doi:10.3969/j.issn.1001-4616.2026.02.010

一种针对物理层攻防特性的电力系统受击损失分析模型

罗逸夫[1],喻志谦[2],王启瑞[3],曾志红[1],刘乃通[1]

(1.长沙理工大学电气与信息工程学院,湖南 长沙 410114)
(2.广东电网有限责任公司珠海供电局,广东 珠海 519075)
(3.南京师范大学南瑞电气与自动化学院,江苏 南京 210096)

[摘要] 聚焦于电力系统作为关键基础设施在军事行动和恐怖袭击等外部物理攻击过程中的易受击性,区别于信息网络单点攻击过程,构建了一种考虑物理层攻防范围特性的电力系统受击损失鲁棒优化模型. 首先,根据电力系统的地理信息和网架结构,建立了区域受击毁伤关联传播模型. 其次,考虑攻防双方的决策互动,建立了零和博弈双层模型. 最后,利用 KKT 条件和对非线性约束的逻辑展开实现模型线性化和精确求解. 算例验证表明,本文所提模型能够准确求解电力系统在面对物理攻击者最优进攻方案时的最小损失;同时,不同防御资源分配方案的优劣会随着攻击者的能力而变化,反映了攻防博弈问题的复杂交互过程,进一步验证模型的合理性.

[关键词] 鲁棒优化,零和博弈,电力系统,安全防御,线性化
[中图分类号]O224 [文献标志码]A [文章编号]1001-4616(2026)02-0098-12

A Power System Loss Analysis Model Targeting the Offensive and Defensive Characteristics at Physical Layer

Luo Yifu[1], Yu Zhiqian[2], Wang Qirui[3], Zeng Zhihong[1], Liu Naitong[1]

(1.School of Electrical and Information Engineering, Changsha University of Science and Technology, Changsha 410114, China)
(2.Zhuhai Power Supply Bureau, Guangdong Power Grid Co., Ltd., Zhuhai 519075, China)
(3.School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing 210096, China)

Abstract: This study focuses on the vulnerability of power system as critical infrastructure during external physical attacks such as military operations and terrorist strikes, distinguishing it from the process of single-point attacks on information networks. A robust optimization model for power system loss under attack is constructed, considering the scope characteristics of attack and defense at the physical layer. Firstly, based on the geographical information and grid structure of the power system, a model for regional damage correlation propagation is established. Secondly, a two-level zero-sum game model is constructed considering the decision-making interactions between the attacker and the defender. Finally, the model is linearized and solved accurately using the Karush-Kuhn-Tucker (KKT) conditions and logical expansion of nonlinear constraints. Case studies demonstrate that the proposed model can accurately determine the minimum loss of the power system when facing the most dangerous attack plan by a physical attacker. Additionally, the superiority and inferiority of different defense resource allocation schemes vary with the attacker's capabilities, reflecting the complex interaction process of the attack-defense game and further validating the rationality of the model.

Key words: robust optimization, zero-sum game, power system, security defense, linearization

电力系统作为国家重要的基础设施,其安全稳定事关国家安全、社会发展全局. 因其重要作用,针对电力系统的恶意攻击行为呈上升趋势. 1999 年科索沃战争中,北约军队的空袭导致了南联盟地区 80%以上的电力设施被摧毁,使得南联盟几乎完全丧失战争潜力;近年来极端分子针对美国电网的物理攻击事件也呈上升趋势[1-2];俄乌战争期间,俄罗斯针对乌克兰境内多处电力供应基础设施的袭击严重阻碍了乌军

收稿日期:2025-04-23.
基金项目:广西青年创新人才科研专项项目(桂科 AD22080052).
通讯作者:罗逸夫,博士研究生,研究方向:电力系统运行优化与受击分析. E-mail:ifluomiou@163.com

兵力调度和作战效能[3]. 这些案例深刻地揭示了传统安全问题不断升级的国际背景下,电力系统在现代战争和恐怖袭击中的关键地位及其被利用为战略软杀伤工具的可能性.

信息化作战的精确打击手段使得电力系统面临的潜在受击威胁具有局部性和精确性的特点,这意味着电力系统的连接结构、地理信息及其防御资源布局对攻击者而言几乎是完全透明的[4-5],同时,真实的战争和恐怖攻击场景具有唯一性和不可重复性. 这使得从防御者角度进行受击分析时,倾向于认为自身即将面对攻击者最危险的进攻策略. 因此,在理论分析时假设攻防双方将在完全信息条件下进行博弈推演[6-7].

电力网络攻击按照攻击对象的不同可以分为两类,第一类是针对电力系统一次侧的物理攻击,这类攻击将直接导致一次设备的故障[6-9];第二类是针对电力信息系统的信息入侵,通过虚假数据注入攻击诱导运行人员做出错误的调度决策,或入侵电力设备使其停止提供服务[10-12]. 当前国内外专家学者针对电力系统外部安全防御的研究重点集中于针对电力系统智能设备信息网络入侵的模拟和防御[12-16]. 相比于物理攻击,信息网络攻击更易实现针对多个同类目标的同时攻击[16-17],如 2015 年乌克兰电力系统遭遇的网络攻击使得 30 座变电站离线,并最终导致 1/5 的基辅地区陷入停电[18]. 同时,通过网络连接对电力系统展开的攻击可以在不暴露攻击者身份的条件下对电力系统的安全稳定和运行经济性产生影响. 但受限于电力系统信息网络实际构成,对电力系统信息网络入侵需要借助电力设备的智能终端实现[15,19],因此可能无法攻击到系统中全部的网络单元. 此外,攻击者还需进行侦察并研究网络条件、获取网络的初始接入途径等一系列实施步骤[20-21].

研究[6-9,22-23]针对物理攻击者的模拟和受击分析采用了与信息网络入侵者类似的交互模型,攻击者虽然能够有选择地针对物理层中包括发电厂、变电站、输电线路在内的各类网络单元制定攻击策略并实施精确打击,但其核心依然沿用了信息网络攻击场景中的单点攻击与级联传播模型[22-23]. 事实上,在实施物理层的热武器攻击时,攻击者并不能同信息网络入侵一样直接地针对特定网络单元实现点对点的攻击或入侵,因为发动物理层面的攻击需要考虑更为复杂的物理因素,如临近防御单位的协防以及地理环境对物理攻击扩散效果的阻隔等. 同时,物理攻击者的单次攻击能够对电力系统造成远超越精确攻击单个网络单元的范围影响. 攻击者在投入热武器等物理形式攻击对电力系统造成毁伤破坏或直接占领时,将有能力导致区域范围内的所有电力设备同时受损或失效. 如 2024 年俄军的大规模空袭导致乌克兰损失 80%的火力发电能力和 35%的水力发电能力[24]. 因此,在针对外部物理攻击者进行建模分析时,应当区别于信息网络入侵的单点攻击,强调其范围攻击特性.

此外,文献[23,25-26]认为,对电力设备设置防御资源必定能够成功防御攻击者的入侵或破坏. 然而,攻击者作为决策者,可以选择投入更多的攻击资源来实现对高价值目标的打击. 理论模型需要量化攻击方和防御方的攻防能力,为此,本文沿用了攻击方在付出足够攻击代价后能够突破防御的假设[6,22],使得电力系统遭遇的进攻策略更加危险.

因此,为分析外部物理攻击者对电力系统造成的损失,本文将物理攻击建模为一个显著区别于信息网络入侵的多区域攻防过程,在建立受击区域与网络单元运行状态关联关系的基础上,提出了用于分析电力系统外部受击损失的攻防双层博弈模型,然后利用 KKT 条件将双层问题转化为单层问题并通过逻辑展开实现了模型的线性化,将原问题转化为一个可解的混合整数线性规划问题(mixed integer linear problem, MILP). 通过计算电力系统在应对最恶劣攻击方案下的最小损失,比较不同防御资源分配方案的有效性,为优化电力系统防御策略、确保电力系统在复杂外部环境下的安全运行提供科学依据.

1 受击区域网络单元毁伤关联传播模型

在实际电力网架中,电气距离较近的网络单元之间地理位置可能较远,而地理位置相距较远的网络单元之间可能电气距离较近. 因此,受地理因素影响,目标电力系统可界定为多个区域. 可以认为各区域的局部电力网络在物理层面上近似相互隔离,因传输线而建立联系.

外部攻击者对电力系统发动物理打击时会连带攻击或占领一定区域内的所有网络单元. 但由于与相邻区域的地理阻隔,在单次攻击中,攻击者的攻击效果仅能作用于一个地理区域. 同时,电力系统中的各个单元通过电力网架相互联系,当某一网络单元毁伤或脱网后,会对与其相邻的网络单元造成传播损伤,

对其他区域的网络单元产生影响,如图 1 所示.

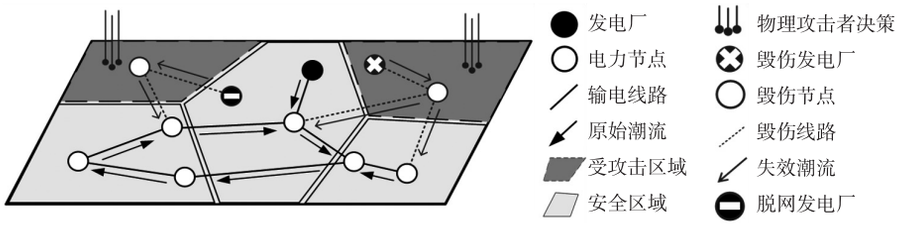


图 1　物理攻击过程示意图

Fig. 1　Diagram of physical attack process

当节点关联线路或发电厂脱网时,系统的潮流分布会发生改变,但节点仍可由其他关联线路供电. 即使成为孤立节点,其所在区域的电力需求始终客观存在,节点失效的事实会在体现系统的失负荷成本当中. 而当网络节点直接遭受攻击时,节点的运行状态则保持为 0,以切断负荷供应. 因此,对于系统中的网络节点,其运行状态仅与自身所在区域的受击状态有关,如式(1)所示:

$$x_k^B = 1 - y_{r(k)}\,, \tag{1}$$

式中,x_k^B 为电力网络节点 k 的运行状态二进制中间变量,正常运行为 1,否则为 0;y_h 为区域 h 受击状态二进制决策变量,受攻击为 1,否则为 0;$r(k)$ 表示包含节点 k 的区域编号.

发电厂的直接受击会导致其因毁伤而脱网. 此外,如果电力系统因受击导致发电厂相邻节点的毁伤或脱网,那么发电厂即使能够正常生产,也无法参与并网运行. 因此发电厂运行状态由其所在区域受击状态和相邻节点运行状态共同决定,如式(2)所示:

$$x_i^G = x_{r(i)}^B (1 - y_{r(i)})\,, \tag{2}$$

式中,x_i^G 为发电厂 i 运行状态中间变量,正常为 1,否则为 0;$r(i)$ 表示包含发电厂 i 的区域编号.

输电线路因其功能属性可能出现同一线路途径多个区域的情况,如果线路的始末节点或与线路自身受到攻击,将导致输电线路停运,其运行状态如式(3)所示:

$$x_j^L = x_{o(j)}^B x_{e(j)}^B \prod_{r(h)=j}^{HL_j} (1 - y_h)\,, \tag{3}$$

式中,x_j^L 为线路 j 的运行状态中间变量,正常运行为 1,否则为 0;$o(j)$ 表示线路 j 的起始节点;$e(j)$ 表示线路 j 的末端节点;HL_j 为线路 j 经过区域的数量;$r(h)=j$ 表示线路 j 所经区域的编号.

2　针对电力系统外部受击损失分析的零和博弈双层模型

2.1　电力系统受击问题攻防博弈框架

在本土战争、恐怖袭击等电力系统外部受击场景下,攻击者希望己方所需投入的攻击成本造成最大化的破坏效果,而防御者希望通过执行己方的运行优化策略,抵抗因电力系统受击造成的不良影响. 双方都会基于对方的选择,优化自身资源部署,形成二人动态博弈过程. 显然,一方的获益将导致另一方的损失,攻防双方之间构成零和博弈关系[27]. 其中攻击者作为上层参与者,防御者作为下层参与者,博弈互动框架如图 2 所示.

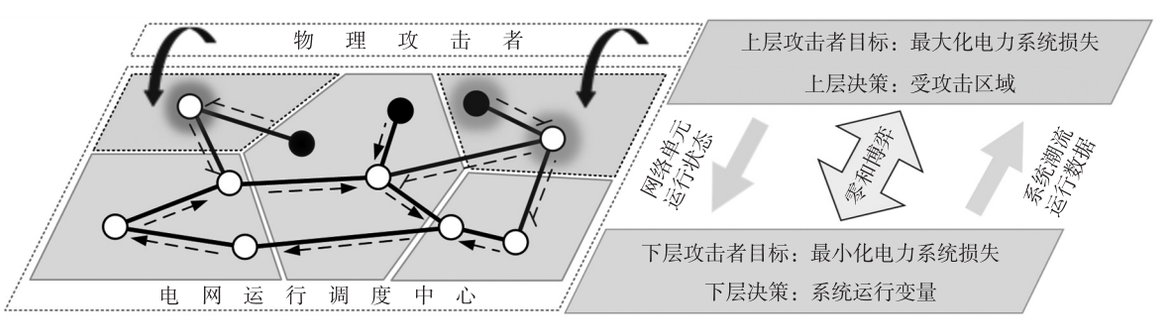


图 2　电力系统攻防零和博弈框架

Fig. 2　Zero-Sum game framework for power system attack-defense

2.2 攻击者模型

攻击者以防御者电力系统损失最大为目标,在投入有限攻击成本的条件下,通过物理攻击手段破坏或占领目标电力系统所在的多个区域,尽可能多的扩大失负荷损失,目标函数为:

$$\max\ C^{loss}, \tag{4}$$

$$C^{loss}=\sum_{k=1}^{K}\alpha_k\Delta P_k^{load}, \tag{5}$$

$$\Delta P_k^{load}=P_{\max}^{load}(k)-P_k^{load}, \tag{6}$$

式中,α_k 为节点 k 供电负荷的单位失负荷成本;ΔP_k^{load} 为节点 k 供电负荷失负荷功率;$P_{\max}^{load}(k)$ 为节点 k 供电负荷的需求量;P_k^{load} 为节点 k 实际供电负荷功率.

如前所述,攻击者通过破坏多个区域的电力设施对电力系统的运行产生影响,但其攻击路径以及对不同区域投放的攻击强度会受到攻击者自身可用攻击成本的限制:

$$\sum_{h=1}^{H}\lambda_h y_h\leqslant R_a, \tag{7}$$

式中,H 是受地理因素影响,目标电力系统被划分的区域总数;λ_h 为成功攻击或占领区域 h 所需付出的攻击代价;R_a 为攻击者最大可用攻击成本.

2.3 防御者模型

防御者在电力系统受到外部攻击后,通过运行优化尽可能维持电力系统的正常运行,同时降低区域内供电损失,目标函数与攻击者完全相反:

$$\min\ C^{loss}. \tag{8}$$

采用最优直流潮流模型模拟调度中心对电力系统受击后的最优运行调整,忽略了电压幅值变化、无功效应和非线性损耗问题,以适应本研究所需的长期粗颗粒度安全分析场景[22-23,28]. 受上层攻击决策导致的网络关联传播效果影响,防御者电力系统运行约束条件如下:

$$\sum_{con(i)=k}^{I}P_i^G-\sum_{o(j)=k}^{J}P_j^L+\sum_{e(j)=k}^{J}P_j^L=P_k^{load}, \tag{9}$$

$$0\leqslant P_i^G\leqslant x_i^G\cdot P_{\max}^G(i), \tag{10}$$

$$P_j^L=\frac{x_j^L(\theta_{o(j)}-\theta_{e(j)})}{b_j}, \tag{11}$$

$$-P_{\max}^L(j)\leqslant P_j^L\leqslant P_{\max}^L(j), \tag{12}$$

$$-\theta_{\max}\leqslant\theta_k\leqslant\theta_{\max}, \tag{13}$$

$$0\leqslant P_k^{load}\leqslant x_k^B\cdot P_{\max}^{load}(k), \tag{14}$$

式中,P_i^G 为发电厂 i 的发电功率;P_j^L 为线路 j 的传输功率;$P_{\max}^G(i)$ 为发电厂 i 发电功率上限;θ_k 为节点 k 的相角;$\theta_{o(j)}$ 为线路 j 起点节点的相角;$\theta_{e(j)}$ 为线路 j 终端节点的相角;b_j 为线路 j 的电抗;$P_{\max}^L(j)$ 为线路 j 传输功率上限;$\theta_{\max}$ 为节点最大相角.

2.4 电力系统受击攻防博弈模型

作为决策者的攻击者和防御者针对同一目标函数 C^{loss} 的优化方向完全相反,因此彼此之间绝无可能开展协同合作,可表示为一个 max-min 问题,如式(15)所示,约束条件为(1)-(3)、(5)-(7)、(9)-(14).

$$F=\max_{a}(\min_{d}(C^{loss}(a,d))), \tag{15}$$

式中,a 为攻击者决策变量(y^G,y^L,y^B)的集合;d 为防御者决策变量的集合$(P^G、P^L、\theta、P^{load})$.

3 博弈模型的转化与求解

本文第 2 章提出的零和博弈双层模型,在数学上是一个混合整数非线性双层模型,除启发式算法外,无法通过常规方法直接求解. 但采用启发式算法存在着容易输出局部最优解,难以获得全局最优解的问题. 因此本章首先利用 KKT 条件将双层问题转化为单层问题,然后对决策变量中的高阶连乘项进行线性化处理,使原问题转化为一个混合整数线性优化问题(mixed integer linear problem,MILP).

3.1　下层问题的模型转换

对于给定的攻击者决策,防御者模型可重新表述为一个以式(16)为目标函数,式(17)-(23)为约束条件的纯线性问题(linear problem,LP):

$$\min_{d}(C^{loss}(d)), \tag{16}$$

$$\sum_{con(i)=k}^{I} P_i^G - \sum_{o(j)=k}^{J} P_j^L + \sum_{e(j)=k}^{J} P_j^L - P_k^{load} = 0, \omega_k, \tag{17}$$

$$0 \leqslant P_i^G \leqslant z_i^G \cdot P_{\max}^G(i), \gamma_i, \tag{18}$$

$$P_j^L = \frac{z_j^L(\theta_{o(j)} - \theta_{e(j)})}{b_j}, \mu_j, \tag{19}$$

$$-P_{\max}^L(j) \leqslant P_j^L \leqslant P_{\max}^L(j), \phi_j, \varphi_j, \tag{20}$$

$$-\theta_{\max} \leqslant \theta_k \leqslant \theta_{\max}, \chi_k, \xi_k, \tag{21}$$

$$0 \leqslant P_k^{load} \leqslant z_k^B \cdot P_{\max}^{load}(k), \sigma_k, \tag{22}$$

$$\Delta P_k^{load} + P_k^{load} = P_{\max}^{load}(k), \kappa_k, \tag{23}$$

式中,z_i^G、z_j^L 和 z_k^B 分别为各类网络单元的运行状态,特别在本节中均可视为常数;ω_k、μ_j、γ_i、ϕ_j、φ_j、σ_k、κ_k、χ_k、ξ_k 分别为下层问题各约束条件对应的对偶变量.

不考虑上层决策影响,下层问题可以推导其对偶问题[29-30]. 对偶问题以式(24)为目标函数,式(25)-(30)为约束条件.

$$\max_{D}\Big\{\sum_{i=1}^{I}\gamma_i z_i^G P_{\max}^G(i) + \sum_{j=1}^{J}(\varphi_j - \phi_j)P_{\max}^L(j) + \sum_{k=1}^{K}[(\xi_k - \chi_k)\theta_{\max} + (z_k^B\sigma_k + \kappa_k)P_{\max}^{load}(k)]\Big\}, \tag{24}$$

$$\omega_{con(i)} + \gamma_i \leqslant 0, P_i^G, \tag{25}$$

$$\kappa_k \leqslant \alpha_k, \Delta P_k^{load}, \tag{26}$$

$$-\omega_k + \sigma_k + \kappa_k \leqslant 0, P_k^{load}, \tag{27}$$

$$\omega_{e(j)} - \omega_{o(j)} + \mu_j + \phi_j + \varphi_j = 0, P_j^L, \tag{28}$$

$$\sum_{e(j)=k}\frac{z_j^L\mu_j}{b_j} - \sum_{o(j)=k}\frac{z_j^L\mu_j}{b_j} + \chi_k + \xi_k = 0, \theta_k, \tag{29}$$

$$\omega_k\,\forall, \mu_j\,\forall, \kappa_k\,\forall, \gamma_i \leqslant 0, \phi_j \geqslant 0, \varphi_j \leqslant 0, \sigma_k \leqslant 0, \chi_k \geqslant 0, \xi_k \leqslant 0, \tag{30}$$

式(16)-(23)是一个目标函数存在且在可行域内可解的简单线性问题,则该问题与其对偶问题的最优解一定满足强对偶性,可以利用 KKT 条件对下层问题进行处理:

$$\sum_{k=1}^{K}\alpha_k \cdot \Delta P_k^{load} = \Big\{\sum_{i=1}^{I}\gamma_i z_i^G P_{\max}^G(i) + (\varphi_j - \phi_j)\sum_{j=1}^{J}P_{\max}^L(j) + \sum_{k}^{K}[(\xi_k - \chi_k)\theta_{\max} + (z_k^B\sigma_k + \kappa_k)P_{\max}^{load}(k)]\Big\}. \tag{31}$$

3.2　原问题模型的转化

利用对偶问题和 KKT 条件可以实现对下层目标函数的钳位效果,可将原双层问题转化为单层混合整数非线性优化问题,目标函数为

$$\max_{a,d,D}(C^{loss}(a,d,D)). \tag{32}$$

约束条件为式(1)-(3)、(5)-(7)、(9)-(14)以及

$$\omega_{con(i)} + \gamma_i \leqslant 0, \tag{33}$$

$$\kappa_k \leqslant \alpha_k, \tag{34}$$

$$-\omega_k + \sigma_k + \kappa_k \leqslant 0, \tag{35}$$

$$\omega_{e(j)} - \omega_{o(j)} + \mu_j + \phi_j + \varphi_j = 0, \tag{36}$$

$$\sum_{e(j)=k}\frac{x_j^L\mu_j}{b_j} - \sum_{o(j)=k}\frac{x_j^L\mu_j}{b_j} + \chi_k + \xi_k = 0, \tag{37}$$

$$\sum_{k=1}^{K}\alpha_k \cdot \Delta P_k^{load} = \Big\{\sum_{i=1}^{I}\gamma_i x_i^G P_{\max}^G(i) + \sum_{j=1}^{J}(\varphi_j - \phi_j)P_{\max}^L(j) + \sum_{k}^{K}[(\xi_k - \chi_k)\theta_{\max} + (x_k^B\sigma_k + \kappa_k)P_{\max}^{load}(k)]\Big\}, \tag{38}$$

$$\omega_k\forall,\mu_j\forall,\kappa_k\forall,\gamma_i\leqslant 0,\phi_j\geqslant 0,\varphi_j\leqslant 0,\sigma_k\leqslant 0,\chi_k\geqslant 0,\xi_k\leqslant 0, \tag{39}$$

式中,D 为对偶问题决策变量集合(ω、μ、κ、γ、ϕ、φ、σ、χ、ξ).

3.3 模型线性化

进一步,对该问题中的非线性连乘项进行逻辑展开. 在式(2)所表示的约束中,$x^B_{r(i)}$ 和 $y_{r(i)}$ 均为二进制变量,当 $x^B_{r(i)}$ 或($1-y_{r(i)}$)为 0 时,x^G_i 的值必为 0,且当 $x^B_{r(i)}$ 和($1-y_{r(i)}$)均为 1 时,x^G_i 的值必为 1. 因此,由式(2)表达的等式约束可展开为不等式约束:

$$x^G_i\leqslant x^B_{r(i)},x^G_i\leqslant 1-y_{r(i)},x^G_i\geqslant x^B_{r(i)}-y_{r(i)}. \tag{40}$$

通过对式(2)的逻辑展开可实现与原等式约束相同的功能,且避免了决策变量连乘,类似的,可对式(3)进行逻辑展开:

$$x^L_j\leqslant 1-\frac{1}{HL_j}\sum_{r(h)=j}^{HL_j}y_h,x^L_j\leqslant x^B_{o(j)},x^L_j\leqslant x^B_{e(j)}, \tag{41}$$

$$x^L_j\geqslant x^B_{o(j)}+x^B_{e(j)}-\sum_{r(h)=j}^{HL_j}y_h-1, \tag{42}$$

式(37)-(38)连乘项中存在着连续变量无取值边界的情况,以式(37)进行说明. 由于决策变量 μ_j 的取值范围无上下界,常规的连乘项线性化方法不再适用. 那么,不妨设 $x^L_j\mu_j=\mu_j-\mu'_j$,对应展开后的约束条件为:

$$\sum_{e(j)=k}\frac{\mu_j-\mu'_j}{b_j}-\sum_{o(j)=k}\frac{\mu_j-\mu'_j}{b_j}+\chi_k+\xi_k=0, \tag{43}$$

$$-x^L_j\cdot M\leqslant\mu_j-\mu'_j\leqslant x^L_j\cdot M, \tag{44}$$

$$-(1-x^L_j)\cdot M\leqslant\mu'_j\leqslant(1-x^L_j)\cdot M, \tag{45}$$

式中,M 为一极大正数. 此时,当 $x^L_j=1$ 时,$\mu_j-\mu'_j=\mu_j$;当 $x^L_j=0$ 时,$\mu_j-\mu'_j=0$. 与展开前的式(37)运算逻辑一致. 同理,式(11)和(38)可分别转化为式(46)-(50)和式(51)-(53):

$$P^L_j=(\theta_{o(j)}-\theta'_{o(j)}-\theta_{e(j)}+\theta'_{e(j)})/b_j, \tag{46}$$

$$-x^L_j\theta_{\max}\leqslant\theta_{o(j)}-\theta'_{o(j)}\leqslant x^L_j\theta_{\max}, \tag{47}$$

$$-x^L_j\theta_{\max}\leqslant\theta_{e(j)}-\theta'_{e(j)}\leqslant x^L_j\theta_{\max}, \tag{48}$$

$$-(1-x^L_j)\theta_{\max}\leqslant\theta'_{o(j)}\leqslant(1-x^L_j)\theta_{\max}, \tag{49}$$

$$-(1-x^L_j)\theta_{\max}\leqslant\theta'_{e(j)}\leqslant(1-x^L_j)\theta_{\max}, \tag{50}$$

$$\sum_{k=1}^{K}\alpha_k\cdot\Delta P^{load}_k=\Big\{\sum_{i=1}^{I}(\gamma_i-\gamma'_i)P^G_{\max}(i)+\sum_{j=1}^{J}(\varphi_j-\phi_j)P^L_{\max}(j)+\sum_{k}^{K}[(\xi_k-\chi_k)\theta_{\max}+(\kappa_k+\sigma_k-\sigma'_k)P^{load}_{\max}(k)]\Big\}, \tag{51}$$

$$-x^G_i\cdot M\leqslant\gamma_i-\gamma'_i\leqslant 0,-(1-x^G_i)\cdot M\leqslant\gamma'_i\leqslant 0, \tag{52}$$

$$-x^B_k\cdot M\leqslant\sigma_k-\sigma'_k\leqslant 0,-(1-x^B_k)\cdot M\leqslant\sigma'_k\leqslant 0. \tag{53}$$

此时,原问题被进一步转化为一个 MILP 问题:

$$\max_{a,d,D,T}(C^{loss}(a,d,D,T)). \tag{54}$$

约束条件为式(1)、(5)-(7)、(9)-(10)、(12)-(14)、(33)-(36)、(39)-(53).

式中,T 为逻辑展开新增变量集合(θ'_o、θ'_e、μ'、γ'、σ').

通过 MATLAB 平台、YALMIP 工具箱调用 CPLEX 求解器可以实现对模型的求解.

4 算例分析

以划分区域后的 IEEE 39 节点系统为案例场景验证本文所提模型的有效性,系统参数来自 MATPOWER 7.0 软件包,地理区域划分与网架结构如图 3 所示,发电厂参数和节点供电参数分别如表 1 和表 2 所示,线路参数见附录 A 表 A1. 所有仿真测试均在 MATLAB 中实现.

4.1 攻击最优性验证

为方便算例分析和后续对比验证,本节设置一种区域防御资源分配方案,记为方案一:

为存在火电厂和负载较重的区域 1、2、3、7、8、9 各分配 4 个防御资源,其他区域各分配 1 个防御资源($\lambda=[4,4,4,1,1,1,4,4,4]$),使用的防御单位总量为 27 p.u..

基于本文所提模型可以计算电力系统极端场景下的受击失负荷损失. 根据方案一布防的电力系统在遭受物理攻击者不同攻击能力 E^{atk} 时的损失评估结果如表 3 所示.

表 1　发电厂参数

Table 1　Power plant parameters

发电厂编号	所处区域	关联节点	功率上限 $P^{G}_{\max}$/MW
1	1	30	250
2	9	31	678
3	9	32	650
4	8	33	632
5	7	34	508
6	5	35	650
7	8	36	560
8	1	37	540
9	2	38	830
10	3	39	1 000

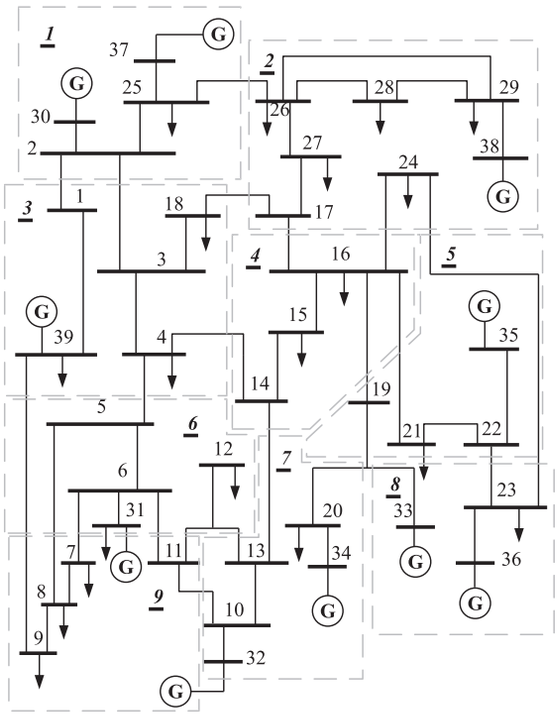


图 3　IEEE 39 节点系统地理区域划分与网架结构

Fig. 3　Geographical zone division and grid structure of the IEEE 39-bus system

表 2　节点与系统供电参数

Table 2　Bus and system power supply parameters

节点编号	所处区域	供电负荷/MW	失负荷成本 α_k/(¥/MW)	节点编号	所处区域	供电负荷/MW	失负荷成本 α_k/(¥/MW)
1	3	97.6	100	22	5	0	0
2	1	0	0	23	8	247.5	100
3	3	322	100	24	2	308.6	100
4	3	500	200	25	1	224	100
5	6	0	0	26	2	139	100
6	6	0	0	27	2	281	100
7	9	233.8	100	28	2	206	100
8	9	522	100	29	2	283.5	100
9	9	6.5	100	30	1	0	0
10	7	0	0	31	6	9.2	200
11	9	0	0	32	7	0	0
12	6	8.53	200	33	8	0	0
13	7	0	0	34	7	0	0
14	4	0	0	35	5	0	0
15	4	320	100	36	8	0	0
16	4	329	100	37	1	0	0
17	2	0	0	38	2	0	0
18	3	158	100	39	3	1 104	100
19	5	0	0			总负荷	总失负荷
20	7	680	200			需求/MW	成本/¥
21	5	274	100	合计	6 254.2	745 196	

由表 3 可知,随着攻击者投入攻击成本的提升,电力系统的受击失负荷损失 C^{loss} 逐渐增大,并最终稳定在 745 196 ¥,这与表 2 提供的系统内用户总失负荷成本保持一致. 同时,电力系统的供电量 $sum(P^{load})$ 逐渐下降并在失负荷成本达到最大值时降至 0,这表明攻击者至少投入 22 个攻击单位即可实现对电力系统的失效打击,造成大停电.

表 3　电力系统受击指标随攻击投入成本变化

Table 3　Indicators of power system impact varying with attack cost investment

E^{atk}/p.u.	C^{loss}/￥	$sum(P^{load})$/MW	E^{atk}/p.u.	C^{loss}/￥	$sum(P^{load})$/MW
0	0	6 254.20	12	607 096	1 381.0
1	172 273	4 703.50	13	628 473	1 149.5
2	241 846	6 254.20	14	698 046	471.5
3	306 846	3 375.50	15	698 046	471.5
4	306 846	3 375.50	16	698 046	471.5
5	347 936	3 292.60	17	698 046	471.5
6	425 720	2 669.03	18	722 796	224.0
7	505 496	1 889.00	19	722 796	224.0
8	505 496	1 889.00	20	722 796	224.0
9	505 496	1 889.00	21	722 796	224.0
10	558 446	1 867.50	22	745 196	0
11	607 096	1 381.00	23	745 196	0

为证明本文所提模型能够准确提供攻击者的最优进攻方案. 分别在攻击者投资为 6($E^{atk}=6$)和 8($E^{atk}=8$)的前提下,遍历所有能够充分利用攻击成本的可行攻击方案并记录其测试结果. 则可实施的攻击方案分别有 18($C_6^1\cdot C_3^2$)种和 21($C_6^2+C_6^1\cdot C_3^3$)种.

本节的目标是确定对电力系统造成最大破坏效果的进攻方案,从而验证通过本文所提模型求解攻击方案的最优性. 攻击者的攻击方案作为输入量,在求解过程中可视为定值,可以借助式(16)-(23)所表述的模型求解各类攻击方案下电力系统受击后的最小损失情况,如图 4 和图 5 所示,其中图 5 仅展示造成受击损失超过 20 万元的攻击方案.

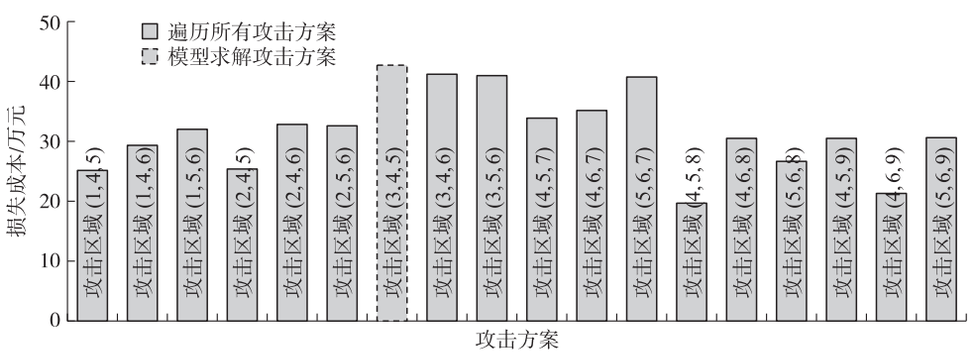


图 4　$E^{atk}=6$ 时各类攻击方案下电力系统受击损失

Fig. 4　Power system impact losses under various attack scenarios when $E^{atk}=6$

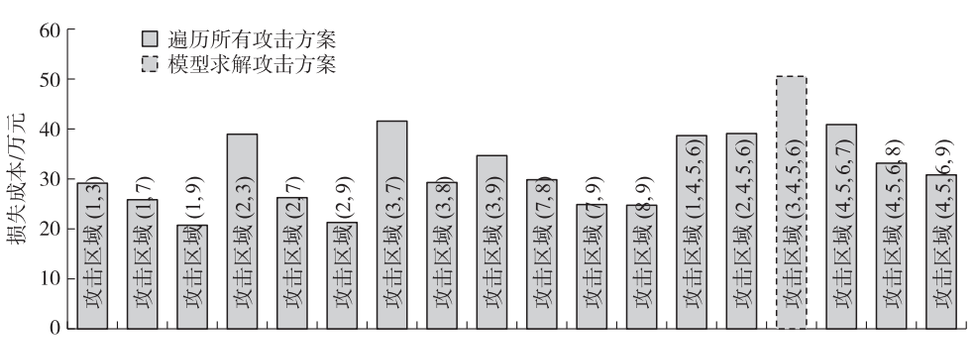


图 5　$E^{atk}=8$ 时各类攻击方案下电力系统受击损失

Fig. 5　Power system impact losses under various attack scenarios when $E^{atk}=8$

由图 4 和图 5 可知,在攻击者的攻击能力为 6 p.u.和 8 p.u.的场景下,攻击者分别在攻击区域为(3,4,5)和(3,4,5,6)的攻击方案中达到了最佳攻击效果,且造成的经济损失与表 3 中提供的模型最优解保持一致. 验证了本文所提模型能够在有限的攻击成本的前提下提供攻击者的最优进攻方案,以分析电力系统可能遭遇最坏情况下的受击损失.

4.2　模型对比

为分析本文模型与同类研究模型之间的共性和区别,本节以文献[22]中面对能够实施精确打击攻击者所建立的安全分析模型为例,与本文所提区域物理攻击的损失分析模型进行对比测试. 同样以 4.1 节中所述 IEEE 39 节点系统为测试场景.

对于精确打击模型,为方便模型验证,参考文献[6]中的防御侧重,简化了对各类网络单元防御资源的分配策略,同时为保证两类模型受击过程中调用的防御资源总量一致,分别为各个发电厂、节点和线路分配 30、12 和 6 个防御单位,使用防御资源的总量为 1 044 p.u..

对于本文区域攻击模型,依据精确打击模型网络单元的防御资源布局,计算各区域内网络单元调用防御资源的总和作为该区域的防御资源. 如前所述,输电线路可能途径多个区域,在本节中不考虑线路实际长度,将输电线路的防御单位平均分配给其途径区域($\lambda=[135,164,125,66,107,80,120,110,137]$),调用的防御资源总量为 1 044 p.u.. 两类模型的电力系统受击损失 C^{loss} 和系统供电能力 $sum(P^{load})$ 对比如图 6 所示.

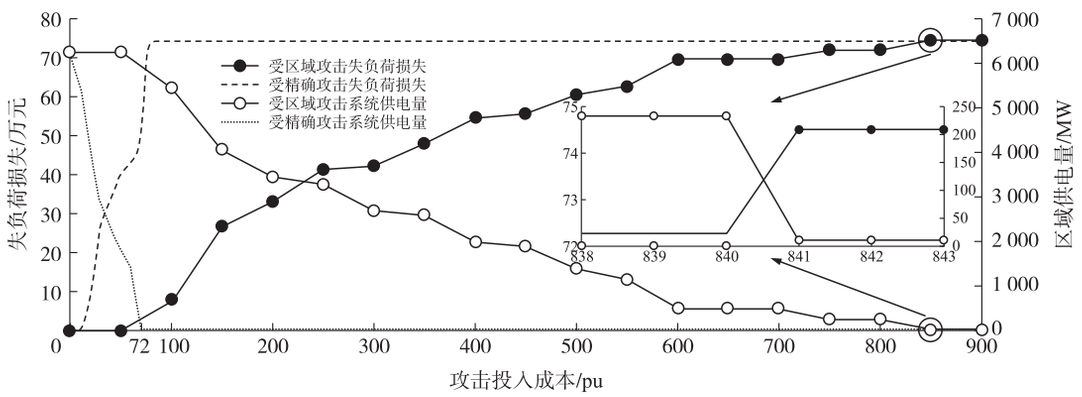


图 6　不同模型受击损失情况对比

Fig. 6　Comparison of impact losses under different models

由图 6 可知,针对案例系统,理想外部攻击者在实施精确打击时能够利用极小的攻击代价实现对电力系统关键单位的精准打击而使电力系统迅速瘫痪. 而物理攻击者则需付出十倍以上的攻击成本才能通过毁坏或占领目标区域的电力设备使电力系统完全失效.

然而,理想攻击者精确打击模型忽视了区域内临近防御单元之间的协同防御效果,使得其计算的攻击效率远高于实际值. 基于该模型的电力系统安全分析将夸大攻击者的攻击能力,造成防御资源的极大浪费. 相比之下,本文所提区域攻击模型通过整合区域防御资源来模拟防御单位的协同能力,使得攻击者完全瘫痪电力系统所需的攻击代价接近电力系统总防御成本.

进一步,图 7 给出了两类模型中电力系统完全瘫痪时遭到攻击的区域或网络单元.

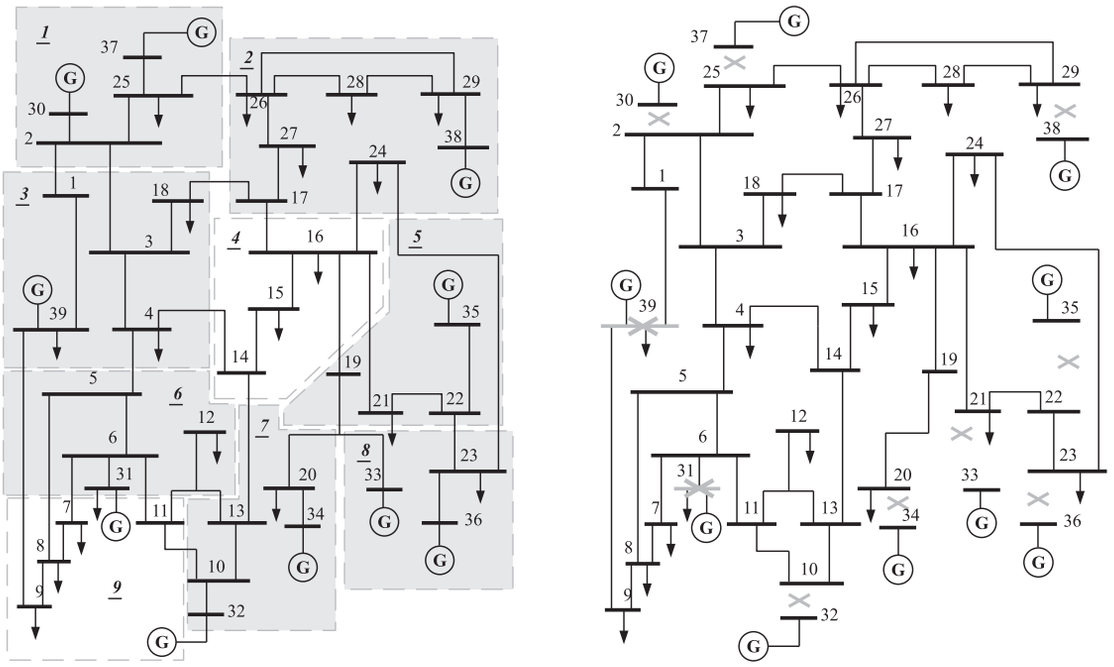
通过图 7 中(a)和(b)的对比可知,理想攻击者模型的精确打击目标完全包含于区域攻击者模型的攻击范围之内. 这表明,两类模型在根据网架结构和布防情况甄别潜在受击目标的判断具有显著一致性,理想攻击者模型对提升电力系统物理层安全性具有一定的指导作用,同时,进一步验证了区域攻击者模型的有效性.

4.3　案例分析

为方便算例分析,本节设置了另一个与方案一总投资相同但侧重不同的国土防御资源分配方案,记为方案二:为各个区域分配 3 个防御单位($\lambda=[3,3,3,3,3,3,3,3,3,3]$),使用的防御单位总量为 27 p.u.. 仅用于模型算例验证的参考参数. 不同防御方案下电力系统的受击指标变化过程如图 8 所示.

通过图 8(a)和(b)的比较可知,采用方案二防御布局对应的两类曲线先一步接近边界值. 这意味着随着攻击者投入成本的提升,采用方案二进行安全防御的电力系统将率先进入崩溃状态.

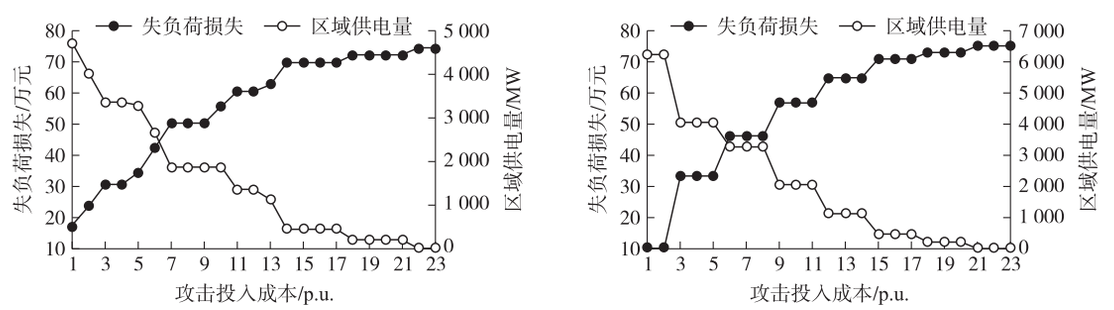
显然,由于致使所涉及系统案例完全失效所需的攻击成本更高,方案一能使电力系统在面对高强度攻击时,具备较强的承受能力. 但在攻击者攻击能力有限甚至较低的条件下,不同方案之间的优劣比较可能会发生变化. 图 9 展示了在攻击者投入不同攻击成本条件下,两类防御方案的受击损失成本及其差值.



(a) 区域攻击模型电力系统失效时的受击情况　　(b) 精确攻击模型电力系统失效时的受击情况

图 7　不同模型电力系统失效时的受击情况

Fig. 7　Areas/Units under attack when power systems malfunction in different models



(a) 防御方案一受击指标随攻击投入成本变化过程　　(b) 防御方案二受击指标随攻击投入成本变化过程

图 8　不同防御方案下电力系统的损失情况

Fig. 8　Loss scenarios of power gird under two defense strategies

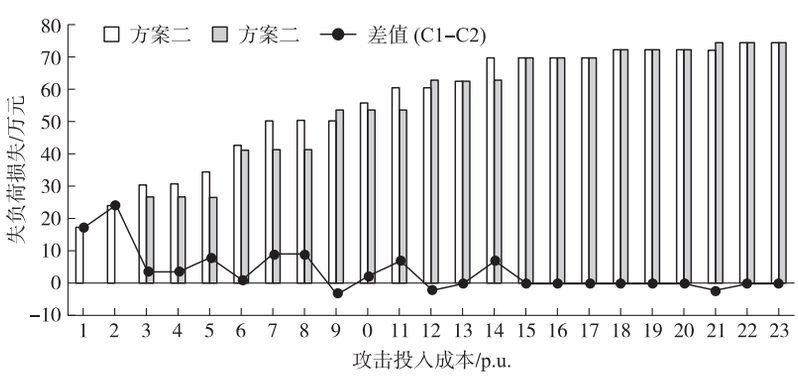


图 9　不同防御方案失负荷成本对比

Fig. 9　Comparison of load loss costs under different defense strategies

由图 9 可知,虽然方案二随着攻击者投入成本的提升最先达到受击损失峰值,但在攻击者攻击能力为 3~14 p.u.的攻防场景中,防御方案二的防护表现总体优于方案一. 特别在攻击者投入攻击成本为 5 p.u.的场景中($E^{atk}=5$),相比于方案一,方案二能够将受击损失降低 22.9%. 这表明防御者的防御侧重需要随着攻击者能力的变化而做出调整.

考虑上述仿真结果,电力系统的防御者应当更加详细的评估各个区域的重要度,相应地调整防御资源的分配. 进一步,如何优化国土资源分配以提高电力系统及区域能源系统的防御能力将作为后续研究的重点.

5　结论

本研究针对电力系统在外部物理攻击下的安全评估问题,构建了一种考虑物理层攻防特性的零和博弈分析框架,并建立了电力系统受击损失分析模型;利用 KKT 条件和对复杂连乘项的逻辑展开,实现对模型的线性化求解;最后借助 IEEE 39 节点系统进行了算例验证和模型对比,结果表明:

(1)区别于信息层网络攻击的单点特性,本研究提出的区域攻防模型充分考虑了物理层攻防资源的范围特性,能够更好地反映电力系统在遭遇物理攻击者时的对弈场景及区域受击的动态过程,为电力系统提供遭遇外部攻击时的损失程度评估.

(2)对于同一案例场景,理想攻击者模型和区域攻击者模型在识别潜在受击网络单元和受击区域时具有一致性,表明精确打击分析模型对提升电力系统物理层安全性具有一定的指导作用,同时也更加证明了区域攻击者模型的有效性.

(3)算例分析表明同一防御方案虽抵御高强度攻击的能力较弱,但在攻击者能力有限的场景下可以相对减少 22.9%的受击损失,表明电力系统的防御侧重需根据攻击者的能力而做出调整.

附录 A

表 A1　线路参数

Table A1　Transmission line parameters

线路编号	所处区域	线路起始节点	线路终端节点	线路电抗标幺值 b	线路编号	所处区域	线路起始节点	线路终端节点	线路电抗标幺值 b
1	1、3	1	2	0.698 7	24	4、10	14	15	0.021 7
2	3	1	39	0.025 0	25	4、10	15	16	0.009 4
3	1、3	2	3	0.015 1	26	2、4	16	17	0.008 9
4	1	2	25	0.008 6	27	4、5	16	19	0.019 5
5	1	2	30	0.018 1	28	4、5	16	21	0.013 5
6	3	3	4	0.021 3	29	2、4	16	24	0.005 9
7	3	3	18	0.013 3	30	2、3	17	18	0.008 2
8	3、6	4	5	0.012 8	31	2	17	27	0.017 3
9	3、4	4	14	0.012 9	32	5、7	19	20	0.013 8
10	6	5	6	0.002 6	33	5、8	19	33	0.014 2
11	6、9	5	8	0.011 2	34	7	20	34	0.018 0
12	6、9	6	7	0.009 2	35	5	21	22	0.014 0
13	6、9	6	11	0.008 2	36	5、8	22	23	0.009 6
14	6	6	31	0.025 0	37	5	22	35	0.014 3
15	9	7	8	0.004 6	38	2、5、8	23	24	0.035 0
16	9	8	9	0.036 3	39	8	23	36	0.027 2
17	3、6、9	9	39	0.025 0	40	1、2	25	26	0.032 3
18	7、9	10	11	0.004 3	41	1	25	37	0.023 2
19	7	10	13	0.004 3	42	2	26	27	0.014 7
20	7	10	32	0.020 0	43	2	26	28	0.047 4
21	6、9	12	11	0.043 5	44	2	26	29	0.062 5
22	6、7	12	13	0.043 5	45	2	28	29	0.015 1
23	4、7	13	14	0.010 1	46	2	29	38	0.015 6

[参考文献]

[1] Soltan S,Zussman G. EXPOSE the line failures following a cyber-physical attack on the power grid[J]. IEEE Transactions on Control of Network Systems,2019,6(1):451-461.

[2] Physical attacks on power grid surge to new peak[EB/OL]. (2022-12-26)[2025-03-15]. https://www.politico.com/news/2022/12/26/physical-attacks-electrical-grid-peak-00075216.

[3] Sanginov A. Chemeris, Resilience of Ukrainian energy system: behavioral simulation of the war influence[C]//2023 13th International Conference on Dependable Systems, Services and Technologies(DESSERT), Athens, Greece, 2023:1-4.
[4] 秦有权,吴爱民,高永红. 电力系统面临的灾害与战争威胁及关键节点防护对策[J]. 防护工程,2018,40(4):64-69.
[5] Zhu Y H, Yan J, Tang Y F, et al. Coordinated attacks against substations and transmission lines in power grids[C]// Proceedings of the IEEE Global Communications Conference, Austin, TX, USA, 2014:655-661.
[6] Salmeron J, Wood K, Baldick R. Analysis of electric grid security under terrorist threat[J]. IEEE Transactions on Power Systems, 2004, 19(2):905-912.
[7] Arroyo J M, Galiana F D. On the solution of the bilevel programming formulation of the terrorist threat problem[J]. IEEE Transactions on Power Systems, 2005, 20(2):789-797.
[8] Shao C W, Li Y F. Optimal defense resources allocation for power system based on bounded rationality game theory analysis [J]. IEEE Transactions on Power Systems, 2021, 36(5):4223-4234.
[9] Xiang Y M, Wang L, Yu D, et al. Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks[C]//2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA, 2015:1-5.
[10] 蔡晔,刘放,曹一家,等. 电力信息物理系统低代价多阶段高危攻击策略研究[J]. 电力系统自动化,2021,45(20):1-8.
[11] 阮振,吕林,刘友波,等. 考虑负荷数据虚假注入的电力信息物理系统协同攻击模型[J]. 电力自动化设备,2019,39(2):181-187.
[12] Li Z, Shahidehpour M, Alabdulwahab A, et al. Analyzing locally coordinated cyber-physical attacks for undetectable line outages[J]. IEEE Transactions on Smart Grid, 2018, 9(1):35-47.
[13] 蔡星浦,王琦,黄建业,等. 电力系统网络攻击信息物理双层协同紧急控制方法[J]. 全球能源互联网,2020,3(6):560-568.
[14] Li Y, Quevedo D E, Dey S, et al. A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 3(1):1-11.
[15] 钱胜,王琦,颜云松,等. 计及网络攻击影响的安全稳定控制系统风险评估方法[J]. 电力工程技术,2022,41(3):14-21.
[16] 刘念,余星火,张建华. 网络协同攻击:乌克兰停电事件的推演与启示[J]. 电力系统自动化,2016,40(6):144-147.
[17] Ranjbar M H, Kheradmandi M, Pirayesh A. Assigning operating reserves in power systems under imminent intelligent attack threat[J]. IEEE Transactions on Power Systems, 2019, 34(4):2768-2777.
[18] 王坤,苏盛,赵奕,等. 变电站自动化系统时间同步协同攻击的检测与防护方法[J]. 电力系统自动化,2021,45(6):231-239.
[19] Liu X, Li Z. Trilevel modeling of cyber attacks on transmission lines[J]. IEEE Transactions on Smart Grid, 2017, 8(2):720-729.
[20] 李田,苏盛,杨洪明,等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化,2017,41(22):162-167.
[21] 杨玉泽,刘文霞,刘耕铭,等. 不完全信息下计及残差污染的虚假数据注入攻击研究[J]. 中国电机工程学报,2025,49(15):7481-7493.
[22] Motto A L, Arroyo J M, Galiana F D. A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat[J]. IEEE Transactions on Power Systems, 2005, 20(3):1357-1365.
[23] Wu X, Conejo A J. An efficient tri-level optimization model for electric grid defense planning[J]. IEEE Transactions on Power Systems, 2017, 32(4):2984-2994.
[24] 俄密集轰炸乌克兰能源设施,法媒:可能是大规模攻势前的针对性措施[EB/OL]. (2024-4-29)[2024-10-25]. http://www.news.cn/mil/2024-04/29/c_1212357993.htm.
[25] 唐夏菲,孙溶佐,谭玉东,等. 面向 IED 攻击的多变电站防御-攻击-防御鲁棒优化模型[J]. 电力系统及其自动化学报,2024,36(9):124-134.
[26] Yuan W, Zhao L, Zeng B. Optimal power grid protection through a defender-attacker-defender model[J]. Reliability Engineering and System Safety, 2014, 121:83-89.
[27] 刘肇军,刘宗谦,冯素芬. 有限策略型博弈中的相关策略与具有合约的博弈及其均衡[J]. 南京师大学报(自然科学版),2008,31(3):33-38.
[28] 伊娜,徐建军,陈月,等. 基于深度强化学习的多阶段信息物理协同拓扑攻击方法[J]. 电力工程技术,2023,42(4):149-158.
[29] 孙旺青,刘晓峰,季振亚,等. 基于分布鲁棒优化的社区型能源系统低碳经济调度[J]. 南京师范大学学报(工程技术版),2022,22(2):15-22.
[30] 马圣容,杨正豪. 一类凸二次规划的对偶方法[J]. 南京师大学报(自然科学版),2003,26(1):39-44.

[责任编辑:陆炳新]