引用格式:田京京,邢康,马永翔,等.基于IKS和潮流熵的电网关键节点识别与抗毁性分析[J].电力科学与技术学报,2024,39(6):1-10.
Citation: TIAN Jingjing, XING Kang, MA Yongxiang, et al. Identification of key nodes and analysis of damage resistance of power grids based on improved K-shell and power flow entropy[J]. Journal of Electric Power Science and Technology,2024,39(6):1-10.

基于IKS和潮流熵的电网关键节点识别与抗毁性分析

田京京[1,2],邢　康[1],马永翔[1],闫群民[1]
(1.陕西理工大学电气工程学院,陕西 汉中 723000;2.陕西理工大学数学与计算机科学学院,陕西 汉中 723000)

摘　要:为提高电网关键节点识别和抗毁性分析的准确性和速度,综合考虑拓扑结构与电气特性,将改进K-shell分解法(improved K-shell algorithm,IKS)中拓扑信息熵用潮流熵代替,将K壳值(K_s)和潮流熵加权求和所得值定义为评估节点重要度的新指标——节点重要度综合值,据该值大小对节点重要度进行排序,从而得到IKS与潮流熵的电网关键节点识别模型。以IEEE-118节点系统为例,用本文所提出方法和4种传统的关键节点识别方法进行节点识别,并以不同的攻击强度实施随机攻击和蓄意攻击试验,通过节点重要度排序、电网的最大连通子图规模及网络效率分析,验证本文所提出的基于IKS与潮流熵的关键节点识别方法优于介数中心性和接近中心性。

关　键　词:电网;关键节点识别;K-shell分解法;潮流熵;抗毁性
DOI:10.19781/j.issn.1673-9140.2024.06.001　　**中图分类号**:TM711　　**文章编号**:1673-9140(2024)06-0001-10

Identification of key nodes and analysis of damage resistance of power grids based on improved K-shell and power flow entropy

TIAN Jingjing[1,2], XING Kang[1], MA Yongxiang[1], YAN Qunmin[1]
(1.School of Electrical Engineering, Shaanxi University of Technology, Hanzhong 723000, China; 2.School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723000, China)

Abstract: In order to improve the accuracy and speed of key node identification and damage resistance analysis of power grids, the topological structure and electrical characteristics are considered comprehensively. The topological information entropy in the improved K-shell algorithm (IKS) is replaced by power flow entropy, and the value obtained by weighted summing of the K-shell (K_s) value and power flow entropy is defined as a new index for evaluating node importance, namely the comprehensive value of node importance. The comprehensive value of node importance is ranked, and the key node identification model with IKS and power flow entropy is obtained. By taking the IEEE-118 node system as an example, the proposed method and four traditional key node identification methods are used to identify nodes, and random attack and deliberate attack tests are carried out with different attack intensities. According to the node importance ranking, the maximum connectivity subgraph scale of power grids, and network efficiency analysis, the proposed key node identification method based on IKS and power flow entropy is superior to betweenness centrality and closeness centrality.

Key words: power grid; key node identification; K-shell algorithm; power flow entropy; damage resistance

中国能源活动所造成的碳排放量达到了全社会碳排放量的87%,其中电力生产活动产生的碳排放量超过了全社会能源活动碳排放量的40%。构建以新能源发电为主体的新型电力系统成为实现“双碳”目标的重要途径。但风力发电、光伏等多种新能源装机容量增长和并网总额迅速扩大,致使发电端不确定性加深,发电供给可控性变差,电网结构复杂性日渐增强,电网的抗毁性能要求将被提

收稿日期:2024-03-30;**修回日期**:2024-07-23
基金项目:国家自然科学基金(11961041);国家社科基金重大项目(21&ZD153)
通信作者:田京京(1979—),女,博士,教授,主要从事图论与复杂网络、电网评价与分析研究;E-mail:tianjingjing2004@163.com

高。评估电网结构与运行情况，发现潜在的故障点，预测系统的风险性，将是解决新能源并网的重要环节，电网关键节点识别和抗毁性评估成为了学界关注的热点课题。

以图论为基础的复杂网络理论是20世纪科学史上的里程碑。作为一门新兴学科，复杂网络理论出现较晚，但是已被广泛应用于经济、社会、计算机、医学、电力等众多学科领域[1-2]。运用复杂网络理论，以电网的拓扑结构为切入点，结合电网的电气特性分析电网的抗毁能力和关键节点识别成为前沿主流研究方法[3-8]。文献[9]提出K-shell分解法弥补了节点近邻、全局路径、特征向量和网络位置等复杂网络节点重要度传统评估方法的缺陷，一时间备受青睐，但由于区分度过低，导致众多节点重要度不能精准区分。以提高K-shell分解的区分度为目的K-shell改进方法(improved K-shell algorithm，IKS)逐步展开。如文献[10]提出混合度分解方法(mixing degree decomposition，MDD)；文献[11]提出了邻域核心中心度方法；文献[12]提出了一种K-shell迭代因子方法；文献[13]提出加权度方法；文献[14]基于K壳和节点信息熵改进K-shell分解法。

上述IKS被认为是简单且高效的重要节点识别方法，其中的信息熵由拓扑结构来确定。但电网作为特殊的复杂网络，其电气特性对网络稳定性的影响是不容忽视的，例如表征系统潮流分布程度的潮流熵，其值大小与电力系统的脆弱性相关，潮流熵值越大表示系统潮流分布越不均衡，系统受到扰动的概率越大，电力系统脆弱性越高，忽略如此重要的电气特性指标，将会影响电网关键节点识别和电网脆弱性分析的准确性。

针对上述问题，本文在运用IKS识别电网关键节点时，引入潮流熵——一种用于刻画电力系统电网运行状态的信息熵，并将IKS中基于拓扑结构的节点信息熵用潮流熵来代替，对K壳值(K_s)值和潮流熵标准化处理之后用熵权法求权重，并进行加权求和，得到本文定义的评估节点重要度的新指标——节点重要度综合值，并依据该值大小，进行节点重要度排序，从而构建一种基于IKS和潮流熵的电网关键节点识别模型。

本文以IEEE-118节点电网为例进行验证，运用MATLAB对本文所提出的关键节点识别方法进行仿真，并通过介数中心性、接近中心性得到节点的重要程度排序结果，从而进行对比分析。为进一步证明本文所构建的电网关键节点识别模型的准确性，利用随机攻击和蓄意攻击算法对电网进行攻击模拟，根据攻击后的电网最大连通子图规模和电网效率，验证本文所提出的基于IKS和潮流熵的电网关键节点识别模型，与介数中心性、接近中心性等方法相比，更具有效性。

1 关键节点识别参数

本文基于复杂网络理论，将电网抽象成拓扑结构为$G=(V,E,W)$的无向加权网络，加权图由节点集合$V=(v_1,v_2,\cdots,v_N)$，边集合$E=(e_1,e_2,\cdots,e_N)$以及边权重集合$W=(w_1,w_2,\cdots,w_N)$组成[15]。本文运用到的关键节点识别参数如下。

1) 介数中心性。

介数中心性[16]一般指在所有最短路径中，经过该节点的路径数目占最短路径总数的比例，经过一个节点的最短路径数越多，该节点就越重要。介数中心性刻画了节点对网络中沿最短路径传输的网络流的控制力。其表达式为

$$B_i=\sum_{s\neq i\neq t}\frac{\sigma_{st}(i)}{\sigma_{st}} \tag{1}$$

式中，B_i为节点i的介数中心性，$i=1,2,\cdots,N$；σ_{st}为所有从节点s到节点t的最短路径的数目；$\sigma_{st}(i)$为这些最短路径中经过节点i的路径数目。

2) 接近中心性。

接近中心性[17]描述节点在网络中的整体影响力，计算节点到其他节点的平均最短距离，如果一个节点的接近中心性越高，意味着该节点到其他节点的平均距离最短，能够更快到达其他任意节点，在网络中传播的速度更快，其表达式为

$$C_i=\frac{1}{d_i}=\frac{1}{N-1}\sum_{j=1}^{N}d_{ij} \tag{2}$$

式中，C_i为节点i的接近中心性；d_i为节点i到其他所有节点的平均最短距离；d_{ij}为节点i到节点j的平均最短距离，$j=1,2,\cdots,N$。

3) K-shell指标。

K-shell分解法是通过逐层分解的方法，将网络中的节点分配到不同层的过程。节点的重要程度依赖于节点在整个网络中的位置，利用K-shell分解的思想获得了节点的重要度排序指标K-shell，该指标的时间复杂度低，适用于大型网络。例如，在一个由17个节点，21条边组成的无向网络中，将度数为1的节点及其连边从网络中删除，删除之后网络中会出现新的度数为1的节点，接着将这些新出现

的度数为1的节点及其连边删除，这些节点记为第1层，重复操作，直至网络中不再出现度数为1的节点，此时所有被删除的节点构成第1层，记为$K_s=1$。剩余网络中节点度数最小为2，依次迭代，直至得到没有节点度数为2的网络，此时删除的节点处于第2层，这些节点记为第2层，$K_s=2$。依此类推，直到网络中所有节点被删除，迭代结果如表1所示。

表1　K-shell分解过程

Table 1　K-shell decomposition process

迭代次数/次	删除节点	K_s
1	1,2,5,6,8,14,17	1
2	3,4,16	1
3	7,9,15	2
4	10,11,12,13	3

K_s值最高的节点是网络的核心节点，也是影响力最大的节点，内层中的节点被认为比外层的节点更具有影响力。K-shell分解示意图如图1所示。

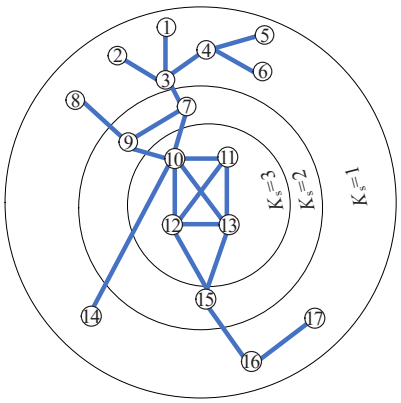

图1　K-shell分解示意图

Figure 1　K-shell decomposition diagram

由于传统的K-shell分解法中大量节点的K_s值相同，众多处于同一壳层的节点的重要度不能被识别，因此一些学者提出了IKS，其中文献[14]提出基于信息熵的IKS。本文结合电网脆弱性分析的实际需求，改变文献[14]用拓扑熵作为信息熵的做法，引入潮流熵，提出了新的电网关键节点识别方法。

4）信息熵。

信息熵[18]是量化一个随机变量结果的不确定性的指标，是对于系统混乱程度和无序程度的度量，熵越大，系统越混乱。信息熵H代表要确定一个事件的发生所需要的信息量的大小，其表达式为

$$H=-\sum_{i=0}^{N}P(x_i)\ln P(x_i) \tag{3}$$

式中，$P(x_i)$为事件在样本中发生的概率。

假设节点i的度数为k_i，则节点i的重要程度为I_i，其表达式如下：

$$I_i=\frac{k_i}{\sum_{i=1}^{N}k_i} \tag{4}$$

因此，IKS中节点的信息熵被定义为

$$H_i=-\sum_{i=0}^{N}I_i\ln I_i \tag{5}$$

由于每个节点具有不同的节点重要度，所以节点信息熵分布不均匀。越重要的节点将具有越大的节点信息熵。

5）潮流介数。

潮流介数是衡量节点在潮流分布中的重要程度或影响力指标[19]，综合考虑电气特性和网络拓扑结构，可揭示网络中节点之间的相互影响和关联程度[20]，其表达式为

$$B_{ij}=\sum_{m\in G}\sum_{n\in L}\min(S_m,S_n)\frac{P_{ij}(m,n)}{P_{mn}} \tag{6}$$

式中，B_{ij}为系统所有节点对线路的潮流介数之和；G为发电机节点集合；L为负荷节点集合；$\min(S_m,S_n)$为发电机G_m实际出力和L_n负荷的最小值；p_{mn}为发电机节点m向负荷节点n传输的功率，表示负荷节点n的功率组成中发电机节点m的贡献率；$P_{ij}(m,n)$为每条电网线路的功率组成中，发电机负荷节点对(m,n)的贡献率。

根据潮流追踪的方法，为了求得电网线路ij上的潮流分布[21]，在顺序、逆序的基础上，进行顺流和逆流追踪计算。其中，线路ij上的潮流流向负荷节点n的功率为

$$p_{ij,n}=\frac{|p_{ij}|}{p_i}\boldsymbol{A}_{\mathrm{d}}^{-1}p_{\mathrm{L}n} \tag{7}$$

式中，p_{ij}为线路ij上的有功功率；p_i为流入或者流出节点i的有功功率之和；$p_{\mathrm{L}n}$为负荷节点n的有功负荷；$\boldsymbol{A}_{\mathrm{d}}$为线路$ij$的顺序矩阵，其矩阵元素$A_{dij}$为

$$A_{dij}=\begin{cases}1, & i=j\\ -\dfrac{|p_{j-i}|}{p_j}, & j\in\alpha_i^{(\mathrm{d})}\\ 0, & \text{其他}\end{cases} \tag{8}$$

式中，$|p_{j-i}|$为线路从节点i流向节点j的有功功率；p_j为流入或流出节点j的有功功率之和；$\alpha_i^{(\mathrm{d})}$为直接从节点i向其余节点供电的节点集合。

线路ij上从发电机节点m流出的有功功率为

$$p_{ij,m}=\frac{|p_{ij}|}{p_i}A_{\mathrm{u}}^{-1}p_{\mathrm{G}m} \tag{9}$$

式中，$p_{\mathrm{G}m}$为发电机节点m的有功出力；$\boldsymbol{A}_{\mathrm{u}}$为线路$ij$的逆序矩阵，其矩阵元素$A_{uij}$为

$$A_{uij}=\begin{cases}1, & i=j\\ -\dfrac{|p_{j-i}|}{p_j}, & j\in\alpha_i^{(\mathrm{u})}\\ 0, & \text{其他}\end{cases} \tag{10}$$

式中，$\alpha_i^{(\mathrm{u})}$为直接从其余节点向节点i供电的节点集合。

发电机节点m到负荷节点n的实际输送有功功率为

$$p_{mn}=\frac{p_{\mathrm{L}n}}{p_n}\boldsymbol{A}_{unm}^{-1}p_{\mathrm{G}m} \tag{11}$$

式中，p_n为所有负荷节点n的有功功率；$\boldsymbol{A}_{unm}$为发电机节点m到负荷节点n的逆序分配矩阵。

线路ij上的潮流分布表达式为

$$p_{ij}(m,n)=\frac{p_{ij,m}p_{ij,n}}{p_{ij}} \tag{12}$$

因此，可以得到线路ij上的潮流介数表达式为

$$F_{ij}=\sum_{m\in G}\sum_{n\in L}\min(S_m,S_n)\frac{P_{ij,m}P_{ij,n}P_n}{P_{ij}P_{\mathrm{L}n}\mathbf{A}_{umn}^{-1}p_{\mathrm{G}m}} \tag{13}$$

节点i上的潮流介数表达式为

$$F_i=\frac{1}{2}\left(\sum_{ij\in l_i}G_{ij}-P_i\right) \tag{14}$$

式中，F_i为节点的潮流介数；l_i为网络中与节点i相连的支路合集；P_i为节点i的注入功率。

2 抗毁性评估参数

评估网络的抗毁性[22]就是评估网络节点受到攻击后的连通性。网络的连通性越高，网络受到攻击之后的崩溃程度越小，因此网络的连通性是衡量网络的崩溃程度的指标之一。故障点数量、连通子图数量、最大连通子图规模以及网络效率都是衡量网络连通性的重要指标，本文选用最大连通子图规模以及网络效率作为抗毁性评估指标。

1）最大连通子图。

网络在受到攻击时，部分节点失效，网络被分为互不联系的子图，其中孤边连接数及节点数量最多的子图被称为最大连通子图[23]，其表达式为

$$L_{\mathrm{c}}=\frac{N_0}{N} \tag{15}$$

式中，N_0为最大连通子图节点数；N为原网络的节点数；L_{c}为最大连通子图规模，L_{c}越大，该网络在受到攻击时破坏程度越低。

2）网络整体效率。

网络效率是指所有节点对之间的效率平均值，是衡量网络通行能力的重要指标[24]。节点i与节点j之间的网络效率表达式为

$$\varepsilon_{ij}=\frac{1}{d_{ij}},\forall i,j,i\neq j \tag{16}$$

式中，d_{ij}为节点i与节点j之间的最短距离。网络的整体效率为网络所有节点对之间效率的平均值，表达式为

$$E=\frac{\sum_{i\neq j\in G}\varepsilon_{ij}}{N(N-1)} \tag{17}$$

3 基于IKS和潮流熵的电网关键节点识别模型

虽然IKS优化了传统分解法无法区分同一壳层节点的重要度的不足，但无论是传统的K-shell分解法，还是IKS以及介数中心性、接近中心性等方法均未考虑电网的电气特性对电网节点重要度排序的影响，仅依据潮流熵进行电网节点重要度排序，且未考虑对网络结构的影响。对此，本文对已有文献的研究成果进行了改进，构建一种基于IKS和潮流熵的电网关键节点识别模型，改进策略和模型算法如下。

3.1 改进策略

对不同的网络，信息熵具有不同的内涵。拓扑熵和潮流熵均是电网的信息熵，但是潮流熵为电力系统中特有的信息熵[18]，拓扑熵仅关注电力系统在网架结构层面的均匀性与合理性，无法反映电网特征及其运行状态。故本文选用潮流熵代替文献[14]所提出的IKS中的信息熵，即式(5)中的信息熵H不再是源自拓扑结构的拓扑熵，而是由式(14)所得到的B_i代替H，可以得到本文构建模型中的电网节点i的信息熵(潮流熵)，其表达式为

$$H_i=-\sum_{i=0}^{N}F_i\log F_i \tag{18}$$

若依据文献[14]所提出的IKS，运用K_{s}值和潮流熵交替排序，无法客观刻画K_{s}值与潮流熵分别对节点重要度排序的影响程度，故本文对此进行改进。首先将潮流熵与K_{s}值进行标准化处理，然后运用熵权法求其权重[25]，并进行加权求和，得到本文定义的评估节点重要度的新指标，节点重要度综合

值I_i，其表达式为

$$I_i = \alpha_1 H_i + \alpha_2 K_s \tag{19}$$

式中，α_1、α_2分别为潮流熵与K_s值的权重。

最后，依据各节点的重要度综合值大小，进行节点重要度排序。重要度综合值越大，节点的重要度越高。

3.2　基于IKS和潮流熵的电网关键节点识别模型和算法流程

本文将文献[14]的IKS中信息熵与表征电网电气特性的潮流熵结合，构造一种基于改进IKS和潮流熵的电网关键节点识别模型，识别模型算法流程如图2所示。

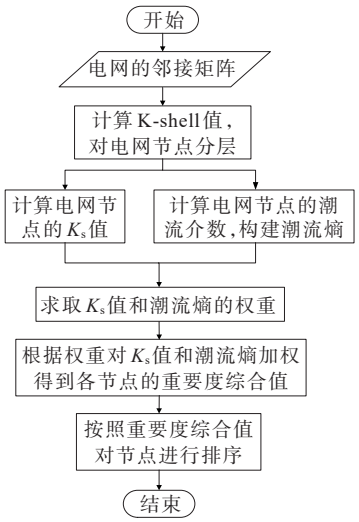

图2　电网关键节点识别模型算法流程

Figure 2　Flowchart of algorithm for key node identification model of power grid

1）计算每个节点的邻居节点数目，即节点的度。首先，将网络最外层度为1的节点删除，这时剩余图中产生新的度为1的节点，再将剩余图中新出现的度为1的节点删除，直至网络中不存在度为1的节点，将这些节点记为第1层，$K_s=1$。其次，按照上述方法删除度为2的节点，直至网络不存在度为2的节点，将这些节点记为第2层，$K_s=2$。依此类推，直到所有节点都被删除。将电网中的所有节点分为K个壳层，记为$K_s=k$。

2）计算电网中的每个节点的潮流介数，然后根据式(18)计算所有节点的潮流熵。

3）将节点的潮流熵和K_s值标准化处理后，熵权法求取权重。

4）根据式(19)对潮流熵和K_s值作加权求和，得到每个节点重要度综合值。

5）根据节点的重要度综合值大小进行排序和整理。

4　算例分析

采用MATLAB中Matpower库对IEEE-118节点系统进行仿真分析。首先，通过接近中心性、介数中心性与本文所提出的方法对系统节点进行重要度排序，将3种方法得到的节点重要度进行对比分析。其次，对IEEE-118节点系统进行不同攻击强度随机地去节点攻击，并按照上述3种方法的排序结果对IEEE-118节点系统进行不同攻击强度的蓄意去节点攻击。分析系统受到攻击后的最大连通子图规模与网络效率，验证本文所提出的电网关键节点识别模型的优越性。

4.1　IEEE-118节点电网拓扑结构

本文以IEEE-118节点网络[26]为例进行仿真实验，该系统由118个节点、186条线路组成，其中有54个发电机节点，64个负荷节点。

4.2　电网关键节点识别

本文对IEEE-118节点系统进行接近中心性、介数中心性计算，根据计算结果对节点进行排序，得到节点的重要度排序结果，以及按照本文所提出的方法对系统节点进行计算，得到节点重要度排序结果，并对3种排序结果进行对比分析。IEEE-118节点系统根据式(1)计算的介数中心性结果如图3所示，根据式(2)计算的接近中心性结果如图4所示。按照本文提出方法对IEEE-118节点进行重要度排序，步骤如下。

1）运用传统的K-shell分解对IEEE-118节点进行分层处理，将电网拓扑图最外层度为1的节点10、73、87、111、112、116与117删除，剩余的电网中出现新的度为1的节点为9和86，将剩余电网中新出现的度为1的节点9和86继续删除，至此电网中不存在度为1的节点，将这些被删除的节点存放在第1壳层，记为$K_s=1$；按照上述方法将剩余电网中度为2的节点全部删除，直至电网中不存在度为2的节点，将这些被删除的节点存放在第2壳层，记为$K_s=2$；剩余电网中只有54、55、56和59这4个节点，此时，剩余电网中最小度为3，将这些度为3的节点删除并存放在第3壳层，记为$K_s=3$，至此电网中所有节点都被删除。按照此方法将IEEE-118节点电网分为3个壳层，结果如表2所示。

2）根据式(6)～(14)计算各节点的潮流介数，

然后根据式(18)计算潮流熵,各节点的潮流熵大小如图5所示。

3)将节点的潮流熵和K_s值标准化处理后,熵权法求取权重,得$\alpha_1=0.674$,$\alpha_2=0.326$。

4)根据式(19)对潮流熵和K_s值作加权处理,得到每个节点的重要度综合值。

5)根据节点的重要度综合值大小进行排序和整理。

将本文方法排序结果与介数中心性、接近中心性、传统的K-shell分解法以及潮流熵的排序结果进行对比,对比结果如表3所示。

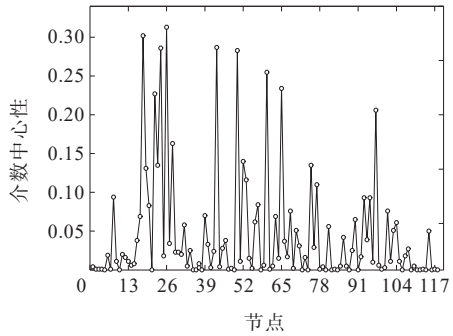

图3 IEEE-118系统节点介数中心性

Figure 3 Betweenness centrality of IEEE-118 system node

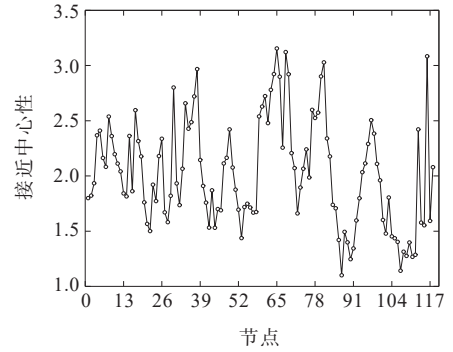

图4 IEEE-118系统节点接近中心性

Figure 4 Closeness centrality of IEEE-118 system node

表2 IEEE-118系统节点K-shell分解结果

Table 2 K-shell decomposition results of IEEE-118 system node

K_s	节点
1	10,73,87,111,112,116,117,9,86
2	1,2,4,6,7,8,13,14,16,18,20,21,22,26,28,29,33,35,36,39,41,43,44,48,50,52,53,57,58,63,67,71,72,74,76,78,79,81,84,88,90,91,93,95,97,98,99,101,102,107,108,109,110,113,114,115,118,3,5,11,12,15,19,24,25,27,30,31,34,37,40,42,45,46,51,64,68,80,83,85,89,106,17,23,32,38,47,65,70,82,92,96,105,66,75,77,94,103,104,49,62,69,100,60,61
3	54,55,56,59

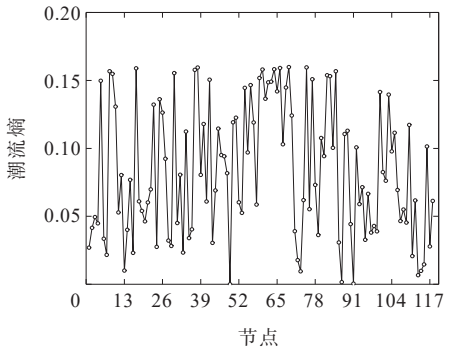

图5 IEEE-118系统节点潮流熵

Figure 5 Power flow entropy of IEEE-118 system node

表3 IEEE-118系统不同方法节点重要度排序

Table 3 Ranking of node importance for different methods in IEEE-118 system

排序	节点按介数中心性排序	节点按接近中心性排序	节点按传统K-shell排序	节点按本文所提出的方法排序/重要度综合值
1	26	65	59	59/0.966
2	18	68	56	56/0.944
3	43	116	54	54/0.936
4	24	81	55	69/0.837
5	50	38	69	75/0.836
6	60	64	75	38/0.836
7	65	69	38	66/0.834
8	22	80	66	17/0.833
9	97	66	17	64/0.830
10	28	30	64	60/0.829
11	52	63	60	37/0.828
12	75、23	61	37	85/0.825
13	19	37	85	8/0.824
14	53	34	8	30/0.819
15	77	60	30	82/0.812
16	8	77	82	83/0.809
17	93、95	17	83	77/0.799
18	57	79	77	42/0.798
19	20	59	42	5/0.795
20	68、101	8	5	63/0.792
⋮	⋮	⋮	⋮	⋮
28	33、34	5	25	55/0.735
⋮	⋮	⋮	⋮	⋮
37	76	67	45	9/0.653
⋮	⋮	⋮	⋮	⋮
118	⋮	87	87	87/0.007

由于篇幅有限,本文仅截取一部分排序结果进行分析,显然各指标的排序结果均不一样。介数中

心性排序时，存在大量度值相同的节点，因此难以区分这些度值相同的节点的重要度，只能将电网118个节点区分为56个等级。

按照传统K-shell分解法，IEEE-118节点电网中118个节点只能被分为3个壳层，按照壳层大小随机选点排列，节点54、55、56、59属于第3壳层，这4个节点重要程度最高。显然，同一壳层中的节点重要度无法识别。

运用本文所提出的方法排序，发现118个节点的重要度综合值均不相同，能够准确区分各节点的重要度。按照各节点重要度综合值对118个节点排列，例如，节点59属于第3壳层，且潮流熵为0.152，由于其重要度综合值最高，为0.966，故认为节点59最重要。而同属第3壳层的节点55，由于其重要度综合值为0.735，该节点被排列至28名。节点9属于第1壳层，流熵为0.155，但重要度综合值为0.653，因此节点9被排列至37名。显然，本文所提出的方法弥补了传统K-shell分解法无法精准实现电网节点重要度排序的不足。

接近中心性排序以及本文所提出的方法均能准确区分每个节点的重要度，但接近中心性排序与传统K-shell分解法、介数中心性排序一样均无法刻画电气特性对电网节点重要度的影响。

基于上述分析，本文所提方法考虑拓扑结构和电气特性，且各节点的重要度均可以区分，排序更精准。

为了充分体现本文研究方法的合理性与准确性，依据各排序结果对IEEE-118节点系统进行抗毁性分析。

4.3　电网抗毁性评估

为了进一步研究本文所提方法的可行性以及准确性，采用随机攻击与蓄意攻击2种攻击模式，将攻击强度定义为$P(0\leqslant P\leqslant 1)$，以此表示电网中被攻击节点占网络总节点的比例[27]，通过分析不同攻击强度下最大连通子图规模以及网络效率2个指标的变化评估电网抗毁性[28]，由数据结果分析可验证本文所提方法的优越性。

4.3.1　随机攻击模拟

在电网受到攻击之后，电网的节点会失去作用而无法正常工作。随着攻击强度的变化，最大连通子图规模以及网络效率2个抗毁性指标可以反映电网受到攻击的程度。具体攻击策略如下：随机攻击即随机按照一定攻击强度删除IEEE-118节点电网中任意节点，重复此过程，直至电网崩溃瘫痪。在这个过程中由于随机攻击的不确定性，对电网进行多次模拟攻击，根据式(15)～(17)计算最大连通子图规模以及网络效率并取平均值。

不同攻击强度下最大连通子图规模以及网络效率变化关系分别如图6、7所示。

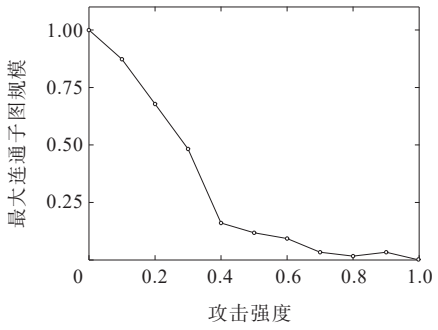

图6　随机攻击下电网最大连通子图规模变化图

Figure 6　Variation of maximum connectivity subgraph scale of power grid under random attack

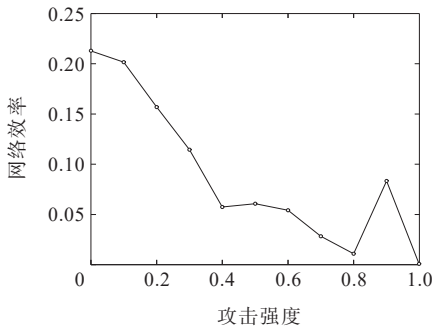

图7　随机攻击下电网网络效率变化图

Figure 7　Variation of network efficiency of power grid under random attack

IEEE-118节点系统正常运行时，电网的最大连通子图规模为1，最大效率为0.212 7。由图6分析可知，电网在受到攻击时最大连通子图规模和网络效率会急速下降。当电网遭受的攻击强度为0.4以内时，最大连通子图规模下降迅速；当攻击强度为0.4时，最大连通子图规模仅为0.2；当攻击强度为0.4～0.8时，最大连通子图规模下降缓慢；当攻击强度为0.8～0.9时，最大连通子图规模缓慢上升；当攻击强度大于0.9时，最大连通子图规模有所下降，但是下降幅度较小；当被攻击节点占比为100%时，最大连通子图规模为0，网络瘫痪。

由图7可知，当攻击强度小于0.4时，随着攻击强度的增加，电网的效率急速下降。当攻击强度为0.4～0.6时，网络效率呈现先升后降趋势，但变化趋于平稳，变化量并不显著；当攻击强度达0.6～0.8时，网络效率呈现下降趋势，变化量较攻击强度小

于0.4时偏小；当攻击强度达0.6～0.8时，变化较为显著；当攻击强度达0.8～0.9时，电网的网络效率有短暂陡然回升；当攻击强度大于0.9时，电网的网络效率急速下降，直至为0。

4.3.2 蓄意攻击模拟

蓄意攻击是指通过攻击电网的脆弱环节来最大程度地破坏电网的结构和运行。根据表3中得到的介数中心性、接近中心性以及本文所提出方法得到的IEEE-118节点电网节点重要度排序结果，按降序排列重要度的方式进行节点攻击，据此提出以下攻击策略。

1）介数中心性降序攻击，即将节点以介数中心性降序排列，然后按照不同攻击强度删除排序节点，重复此过程，直至电网崩溃。

2）接近中心性降序攻击，即将节点以接近中心性降序排列，然后按照不同攻击强度删除排序节点，重复此过程，直至电网崩溃。

3）本文方法降序攻击，即将节点以本文方法降序排列，然后按照不同攻击强度删除排序节点，重复此过程，直至电网崩溃。

根据式(15)～(17)得到不同攻击强度下电网的最大连通子图规模和网络效率的变化。通过最大连通子图规模以及网络效率的变化量来分析3种方法的准确性。最大连通子图规模及网络效率仿真结果如图8、9所示。

IEEE-118系统在正常运行时，电网的最大连通子图大小为1，最大网络效率为0.212 7。根据图8结果分析，当电网受到攻击时，随着攻击强度逐渐增加，电网的最大连通子图规模呈现急剧下降的趋势。当根据本文所提方法的排序结果对电网进行蓄意攻击，攻击强度为0.1时，最大连通子图规模大小降为0.517，约为原始规模大小的50%。按照本文所提出方法，蓄意攻击的网络最大连通子图规模下降速度最快，约为随机攻击时电网下降速率的3.8倍。而按照接近中心性排序结果，蓄意攻击的网络最大连通子图规模下降速率约为随机攻击时的0.8倍。按照本文所提方法蓄意攻击的网络最大连通子图规模下降速度约为按照接近中心性方法蓄意攻击的4.7倍。当攻击强度达到0.5时，最大连通子图大小不足0.1，并逐渐接近于0，电网逐渐崩溃。此外，按照本文所提方法排序结果进行蓄意攻击的网络的最大连通子图大小始终随着攻击强度的增大而减小。由此可得出，本文所提出的方法比接近中心性排序、介数中心性排序在重要节点识别方面更有效。

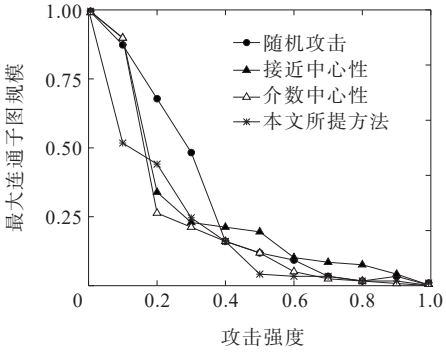

图8 蓄意攻击下电网最大连通子图规模变化

Figure 8 Variation of maximum connectivity subgraph scale of power grid under deliberate attack

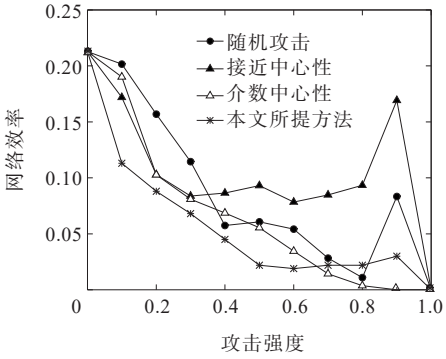

图9 蓄意攻击下电网网络效率变化

Figure 9 Variation of network efficiency of power grid under deliberate attack

由图9分析可知，在电网中攻击强度为0.1时，按照本文所提方法得到的排序结果进行攻击会导致网络效率下降最快，其下降速率约为随机攻击时的9倍。而按照接近中心性排序进行攻击的网络下降速率只有随机攻击时的3.7倍。因此，按照本文所提方法得到的排序结果进行攻击的网络效率下降速率约为按照接近中心性排序进行攻击的2.4倍。此外，随着攻击强度的增加，电网的网络效率逐渐降低。显然，按照本文所提出方法的排序结果进行攻击的电网网络效率下降最为显著，并且按照该排序结果攻击的电网网络效率普遍低于随机攻击的电网。由此可得出，本文所提出的方法比接近中心性排序、介数中心性排序等方法更具优势。

5 结语

本文提出了一种基于IKS与潮流熵的电网关键节点识别模型，该方法同时考虑了电网的潮流熵以及电网度中心性的信息熵，消除了在电网中运用传统K-shell算法只基于拓扑结构进行节点识别带来的弊端，更准确地描述了节点的影响力。为了验证

该方法的优越性和准确性，对IEEE-118节点系统进行节点识别，然后对比在随机攻击以及按照3种方法的排序结果对电网进行蓄意攻击的情况下，抗毁性指标（最大连通子图规模以及网络效率）的变化。实验结果表明：1）本文所提出的方法可以准确度量每个节点的重要程度，消除了传统K-shell算法中，大量节点度值相同，不能区分重要度的弊端。2）介数中心性排序同样存在节点难以区分的现象，对于IEEE-118系统节点，根据介数中心性排序只能将节点识别为56个等级，而本文所提出的方法能够准确识别118个节点。3）当受到攻击的节点占比为10%以内时，按照本文所提出的方法进行蓄意攻击，电网最大连通子图规模的下降速率约为接近中心性的4.7倍，电网效率的下降速率约为接近中心性的2倍。由此说明，本文所提出的方法在识别节点重要度方面更准确。

本研究可以用于识别电网的薄弱环节，以便制定有针对性的保护措施，确保电力系统稳定运行。同时能够揭示电力系统故障的原因和发展规律，从而预防未来事故的发生，可为电网规划提供有力的依据。

本文在抗毁性评估时，主要采用随机攻击以及蓄意攻击2种模拟方法对节点进行评估，但是仅考虑了电网在静态时，不同方法排序下在电网节点受到不同攻击强度的最大连通子图规模以及网络效率的变化情况，未考虑电网作为动态网络，在遭受攻击后，电网会发生级联失效，产生一系列连锁反应的情况。后续的研究将会充分考虑电网在动态攻击下网络抗毁性的评估，拟考虑运用本文提出的方法，对多种新能源并网下电网脆弱性问题和抗毁性问题展开实证研究。

参考文献：

[1] 李泽鹏,左杨,王宏宇.基于社交网络结构的节点影响力度量方法[J].电子学报,2016,44(12):2967-2974.
LI Zepeng, ZUO Yang, WANG Hongyu. An influence measure of nodes based on structures of social networks [J].Acta Electronica Sinica,2016,44(12):2967-2974.

[2] 张哲亮,夏沛,张晓星,等.源–网–荷–储–体化环境下复杂电网投资决策指标体系的研究[J].电力科学与技术学报,2023,38(3):1-13.
ZHANG Zheliang, XIA Pei, ZHANG Xiaoxing, et al. Research on the complex grid investment decision indexes system under the integrated source-grid-load-storage environment[J]. Journal of Electric Power Science and Technology,2023,38(3):1-13.

[3] 张英敏,张文馨,李保宏,等.柔直电网拓扑对故障电流的影响机理分析[J].电力工程技术,2022,41(5):94-102.
ZHANG Yingmin, ZHANG Wenxin, LI Baohong, et al. Influence mechanism of MMC-HVDC grid topology on fault current[J]. Electric Power Engineering Technology, 2022,41(5):94-102.

[4] 郭明健,高岩.基于复杂网络理论的电力网络抗毁性分析[J].复杂系统与复杂性科学,2022,19(4):1-6.
GUO Mingjian, GAO Yan. Invulnerability analysis of power network based on complex network[J]. Complex Systems and Complexity Science,2022,19(4):1-6.

[5] 何铭,邹艳丽,梁明月,等.基于多属性决策的电力网络关键节点识别[J].复杂系统与复杂性科学,2020,17(3):27-37.
HE Ming, ZOU Yanli, LIANG Mingyue, et al. Critical node identification of a power grid based on multi-attribute decision[J]. Complex Systems and Complexity Science,2020,17(3):27-37.

[6] 任鹏,李翀,陶鹏,等.基于加权熵TOPSIS法的电网节点脆弱度评估[J].电力科学与技术学报,2019,34(3):143-149.
REN Peng,LI Chong,TAO Peng,et al.Node vulnerability evaluation for power network based on weighted entropy TOPSIS method[J]. Journal of Electric Power Science and Technology,2019,34(3):143-149.

[7] 魏刚.基于介权熵度的电网关键节点评估方法[J].计算机应用研究,2020,37(增刊1):27-30+33.
WEI Gang. Evaluation for critical buses of power grids by betweenness-weighted entropic degree[J]. Application Research of Computers,2020,37(Sup 1):27-30+33.

[8] 卢鹏丽,郭旭东,董瑞,等.基于介度熵的复杂网络节点重要度识别方法[J].兰州理工大学学报,2020,46(2):111-115.
LU Pengli, GUO Xudong, DONG Men, et al. Importance identification method of complex network nodes based on betweenness and degree entropy[J]. Journal of Lanzhou University of Technology,2020,46(2):111-115.

[9] KITSAK M, GALLOS L K, HAVLIN S, et al. Identification of influential spreaders in complex networks[J].Nature Physics,2010,6:888-893.

[10] ZENG A, ZHANG C J. Ranking spreaders by decomposing complex networks[J]. Physics Letters A, 2013,377(14):1031-1035.

[11] BAE J, KIM S. Identifying and ranking influential spreaders in complex networks by neighborhood coreness[J]. Physica A: Statistical Mechanics and Its Applications,2014,395:549-559.

[12] WANG Z X, ZHAO Y, XI J K, et al. Fast ranking influential nodes in complex networks using a k-shell iteration factor[J]. Physica A: Statistical Mechanics and Its Applications,2016,461:171-181.

[13] 朱晓霞,胡小雪.基于改进 K-shell 算法的节点影响力

的识别[J].计算机工程与应用,2019,55(1):35-41.
ZHU Xiaoxia, HU Xiaoxue. Identification of node influence based on improved K-shell algorithm[J]. Computer Engineering and Applications,2019,55(1):35-41.

[14] WANG M,LI W C,GUO Y N,et al.Identifying influential spreaders in complex networks based on improved k-shell method[J]. Physica A: Statistical Mechanics and Its Applications,2020,554:124229.

[15] 龚立,王先培,田猛,等.电力信息物理系统韧性的概念与提升策略研究进展[J].电力系统保护与控制,2023,51(14):169-187.
GONG Li, WANG Xianpei, TIAN Meng, et al. Concepts and research progress on enhancement strategies for cyber physical power system resilience[J]. Power System Protection and Control,2023,51(14):169-187.

[16] 谭阳红,张婧,李肖.基于复杂网络理论的电网节点重要度评估[J].计算机工程,2019,45(11):281-286+297.
TAN Yanghong, ZHANG Jing, LI Xiao. Importance evaluation of power grid nodes based on complex network theory[J]. Computer Engineering, 2019, 45(11): 281-286+297.

[17] 吴昊,朱自伟.基于熵权-层次分析法综合指标的电网关键线路辨识[J].中国电力,2020,53(5):39-47+55.
WU Hao, ZHU Ziwei. Key lines identification in power grid based on comprehensive index calculated by the entropy weight-analytical hierarchy process[J]. Electric Power,2020,53(5):39-47+55.

[18] 张广伦,钟海旺.信息熵在电力系统中的应用综述及展望[J].中国电机工程学报,2023,43(16):6155-6181.
ZHANG Guanglun, ZHONG Haiwang. Review and prospect of information entropy and its applications in power systems[J]. Proceedings of the CSEE,2023,43(16): 6155-6181.

[19] 孙珂,曹阳,陈天一,等.大电网脆弱性评估的潮流介数分析方法[J].电力电容器与无功补偿,2021,42(1):101-107.
SUN Ke, CAO Yang, CHEN Tianyi, et al. Power flow number analysis method for vulnerability assessment of power systems[J]. Power Capacitor & Reactive Power Compensation,2021,42(1):101-107.

[20] 胡福年,陈灵娟,陈军.基于交流潮流的连锁故障建模与鲁棒性评估[J].电力系统保护与控制,2021,49(18):35-43.
HU Funian, CHEN Lingjuan, CHEN Jun. Cascading failure modeling and robustness evaluation based on AC power flow[J]. Power System Protection and Control, 2021,49(18):35-43.

[21] 冉晴月,林伟,杨知方,等.基于可信深度神经网络的最优潮流计算方法[J/OL].电工技术学报,1-14[2024-03-06].
RAN Qingyue, LIN Wei, YANG Zhifang, et, al. Optimal power flow calculation based on a trustworthy deep neural network[J/OL]. Transactions of China Electrotechnical Society,1-14[2024-03-06].

[22] 程紫运,吕明卉,田云飞,等.基于结构熵的电力骨干通信网抗毁性研究[J].电力系统保护与控制,2020,48(5):112-118.
CHENG Ziyun, LYU Minghui, TIAN Yunfei, et al. Research on invulnerability for electric power backbone communication network based on structural entropy[J]. Power System Protection and Control,2020,48(5):112-118.

[23] 狄鑫.基于电力光网络的关键节点辨识方法研究[D].北京:北京邮电大学,2023.
DI Xin. Research on key node identification method based on power optical network[D]. Beijing: Beijing University of Posts and Telecommunications,2023.

[24] 龙覃飞,王涛,顾雪平,等.基于社团重叠的电力通信相依网络建模及其抗毁性分析[J].电力自动化设备,2019,39(11):165-173+204.
LONG Qinfei, WANG Tao, GU Xueping, et al. Modeling and invulnerability analysis of power communication interdependent network based on community overlapping [J]. Electric Power Automation Equipment, 2019, 39(11): 165-173+204.

[25] 胡润泽,吕世轩,张灿,等.基于状态熵权和双轨制TOPSIS的电能质量实时综合评估方法[J].电力系统保护与控制,2023,51(23):102-114.
HU Runze, LYU Shixuan, ZHANG Can, et al. Real time comprehensive evaluation method of power quality based on state entropy and dual track TOPSIS[J]. Power System Protection and Control,2023,51(23):102-114.

[26] 高洁,马杰,杨丽新.基于非线性容量负载模型下电网的级联故障分析[J].科学技术与工程,2022,22(9):3601-3606.
GAO Jie,MA Jie,YANG Lixin.Cascading failure analysis of power grid based on nonlinear capacity load model[J]. Science Technology and Engineering, 2022, 22(9): 3601-3606.

[27] 周冬玥,胡福年,陈军.基于复杂网络的电力系统鲁棒性分析[J].电力系统保护与控制,2021,49(1):72-80.
ZHOU Dongyue, HU Funian, CHEN Jun. Robustness analysis of power system based on a complex network[J]. Power System Protection and Control,2021,49(1):72-80.

[28] 肖祥慧,张振山,谭海曙.基于相依网络理论的配电信息物理系统脆弱性[J].电力科学与技术学报,2022,37(4):125-133.
XIAO Xianghui, ZHANG Zhenshan, TAN Haishu. Research on vulnerability analysis of cyber-physical distribution system based on interdependent network theory[J]. Journal of Electric Power Science and Technology,2022,37(4):125-133.