第 50 卷 第 12 期：5584-5595 高电压技术 Vol.50, No.12: 5584-5595
2024 年 12 月 31 日 High Voltage Engineering December 31, 2024
DOI: 10.13336/j.1003-6520.hve.20231057

计及风电波动的电力系统不确定性恶意攻击防御策略

王 峰[1]，刘 洋[1]，杜 敏[2]，刘 绚[2]，郑豪丰[2]，宋宇飞[2]
（1. 国网山东省电力公司电力科学研究院，济南 250003；2. 湖南大学电气与信息工程学院，长沙 410082）

摘 要：在风电波动的电力系统中，风电出力和恶意攻击的不确定性给电力系统安全稳定运行带来了极大的威胁。为了增强电力系统抵御风电波动和不确定性恶意攻击的能力，提出了一种考虑风电出力不确定性并以不确定性恶意攻击为导向的防御-攻击-调度模型。首先，考虑风电出力不确定性，构建了风电出力多面体不确定性集合；其次，考虑不确定性恶意攻击，提出在防御-攻击-调度的框架中构建以不确定性恶意攻击为核心的电力系统防御模型。最后，该模型在 IEEE RTS-79 和 IEEE RTS-96 测试系统上进行仿真验证，并采用 C&CG(column-and-constraint generation)算法进行求解，所得结果充分验证了模型及求解方法的有效性，同时表明考虑风电波动和不确定性恶意攻击的防御技术可以降低电力系统总运行成本，并且能够协助防御人员调控电力系统运行风险。
关键词：不确定性恶意攻击；风电波动；电力系统；多面体不确定性集合；电力系统防御；C&CG

Defense Strategies Against Uncertain Malicious Attacks on Power Systems Considering Wind Power Fluctuations

WANG Feng[1], LIU Yang[1], DU Min[2], LIU Xuan[2], ZHENG Haofeng[2], SONG Yufei[2]
(1. State Grid Shandong Electric Power Research Institute, Jinan 250003, China;
2. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China)

Abstract: In a power system with fluctuating wind power, the uncertainty of wind power output and malicious attacks pose a great threat to the safe and stable operation of the power system. In order to enhance the power system's ability to resist wind power fluctuations and uncertain malicious attacks, a defense-attack-dispatch model is proposed that considers wind power output uncertainty and is oriented to uncertain malicious attacks. Firstly, a polyhedral uncertainty set is formed with considering the wind power generation uncertainty. Secondly, the uncertainty malicious attack is taken into account, and it is proposed to construct a power system defense model with uncertainty malicious attack as the core in the defense-attack-dispatch framework. Finally, the proposed model is simulated and verified on the IEEE RTS-79 and IEEE RTS-96 test systems, and the C&CG (column-and-constraint generation) algorithm is used to solve this model. The simulation results fully verify the effectiveness of the proposed model and solution method and reveal that the defense technology that considers wind power fluctuations and uncertain malicious attacks can reduce the total operating cost of the power system, and can help defenders adjust the risk of power system operation.
Key words: uncertain malicious attacks; wind power fluctuation; power system; polyhedral uncertainty set; power system defense; C&CG

0 引言

近年来，全球恶意攻击事件(自然灾害、人为攻击或网络攻击)频频发生，不仅给电力系统的安全运行造成了严重影响，也对人类的生命财产安全构成了威胁。2008 年，中国 20 多个省市均遭受了不同程度的冰灾影响，其中多个省市的电力基础设施遭受到严重地损坏，直接经济损失超过 104.5 亿元[1]。2015 年，乌克兰电网遭遇到黑客的恶意攻击，导致乌克兰西部地区超过22.5万户居民家中长达数小时停电[2]。2021 年，美国得克萨斯州遭遇了极端严寒天气，发电设施出现大规模停运，导致用户大范围轮流停电[3]。

由于恶意攻击具有破坏性强、危害性大和目标性明确等特点，国内外学者针对电力系统恶意攻击机理和模型展开了深入的研究。在现有的电力系统恶意攻击研究中，电力系统遭受的恶意攻击类别主要考虑 2 大类。第 1 类是针对信息系统的网络攻击，

基金资助项目：国网山东省电力公司科技项目(520626230043)。
Project supported by Science and Technology Project of State Grid Shandong Electric Power Company (520626230043).

文献[4]指出攻击者可以在篡改负荷节点数量最小的前提下，构造恶意的攻击向量致使目标线路过载。文献[5]揭示了攻击者可以致使电力传输线路过载中断进而引发电力系统解列。文献[6]指出攻击者可以对损坏的电力传输线路或设备进行掩盖，致使维修人员无法发现损坏的电力基础设施并及时进行修复，进而影响电力系统的安全稳定运行。第 2 类是以物理系统为目标的物理攻击，主要包括自然灾害、战争和人为破坏在内的极端事件。文献[7]指出攻击者可以通过考虑线路攻击的时间特性，通过构建双层优化模型确定电力传输线路攻击的最佳位置和最佳攻击时间。文献[8]提出了基于连锁故障网络图的电力传输电线路脆弱性评估方法，该方法揭示了电力传输线路攻击与线路故障传播之间的时序关系。文献[9]指出电力系统若出现多条电力传输线路中断，则极有可能会引发连锁故障而导致大规模停电事故。因此，从恶意攻击角度而言，攻击者对电力传输线路的破坏将会给电力系统的安全性、稳定性、经济性和可靠性带来巨大的影响。

针对电力系统面临的恶意攻击威胁，国内外学者开展了相应的防御策略研究，旨在提升电力系统应对恶意攻击的防御能力。电力系统防御能力是指电力系统在遭受恶意攻击时，能够抵御其冲击并维持自身稳定运行状态的能力。为了提升电力系统防御能力，文献[10]基于 N-K 准则提出了面向恶意攻击的攻击-防御模型以确定线路加固策略，进而提升电力系统的防御能力，但该模型只能协助安全人员制定次优的防御策略。为了制定最优的线路加固防御策略，文献[11]提出了防御-攻击-防御模型以制定最佳的防御策略。此外，文献[12]考虑自然灾害和人为攻击下的综合能源优化配置问题，建立了防御-攻击-防御的随机优化模型，以此来确定电力系统的防御策略，进而提升系统防御能力。文献[13]提出了一种台风场景下基于多种分布式资源协同的配电网韧性增强策略，用于解决灾后配电网部分线路损坏的问题，从而实现电网灾后快速恢复。文献[14]以电力传输线路加固为核心，提出了一种考虑恶意物理攻击的线路故障概率信息韧性导向分布鲁棒优化模型，以提升电力系统的韧性。文献[15]运用安全博弈理论构建了防御-攻击-防御的零和主从博弈模型，旨在提升电力系统安全防御能力。文献[16]考虑信息系统与电力系统之间的相互影响，提出了一种电力信息物理系统应对极端自然灾害的韧性增强策略。文献[17]提出了一种鲁棒优化的电力系统网络结构加固模型，以提升电力系统抵抗自然灾害攻击的能力。文献[18]提出了一种在极端天气下保底电网骨干网架的优化方法，以提升电力系统韧性，从而达到降低极端事件危害的目的。文献[19]提出了一种防御-攻击-防御模型来识别和保护连接天然气和电力基础设施的脆弱性线路，以应对恶意攻击。然而，上述研究均是在最极端的攻击场景下确定最佳的防御策略，忽视了风电波动和攻击场景不确定性对防御策略的影响。

目前，电力系统正朝着清洁低碳、安全高效的现代综合能源体系转型[20]。其中，风电等可再生能源的大规模并网是实现电力系统转型的有效途径。然而，风电等可再生能源具有不确定性、间歇性和波动性[21]，这给电力系统安全人员制定防御策略应对恶意攻击提出了更高的要求。如果不考虑风电出力不确定性问题，那么基于传统防御模型所制定的线路加固防御策略可能无法有效地抵御恶意攻击，从而会影响电力系统的安全稳定运行。文献[22-23]提出一种考虑不确定性环境下的电力系统韧性提升策略，然而忽视了恶意攻击的不确定性。恶意攻击(自然灾害、人为攻击或网络攻击)通常也具有不确定性和随机性。例如，攻击者的攻击资源无法被精准预测，雨季时期所伴随的暴雨、强风或洪水的强度以及地震的危害均无法被精准估计。不同于风电出力不确定性，恶意攻击不确定性不具有时空相关性和历史数据统计规律，因此难以精准预测。与此同时，恶意攻击造成的破坏通常是灾难性的且无法事先精准评估其危害。若忽视恶意攻击的不确定性，则会影响电力系统韧性增强策略的有效性，进而影响电力系统的安全稳定运行。因此，考虑恶意攻击不确定性有利于防御人员制定更为实际的防御策略，从而提升电力系防御策略的鲁棒性。综上所述，为了提升电力系统应对风电出力不确定性所引发的内部波动及造成恶意攻击事件外部冲击的能力，亟需研究适用于风电等高比例可再生能源电力系统应对不确定性恶意攻击的防御策略，以降低电力系统脆弱性，增强电力系统防御能力。

为此，本文提出一种考虑风电波动的电力系统不确定性恶意攻击防御策略模型。本文主要创新点为：1）构建了风电出力多面体不确定集，有效地描述了风电出力不确定性与电力系统防御策略之间的内在联系；2）增加了风电出力不确定度参数，可供

安全人员灵活调控电力系统防御策略的保守程度；3）考虑了恶意攻击的不确定性，基于风电出力多面体不确定集构建了应对不确定性恶意攻击的防御-攻击-防御模型；最后，通过对 IEEE 可靠性测试系统进行仿真分析，充分验证了本文模型和求解算法的有效性。

1 电力系统防御策略整体框架的描述

本文基于风电波动的电力系统不确定性恶意攻击构建了防御-攻击-防御框架。其中，防御-攻击-防御框架如图 1 所示，上层表示防御措施：防御人员基于所有可能的攻击场景及其相应的概率，确定需要保护的组件，从而使整体系统总期望成本最低；中层表示攻击策略：在每个合理的攻击场景中，攻击者确定最极端的攻击场景，使电力系统运行成本最高；下层表示调度策略：基于上层防御策略和中层攻击策略，电力系统运营商通过矫正调度方案确保电力系统运行成本最低。其中，中层和下层形成了典型的攻击-防御模型，描述了攻击者确定攻击破坏系统部件的决策方案。这种攻击-防御模型是一个双层优化问题，其攻击资源对攻击策略和防御策略具有很大的影响。所提防御模型考虑了攻击资源不确定性，给电力系统安全部门制定防御措施提供了有效的指导。此外，所提不确定性恶意攻击防御模型，可以很容易地转化为传统防御模型，即仅需要考虑在单一的攻击场景下确定防御策略。

2 电力系统防御模型的构建

2.1 目标函数

本文提出一种考虑风电波动的电力系统不确定性恶意攻击防御模型，能在风电出力和恶意攻击组合的极端场景下确定最佳防御策略，并保证系统总期望成本最小化(包括线路加固成本、机组出力和切负荷惩罚的期望成本)。其中，目标函数如式(1)所示。

$$f=\min_{v_{ij}\in V}\sum_{(i,j)\in L}I_{\mathrm{L},ij}v_{ij}+E_{\Omega(s)}\left(\max_{z_{ij}(s)\in Z,P_{\mathrm{W},b}(s)\in W}Q\left(v_{ij},P_{\mathrm{W},b}(s),z_{ij}(s)\right)\right)\tag{1}$$

式中：$Q\left(v_{ij},P_{\mathrm{W},b}(s),z_{ij}(s)\right)$ 为电力系统运行优化成本，即 $\min_{P_{\mathrm{G},b}(s),F_{ij}(s),\theta_b(s),\Delta S_{\mathrm{D},b}(s)}\sum_{b\in\boldsymbol{B}}\left(I_{\mathrm{G},b}P_{\mathrm{G},b}(s)+I_{\mathrm{D},b}\Delta S_{\mathrm{D},b}(s)\right)$。其中，$I_{\mathrm{L},ij}$ 为线路 (i,j) 的加固成本；v_{ij} 为线路 (i,j) 的加固状态；$z_{ij}(s)$ 为线路 (i,j) 在攻击场景 s 中的中断状态；$I_{\mathrm{G},b}$ 为位于节点 b 的机组出力成本；$I_{\mathrm{D},b}$ 为位于节点 b 的负荷切除惩罚系数；$P_{\mathrm{G},b}(s)$ 为位于节点 b 的机组在攻击场景 s 中的有功出力值；$P_{\mathrm{W},b}(s)$ 为位于节点 b 的风电场在攻击场景 s 中的实际出力值；$\Delta S_{\mathrm{D},b}(s)$ 为位于节点 b 的负荷在攻击场景 s 中的负荷切除量；$F_{ij}(s)$ 为传输线路 (i,j) 在攻击场景 s 中的线路潮流；$\theta_b(s)$ 为节点 b 在攻击场景 s 中的相位角；L、V、Z、B 和 W 分别为传输线路、加固线路、攻击线路、节点和风电出力不确定性的集合；s 为攻击场景；$\Omega(s)$ 为攻击场景 s 的概率。

2.2 电力系统防御策略约束条件

2.2.1 上层电力系统防御策略约束

线路加固资源约束为：

$$\sum_{(i,j)\in L}v_{ij}\le V_{\mathrm{L}},\quad \forall v_{ij}\in\{0,1\}\tag{2}$$

式中：V_{L} 表示防御资源，即线路加固总数；线路 (i,j) 的加固状态 v_{ij} 为二进制变量，取值为 1 表示线路 (i,j) 被加固；取值为 0 表示线路 (i,j) 未被加固。

2.2.2 中层不确定性场景约束

1）风电出力的不确定性集构建

实时风电出力与预测值之间存在一定的偏差，

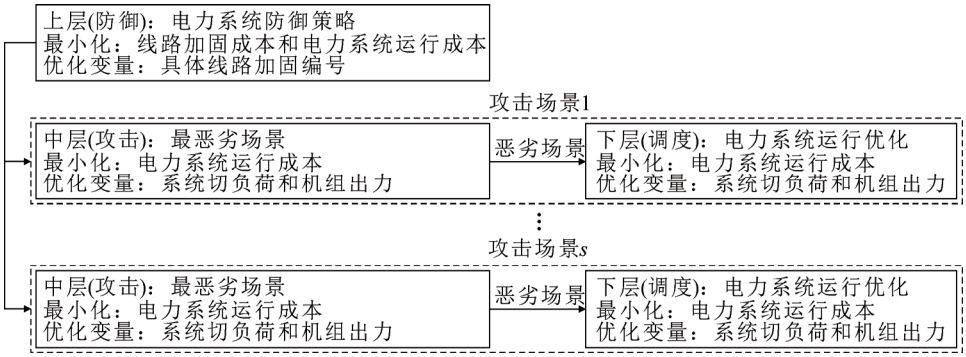


图 1 电力系统防御框架

Fig.1 Defense framework of power systems

成为电力系统中不确定性的来源。本文假设风电有功出力预测值为 $\overline{P}_{\mathrm{W},b}$ 且可能出现的最大波动偏差为 $\Delta P_{\mathrm{W},b}$。因此，风电出力的置信区间可以描述为 $[\overline{P}_{\mathrm{W},b}-\Delta P_{\mathrm{W},b},\overline{P}_{\mathrm{W},b}+\Delta P_{\mathrm{W},b}]$。本文通过引入不确定度参数 Γ 构建风电出力不确定区间，该区间可由凸多面体形式的盒式集合描述为：

$$W=\begin{Bmatrix}\overline{P}_{\mathrm{W},b}\in\mathbb{R}\\ P_{\mathrm{W},b}=\overline{P}_{\mathrm{W},b}+u_b^{+}\Delta P_{\mathrm{W},b}-u_b^{-}\Delta P_{\mathrm{W},b}\\ \sum_{b=1}^{N_{\mathrm{B}}}\left(u_b^{+}+u_b^{-}\right)\le\Gamma\\ u_b^{+}+u_b^{-}\le 1\end{Bmatrix} \tag{3}$$

式中：N_{B} 为节点总数目；N_{w} 为风电场总数目；Γ 为风电出力不确定度参数且 $\Gamma\in[0,N_{\mathrm{w}}]$，$\Gamma$ 数值越大，表示风电有功出力的波动越大，从而所获取的防御策略鲁棒性越强，但其保守性也越大；u_w^{+} 和 u_w^{-} 为二进制变量，当 u_w^{+}/u_w^{-} 取值为 1 时，表示风电出力达到其区间的上界/下界；当 u_w^{+}/u_w^{-} 取值为 0 时，表示风电出力为预测值。为了简单起见，本文不考虑风电场之间的相关性。

2）攻击场景不确定性集构建

$$\sum_{(i,j)\in L}\left(1-z_{ij}(s)\right)\le H_{\mathrm{A}}(s)\ \ \forall z_{ij}(s)\in\{0,1\},s\in S \tag{4}$$

式中：$H_{\mathrm{A}}(s)$ 表示在攻击场景 s 中的攻击资源，即攻击资源为攻击中断线路总数；线路 (i,j) 的中断状态 z_{ij} 为二进制变量，取值为 0 时表示线路 (i,j) 遭受恶意攻击而中断，取值为 1 时表示线路 (i,j) 正常。该约束条件表示电力传输线路中断总数在每个攻击场景 $s\in S$ 下不超过攻击资源 $H_{\mathrm{A}}(s)$；S 表示攻击中断线路总数场景集(即攻击场景集)，其中每个攻击场景 $s\in S$ 均以线路中断数为特征。这意味着攻击者攻击中断线路总数不再是一个固定数值，而是与攻击者所拥有的攻击线路资源相关的一个集合上的概率分布。

2.2.3　下层电力系统运行约束

1）功率平衡约束

$$P_{\mathrm{G},b}(s)+P_{\mathrm{W},b}(s)-\left(P_{\mathrm{D},b}^{\max}-\Delta S_{\mathrm{D},b}(s)\right)=\sum_{j\in L_l(i,\cdot)}F_{ij}(s)-\sum_{j\in L_l(\cdot,i)}F_{ji}(s) \tag{5}$$

式中：$P_{\mathrm{D}d}^{\max}$ 为位于节点 b 的最大负荷需求；$L_l(\cdot,i)$、$L_l(i,\cdot)$分别为连接线路(i,j)输入端 i、输出端 i 的节点集合。

2）线路潮流约束

$$\left(1-\left(1-v_{ij}\right)\left(1-z_{ij}(s)\right)\right)\cdot\left(\theta_i(s)-\theta_j(s)\right)X_{ij}^{-1}=F_{ij}(s) \tag{6}$$

式中：X_l 为线路 l 的电抗；θ_i 和 θ_j 为线路 (i,j) 两端的节点电压相角。

3）线路潮流容量约束

$$-F_{ij}^{\max}\le F_{ij}(s)\le F_{ij}^{\max} \tag{7}$$

式中：$F_{ij}^{\max}$ 为线路 (i,j) 的最大线路潮流。

4）切负荷容量约束

$$0\le\Delta S_{\mathrm{D},b}(s)\le P_{\mathrm{D},b}^{\max} \tag{8}$$

5）节点相角容量约束

$$-\theta_b^{\max}\le\theta_b(s)\le\theta_b^{\max} \tag{9}$$

式中：$\theta_b^{\max}$ 为节点 b 的最大电压相角。

6）机组出力约束

$$0\le P_{\mathrm{G},b}(s)\le P_{\mathrm{G},b}^{\max} \tag{10}$$

式中：$P_{\mathrm{G},b}^{\max}$ 为位于节点 b 的机组最大有功出力。

7）其他约束条件

$$\forall(i,j)\in L,\forall b\in B,\forall s\in S \tag{11}$$

3　求解方法

本文采用文献[24]中的 C&CG 算法对所提模型进行求解。基于 C&CG 算法原理，本章将原问题分解为主问题和双层 max-min 子问题，然后对主、子问题进行交替求解得到原问题的最优解，即电力系统防御策略。

3.1　子问题

基于防御策略 $\hat{v}_{ij}$ 求解子问题可以确定恶劣的攻击场景，子问题的具体数学模型描述如式(12)所示，计算了电力系统在攻击中断线路总数场景集 S 下的系统运行期望总成本 η。

$$\eta=\sum_{s\in S}\left(\Omega(s)\tau(s)\right) \tag{12}$$

式中：$\tau(s)$ 为电力系统在攻击场景 s 下的最大运行成本。基于每个攻击场景所对应的防御策略，攻击者将最大化电力系统运行成本。基于攻击场景 s，子问题可以描述为如式(13)所示的双层 max-min 模型。

$$\max_{z_{ij}(s)\in Z,P_{\mathrm{W},b}(s)\in W}\tau(s) \tag{13}$$

式(13)的约束条件为式(3)—式(4)，其中：

$$\tau(s)=\min_{\substack{P_{\mathrm{G},b}(s),F_{ij}(s),\\ \theta_b(s),\Delta S_{\mathrm{D},b}(s)}}\sum_{b\in B}\left(I_{\mathrm{G},b}P_{\mathrm{G},b}(s)+I_{\mathrm{D},b}\Delta S_{\mathrm{D},b}(s)\right) \tag{14}$$

式(14)的约束条件为：

$$\begin{aligned}&P_{\mathrm{G},b}(s)+P_{\mathrm{W},b}(s)+\sum_{j\in L_l(\cdot,i)}F_{ji}(s)-\sum_{j\in L_l(i,\cdot)}F_{ij}(s)=\\ &P_{\mathrm{D},b}^{\max}-\Delta S_{\mathrm{D},b}(s)\qquad\qquad\left(\beta_b(s)\right)\end{aligned} \tag{15}$$

$$\left(1-\left(1-\hat{v}_{ij}\right)\left(1-z_{ij}(s)\right)\right)\left(\theta_i(s)-\theta_j(s)\right)X_{ij}^{-1}=F_{ij}(s)\qquad\left(\pi_{ij}(s)\right) \tag{16}$$

$$0 \le P_{\mathrm{G},b}(s) \le P_{\mathrm{G},b}^{\max} \quad \left(\delta_b(s)\right) \tag{17}$$

$$0 \le \Delta S_{\mathrm{D},b}(s) \le P_{\mathrm{D},b}^{\max} \quad \left(\zeta_b(s)\right) \tag{18}$$

$$-F_{ij}^{\max} \le F_{ij}(s) \le F_{ij}^{\max} \quad \left(\underline{\omega}_{ij}(s), \overline{\omega}_{ij}(s)\right) \tag{19}$$

式中：$\beta_b(s)$、$\pi_{ij}(s)$、$\delta_b(s)$、$\zeta_b(s)$、$\underline{\omega}_{ij}(s)$和$\overline{\omega}_{ij}(s)$分别为子问题约束条件式(15)—式(19)在攻击场景s中所对应的对偶变量。

子问题是 max-min 问题，难以直接求解，需要采用最恶劣场景辨别法将其转换为单层 max 优化模型进行求解。基于对偶理论，可以将攻击场景s下的 max-min 问题对偶转化为单层的 max 问题。为简洁起见省略了攻击场景符号s，对偶转化合并后的 max 问题如式(20)—式(26)所示。其中，式(20)为对偶变换后的子问题目标函数；式(3)—式(4)为攻击资源约束；式(21)为节点电压相位角θ_b的对偶变换约束；式(22)为线路潮流F_{ij}的对偶变换约束；式(23)为机组出力$P_{\mathrm{G},b}$的对偶变换约束；式(24)为切负荷量$\Delta S_{\mathrm{D},b}$的对偶变换约束；式(25)为对偶变量的约束条件。

$$\tau = \max \begin{pmatrix} \sum_{(i,j)\in L} \left(\overline{\omega}_{ij} - \underline{\omega}_{ij}\right) F_{ij}^{\max} - \sum_{b\in B} \beta_b P_{\mathrm{W},b} + \\ \sum_{b\in B} \left(\delta_b P_{\mathrm{G},b}^{\max} + \left(\zeta_b + \beta_b\right) P_{\mathrm{D},b}^{\max}\right) \end{pmatrix} \tag{20}$$

约束条件为式(3)—式(4)及如下表达式：

$$\begin{aligned} &\sum_{(i,j)\in L(\cdot,i)} \left(1-\hat{v}_{ij}\right) X_{ij}^{-1} \cdot z_{ij}\pi_{ij} + \sum_{(i,j)\in L(\cdot,i)} \left(\hat{v}_{ij} X_{ij}^{-1} \pi_{ij}\right) - \\ &\sum_{(i,j)\in L(i,\cdot)} \left(1-\hat{v}_{ij}\right) X_{ij}^{-1} \cdot z_{ij}\pi_{ij} - \sum_{(i,j)\in L(i,\cdot)} \left(\hat{v}_{ij} X_{ij}^{-1} \pi_{ij,t}\right) = 0 \end{aligned} \tag{21}$$

$$-\beta_i + \beta_j + \pi_{ij} + \overline{\omega}_{ij} + \underline{\omega}_{ij} = 0 \tag{22}$$

$$\beta_b + \delta_b \le I_{\mathrm{G},b} \tag{23}$$

$$\beta_b + \zeta_b \le I_{\mathrm{D},b} \tag{24}$$

$$\delta_b \le 0, \zeta_b \le 0, \overline{\omega}_{ij} \le 0, \underline{\omega}_{ij} \ge 0 \tag{25}$$

$$\forall (i,j) \in L, \forall b \in B \tag{26}$$

3.2 主问题

基于 C&CG 求解算法理论，将切割约束集添加到原问题约束中可以获取主问题，主问题的目标函数如式(27)所示。

$$\partial = \min_{v_{ij}\in V} \sum_{(i,j)\in L} I_{\mathrm{L},ij} v_{ij} + \Psi \tag{27}$$

约束条件为：

$$\sum_{(i,j)\in L} v_{ij} \le V_{\mathrm{L}}, \quad \forall v_{ij} \in \{0,1\} \tag{28}$$

$$\Psi \ge \sum_{s\in S} \left(\Omega(s) \sum_{b\in B} \left(I_{\mathrm{G},b} P_{\mathrm{G},b}(s) + I_{\mathrm{D},b} \Delta S_{\mathrm{D},b}(s)\right)\right) \tag{29}$$

$$-\left(1-\hat{z}_{ij,k}(s)\right)\left(1-v_{ij}\right)M \le X_{ij}F_{ij,k}(s) - \left(\theta_{i,k}(s) - \theta_{j,k}(s)\right) \tag{30}$$

$$X_{ij}F_{ij,k}(s) - \left(\theta_{i,k}(s) - \theta_{j,k}(s)\right) \le \left(1-\hat{z}_{ij,k}(s)\right)\left(1-v_{ij}\right)M \tag{31}$$

$$0 \le \Delta S_{\mathrm{D},b,k}(s) \le P_{\mathrm{D},b}^{\max} \tag{32}$$

$$\begin{aligned} &P_{\mathrm{G},b,k}(s) + \hat{P}_{\mathrm{W},b,k}(s) - \left(P_{\mathrm{D},b}^{\max} - \Delta S_{\mathrm{D},b,k}(s)\right) = \\ &\sum_{j\in L_i(i,\cdot)} F_{ij,k}(s) - \sum_{j\in L_i(\cdot,i)} F_{ji,k}(s) \end{aligned} \tag{33}$$

$$-\theta_b^{\max} \le \theta_{b,k}(s) \le \theta_b^{\max} \tag{34}$$

$$0 \le P_{\mathrm{G},b,k}(s) \le P_{\mathrm{G},b}^{\max} \tag{35}$$

$$-\left(\hat{z}_{ij,k}(s) F_{ij}^{\max} + \left(1-\hat{z}_{ij,k}(s)\right) v_{ij} F_{ij}^{\max}\right) \le F_{ij,k}(s) \tag{36}$$

$$F_{ij,k}(s) \le \hat{z}_{ij,k}(s) F_{ij}^{\max} + \left(1-\hat{z}_{ij,k}(s)\right) v_{ij} F_{ij}^{\max} \tag{37}$$

$$\forall (i,j) \in L, \forall b \in B, \forall s \in S, \forall k \tag{38}$$

需要注意的是，子问题所含有的双线性约束可以转化为线性约束条件[25]。最后，本文所提的防御模型最终解耦为混合整数线性形式的主问题和子问题，然后采用 C&CG 算法进行求解。其中，C&CG 算法求解本文模型的具体步骤可以描述为：

1）初始化下界$L_{\mathrm{B}} = -\infty$、上界$U_{\mathrm{B}} = +\infty$和当前迭代次数 k=0；设定算法的收敛阈值$\varepsilon = 1\%$；给定一组攻击策略Z和风电出力场景集W作为初始的极端场景。

2）基于攻击策略 Z 和风电出力场景集 W 求解主问题以确定最优防御策略和主问题目标函数值∂，并更新下界$L_{\mathrm{B}} = \partial$。

3）求解子问题有 2 个子步骤：①基于防御策略$\hat{v}_{ij}$求解子问题以确定“最恶劣”的组合场景(即风电出力场景$\hat{P}_{\mathrm{W},k}(s)$和攻击场景$\hat{z}_k(s)$)和子问题目标函数值$\tau(s)$，场景集 S 中的每个场景s都要执行子步骤①)；②更新线路中断策略集$Z = Z \bigcup \hat{z}_k(s)$、风电出力场景集$W = W \bigcup \hat{P}_{\mathrm{W},k}(s)$和上界$U_{\mathrm{B}} = \min\left(U_{\mathrm{B}}, \eta + \sum_{(i,j)\in \boldsymbol{L}} C_{\mathrm{L},ij}\hat{v}_{ij}\right)$。

4）如果$|U_{\mathrm{B}} - L_{\mathrm{B}}|/L_{\mathrm{B}} \le \varepsilon$，则停止迭代并输出最优解，即最佳防御策略；否则，更新迭代次数 k=k+1 并跳转到步骤 2）运行，直至算法收敛。

4 算例分析

为了验证所提模型和算法的有效性，本文在 IEEE RTS-79 和 IEEE RTS-96 测试系统上进行仿真验证[26]。本文设定切负荷成本为 150 元/MW，线路加固成本为 400 元/条。假设风电出力的最大偏差为 20%[27]。本文利用 Matlab2014a 实现上述程序，并调用求解器 Cplex12.4 进行求解，测试系统的硬件环境为 Intel Xeon 6138 CPU 处理器，主频为 2.0 GHZ，内存为 64 GB。

4.1　IEEE RTS-79 测试系统计算结果分析

为了验证本文所提方法的有效性，本节采用 IEEE RTS-79 测试系统为例进行仿真分析。该系统含有 12 台机组、17 个负荷节点和 36 条输电线路，总负荷水平修订为 2 400 MW，具体数据可以参考文献[26]。本文假设共有 6 个风电场，其所在位置如图附录 A 附图 A1 所示，装机容量均为 200 MW。其中，风电场总装机容量占总负荷的 50%。

4.1.1　不确定性因素的影响分析

本文提出一种考虑风电出力不确定性并以不确定性恶意攻击(即攻击资源不确定)为导向的防御-攻击-防御模型，以增强电力系统的防御能力。本节将从 2 个角度来分析验证所提模型的有效性：角度 1，分析风电出力不确定性对电力系统的影响；角度 2，分析攻击资源不确定性对电力系统的影响。

角度 1：为了研究风电出力不确定度参数Γ对电力系统的影响，本节设定不确定性参数Γ的取值范围为[0, 5]。表 1 给出在攻击场景集$S=\{3,5\}$且对应攻击场景概率为{0.6, 0.4}下的实验仿真结果，以验证所提方法的有效性。

当线路加固资源$V_{\mathrm{L}}=4$时，电力系统在不同不确定性参数Γ下的防御策略和每个攻击场景下的运行成本以及总期望成本如表 1 所示。电力系统在不同的不确定性参数Γ和线路加固资源下的总期望成本如附录 A 表 A1 所示。根据表 1 和附录表 A1 可知，电力系统运行成本和总期望成本随着不确定性参数Γ的增大而增加。这是因为，风电出力不确定性预算的增大会导致所构建的风电出力不确定性集含有更多的不确定性参数，即风电出力极端场景增加，从而导致电力系统总成本增加。此外，根据表 1 可知，当不确定性参数Γ取值为{1, 4, 5}时，电力系统防御策略保持不变，均为{1, 9, 31, 38}。这意味着，风电出力不确定性对电力系统防御策略影响相对较小，防御者可以通过合理地调整风电出力不确定性集的区间大小从而有效地调控电力系统安全经济运行风险程度，这给实际应用中的模型参数选择提供了指导。根据附附录表 A1 可知，电力系统期望总成本随着线路加固资源V_{L}的增大而减少，这给电力系统运行人员减缓系统运行成本提供了有效的指导。与此同时，表 1 和附表 A1 给出了基于鲁棒优化模型[28]所制定的防御策略下的电力系统总成本。可以发现，基于鲁棒优化模型下的电力系统总成本高于本文提出的自适应鲁棒防御模型下的电力系统总成本。这是因为，基于鲁棒优化模型仅简单地考虑了在最极端情况下制定线路加固策略。虽然，在不同的不确定度参数Γ下具有不同的系统总成本，但在不同的风电出力不确定性参数Γ下的电力系统总期望成本均低于鲁棒防御模型[28]下的电力系统总成本。

表 1　不同不确定度参数Γ下的仿真结果

Table 1　Simulation results under different uncertainty parameter Γ

Γ	V_{L}=4 防御策略	电力系统运行成本/(元·h^{-1})		总期望成本/(元·h^{-1})
		H_{A}=3	H_{A}=5	
0	2, 9, 26, 30	53 942.20	76 423.60	64 534.76
1	1, 9, 31, 38	54 296.50	76 777.91	64 889.07
2	2, 9, 30, 32	54 616.12	77 097.53	65 208.68
3	1, 9, 25, 30	54 898.57	77 379.98	65 491.14
4	1, 9, 31, 38	55 168.64	77 650.05	65 761.20
5	1, 9, 31, 38	55 413.93	77 895.33	66 006.49
文献[28]	1, 9, 26, 30	55 624.53	78 105.93	66 217.09

角度 2：假设攻击场景集$S=\{2,4\}$以及对应的场景概率为{0.7, 0.3}。当线路加固资源$V_{\mathrm{L}}=3$时，电力系统在基于角度 2 下的防御策略和在每个攻击场景下的运行成本以及总期望成本如表 2 所示。可以发现，电力系统在防御策略为{1, 9, 28}时，总期望成本为 47 757.52 元/h。本文提出的不确定性恶意攻击下的防御-攻击-防御模型，虽然在某些单一攻击场景下的电力系统总成本可能不是最小的，但在多个攻击场景下系统总期望成本最小。虽然，基于传统防御-攻击-防御模型可以在单一极端场景下制定最优的防御策略，但其制定的决策方案过于保守且无法调整策略的保守程度。根据附表 A2 可知，在本文所提防御模型确定的防御策略下，电力系统总期望成本为 47 757.52 元/h；然而基于文献[28]所构建的防御模型是在“最恶劣”的风电出力场景集下考虑攻击场景不确定性问题，以确定最佳线路加固策略，其电力系统总期望成本为 48 483.49 元/h；基于文献[11]和文献[28]所构建的防御模型是仅考虑单一“最恶劣”的组合场景，其系统总成本为 60 116.44 元/h。这是因为，基于文献[28]所构建的防御模型是在单一极端风电出力场景下制定线路加固策略；基于文献[11]和文献[28]所构建的防御模型是在单一“最恶劣”组合场景下制定的防御策略，因此具有一定的保守性。本文提出的防御模型适用于在不

确定性恶意攻击场景下制定最佳防御策略，可以有效地调整防御策略的保守程度。其中，基于本文模型所确定的最佳防御策略和攻击策略如附图 A1 所示。

4.1.2 线路加固资源的影响分析

在风电出力不确定度参数 $\Gamma=4$ 和攻击场景集 $S=\{3,4,5\}$ 以及相应概率为(0.2, 0.5, 0.3)的组合场景下，图 2 给出不同线路加固资源 V_{L} 对电力系统总成本的影响。根据图 2 可知，电力系统期望总成本随着线路加固资源 V_{L} 的增大而减少。此外，在不同的不确定度参数 Γ 下，系统具有不同的总期望成本。这表明，防御者可以通过调节风电出力不确定性集的区间大小来调控韧性，以增强策略的保守程度，这给实际应用中的模型参数选择提供了明确指导。此外，表 3 给出了在不同线路加固资源 V_{L} 下的电力系统防御策略，即为线路加固方案。可以看出，随着线路加固资源 V_{L} 的增加，极端事件所导致的中断线路将会被加固。例如，当线路加固资源 $V_{\mathrm{L}}=4$ 时，线路 36 被中断；然而 $V_{\mathrm{L}}=5$ 时，线路 36 将会被加固。因此，当线路加固资源 V_{L} 较大时，电力系统期望总成本相对较低。

4.1.3 不同攻击场景概率的影响分析

为了研究攻击场景概率对电力系统运行的影响，假设攻击场景集 S={3, 4}以及线路加固资源 V_{L}=4 的情况下，电力系统在攻击场景概率从(0.1, 0.9)到(0.9, 0.1)变化及风电出力不确定度参数 Γ 从 0 到 5 变化下的电力系统总期望成本如附表 B3 所示。其中，风电出力不确定度参数 Γ 为 0 表示风电出力实际值为预测值。可以看出，当风电出力不确定性参数 Γ 越大时，电力系统的总期望成本就越高；不同攻击情景概率可以诱导出不同的电力系统总期望成本。当风电出力不确定性参数 Γ 一定时，电力系统总期望成本随着攻击场景集 S={3, 4}中攻击场景 H_{A}=3 的概率增大而减少，随着 H_{A}=4 的概率减少而减少。例如，当风电出力不确定度参数 Γ 为 3 时，电力系统在攻击场景概率为(0.3, 0.7)下的总期望成本为 55 191.65 元/h，在攻击场景概率为(0.7, 0.3)下的总期望成本为 50 204.36 元/h。这是因为，考虑攻击场景 H_{A}=3 的概率越大则相应攻击场景 H_{A}=4 的概率越小，电力系统安全部门防御人员制定的策略就越发激进，以至于电力系统总期望成本越低，这有助于防御者灵活地调整电力系统防御策略和调度策略。

表 2 基于恶意攻击不确定性的仿真结果(V_{L}=3; $\Gamma=3$)

Table 2 Simulation results based on malicious attack uncertainty(V_{L}=3; $\Gamma=3$)

参数	H_{A}=2	H_{A}=4
攻击策略	19, 23	11, 29, 36, 37
系统运行成本/(元·h^{-1})	41 571.97	58 190.49
总期望成本/(元·h^{-1})	47 757.52=3×400+41 571.97×0.7+58 190.49×0.3	
线路加固策略	1, 9, 28	

表 3 不同线路加固资源下的仿真结果

Table 3 Simulation results under different line hardening resources

V_{L}	防御策略	H_{A}=3	H_{A}=4	H_{A}=5
4	1, 9, 25, 30	29, 36, 37	11, 29, 36, 37	19, 23, 29, 36, 37
5	2, 9, 31,36,38	11,19,23	5,10,19,23	15,17,18,23,27
6	1,9,23,28,33,36	11,12,13	4,5,8,10	5,10,11,12,13
7	2,5,9,23,28,29,33	11,12,13	11,12,13,36	7,14,16,20,21
8	2,5,9,11,23,28,29,33	4,8,12	7,19,21,22	7,18,19,20,21

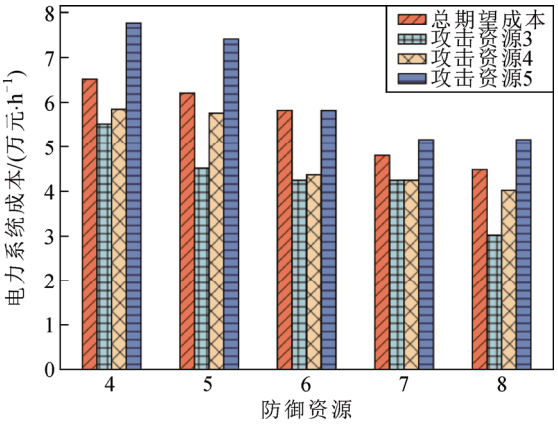


图 2 不同线路加固资源下的电力系统成本

Fig.2 Power system cost under different line hardening resources

为了进一步分析攻击场景概率对防御策略的影响，在线路加固资源 V_{L}=3 的场景下，当攻击场景集 S={3, 5}时，攻击场景概率从(0.1, 0.9)到(0.9, 0.1)变化时，电力系统所对应的防御策略、攻击策略和总期望成本如表 4 所示。可以发现，不同的攻击场景概率可能会诱导出不同的防御策略和攻击策略。在某些情况下，防御策略对攻击场景概率很敏感，攻击场景概率微小的变化可能会导致防御者制定不同的防御策略。例如，当攻击场景概率为(0.2, 0.8)时，防御策略为{1, 9, 28}；然而在攻击场景概率为(0.3, 0.7)时，防御策略为{2, 9, 28}。不过，在其他情况下，防御策略并不受攻击场景概率的影响。

例如，攻击场景概率从(0.4, 0.6)到(0.9, 0.1)变化时，防御策略并未发生变化。这表明，基于本文模型所制定的防御策略受攻击场景概率误差估计的影响较小，具有良好的鲁棒性和普适性。

4.2　IEEE RTS-96 测试系统计算结果分析

为了测试所提模型的有效性，本节采用的 IEEE RTS-96 测试系统共有 36 台发电机，51 个负荷节点及 120 条线路，其总负荷水平为 8 550 MW。本文假设共有 6 个风电场，分别接在系统 1，17，33，49，65，73 节点上，其装机容量均为 600 MW，风电场总装机容量占总负荷的 40%以上。

当在不确定度参数 Γ=3 和攻击场景集 $S=\{2,3\}$ 以及相应攻击场景概率为 (0.6,0.4) 的组合下，电力系统在线路加固资源 $V_{\mathrm{L}}=4$ 场景下的防御策略、期望总成本和求解时间如表 5 所示。可以发现，电力系统防御策略为{32, 41, 82, 109}，总期望成本为 144 083.32 元/h。此外，电力系统基于不同防御模型下的防御策略和电力系统总成本如附表 B4 所示，相比基于文献[28]所构建的防御模型和基于文献[11]和文献[28]所构建的防御模型下的线路加固策略，本文所提模型的防御策略可以使得电力系统总成本最低。与此同时，针对最大的可靠性 IEEE RTS-96 测试系统而言，求解时间仅为 160.12 s (即计算时间为 2.67 min，不足 5 min)。此外，C&CG 算法求解模型的迭代过程如附图 A2 所示，仅需 5 次迭代即可收敛。综上所述，本文采用 C&CG 算法可以快速求解本文所提模型并确定最佳的线路加固策略。

在攻击场景集 $S=\{2,4\}$ 以及概率为(0.6, 0.4)的场景下，当不确定度参数 $\Gamma=3/5$ 时，电力系统在不同线路加固资源下的防御策略如附表 A5 所示。可以发现，不确定度参数 Γ 可以使防御者制定不同的防御策略。例如，当线路加固资源 $V_{\mathrm{L}}=6$ 时，在不确定度参数 $\Gamma=3$ 场景下，电力系统的最佳防御策略为{25, 30, 41, 83, 104, 109}；在不确定度参数 $\Gamma=5$ 场景下，防御策略为{25, 30, 83, 104, 111, 120}。此外，附表 A5 呈现出一个有趣的现象：当不确定度参数 $\Gamma=3$ 且线路加固资源 $V_{\mathrm{L}}=8$ 时，加固线路的总数并不会随线路加固资源 B_{L} 的增加而增加，实际加固线路的总数为 7。这是因为，切负荷的边际成本低于加固线路的边际成本。综上所述，本文提出的防御模型可以有效地指导防御人员制定事前防御策略，用以应对风电出力和恶意攻击不确定性等因素对电力系统安全运行的影响。

表 4　不同攻击场景概率下的仿真结果

Table 4　Simulation results under different probability of attack scenarios

场景概率	防御策略	H_{A}=3	H_{A}=5	总期望成本(元·h^{-1})
(0.1,0.9)	1,9,28	29,36,37	11,29,36,37	59 061.29
(0.2,0.8)	1,9,28	29,36,37	11,29,36,37	58 732.11
(0.3,0.7)	2,9,28	29,36,37	11,29,36,37	58 402.91
(0.4,0.6)	1,9,28	29,36,37	5,10,19,23	57 558.71
(0.5,0.5)	1,9,28	29,36,37	5,10,19,23	57 315.35
(0.6,0.4)	1,9,28	29,36,37	11,29,36,37	57 415.34
(0.7,0.3)	1,9,28	29,36,37	11,29,36,37	57 086.15
(0.8,0.2)	1,9,28	29,36,37	11,29,36,37	56 756.96
(0.9,0.1)	1,9,28	29,36,37	11,29,36,37	56 427.77

表 5　IEEE RTS-96 系统中不确定性恶意攻击的仿真结果 (V_{L}=4; Γ=3)

Table 5　Simulation results for malicious attack uncertainty in IEEE RTS-96 system (V_{L}=4; Γ=3)

参数	H_{A}=2	H_{A}=3
攻击策略	20,25	31,38,39
电力系统运行成本/(元·h^{-1})	137 591.75	149 820.68
总期望成本/(元·h^{-1})	144 083.32=4×400+137 591.75×0.6+149 820.68×0.4	
线路加固策略	32,41,82,109	
求解时间/s	160.12	

本节在攻击场景集 $S=\{2,3\}$ 以及相应概率为(0.7, 0.3)场景下，设定线路加固资源 V_{L} 的取值区间为[4, 8]，不确定度参数 Γ 的取值区间为[0, 5]，电力系统在不同线路加固资源 V_{L} 和不确定度参数 Γ 组合下的总期望成本如附图 A3 所示。可以发现，电力系统总期望成本随着不确定度参数 Γ 的增大而增大。这是因为不确定度参数 Γ 的增大会导致所构建的风电出力不确定性集含有更多的不确定性参数，即风电出力的极端场景增加，从而导致电力系统总成本增加。当风电出力不确定性预算 Γ 一定时，随着线路加固资源 V_{L} 的增大，电力系统运行总期望成本整体呈现出下降趋势。不过，可以发现线路加固资源在一定范围内取值时，电力系统期望总成本保持不变，即没有随线路加固资源 V_{L} 的增加而持续增加。这表明在一定范围内，实际加固线路的总数保持不变，有利于防御人员制定合理的线路加固策略。

5 结论

为了提升风电等高比例可再生能源电力系统应对不确定性恶意攻击的能力，本文建立了更符合实际情况的电力系统防御模型。仿真结果分析表明：

1）建立的多面体不确定性集合，可以灵活地调整电力系统防御策略的保守性，协助防御人员在系统成本和运行风险之间进行选择。

2）较传统防御模型而言，本文所提模型可以协助防御人员在最恶劣场景下制定电力系统总期望成本最小的防御策略。

3）仿真结果表明，所提模型指导防御人员制定的防御策略可以有效地减缓风电出力和恶意攻击不确定性等因素对电力系统的影响，具有较好的鲁棒性。

综上，本文所提出的考虑风电波动和不确定性恶意攻击的防御-攻击-防御模型，能够有效地将不确定性因素考虑到电力系统防御策略制定的过程中去，为电力系统安全人员制定更合理的防御策略提供了新的方法和思路。

附录见本刊网络版(http://hve.epri.sgcc.com.cn)。

参考文献 References

[1] 张文亮，于永清，宿志一，等. 湖南电网 2008 年冰雪灾害调研分析[J]. 电网技术，2008，32(8)：1-5.
ZHANG Wenliang, YU Yongqing, SU Zhiyi, et al. Investigation and analysis of icing and snowing disaster happened in Hunan power grid in 2008[J]. Power System Technology, 2008, 32(8): 1-5.

[2] 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.

[3] 寇 岩，刘宇明，郭 亮. 美国得州“2.15 停电”事件分析及对山东电力市场的启示[J]. 山东电力技术，2021，48(11)：15-20，28.
KOU Yan, LIU Yuming, GUO Liang. Analysis of the “2.15 power outage” in Texas, USA and its enlightenment to Shandong electric power retail market[J]. Shandong Electric Power, 2021, 48(11): 15-20, 28.

[4] TAN Y, LI Y, CAO Y J, et al. Cyber-attack on overloading multiple lines: a bilevel mixed-integer linear programming model[J]. IEEE Transactions on Smart Grid, 2018, 9(2): 1534-1536.

[5] CHE L, LIU X, LI Z Y, et al. False data injection attacks induced sequential outages in power systems[J]. IEEE Transactions on Power Systems, 2019, 34(2): 1513-1523.

[6] LIU X, LI Z Y, LIU X D, et al. Masking transmission line outages via false data injection attacks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(7): 1592-1602.

[7] SAYYADIPOUR S, YOUSEFI G R, LATIFY M A. Mid-term vulnerability analysis of power systems under intentional attacks[J]. IET Generation, Transmission & Distribution, 2016, 10(15): 3745-3755.

[8] 韦晓广，高仕斌，李 多，等. 基于连锁故障网络图和不同攻击方式的输电线路脆弱性分析[J]. 中国电机工程学报，2018，38(2)：465-474.
WEI Xiaoguang, GAO Shibin, LI Duo, et al. Cascading fault graph for the analysis of transmission network vulnerability under different attacks[J]. Proceedings of the CSEE, 2018, 38(2): 465-474.

[9] 阳育德，蓝水岚，覃智君，等. 电力信息物理融合系统的网络-物理协同攻击[J]. 电力自动化设备，2020，40(2)：97-102.
YANG Yude, LAN Shuilan, QIN Zhijun, et al. Coordinated cyber-physical attacks of cyber-physical power system[J]. Electric Power Automation Equipment, 2020, 40(2): 97-102.

[10] 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.

[11] 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.

[12] 黄格超，李更丰，肖 遥，等. 综合考虑自然灾害与人为攻击的电-气互联系统优化配置方法[J]. 电网技术，2021，45(3)，959-969.
HUANG Gechao, LI Gengfeng, XIAO Yao, et al. Optimal placement for integrated electricity and gas energy system considering natural disasters and man-made attacks[J]. Power System Technology, 2021, 45(3): 959-969.

[13] 李明昊，杨祺铭，李更丰，等. 台风场景下基于多种分布式资源协同的弹性配电网两阶段供电恢复策略[J]. 高电压技术，2024，50(1)：93-104.
LI Minghao, YANG Qiming, LI Gengfeng, et al. Two-stage power supply restoration strategy of resilient distribution network based on coordination of multiple distributed resources in typhoon scenario[J]. High Voltage Engineering, 2024, 50(1): 93-104.

[14] 张亚超，易 杨，胡志鹏，等. 基于分布鲁棒优化的电-气综合能源系统弹性提升策略[J]. 电力系统自动化，2021，45(13)：76-84.
ZHANG Yachao, YI Yang, HU Zhipeng, et al. Resilience enhancement strategy of electricity-gas integrated energy system based on distributionally robust optimization[J]. Automation of Electric Power Systems, 2021, 45(13): 76-84.

[15] 王 丹，赵 平，臧宁宁，等. 基于安全博弈的综合能源系统安全性分析及防御策略[J]. 电力自动化设备，2019，39(10)：10-16.
WANG Dan, ZHAO Ping, ZANG Ningning, et al. Security analysis and defense strategy of integrated energy system based on security game[J]. Electric Power Automation Equipment, 2019, 39(10): 10-16.

[16] 刘天浩，朱元振，孙润稼，等. 极端自然灾害下电力信息物理系统韧性增强策略[J]. 电力系统自动化，2021，45(3)：40-48.
LIU Tianhao, ZHU Yuanzhen, SUN Runjia, et al. Resilience-enhanced strategy for cyber-physical power system under extreme natural disasters[J]. Automation of Electric Power Systems, 2021, 45(3): 40-48.

[17] HE C, DAI C X, WU L, et al. Robust network hardening strategy for enhancing resilience of integrated electricity and natural gas distribution systems against natural disasters[J]. IEEE Transactions on Power Systems, 2018, 33(5): 5787-5798.

[18] 林 佳，陈 浩，寇伟宏，等. 极端天气下保底电网骨干网架优化及弹性提升方法[J]. 高电压技术，2023，49(4)：1591-1599.
LIN Jia, CHEN Hao, KOU Weihong, et al. Optimization and resilience enhancement method of core backbone network framework under extreme weather[J]. High Voltage Engineering, 2023, 49(4): 1591-1599.

[19] WANG C, WEI W, WANG J H, et al. Robust defense strategy for gas-electric systems against malicious attacks[J]. IEEE Transactions

on Power Systems, 2017, 32(4): 2953-2965.

[20] 韩肖清，李廷钧，张东霞，等. 双碳目标下的新型电力系统规划新问题及关键技术[J]. 高电压技术，2021，47(9)：3036-3046.
HAN Xiaoqing, LI Tingjun, ZHANG Dongxia, et al. New issues and key technologies of new power system planning under double carbon goals[J]. High Voltage Engineering, 2021, 47(9): 3036-3046.

[21] 朱琼锋，李家腾，乔　骥，等. 人工智能技术在新能源功率预测的应用及展望[J]. 中国电机工程学报，2023，43(8)：3027-3048.
ZHU Qiongfeng, LI Jiateng, QIAO Ji, et al. Application and prospect of artificial intelligence technology in renewable energy forecasting[J]. Proceedings of the CSEE, 2023, 43(8): 3027-3048.

[22] 杨祺铭，李更丰，别朝红，等. 计及间歇性新能源的弹性城市电网输配电协同供电恢复方法[J]. 高电压技术，2023，49(7)：2764-2774.
YANG Qiming, LI Gengfeng, BIE Zhaohong, et al. Coordinated power supply restoration method of resilient urban transmission and distribution networks considering intermittent new energy[J]. High Voltage Engineering, 2023, 49(7): 2764-2774.

[23] 李雨佳，殷文倩，龙覃飞，等. 多元不确定性环境下含海量资源电力系统的弹性提升技术[J]. 高电压技术，2022，48(9)：3484-3496.
LI Yujia, YIN Wenqian, LONG Qinfei, et al. Review on resilience enhancement strategies for power systems with massive resources under multi-source uncertainties[J]. High Voltage Engineering, 2022, 48(9): 3484-3496.

[24] ZENG B, ZHAO L. Solving two-stage robust optimization problems using a column-and-constraint generation method[J]. Operations Research Letters, 2013, 41(5): 457-461.

[25] 李　珂，邵成成，王雅楠，等. 考虑电-气-交通耦合的城市综合能源系统规划[J]. 中国电机工程学报，2023，43(6)：2263-2273.
LI Ke, SHAO Chengcheng, WANG Yanan. Optimal planning of urban integrated energy systems considering electricity-gas-transportation interactions[J]. Proceedings of the CSEE, 2023, 43(6): 2263-2273.

[26] GRIGG C, WONG P, ALBRECHT P, et al. The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee[J]. IEEE Transactions on Power Systems, 1999, 14(3): 1010-1020.

[27] FOLEY A M, LEAHY P G, MARVUGLIA A, et al. Current methods and advances in forecasting of wind power generation[J]. Renewable Energy, 2012, 37(1): 1-8.

[28] YE H X, WANG J H, GE Y Y, et al. Robust integration of high-level dispatchable renewables in power system operation[J]. IEEE Transactions on Sustainable Energy, 2017, 8(2): 826-835.



王　峰
1990—，男，博士，高工
主要研究方向为配电自动化、电力系统稳定与控制等
E-mail: wf_scu@@163.com

WANG Feng
Ph.D.
Senior engineer



杜　敏(通信作者)
1994—，男，博士
主要研究方向为网络安全、电力系统韧性提升和新能源经济调度
E-mail: dumin94@hnu.edu.cn

DU Min
Ph.D.
Corresponding author

收稿日期　2023-06-10　修回日期　2023-11-13　　编辑　何秋萍

附录 A

表 A1　不同不确定度参数 Γ 的电力系统运行总期望成本

Table A1　Total expected costs of power system operation under different uncertainty parameter Γ

Γ	B_L=4	B_L=5	B_L=6	B_L=7	B_L=8
0	63 932.58	58 086.45	48 984.01	46 259.09	39 051.30
1	64 286.88	59 328.33	49 338.31	46 969.10	40 909.97
2	64 606.50	60 696.39	49 657.93	47 288.72	42 761.58
3	64 888.95	61 785.11	49 940.38	47 740.84	44 238.60
4	65 159.02	62 058.89	50 210.44	48 014.62	44 858.29
5	65 404.31	62 311.61	50 455.73	48 267.34	45 129.60
文献[28]	65 614.91	62 522.21	50 666.34	48 477.94	45 340.20

表 A2　基于恶意攻击不确定性的对比结果($\Gamma=3$)

Table A2　Comparison results based on malicious attack uncertainty($\Gamma=3$)

方法	防御策略 B_L=3	电力系统运行成本/(元·h^{-1})		总期望成本/(元·h^{-1})
		B_A=2	B_A=4	
文献[28]	2, 9, 28	42 297.92	58 916.44	48 483.49
		48 483.49=3×400+42 297.92×0.7+58 190.49×0.3		
文献[11]+[28]	1, 9, 28	0	58 916.44	60 116.44
		60 116.44=3×400+58 190.49×1		
本文	1, 9, 28	41 571.97	58 190.49	47 757.52
		47 757.52=3×400+41 571.97×0.7+58 190.49×0.3		

表 A3　不同攻击场景概率下的对比结果

Table A3　Comparison results under different attack scenario probabilities

攻击场景概率	Γ=0	Γ=1	Γ=2	Γ=3	Γ=4	Γ=5	文献[28]
(0.1,0.9)	56 728.91	57 083.23	57 402.85	57 685.30	57 955.36	58 200.66	58 411.25
(0.2,0.8)	55 482.10	55 836.40	56 156.03	56 438.47	56 708.54	56 953.83	57 164.43
(0.3,0.7)	54 235.28	54 589.58	54 909.20	55 191.65	55461.72	55 707.01	55 917.61
(0.4,0.6)	52 988.45	53 342.76	53 662.38	53 944.83	54 214.90	54 460.18	54 670.78
(0.5,0.5)	51 741.63	52 095.93	52 415.55	52 698.01	529 68.07	53 213.36	53 423.96
(0.6,0.4)	50 494.80	50 849.11	51 168.73	51 451.18	51 721.25	51 966.53	52 177.14
(0.7,0.3)	49 247.98	49 602.29	49 921.90	50 204.36	50 474.42	50 719.71	50 930.31
(0.8,0.2)	48 001.16	48 355.46	48 675.08	48 957.53	49 227.60	49 472.89	49 683.49
(0.9,0.1)	46 754.33	47 108.64	47 428.25	47 710.71	47 980.77	48 226.06	48 436.66

表 A4　IEEE RTS-96 系统中不确定性恶意攻击的对比结果

Table A4　Comparison results for malicious attack uncertainty in IEEE RTS-96 system

$\Gamma=3$	防御策略 B_L=4	电力系统运行成本/(元·h^{-1})		总期望成本/(元·h^{-1})
		B_A=2	B_A=3	
文献[28]	30,82,109,120	140700.45	152 929.38	147 192.02
		147 192.02=4×400+140 700.45×0.6+152 929.38×0.4		
文献[11]+[28]	32,82,109,120	0	152 929.38	154 529.38
		154 529.38=4×400+152 929.38×1		
本文	32,41,82,109	137591.75	149 820.68	144 083.32
		144 083.32=4×400+137 591.75×0.6+149 820.68×0.4		

表 A5　不同线路加固资源下的防御策略

Table A5　The defense strategies under different line hardening resources

B_L	$\Gamma=3$	$\Gamma=5$
4	30,82,109,120	30,82,111,120
5	30,83,102,109,120	30,83,104,109,120
6	25,30,41,83,104,109	25,30,83,104,111,120
7	25,32,61,83,104,111,1202	3,25,32,83,104,109,120
8	25,30,41,65,83,104,109	3,25,30,65,83,104,109,120

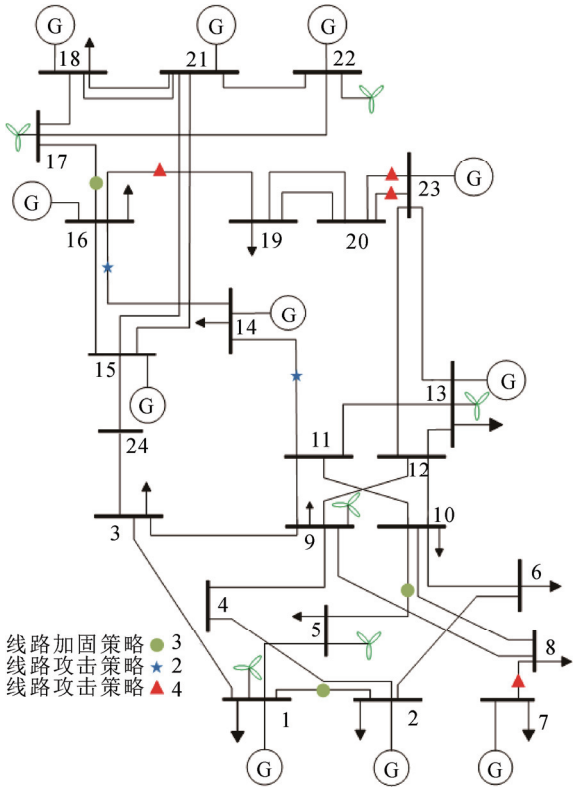


图 A1　不确定性恶意攻击下的防御策略

Fig.A1　Defense strategy under malicious attacks uncertainty

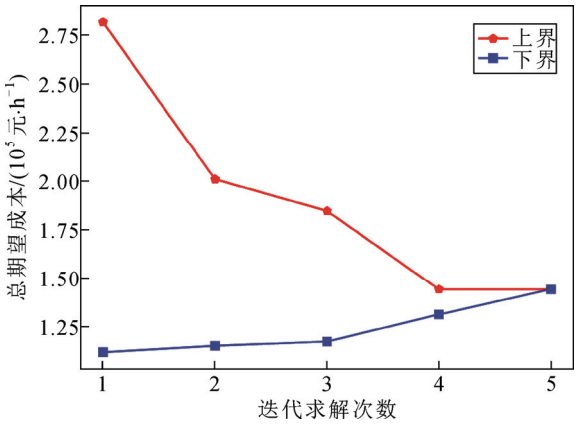


图 A2　C&CG 求解算法收敛示意图

FigA2　Convergence of the C&CG solution methodology

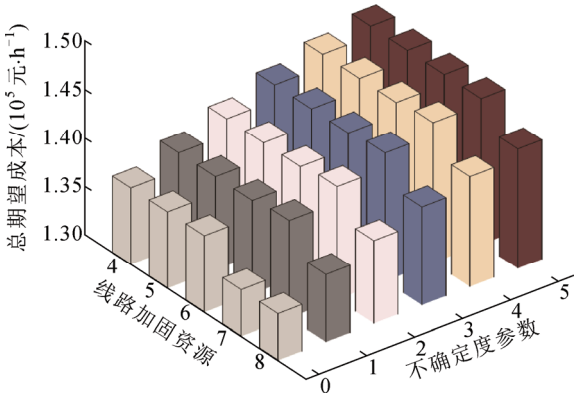


图 A3　不同场景下的总期望成本

Fig.A3　Total expected costs under different scenario