

Decision-Dependent Adversarial Planning for Cyber-Resilient Solar-Rich Power Grids

Yifan Liu

Zhejiang University

Bowen Xu

Zhejiang University

Wenxuan Ma

Zhejiang University

Shiyi Zhao

Zhejiang University

Mengxiang Liu

University of Bristol

Ruilong Deng

dengrui long@zju.edu.cn

Zhejiang University

Peng Cheng

Zhejiang University

Jiming Chen

Zhejiang University

Research Article

Keywords:

Posted Date: October 26th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10917027/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Decision-Dependent Adversarial Planning for Cyber-Resilient Solar-Rich Power Grids

Yifan Liu¹, Bowen Xu¹, Wenxuan Ma¹, Shiyi Zhao¹, Mengxiang Liu², Ruilong Deng^{1*}, Peng Cheng¹, and Jiming Chen¹

¹State Key Laboratory of Industrial Control Technology and College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China

²School of Computer Science, University of Bristol, Bristol, BS8 1UB, UK

*Correspondence: dengruilong@zju.edu.cn

Abstract

The rapid expansion of solar photovoltaic (PV) capacity has exposed the grid to escalating cyber threats that exploit the growing digital footprint of renewable infrastructure. Existing joint planning methods for PV and battery energy storage systems (BESSs) largely optimize techno-economic performance without capturing how deployment decisions reshape cyber threats. Temporal aggregation can obscure seasonal operations and storage-state evolution, while plan-dependent attacks create a costly mixed-integer search. To bridge the gap, we develop a simulation-driven Decision-Dependent Adversarial Bayesian Optimization (DD-ABO) framework that combines hourly full-year simulations preserving seasonal operations and BESS trajectories, candidate-specific adversarial PV-curtailment evaluation, and a random-forest surrogate with expected improvement for sample-efficient PV-BESS planning. Experiments using 2025 New England load and solar data mapped to the IEEE 39-bus system show that approximately half of the selected worst-case attacks begin at the upper neck of the duck curve, and meanwhile the resulting plans exhibit cross-zone and vendor diversification under the modeled dependencies. Relative to attack-agnostic Bayesian optimization, DD-ABO reduces the mean worst-case attack-induced operational penalty and mean expected energy not served within the evaluated scenarios by 80.2% and 85.0%, respectively, with only a marginal increase in base-case operational cost and no statistically significant increase in annualized investment or fixed maintenance costs. These results demonstrate that, in this case study, decision-dependent adversarial planning can improve cyber resilience through deployment structure rather than capital or maintenance over-provisioning.

Introduction

The rapid decline in solar photovoltaic (PV) electricity costs, supported by favorable policies, is reshaping the global energy transition through an unprecedented surge in installed capacity^{1,2}. From 2018 to 2023, the total installed PV capacity tripled, with utility-scale PV accounting for 57% of new additions. Between 2024 and 2030, solar PV is projected to contribute 80% of global renewable capacity growth³. Under the IEA Net Zero by 2050 Scenario, installed solar PV capacity is projected to overtake all other generation technologies, accounting for the largest share of global electrical capacity by mid-century, with a compound average annual growth rate (CAAGR) exceeding 15% (see Fig. 1a-b)⁴.

This rapid digitalization and decentralization of the grid, accompanying the PV boom, has simultaneously expanded the cyber-attack surface⁵⁻⁷. A systematic review of major cybersecurity incidents from 2019 to 2026 reveals a growing exposure of solar infrastructure, spanning inverter systems, remote monitoring platforms and SCADA networks (Fig. 1c). Reported incidents include DDoS attacks disrupting renewable generation, unauthorized manipulation of inverter settings, botnet hijacking of solar monitoring devices and coordinated compromises of renewable power plants⁸⁻¹². The scale of the exposure is equally concerning, with more than 35,000 solar devices exposing known high-severity vulnerabilities, including flaws affecting inverters and monitoring ecosystems^{13,14}. These events demonstrate that the cyber vulnerability of PV infrastructure is no longer a hypothetical concern, but an emerging system-level risk.

Yet cyber vulnerability in PV systems is not simply an exogenous condition to be addressed after deployment. It is fundamentally shaped by planning decisions made long before an attack occurs. The choice of vendor determines the firmware and vulnerabilities embedded across the installed base, geographical dispersion determines how many independent control domains an adversary must compromise to induce widespread disruption, and the integration of monitoring and control interfaces determines the remote entry points available to attackers¹⁵. Planning decisions therefore do more than determining the economic and operational characteristics of a PV system. They actively shape its attack surface and the potential physical consequences inducible by an adversary. A configuration that is optimal under normal operating conditions may therefore be catastrophically fragile under targeted attack. Cyber resilience must consequently move beyond post-deployment protection and become an intrinsic dimension of infrastructure planning to enhance power grid's survivability under extreme attack incidents.

Research on planning renewable generation with battery energy storage systems (BESS) provides an operational foundation for this problem. Energy-storage coordination has been shown to support frequency regulation, voltage control, and system

flexibility^{16–18}. Related studies have examined distributed storage control, coordinated PV-BESS operation, and resilience-oriented PV-storage allocation^{19–21}. As storage deployment has matured, technical and economic assessments have compared stand-alone and AC- or DC-coupled PV-BESS architectures^{22–24}. Planning studies have optimized the siting, sizing, and operation of these systems using mathematical and heuristic methods^{25–27}. Transmission-scale BESS allocation has also been investigated²⁸. These studies have established the operational and economic value of joint PV-BESS planning, but largely treat cyber threats as external conditions specified independently of deployment decisions. They therefore do not capture the security coupling inherent to networked PV infrastructure, where choices of capacity, location, vendor and control-domain integration jointly determine both the attackable fleet and the physical consequences of compromise.

Moving from this foundation to cyber-resilient planning introduces several coupled technical challenges. Long-horizon storage planning often relies on reduced temporal representations to control computational burden, but temporal aggregation can obscure seasonal variability, inter-day dependencies, and storage-state evolution^{29,30}. Preserving the hourly full-year trajectory is important here because it determines both normal operation and the system state at the onset of an attack. At the same time, the attack space cannot be specified independently of the deployment plan, because changes in PV capacity, location, vendor, and control-domain composition alter the attackable fleet and the feasible attack scenarios. Combining this decision-dependent attack space with the long operational horizon produces a mixed discrete-continuous planning problem with nonlinear system responses and nested adversarial simulations. Each candidate plan is therefore expensive to evaluate. At full-year resolution, exact mathematical reformulations can become computationally burdensome, while population-based metaheuristics may require many evaluations without building an explicit model of the response surface. A suitable method must retain long-term operational dynamics, reconstruct the attack space for each candidate plan, and allocate a limited simulation budget efficiently.

These requirements make sample-efficient black-box search a natural foundation for the proposed framework. Bayesian optimization (BO) learns a surrogate of an expensive objective and uses predictive uncertainty to guide sequential sampling³¹. Its use in power-system design and controller tuning further illustrates its suitability when individual evaluations are costly^{32,33}. A random-forest surrogate is particularly appropriate for the present problem because it accommodates mixed variable types and nonlinear response surfaces³⁴, while Expected Improvement balances promising predicted performance against uncertainty when selecting each new evaluation. On this basis, we propose a simulation-driven Decision-Dependent Adversarial Bayesian Optimization (DD-ABO) framework for joint PV-BESS planning under networked PV curtailment attacks. For each candidate plan, an hourly full-year baseline simulation preserves seasonal operating conditions and the intertemporal BESS state trajectory. The installed PV capacities, locations, vendors, and control-domain relationships then define a candidate-specific attack space, within which an adversarial inner search identifies a high-impact realization. Shorter-horizon operational simulations quantify the resulting disruption relative to the baseline, and the attack-aware objective is returned to the random-forest surrogate so that Expected Improvement can select the next plan. Through this nested interaction, the threat landscape evolves with the planning decisions while the long-term operational chronology remains intact, integrating these requirements within a limited simulation budget. Applied to the IEEE 39-bus system with real New England data, DD-ABO shows that cyber resilience can be engineered through deployment choices rather than costly over-provisioning. Relative to attack-agnostic planning, it reduces the worst-case attack-induced operational penalty and expected unserved energy by 80.2% and 85.0%, respectively, without a statistically significant increase in capital or maintenance costs. The analysis further shows that the most damaging PV attacks concentrate in the upper neck of the duck curve, while spatial and vendor diversification emerge as intrinsic defence mechanisms that reshape the adversary's effective attack surface. These methodological and empirical findings demonstrate that cyber resilience can be embedded directly into renewable infrastructure planning without sacrificing economic efficiency.

Results

A Decision-Dependent Adversarial Framework for Grid Planning

The proposed DD-ABO framework addresses a fundamental limitation in conventional power system planning, which treats cyber threats as exogenous and static. As solar PV capacity expands, planning decisions increasingly shape both when and where the grid is vulnerable to cyber attacks. DD-ABO operationalizes this coupling through a closed-loop architecture in which an outer-loop Bayesian optimizer generates candidate PV-BESS planning decisions (Steps 1-3 of Fig. 2), while an inner-loop adversarial search constructs attack scenarios conditioned on each candidate plan (Step 4 of Fig. 2). The decision-dependent attack model explicitly characterizes vulnerability along two complementary dimensions. The temporal dimension identifies critical attack windows from the evolving relationship between PV generation, system load, and net-load ramping, while the spatial dimension determines attackable PV devices according to their installed locations, control-domain connections, vendor relationships, and topological proximity. Consequently, each planning decision induces a distinct attack surface and a corresponding set of feasible attack scenarios. The resulting worst-case operational impact is then evaluated through lower-level power system simulations and fed back to the surrogate model for subsequent planning decisions (Step 5 of Fig. 2).

The integration of temporal and spatial attack modelling enables DD-ABO to capture how infrastructure design reshapes adversarial opportunities. The temporal analysis links attack timing to system operating stress, allowing the adversarial search to identify attack windows in which PV curtailment is most consequential. The spatial analysis captures correlations among installed PV devices and determines which devices may be compromised jointly through shared vendors, control domains,

and topological proximity. These two dimensions are jointly conditioned on the planning decision, so changes in PV capacity, location, vendor assignment, or control-domain integration modify the resulting attack scenario space rather than merely changing the system response to a fixed threat set. This formulation therefore provides the basis for identifying both the temporal vulnerability of PV-rich grids and the spatial and vendor diversification patterns that can emerge as intrinsic defence mechanisms. The random-forest surrogate further enables efficient exploration of the resulting mixed-integer planning space, while expected improvement balances exploration and exploitation as new decision-dependent evaluations are obtained. Through this nested interaction between planning, adversarial scenario construction, and operational simulation, DD-ABO progressively searches for PV-BESS configurations that remain resilient to the most consequential cyber attacks.

Beyond optimization efficiency, the framework establishes a direct link between infrastructure planning and cyber resilience. Rather than treating security as a post-deployment protection layer, DD-ABO allows the planning process itself to shape the temporal exposure and spatial structure of the PV attack surface. This provides a basis for examining how renewable infrastructure can be configured to reduce adversarial impact through strategic deployment rather than relying solely on additional protective measures or over-provisioning. The following analyses therefore examine the vulnerability landscape from two complementary perspectives, first identifying when PV attacks are most damaging and then revealing how spatial and vendor diversity can provide intrinsic resilience.

Temporal Characterization of PV Attack Vulnerability

The criticality of PV attack timing is rooted in the duck curve phenomenon, which emerges as high midday PV output depresses net load before a steep afternoon ramp as solar generation declines^{35,36}. Using 2025 real-world data from ISO New England^{37,38}, we first characterize the annual load and PV capacity factor profiles to identify when the system is most dependent on solar generation (Fig. 3a). High electricity demand is concentrated in the summer months and substantially overlaps with periods of high PV availability. This seasonal coincidence creates a critical operating condition in which the grid relies heavily on PV generation precisely when system stress is greatest. Consequently, the severity of a PV generation attack is expected to depend not only on which PV resources are targeted, but also on when the attack occurs.

At the intraday scale, PV generation and system load exhibit a pronounced temporal relationship that further shapes this vulnerability (Fig. 3b). PV output reaches its maximum around midday, whereas the strongest negative correlation between PV generation and load occurs in the afternoon as solar output declines while demand remains elevated. This transition increases the contribution of PV generation to net-load shaping and precedes the steep afternoon ramp. The strength of this relationship varies seasonally, with summer exhibiting the highest load levels and the strongest afternoon PV-load coupling (Fig. 3c)³⁹. These seasonal and diurnal patterns indicate that the temporal vulnerability of PV generation is highly structured rather than uniformly distributed across the year, providing an exploitable dimension for adversarial scenario construction.

We therefore incorporate temporal vulnerability directly into the inner-loop adversarial search by evaluating attack scenarios across three operational regimes along the duck neck on the annual peak-load day. The lower neck represents the period of maximum PV output, the middle neck captures the transition as PV generation declines, and the upper neck corresponds to the steepest net-load ramp, by which time operational flexibility has already been substantially committed. These windows provide structurally distinct operating conditions (Fig. 3e-f), under which identical PV generation losses can produce markedly different system consequences. Across independent runs, approximately 50% of the selected worst-case PV-curtailment scenarios begin at the upper neck (Fig. 3d). This concentration persists across planning algorithms, indicating that the upper neck reflects an intrinsic temporal vulnerability of the system rather than an optimization artifact. At this stage, the system has limited remaining ramping flexibility to compensate for a sudden loss of PV generation, amplifying the operational consequences of an otherwise identical attack.

These results establish attack timing as an endogenous planning consideration rather than a fixed operational parameter. By explicitly searching across temporally distinct attack regimes, DD-ABO identifies when a given PV-BESS configuration is most exposed to adversarial disruption and incorporates this information into the planning objective. The resulting temporal vulnerability profile therefore links grid planning decisions with the timing of their worst-case consequences, demonstrating that resilient renewable planning must account not only for where and how much PV and BESS capacity is deployed, but also for when the configuration is most vulnerable to attack.

Spatial and Vendor Diversity as Intrinsic Defence Mechanisms

The spatial organization and vendor composition of PV deployment provide a second dimension through which planning decisions shape cyber resilience. To elucidate this mechanism, we analyzed the control-domain distribution and vendor composition of the final planning decisions across independent runs. DD-ABO produces the largest number of cross-zone co-occurrence edges (Fig. 4a). The cross-zone integration ratio is 73.8% for the group of decision-dependent algorithms (DD-X), compared with 65.5% for BO and 69.3% for fixed-adversary Bayesian optimization (F-ABO) (Fig. 4b). By distributing PV resources across multiple control domains, the resulting configurations reduce the concentration of remotely controllable assets within any single cyber domain. An adversary seeking widespread disruption must therefore compromise multiple control domains rather than exploiting a single domain to affect a large fraction of the installed fleet. Spatial dispersion consequently acts as an intrinsic barrier to the propagation of cyber-induced disturbances across the electrical network.

Vendor composition provides a complementary layer of protection. DD-ABO yields higher mean vendor Shannon diversity, with a mean index of approximately 1.0 compared with approximately 0.9 under BO (Fig. 4c). This diversification reduces dependence on any single vendor and limits the extent to which a common firmware or software vulnerability can be propagated across the PV fleet. The effect is particularly relevant for networked PV infrastructure, where common vendor technologies can create shared cyber dependencies across geographically distributed assets. Rather than treating vendor diversity as a post-deployment security measure, DD-ABO incorporates it implicitly through decision-dependent adversarial evaluation, allowing configurations with concentrated technological dependencies to be penalized whenever they create more exploitable attack surfaces. These planning-level defences complement traditional security measures such as encryption, multi-factor authentication, and zero-trust architectures by reducing the structural consequences of a successful compromise rather than relying solely on preventing unauthorized access.

The resulting planning patterns also reveal a distinction between selective diversification and indiscriminate spatial dispersion. As shown by the PV-BESS co-occurrence networks in Fig. 4d, the three BO-based methods (DD-ABO, BO, and F-ABO) select a compact set of recurring BESS locations across independent runs, whereas the two population-based methods exhibit substantially greater placement variability. At the same time, DD-ABO has the highest mean vendor diversity among the methods (Fig. 4c). In this case study, this finding suggests that cyber-resilient planning does not necessitate uniformly dispersing infrastructure across the network. Instead, the optimization selectively diversifies the dimensions that determine attack propagation while preserving economically and operationally favorable deployment configurations.

These results indicate that spatial and technological diversity can function as intrinsic defence mechanisms when incorporated into infrastructure planning. Cross-zone integration limits the concentration of PV assets within individual control domains, while vendor diversification reduces shared technological dependencies that could enable common-mode compromise. More broadly, the findings suggest that the security posture of a renewable system can be shaped directly by deployment decisions without requiring indiscriminate over-provisioning. Cyber resilience may therefore be strengthened through the architecture of renewable infrastructure itself, with planning decisions influencing not only system cost and operational performance, but also the structure of the attack surface available to future adversaries.

Convergence and Attack-Scenario Solution Quality

We compared DD-ABO with two decision-dependent benchmark algorithms, namely decision-dependent particle swarm optimization (DD-PSO)⁴⁰ and decision-dependent genetic algorithm (DD-GA)⁴¹. Each algorithm was evaluated in 10 independent runs of 200 iterations each. DD-ABO converges more rapidly to a lower plateau and exhibits less run-to-run variation than DD-PSO and DD-GA (Fig. 5a,b). Its final mean objective value is approximately 6.0% lower than that of DD-GA and 8.6% lower than that of DD-PSO (Fig. 5b). This performance is consistent with the suitability of the random-forest surrogate for the nonsmooth, mixed-integer response surface of the bilevel planning problem and with prior applications of BO to expensive strategic-investment and multivector energy-planning problems^{42,43}.

The algorithms also differ in the adversarial vulnerability of their sampled and final plans. Heatmaps of the attack-induced operational penalty Q^{atk} over the installed PV and BESS capacity space visualize the vulnerability landscape sampled by each algorithm (Fig. 5c-e). Although some intermediate DD-PSO and DD-GA solutions attain lower Q^{atk} than some DD-ABO samples, DD-ABO covers a wider range of PV and BESS capacity combinations. The clearest distinction occurs in the final solutions. As shown in Fig. 5f, DD-ABO identifies final configurations with lower Q^{atk} , generally higher installed PV capacity, and less BESS capacity than the heuristic alternatives. This confirms that DD-ABO actively steers the planning solution away from adversarial attractors by exploiting a learned approximation of the mapping from deployment decisions to the attack-aware objective via its random-forest surrogate, a capability that heuristic methods lack. Compared with attack-agnostic BO and fixed-set F-ABO, all DD-X algorithms (DD-ABO, DD-PSO, and DD-GA) also yield lower final Q^{atk} values, confirming that decision-dependent adversarial planning fundamentally alters the optimization landscape. Planning decisions obtained without accounting for adaptive adversarial threats are inherently vulnerable. Conventional optimization approaches that ignore the decision-dependence of cyber threats may inadvertently converge to solutions that are optimal under assumed conditions yet catastrophically vulnerable under actual adversarial behaviour, a risk that is magnified as PV penetration increases globally.

Decision-Dependent Adversarial Planning Enables Intrinsic Cyber Resilience

To quantify the value of explicitly modelling the coupling between planning decisions and adversarial behaviour, we benchmarked DD-ABO against conventional BO and F-ABO. BO neglects cyber threats during planning, whereas F-ABO assumes a predefined attack set independent of deployment decisions. DD-ABO instead anticipates how infrastructure decisions reshape the adversary's optimal targets. Relative to BO, DD-ABO reduces the mean worst-case attack-induced operational penalty Q^{atk} by 80.2% and the mean expected energy not served $EENS^{atk}$ by 85.0% (Fig. 6a-d; both $p < 0.001$). In contrast, F-ABO provides no statistically significant improvement over BO in either metric, indicating that static threat assumptions can be fundamentally misleading for resilience-oriented planning because they overlook the adaptive coupling between infrastructure and adversarial behaviour. The failure of fixed-attack formulations to improve resilience demonstrates that effective cyber-resilient planning requires the threat landscape to be co-optimized with infrastructure decisions. More broadly, these results show that the cyber attack surface of renewable infrastructure is not a fixed system attribute, but an emergent property of

deployment decisions that reshape both vulnerability exposure and adversarial incentives.

Crucially, this resilience gain does not require a statistically significant increase in annualized investment cost C^{inv} or fixed maintenance cost C^m relative to BO (Fig. 6e,f). DD-ABO incurs only a marginal increase in base-case operational cost Q^{base} (Fig. 6g), revealing a limited trade-off between nominal operating efficiency and resilience. Rather than purchasing resilience through over-provisioning, DD-ABO embeds it in the structure of infrastructure deployment by diversifying spatial, control-domain and vendor dependencies. Thus, in this case study, cyber resilience emerges as an intrinsic property of how renewable assets are configured, rather than as a capital or maintenance-cost premium.

Discussion

The cyber vulnerability of a PV-rich grid is not merely an exogenous constraint to be addressed after infrastructure has been planned. It is also an endogenous property of the infrastructure itself, shaped by decisions about capacity, location, control-domain and vendor selection. Our results show that explicitly accounting for this coupling can transform infrastructure planning from a passive response to cyber risk into a mechanism for engineering resilience. DD-ABO reduces worst-case attack-induced operational penalties by 80.2% and expected energy not served by 85.0%, without statistically significant increases in annualized investment or fixed maintenance costs. These results point to a shift from reactive vulnerability mitigation towards proactive security engineering, in which the configuration of renewable infrastructure itself becomes part of the defence strategy.

An important insight from our analysis is that cyber risk is not only spatially structured but also temporally concentrated. The duck curve phenomenon^{35,36}, characteristic of grids with high solar penetration, creates a predictable period of operational stress during the afternoon ramp, when declining solar generation coincides with increasing demand and constrained ramping flexibility⁴⁴. Across the three decision-dependent algorithms, approximately half of the selected worst-case PV-curtailment scenarios initiate during the upper neck interval, where system flexibility is most constrained. This concentration suggests that cyber defence can be prioritized around periods of heightened system susceptibility rather than distributed uniformly across time. In practice, monitoring, anomaly detection and data validation could therefore be intensified during these critical windows. More fundamentally, this result illustrates how adversarial planning can reveal temporal patterns of cyber-physical vulnerability that remain obscured when cyber threats are treated as static or independent of system operation.

Spatial and vendor diversification provide a complementary structural mechanism for resilience. Conventional security engineering often advocates for redundancy and overbuilding as primary routes to resilience⁴⁵. Our results point to a different mechanism in which resilience can emerge from how much capacity is distributed rather than simply from how much capacity is installed. DD-ABO favours deployment across control areas and vendor ecosystems, resulting in greater cross-zone integration and higher vendor Shannon diversity. Under the dependency structure represented in our model, these configurations reduce the concentration of shared control domain and vendor dependencies and limit the fraction of the PV fleet that can be affected through a common compromise. This interpretation is consistent with network science studies showing that concentrated dependencies can amplify cascading failures⁴⁶⁻⁴⁸. More broadly, infrastructure diversity can function as a form of cyber defence by limiting the systemic consequences of correlated compromise.

This perspective becomes increasingly important as renewable deployment accelerates. Under the IEA Net Zero Scenario, solar capacity is projected to grow substantially⁴, while the marginal cost of adding new generation assets continues to decline^{1,2}. Meanwhile, the growing digital connectivity of renewable infrastructure is expanding the potential cyber attack surface^{5,15}, creating a growing need to incorporate cybersecurity into infrastructure planning. This need is particularly acute in developing economies and emerging markets⁴⁹, where rapid renewable expansion must be achieved under constrained financial and institutional resources. The computational performance observed on the IEEE 39-bus system under a 200 evaluation budget, together with the use of publicly available New England data, provides an initial indication that decision-dependent adversarial planning can be implemented with realistic planning information and computational resources.

We acknowledge several limitations. First, the present attack model focuses on PV curtailment attacks targeting PV generation assets. Real-world adversaries may orchestrate coordinated attacks across heterogeneous device types^{50,51}, including load demand^{52,53}, transmission infrastructure⁵⁴, and BESS control interfaces⁵⁵. Such coordinated attacks could exploit interactions among multiple attack surfaces and produce physical consequences beyond those captured here. Second, the current framework adopts a single stage planning formulation and therefore does not capture the evolution of infrastructure, operating conditions and adversarial capabilities over multiple years. The deployment decision z^* , grid topology and attack capabilities are treated as fixed over the planning horizon, whereas power systems evolve through transmission expansion and retirement^{56,57}, changes in demand patterns⁵⁸, and replacement or expansion of PV and BESS assets⁵⁷. Adversarial capabilities may likewise evolve as new vulnerabilities and attack strategies emerge. These changes could alter both the optimal deployment configuration and the relative value of different resilience mechanisms. Third, computational performance was evaluated only on the IEEE 39-bus system under a 200 evaluation budget, so scalability to larger and more heterogeneous networks remains unresolved.

Despite these limitations, the framework offers a practical basis for embedding cyber resilience into infrastructure planning. DD-ABO can be interfaced with existing power system planning workflows through a power flow solver and attack simulation routines, while its random forest surrogate provides interpretable feature importance measures that help identify planning decisions most strongly associated with resilience. Future advances in surrogate modelling, including graph neural networks,

deep neural networks and other data efficient learning methods, could replace the current surrogate to improve scalability to larger networks, higher dimensional planning spaces and more complex cyber-physical interactions. Large language model agents could further complement this optimization layer by synthesizing heterogeneous threat intelligence, identifying emerging attack patterns, assisting in the generation and refinement of attack scenarios, and translating optimization results into actionable recommendations for planners and regulators. Beyond PV BESS planning, the same decision-dependent adversarial planning paradigm could be extended to other critical infrastructures, including microgrid design, EV charging infrastructure and industrial control systems, where infrastructure configuration can shape both cyber exposure and the physical consequences of compromise. These developments could enable adaptive planning frameworks that integrate evolving system conditions and cyber threats while retaining computational tractability and decision interpretability. As renewable penetration and digital connectivity continue to increase, embedding cyber resilience into infrastructure design will become increasingly important for building power systems that remain reliable and secure under evolving threats.

Methods

Overall Planning Model

We investigate a resilience-oriented joint planning problem for PV generation and BESS under PV attack scenarios. The problem is formulated as a bi-level model. The upper level determines the device-level PV-BESS deployment decision, including the number of installed devices, their bus locations, capacities, and PV vendor assignments. The lower level evaluates the operational performance of the system under both baseline and attack scenarios. By jointly considering investment cost, fixed maintenance cost, baseline operating cost, and the worst attack-induced additional loss, the upper-level objective is defined as

$$\min_{z \in \mathcal{Z}} C^{inv}(z) + C^m(z) + Q^{base}(z) + Q^{atk}(z), \quad (1)$$

where z denotes the planning decision vector and $\mathcal{Z}$ is the feasible planning set; $C^{inv}(z)$ denotes the annualized investment cost, $C^m(z)$ denotes the annual fixed maintenance cost, $Q^{base}(z)$ and $Q^{atk}(z)$ denote the lower-level optimal operational values under the baseline and attack scenarios, respectively. All costs are expressed on an annual basis.

Upper-Level Device-Based Planning Model

Instead of deciding whether each bus installs PV or BESS, the upper level directly plans a finite number of candidate PV and BESS devices. Let $\mathcal{K}^{PV} = \{1, \dots, K_{\max}^{PV}\}$, $\mathcal{K}^{BESS} = \{1, \dots, K_{\max}^{BESS}\}$ denote the candidate sets of PV and BESS devices. For each candidate PV device $k \in \mathcal{K}^{PV}$, the decision variables include a binary installation indicator $y_k^{PV} \in \{0, 1\}$, a bus location $n_k^{PV} \in \mathcal{N}$, an installed capacity $P_k^{PV} \in \mathcal{P}^{PV}$, and a vendor type $m_k \in \mathcal{M}$. For each candidate BESS device $k \in \mathcal{K}^{BESS}$, the decision variables include a binary installation indicator $y_k^{BESS} \in \{0, 1\}$, a bus location $n_k^{BESS} \in \mathcal{N}$, a rated power $P_k^{BESS} \in \mathcal{P}^{BESS}$, and a rated duration $T_k^{BESS} \in \mathcal{T}^{BESS}$, with energy capacity defined as $E_k^{BESS} = P_k^{BESS} T_k^{BESS}$. If a candidate device is not installed, all associated capacity variables are set to zero. Otherwise, the PV capacity and BESS configuration variables are restricted to their respective discrete candidate sets. Then, the planning decision vector can be expressed as

$$z = \left(\{y_k^{PV}, n_k^{PV}, P_k^{PV}, m_k\}_{k \in \mathcal{K}^{PV}}, \{y_k^{BESS}, n_k^{BESS}, P_k^{BESS}, T_k^{BESS}\}_{k \in \mathcal{K}^{BESS}} \right). \quad (2)$$

The investment and fixed maintenance costs are calculated as

$$C^{inv}(z) = \frac{r(1+r)^{L_{PV}}}{(1+r)^{L_{PV}} - 1} \sum_{k \in \mathcal{K}^{PV}} (1 - \rho^{ITC}) c_{PV}^{inv} P_k^{PV} + \frac{r(1+r)^{L_{BESS}}}{(1+r)^{L_{BESS}} - 1} \sum_{k \in \mathcal{K}^{BESS}} (c_{B,p}^{inv} P_k^{BESS} + c_{B,e}^{inv} E_k^{BESS}) \quad (3)$$

$$C^m(z) = \sum_{k \in \mathcal{K}^{PV}} c_{PV}^m P_k^{PV} + \sum_{k \in \mathcal{K}^{BESS}} c_B^m P_k^{BESS}. \quad (4)$$

To avoid permutation-equivalent solutions and reduce the search space, symmetry-breaking constraints are imposed on device indices, locations and capacities:

$$\begin{cases} y_k^{PV} \geq y_{k+1}^{PV}, \\ y_{k+1}^{PV} = 1 \Rightarrow n_k^{PV} \leq n_{k+1}^{PV}, \\ y_k^{BESS} \geq y_{k+1}^{BESS}, \\ y_{k+1}^{BESS} = 1 \Rightarrow n_k^{BESS} \leq n_{k+1}^{BESS}. \end{cases} \quad (5)$$

To further reduce symmetry when multiple devices are co-located at the same bus, capacities should be ordered within the same location:

$$\begin{cases} y_{k+1}^{PV} = 1, n_k^{PV} = n_{k+1}^{PV} \Rightarrow P_k^{PV} \geq P_{k+1}^{PV}, \\ y_{k+1}^{BESS} = 1, n_k^{BESS} = n_{k+1}^{BESS} \Rightarrow P_k^{BESS} \geq P_{k+1}^{BESS}, \\ y_{k+1}^{BESS} = 1, n_k^{BESS} = n_{k+1}^{BESS}, P_k^{BESS} = P_{k+1}^{BESS} \\ \Rightarrow E_k^{BESS} \geq E_{k+1}^{BESS}, \end{cases} \quad (6)$$

Lower-Level Baseline Operation Model

Under the baseline scenario, the lower level minimizes the operating cost only. The carbon cost is internalized into the SG marginal operating cost through the carbon price. The baseline operation problem is defined as

$$Q^{base}(z) = \min_{u^{(0)} \in \mathcal{U}^{base}(z)} C^{op,base}(z), \quad (7)$$

where $u^{(0)}$ denotes the hourly operating decisions over a one-year baseline horizon, and $\mathcal{U}^{base}(z)$ is the feasible region defined by the operation constraints. The baseline operating cost is given by

$$C^{op,base}(z) = \sum_{t \in \mathcal{T}} \left[\sum_{g \in \mathcal{G}} (c_g^{fuel} + \pi^{CO_2} e_g) p_{g,t}^{(0)} + \sum_{k \in \mathcal{K}^{BESS}} c_k^{cyc} (p_{k,t}^{ch,(0)} + p_{k,t}^{dis,(0)}) - \sum_{k \in \mathcal{K}^{PV}} \pi^{PPA} p_{k,t}^{PV,(0)} \right] \Delta t, \quad (8)$$

where $p_{g,t}^{(0)}$, $p_{k,t}^{ch,(0)}$, and $p_{k,t}^{dis,(0)}$ denote the output of synchronous generator g , the charging and discharging powers of BESS device k at time t under the baseline scenario, and the third term represents the revenue from PV generation under a fixed power purchase agreement (PPA) contract⁵⁹. To ensure no load curtailment under the normal scenario, i.e., $EENS^{base}(z) = 0$, the following constraint is imposed:

$$p_{i,t}^{shed,(0)} = 0, \quad \forall i \in \mathcal{N}, t \in \mathcal{T}. \quad (9)$$

Lower-Level Attack Operation Model

An attack scenario is defined as

$$s = (\mathcal{A}, t^*, \tau^*, r^*), \quad \mathcal{A} \in \mathbb{A}(z), \quad (10)$$

where $\mathcal{A}$ is the attacked PV device set, t^* is the attack start time, $\tau^* = 24$ h is the attack duration, and r^* denotes the sudden full recovery mode. Since the planning decision changes the spatial distribution, vendor composition, and capacity allocation of PV devices and thereby modifies the attack surface, the attack scenario set is decision-dependent:

$$\Omega(z) = \{(\mathcal{A}, t^*, \tau^*, r^*) : \mathcal{A} \in \mathbb{A}(z)\}. \quad (11)$$

The attack start time is determined by the duck curve phenomenon, where high PV penetration reshapes the net-load profile and produces a steep afternoon net-load ramp^{35,36}. The most critical operating period is the afternoon neck, when the system faces severe ramping pressure while solar generation declines. To comprehensively evaluate system vulnerability, the attack start time t^* is selected with three options along the duck neck, namely the upper neck, the middle neck, and the lower neck. These correspond to three consecutive hours within the afternoon ramp period. The attack is launched on the day with the annual peak system load, as this represents the grid's most stressed condition. On that day, the hour with the highest PV generation is designated as the lower neck point, the following hour as the middle neck point, and the next hour as the upper neck point. This design captures the transition from high PV output with moderate ramping at the lower neck to low PV output with severe ramping at the upper neck. Given that the power system cannot instantly return to its baseline after the attack is cleared, a five-day simulation horizon is adopted, consisting of one attack day followed by four recovery days. Let $t_e = t^* + 119$ denote the end of the recovery horizon. The attack simulation horizon is denoted by

$$\mathcal{T}^{atk} = \{t^*, t^* + 1, \dots, t_e\}. \quad (12)$$

For a given planning decision z , the set of attackable PV devices is $\mathcal{K}_{act}^{PV}(z) = \{k \in \mathcal{K}^{PV} \mid y_k^{PV}(z) = 1\}$. A seed-driven attack generation mechanism is adopted. First, an initial attacked PV device k_0 is selected from $\mathcal{K}_{act}^{PV}(z)$ according to a capacity-weighted probability:

$$\Pr(k_0 = k \mid z) = \frac{P_k^{PV}(z)}{\sum_{j \in \mathcal{K}_{act}^{PV}(z)} P_j^{PV}(z)}, \quad k \in \mathcal{K}_{act}^{PV}(z). \quad (13)$$

Then, the final attack set is generated according to the pairwise correlation among installed PV devices. The composite correlation between PV devices k and j is defined as

$$\rho_{k,j}(z) = \lambda_1 \rho_{k,j}^{vendor} + \lambda_2 \rho_{k,j}^{control} + \lambda_3 \rho_{k,j}^{distance}, \quad (14)$$

where $\lambda_1, \lambda_2, \lambda_3 \geq 0$ and $\lambda_1 + \lambda_2 + \lambda_3 = 1$. The three components are defined as follows:

$$\begin{cases} \rho_{k,j}^{vendor} = \begin{cases} 1, & \text{if } v_k = v_j, \\ 0, & \text{otherwise,} \end{cases} \\ \rho_{k,j}^{control} = \begin{cases} 1, & \text{if } d^{ctrl}(n_k^{PV}) = d^{ctrl}(n_j^{PV}), \\ 0, & \text{otherwise,} \end{cases} \\ \rho_{k,j}^{distance} = \exp\left(-\frac{d_{n_k^{PV}, n_j^{PV}}}{d_0}\right), \end{cases} \quad (15)$$

where $d^{ctrl}(n)$ denotes the control domain of bus n , $d_{n_k^{PV}, n_j^{PV}}$ denotes the topological distance between the buses hosting PV devices k and j , and $d_0 > 0$ is a distance decay parameter. Given the seed device k_0 , the probability that another PV device j is included in the attack set is defined by

$$p_{j|k_0}(z) = \min \{1, \alpha \rho_{k_0, j}(z)\}, \quad (16)$$

where $\alpha > 0$ is an attack-propagation parameter. Let $\xi_j \sim \text{Bernoulli}(p_{j|k_0}(z))$. Then the attack set is constructed as

$$\mathcal{A} = \{k_0\} \cup \{j \in \mathcal{K}_{act}^{PV}(z) \setminus \{k_0\} \mid \xi_j = 1\}. \quad (17)$$

The above mechanism induces a candidate scenario set $\Omega(z)$ for each planning decision z . Each scenario $s \in \Omega(z)$ is associated with an occurrence probability $q_s(z)$, induced by (13) and (16). This probability is used for scenario generation and search prioritization, but not directly included in the robust lower-level objective, which follows a worst-case criterion.

The attack is assumed to start at time period t^* and is immediately known to the system operator at the beginning of that period. All attack scenarios must follow the baseline trajectory before the attack starts. To ensure a consistent initial condition, the attack simulation is initialized from the baseline trajectory at the end of the previous period, i.e., at time $t^* - 1$:

$$p_{g, t^*-1}^{(s)} = p_{g, t^*-1}^{(0)}, p_{k, t^*-1}^{PV, (s)} = p_{k, t^*-1}^{PV, (0)}, SOC_{k, t^*-1}^{(s)} = SOC_{k, t^*-1}^{(0)}. \quad (18)$$

Similarly, at the end of the recovery period t_e , the system must return to the baseline trajectory to ensure no persistent deviation caused by the attack:

$$p_{g, t_e}^{(s)} = p_{g, t_e}^{(0)}, p_{k, t_e}^{PV, (s)} = p_{k, t_e}^{PV, (0)}, SOC_{k, t_e}^{(s)} = SOC_{k, t_e}^{(0)}. \quad (19)$$

For each scenario $s \in \Omega(z)$, the operating decisions must satisfy $u^{(s)} \in \mathcal{U}^{atk}(z, s)$, where $\mathcal{U}^{atk}(z, s)$ denotes the feasible operating region under scenario s , which includes the PV availability reduction and all device-level and network constraints.

For a given planning solution z , the lower-level attack problem aims to minimize the sum of the worst-case additional operating costs and the unserved energy penalty across all attack scenarios, subject to initialization constraints, recovery constraints, and scenario-wise feasible operating constraints. The problem is formulated as follows:

$$Q^{atk}(z) = \min_{\{u^{(s)}\}_{s \in \Omega(z)}} \max_{s \in \Omega(z)} \{ \Delta C^{op}(z, s) + \pi EENS^{atk}(z, s) \}. \quad (20)$$

Since the baseline one-year horizon operating cost is already accounted for in $Q^{base}(z)$, the attack operating cost is considered in incremental terms over the attack simulation horizon:

$$\begin{aligned} \Delta C^{op}(z, s) = C^{op, atk}(z, s) - C^{op, base, win}(z) = & \sum_{t \in \mathcal{T}^{atk}} \left[\sum_{g \in \mathcal{G}} (c_g^{fuel} + \pi^{CO_2} e_g) (p_{g, t}^{(s)} - p_{g, t}^{(0)}) \right. \\ & \left. + \sum_{k \in \mathcal{K}^{BESS}} c_k^{cyc} (p_{k, t}^{ch, (s)} + p_{k, t}^{dis, (s)} - p_{k, t}^{ch, (0)} - p_{k, t}^{dis, (0)}) - \sum_{k \in \mathcal{K}^{PV}} \pi^{PPA} (p_{k, t}^{PV, (s)} - p_{k, t}^{PV, (0)}) \right] \Delta t, \end{aligned} \quad (21)$$

and the attack-scenario unserved energy is

$$EENS^{atk}(z, s) = \sum_{t \in \mathcal{T}^{atk}} \sum_{i \in \mathcal{N}} p_{i, t}^{shed, (s)} \Delta t. \quad (22)$$

Device-Level Operational Constraints

The feasible sets $\mathcal{U}^{base}(z)$ and $\mathcal{U}^{atk}(z, s)$ are defined by the following device-level and network constraints. PV generation is limited by the installed capacity and the time-dependent capacity factor. The output of PV device k at time t under scenario s , denoted by $p_{k, t}^{PV, (s)}$, satisfies

$$0 \leq p_{k, t}^{PV, (s)} \leq P_k^{PV} \phi_t a_{k, t}^{(s)}, \quad (23)$$

where $\phi_t \in [0, 1]$ is the PV capacity factor and $a_{k, t}^{(s)} \in \{0, 1\}$ represents PV availability. Under the baseline scenario, $a_{k, t}^{(0)} = 1$, while under attack scenarios, $a_{k, t}^{(s)} = 0$ if device $k \in \mathcal{A}$ during the attack duration. BESS devices are subject to power limits, state-of-charge dynamics and state-of-charge bounds:

$$\begin{cases} 0 \leq p_{k, t}^{ch, (s)} \leq P_k^{BESS}, \\ 0 \leq p_{k, t}^{dis, (s)} \leq P_k^{BESS}, \\ SOC_{k, t+1}^{(s)} = SOC_{k, t}^{(s)} + \frac{\eta_{ch} p_{k, t}^{ch, (s)} \Delta t}{E_k^{BESS}} - \frac{p_{k, t}^{dis, (s)} \Delta t}{\eta_{dis} E_k^{BESS}}, \\ SOC_{\min} \leq SOC_{k, t}^{(s)} \leq SOC_{\max}. \end{cases} \quad (24)$$

To ensure temporal consistency over the annual baseline simulation, the baseline feasible set $\mathcal{U}^{base}(z)$ imposes a cyclic SOC constraint for each BESS:

$$SOC_{k,1}^{(0)} = SOC_{k,\max}^{(0)} \tau, \quad \forall k \in \mathcal{K}^{BESS}, \quad (25)$$

which is not enforced in the attack feasible region $\mathcal{U}^{atk}(z, s)$ that models short-term transient operation under PV attacks. Synchronous generators are subject to output limits and ramping constraints⁵⁹:

$$\begin{cases} P^{\min} P_g \leq p_{g,t}^{(s)} \leq P^{\max} P_g, \\ p_{g,t}^{(s)} - p_{g,t-1}^{(s)} \leq R^{up} P_g, \\ p_{g,t-1}^{(s)} - p_{g,t}^{(s)} \leq R^{down} P_g. \end{cases} \quad (26)$$

Network constraints are modelled using DC power flow, with line flow limits and nodal balance enforced at each time period⁵⁹:

$$\begin{cases} f_{l,t}^{(s)} = B_l(\theta_{n(l),t}^{(s)} - \theta_{m(l),t}^{(s)}), \\ |f_{l,t}^{(s)}| \leq F_l^{\max}, \\ \sum_{g \in \mathcal{G}(i)} p_{g,t}^{(s)} + \sum_{k: n_k^{PV} = i} p_{k,t}^{PV,(s)} + \sum_{k: n_k^{BESS} = i} (p_{k,t}^{dis,(s)} - p_{k,t}^{ch,(s)}) + \sum_{l \in \mathcal{L}_{in}(i)} f_{l,t}^{(s)} - \sum_{l \in \mathcal{L}_{out}(i)} f_{l,t}^{(s)} = P_{i,t}^{load} - p_{i,t}^{shed,(s)}. \end{cases} \quad (27)$$

Decision-Dependent Adversarial Bayesian Optimization

The planning model presents three fundamental challenges that preclude the application of classical robust optimization (RO) approaches. First, the attack scenario set $\Omega(z)$ is decision-dependent, i.e., the set of possible attack realizations changes with the planning decision z itself. This dependency arises because the composition and spatial distribution of installed PV devices directly shape the attack surface (see (13)-(17)). In conventional BO, the uncertainty set is fixed a priori. Here, however, the set $\Omega(z)$ depends on z in a combinatorial manner, rendering standard robust reformulations such as box, ellipsoidal, or polyhedral uncertainty sets inapplicable. Second, the lower-level problem involves a max-min structure (see (20)) where the inner maximization is taken over a scenario set $\Omega(z)$. While such a structure can be linearized in principle via enumeration or duality, the decision-dependent nature of $\Omega(z)$ eliminates the possibility of a compact, scenario-independent dual formulation. Third, even if the first two issues were resolved, the full-year temporal resolution (8760 hours) coupled with multiple attack scenarios would lead to an extremely large-scale optimization problem with millions of constraints. Moreover, the overall problem does not admit a tractable mixed-integer linear or convex formulation due to the nested max-min structure, the decision-dependent uncertainty set, and the coupling between planning and operation across multiple time scales. Consequently, an exact RO solution is computationally intractable.

To overcome these challenges, we propose a Decision-Dependent Adversarial Bayesian Optimization (DD-ABO) framework that replaces the intractable model, guided by a data-driven surrogate model. Let the black-box robust planning objective be

$$f(z) = C^{inv}(z) + C^m(z) + Q^{base}(z) + Q^{atk}(z). \quad (28)$$

Since $f(z)$ is expensive to evaluate and lacks a tractable closed-form representation, it is optimized through sequential simulation-based learning. At the k -th iteration, the outer-loop Bayesian optimizer proposes a candidate planning decision z_k . Based on z_k , the decision-dependent attack scenario set is constructed as $\Omega(z_k)$. An adversarial search procedure is performed over $\Omega(z_k)$ to identify a high-risk attack scenario

$$s_k^* \approx \arg \max_{s \in \Omega(z_k)} \Phi(z_k, s), \quad (29)$$

where $\Phi(z_k, s)$ denotes the attack-scenario operational value under scenario s , namely,

$$\Phi(z_k, s) = \Delta C^{op}(z_k, s) + \pi EENS^{atk}(z_k, s). \quad (30)$$

Accordingly, the robust objective value associated with z_k is approximated by

$$y_k = C^{inv}(z_k) + C^m(z_k) + Q^{base}(z_k) + \Phi(z_k, s_k^*). \quad (31)$$

The observed sample pair (z_k, y_k) is then added to the training dataset and used to update the surrogate model. By iteratively alternating between candidate-plan generation, decision-dependent attack construction, adversarial scenario search, and surrogate updating, DD-ABO progressively approaches the robust PV-BESS planning solution.

This process can be summarized as a nested search-and-evaluation framework: the outer loop explores the planning space, while the inner loop, conditioned on each candidate plan, searches for a high-impact attack realization. In this way, the optimization explicitly accounts for the fact that different PV deployment decisions induce different attack surfaces and, consequently, different worst-case operational consequences.

Random-Forest Surrogate and Acquisition Function

A random-forest (RF) surrogate is adopted to approximate the expensive black-box mapping from planning decision z to objective value $f(z)$. The RF surrogate is particularly suitable for the present problem because the planning vector contains mixed variable types, and the response surface may be highly nonlinear and nonsmooth due to operational constraints, scenario switching, and inner-loop adversarial search.

Let $t_m(z)$ denote the prediction of the m -th tree in an ensemble of M trees, and let $\bar{t}(z) = \frac{1}{M} \sum_{m=1}^M t_m(z)$ be the mean prediction. To account for the approximation uncertainty induced by finite training data and the inexact inner adversarial search, the predictive distribution is constructed by decomposing the total uncertainty into two components: model uncertainty arising from tree disagreement, and evaluation noise. The model uncertainty is estimated by the variance of the tree predictions:

$$\sigma_{\text{model}}^2(z) = \frac{1}{M-1} \sum_{m=1}^M (t_m(z) - \bar{t}(z))^2. \quad (32)$$

The evaluation noise σ_ϵ^2 is estimated from the out-of-bag residuals during RF training,¹ reflecting the inherent noise in the simulation-based evaluation. The total predictive distribution is then approximated as a Gaussian distribution:

$$Y(z) \sim \mathcal{N}(\bar{t}(z), \sigma_{\text{model}}^2(z) + \sigma_\epsilon^2). \quad (33)$$

This representation provides both a point prediction and an uncertainty estimate, enabling acquisition optimization in Bayesian optimization. The RF surrogate is retrained as new samples $\{(z_k, y_k)\}$ are collected, progressively improving its accuracy in the relevant regions of the planning space.

To determine the next planning decision to evaluate, the proposed framework uses the Expected Improvement (EI) acquisition function. Since the predictive distribution in (33) is Gaussian, a closed-form EI expression is available:

$$EI(z) = (f^* - \bar{t}(z)) \Phi\left(\frac{f^* - \bar{t}(z)}{\sigma(z)}\right) + \sigma(z) \phi\left(\frac{f^* - \bar{t}(z)}{\sigma(z)}\right), \quad (34)$$

where $\sigma(z) = \sqrt{\sigma_{\text{model}}^2(z) + \sigma_\epsilon^2}$, $f^* = \min_{1 \leq r \leq k} y_r$ is the best objective value observed so far, and $\Phi(\cdot)$ and $\phi(\cdot)$ denote the cumulative distribution function and probability density function of the standard normal distribution, respectively. Due to the mixed discrete-continuous nature of the planning space and the potential nonconvexity of the acquisition landscape, directly optimizing $EI(z)$ over $\mathcal{Z}$ is nontrivial. Instead, the next candidate is selected approximately over a finite candidate set $\mathcal{Z}_{\text{cand}} \subset \mathcal{Z}$:

$$z_{\text{next}} \approx \arg \max_{z \in \mathcal{Z}_{\text{cand}}} EI(z). \quad (35)$$

In practice, $\mathcal{Z}_{\text{cand}}$ is generated by combining random sampling with local perturbations around the current best solution. Through this acquisition mechanism, the algorithm balances exploitation by favoring plans with low predicted objective values and exploration by preferring those with high predictive uncertainty. Together with the decision-dependent adversarial inner search, this approach efficiently identifies robust PV-BESS planning decisions under attack-aware uncertainty.

Experiment Settings

The DD-ABO framework is tested on the IEEE 39-bus transmission system, which serves as a standard benchmark for transmission optimization. All buses are considered candidate locations for PV and BESS installation. To capture realistic operational dynamics, the annual load fluctuations, including both seasonal and diurnal patterns, are synthesized based on New England's 2025 load data³⁷ and mapped onto the IEEE 39-bus system. Similarly, the annual PV availability, represented by the capacity factor profile, is derived from New England's 2025 utility-scale solar data³⁸. Both the PV capacity factor and the load profile are shown in Fig. 3a, which provides hourly resolution data for the entire year. Parameter settings are provided in Supplementary Table S2. Under this configuration, all model constraints are enforced except those inherently satisfied by the simulation process.

Data availability

All data used are open (various licenses). Intermediate data are available via Zenodo at <https://zenodo.org/records/22130548>.

Code availability

The code for all algorithms (DD-ABO, DD-PSO, DD-GA, BO, and F-ABO), simulation and evaluation routines, and data analysis and figure generation is available via Zenodo at <https://zenodo.org/records/22130548>.

¹For each training sample i , let $\hat{y}_i^{\text{OOB}}$ be the average prediction of all trees for which i is out-of-bag. The noise variance is estimated as $\sigma_\epsilon^2 = \frac{1}{K} \sum_{i=1}^K (y_i - \hat{y}_i^{\text{OOB}})^2$, where K is the number of training samples.

References

- [1] K. Alberi, I. Peters, P. Verlinden *et al.*, “Historical and future learning for the new era of multi-terawatt photovoltaics,” *Nature Energy*, vol. 11, pp. 38–46, 2026.
- [2] F. J. M. M. Nijssse, J.-F. Mercure, N. Ameli *et al.*, “The momentum of the solar energy transition,” *Nature Communications*, vol. 14, no. 1, p. 6542, 2023.
- [3] International Energy Agency, “Solar PV,” <https://www.iea.org/energy-system/renewables/solar-pv>, 2024.
- [4] International Energy Agency, “Net Zero by 2050,” IEA, Paris, Data Product, 2021, License: Creative Commons Attribution CC BY-NC-SA 3.0 IGO. [Online]. Available: <https://www.iea.org/data-and-statistics/data-product/net-zero-by-2050-scenario>
- [5] A. S. Musleh, G. Chen, B. Liu *et al.*, “Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies,” *Cell Reports Physical Science*, vol. 7, no. 5, p. 103261, 2026.
- [6] F. Yang, Z. Dan, K. Pan *et al.*, “Rethink: Reveal the threat of electromagnetic interference on power inverters,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.
- [7] A. Barua and M. A. Al Faruque, “Hall spoofing: A Non-Invasive DoS attack on Grid-Tied solar inverter,” in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 1273–1290.
- [8] P. Paganini, “sPower it the first renewable energy provider hit by a cyber attack that caused communications outages,” Security Affairs, 2019. [Online]. Available: <https://securityaffairs.com/93271/hacking/spower-cyber-attack.html>
- [9] HotNews, “Fraudă cu panouri fotovoltaice: Unii prosumatori modifică ilegal setările invertorului și injectează mai multă electricitate în rețea / Ce soluții vede ANRE,” HotNews, 2023. [Online]. Available: <https://hotnews.ro/frauda-cu-panouri-fotovoltaice-unii-prosumatori-modifica-ilegal-setarile-invertorului-si-injecteaza-mai-multa-electricitate-n-retea-ce-solutii-vede-anre-26707>
- [10] CONTEC, “Reporting on cyber attacks on our remote monitoring equipment for solar power generation facilities,” CONTEC, 2024. [Online]. Available: <https://www.contec.com/jp/info/2024/2024050700/>
- [11] Cyble Research and Intelligence Labs (CRIL), “Solar Monitoring Solutions in Hacktivists’ Crosshairs,” Cyble Blog, 2024. [Online]. Available: <https://cyble.com/blog/solar-monitoring-solutions-in-hacktivists-crosshairs/>
- [12] CERT Polska, “Energy Sector Incident Report - 29 December 2025,” CERT Polska, Incident Report, 2025. [Online]. Available: <https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/>
- [13] Vedere Labs, “SUNDOWN: A Dark Side to Solar Energy Grids,” Forescout Research Labs, Research Report, 2025. [Online]. Available: <https://www.forescout.com/research-labs/sun-down-a-dark-side-to-solar-energy-grids/>
- [14] CyberNews, “35,000 solar power systems found exposed online, targeted by hackers,” CyberNews, 2025. [Online]. Available: <https://cybernews.com/security/thousands-solar-power-systems-exposed-and-vulnerable/>
- [15] N. L. Chang, M. Dehghanimadvar, and R. Egan, “The cost of risk mitigation—diversifying the global solar pv supply chain,” *Joule*, vol. 6, no. 12, pp. 2686–2688, 2022.
- [16] S. Chen, T. Zhang, H. B. Gooi *et al.*, “Penetration rate and effectiveness studies of aggregated BESS for frequency regulation,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 167–177, 2016.
- [17] L. Wang, F. Bai, R. Yan *et al.*, “Real-time coordinated voltage control of PV inverters and energy storage for weak networks with high PV penetration,” *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3383–3395, 2018.
- [18] S. Zou, Y. Cao, H. Zhang *et al.*, “Stochastic joint planning of energy storage and transmission for power system flexibility,” in *2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia)*, 2022, pp. 1356–1361.
- [19] L. He, Z. Tan, Y. Li *et al.*, “A coordinated consensus control strategy for distributed battery energy storages considering different frequency control demands,” *IEEE Transactions on Sustainable Energy*, vol. 15, no. 1, pp. 304–315, 2024.
- [20] D. Xu, Z. Zhang, Y. Ye *et al.*, “Multiagent-based model predictive control of parallel PV/BESS electric springs in microgrids,” *IEEE Transactions on Industrial Informatics*, vol. 21, no. 5, pp. 3616–3626, 2025.
- [21] B. Zhang, P. Dehghanian, and M. Kezunovic, “Optimal allocation of PV generation and battery storage for enhanced resilience,” *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 535–545, 2019.
- [22] P. L. Denholm, R. M. Margolis, and J. D. Eichman, “Evaluating the technical and economic performance of PV plus storage power plants,” National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2017.
- [23] V. Rallabandi, O. M. Akeyo, N. Jewell *et al.*, “Incorporating battery energy storage systems into multi-MW grid connected PV systems,” *IEEE Transactions on Industry Applications*, vol. 55, pp. 638–647, 2019.
- [24] A. H. Schleifer, C. A. Murphy, W. J. Cole *et al.*, “The evolving energy and capacity values of utility-scale PV-plus-battery hybrid system architectures,” *Adv. Appl. Energy*, vol. 2, no. 26, 2021.
- [25] B. Trivić and A. Savić, “Optimal allocation and sizing of BESS in a distribution network with high PV production using NSGA-II and LP optimization methods,” *Energies*, vol. 18, no. 5, 2025.
- [26] I. Ranaweera and O.-M. Midtgård, “Optimization of operational cost for a grid-supporting PV system with battery storage,” *Renewable Energy*, vol. 88, pp. 262–272, 2016.
- [27] E. Gul, G. Baldinelli, P. Bartocci *et al.*, “A techno-economic analysis of a solar PV and DC battery storage system for a community energy sharing,” *Energy*, vol. 244, p. 123191, 2022.
- [28] A. Chen, Y. N. Velaga, J. Ausmus *et al.*, “Optimization of large-scale battery energy storage applications in transmission system,” in *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2020, pp. 1–5.
- [29] J. Zhao, Q. Zhai, Y. Zhou *et al.*, “Adaptive characteristic modeling of long-period uncertainties: A multi-stage robust energy storage planning approach based on the finite covering theorem,” *IEEE Transactions on Sustainable Energy*, vol. 15, no. 4, pp. 2393–2404, 2024.
- [30] Y. Qiu, Q. Li, T. Wang *et al.*, “Optimal planning of cross-regional hydrogen energy storage systems considering the uncertainty,” *Applied Energy*, vol. 326, p. 119973, 2022.
- [31] X. Wang, Y. Jin, S. Schmitt *et al.*, “Recent advances in bayesian optimization,” *ACM Computing Surveys*, vol. 55, pp. 1 – 36, 2022.
- [32] N. Palm, M. Landerer, and H. Palm, “Gaussian process regression based multi-objective bayesian optimization for power system design,” *Sustainability*, vol. 14, no. 19, 2022.
- [33] K. Kumar, A. A. Mantha, and G. Ravikumar, “Bayesian optimization for deep reinforcement learning for robust volt-var control,” in *2024 IEEE Power & Energy Society General Meeting (PESGM)*, 2024, pp. 1–5.
- [34] F. Hutter, H. H. Hoos, and K. Leyton-Brown, “Sequential model-based optimization for general algorithm configuration,” in *International conference on learning and intelligent optimization*. Springer, 2011, pp. 507–523.
- [35] California Independent System Operator (CAISO), “What the Duck Curve Tells Us About Managing a Green Grid,” 2013. [Online]. Available: https://www.caiso.com/documents/flexibleresourceshelprenewables_fastfacts.pdf
- [36] P. Denholm, M. O’Connell, G. Brinkman *et al.*, “Overgeneration from solar energy in California: A field guide to the duck chart,” *National Renewable Energy Laboratory (NREL)*, no. NREL/TP-6A20-65023, 2015.
- [37] ISO New England, “Real-Time System Demand: Hourly System Demand Data,” ISO New England ISO Express Web Reports, 2026. [Online]. Available: <https://www.iso-ne.com/isoexpress/web/reports/load-and-demand/-/tree/dmnd-rt-hourly-sys>
- [38] ISO New England, “Daily Generation by Fuel Type,” ISO New England ISO Express Web Reports, 2026. [Online]. Available: <https://www.iso-ne.com/isoexpress/web/reports/operations/-/tree/daily-gen-fuel-type>

- [39] D. Tong, D. J. Farnham, L. Duan *et al.*, “Geophysical constraints on the reliability of solar and wind power worldwide,” *Nature communications*, vol. 12, no. 1, pp. 1–12, 2021.
- [40] J. Kennedy and R. C. Eberhart, “Particle swarm optimization,” in *Proceedings of ICNN’95 - International Conference on Neural Networks*, vol. 4. IEEE, 1995, pp. 1942–1948.
- [41] J. H. Holland, *Adaptation in Natural and Artificial Systems*. Ann Arbor, MI: University of Michigan Press, 1975.
- [42] M. Jalali, S. Taheri, and V. Kekatos, “Strategic investment in energy markets using bayesian optimization,” in *2023 IEEE Power & Energy Society General Meeting (PESGM)*, 2023, pp. 1–5.
- [43] V. Selicati, A. Jahanbin, and U. Berardi, “Bayesian multi-criteria decision-making for optimal capacity planning of district-scale multi-vector energy hubs,” *Sustainable Energy Technologies and Assessments*, vol. 91, p. 105082, 2026.
- [44] A. J. Albarakati, “Influence of generation and load variations in the vulnerability of power systems,” *Journal of Electrical Engineering & Technology*, vol. 16, pp. 2397 – 2406, 2021.
- [45] A. A. Ganin, E. Massaro, A. Gutfraind *et al.*, “Operational resilience: concepts, design and analysis,” *Scientific Reports*, vol. 6, no. 1, p. 19540, Jan 2016.
- [46] A. D. Broido and A. Clauset, “Scale-free networks are rare,” *Nature Communications*, vol. 10, no. 1, p. 1017, 2019.
- [47] R. Albert, H. Jeong, and A.-L. Barabási, “Error and attack tolerance of complex networks,” *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.
- [48] S. V. Buldyrev, R. Parshani, G. Paul *et al.*, “Catastrophic cascade of failures in interdependent networks,” *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.
- [49] Y. Wang, R. Wang, K. Tanaka *et al.*, “Accelerating the energy transition towards photovoltaic and wind in china,” *Nature*, vol. 619, pp. 761–767, 2023.
- [50] Y. Liu, M. Liu, W. Ma *et al.*, “Enhancing cyber resilience of high-renewable power systems: Threat pathways and targeted countermeasures,” *The Innovation Energy*, vol. 3, p. 100169, 2026.
- [51] N. Rodríguez-Pérez, J. Matanza, L. Sigrist *et al.*, “MaDioT 3.0: Assessment of attacks to distributed energy resources and demand in a power system,” *IEEE Open Access Journal of Power and Energy*, vol. 12, pp. 552–563, 2025.
- [52] S. Soltan, P. Mittal, and H. V. Poor, “BlackIoT: IoT botnet of high wattage devices can disrupt the power grid,” in *Proceedings of the 27th USENIX Security Symposium*. Baltimore, MD, USA: USENIX Association, Aug. 2018, pp. 15–32.
- [53] T. Shekari, A. A. Cardenas, and R. Beyah, “MaDioT 2.0: Modern high-wattage IoT botnet attacks and defenses,” in *Proceedings of the 31st USENIX Security Symposium*. Boston, MA, USA: USENIX Association, Aug. 2022, pp. 3539–3556.
- [54] C. Li, T. Zang, and B. Zhou, “Multi-stage robust optimization of reliability improvement for power transmission cyber-physical systems under sequential coordinated attacks: an extreme attack scenario search-assisted framework,” *Reliability Engineering & System Safety*, vol. 273, p. 112319, 2026.
- [55] B. Yang and Z. Zhao, “Energy storage overcapacity can cause power system instability and blackouts, too,” *Nature*, vol. 633, no. 8029, p. 286, Sep. 2024.
- [56] J. R. L. Senga, A. Botterud, J. E. Parsons *et al.*, “Implications of policy-driven transmission expansion for costs, emissions and reliability in the USA,” *Nature Energy*, vol. 11, no. 2, pp. 230–243, Feb. 2026.
- [57] T. Levin, J. Bistline, R. Sioshansi *et al.*, “Energy storage solutions to decarbonize electricity through enhanced capacity expansion modelling,” *Nature Energy*, Sep. 2023.
- [58] L. Qiu, R. Khorramfar, S. Wang *et al.*, “Climate change reshapes resource adequacy risks and optimal renewable energy siting in wind and solar energy systems,” *Nature Energy*, pp. 1–10, 2026.
- [59] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power generation, operation, and control*. John Wiley & sons, 2013.
- [60] Cyble Research Labs, “Photovoltaic Plants (PV) Facing Risk of Cyberattack,” Cyble Blog, 2022. [Online]. Available: <https://cyble.com/blog/photovoltaic-plants-pv-facing-risk-of-cyberattack/>

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 62293503, 62293500, 62293502; in part by the Frontier Technologies R&D Program of Jiangsu under Grant BF2024065; in part by the State Key Laboratory of Industrial Control Technology under Grant ICT2024A13, ICT2025C04; in part by the Xiaomi Foundation; and in part by the Fundamental Research Funds for the Central Universities under Grant 226-2025-00165.

Author contributions

Conceptualization: all authors. Methodology: Y.L. and B.X. Data curation: Y.L. Software and formal analysis: Y.L. Writing—original draft preparation: Y.L. Writing—review and editing: all authors. Supervision: R.D., M.L. and S.Z. Funding acquisition: P.C. and J.C. All authors have read and approved the final version of the manuscript.

Competing interests

The authors declare no competing financial or non-financial interests.

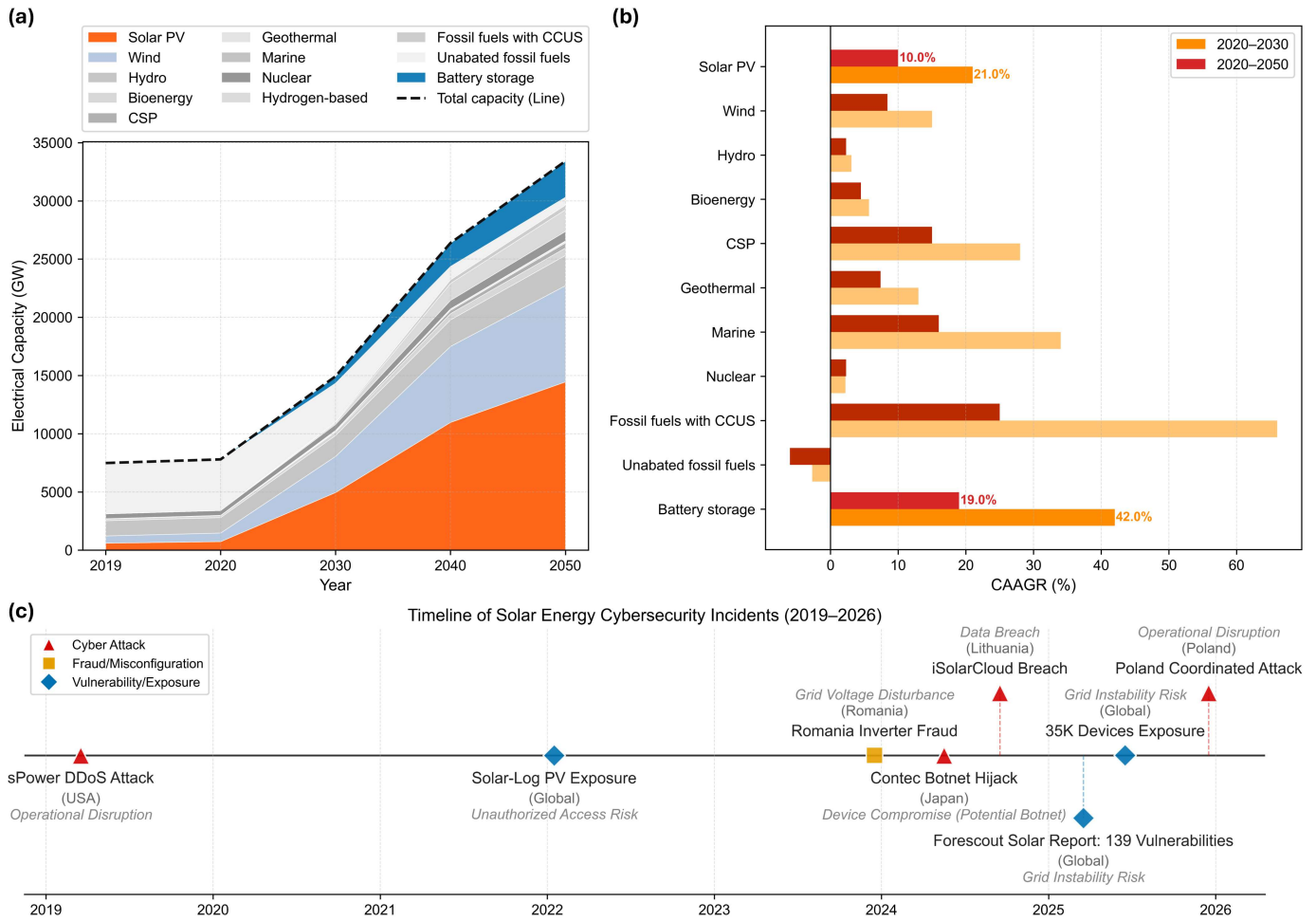


Fig. 1. **Projected solar PV dominance and the parallel rise of cyber-physical security risks.** **a** Global installed electrical capacity by technology, 2019–2050. The black dashed line represents total installed capacity across all technologies. Bioenergy includes bioenergy with carbon capture and storage (BECCS). Fossil fuels with carbon capture, utilization and storage (CCUS) include coal with CCUS and natural gas with CCUS. Unabated fossil fuels include coal, natural gas and oil. Data from the IEA Net Zero by 2050 Scenario⁴. **b** CAAGR of electrical capacity by technology, 2019–2050, with the same technology definitions as in **a**. Data from the IEA Net Zero by 2050 Scenario⁴. **c** Major cybersecurity incidents affecting solar energy infrastructure, 2019–2026^{8–14,60}. Red triangles, orange squares, and blue diamonds denote cyber attack events, fraud or misconfiguration events, and reported vulnerabilities or device exposures, respectively.

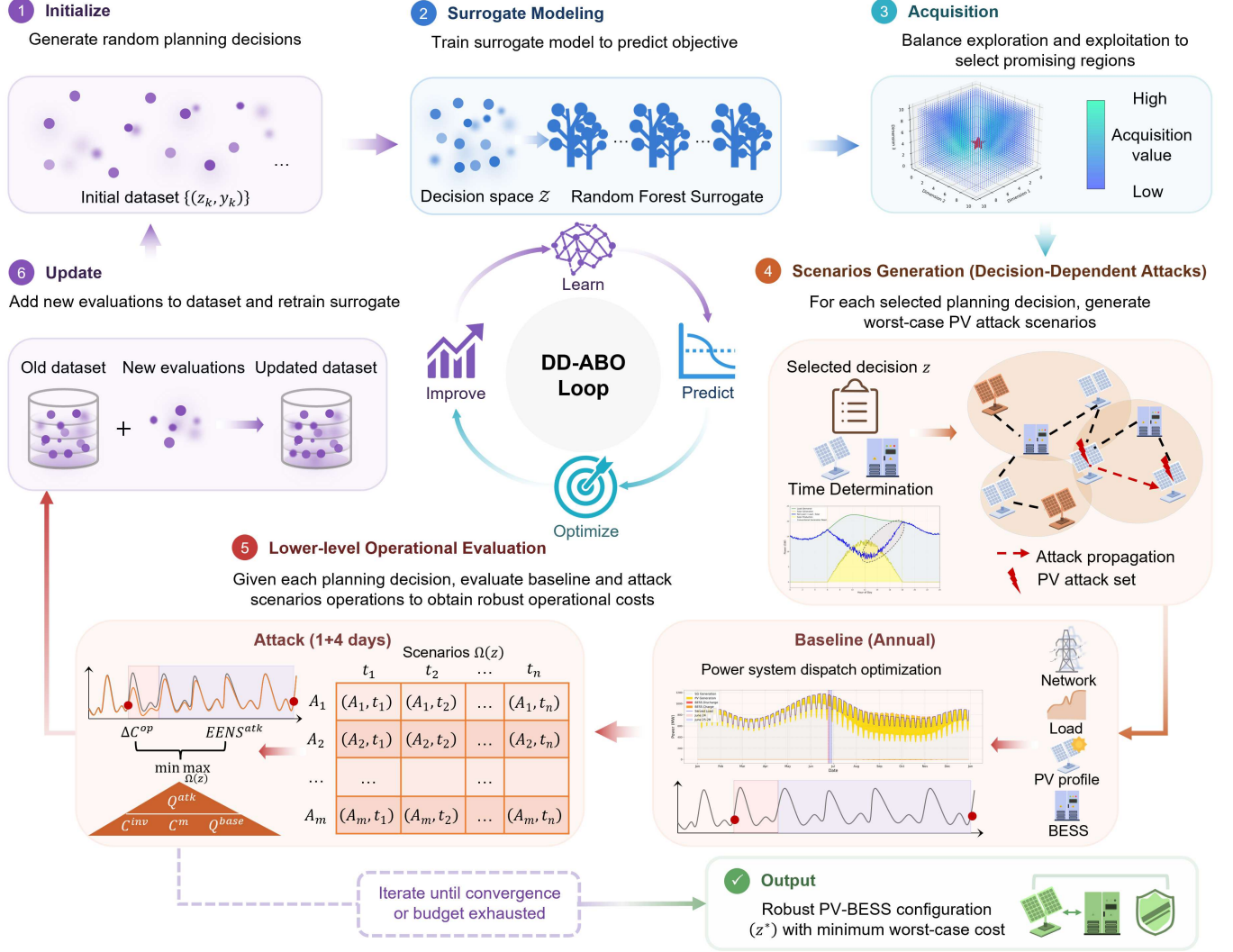


Fig. 2. **Decision-Dependent Adversarial Bayesian Optimization (DD-ABO) framework for robust PV-BESS planning.** The framework sequentially integrates random-forest surrogate modelling and acquisition-based sampling (Steps 1–3) to explore the planning space, followed by decision-dependent attack scenario generation (Step 4) and lower-level operational evaluation under both baseline and PV attack conditions (Step 5). In Step 4, for each candidate planning decision z , the PV attack set $\mathcal{A}$ is constructed based on the installed PV units, with attack timing selected along the duck curve ramp^{35,36}. Step 5 first performs a full-year baseline simulation (8760 hours) to obtain the baseline trajectories of all generators, BESS state of charge, and PV outputs, yielding the baseline operating cost $Q^{base}(z)$. For each PV attack scenario, a shorter-horizon simulation (attack day plus four recovery days) is then executed, with initial and terminal states constrained to match the corresponding baseline trajectories at the start and end of the attack time window. The lower-level adversarial search identifies the worst-case PV attack scenario for each z , and the corresponding worst-case additional cost $Q^{atk}(z)$ is obtained by solving $\min_u \max_{s \in \Omega(z)} \{\Delta C^{op}(z, s) + \pi EENS^{atk}(z, s)\}$. The overall objective for planning decision z is then $y(z) = C^{inv}(z) + C^m(z) + Q^{base}(z) + Q^{atk}(z)$. The upper-level minimizes $y(z)$ over the planning space, and the observed sample (z, y) updates the surrogate. The iteration continues until convergence or budget exhaustion, ultimately outputting the robust configuration $z^* = \arg \min_z y(z)$.

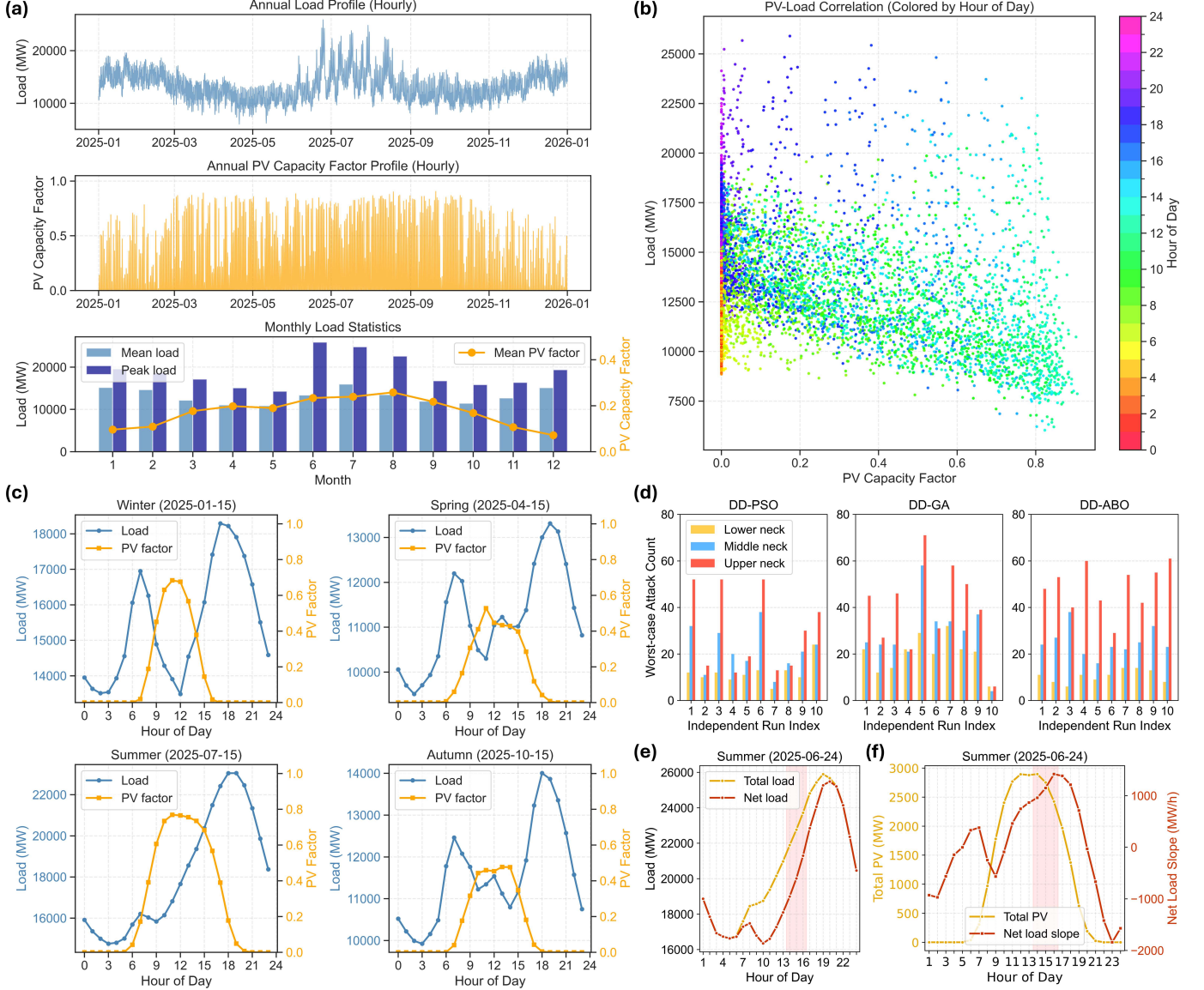


Fig. 3. Temporal characterization of load and PV profiles and identification of the optimal timing for PV curtailment attacks on the IEEE 39-bus system driven by real-world New England data. Based on 2025 load and utility-scale solar data from New England^{37,38}, **a** shows the annual hourly load and PV capacity factor profiles alongside monthly statistics comprising mean load, peak load and mean PV factor. **b** A scatter plot of PV-load correlations coloured by the hour of the day. **c** Illustrates the hourly load and PV factor variations across four representative seasonal days. **d** Presents the neck-interval distribution of worst-case PV attacks across 10 independent runs with 200 evaluations each for three Decision-Dependent algorithms, DD-PSO, DD-GA and DD-ABO. The total counts in each run below 200, as overly aggressive planning decisions render the base case infeasible and preclude attack execution, whereas conservative decisions invalidate all attack attempts. **e**, **f** Further deconstruct 24 June 2025, which represents the annual peak system load day, by depicting the hourly total load and net load, defined as total load minus total PV output, in **e** and plotting the hourly total PV output and net load slope in **f**. The red-shaded regions in **e** and **f** highlight the three-hour duck neck intervals comprising the lower neck, middle neck and upper neck.

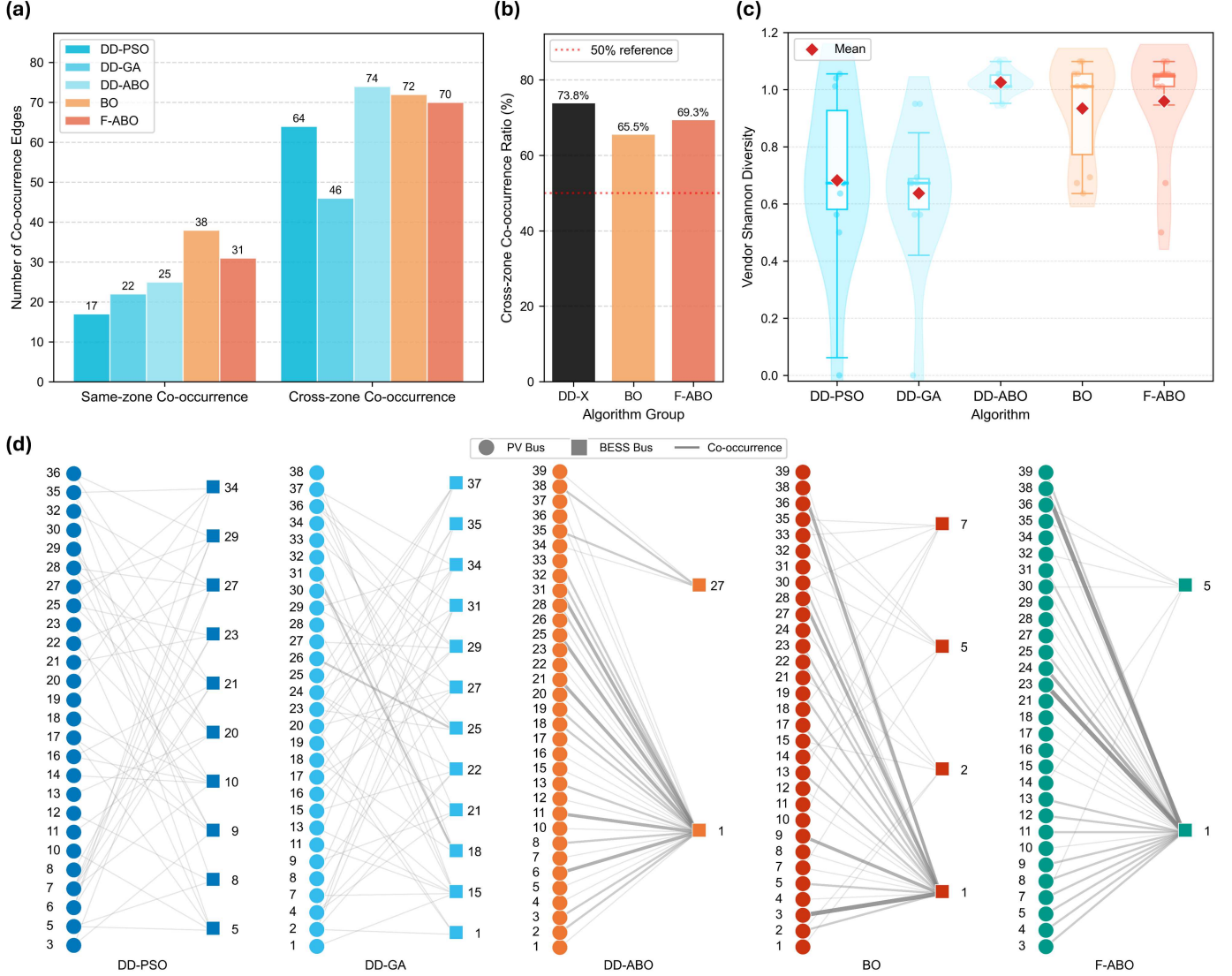


Fig. 4. Characterization of the control-domain and vendor diversity of PV installations, alongside the spatial co-occurrence patterns between PV and BESS units, in the final planning decisions of different algorithms. **a**, Same-zone and cross-zone control-domain distributions of the PV installations within each final planning decision, showing that DD-family algorithms consistently yield significantly higher numbers of cross-zone control-domain connections. **b**, Cross-zone integration ratio of the final planning decisions across DD-X group, BO and F-ABO, defined as the percentage of cross-zone co-occurrence edges over the total co-occurrence edges, with a 50% reference line. **c**, Distributions of vendor Shannon diversity computed for the planned PV installations in each final planning decision, with the mean values marked by red diamonds and the interquartile ranges indicated by the box-and-whisker overlays. **d**, Network visualizations of the co-occurrence of installed PV and BESS positions aggregated from the final planning decisions of the five algorithms, where an edge represents the co-installation of a PV unit on the left-side bus and a BESS unit on the right-side bus within a planning decision.

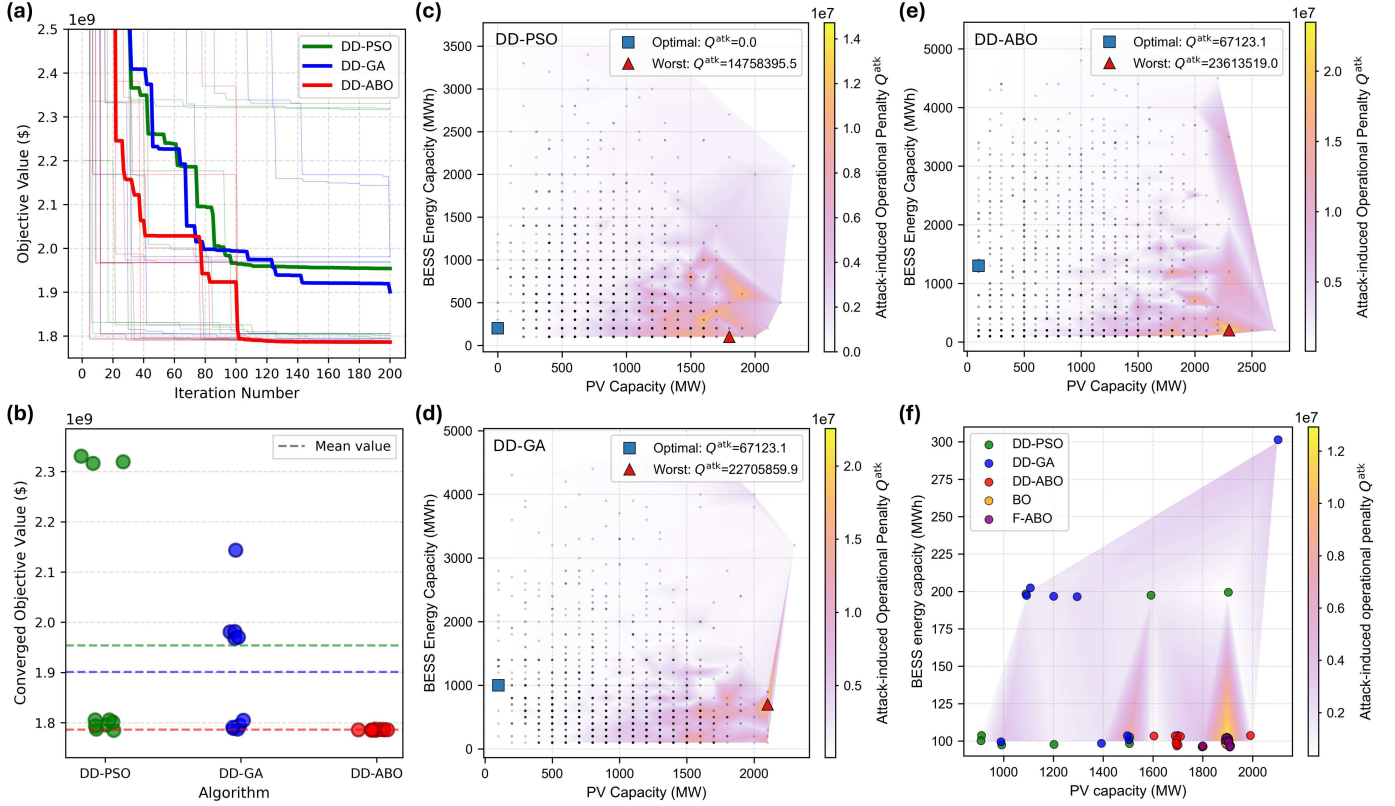


Fig. 5. Comparative assessment of Decision-Dependent (DD) attack algorithms, denoted as DD-X, in convergence performance and solution stability, and their planning-decision vulnerability against adversarial PV curtailment attacks as compared to F-ABO and attack-agnostic BO. **a** Convergence trajectories of objective values over 200 iterations for DD-PSO, DD-GA and DD-ABO. **b** Scatter distributions of the converged objective values across independent runs, where the dashed lines denote the mean values for each algorithm. **c–e** Spatial heatmaps showing the attack-induced operational penalty Q^{atk} against the total installed PV and BESS capacities corresponding to the intermediate planning decision z at each evaluation for DD-PSO, DD-GA and DD-ABO, respectively. The black dots in **c–e** denote the coordinates (P^{PV}, E^{BESS}) of all intermediate planning decisions z evaluated during the optimization process. **f** Heatmap of the attack-induced operational penalty Q^{atk} overlaid with the scatter points representing the final optimal planning decision z^* obtained in each of the 10 independent runs for DD-PSO, DD-GA, DD-ABO, BO and F-ABO. For the heatmaps in **c–f**, in cases where multiple data points share identical (P^{PV}, E^{BESS}) coordinates, the color mapping is determined by the highest Q^{atk} value among them, ensuring the most conservative (worst-case) penalty is visualized. BO and F-ABO are not inherently equipped with Q^{atk} during the optimization process, as BO does not consider the PV attack model at all and F-ABO adopts only fixed PV attack sets. Their Q^{atk} values are consequently computed in a post-hoc manner using the adversarial modelling approach of the DD-X algorithms.

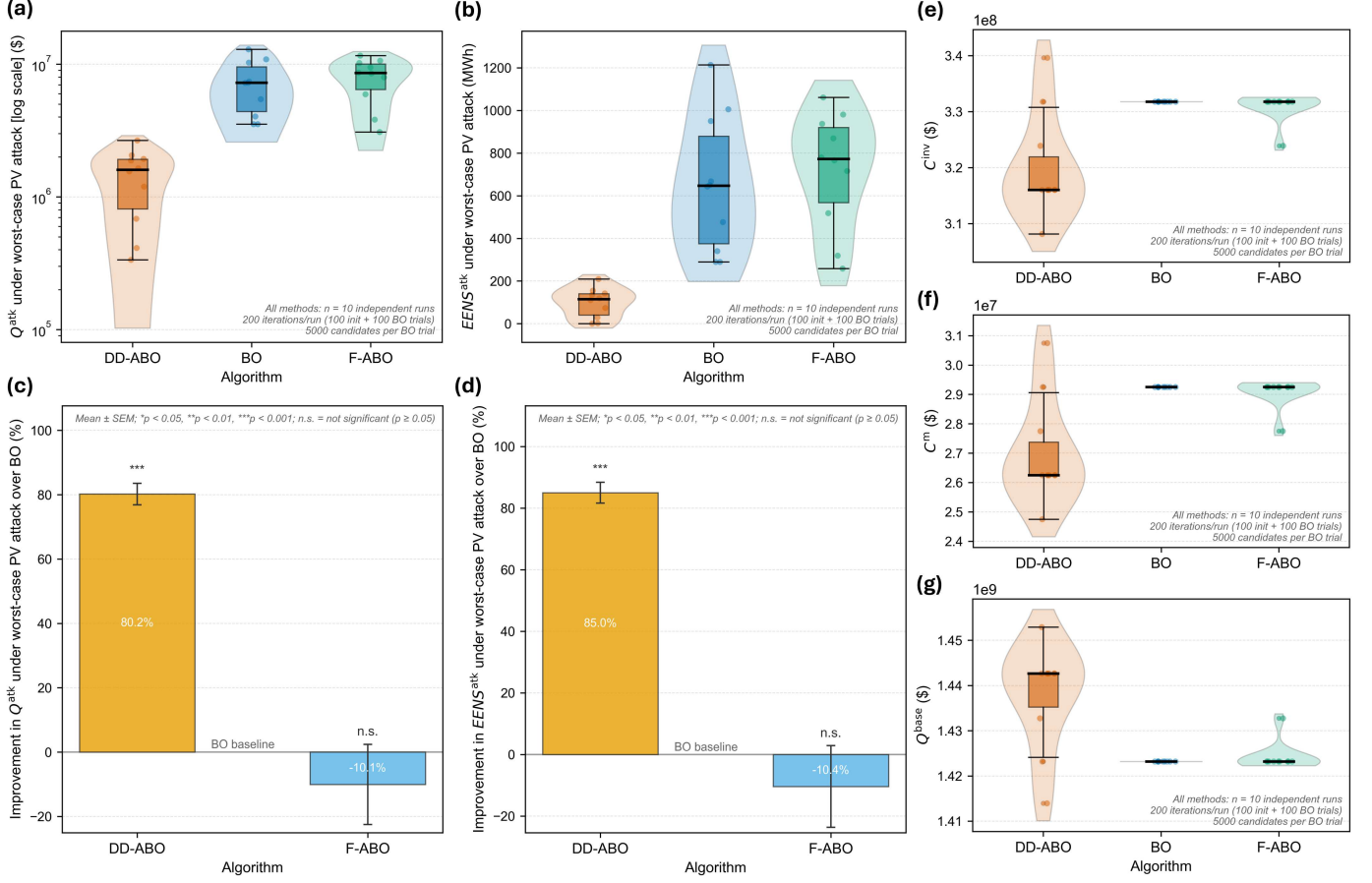


Fig. 6. **Performance comparison of DD-ABO, BO and F-ABO under worst-case PV attacks and base-case conditions.** **a** Distribution of attack-induced operational penalties Q^{atk} under worst-case PV attacks across independent runs. **b** Distribution of the expected energy not served $EENS^{atk}$ under the same attack scenarios. **c, d** Percentage improvements of DD-ABO and F-ABO in Q^{atk} and $EENS^{atk}$ over the BO baseline, with statistical significance indicated by asterisks. **e-g** Distributions of annualized capital investment cost C^{inv} , fixed maintenance cost C^m and base-case operational cost Q^{base} for the three algorithms. All figures are based on $n = 10$ independent runs with 200 evaluations per run.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [Supplementarymaterial.pdf](#)