.
LIU Zifa, ZHANG Jianhua. Optimal planning of substation of locat ing and sizing based on GIS and adaptive mutation PSO algorithm[J]. Proceedings of the CSEE, 2007, 27(1): 105-111.
[18] 潘磊，金杰，王崇骏，等. 社会网络中基于局部信息的边社区挖掘[J]. 电子学报，2012，40(11)：2255-2263.
PAN Lei, JIN Jie, WANG Chongjun, et al. Detecting link communities based on local information in social networks[J]. Acta Electronica Sinica, 2012, 40(11): 2255-2263.
[19] AHN Y Y, BAGROW J P, LEHMANN S. Link communities reveal multiscale complexity in networks[J]. Nature, 2010, 466(7307): 761-764.
[20] JOHNSON S C. Hierarchical clustering schemes[J]. Psychometrika, 1967, 32(3): 241-254.
[21] PALLA G, DERENYI I, FARKAS I, et al. Uncovering the overlapping community structure of complex networks in nature and society[J]. Nature, 2005, 435(7043): 814-818.
[22] LANCICHINETTI A, FORTUNATO S, KERTÉSZ J. Detecting the overlapping and hierarchical community stru-cture in complex net-works[J/OL]. [2018-10-30]. https://iopscience.iop.org/article/10.1088/1367-2630/11/3/033015/meta.
[23] DONGEN S. Performance criteria for graph clustering and Markov cluster experiments[J/OL]. [2018-10-30]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.26.9783.
[24] 王涛，孙聪，顾雪平，等. 电力通信耦合网络建模及其脆弱性分析[J]. 中国电机工程学报，2018，38(12)：3556-3567.
WANG Tao, SUN Cong, GU Xueping, et al. Modeling and vulnerability analysis of electric power communication coupled network[J]. Proceedings of the CSEE, 2018, 38(12): 3556-3567.
[25] 刘沛清，李华强，赵阳，等. 考虑元件综合重要度的电网安全性风险评估方法[J]. 电力自动化设备，2015，35(4)：132-138.
LIU Peiqing, LI Huaqiang, ZHAO Yang, et al. Power grid security risk assessment considering comprehensive element importance index[J]. Electric Power Automation Equipment, 2015, 35(4): 132-138.
[26] 郭庆来，辛蜀骏，王剑辉，等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化，2016，40(5)：145-147.
GUO Qinglai, XIN Shujun, WANG Jianhui, et al. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016, 40(5): 145-147.
[27] 陈柯任，文福拴，赵俊华，等. 考虑物理-信息虚拟连接的电力信息物理融合系统的脆弱性评估[J]. 电力自动化设备，2017，37(12)：67-72.
CHEN Keren, WEN Fushuan, ZHAO Junhua, et al. Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections[J]. Electric Power Automation Equipment, 2017, 37(12): 67-72.
[28] 刘涤尘，冀星沛，王波，等. 基于复杂网络理论的电力通信网拓扑脆弱性分析及对策[J]. 电网技术，2015，39(12)：3615-3621.
LIU Dichen, JI Xingpei, WANG Bo, et al. Topological vulnerability analysis and countermeasures of electrical communication network based on complex network theory[J]. Power System Technology, 2015, 39(12): 3615-3621.
[29] SOU K C, SANDBERG H, JOHANSSON K H. On the exact solution to a smart grid cyber-security analysis problem[J]. IEEE Transactions on Smart Grid, 2013, 4(2): 856-865.

作者简介：


龙覃飞

龙覃飞（1994—），男，广西忻城人，硕士研究生，主要研究方向为电力系统安全防御与恢复控制（**E-mail**：s39632852@foxmail.com）；

王　涛（1976—），男，陕西户县人，副教授，博士，主要研究方向为电力系统安全防御与恢复控制、复杂网络理论及其应用（**E-mail**：wtwxx@126.com）；

顾雪平（1964—），男，河北行唐人，教授，博士研究生导师，博士，主要研究方向为电力系统安全防御与恢复控制、电力系统安全稳定评估与控制、智能技术在电力系统中的应用（**E-mail**：xpgu@ncepu.edu.cn）；

王铁强（1970—），男，河北保定人，高级工程师，博士，主要研究方向为电力系统运行方式分析与管理工作（**E-mail**：18003218260@189.cn）。

（下转第 204 页 continued on page 204）

Forecasting regional E-GDP value using power big data

TIAN Shiming[1], GONG Taorong[1], HUANG Xiaoqing[2], YU Wenlong[2]
(1. Beijing Key Laboratory of Demand Side Multi-Energy Carriers Optimization and Interaction Technique, China Electric Power Research Institute Co., Ltd., Beijing 100192, China;
2. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China)

Abstract: In order to evaluate the economic development level of a region by using data of power development and utilization, a prediction method of E-GDP(E-Gross Domestic Product) which represents the development trend of regional GDP is proposed. Based on multi-source power big data and DBN(Dynamic Bayesian Network) machine learning, this method can screen out the key power data with a large correlation with the GDP change trend by gray correlation analysis method. Then, Granger causal analysis is used to determine the power indicators that have a causal relationship with GDP changes, and to determine the causal relationship among the various power indicators. Furthermore, the resulting causal relationship is used to establish a DBN to predict E-GDP. Finally, the proposed method is applied to the prediction of Shanghai E-GDP value. The example shows that the proposed method can accurately predict regional E-GDP value, and can also measure the probability distribution of GDP.

Key words: gray correlation analysis; Granger causal analysis; DBN; machine learning; GDP; power big data

(上接第173页 continued from page 173)

Modeling and invulnerability analysis of power communication interdependent network based on community overlapping

LONG Qinfei[1], WANG Tao[1], GU Xueping[1], WANG Tieqiang[2]
(1. School of Electrical and Electronic Engineering, North China Electric Power University, Baoding 071003, China;
2. Hebei Power Dispatch and Communication Center, Shijiazhuang 050021, China)

Abstract: In order to better reveal the characteristics of the power communication network, a more practical modeling method of power communication network is proposed based on the theory of community overlapping and the model of interdependent network. The characteristics of the actual communication network structure are analyzed, the power grid are divided into communities by point-to-edge community transformation and Markov clustering algorithm, and then the community overlapping nodes are determined. In accordance with the community overlapping nodes and the interdependent network model, a communication network model is established and then the hierarchical topology structure and coupling relationship of the power communication interdependent network system are constructed. A corresponding power communication network is set up for IEEE standard examples, and an improved failure model of the power communication network is established on the basis of information attacks. The invulnerability analysis is performed based on the node loss ratio, load loss ratio, and network relative efficiency index. The results show that the damage to the system caused by the attack is worse with the improvement of the attack method, and the expansion of the network scale can significantly improve the network's tolerance to random attacks. Compared with the traditional model, the proposed model demonstrates the anti-destructive ability of the actual power communication network with high accuracy.

Key words: cyber-physical power system; hybrid system model; overlapping community; interdependent network; invulnerability analysis

附录

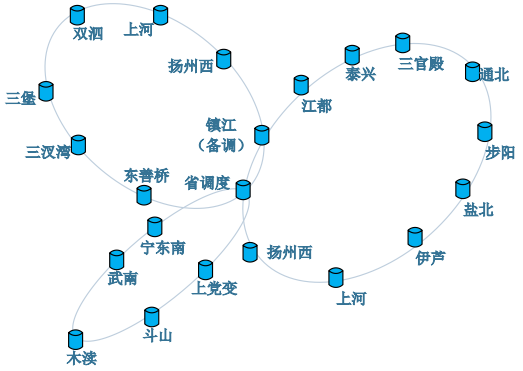

图 A1 江苏省骨干网通信拓扑示意图

Fig.A1 Topology diagram of backbone network communication in Jiangsu province

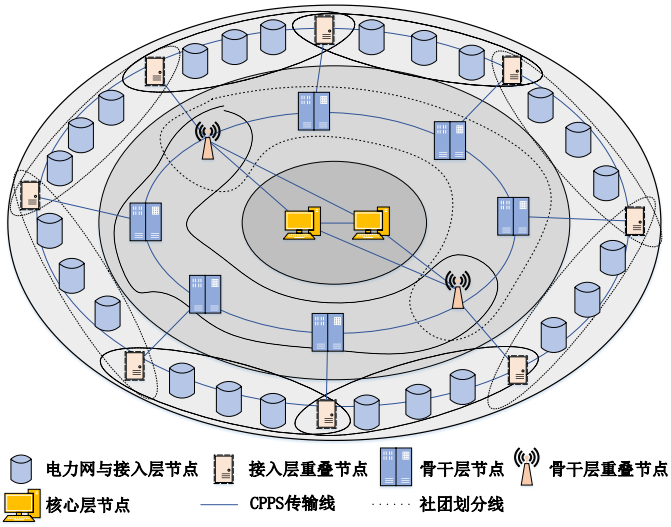

图 A2 基于社团重叠的 CPPS 网络示意图

Fig.A2 Schematic diagram of CPPS network based on community overlapping

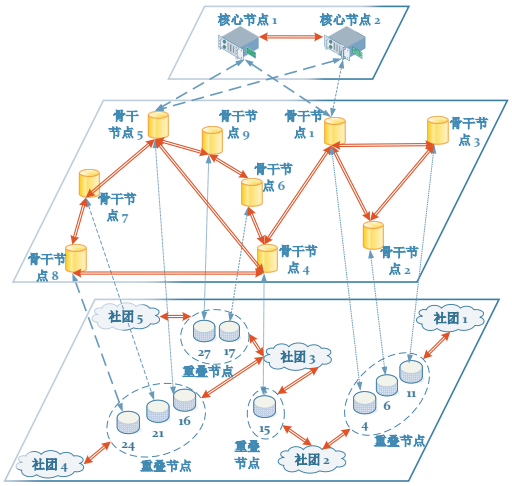

图 **A3** IEEE39 节点 CPPS 网络模型示意图

Fig.A3 Schematic diagram of IEEE 39-bus CPPS network model