弹性异质电网的重要目标识别算法

王 磊[1]，陈端兵[1,2*]，周俊临[1,2]，傅 彦[1,2]

(1. 成都数之联科技股份有限公司 成都 610041；2. 电子科技大学大数据研究中心 成都 611731)

【摘要】在现代信息化战争中，识别电网中的重要目标能有效指导攻击方或防御方战术的制定。而现有的电网攻防策略研究通常忽略真实电网具有弹性这一特性，因此提出 RHGEle_Rank 方法用于在电网的多轮攻防博弈中识别重要的变电站和输电线。首先基于仿真的弹性电力网络模型，考虑电站节点的工作效率，设计了节点的自我恢复策略用于模拟多轮攻防博弈下变电站的自我修复场景。然后，针对电网的异质特征，构建了基于过载式和断电式的级联失效模型。最后，利用贪心算法，识别每轮攻防博弈中的最佳攻击 (防御) 目标。实验表明，相较于传统的度中心性、介数中心性方法，攻击 RHGEle_Rank 选择出的重要目标能更大程度上破坏电网的供电能力。同时，考虑网络弹性的贪心算法能有效避免多轮攻防博弈中出现“无效攻击”。

关 键 词 级联失效； 复杂网络； 贪心算法； 弹性异质电网

中图分类号 TP301 **文献标志码** A doi:10.12178/1001-0548.2022077

An Important Element Identification Based on Resilient Heterogeneous Grid

WANG Lei[1], CHEN Duanbing[1,2*], ZHOU Junlin[1,2], and FU Yan[1,2]

(1. Chengdu Union Big Data Tech. Inc. Chengdu 610041;

2. Big Data Research Center, University of Electronic Science and Technology of China Chengdu 611731)

Abstract In modern information warfare, identifying important targets in the grid can effectively guide the tactics of the attacker or defender. The existing research on grid attack and defense strategy usually ignores the resilient of the real grids, therefore, RHGEle_Rank (important Element identification based on Resilient Heterogeneous Grid) method is proposed to identify important substations and transmission lines in a multi-round attack and defense game of the grid. Based on simulated resilient power network model, a self-recovery strategy for nodes is designed to simulate the self-healing scenario of the substation under multiple rounds of attack and defense game by considering the efficiency of the nodes. Then, according to the heterogeneous characteristics of power network, cascade failure models based on overload and outage modes are constructed. Finally, a greedy algorithm is used to identify the best attack (defense) target in each round of the offense-defense game. Experiments show that power supply capacity of grid can be destroyed to a greater extent by RHGEle_Rank method than that by the traditional degree centrality and betweenness centrality methods. At the same time, "invalid attack" in multi-round attack and defense games can be effectively avoided if network resilience is considered in the important element identification algorithm.

Key words cascading failure; complex networks; greedy algorithms; resilient heterogeneous grids

在现代信息化战争中，电力网络是重要的攻击目标之一，节点打击、毁点瘫面能帮助攻击方快速取得战事的优势。作为攻击方，如果能预先识别出电力网络中的重要节点，将有效指导该方对电网实施有效打击，对敌方电力系统造成大规模影响甚至瘫痪。而作为电网系统管理人员，若能提前检测当前电网的重要节点，对重要目标加强防护和定时保养维修，将极大提升电力系统的鲁棒性和抗毁能力。在复杂网络研究中，节点的重要性通常用节点中心性[1]度量。通过对节点中心性进行计算和排

收稿日期：2022－03－14；修回日期：2022－08－14

基金项目：国家自然科学基金 (61673085)

作者简介：王磊 (1993－)，男，博士生，主要从事复杂网络分析及网络表征等方面的研究.

*通信作者：陈端兵，E-mail：dbchen@uestc.edu.cn

序，能有效发现网络中的重要节点。

目前已有不少成熟的节点中心性计算方法，主要分为 4 类[2]：1) 基于节点近邻的指标和方法；2) 基于路径的指标和方法；3) 基于特征向量的指标和方法；4) 基于节点移除和收缩的指标和方法。基于节点近邻的指标和方法[3−6] 主要根据节点的邻居结构特征定义其重要性。考虑节点对网络中信息传播的影响力，基于路径的方法[7−9] 衡量了节点在信息传播过程中作为“桥梁”的重要性。基于特征向量的方法[10-11] 利用网络的全局信息衡量节点的重要性。在不考虑时间开销的前提下，从初始节点出发，采用随机游走策略向外传播信息，当传播趋于稳定时，信息保留越多的节点越重要。除了上述方法，还有利用系统科学中的“核与核度”理论[12]，基于节点移除和收缩的方法[13-15] 通过量化节点被移除后对网络的破坏情况衡量节点的重要性。网络中的重要节点一旦失效或被移除，网络就会陷入瘫痪或者分化为多个不连通的子网。

利用这些指标，学者们分析了蓄意攻击下的北美电网、欧洲电网及一些欧盟国家电网的脆弱性。但是，仅利用传统复杂网络的重要节点识别方法，不考虑实际电网中的电流电压信息，无法解决电网中因线路、元件过载而引起的级联失效问题。为了考虑级联失效对重要节点识别带来的影响，研究者基于虚拟负荷的拓扑结构模型，根据电网拓扑结构定义节点或边负荷大小，分析了电网拓扑结构对系统级联失效过程的影响[16-18]。近年来，针对不同电网模型，研究人员通过改进复杂网络分析方法以识别不同情形下的电网关键元件[16,19-20]。

然而在电力系统中，除了元件负载，电站和电力线往往还富有弹性。网络的弹性 (cyber resilience) 是指系统在遭受故障时维持一定的功能，并在指定的时间与成本内恢复到正常运行状态的能力[21]。电网系统中，灾难事件往往指使用年限过长导致设备输电故障、变电站输电线被恶意攻击破坏或技术人员的错误操作导致的故障等。电网故障响应过程通常分为 3 个阶段[22]：故障吸收阶段、故障渗透阶段和故障恢复阶段。故障吸收阶段是指系统发生故障并吸收故障的发生的阶段；故障渗透阶段指电网故障由于级联效应导致系统性能下降的阶段；故障恢复阶段指运营者组织电网修复并使电网逐渐恢复到正常运行水平的阶段。在故障恢复阶段，现有方法[23] 都旨在对恢复过程进行仿真模拟，以寻找最优恢复目标，从而尽快恢复电网系统的供电功能。

针对弹性异质电力网络，如何在现代信息化战争的多轮攻防博弈中，识别重要变电站和输电线是当前的一大挑战。现有复杂网络中的重要节点挖掘方法都没有考虑网络的弹性，即被攻击的节点或连边将永久性瘫痪。因此，基于仿真的电力网络模型[16] 首先设计了一个节点自我恢复策略用于模拟多轮攻击下变电站的自我修复场景。其次，针对修复后的弹性异质电力网络，设计了一个攻击得分函数，以评估当前状态电网中每个备选项目的攻击受益。最后，利用贪心策略，在每次迭代过程中识别出当前状态下弹性电网的最佳攻击目标 (节点或边)。通过对不同攻击目标的受益得分进行排序，提出了一种新的弹性异质电网重要目标识别方法 (important element identification based on resilient heterogeneous grid, RHGEle_Rank)，用于识别当前电网中重要的边和点。实验表明，相比于其他复杂网络中重要节点识别方法，攻击 RHGEle_Rank 选出的重要目标将使电网系统的供电能力下降得更快。若以完全破坏弹性电力系统的供电能力为目标，本文提出的方法能指导作战部更高效地完成任务。同时，考虑“网络弹性”的贪心策略能避免多轮攻防博弈中出现“无效攻击”，也能更大程度地破坏电网的供电能力。

1　弹性异质电网的仿真建模

为了识别弹性电网中的关键目标，首先对弹性异质电网进行仿真和建模，主要包含弹性异质电网基础模型的搭建、弹性电网自我恢复设计和电网级联失效设计 3 部分。

1.1　弹性异质电网基础模型搭建

针对一个异质电网$G=\{V,E,\varphi\}$，边$(v_i,v_j)\in E$代表现实中的输电线，每个节点$v_i\in V$有一个类型$\varphi(v_i)$。在电网环境下，节点类型集合为$\varphi=\{$发电站P, 变电站S, 用电区域$C\}$。针对上述 3 种类型的节点，分别定义其负载如下。

1) 针对每个用电区域$v\in\varphi_C$，往往需要$L(v)$的供电功率才能正常运作。而每个供电区域，往往有不止一个变电站对其供电。用电区域也分为一级用电区域和二级用电区域。

2) 针对每个变电站$v\in\varphi_S$，为了完成对下级用电区域的供电，每个变电站当前负载功率为：

$$L(v_i)=\sum_{(v_i,v_j)\in E}\frac{1}{N_j}L(v_j) \tag{1}$$

式中，$v_j\in\varphi_C$；N_j是为用电区域v_j提供电力的变电站数目。现实生活中，为了抵御一些故障对电网造成的危害，每个变电站都不会满负荷运行。因此，本文为变电站设计一个最大容忍系数$K>1$来模拟该情况。此时，变电站v_i在满负载的情况下的最大功率为：$\overline{L}(v_i)=K\cdot L(v_i)$。同时，每个变电站并不一定与发电站相连，通过其他变电站作为中间介质，同样可以从发电站获取电能。

3) 针对每个发电站$v_i\in\varphi_P$，由于现实电网中，防守方通常会重点防护发电站，发电站被攻击或发生故障的可能性极低，因此本文不关注发电站的攻击与故障，发电站的供给功率设定为$L(v_i)=\infty$。

电网中，各个变电站由于被攻击或发生故障，变电站的工作效率η会降低。在电网仿真模型构建过程中，设定所有变电站$v_i\in\varphi_S$的初始工作效率为$\eta(v_i)=1$，变电站被攻击或发生故障后，工作效率$\eta(v_i)<1$。

1.2 弹性电网的自我恢复设计

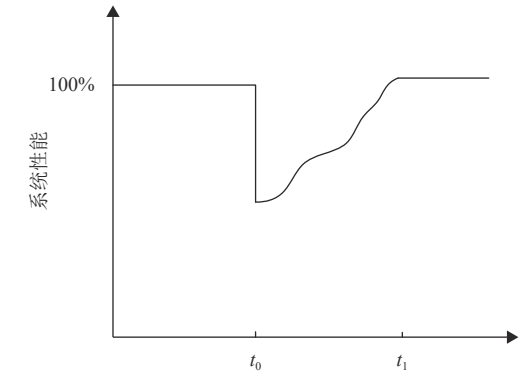
弹性在不同学科与应用中有不同的定义，系统弹性的度量也有所不同。文献 [24] 指出，随着时间的推移，系统性能可能发生变化，有时是逐渐变化，有时是突然变化。在发生大地震等灾难性事件时，系统性能会发生突然变化，从而导致部分或所有设施的性能大幅下降甚至完全丧失。突发事件后，需要利用额外资源将系统性能恢复到正常水平，图 1a[24] 为地震后系统性能恢复示意图。而电网系统变电站被攻击后的恢复过程和地震这一类突发事件类似，其恢复过程也具有非线性的特征。在恢复早期，变电站破坏严重，修复难度较大，此时电站恢复速度缓慢。随着修复的进行，变电站各功能逐渐趋于正常，此时变电站的恢复速度也变快。综合上述特点，本文设计了更加贴近真实的变电站恢复函数来模拟变电站在电网攻防中的恢复能力，如图 1b 所示，恢复量$r(v_i)$定义为：

$$r(v_i)=(\eta(v_i)+\xi)^k-(\eta(v_i))^k \tag{2}$$

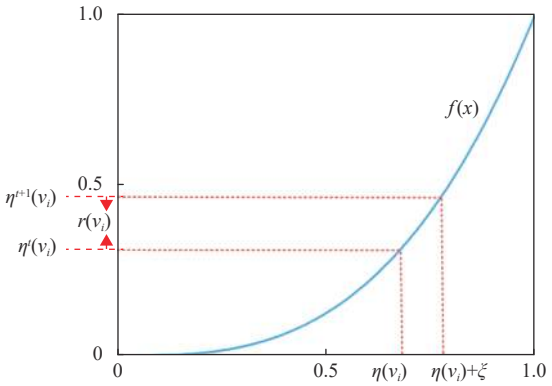
式中，k为一个大于 1 的常数；ξ为步长，本文取$\xi=0.1$；针对网络中的节点v_i，每次模拟攻击后节点v_i的恢复量$r(v_i)$与节点工作效率$\eta(v_i)$负相关，即被破坏得越严重，修复周期越长，进度越缓慢。如图 1b 所示，在t轮攻击后，节点v_i的效率为$\eta^t(v_i)$。在t时刻到下次攻击$t+1$时刻的阶段，节点恢复量$r(v_i)$按式 (2) 计算。此时，在下一次攻击到来时，节点v_i的效率修复为：

$$\eta^{t+1}(v_i)=\min(1,\eta^t(v_i)+r(v_i)) \tag{3}$$

在t到$t+1$轮攻击的间歇，网络中被攻击的节点将进行自我修复，电力网络结构以一定的概率进行重构，此时网络中因为级联失效而造成的大规模断电得到缓解。因此，针对恢复后的电力网络进行重要目标挖掘会更为合理、更贴合实际。



a. 地震后系统性能恢复示意图[24]



b. 变电站性能“恢复”函数

图 1 系统性能恢复示意图

1.3 电网级联失效设计

级联失效反映的是网络的动态特性，网络拓扑结构的改变将造成网络数据流的重新分配[25]。本文主要考察两种情况的级联失效：1) 过载式级联失效：针对变电站，受制于硬件成本，每个变电站节点都具有给定的负载能力。最初，网络处于稳定状态，每个变电站都不会满负载运行，其负载都小于容量。在变电站遭到破坏或节点发生故障时，电网系统会受到干扰。故障的发生将破坏电网中流量的平衡，用电区域的负载将重新分配给其他变电站，并可能进一步导致其它变电站过载，从而引起整个系统故障。2) 断电式级联失效：有的变电站与发电

站并无直接连接，需要途经某变电站。而当中间变电站过载而失效，其下游变电站若没有其他路径从发电站获取电能，此时，该变电站由于中间电站的故障而发生级联失效，从而引起电力系统的“链式”瘫痪。

大部分研究关注变电站过载造成的电网级联失效。而基于 1.1 节中异质电力网络模型，加入第二种级联失效的判断，使得电网在故障渗透阶段的仿真更加真实、可靠。

2　基于弹性异质电网的重要目标多轮攻击仿真

以现代战争中的多轮攻击为背景，以破坏电网供电为目标，本文设计了一个评估电网中目标被破坏后受益的得分函数，提出一种弹性异质电网的重要目标识别方法，用于识别当前电网状态中的最佳攻击目标。

2.1　RHGEle_Rank 重要目标识别方法

区别于其他重要节点和边识别方法，本文的研究对象主要针对节点具有恢复功能的弹性异质动态电网。与静态的电力网络相比，节点的主动恢复机制会导致在多轮电网攻防博弈中发生复杂的“级联失效”和“级联增益”事件。而传统的复杂网络方法在多轮的攻防博弈中，往往只针对当前网络的状态识别出当前电网中的重要节点，而忽略了节点恢复机制产生的“级联增益”。特别地，若节点在受到攻击后，在下一轮攻击时能恢复到正常供电状态，本文称这种攻击为“无效攻击”。而现有的重要节点识别方法都没有考虑节点的恢复能力，从而在真实的电网攻防过程中，会多次选择“无效攻击”的节点进行破坏而不造成任何攻击收益。而本文考虑节点自我恢复产生的“级联”效益，提出了一种基于弹性异质电网的重要目标方法 (RHGEle_Rank)，用于识别电网中能最大影响电网供电能力的重要目标 (边或者点)。与其他方法识别的重要目标不同，该重要目标一旦受到破坏，即使节点会被短暂抢修进行恢复，此次目标的破坏也能最大程度上影响电网系统的供电能力。作为电网攻击方，分析当前电网的最佳攻击目标，能指导作战部最快破坏该电力系统。而作为电网的防守方，通过分析当前电力拓扑结构中的重要变电站或输电线，能对该重要目标快速部署防御，从而提高电力系统的抗毁能力。

为了能识别出当前电网的重要目标，本文选择对备选目标集中的每个目标a进行模拟攻击以评估攻击收益。考虑变电站自我修复机制，设计一个“战后”攻击收益得分函数，从而对电网中目标 (变电站、输电线) 的重要性进行评估。从攻击者的角度看，目标a被破坏后，电网的电能供给情况毁坏越大，该目标a应该被优先攻击。从防守方角度看，目标a一旦被破坏，电网会大规模瘫痪，说明该输电线或者该变电站a尤为重要，需要重点防护。区别于常规复杂网络中，根据最大连通子图评估网络的效益，本文研究的电网攻击的目的旨在最快降低网络电能效率。因此，在模拟攻击$a \in A$目标并进行“战后”的模拟恢复后，将“战后”正常供电区域C_a的电能总和与上一轮攻击后的电能总和$\overline{L}$之差作为当前攻击的得分Score(a)，计算如下：

$$\text{Score}(a) = \overline{L} - \sum_{v \in C_a} L(v) \tag{4}$$

按照式 (4) 计算备选攻击项A中每个目标a的攻击得分，选取最大攻击得分作为最佳攻击目标$a_{\max}$。该攻击目标往往也是电网中最重要的元素，需要被优先攻击 (保护)。

2.2　基于弹性异质电网的重要目标识别流程

以 1.1 节中建立的异质弹性电网为例，从攻击者的角度，对弹性异质电网进行多轮重要目标的识别和攻击。具体步骤如下：1) 为了分析当前电网的最佳重要目标，首先对当前电网构建一个备选集合A，从备选攻击集A中按顺序选出备选攻击目标a。2) 对a按顺序进行模拟攻击和网络修复。若攻击目标a是节点，则降低其工作效率。3) 受到破坏后，首先需要对电网中所有变电站进行级联失效判断。无论目标a是节点还是边，在受到攻击后，电网的拓扑结构都会发生改变，电网中的变电站由于电网结构的变化而以一定概率发生“断电式”和“过载式”级联失效。4) 基于本文设计的节点自我修复机制，对网络中所有遭到破坏的目标进行自我修复。特别地，若攻击目标a是输电线，由于输电线的防御能力较低，输电线一旦被作为攻击目标会立刻被破坏。因此，在仿真过程中，若攻击目标a是边，直接去除边a，本文不考虑输电线的修复情况。5) 由于在修复过程中电网将以一定的概率产生级联增益，使得之前超负载的变电站恢复正常工作，从而大规模恢复区域的供电。因此需要对修复后的电网进行第二次级联判断。6) 待电网中级联增益达到稳定后，按照式 (4) 计算目标a的模拟攻击得分

Score(a)。此时，目标a的一次模拟攻击完成。7) 对备选攻击集合A中所有目标进行模拟攻击后，选取攻击得分最高的目标作为本轮最佳攻击目标$a_{\max}$。当按照模拟攻击的方法真正攻击$a_{\max}$并自动恢复后，完成弹性异质电网一轮的重要目标攻击。

由于真实战场上，针对电网的攻击往往不是一轮，双方要进行多轮博弈。因此，本文对电网进行 K 轮攻击仿真。若在 K 轮仿真过程中电网的供电能力降为 0，此次电网的攻击行动完成，终止后续的电网攻击仿真，具体流程如图 2 所示。

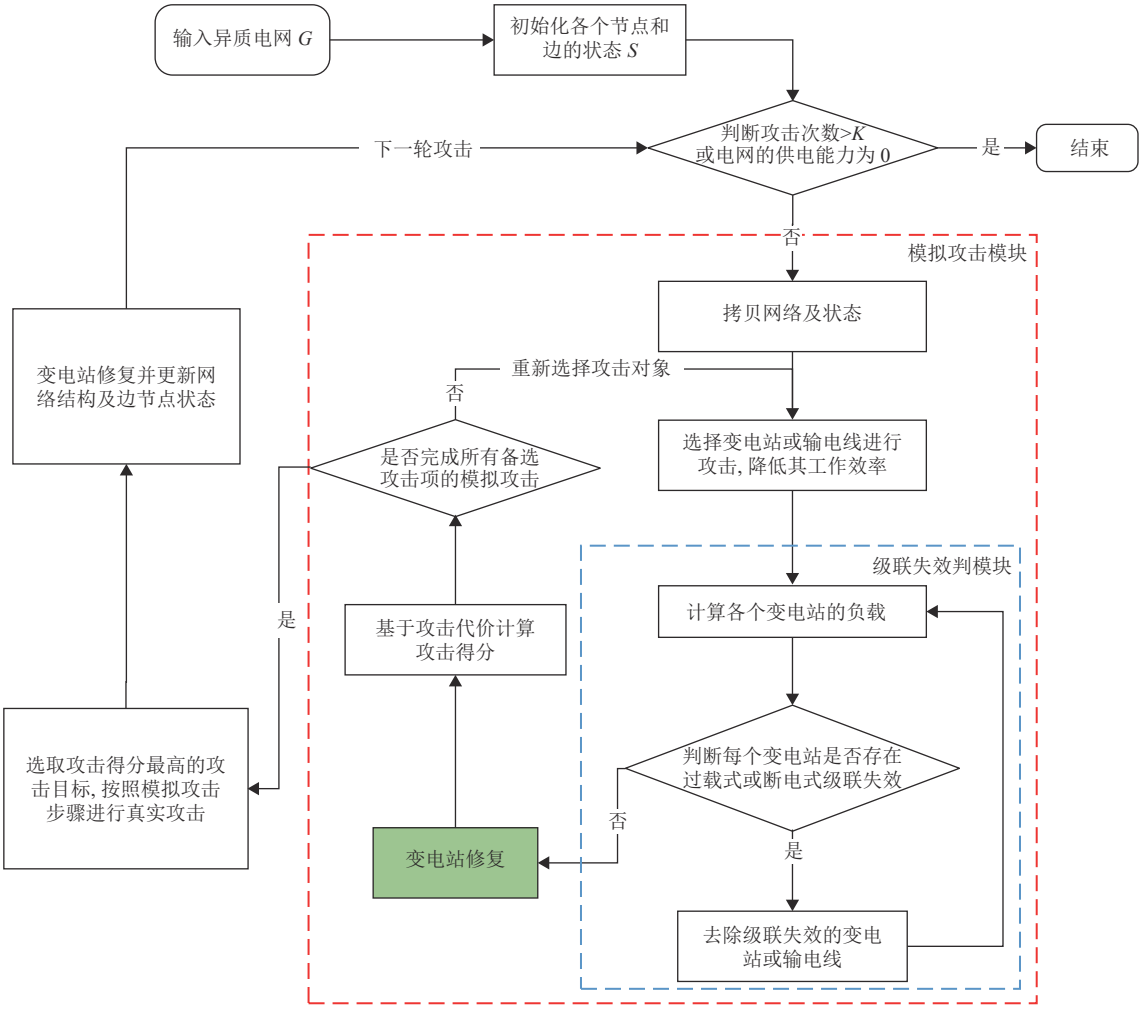


图 2 异质弹性电网仿真系统流程图

2.3 HGEle_Rank 消融方法

为了验证本文提出的考虑网络弹性的重要节点识别方法的优势，在去掉 2.2 节流程图 2 中“模拟攻击模块–变电站修复”步骤 (图 2 中变电站修复模块) 后，将其命名为 HGEle_Rank 方法。由于节点恢复机制，节点受到攻击后，在下一轮攻击时可能已经恢复到正常工作状态。重复选择这一类节点作为攻击目标不会产生任何级联事故和攻击收益。不考虑“变电站恢复”机制的 HGEle_Rank 方法在计算得分函数时，仅考虑当前电网中变电站和输电线的状态，可能会陷入“无效攻击”的困境。因此，本文对去除 RHGEle_Rank 方法中的变电站修复模块而得到的 HGEle_Rank 方法用于对比消融实验。

2.4 实验仿真及分析

如图 3 所示的电力网中，电力从发电站出发，经过变电站传输给各个用电区域。为了增加该电网中电能的协调性和电网的抗毁能力，仿真电网在各个变电站之间随机初始化变电站之间的输电线。各个用电区域当前负载情况如图 3 所示。此时，根据 1.1 节中的仿真建模方法，设置最大容忍系数 K 为 1.5，各个变电站的仿真运行参数如表 1 所示。

针对当前电网状态，不同的方法选择的攻击目标是不同的。为了比较本文提出的 RHGEle_Rank，

HGELe_Rank 与现有重要节点识别方法，首先选择度中心性和介数中心性识别电网中的重要节点。同时，考虑到电网的区域负载情况，本文对度中心性进行改进。将用电区域负载作为变电站–用电区域的边权重后，设计了一个加权度中心性，边(v_i, v_j)的权重为：

$$w_{ij} = \frac{1}{N_i} L(v_j) \tag{5}$$

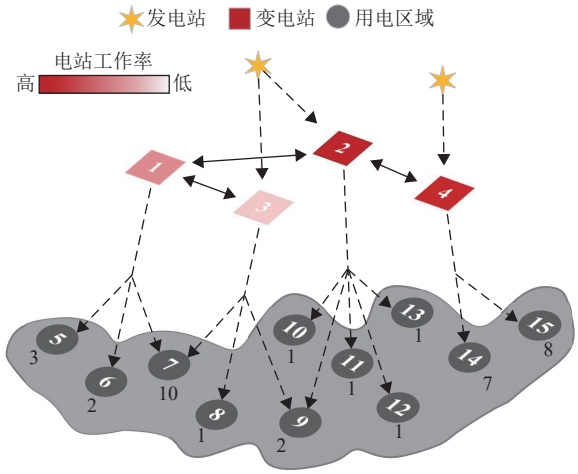


图 3　仿真实验示例电网 (用电区域中各节点旁边的数字表示该用电区域的用电量)

此时，节点v_i的加权中心性为：

$$W_{\text{Degree}}(v_i) = \sum_{(v_i, v_j) \in E} w_{ij} \tag{6}$$

表 1　变电站仿真参数

节点序号v	所需负载$L(v)$	工作效率$\eta(v)$/%	最大负载$\bar{L}(v)$
1	10	85	15.0
2	5	100	7.5
3	6	70	9.0
4	15	100	22.5

为了方便计算和展示，本文实验中设定单次节点破坏量为 30%，非线性节点自动恢复函数中k=2。上述 4 种重要节点挖掘方法和 RHGEle_Rank 的识别结果如表 2 所示。

从表 2 可看出，不同方法识别出的重要变电站不同。传统复杂网络分析方法 (度中心、介数中心性) 认为节点v_2在网络中更重要，若需要破坏该电力系统，需优先攻击v_2变电站。而结合电网负载改进的加权度中心性认为变电站v_4当前供电最多，理应优先被攻击。若不考虑节点恢复对后续攻击的影响 (即每一次攻击只考虑当前电网中的供电情况)，在模拟攻击后发现攻击变电站v_1和v_3的收益最大，只有$v_9 \to v_{15}$的用电区能正常供电，因此 HGEle_Rank 方法认为变电站v_1和v_3更为重要。

表 2　不同方法重要节点识别结果

度中心性		介数中心性		加权度中心性		HGEle_Rank		RHGEle_Rank	
节点	值	节点	值	节点	值	节点	值	节点	值
2	9	2	0.104	4	15	1	17	3	2
1	8	1	0.093	1	10	3	17	1	0
3	4	4	0.033	3	6	4	15	2	0
4	4	3	0	2	5	2	0	4	0

如果考虑了网络弹性的影响，当节点v_1在t时刻被破坏 30% 后，$\eta^t(v_1) = 55\%$。此时该变电站处于超负载失效状态。由于在变电站遭到损坏后，维修人员会对变电站进行维修，变电站的工作效率会在$t+1$时刻恢复一部分。根据本文提出的节点恢复策略，节点v_1在$t \to t+1$之间，恢复量为$r(v_1) = 0.65^2 - 0.55^2 = 0.422\,5 - 0.302\,5 = 0.12$。因此，在$t+1$时刻攻击到来时，节点$v_1$的工作效率为$\eta^{t+1}(v_i) = \eta^t(v_i) + r(v_1) = 0.55 + 0.12 = 0.67$。由于$t+1$时刻，变电站$v_1$需要供给总共 10 负载的区域。而变电站的最大负载为$\bar{L}(v_1) = 15$，工作效率为 67%，此时能供给的有效电能为$\eta^t(v_1)\bar{L}(v_1) = 10.05$，大于当前的供电所需，已恢复正常。即本文提出的 RHGEle_Rank 方法认为，当前变电站v_1虽然很重要，但在遭到攻击或发生故障后，变电站能快速修复。短时间内，该变电站就可以从故障状态恢复到正常状态，属于“无效攻击”。因此，本文提出的 RHGEle_Rank 方法在对重要节点识别的过程中，降低了这类节点的重要性。在上述例子中，认为节点 3 更为重要。

为了验证各个方法是否能在更复杂的场景下准

确识别出重要节点，重新构建了一个规模更大的弹性异质电网进行多轮电网攻防模拟实验。实验选取复杂网络中的经典的度中心性作为重要节点识别对比方法。针对选取的最重要节点，降低其 30% 的工作效率。随即，对所有变电站进行级联失效判断，将当前所有正常供电的区域的负载总和作为评价指标。最后，利用本文提出的节点恢复仿真方法，对当前所有受损变电站进行修复。在进行了 65 次仿真攻击和节点恢复后，攻击效果如表 3 所示。

表 3　不同方法的攻击次数与网络剩余供电力对比

破坏供电能力/%	RHGEle_Rank/次	HGEle_Rank/次	度中心性/次
10	5	5	15
20	16	-	21
35	21	-	25
60	36	-	45
80	46	-	55
100	59	-	65

表 3 展示了不同方法以破坏相同供电能力为目标的攻击次数对比。其中去除“变电站修复”步骤的 HGEle_Rank 方法最大只能降低电网 10% 的供电能力，因此超过 10% 的实验数据为空 (“-”)。从表 3 可看出，本文提出的方法相较于传统的度中心性攻击方法，破坏电网的能力更强。以破坏 60% 的电网供电能力为目标，本文提出的方法只需进行 36 次攻击，而传统的度中心性攻击方法则最少需要 45 次攻击。特别地，为了使整个电网完全瘫痪，基于度中心性的攻击，第 64 次攻击才完全破坏该电力系统。然而在 RHGEle_Rank 方法的指导下，59 次攻击后电网系统已完全瘫痪。因此，相比于传统重要节点识别方法，RHGEle_Rank 所选择的目标对电网有更大的影响力。图 4 展示了剩余正常供电的用电区域负载随攻击次数的变化情况。每个时刻正常供电区域负载越大，说明此刻电网系统破坏量越少，该电网攻击方法的效果越差。从图 4 中可以看出，在大部分时间，在攻击了 RHGEle_Rank 选择的重要目标后，正常供电的用电区域更少，电网系统遭到的破坏更大。

特别地，在重要节点识别中得分函数计算阶段，对只考虑当前电网供电状态的 HGEle_Rank 方法在第 15 次攻击后，就会陷入“无效攻击”的困境。而真实的电力网络往往富有弹性，每一次攻击时，需要考虑节点的恢复情况对后续攻击的影响。由于 HGEle_Rank 方法没有考虑这种影响，攻击由 HGEle_Rank 方法选择的重要节点，不会产生任何级联事故甚至在下次攻击前该变电站就已经完全恢复其工作效率而正常运转。为了减少对“无效攻击”节点的选择，RHGEle_Rank 在贪心策略中加入了节点恢复机制，使得在每次受到攻击前先降低“无效攻击”节点的攻击收益，从而能有效识别出当前攻击 (防御) 收益最高的关键目标，避免频繁的“无效攻击”。

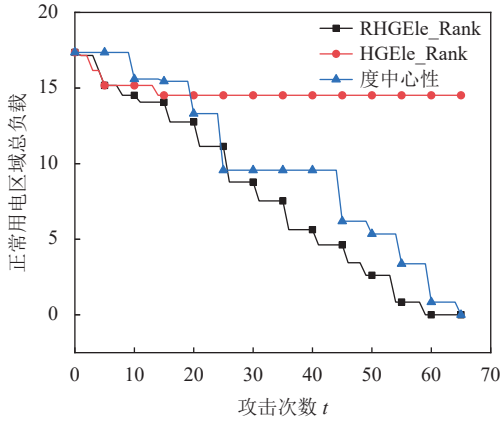


图 4　弹性异质电网的多轮博弈仿真实验结果

为了验证 RHGEle_Rank 的普适性和鲁棒性，本文基于权威的电力网络 WECC(western electricity coordinating council) 进行仿真实验。WECC 数据集中的 Bus 节点、Load 节点和 Generator 节点分别看作本文仿真模型中的变电站节点、负载节点和发电站节点。特别地，WECC 数据集中的 branch 描述了 Bus 节点之间的电流传输状态。因此，基于 branch 可以建立变电站之间的电力传输关系。为了更好地对比本文方法与其他方法，在初始化 WECC 网络阶段，设置变电站最大容忍系数 K=1.1，最大攻击次数为 400，其余参数与前述仿真实验相同。WECC 中，正常供电的用电区域的负载随攻击次数的变化情况如图 5 所示。从图中可以看出，相较于传统复杂网络重要节点挖掘方法，本文的 RHGEle_Rank 方法挖掘出的重要节点对网络的影响更大，在 140 次攻击后，WECC 电网系统已经完全丧失供电能力，而度中心性方法在 400 次攻击后仍存在正常供电区域。除此以外，对 HGEle_Rank 方法，攻击的早期就选择了攻击后能立刻恢复或者有协同供电的变电站。这类变电站虽然受到一定的损坏，但整个电力系统依旧能为下游用电区域提供足够的电能，陷入“无效攻击”的困境，导致攻

击 HGEle_Rank 方法选出的重要节点无法影响整个电网系统的供电能力。

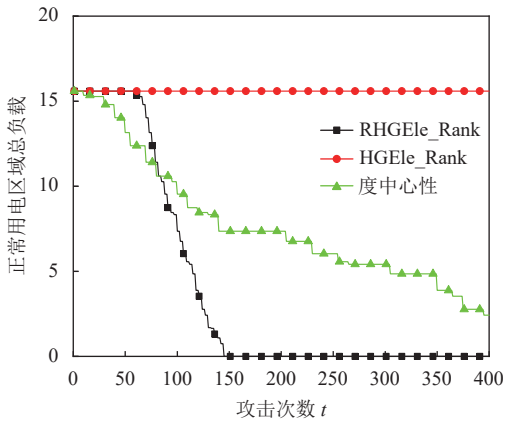


图 5　WECC 异质电网的多轮博弈仿真实验结果

3　结 束 语

以当前信息化战争为背景，考虑真实电网的弹性和异质特性，本文首先搭建了一个多轮博弈的电网仿真模型。针对电网的弹性特征，为了模拟多轮攻击下变电站的自我修复场景，设计了节点自我恢复机制模型。针对电网的异质特征，设计了基于过载式和断电式的级联失效模型。最后，基于此弹性异质电网仿真模型，采用贪心策略设计了一个攻击收益函数，提出了一个电网的重要目标识别方法 RHGEle_Rank。在攻击 RHGEle_Rank 选择的重要目标后，相比于其他重要目标识别方法，RHGEle_Rank 能有效避免“无效攻击”，更大程度地破坏电网的供电能力。然而，在真实信息化战争中，往往每次攻击是有代价的，且不同攻击目标的代价都是不同的。因此，结合电网目标的攻击代价，设计一个更为真实、复杂的电网仿真模型，从而提高电网重要目标识别的准确率是今后重要的研究方向。

参　考　文　献

[1] LYU L Y, CHEN D B, REN X L, et al. Vital nodes identification in complex networks[J]. Physics Reports, 2016, 650: 1-63.

[2] 任晓龙, 吕琳媛. 网络重要节点排序方法综述[J]. 科学通报, 2014, 59(13): 1175-1197.
REN X L, LYU L Y. Review of ranking nodes in complex networks[J]. Chinese Science Bulletin, 2014, 59(13): 1175-1197.

[3] CHEN D B, GAO H, LYU L Y, et al. Identifying influential nodes in large-scale directed networks: The role of clustering[J]. PloS One, 2013, 8(10): e77455.

[4] CHEN D B, LYU L Y, SHANG M S, et al. Identifying influential nodes in complex networks[J]. Physica A, 2012, 391(4): 1777-1787.

[5] KITSAK M, GALLOS L K, HAVLIN S, et al. Identification of influential spreaders in complex networks[J]. Nature Physics, 2010, 6(11): 888-893.

[6] 潘侃, 尹春林, 王磊, 等. 基于特征工程的重要节点挖掘方法[J]. 电子科技大学学报, 2021, 50(6): 930-937.
PAN K, YIN C L, WANG L, et al. Identifying critical nodes based on feature engineering[J]. Journal of University of Electronic Science and Technology of China, 2021, 50(6): 930-937.

[7] KATZ L. A new status index derived from sociometric analysis[J]. Psychometrika, 1953, 18(1): 39-43.

[8] FREEMAN L C. Centrality in social networks conceptual clarification[J]. Social Networks, 1978, 1(3): 215-239.

[9] NEWMAN M E J. A measure of betweenness centrality based on random walks[J]. Social Networks, 2005, 27(1): 39-54.

[10] BRIN S, PAGE L. The anatomy of a large-scale hypertextual web search engine[J]. Computer Networks, 1998, 30: 107-117.

[11] KLEINBERG J M. Authoritative sources in a hyperlinked environment[J]. Journal of the ACM, 1999, 46(5): 604-632.

[12] 李鹏翔, 任玉晴, 席酉民. 网络节点 (集) 重要性的一种度量指标[J]. 系统工程, 2004, 22(4): 13-20.
LI P X, REN Y Q, XI X M. An importance measure of actors (set) within a network[J]. Systems Engineering, 2004, 22(4): 13-20.

[13] RESTREPO J G, OTT E, HUNT B R. Characterizing the dynamical importance of network nodes and links[J]. Physical Review Letters, 2006, 97(9): 094102.

[14] 谭跃进, 吴俊, 邓宏钟. 复杂网络中节点重要度评估的节点收缩方法[J]. 系统工程理论与实践, 2006, 26(11): 79-83.
TAN Y J, WU J, DENG H Z. Evaluation method for node importance based on node contraction in complex networks[J]. Systems Engineering-Theory and Practice, 2006, 26(11): 79-83.

[15] 陈勇, 胡爱群, 胡啸. 通信网中节点重要性的评价方法[J]. 通信学报, 2004, 25(8): 129-134.
CHEN Y, HU A Q, HU X. Evaluation method for node importance in communication networks[J]. Journal of China Institute of Communications, 2004, 25(8): 129-134.

[16] MOTTER A E, LAI Y C. Cascade-Based attacks on complex networks[J]. Physical Review E, 2002, 66(6): 065102.

[17] DUENAS-OSORIO L, VEMURU S M. Cascading failures in complex infrastructure systems[J]. Structural Safety, 2009, 31(2): 157-167.

[18] CRUCITTI P, LATORA V, MARCHIORI M. Model for cascading failures in complex networks[J]. Physical Review E, 2004, 69(4): 045104.

[19] ALBERT R, JEONG H, BARABASI A L. Error and attack tolerance of complex networks[J]. Nature, 2000, 406(6794): 378-382.

[20] ALBERT R, ALBERT I, NAKARADO G L. Structural vulnerability of the North American power grid[J]. Physical Review E, 2004, 69(2): 025103.

[21] HAIMES Y Y. On the definition of resilience in systems[J]. Risk Analysis, 2010, 29(4): 498-501.

[22] 赵丽敬. 电网的弹性建模与评估[D]. 武汉: 华中科技大学, 2015.
ZHAO L J. Resilience modeling and assessment of power grid[D]. Wuhan: Huazhong University of Science and Technology, 2015.

[23] 刘莉, 陈学锋. 智能配电网故障恢复的现状与展望[J]. 电力系统保护与控制, 2011, 39(13): 148-154.
LIU L, CHEN X F. Status and prospect of service restoration in smart distribution network[J]. Power System Protection and Control, 2011, 39(13): 148-154.

[24] BRUNEAU M, CHANG S E, EGUCHI R T, et al. A framework to quantitatively assess and enhance the seismic resilience of communities[J]. Earthquake Spectra, 2012, 19(4): 733-752.

[25] 吴嫣媛, 刘向军. 考虑级联失效影响的复杂网络关键节点识别[J]. 计算机工程与设计, 2021, 42(4): 920-926.
WU Y Y, LIU X J. Identification of key nodes in wireless sensor networks considering cascading failure[J]. Computer Engineering and Design, 2021, 42(4): 920-926.

编 辑 蒋 晓