Preventing Outages under Coordinated Cyber-Physical Attack with Secured PMUs

Yudi Huang, *Student Member, IEEE*, Ting He, *Senior Member, IEEE*, Nilanjan Ray Chaudhuri, *Senior Member, IEEE*, and Thomas La Porta *Fellow, IEEE*

***Abstract*—Due to the potentially severe consequences of coordinated cyber-physical attacks (CCPA), the design of defenses has gained significant attention. A popular approach is to eliminate the existence of attacks by either securing existing sensors or deploying secured PMUs. In this work, we improve this approach by lowering the defense target from *eliminating attacks* to *preventing outages* and reducing the required number of PMUs. To this end, we formulate the problem of *PMU Placement for Outage Prevention (PPOP)* under DC power flow model as a tri-level non-linear optimization problem and transform it into a bi-level mixed-integer linear programming (MILP) problem. Then, we propose an alternating optimization framework to solve PPOP by iteratively adding constraints, for which we develop two constraint generation algorithms. In addition, for large-scale grids, we propose a polynomial-time heuristic algorithm to obtain suboptimal solutions. Next, we extend our solution to achieve the defense goal under AC power flow model. Finally, we evaluate our algorithm on IEEE 30-bus, 57-bus, 118-bus, and 300-bus systems, which demonstrates the potential of the proposed approach in greatly reducing the required number of PMUs.**

I. Introduction

Coordinated cyber-physical attacks (CCPA) [2] have gained a great deal of attention due to the stealthiness of such attacks and the potential for severe damage on to the smart grid. The power of CCPA is that its physical component damages the grid while its cyber component masks such damage from the control center (CC) to prolong outages and potentially enable cascades. For instance, in the Ukrainian power grid attack [3], attackers remotely switched off substations (damaging the physical system) while disrupting the control through telephonic floods and KillDisk server wiping (damaging the cyber system).

Defenses against CCPA can be broadly categorized into *detection* and *prevention*. Attack detection mechanisms aim at detecting attacks that are otherwise undetectable using traditional bad data detection (BDD) by exploiting knowledge unknown to the attacker [4]. However, the knowledge gap between the attacker and the defender may disappear due to more advanced attacks, and relying on detection alone risks severe consequences in case of misses. Therefore, in this work, we focus on preventing attacks using secured sensors.

We consider a powerful attacker with full knowledge of the pre-attack state of the grid and the locations of secured PMUs. The attacker launches an optimized CCPA where the physical attack disconnects a limited number of lines and the cyber attack falsifies the breaker status and the measurements from unsecured sensors to mask the physical attack while misleading security constrained economic dispatch (SCED) at the CC. Such attacks can result in severe cascading failures. For example, under the setting in Section V, CCPA in absence of secured PMUs can cause initial overload-induced tripping at 2, 1, and 2 lines in IEEE 30-bus, 57-bus, and 118-bus systems, respectively. Moreover, the re-distribution of power flows on the initially tripped lines may cause cascading outages. Take IEEE 118-bus system as an example. There is an attack that physically disconnects line 144 and manipulates the measurements to cause overload-induced tripping at line 109. These initial outages will trigger a cascade that eventually results in outages at 82 lines. This observation highlights the importance of defending against such attacks.

While attack prevention traditionally aims at eliminating undetectable attacks by deploying secured PMUs to achieve full observability [5], this approach can require a large number of PMUs. Little is known about how to achieve a good tradeoff between the efficacy of protection and the cost of PMU placement during the deployment process before full observability is achieved. In addition, the operators may be only interested in using secured PMUs to prevent severe consequences, while leaving the defense of less severe attacks to other mechanisms [6]. To fill this gap, we lower the goal of PMU placement to *preventing undetectable attacks from causing outages*. Specifically, we want to deploy the minimum number of secured PMUs such that the attacker will not be able to cause overload-induced line tripping due to overcurrent protection devices. The key novelty of our approach is that we allow undetectable attacks to exist but prevent them from causing any outages, hence potentially requiring fewer secured PMUs. For instance, we can prevent overload-induced tripping using 71% fewer secured PMUs compared to the requirement of full observability in IEEE 118-bus system.

A. Related Work

Attacks: False data injection (FDI) [7], [8] is widely adopted to launch cyber attacks in CCPA to bypass the traditional BDD [2]. A typical form of FDI is load redistribution attack [9], which together with physical attacks [2], [10], [11] that alter grid topology, aims to mislead SCED by injecting false data for economic loss or severe physical consequences such as sequential outages [11]. Bi-level optimization is widely adopted for analyzing the impact of CCPA on state deviation [12] or line flow changes [13]. In this work, we extend them

The authors are with the School of Electrical Engineering and Computer Science, Pennsylvania State University, University Park, PA 16802, USA (e-mail: {yxh5389, tzh58, nuc88, tfl12}@psu.edu).

A preliminary version of this work was presented at SmartGridComm'21 [1].

This work was supported by the National Science Foundation under award ECCS-1836827.

into a stronger attacker that jointly optimizes the location of physical attacks and the attack target. Besides misleading SCED, similar physical consequences can also be achieved by attacking the commands issued by the control center [14], [15], which is not the focus of this work.

Defenses: Defending against CCPA requires a systematic mechanism [6], which can be decomposed into three modules: *prevention* that postpones the onset of attacks [10], *detection* that identifies the attack before it starts affecting the system [5], [14], [16]–[21], and *resilience* which limits the impact of the attacks that successfully bypass the detection [18], [22]–[24]. Our focus is on an intermediate stage of PMU deployment where not enough PMUs are installed to achieve perfect detection of all FDI attacks.

To eliminate the existence of FDI by detection, different strategies have been studied, such as directly protecting meters [16]–[20], [25] or deploying secured PMUs [5], [21]. Due to the connection between observability of the grid and FDI [17], solutions on achieving full observability through PMUs [26] can also be leveraged to defend against FDI. Unlike the aforementioned works, our work only aims to prevent attacks from causing outages, which can significantly reduce the required number of secured PMUs while maintaining the system *resilience*.

Tri-level optimization is widely used for modeling interactions among the defender, the attacker and the operator in smart grid. To name a few, a tri-level model is proposed in [23] to find the optimal set of lines to protect from physical attacks to minimize load shedding. In [18], [22], [24], the measurements to protect were chosen by solving a budget-constrained optimization problem, which was also adopted in [27] for distribution networks. However, existing works are limited in the following aspects. From the formulation perspective, their solution may become sub-optimal if the cost vector in SCED changes due to the dependence of their methods on the KKT conditions of linear programming. Such dependence also limits the extension of their formulation to the AC power flow model. From the computational perspective, the method in [18] solves a MIP for each possible physical attack and thus is not scalable to multi-line physical attacks. The method in [23] introduces bilinear terms, which leads to a high computational cost. To overcome such limitations, we will develop a formulation for CCPA that can (i) model multi-line physical attacks without bilinear terms, and (ii) be extended to the AC power flow model. Moreover, the PMU placement obtained from our solution can prevent overloading-induced line tripping regardless of the cost vector in SCED. Furthermore, securing PMU measurements instead of (legacy) measurements for individual nodes/lines has the advantage that it aligns with the ongoing trend of deploying PMU-based power grid monitoring systems.

Power flow models: Due to the nonlinear and nonconvex nature of AC power flow equations, it is a common practice [28] to develop FDI/CCPA or its countermeasure under the DC power flow model and validate the solutions under the AC power flow model. Although much efforts [29]–[31] have been devoted into directly formulating FDI under the AC model, most of them targeted at causing erroneous state estimation, with very limited results on load redistribution attack aiming at causing outages. The works [29] formulated FDI under the AC model through convex relaxation, but did not accurately model the impact of FDI on SCED. In [25], [28], [32], the design of FDI was based on the DC model, although the feasibility of the attack was tested under the AC model. In [30], [31], a formulation based on convex relaxation was proposed to model load redistribution attack under the AC model. They adopted DC-based *line outage distribution factors (LODF)* to infer the impact of attacks on SCED, which leads to the use of active power flows as the criterion to determine overloading. This is inaccurate as the true criterion should be the magnitude of current. To the best of our knowledge, it remains an open problem to compute the optimal load redistribution attack under the AC power flow model. Our approach is to circumvent this problem by (i) first finding a PMU placement to prevent load redistribution attack from causing outages under the DC model, (ii) then developing a method to test the feasibility of the found PMU placement under the AC model based on a recently developed approximation of AC power flow equations [33], and (iii) finally refining the PMU placement to prevent outages under the AC model.

B. Summary of Contributions

We summarize our contributions as follows:

1) Instead of eliminating the existence of FDI, we investigate the optimal secured *PMU Placement for Outage Prevention (PPOP)* problem to defend against CCPA, where we formulate a strong attacker that jointly optimizes physical attack locations and target lines. The proposed approach can potentially require fewer PMUs than approaches that eliminate FDI.
2) We propose an alternating optimization algorithm to solve PPOP by generating additional constraints from each infeasible PMU placement. Specifically, we demonstrate how to generate "No-Good" constraints and "Attack-Denial" constraints to solve PPOP optimally.
3) We develop a heuristic algorithm for PPOP to produce a possibly suboptimal solution. The complexity of the proposed heuristic is polynomial in the grid size, which makes it scalable to large networks.
4) We develop an algorithm to test whether a given PMU placement can achieve our defense goal under the AC power flow model. In addition, we propose a heuristic to augment the given PMU placement to pass the test.
5) We systematically evaluate the proposed solution on IEEE 30-bus, IEEE 57-bus, IEEE 118-bus, and IEEE 300-bus systems. The results demonstrate that the proposed solution can substantially reduce the number of required PMUs while preventing CCPA from causing outages, even with the AC-based augmentation.

Roadmap: We formulate the PPOP problem under the DC model in Section II and present both optimal algorithms and heuristics to solve PPOP in Section III. We then show how the DC-based solution can be refined to work under the AC model in Section IV. We evaluate the performance of PPOP in Section V and conclude the paper in Section VI. Additional contents and proofs are given in the appendices.

II. Problem formulation

Notations: For a matrix $\boldsymbol{A}$, we denote by $\boldsymbol{a}_i$ its i-th column and $\boldsymbol{A}_k$ its k-th row. We slightly abuse the notation $|\cdot|$ in that $|A|$ indicates the cardinality if A is a set and the element-wise absolute value if A is a vector or matrix. Logical expression $\leftrightarrow$ indicates the "if and only if" logic, while $\rightarrow$ denotes the "if then" logic. When the operators $\geq, \leq, =$ are applied to two vectors, they indicate element-wise operations. Let $\boldsymbol{a} \in \mathbb{R}^{n_a}, \boldsymbol{b} \in \mathbb{R}^{n_b}$ be two vectors, then $\boldsymbol{a} \oplus \boldsymbol{b} \in \mathbb{R}^{n_a+n_b}$ indicates the vertical concatenation of $\boldsymbol{a}$ and $\boldsymbol{b}$. Let $\lceil \boldsymbol{a} \rceil$ denote the element-wise ceiling. If $n_a = n_b = n$, then $\boldsymbol{a} \odot \boldsymbol{b} := (a_i b_i)_{i=1}^n$ denotes the Hadamard product, i.e., the element-wise product. We use $\boldsymbol{\Lambda}_{(\cdot)} \in \{0,1\}^{m \times n}$ with one nonzero element in each row to select entries from a vector such that $\boldsymbol{\Lambda}_{(\cdot)}\boldsymbol{x}$ is a subvector of $\boldsymbol{x}$.

A. Power Grid Modeling

We model the power grid as a connected undirected graph $\mathcal{N} = (V, E)$, where E denotes the set of lines (lines) and V the set of nodes (buses). Majority of our results will be based on the DC power flow model, which is an approximation widely adopted for studying security issues in power grids [2], [5], [9]–[13], [18]; extension to the AC power flow model is deferred to Section IV. Under this approximation, each line $e = (s,t)$ is characterized by reactance $r_e = r_{st} = r_{ts}$. The grid topology can be represented by the *admittance matrix* $\boldsymbol{B} := (B_{uv})_{u,v \in V} \in \mathbb{R}^{|V| \times |V|}$, defined as

$$B_{uv} = \begin{cases} 0 & \text{if } u \neq v, (u,v) \notin E, \\ -1/r_{uv} & \text{if } u \neq v, (u,v) \in E, \\ -\sum_{w \in V \setminus \{u\}} B_{uw} & \text{if } u = v. \end{cases} \tag{1}$$

Besides $\boldsymbol{B}$, the grid topology can also be described by *incidence matrix* $\boldsymbol{D} \in \{-1, 0, 1\}^{|V| \times |E|}$, which is defined as follows:

$$D_{ij} = \begin{cases} 1 & \text{if line } e_j \text{ comes out of node } v_i, \\ -1 & \text{if line } e_j \text{ goes into node } v_i, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

where the orientation of each line is assigned arbitrarily. By defining $\boldsymbol{\Gamma} \in \mathbb{R}^{|E| \times |E|}$ as a diagonal matrix with diagonal entries $\Gamma_e = \frac{1}{r_e}$ ($e \in E$), we have $\boldsymbol{B} = \boldsymbol{D}\boldsymbol{\Gamma}\boldsymbol{D}^T$ and $\boldsymbol{f} = \boldsymbol{\Gamma}\boldsymbol{D}^T\boldsymbol{\theta} \in \mathbb{R}^{|E|}$ where $\boldsymbol{f}$ denotes the line flows. By defining network states as phase angles $\boldsymbol{\theta} := (\theta_u)_{u \in V}$ and active powers as $\boldsymbol{p} = (p_u)_{u \in V}$, the relationship between $\boldsymbol{p}, \boldsymbol{\theta}$ and $\boldsymbol{f}$ is given as

$$\boldsymbol{p} = \boldsymbol{B}\boldsymbol{\theta} = \boldsymbol{D}\boldsymbol{f}, \tag{3}$$

The CC will periodically conduct state estimation, whose results will be used for SCED to re-plan the power generation [9], [11]. Formally, let $\boldsymbol{z} = [\boldsymbol{z}_N^T, \boldsymbol{z}_L^T]^T \in \mathbb{R}^m$ denote the unsecured meter measurements, where $\boldsymbol{z}_N \in \mathbb{R}^{m_N}$ denotes the power injection measurements over (a subset of) nodes and $\boldsymbol{z}_L \in \mathbb{R}^{m_L}$ denotes the power flow measurements over (a subset of) lines. Let $\boldsymbol{\Lambda}_N$ and $\boldsymbol{\Lambda}_p$ be two row selection matrices such that $\boldsymbol{z}_N = \boldsymbol{\Lambda}_N\boldsymbol{z} = \boldsymbol{\Lambda}_p\boldsymbol{p}$. Similarly, we define row selection matrices $\boldsymbol{\Lambda}_L$ and $\boldsymbol{\Lambda}_f$ such that $\boldsymbol{z}_L = \boldsymbol{\Lambda}_L\boldsymbol{z} = \boldsymbol{\Lambda}_f\boldsymbol{f}$. Then, we have

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{\epsilon} \quad \text{for } \boldsymbol{H} := \begin{bmatrix} \boldsymbol{\Lambda}_p\boldsymbol{B} \\ \boldsymbol{\Lambda}_f\boldsymbol{\Gamma}\boldsymbol{D}^T \end{bmatrix}, \tag{4}$$

where $\boldsymbol{H}$ is the measurement matrix based on the meter locations and the reported breaker status, and $\boldsymbol{\epsilon}$ is the measurement noise. In the rest of the paper, we assume that the measurements satisfy the conditions of [34, Theorem 5] such that $\boldsymbol{H}$ has full column rank to support unique recovery of $\boldsymbol{\theta}$ from (4) (before attack). If $\bar{\boldsymbol{\theta}}$ is the estimated phase angle from $\boldsymbol{z}$ and $\boldsymbol{H}$, then BDD will raise alarm if $\|\boldsymbol{z} - \boldsymbol{H}\bar{\boldsymbol{\theta}}\|$ is greater than a predefined threshold.

Given $\boldsymbol{p}_0 := \boldsymbol{B}\bar{\boldsymbol{\theta}}$, the CC will conduct SCED to calculate new generation to meet the demand with minimal cost. Specifically, let $\boldsymbol{\Lambda}_g \in \{0,1\}^{|V_g| \times |V|}$, $\boldsymbol{\Lambda}_d \in \{0,1\}^{|V_d| \times |V|}$ be row selection matrices for generator/load buses in $\boldsymbol{p}$, where V_d and V_g denote the sets of load buses and generator buses, respectively. Denote $\hat{\boldsymbol{\theta}}$ as the decision variable where $\boldsymbol{B}\hat{\boldsymbol{\theta}}$ represents the new power injection after SCED, and $\boldsymbol{\phi} \in \mathbb{R}^{|V_g|}$ as the cost vector for power generation. Then, SCED can be formulated as follows [11]:

$$\psi_s(\boldsymbol{p}_0, \boldsymbol{D}) = \arg\min_{\hat{\boldsymbol{\theta}}} \quad \boldsymbol{\phi}^T(\boldsymbol{\Lambda}_g\boldsymbol{B}\hat{\boldsymbol{\theta}}) \tag{5a}$$

$$\text{s.t.} \quad \boldsymbol{\Lambda}_d\boldsymbol{B}\hat{\boldsymbol{\theta}} = \boldsymbol{\Lambda}_d\boldsymbol{p}_0, \tag{5b}$$

$$\boldsymbol{\Gamma}\boldsymbol{D}^T\hat{\boldsymbol{\theta}} \in [-\boldsymbol{f}_{\max}, \boldsymbol{f}_{\max}], \tag{5c}$$

$$\boldsymbol{\Lambda}_g\boldsymbol{B}\hat{\boldsymbol{\theta}} \in [\boldsymbol{p}_{g,min}, \boldsymbol{p}_{g,max}], \tag{5d}$$

where $\boldsymbol{f}_{\max} \in \mathbb{R}^{|E|}$ indicates the normal line flow limits, $\boldsymbol{p}_{g,min}$ and $\boldsymbol{p}_{g,max}$ denote lower/upper bounds on generation, and (5b) indicates that demands on all load buses are satisfied.

B. Modeling Coordinated Cyber-Physical Attack (CCPA)

In this section, we formulate the attack model according to a load redistribution attack [9] that aims at causing the maximum outages, so that a defense against this attack can prevent outage under any attack under the same constraints. In the sequel, "ground truth" means the estimated value based on unmanipulated measurements, which may contain noise.

For ease of presentation, we summarize the timeline of the entire attack process, as shown in Fig 1. Specifically,

- At t_0, the attacker estimates $\boldsymbol{\theta}_0$ and $\boldsymbol{p}_0 := \tilde{\boldsymbol{B}}\boldsymbol{\theta}_0$ by eavesdropping on $\boldsymbol{z}_0$ and $\tilde{\boldsymbol{H}}$.
- At t_1, CCPA is deployed to change the ground-truth from $\boldsymbol{z}_0, \tilde{\boldsymbol{H}}, \boldsymbol{\theta}_0$ to $\boldsymbol{z}_1, \boldsymbol{H}$ and $\boldsymbol{\theta}_1$, respectively.
- At t_2, the CC receives falsified information, i.e., $\tilde{\boldsymbol{H}}$ and $\tilde{\boldsymbol{z}}_2$, which leads to $\tilde{\boldsymbol{\theta}}_2$. Then the CC will deploy a new dispatch of power generation as $\tilde{\boldsymbol{p}}_3 := \tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3$, where $\tilde{\boldsymbol{\theta}}_3$ denotes the associated predicted phase angles.
- At t_3, the new dispatch takes effect and reaches steady state, with the true phase angles $\boldsymbol{\theta}_3$ and power flows $\boldsymbol{f}_3$.

Key notations at different time instances are summarized in Table I, where "—" means that the information is not available to the CC at the given time instance.

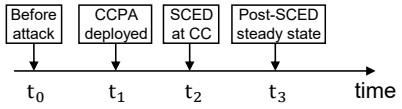


Figure 1. Timeline of an instance of CCPA

First, we model the influence of attacks on SCED. We define $\boldsymbol{a}_c \in \mathbb{R}^m$ to be the *cyber-attack vector*, which changes the measurements received by the CC to $\tilde{\boldsymbol{z}}_2 = \boldsymbol{z}_2 + \boldsymbol{a}_c$, and

Table I
NOTATIONS V.S. TIMELINE

time	t_0	t_1	t_2	t_3
True measurement matrix	$\tilde{\boldsymbol{H}}$	$\boldsymbol{H}$	$\boldsymbol{H}$	$\boldsymbol{H}$
Measurement matrix at CC	—	—	$\tilde{\boldsymbol{H}}$	$\tilde{\boldsymbol{H}}$
True phase angle	$\boldsymbol{\theta}_0$	$\boldsymbol{\theta}_1$	$\boldsymbol{\theta}_2 = \boldsymbol{\theta}_1$	$\boldsymbol{\theta}_3$
Phase angle at CC	—	—	$\tilde{\boldsymbol{\theta}}_2$	$\tilde{\boldsymbol{\theta}}_3$
True measurement	$\boldsymbol{z}_0$	$\boldsymbol{z}_1$	$\boldsymbol{z}_2 = \boldsymbol{z}_1$	$\boldsymbol{z}_3$
measurement at CC	—	—	$\tilde{\boldsymbol{z}}_2$	—

$\boldsymbol{a}_p \in \{0,1\}^{|E|}$ the *physical-attack vector*, where $a_{p,e} = 1$ indicates that line e is disconnected by the physical attack. As the physical attack changes the topology, we use $\tilde{\mathcal{N}}$ to denote the pre-attack topology and $\mathcal{N}$ the post-attack topology. Accordingly, $\tilde{\boldsymbol{B}}, \tilde{\boldsymbol{D}}, \tilde{\boldsymbol{H}}$ denote the pre-attack admittance, incidence, and measurement matrices, and $\boldsymbol{B}, \boldsymbol{D}, \boldsymbol{H}$ their (true) post-attack counterparts, related by

$$\boldsymbol{B} = \tilde{\boldsymbol{B}} - \tilde{\boldsymbol{D}}\boldsymbol{\Gamma}\text{diag}(\boldsymbol{a}_p)\tilde{\boldsymbol{D}}^T, \quad \boldsymbol{D} = \tilde{\boldsymbol{D}} - \tilde{\boldsymbol{D}}\text{diag}(\boldsymbol{a}_p), \quad (6)$$

and $\boldsymbol{H} = \tilde{\boldsymbol{H}} - [(\boldsymbol{\Lambda}_p\tilde{\boldsymbol{D}}\boldsymbol{\Gamma}\text{diag}(\boldsymbol{a}_p)\tilde{\boldsymbol{D}}^T)^T, (\boldsymbol{\Lambda}_f\tilde{\boldsymbol{D}}\text{diag}(\boldsymbol{a}_p))^T]^T$. Falsified measurements in $\tilde{\boldsymbol{z}}_2$ and breaker status will mislead CC to an incorrect state estimation and thus falsified SCED decisions. Hence, overload-induced line tripping can happen at t_3.

To bypass BDD, the attacker has to manipulate breaker status information to mask the physical attack, misleading the CC to believe that the measurement matrix is $\tilde{\boldsymbol{H}}$ instead of $\boldsymbol{H}$. Also, measurements have to be modified into $\tilde{\boldsymbol{z}}_2$ such that BDD with $\tilde{\boldsymbol{z}}_2$ and $\tilde{\boldsymbol{H}}$ as input will not raise any alarm. Below, we will derive constraints on $\boldsymbol{a}_p$ and $\boldsymbol{a}_c$ such that the modified data can pass BDD under the assumption that the pre-attack data can pass BDD as assumed in FDI [2]. Considering that $\tilde{\boldsymbol{z}}_2 = \boldsymbol{z}_2 + \boldsymbol{a}_c$, $\boldsymbol{a}_c$ should be constructed such that

$$\begin{aligned}\|\tilde{\boldsymbol{z}}_2 - \tilde{\boldsymbol{H}}\tilde{\boldsymbol{\theta}}_2\| &= \|\boldsymbol{z}_0 - \tilde{\boldsymbol{H}}\boldsymbol{\theta}_0 + \boldsymbol{z}_2 + \boldsymbol{a}_c - \boldsymbol{z}_0 + \tilde{\boldsymbol{H}}\boldsymbol{\theta}_0 - \tilde{\boldsymbol{H}}\tilde{\boldsymbol{\theta}}_2\| \\ &= \|\boldsymbol{z}_0 - \tilde{\boldsymbol{H}}\boldsymbol{\theta}_0\|, \quad \text{(pre-attack residual)} \quad (7)\end{aligned}$$

which leads to the following construction of $\boldsymbol{a}_c$:

$$\begin{aligned}\boldsymbol{a}_c &= \boldsymbol{z}_0 - \boldsymbol{z}_2 + \tilde{\boldsymbol{H}}(\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{\theta}_0) \quad (8)\\ &= \tilde{\boldsymbol{H}}\boldsymbol{\theta}_0 + \epsilon_0 - (\boldsymbol{H}\boldsymbol{\theta}_2 + \epsilon_0) + \tilde{\boldsymbol{H}}(\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{\theta}_0) \quad (9)\\ &= \begin{bmatrix} \boldsymbol{\Lambda}_p\tilde{\boldsymbol{B}} \\ \boldsymbol{\Lambda}_f\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T \end{bmatrix}\tilde{\boldsymbol{\theta}}_2 - \begin{bmatrix} \boldsymbol{\Lambda}_p\boldsymbol{B} \\ \boldsymbol{\Lambda}_f\boldsymbol{\Gamma}\boldsymbol{D}^T \end{bmatrix}\boldsymbol{\theta}_2. \quad (10)\end{aligned}$$

Besides (8), there may be additional constraints on $\boldsymbol{a}_c$ to avoid causing suspicion. Specifically, following [9], we assume that all the power injections at generator buses are measured and not subject to attacks, i.e.,

$$\boldsymbol{\Lambda}_g\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 = \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2 = \boldsymbol{\Lambda}_g\boldsymbol{B}\boldsymbol{\theta}_2 = \boldsymbol{\Lambda}_g\boldsymbol{D}\boldsymbol{f}_2 = \boldsymbol{\Lambda}_g\boldsymbol{p}_0, \quad (11)$$

recalling that $\boldsymbol{\Lambda}_g$ is the row selection matrix corresponding to generator buses. Moreover, by representing the maximum normal load fluctuation through $\alpha \geq 0$, the magnitude of falsification at load buses needs to be constrained due to load forecasting [9], [11], which can be modeled by [1]

$$-\alpha|\boldsymbol{p}_0| \leq \tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{p}_0 \leq \alpha|\boldsymbol{p}_0|. \quad (12)$$

Following the convention in [9], [23], the attack is constrained by a predefined constant ξ_p denoting the maximum number of attacked lines and another constant ξ_c denoting the maximum number of manipulated measurements, i.e.,

$$\|\boldsymbol{a}_p\|_0 \leq \xi_p, \quad \|\boldsymbol{a}_c\|_0 \leq \xi_c. \quad (13)$$

In addition, we constrain $\boldsymbol{a}_p$ so that the graph after physical attack remains connected, which is needed for stealth of the attack according to [11], [12]. Specifically, defining $\boldsymbol{f}_{con} \in \mathbb{R}^{|E|}$ as a pseudo flow and u_0 as the reference node, we can guarantee network connectivity at t_2 by ensuring

$$\tilde{\boldsymbol{D}}_u\boldsymbol{f}_{con} = \begin{cases} |V| - 1, & \text{if } u = u_0, \\ -1, & \text{if } u \in V \setminus \{u_0\}, \end{cases} \quad (14a)$$

$$-|V| \cdot (1 - a_{p,e}) \leq f_{con,e} \leq |V| \cdot (1 - a_{p,e}). \quad (14b)$$

With lines oriented as in $\tilde{\boldsymbol{D}}$, (14a) (flow conservation constraint) and (14b) (line capacity constraint) ensure the existence of a unit pseudo flow from u_0 to every other node in the post-attack grid and hence the connectivity of the post-attack grid, where $f_{con,e} > 0$ if the flow on e is in the same direction of the line and $f_{con,e} < 0$ otherwise.

In practice, transmission lines are equipped with overcurrent protection devices, which will trip the lines when the power flow exceeds the tripping threshold. Thus, heavy overloading caused by the SCED misled by cyber attacks can lead to initial outages at t_3, which can create cascading outages [11]. Specifically, let $\boldsymbol{f}_{max} \in \mathbb{R}^{|E|}$ be the normal power flow limits imposed in SCED [35]. Then, a line $e \in E$ will be tripped by protection devices (i.e., having an outage) if

$$|f_e| > \gamma_e f_{\max,e}, \quad (15)$$

where γ_e denotes the tripping threshold based on the thermal limit of the line. In practice, although [36] suggests $\gamma_e \geq 1.5$, the operator may choose higher $f_{\max,e}$, which leads to a smaller γ_e. As discussed in [11], [37], a small γ_e implies that the system is operating with a low margin of overload. A large γ_e may contribute to robustness to cascading failure [37], but leads to underutilization of transmission lines.

C. Modeling the Protection Effect of Secured PMUs

Let $\boldsymbol{\beta} \in \{0,1\}^{|V|}$ be the indicator vector for PMU placement such that $\beta_u = 1$ if and only if a secured PMU is installed at node u. We define $\Omega(\boldsymbol{\beta}) := \{u|\beta_u > 0\}$ and the inverse process $\boldsymbol{\beta}(\Omega) : \beta_u = 1$ if $u \in \Omega$ and $\beta_u = 0$ otherwise. Let $\mathcal{V}_u$ be the node set containing neighbors of node u (including u) and E_u be the line set composed of lines incident on u. According to [21], by measuring both voltage and current phasor, a PMU on node u can guarantee the correctness of phase angles in $\mathcal{V}_u$

[1] In contrast to [1] that only imposes the magnitude constraint on measured buses, constraint (12) is imposed on all buses (although subsumed by (11) for generator buses). This is because under the assumption of full-rank measurement matrix (Section II-A), the CC can recover all the phase angles and hence the power injections at all the buses, and thus the attacker needs to avoid causing too much deviation in the power injections at all the buses.

and protect lines in E_u from both cyber and physical attacks. Formally, we define $\boldsymbol{x}_N \in \{0,1\}^{|V|}$ such that $(x_{N,u}=1) \leftrightarrow (\exists v \in \mathcal{V}_u$ such that $\beta_v = 1)$, which can be modeled as

$$\boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} \le \boldsymbol{x}_N \le \boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} + \frac{\|\boldsymbol{\Delta}\|_\infty - 1}{\|\boldsymbol{\Delta}\|_\infty}, \tag{16}$$

where $\boldsymbol{\Delta} \in \mathbb{Z}^{|V|\times|V|}$ is a diagonal matrix with $\Delta_{uu} = |\mathcal{V}_u|$, while $\underline{\boldsymbol{A}} := \boldsymbol{A}+\boldsymbol{I}$ is the adjacency matrix of the grid with added self-loops at all nodes. Similarly, we define ζ to be any constant within $[0.5, 1)$ and $\boldsymbol{x}_L \in \{0,1\}^{|E|}$ satisfying $(x_{L,e}=1) \leftrightarrow (\exists v$ with $e \in E_v$ and $\beta_v = 1)$, which can be linearlized as

$$0.5|\boldsymbol{D}|^T\boldsymbol{\beta} \le \boldsymbol{x}_L \le 0.5|\boldsymbol{D}|^T\boldsymbol{\beta} + \zeta. \tag{17}$$

We assume that the PMU locations are known to the attacker, thus the cyber attack is constrained as follows:

$$x_{N,u} = 1 \rightarrow \tilde{\boldsymbol{\theta}}_{2,u} = \boldsymbol{\theta}_{2,u}, \forall u \in V, \tag{18a}$$
$$x_{L,e} = 1 \rightarrow a_{p,e} = 0, \quad \forall e \in E. \tag{18b}$$

Note that (16)-(18) implicitly protect the power flow measurements on lines incident to a PMU. To see this, suppose that $e = (s,t)$ and $\beta_s = 1$. Then we must have $x_{N,s} = x_{N,t} = x_{L,e} = 1$ due to (16)-(17). By (18), it is guaranteed that $\tilde{z}_{2,e} := (\tilde{\theta}_{2,s} - \tilde{\theta}_{2,t})/r_{st} = (\theta_{2,s} - \theta_{2,t})/r_{st} =: z_{2,e}$. In addition, PMU data are usually collected at a high frequency (e.g., around 60-200 samples per second). Thus, the PMUs can "instantly" detect any attack violating (18) even though they cannot prevent the attack from happening. In this way, the PMUs can reduce the potential damage by restricting the attacker's choices of attack vectors.

D. Optimal PMU Placement Problem

Our main problem, named *PMU Placement for Outage Prevention (PPOP)*, aims at placing the minimum number of secured PMUs so that no undetectable CCPA can cause overload-induced tripping. To achieve this, we model the problem as a tri-level optimization problem (an overview of PPOP is given in Fig. 4 in Appendix A).

The *middle-level* optimization is the attacker's problem, which aims to maximize the number of overloaded lines without being detected. Instead of using $\boldsymbol{a}_c$ as decision variable, we propose to formulate over $\tilde{\boldsymbol{f}}_i, \boldsymbol{f}_i$ and $\tilde{\boldsymbol{\theta}}_i, \boldsymbol{\theta}_i$ where $i \in \{2,3\}$. In the rest of the paper, we will apply big-M modeling technique that introduces sufficiently large constants denoted as $M_{(\cdot)}$ for linearization. The calculation of $M_{(\cdot)}$ is given in Appendix B. Specifically, the constraints on $\boldsymbol{\theta}_2$ and $\boldsymbol{f}_2$ are:

$$-M_{2,a,e}\left(\mathbf{1}-\boldsymbol{a}_p\right) \le \boldsymbol{f}_2 \le M_{2,a,e}\left(\mathbf{1}-\boldsymbol{a}_p\right), \tag{19a}$$
$$\tilde{\boldsymbol{D}}\boldsymbol{f}_2 = \boldsymbol{p}_0, \tag{19b}$$
$$-M_{2,f}\boldsymbol{a}_p \le \boldsymbol{\Gamma}\boldsymbol{D}\boldsymbol{\theta}_2 - \boldsymbol{f}_2 \le M_{2,f}\boldsymbol{a}_p. \tag{19c}$$

The constraints (19a) and (19b) guarantee the consistency between $\boldsymbol{f}_2$ and $\boldsymbol{p}_0$ given $\boldsymbol{a}_p$, where $a_{p,e} = 1$ will force $f_{2,e} = 0$. The role of (19c) is to force the consistency between $\boldsymbol{f}_2$ and $\boldsymbol{\theta}_2$ for all e with $a_{p,e} = 0$, which is necessary for the uniqueness of $\boldsymbol{f}_2$. Similarly, we can transform (7)-(13) into constraints over $\tilde{\boldsymbol{f}}_2$, $\tilde{\boldsymbol{\theta}}_2$, and $\boldsymbol{a}_p$, which are

$$-\boldsymbol{f}_{\max} \le \tilde{\boldsymbol{f}}_2 \le \boldsymbol{f}_{\max}, \tag{20a}$$
$$\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\tilde{\boldsymbol{\theta}}_2 - \tilde{\boldsymbol{f}}_2 = 0, \tag{20b}$$
$$\tilde{\theta}_{2,u} - \theta_{2,u} \le M_{2,\theta}\cdot(1-\boldsymbol{x}_{N,u}), \tag{20c}$$
$$\tilde{\theta}_{2,u} - \theta_{2,u} \ge -M_{2,\theta}\cdot(1-\boldsymbol{x}_{N,u}), \tag{20d}$$
$$-\alpha|\boldsymbol{p}_0| \le \tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 - \boldsymbol{p}_0 \le \alpha|\boldsymbol{p}_0|, \tag{20e}$$
$$\boldsymbol{\Lambda}_g\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 = \boldsymbol{\Lambda}_g\boldsymbol{p}_0, \tag{20f}$$
$$\|\boldsymbol{\Lambda}_f\left(\tilde{\boldsymbol{f}}_2 - \boldsymbol{f}_2\right)\|_0 + \|\boldsymbol{\Lambda}_p\left(\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 - \boldsymbol{p}_0\right)\|_0 \le \xi_c, \tag{20g}$$
$$\|\boldsymbol{a}_p\|_0 \le \xi_p, \tag{20h}$$

where (20a)-(20b) guarantee the validity of $\tilde{\boldsymbol{f}}_2$ as in (19a)-(19c), (20c)-(20d) linearize (18a) ($M_{2,\theta}$ defined in Appendix B), while (20e), (20f), and (20g)–(20h) correspond to (12), (11), and (13), respectively. It is worth noting that there exists an $\boldsymbol{a}_c$ in the form of (10) for any $\tilde{\boldsymbol{f}}_2$ and $\tilde{\boldsymbol{\theta}}_2$ satisfying (20) due to the relationship between $\tilde{\boldsymbol{f}}_2$, $\tilde{\boldsymbol{\theta}}_2$ and $\boldsymbol{a}_c$ shown in (10) and (20b). Moreover, the constraints on $\boldsymbol{\theta}_3, \tilde{\boldsymbol{\theta}}_3$, and $\boldsymbol{f}_3$ are

$$\boldsymbol{p}_{g,min} \le \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 \le \boldsymbol{p}_{g,max} \tag{21a}$$
$$-\boldsymbol{f}_{\max} \le \boldsymbol{\Gamma}\boldsymbol{D}^T\tilde{\boldsymbol{\theta}}_3 \le \boldsymbol{f}_{\max}, \tag{21b}$$
$$\boldsymbol{\Lambda}_d\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 = \boldsymbol{\Lambda}_d\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 \tag{21c}$$
$$-M_{3,a}(\mathbf{1}-\boldsymbol{a}_p) \le \boldsymbol{f}_3 \le M_{3,a}(\mathbf{1}-\boldsymbol{a}_p), \tag{21d}$$
$$\boldsymbol{\Lambda}_d\tilde{\boldsymbol{D}}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_d\boldsymbol{p}_0, \quad \boldsymbol{\Lambda}_g\tilde{\boldsymbol{D}}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3, \tag{21e}$$
$$-M_{3,f}\boldsymbol{a}_p \le \boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\boldsymbol{\theta}_3 - \boldsymbol{f}_3 \le M_{3,f}\boldsymbol{a}_p, \tag{21f}$$

where (21a)-(21c) describe the feasible region of $\tilde{\boldsymbol{\theta}}_3$ under false data injection, and (21d)–(21f) are used to enforce the power flow equation (3) at t_3, where $\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3$ is the post-SCED generation predicted by the attacker. While a straightforward formulation of the power flow equation should be

$$\boldsymbol{\Gamma}\boldsymbol{D}^T\boldsymbol{\theta}_3 = \boldsymbol{f}_3,\ \boldsymbol{\Lambda}_d\boldsymbol{D}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_d\boldsymbol{p}_0,\ \boldsymbol{\Lambda}_g\boldsymbol{D}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3, \tag{22}$$

such a formulation will introduce bilinear terms $\boldsymbol{D}^T\boldsymbol{\theta}_3$ and $\boldsymbol{D}\boldsymbol{f}_3$, as the post-attack incidence matrix $\boldsymbol{D}$ is a function of the physical-attack vector $\boldsymbol{a}_p$ that is also a decision variable for the attacker. To avoid the bilinear terms, we use (21d) to force $f_{3,e} = 0$ when $a_{p,e} = 1$ (line e is disconnected), and (21f) to force $\Gamma_e\tilde{\boldsymbol{d}}_e^T\boldsymbol{\theta}_3 = \Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3 = f_{3,e}$ when $a_{p,e} = 0$. Moreover, under (21d), we observe that $\boldsymbol{D}\boldsymbol{f}_3 = \sum_{e\in E}\boldsymbol{d}_e f_{3,e} = \sum_{e\in E}\tilde{\boldsymbol{d}}_e f_{3,e} = \tilde{\boldsymbol{D}}\boldsymbol{f}_3$, as $\boldsymbol{d}_e = \tilde{\boldsymbol{d}}_e$ if $a_{p,e} = 0$ and $\boldsymbol{d}_e f_{3,e} = \tilde{\boldsymbol{d}}_e f_{3,e} = \mathbf{0}$ if $a_{p,e} = 1$, which explains (21e).

Thus, the attacker's problem, which defines the optimal attack strategy, can be formulated as:

$$\psi_a(\boldsymbol{\beta}) := \max \quad \|\boldsymbol{\pi}\|_0 \tag{23a}$$
$$\text{s.t.} \quad (14), (16)-(21), \tag{23b}$$
$$\theta_{2,u_0} = \theta_{3,u_0} = \tilde{\theta}_{2,u_0} = \tilde{\theta}_{3,u_0} = 0, \tag{23c}$$
$$\tilde{\boldsymbol{\theta}}_3 = \psi_s(\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2, \tilde{\boldsymbol{D}}), \tag{23d}$$
$$\frac{|f_{3,e}|}{f_{\max,e}} > \gamma_e \leftrightarrow \pi_e = 1, \forall e \in E, \tag{23e}$$

where $\boldsymbol{y}_c := \tilde{\boldsymbol{\theta}}_2 \oplus \tilde{\boldsymbol{\theta}}_3 \oplus \boldsymbol{\theta}_2 \oplus \boldsymbol{\theta}_3 \oplus \boldsymbol{f}_2 \oplus \boldsymbol{f}_3 \oplus \tilde{\boldsymbol{f}}_2 \oplus \boldsymbol{f}_{con}$ and $\boldsymbol{y}_b := \boldsymbol{\pi} \oplus \boldsymbol{a}_p \oplus \boldsymbol{x}_N \oplus \boldsymbol{x}_L$ are continuous and binary decision variables, respectively. Here, $\pi_e = 1$ if and only if line e is overloaded to be tripped, which is ensured by (23e). Thus, the objective is to maximize the number of overload-induced tripped lines due to the attack-induced load redistribution. The

constraints (23c) fixes the phase angle at the reference node, denoted as node u_0. The constraint (23d) incorporates the *lower-level* optimization of SCED (5) by specifying the post-SCED generation, determined by $\tilde{\boldsymbol{\theta}}_3$.

We formulate the *upper-level* PMU placement problem as

$$\min \quad \|\boldsymbol{\beta}\|_0 \tag{24a}$$

$$\text{s.t.} \quad \psi_a(\boldsymbol{\beta}) = 0 \tag{24b}$$

where the decision variable is $\boldsymbol{\beta} \in \{0,\ 1\}^{|V|}$, and $\psi_a(\boldsymbol{x})$ defined in (23) denotes the maximum number of lines that will be tripped according to (15) at t_3. In the sequel, we call $(\boldsymbol{a}_p, \boldsymbol{a}_c, e)$ an *attack tuple*, which is called "successful" under PMU placement $\boldsymbol{\beta}$ if there exists a feasible solution to (23) with physical attack $\boldsymbol{a}_p$ and cyber attack $\boldsymbol{a}_c$ such that $\pi_e = 1$. Moreover, we call $(\boldsymbol{a}_p, e)$ a successful *attack pair* under $\boldsymbol{\beta}$ if it can form a successful attack tuple under $\boldsymbol{\beta}$.

Remark 1: While the above formulation treats the load profile $\boldsymbol{p}_0$ as a constant, it can be easily extended to handle the fluctuations in loads. This can be modeled by treating $\boldsymbol{p}_0$ as a decision variable in the attacker's optimization, constrained by the expected range of fluctuation, e.g., $\boldsymbol{p}_0 \in [\underline{\kappa}\boldsymbol{p}^{(0)}, \overline{\kappa}\boldsymbol{p}^{(0)}]$, or the union of ranges around multiple operating points:

$$\boldsymbol{p}_0 \in \bigcup_{i=1}^{i_0} \{\underline{\kappa}_i \boldsymbol{p}^{(i)} \le \boldsymbol{p} \le \overline{\kappa}_i \boldsymbol{p}^{(i)}\}. \tag{25}$$

This enlarges the solution space for the attacker, which changes the meaning of $\psi_a(\boldsymbol{\beta})$ to the *maximum number of tripped lines under the worst load profile and the worst attack under this load profile*. Clearly, a PMU placement that avoids overload-induced tripping in this worst scenario can avoid overload-induced tripping in any scenario encountered during operation, as long as the load profile stays within the predicted range.

Remark 2: In practice, PMUs are often deployed in stages. Thus, it may be desirable that a temporary PMU placement designed to prevent outages can be augmented into an optimal PMU placement $\boldsymbol{\beta}^{opt}$ in the long run (e.g., a minimum placement that provides full observability). This can be modeled by adding a constraint in (24) that requires $\boldsymbol{\beta} \le \boldsymbol{\beta}^{opt}$.

III. Solving PPOP

The PPOP problem (23)-(24) is a tri-level non-linear mixed integer problem, which is notoriously hard [12]. In this section, we first formally prove that the problem is NP-hard, and then demonstrate how to transform it into a *bi-level mixed-integer linear programming (MILP)* problem. Next, we propose an alternating optimization framework based on constraint generation to solve the problem optimally. Finally, to accelerate the computation, we develop a polynomial-time heuristic.

A. Hardness and Conversion to Bi-Level MILP

Although multi-level non-linear mixed integer programming is generally hard, PPOP is only a special case and hence needs to be analyzed separately. Nevertheless, we show that PPOP is NP-hard (see proof in Appendix H).

Theorem III.1. *The PPOP problem* (24) *is NP-hard.*

The attacker's problem (23) can be linearized into a MILP (see details in Appendix A), which implies that PPOP can be converted into a bi-level MILP.

B. An Alternating Optimization Framework

Algorithm 1: Alternating Optimization

1 **Initialization:** $k = 1$, $\hat{\boldsymbol{\beta}}^{(k)} = \mathbf{0}$;
2 **while** *True* **do**
3 Solve (23) under $\hat{\boldsymbol{\beta}}^{(k)}$ to obtain $\psi_a(\hat{\boldsymbol{\beta}}^{(k)})$;
4 **if** $\psi_a(\hat{\boldsymbol{\beta}}^{(k)}) > 0$ **then**
5 Add constraints to (24);
6 $k \leftarrow k + 1$, obtain $\hat{\boldsymbol{\beta}}^{(k)}$ by solving (24), with (24b) replaced by the generated constraints
7 **else** break ;
8 Return $\hat{\boldsymbol{\beta}}^{(k)}$, indicators of the selected PMU placement;

As a bi-level MILP, PPOP is still difficult to solve due to the integer variables in (23) and (24). Since one of the fundamental challenges in solving bi-level MILPs is the lack of explicit description of the upper-level optimization's feasible region, we propose an alternating optimization framework shown in Alg. 1 to solve PPOP by gradually approximating the feasible region of the upper-level optimization through constraint generation. In Sections III-C–III-D, we will give two concrete constraint generation methods for Line 5 of Alg. 1 based on the results of (23).

In the sequel, we assume that solving (23) returns a successful attack tuple $(\boldsymbol{a}_p^{(k)}, \boldsymbol{a}_c^{(k)}, e^{(k)})$ if $\psi_a(\hat{\boldsymbol{\beta}}^{(k)}) > 0$.

C. Alternating Optimization with No-Good Constraints (AONG)

In this section, we give the first specific algorithm under the framework of Alg. 1, in which the added constraints in Line 5 are motivated by the following observation:

Lemma III.1. *Given $\hat{\boldsymbol{\beta}}$ and $\Omega(\hat{\boldsymbol{\beta}}) := \{u \in V :\ \hat{\beta}_u > 0\}$, if there exists a successful attack tuple $(\boldsymbol{a}_p, \boldsymbol{a}_c, e)$, then for all $\boldsymbol{\beta}$ with $\Omega(\boldsymbol{\beta}) \subseteq \Omega(\hat{\boldsymbol{\beta}})$, there exists a successful attack tuple.*

Proof. For any $\boldsymbol{\beta}$ with $\Omega(\boldsymbol{\beta}) \subseteq \Omega(\hat{\boldsymbol{\beta}})$, $(\boldsymbol{a}_p, \boldsymbol{a}_c, e)$ remains a successful attack tuple. □

The above observation indicates that at least one PMU must be placed in $\Omega(\hat{\boldsymbol{\beta}})^c := V \setminus \Omega(\hat{\boldsymbol{\beta}})$. Therefore, the optimal $\boldsymbol{\beta}$ can be obtained in an iterative manner: during each iteration, we use the PMU placement $\hat{\boldsymbol{\beta}}$ from the previous iteration (initially, $\hat{\boldsymbol{\beta}} = \mathbf{0}$) to solve (23) for $\psi_a(\hat{\boldsymbol{\beta}})$. If $\psi_a(\hat{\boldsymbol{\beta}}) = 0$, $\hat{\boldsymbol{\beta}}$ is the final solution; otherwise, we will add the following "No-Good" constraint: $\sum_{i:\hat{\beta}_i=0} \beta_i \ge 1$ to (24) for the next iteration to rule out the infeasible solution $\hat{\boldsymbol{\beta}}$.

However, the above procedure will converge very slowly as $|\Omega(\hat{\boldsymbol{\beta}})^c|$ is usually large. To speed up convergence, we augment each discovered infeasible solution $\hat{\boldsymbol{\beta}}$ into a maximal infeasible solution $\hat{\boldsymbol{\beta}}'$ to narrow down candidate solutions. This can be achieved by solving the following problem:

$$\max \quad \|\hat{\boldsymbol{\beta}}'\|_0 \tag{26a}$$

$$\text{s.t.} \quad \psi_a(\hat{\boldsymbol{\beta}}') \geq 1, \tag{26b}$$

$$\hat{\beta}'_u = 1, \forall u \in V \text{ with } \hat{\beta}_u = 1, \tag{26c}$$

which has the same decision variables as (23) and the additional $\hat{\boldsymbol{\beta}}'$. Algorithm AONG adds the following "No-Good" constraint in Line 5 of Alg. 1:

$$\sum_{i:\hat{\beta}'_i=0} \beta_i \geq 1. \tag{27}$$

AONG solves PPOP optimally, as proved in Appendix H.

Theorem III.2. *AONG converges in finite time to an optimal solution to* (24).

Given the MILP formulation of (23) in Appendix A, it is easy to write (26) as a MILP and solve it by existing MILP solvers. It is worth noting that solving (26) suboptimally does not affect the optimality of AONG. Thus, we can also apply heuristic algorithms (e.g., LP relaxation with rounding).

D. Alternating Optimization with Double Constraints (AODC)

Building on AONG, we develop an additional constraint as a complement of (27) to accelerate convergence, in the special case where $\xi_c = \infty$ and $\psi_s(\boldsymbol{p}, \boldsymbol{D})$ returns the set of $\boldsymbol{\theta}$'s satisfying (5b)-(5d), i.e., it returns the feasible region of SCED rather than a single solution. Such a special case is worth consideration because (i) $\xi_c = \infty$ represents the strongest cyber attack, and (ii) relaxing the optimality requirement in (23d) means that the attacker is allowed to pick a solution for SCED within its feasible region, both making the attack stronger and hence the resulting PMU placement more robust in preventing outages.

Below we will first introduce the new constraints, called "Attack-Denial" constraints, and then give the AODC algorithm, in which both "No-Good" constraints and "Attack-Denial" constraints are added in Line 5 of Alg. 1. The new constraints are motivated by the following observations about AONG: many PMU placements enumerated by AONG are vulnerable to attacks formed from the same attack pair $(\boldsymbol{a}_p, e)$, indicating that it is more efficient to generate constraints that can invalidate the identified attack pairs. More discussions are given in Appendix C.

The above observations motivate the following idea of "Attack-Denial" constraints: *given a successful attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ under $\boldsymbol{\beta}^{(k)}$, the added constraints should guarantee that any PMU placement satisfying the constraints can prevent attacks that fail lines according to $\boldsymbol{a}_p^{(k)}$ from causing overload-induced tripping at line $e^{(k)}$*. We focus on $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ instead of $(\boldsymbol{a}_p^{(k)}, \boldsymbol{a}_c^{(k)}, e^{(k)})$ due to the following observations:

1) The number of $(\boldsymbol{a}_p^{(k)}, \boldsymbol{a}_c^{(k)}, e^{(k)})$'s is infinite since $\boldsymbol{a}_c^{(k)}$ is continuous, but the number of $(\boldsymbol{a}_p^{(k)}, e^{(k)})$'s is finite.
2) Given $\boldsymbol{x}_N$ and $(\boldsymbol{a}_p^{(k)}, e^{(k)})$, (23b)-(23e) reduce to a linear system with only the continuous variables contained in $\boldsymbol{y}_c$ under the assumptions that $\xi_c = \infty$ and $\psi_s(\boldsymbol{p}, \boldsymbol{D})$ returns the set of $\boldsymbol{\theta}$'s satisfying (5b)-(5d). The linear system can be summarized as

$$\boldsymbol{F}_1^{(k)} \boldsymbol{y}_c = \boldsymbol{s}_1^{(k)}, \tag{28a}$$

$$\boldsymbol{F}_2^{(k)} \boldsymbol{y}_c \leq \boldsymbol{s}_2^{(k)} + \boldsymbol{F}_3 \boldsymbol{x}_N, \tag{28b}$$

where $\boldsymbol{F}_1^{(k)}$, $\boldsymbol{F}_2^{(k)}$, $\boldsymbol{F}_3$, $\boldsymbol{s}_1^{(k)}$, $\boldsymbol{s}_2^{(k)}$ are constant matrices/vectors defined in Appendix D. An attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ can form a successful attack if and only if (28) has a feasible solution.

The above assumptions (i.e., $\xi_c = \infty$ and $\psi_s(\boldsymbol{p}, \boldsymbol{D})$ returns all the $\boldsymbol{\theta}$'s satisfying (5b)-(5d)) are needed because: (i) $\xi_c = \infty$ implies that we no longer need the binary variables used to linearize (20g) (i.e., $\boldsymbol{w}_f$ and $\boldsymbol{w}_p$ in (40) in Appendix A); (ii) when the lower-level optimization returns the feasible region of (5), (23d) can be replaced by (5b)-(5d) without introducing binary variables required for transforming (5) into its KKT conditions [9].

Our key observation is that a PMU placement $\boldsymbol{\beta}$ can defend against an attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ by either preventing the physical attack $\boldsymbol{a}_p^{(k)}$ or making (28) infeasible. The former can be achieved by adding constraint $\sum_{l:a_{p,l}^{(k)}=1} x_{L,l} \geq 1$ (i.e., at least one attacked line must be incident to a PMU). The latter holds according to Gale's theorem of alternative [38] if and only if there exists $\boldsymbol{q}_1^{(k)}$ and $\boldsymbol{q}_2^{(k)} \geq \boldsymbol{0}$ satisfying

$$(\boldsymbol{F}_1^{(k)})^T \boldsymbol{q}_1^{(k)} + (\boldsymbol{F}_2^{(k)})^T \boldsymbol{q}_2^{(k)} = \boldsymbol{0}, \tag{29a}$$

$$(\boldsymbol{s}_1^{(k)})^T \boldsymbol{q}_1^{(k)} + (\boldsymbol{s}_2^{(k)} + \boldsymbol{F}_3 \boldsymbol{x}_N)^T \boldsymbol{q}_2^{(k)} < 0, \tag{29b}$$

where $\boldsymbol{q}_1^{(k)} \in \mathbb{R}^{m_1}$ and $\boldsymbol{q}_2^{(k)} \in \mathbb{R}^{m_2}$ can be treated as the dual variables for (28a) and (28b), respectively.

Based on the above observation, the "Attack-Denial" constraints for defending against $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ are:

$$(\boldsymbol{F}_1^{(k)})^T \boldsymbol{q}_1^{(k)} + (\boldsymbol{F}_2^{(k)})^T \boldsymbol{q}_2^{(k)} = \boldsymbol{0}, \tag{30a}$$

$$(\boldsymbol{s}_1^{(k)})^T \boldsymbol{q}_1^{(k)} + (\boldsymbol{s}_2^{(k)} + \boldsymbol{F}_3 \boldsymbol{x}_N)^T \boldsymbol{q}_2^{(k)} \leq w_{a,k} - 1, \tag{30b}$$

$$\sum_{l:a_{p,l}^{(k)}=1} x_{L,l} \geq w_{a,k}, \tag{30c}$$

$$\boldsymbol{q}_2^{(k)} \geq \boldsymbol{0}, w_{a,k} \in \{0, 1\}, \tag{30d}$$

where $\boldsymbol{q}_1^{(k)}$, $\boldsymbol{q}_2^{(k)}$, and $w_{a,k}$ are newly introduced variables. Note that (29b) and (30b) are equivalent when $w_k = 0$ since we can scale $\boldsymbol{q}_1^{(k)}$ and $\boldsymbol{q}_2^{(k)}$ to satisfy (30b) if (29b) holds. The binary variable $w_{a,k}$ indicates which approach to use for defending against $(\boldsymbol{a}_p^{(k)}, e^{(k)})$. When $w_{a,k} = 0$, (30c) holds trivially, in which case $\boldsymbol{\beta}$ defends against $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ by satisfying (29), i.e., preventing the cyber attack from causing overload-induced tripping at line $e^{(k)}$. When $w_{a,k} = 1$, $\boldsymbol{q}_1^{(k)} = \boldsymbol{0}$ and $\boldsymbol{q}_2^{(k)} = \boldsymbol{0}$ will satisfy the constraints (30a)-(30b), in which case $\boldsymbol{\beta}$ defends against $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ by preventing the physical attack $\boldsymbol{a}_p^{(k)}$.

Now, we are ready to present the AODC algorithm, where $\hat{\boldsymbol{\beta}}^{(K+1)}$ in Line 6 of Alg. 1 is obtained by solving:

$$\min \quad \|\boldsymbol{\beta}\|_0 \tag{31a}$$

$$\text{s.t.} \quad (16)-(17), (30) \text{ for } k = 1, \cdots, K, \tag{31b}$$

$$\sum_{i:\hat{\beta}_i'^{(k)}=0} \beta_i \geq 1, k = 1, \cdots, K, \tag{31c}$$

$$\boldsymbol{\beta} \in \{0,\ 1\}^{|V|}, \tag{31d}$$

where the decision variables are $\boldsymbol{\beta}$, $\boldsymbol{x}_N$, $\boldsymbol{x}_L$, $\boldsymbol{q}_1^{(k)}$, $\boldsymbol{q}_2^{(k)}$, and $w_{a,k}$ for $k = 1, \cdots, K$.

To convert (31) to a MILP, we linearize $(\boldsymbol{F}_3\boldsymbol{x}_N)^T\boldsymbol{q}_2^{(k)}$ using McCormick's relaxation. Concretely, note that

$$(\boldsymbol{F}_3\boldsymbol{x}_N)^T\boldsymbol{q}_2^{(k)} = \sum_{u\in V}\boldsymbol{x}_{N,u}\left(\sum_{i=1}^{m_2}F_{3,i,u}q_{2,i}^{(k)}\right), \forall k. \quad (32)$$

Assuming that $\sum_i F_{3,i,u}q_{2,i}^{(k)} \in [\underline{M}_F, \overline{M}_F]$, we introduce a continuous auxiliary variable y_u and the following constraints:

$$\underline{M}_F x_{N,u} \le y_u \le \overline{M}_F x_{N,u}, \quad (33a)$$

$$y_u \le \left(\sum_{i=1}^{m_2}F_{3,i,u}q_{2,i}^{(k)}\right) + \underline{M}_F x_{N,u} - \underline{M}_F, \quad (33b)$$

$$y_u \ge \left(\sum_{i=1}^{m_2}F_{3,i,u}q_{2,i}^{(k)}\right) + \overline{M}_F x_{N,u} - \overline{M}_F. \quad (33c)$$

Note that $y_u = \sum_{i=1}^{m_2}F_{3,i,u}q_{2,i}^{(k)}$ if $x_{N,u}=1$ and $y_u=0$ otherwise, i.e., $y_u = \boldsymbol{x}_{N,u}\left(\sum_{i=1}^{m_2}F_{3,i,u}q_{2,i}^{(k)}\right)$. Then, $(\boldsymbol{F}_3\boldsymbol{x}_N)^T\boldsymbol{q}_2^{(k)}$ in (30b) can be replaced by $\sum_{u\in V}y_u$ subject to (33).

AODC guarantees an optimal solution at convergence in the considered special case (see proof in Appendix H).

Theorem III.3. *If $\xi_c=\infty$ and $\psi_s(\boldsymbol{p},\boldsymbol{D})$ returns the feasible region of* (5)*, then AODC will converge in finite time to an optimal solution to* (24)*.*

Although in the worst case AODC may still enumerate all the attack pairs, which can be exponential in $|E|$, we have observed that in practice it usually converges after identifying a relatively small set of "typical attack pairs", as shown in Table V.

E. Efficient Heuristics

Although Alg. 1 is guaranteed to find the optimal solution, the computational complexity can grow exponentially with the network size due to the requirement of solving MILPs in each iteration, which motivates us to develop polynomial-time heuristics. A scenario of particular interest is when ξ_p is small, i.e., $\xi_p=\mathcal{O}(1)$. In this case, the total number of attack pairs is polynomial in $|E|$, and thus the number of iterations in AODC and the complexity of computing a new attack pair in each iteration are both polynomial in $|E|$. Our focus in this case is thus on solving (31) approximately in polynomial time.

Relaxation: One idea is to directly relax the MILP version of (31) into an LP. However, simple LP relaxation will not work:

1) The LP relaxation will invalidate the McCormick relaxation (33) for the bilinear term $(\boldsymbol{F}_3\boldsymbol{x}_N)^T\boldsymbol{q}_2^{(k)}$.
2) The feasible region is significantly extended by the LP relaxation due to the adopted big-M modeling technique.
3) Given a continuous solution $\tilde{\boldsymbol{\beta}}$ obtained from the LP relaxation, it is non-trivial to determine which subset of $\Omega(\tilde{\boldsymbol{\beta}})$, if any, can achieve our defense goal.

We have developed a polynomial-time heuristic that can find a better PMU placement. The core of our heuristic is a different "LP relaxation" of (31). Recall that the main challenge in directly relaxing the MILP version of (31) is the invalidation of (33) for linearizing $(\boldsymbol{F}_3\boldsymbol{x}_N)^T\boldsymbol{q}_2^{(k)}$. To overcome this issue, we make the following observation (see proof in Appendix H):

Lemma III.2. *Define $\boldsymbol{\Lambda}_{x,p},\boldsymbol{\Lambda}_{x,n}\in\{0,1\}^{|V|\times m_2}$ such that $(\boldsymbol{\Lambda}_{x,p}\boldsymbol{q}_2)_u$ is the dual variable for* (20c) *and $(\boldsymbol{\Lambda}_{x,n}\boldsymbol{q}_2)_u$ is the dual variable for* (20d)*. Suppose that the linear system*

$$(\boldsymbol{F}_1^{(k)})^T\boldsymbol{q}_1^{(k)} + (\boldsymbol{F}_2^{(k)})^T\boldsymbol{q}_2^{(k)} = \boldsymbol{0}, \quad (34a)$$

$$(\boldsymbol{s}_1^{(k)})^T\boldsymbol{q}_1^{(k)} + (\boldsymbol{s}_2^{(k)}+\boldsymbol{F}_3)^T\boldsymbol{q}_2^{(k)} \le -1, \quad (34b)$$

$$(\boldsymbol{\Lambda}_{x,p}+\boldsymbol{\Lambda}_{x,n})\boldsymbol{q}_2 \le M_q\underline{\boldsymbol{A}}\boldsymbol{\beta}, \quad (34c)$$

$$\boldsymbol{q}_2^{(k)} \ge \boldsymbol{0},\ \boldsymbol{1}\ge\boldsymbol{\beta}\ge\boldsymbol{0} \quad (34d)$$

for attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ is feasible under $\boldsymbol{\beta}=\check{\boldsymbol{\beta}}$, where M_q is a large constant (defined in Appendix B). Then, $\boldsymbol{\beta}=\lceil\check{\boldsymbol{\beta}}\rceil$ satisfies (16)–(17) *and* (30) *with $w_{a,k}=0$ for the attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$.*

Lemma III.2 suggests that given an attack pair $(\boldsymbol{a}_p^{(k)}, e^{(k)})$, we can relax the mixed integer "Attach-Denial" constraints (30) into the linear constraints (34) and round up the fractional solution to obtain a valid PMU placement, which is guaranteed to prevent the given attack pair from forming successful attack tuples. According to Gale's theorem of alternative, $\left((\boldsymbol{\Lambda}_{x,p}+\boldsymbol{\Lambda}_{x,n})\boldsymbol{q}_2^{(k)}\right)_u > 0$ only if at least one of (20c) and (20d) is *effective* for making (28) infeasible[2]. Since (20c)-(20d) is effective if and only if $x_{N,u}=1$ (under the constraint of $x_{N,u}\in\{0,1\}$), we use $(\boldsymbol{\Lambda}_{x,p}+\boldsymbol{\Lambda}_{x,n})\boldsymbol{q}_2^{(k)}$ as a proxy of $\boldsymbol{x}_N$ in Lemma III.2.

Lemma III.2 motivates us to formulate the following LP based on a given set $\mathcal{C}$ of infeasible PMU placements and a given set $\{(\boldsymbol{a}_p^{(k)}, e^{(k)})\}_{k=1}^K$ of attack pairs:

$$\min \quad \sum_{u\in V}\beta_u \quad (35a)$$

$$\text{s.t.} \quad (34) \text{ for } k=1,\cdots,K, \quad (35b)$$

$$\sum_{i:\hat{\beta}_i=0}\beta_i \ge 1, \forall\hat{\boldsymbol{\beta}}\in\mathcal{C}, \quad (35c)$$

where (35b) models relaxed "Attack-Denial" constraints and (35c) models relaxed "No-Good" constraints. In this sense, (35) is a "LP relaxation" of (31). However, instead of directly computing a PMU placement from (35) which still faces some of the issues for simple LP relaxation, our idea is to use the result of (35) to identify important nodes for PMU placement to defend against the given attack pairs in the case of $w_{a,k}=0$ in (30). We will account for the case of $w_{a,k}=1$ separately in the proposed algorithm to avoid scaling and numerical issues.

Algorithm: The details of the proposed heuristic is given in Alg. 2, which relies on the function *UpdateCandidate(·)* shown in Alg. 3. The logic behind the heuristic is similar to that in AODC, i.e., iteratively updating PMU placements based on newly found attack pairs. The questions are: (i) how to generate initial placements, (ii) how to find attack pairs that can cause outages under given placements, and (iii) how to update the given placements to defend against the newly found attack pairs, all in polynomial time. Since this algorithm is designed for the case of $\xi_p=\mathcal{O}(1)$, under which question (ii) is easily solvable, our focus will be on questions (i) and (iii).

[2]We say that an inequality in (28) is *effective* for making (28) infeasible if removing it will change the feasibility of (28).

Algorithm 2: 3-phase Secured PMU Placement

/* Phase-1: find a set $\mathcal{A}_0$ of attack pairs */
Initialization: $k=1$, $\hat{\boldsymbol{\beta}}^{(k)}=\mathbf{0}$, $\mathcal{A}_0=\emptyset$, $\mathcal{C}=\emptyset$;
while $\psi_a(\hat{\boldsymbol{\beta}}^{(k)})>0$ **do**
  $\mathcal{A}_0 \leftarrow \mathcal{A}_0 \cup \{(\boldsymbol{a}_p^{(k)}, e^{(k)})\}$, where $(\boldsymbol{a}_p^{(k)}, e^{(k)})$ is obtained by solving (23) under $\hat{\boldsymbol{\beta}}^{(k)}$;
  $\mathcal{C} \leftarrow \mathcal{C} \cup \{\hat{\boldsymbol{\beta}}^{(k)}\}$, $k \leftarrow k+1$;
  obtain $\check{\boldsymbol{\beta}}^{(k)}$ by solving (35) over $\mathcal{C}$ and $\mathcal{A}_0$;
  Rounding: $\hat{\boldsymbol{\beta}}^{(k)} \leftarrow \lceil \check{\boldsymbol{\beta}}^{(k)} \rceil$;
/* Phase-2: find candidate placements $\{\Omega_i\}_{i=1}^{K_c}$ to defend against $\mathcal{A}_0$ */
Set $\Omega_i := \{u_i\}, i=1,\cdots,K_c$, where $\{u_i\}_{i=1}^{K_c}$ are the indices of the largest K_c elements of $\check{\boldsymbol{\beta}}^{(k)}$ that is obtained in the last iteration of phase-1;
$\{\Omega_i\}_{i=1}^{K_c}, \mathcal{C} \leftarrow$ UpdateCandidate $\Big(\{\Omega_i\}_{i=1}^{K_c}, \mathcal{A}_0, \mathcal{C}\Big)$;
/* Phase-3: augment $\{\Omega_i\}_{i=1}^{K_c}$ to find a placement Ω with $\psi_a(\boldsymbol{\beta}(\Omega))=0$ */
while *True* **do**
  $\mathcal{A} \leftarrow \emptyset$;
  for $i \leftarrow 1$ **to** K_c **do**
    if $\psi_a(\boldsymbol{\beta}(\Omega_i))>0$ **then** Generate $(\boldsymbol{a}_p^{(i)}, e^{(i)})$ and $\mathcal{A} \leftarrow \mathcal{A} \cup (\boldsymbol{a}_p^{(i)}, e^{(i)})$;
    else Return $\Omega^* = \arg\min_{\Omega_j:\psi_a(\boldsymbol{\beta}(\Omega_j))=0} |\Omega_j|$ if $|\Omega^*| \le 1 + \min_{\Omega_j:\psi_a(\boldsymbol{\beta}(\Omega_j))>0} |\Omega_j|$;
  $\{\Omega_i\}_{i=1}^{K_c}, \mathcal{C} \leftarrow$ UpdateCandidate $\Big(\{\Omega_i\}_{i=1}^{K_c}, \mathcal{A}, \mathcal{C}\Big)$;

Algorithm 3: UpdateCandidate$\big(\{\Omega_i\}_{i=1}^{K_c}, \mathcal{A}, \mathcal{C}\big)$

1 **Initialization:** $\mathcal{A}_i = \mathcal{A}, i=1,\cdots,K_c$;
2 **while** $\exists i$ *such that* $\mathcal{A}_i \neq \emptyset$ **do**
3 $\mathcal{Q} \leftarrow \emptyset$;
4 **for** $i \leftarrow 1$ **to** K_c **do**
5 **if** $\mathcal{A}_i = \emptyset$ **then** $\mathcal{Q} \leftarrow \mathcal{Q} \bigcup \{\Omega_i\}$ and continue;
6 **else** $\mathcal{C} \leftarrow \mathcal{C} \cup \{\boldsymbol{\beta}(\Omega_i)\}$;
7 $\mathcal{Q} \leftarrow \mathcal{Q} \bigcup (\Omega_i \cup \{v_j\})$ for $j=1,\cdots,K_L$, where v_j can prevent the j-th most physical attacks in $\mathcal{A}_i$;
8 Solve (35) over $\mathcal{A}$, $\mathcal{C}$, and the constraints $\beta_u = 1, \forall u \in \Omega_i$, which results in $\check{\boldsymbol{\beta}}$;
9 $\mathcal{Q} \leftarrow \mathcal{Q} \bigcup (\Omega_i \cup \{u_j\})$ for $j=1,\cdots,K_A$, where u_j is the index of the j-th largest element in $\{\check{\beta}_u\}_{u \in V \setminus \Omega_i}$;
10 Update $\{\Omega_i\}_{i=1}^{K_c}$ as the K_c elements in $\mathcal{Q}$ that can defend against the most attack pairs in $\mathcal{A}$;
11 $\mathcal{A}_i \leftarrow \{(\boldsymbol{a}_p, e) \in \mathcal{A} | \Omega_i$ cannot defend against $(\boldsymbol{a}_p, e)\}$, $\forall i = 1,\ldots,K_c$;
12 Return $\{\Omega_i\}_{i=1}^{K_c}$ and $\mathcal{C}$;

We answer question (i) in two phases. Specifically, in *phase-1*, we iteratively find a set of attack pairs $\mathcal{A}_0$ such that solving (35) over $\mathcal{A}_0$ leads to a fractional solution $\check{\boldsymbol{\beta}}$ with $\psi_a\left(\lceil \check{\boldsymbol{\beta}} \rceil\right) = 0$. Then in *phase-2*, we search for a set of candidate PMU placements $\{\Omega_i\}_{i=1}^{K_c}$ to defend against $\mathcal{A}_0$ in the hope that $|\Omega_i| < |\Omega(\lceil \check{\boldsymbol{\beta}} \rceil)|$. The motivation for maintaining $K_c > 1$ candidates is to avoid the situation where the computed placement is effective in defending against the given attacks but ineffective for other attacks.

We answer (iii) in Alg. 3, which iteratively augments a given set of candidate placements $\{\Omega_i\}_{i=1}^{K_c}$ to defend against a given set $\mathcal{A}$ of attack pairs. For each candidate placement not effective against all the attack pairs in $\mathcal{A}$, Alg. 3 will generate K_L and K_A new candidate placements in Line 7 and Lines 8-9, respectively. Then, Line 10 will select the K_c placements most effective in defending against the attack pairs in $\mathcal{A}$ from the pool of $K_c \cdot (K_A + K_L)$ candidate placements. We now characterize the complexity of Alg. 2 (see proof in Appendix H).

Theorem III.4. *If $\xi_p = \mathcal{O}(1)$, then the complexity of Alg. 2 is polynomial in $|V|$, $|E|$, and K_c.*

IV. Extension to AC Power Flow Model

So far we have assumed the DC power flow approximation for the power grid given in Section II-A. It remains to validate the resulting PMU placement under the AC power flow model that describes the grid state more accurately. To this end, we will address the following questions: given a PMU placement $\Omega_{\text{DC}} \subseteq V$ obtained under the DC power flow model, (i) how to test the feasibility of Ω_{DC} in preventing outages under the AC power flow model, and (ii) how to refine Ω_{DC} if needed to achieve our defense goal under the AC power flow model.

A. Testing a PMU Placement under AC Model

One challenge to answer the first question is the nonlinear and nonconvex nature of *AC power flow based SCED (AC-SCED)*, which invalidates the transformation of (23) into a single-level MILP through KKT conditions. Another challenge lies in formulating a single optimization to maximize the overloading of a target line after SCED (at t_3 in Fig. 1). Specifically, since solving nonlinear AC power flow equations usually requires iterative methods (e.g., Newton-Raphson method [39]), we cannot directly formulate the AC-SCED at t_2 and the corresponding ground-truth grid state at t_3 in an optimization problem. Existing works handled this challenge by approximating the grid state at t_3 by the DC power flow model [28], [32] or DC-based line outage distribution factors [30], [31]. However, such DC-based approximations cannot be directly used to compute the magnitude of currents, which determines the overloading and related tripping of lines.

In the following, we provide a method, as shown in Alg. 4, to check the existence of an AC-based CCPA that can cause overloading under a given PMU placement. To overcome the challenges discussed before, we first remove the optimality requirement in AC-SCED, similar to our derivation of "Attack-Denial" constraints in Section III-D. Omitting this optimality requirement is equivalent to allowing the attacker to choose the objective for AC-SCED, which enlarges the feasible region for the attacker's optimization. To jointly model the current at t_3 and the AC-SCED at t_2, we adopt the *linearized approximation*

of AC power flow equations [33]. Based on these two strategies, we formulate the following optimization problem for the attacker to maximize the magnitude of current on a given target line e_t under a given physical attack (i.e., $\boldsymbol{a}_p$):

$$\max \quad |\hat{I}_{3,e_t}|^2 \tag{36a}$$

$$\text{s.t.} \quad \text{Constraints on } \tilde{\boldsymbol{v}}_2, \tilde{\boldsymbol{\theta}}_2 \text{ to bypass BDD}, \tag{36b}$$

$$\text{ACOPF constraints on } \tilde{\boldsymbol{v}}_3, \tilde{\boldsymbol{\theta}}_3, \tag{36c}$$

$$\text{Constraints to solve } \hat{\boldsymbol{v}}_3, \hat{\boldsymbol{\theta}}_3, |\hat{\boldsymbol{I}}_3|, \tag{36d}$$

where $\tilde{\boldsymbol{v}}_2, \tilde{\boldsymbol{\theta}}_2$ denote the voltage magnitudes and phase angles estimated at t_2 by the control center based on falsified measurements, $\tilde{\boldsymbol{v}}_3, \tilde{\boldsymbol{\theta}}_3$ denote the same variables predicted by AC-SCED for t_3 (computed at t_2), and $\hat{\boldsymbol{v}}_3, \hat{\boldsymbol{\theta}}_3, |\hat{\boldsymbol{I}}_3|$ denote the approximated ground-truth of voltage magnitudes, phase angles and line current magnitude at t_3. The details of (36) are given in Appendix E. Similar to Table I, for a given variable x, we use $\tilde{x}_2$ to denote its estimate based on falsified measurements at t_2, x_2 to denote its ground-truth value at t_2, $\tilde{x}_3$ to denote the value predicted by AC-SCED (at t_2) for t_3, and x_3 to denote the ground-truth value at t_3. Given the voltage magnitudes $\tilde{\boldsymbol{v}}_3$ and the phase angles $\tilde{\boldsymbol{\theta}}_3$, the approximated values of x at t_3 is denoted as $\hat{x}_3$.

In (36), we have the following three types of constraints and decision variables:

1) Constraint (36b) is the counterpart of (20) under the AC power flow model, in which the main decision variables are $\tilde{\boldsymbol{v}}_2$ and $\tilde{\boldsymbol{\theta}}_2$. Similar to (20), we use $\tilde{\boldsymbol{v}}_2$ and $\tilde{\boldsymbol{\theta}}_2$ as the decision variables to model the cyber attack that can bypass the BDD. Following [30], we adopt the quadratic convex (QC) relaxation [40] in (36b) to model the AC power flow equations.
2) As the counterpart of (21a)-(21c) under the AC power flow model, (36c) models the reaction of AC-SCED to the falsified measurements based on the QC relaxation.
3) The real grid state at t_3 is formulated in (36d) as the counterpart of (21d)-(21f), based on the approximation of AC power flow equations proposed in [33].

As we have enlarged the feasible region for the attacker in (36b)-(36c) by using the QC relaxation, (36) models a stronger attack, and hence a PMU placement that prevents overloading under this attack can prevent overloading under the original attack. We will use x^* to denote the value of decision variable x in the optimal solution to (36).

Based on (36), we develop an algorithm to check the feasibility of a PMU placement $\Omega \subseteq V$ in preventing outages under AC-based CCPA, shown in Algorithm 4. Specifically, at Lines 2, we compute $\boldsymbol{v}_2, \boldsymbol{\theta}_2, |\boldsymbol{I}_2|$ by solving power flow equations. Thus, the counterpart of (19) is no longer needed to compute the real grid states after physical attacks. Then, at Line 3, we obtain the optimal solution $(|\hat{I}^*_{3,e_t}|, \tilde{\boldsymbol{v}}^*_3, \tilde{\boldsymbol{\theta}}^*_3)$ to (36) for the given attack pair $(\boldsymbol{a}_p, e_t)$ (recall that $|\hat{I}^*_{3,e_t}|$ is the approximated current magnitude on line e_t at time t_3 while $|I^*_{3,e_t}|$ is the corresponding true value). Alg. 4 considers the PMU placement Ω to successfully defend against $(\boldsymbol{a}_p, e_t)$ (i.e., preventing overloading at line e_t under physical attack $\boldsymbol{a}_p$) if one of the following conditions hold:

1) no cyber attack $\boldsymbol{a}_c$ can bypass the BDD, i.e., (36) is infeasible, as checked in Line 9, or
2) $|\hat{I}^*_{3,e_t}| \le \hat{I}_{max,e_t}$ and $|I^*_{3,e_t}| \le \gamma_e I_{max,e_t}$, as checked in Lines 4–7, where $\hat{I}_{max,e_t}$ (derived in Theorem IV.1) is the threshold used by Alg. 4 to detect the tripping of line e_t based on the approximated current magnitude $|\hat{I}^*_{3,e_t}|$.

The use of $\hat{I}_{max,e}$ rather than $\gamma_e I_{max,e}$ allows us to compensate for the approximation error at t_3. As stated in Theorem IV.1, under a properly-set $\hat{I}_{max,e}$, a PMU placement Ω is guaranteed to achieve our defense goal under the AC model if Ω can pass the test of Alg. 4, i.e., no overloading is reported. How to bound the approximation errors as assumed in Theorem IV.1 is not the focus of this work; we refer interested readers to [33] for details.

Theorem IV.1. *Assume that the approximation used in* (36d) *satisfies* $|\hat{v}_{3,u} - v_{3,u}| \le \epsilon_{v,u}, |\hat{\theta}_{3,u} - \theta_{3,u}| \le \epsilon_{\theta,u}$, $\forall u \in V$ *and* $|\hat{p}_{3,f,e} - p_{3,f,e}| \le \epsilon_{p,e}$, $|\hat{q}_{3,f,e} - q_{3,f,e}| \le \epsilon_{q,e}$, $\forall e \in E$. *Then, there exists* $\epsilon_{I,e}, \forall e \in E$ *(see proof in Appendix H for details) and* $\hat{I}_{max,e} := \gamma_e I_{max,e} - \epsilon_{I,e}$ *such that any PMU placement passing the test of Alg. 4 can prevent overload-induced tripping under the AC power flow model.*

Algorithm 4: Test Feasibility of Ω under AC Model

```
1  for each possible attack pair (a_p, e_t) under the given
     PMU placement Ω do
2      Obtain v_2, θ_2, |I_2| from AC power flow equations;
3      Solve (36) to obtain |Î*_{3,e_t}|, ṽ*_3, θ̃*_3;
4      if (36) is feasible AND |Î*_{3,e_t}| ≤ Î_{max,e_t} then
5          Compute |I*_{3,e_t}| from AC power flow equations;
6          if |I*_{3,e_t}| ≤ γ_e I_{max,e_t} then
7              Continue;
8          else Terminate and report overloading;
9      else if (36) is infeasible then
10         Continue;
11     else Terminate and report overloading;
```

B. Refining PMU Placement

In the case that the DC-based PMU placement Ω_{DC} fails the test by Alg. 4, we provide a simple heuristic to augment it into a new placement Ω_{AC} that can achieve our defense goal under the AC model. The intuition is to iteratively augment Ω_{DC} by placing more PMUs until the resulting placement Ω_{AC} can pass the test of Alg. 4. The key question is which node to add. To answer this question, we first augment Ω_{DC} into a PMU placement $\Omega_C := \Omega(\boldsymbol{\beta}_C)$ that can achieve full observability by solving (37):

$$\min_{\boldsymbol{\beta}_C \in \{0,1\}^{|V|}} \quad \|\boldsymbol{\beta}_C\|_1 \tag{37a}$$

$$\text{s.t.} \quad \boldsymbol{\beta}_C \ge \boldsymbol{\beta}(\Omega_{\text{DC}}), \tag{37b}$$

$$\underline{\boldsymbol{A}}\boldsymbol{\beta}_C \ge 1, \tag{37c}$$

where (37b) guarantees $\Omega_{\text{DC}} \subseteq \Omega_C$, and (37c) forces Ω_C to achieve full observability. Then equipped with Ω_C, we augment Ω_{DC} into Ω_{AC} by Alg. 5. If a PMU placement cannot

defend against an attack pair $(\boldsymbol{a}_p, e_t)$ (Line 6), then we update the PMU placement by the following rules:

1) If there exists a node $u \in \Omega_C$ that can prevent the physical attack $\boldsymbol{a}_p$ as in (18b), we add node u to the current PMU placement (Line 8).
2) Otherwise, we add the node in Ω_C with the maximum deviation in phase angle due to false data injection (Line 11), with ties broken arbitrarily.

Algorithm 5: Augment PMU Placement for AC Model

1 **Initialization:** $\Omega_{\text{AC}} = \Omega_{\text{DC}}$;
2 **while** *True* **do**
3 Test Ω_{AC} through Alg. 4;
4 **if** *No overloading is reported* **then** Return Ω_{AC};
5 **else**
6 Let $(\boldsymbol{a}_p, e_t)$ be the attack pair under which overloading is reported, and $U := \{u \in V : \exists e \text{ with } a_{p,e} = 1, D_{u,e} \neq 0\}$ (all end-nodes of physically-attacked lines);
7 **if** $\Omega_C \cap U \neq \emptyset$ **then**
8 Arbitrarily choose a node $u \in \Omega_C \cap U$;
9 **else**
10 Let $\tilde{\boldsymbol{\theta}}_2, \boldsymbol{\theta}_2$ be the falsified/true phase angles at t_2 under attack pair $(\boldsymbol{a}_p, e_t)$;
11 Set $u := \arg\max_{v \in \Omega_C} |\tilde{\theta}_{2,v} - \theta_{2,v}|$;
12 $\Omega_{\text{AC}} \leftarrow \Omega_{\text{AC}} \cup \{u\}$;

V. Numerical Experiments

Simulation Settings: We evaluate our solution against benchmarks in several standard systems: IEEE 30-bus, IEEE 57-bus, IEEE 118-bus, and IEEE 300-bus system, where the system parameters as well as load profiles are obtained from [41]. The parameters for our evaluation are set as follows unless specified otherwise: We set $\alpha = 0.25$ according to [11]. We allow $\tilde{\boldsymbol{\theta}}_3$ to take any value specified by the attacker subject to (5b)-(5d), which makes our defense effective under any SCED cost vector. The attacker's capability is set as $\xi_p = 2$, $\xi_c = \infty$ (no constraint on the number of manipulated meters). We set the overload-induced tripping threshold to $\gamma_e = 1.2, \forall e \in E$, which is slightly smaller than the one used in [11] to make the solution more robust. For Alg. 2, we set $K_c = K_A = K_L = 10$.

In the rest of this section, we will compare the performance of Alg. 1 (AONG or AODC) and Alg. 2 with the following benchmarks: (i) PMU placement to achieve full observability as proposed in [26]; (ii) greedily placing PMUs in the descending order of node degrees until attack-induced overload-induced tripping is prevented, referred to as "GreedyDegree". Benchmark (i) represents the current approach, and benchmark (ii) represents a baseline solution under the lowered goal of defense.

Savings in the Number of PMUs: In Table II, we compare the number of secured PMUs required by the proposed algorithms (Alg. 1, Alg. 2) with the benchmarks under the nominal operating point [41]. The minimum number of PMUs required to avoid outages, given by Alg. 1 (either AONG or AODC), is significantly smaller than what is required to achieve full observability. Alg. 2 closely approximates the minimum for the tested systems, but a simple heuristic such as GreedyDegree does not. For IEEE 300-bus system, we have skipped Alg. 1 as neither AODC nor AONG can converge within 72 hours. The details of PMU locations are given in Appendix F.

Table II
Comparison of the Required Number of PMUs

	30-bus	57-bus	118-bus	300-bus
Alg. 1 (optimal)	2	3	9	—
Alg. 2	2	3	10	31
GreedyDegree	3	3	14	85
Full observability	10	17	32	87

Then, we evaluate the scenario when the solution by PPOP is used as a temporary PMU placement that will eventually be augmented into a placement achieving full observability, as discussed at the end of Section II (Remark 2). To this end, we evaluate the following metrics: (i) the minimum number of PMUs required by PPOP $|\Omega_{\text{PPOP}}|$, (ii) the minimum number of PMUs for achieving full observability $|\Omega_{\text{FO}}|$, (iii) the size of a full-observability placement Ω_C augmented from Ω_{PPOP} given by (37), and (iv) the size of the optimal solution Ω'_{PPOP} to a variation of PPOP with the additional constraint that $\Omega'_{\text{PPOP}} \subseteq \Omega_{\text{FO}}$. In Table III, we observe that (i) $|\Omega'_{\text{PPOP}}|$ is only slightly larger than $|\Omega_{\text{PPOP}}|$, i.e., most of the cost savings by PPOP is still achievable when its solution is required to be consistent with the optimal long-term solution that achieves full observability, but (ii) $|\Omega_C|$ can be notably larger than $|\Omega_{\text{FO}}|$ for large systems, i.e., augmenting an arbitrary solution to PPOP to achieve full observability may require notably more PMUs compared to a clean-slate solution.

Table III
Comparison of #PMUs under Temporary/Long-term Placement

	30-bus	57-bus	118-bus	300-bus
$\lvert\Omega_{\text{PPOP}}\rvert$	2	3	9	31
$\lvert\Omega'_{\text{PPOP}}\rvert$	2	3	10	34
$\lvert\Omega_C\rvert$	10	17	33	95
$\lvert\Omega_{\text{FO}}\rvert$	10	17	32	87

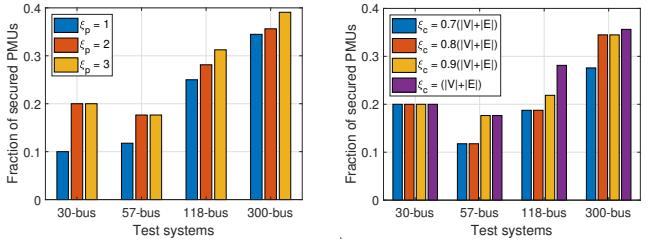
Impact of System Parameters: We evaluate the impact of various system parameters on the number of PMUs required by PPOP, given by Alg. 1 (by Alg. 2 for the 300-bus system).

First, we study the effect of α introduced in (12), where a larger α implies a larger feasible region for the attacker. It can be seen from Table IV that (i) PPOP can still significantly reduce the required number of PMUs compared to "Full observability" (see Table II) even if α is large, and (ii) PPOP benefits from a small value of α, which signifies the importance of precise load forecasting in defending against CCPA.

Table IV
Number of PMUs in PPOP under varying α

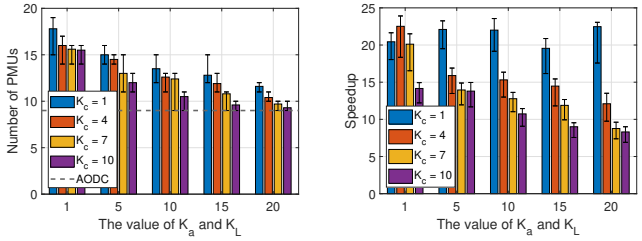
	30-bus	57-bus	118-bus	300-bus
$\alpha = 0.01$	1	1	4	24
$\alpha = 0.10$	1	2	6	30
$\alpha = 0.25$	2	3	9	31
$\alpha = 0.50$	3	3	11	34

Then, we vary ξ_p and ξ_c to evaluate the impact of the attacker's capability. As shown in Figure 2, (i) defending



(a) Effect of ξ_p (b) Effect of ξ_c

Figure 2. $\frac{\text{\#PMUs required by PPOP}}{\text{\#PMUs required by full observability}}$ ($\xi_c = |V|+|E|$ means no ξ_c-constraint).



(a) Number of secured PMUs (b) Computation time

Figure 3. The performance of Alg. 2 under different K_c, K_A, and K_L.

against a stronger attacker requires more PMUs as expected, (ii) PPOP still requires much fewer PMUs than "Full observability" when the attacker can disconnect multiple lines and manipulate all the meters (except for the secured PMUs), which is stronger than the attack model considered in [11], [18], and (iii) PPOP can save a larger fraction of PMUs in IEEE 57-bus system since $\boldsymbol{f}_{\max}$ given in [41] is large.

In addition, we consider the case that the load profile $\boldsymbol{p}_0$ can vary as shown in (25). We assume $\boldsymbol{p}_0 \in [\underline{\kappa}\boldsymbol{p}^{(0)}, \overline{\kappa}\boldsymbol{p}^{(0)}]$, where $\boldsymbol{p}^{(0)}$ is the nominal load profile from [41], $\underline{\kappa} = 0.5$ and $\overline{\kappa}$ is set to the maximum value that keeps (5) feasible under $\overline{\kappa}\boldsymbol{p}^{(0)}$. In our evaluations, we set $\overline{\kappa}$ as $1.95, 2.69$, 2.41 and 1.61 for IEEE 30-bus, 57-bus, 118-bus and 300-bus systems, respectively. For the given range, PPOP requires 3, 4, 19, and 33 PMUs for the 30-bus, 57-bus, 118-bus, and 300-bus systems, which is more than what is required under a single load profile as expected. Nevertheless, PPOP can still save PMUs compared to "Full observability" as shown in Table II.

Computational Efficiency: We compare AODC and AONG in terms of the number of iterations (which is also the number of examined attack pairs) and the running time, which is evaluated in a platform with Intel i7-8700 CPU with Gurobi as the solver. Since any feasible solution to (26) can form an "No-Good" constraint, we set an upper-bound on the time for solving (26), which is 1200 seconds. As shown in Table V, while the two algorithms perform similarly for small systems, AODC converges notably faster for larger systems such as the 118-bus system thanks to its reduced solution space due to the adoption of both "No-Good" and "Attack-Denial" constraints. Note that both algorithms converge after examining a small fraction of possible attack pairs (the total number of attack pairs is 33620, 252800, and 3200130 for these systems, respectively).

Table V
NUMBER OF ITERATIONS/CONVERGENCE TIME (10^3 SEC)

	30-bus	57-bus	118-bus
AODC	8/0.021	3/2.188	16/26.64
AONG	7/0.014	4/2.163	78/74.44

Moreover, we use IEEE 118-bus system as an example to demonstrate the trade-off in tuning the parameters K_c, K_A, K_L for Alg. 2 (assuming $K_A = K_L$). We run Alg. 2 for 5 times under each setting due to the randomness in solving (23) and breaking ties. The results are given in Fig. 3, where the bar denotes the mean and the error bar denotes the minimum/maximum. In Fig. 3 (b), we show the speedup of the heuristic compared to AODC in convergence time, i.e., $(\text{time of AODC})/(\text{time of heuristic})$. We observe that (i) Alg. 2 can return a good solution when $K_c \geq \%10 \cdot |V|$ and $K_A = K_L \geq K_c$, and (ii) under this configuration, Alg. 2 is significantly faster than AODC at a small cost of requiring a couple of more PMUs.

Extension to AC model: We compare the solution Ω_{AC} obtained by Alg. 5 with the best previous solution Ω_{DC} obtained under the DC approximation. As shown in Table VI, although the DC-based solution may need augmentation to defend against AC-based CCPA, the gap (i.e., $|\Omega_{\text{AC}}| - |\Omega_{\text{DC}}|$) is small. More importantly, $|\Omega_{\text{AC}}|$ is still much smaller (by 60–80%) than the number of PMUs $|\Omega_{\text{FO}}|$ required to achieve full observability (see Table III), indicating the efficacy of our approach of first computing an initial solution under the DC approximation and then augmenting it to achieve our defense goal under the AC model. We note that the values of $|\Omega_{\text{AC}}|$ in Table VI are only upper bounds on the number of PMUs required to prevent outages under AC-based CCPA, suggesting great potential of saving PMUs by adopting the proposed defense goal.

Table VI
NUMBER OF PMUS UNDER AC POWER FLOW MODEL

	30-bus	57-bus	118-bus	300-bus
$\lvert\Omega_{\text{AC}}\rvert$	3	3	10	34
$\lvert\Omega_{\text{DC}}\rvert$	2	3	9	31

VI. CONCLUSION

We formulate a tri-level optimization problem under the DC power flow model to find the optimal secured PMU placement to defend against the coordinated cyber-physical attack (CCPA) in the smart grid. Rather than completely eliminating the attack, we propose to limit the impact of the attack by preventing overload-induced outages. To solve the proposed problem, we first transform it into a bi-level MILP and then propose an alternating optimization algorithm framework to obtain optimal solutions. The core of the proposed algorithm framework is constraint generation based on infeasible placements, for which we develop two constraint generation approaches. Furthermore, we propose a polynomial-time heuristic algorithm that can scale to large-scale grids. In addition, we demonstrate how to extend the obtained PMU placement to achieve our defense goal under the AC power flow model. Our experimental results on standard test systems demonstrate great promise of the proposed approach in reducing the requirement of PMUs. Our work lays the foundation for tackling a number of further questions in future work, e.g., how to characterize the optimal attack without solving MILPs, how to directly optimize the

PMU placement for outage prevention under the AC model, and how to improve the robustness of the solution against the failures of PMUs themselves.

REFERENCES

[1] Y. Huang, T. He, N. R. Chaudhuri, and T. L. Porta, "Preventing outages under coordinated cyber-physical attack with secured PMUs," in *IEEE SmartGridComm*. IEEE, 2021.

[2] R. Deng, P. Zhuang, and H. Liang, "Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[3] P. Fairley, "Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory," *IEEE Spectrum*, vol. 53, no. 5, pp. 11–13, May 2016.

[4] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[5] K. C. Sou, "Protection placement for power system state estimation measurement data integrity," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 638–647, 2019.

[6] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual reviews in control*, vol. 47, pp. 394–411, 2019.

[7] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

[8] T. A. Alexopoulos, G. N. Korres, and N. M. Manousakis, "Complementarity reformulations for false data injection attacks on pmu-only state estimation," *Electric Power Systems Research*, vol. 189, p. 106796, 2020.

[9] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[10] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Transactions on Smart Grid*, 2021.

[11] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, 2018.

[12] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592–1602, 2016.

[13] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2015.

[14] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 163–178, 2016.

[15] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. A. Mohammed, and S. A. Zonouz, "Hey, my malware knows physics! attacking PLCs with physical model aware rootkit." in *NDSS*, 2017.

[16] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2015.

[17] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1802–1810, 2016.

[18] M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin, and L. Zhao, "Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid," *IEEE Access*, vol. 7, pp. 9836–9847, 2019.

[19] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[20] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1–12, 2015.

[21] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal pmu placement-based defense against data integrity attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1735–1750, 2017.

[22] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electric Power Systems Research*, vol. 151, pp. 12–25, 2017.

[23] X. Wu and A. J. Conejo, "An efficient tri-level optimization model for electric grid defense planning," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2984–2994, 2016.

[24] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 4, pp. 712–718, 2007.

[25] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *First Workshop on Secure Control Systems*, vol. 2010. Stockholm, Sweden, 2010.

[26] S. Chakrabarti, E. Kyriakides, and D. G. Eliades, "Placement of synchronized measurements for power system observability," *IEEE Transactions on power delivery*, vol. 24, no. 1, pp. 12–19, 2008.

[27] W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang, and B. Zeng, "Robust optimization-based resilient distribution network planning against natural disasters," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2817–2826, 2016.

[28] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2015.

[29] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid ac-based state estimation: Vulnerability analysis against cyber attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 1784–1799, 2019.

[30] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4577–4588, 2018.

[31] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "N-1 reliability makes it difficult for false data injection attacks to cause physical consequences," *IEEE Transactions on Power Systems*, 2021.

[32] ——, "Vulnerability assessment of large-scale power systems to false data injection attacks," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2020, pp. 1–6.

[33] Z. Yang, K. Xie, J. Yu, H. Zhong, N. Zhang, and Q. Xia, "A general formulation of linear power flow models: Basic theory and error analysis," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1315–1324, 2018.

[34] G. Krumpholz, K. Clements, and P. Davis, "Power system observability: a practical algorithm using network topology," *IEEE Transactions on Power Apparatus and Systems*, no. 4, pp. 1534–1542, 1980.

[35] "System operating limit definition and exceedance clarification," Online, March 2014, https://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/2014_03_fourth_posting_white_paper_sol_exceedance_20141201_clean.pdf.

[36] "Nerc standard prc-023-1," Online, February 2008, https://www.nerc.com/files/prc-023-1.pdf.

[37] M. H. Athari and Z. Wang, "Impacts of wind power uncertainty on grid vulnerability to cascading overload failures," *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 128–137, 2017.

[38] O. L. Mangasarian, *Nonlinear programming*. SIAM, 1994.

[39] A. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[40] C. Coffrin, H. L. Hijazi, and P. Van Hentenryck, "The qc relaxation: A theoretical and computational study on optimal power flow," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3008–3018, 2015.

[41] S. Babaeinejadsarookolaee, A. Birchfield, R. D. Christie, C. Coffrin, C. DeMarco, R. Diao, M. Ferris, S. Fliscounakis, S. Greene, R. Huang *et al.*, "The power grid library for benchmarking ac optimal power flow algorithms," *arXiv preprint arXiv:1908.02788*, 2019.

[42] C. Coffrin, H. L. Hijazi, and P. Van Hentenryck, "Distflow extensions for ac transmission systems," *arXiv preprint arXiv:1506.04773*, 2015.

[43] M. Porter, P. Hespanhol, A. Aswani, M. Johnson-Roberson, and R. Vasudevan, "Detecting generalized replay attacks via time-varying dynamic watermarking," *IEEE Transactions on Automatic Control*, vol. 66, no. 8, pp. 3502–3517, 2020.

[44] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[45] J. P. Vielma, "Mixed integer linear programming formulation techniques," *Siam Review*, vol. 57, no. 1, pp. 3–57, 2015.

[46] T. Terlaky, *Interior point methods of mathematical programming*. Springer Science & Business Media, 2013, vol. 5.

APPENDIX A
MILP FORMULATION OF ATTACKER'S PROBLEM

In this section, we will demonstrate how to transform (23) into a MILP, which can be efficiently solved by existing solver such as Gurobi.

To begin with, we give an overview of the PPOP, as shown in Fig. 4.

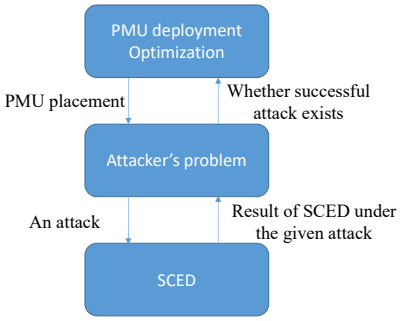


Figure 4. Overview of the PPOP

We first consider the case that lower-level optimization (5) returns the set of $\boldsymbol{\theta}$'s satisfying (5b)-(5d), i.e., it returns the feasible region of SCED rather than a single solution. In this case, (23) becomes a single-level problem.

Below, we show how to convert the single-level formulation of (23) into a MILP. To convert (18) and (23e) into linear constraints, we introduce a constant $M_{2,\theta}$ (defined in Appendix B) such that (18a) holds if and only if the following holds:

$$\tilde{\theta}_{2,u} - \theta_{2,u} \le M_{2,\theta} \cdot (1 - \boldsymbol{x}_{N,u}), \tag{38a}$$

$$\tilde{\theta}_{2,u} - \theta_{2,u} \ge -M_{2,\theta} \cdot (1 - \boldsymbol{x}_{N,u}), \tag{38b}$$

and similar conversion applies to (18b). As for (23e), by defining a sufficiently large constant $M_{\pi,e}$ (see Appendix B) and two binary auxiliary variables $\pi_{n,e}, \pi_{p,e}$ to get rid of the absolute value operation, (23e) is transformed into

$$-M_{\pi,e} \cdot (1 - \pi_{p,e}) < \frac{f_{3,e}}{f_{\max,e}} - \gamma_e \le M_{\pi,e} \cdot \pi_{p,e}, \tag{39a}$$

$$-M_{\pi,e} \cdot (1 - \pi_{n,e}) < \frac{-f_{3,e}}{f_{\max,e}} - \gamma_e \le M_{\pi,e} \cdot \pi_{n,e}. \tag{39b}$$

We claim that $\pi_e = \pi_{n,e} + \pi_{p,e}$. To see this, suppose that $f_{3,e} \ge 0$. Then, we must have $-\frac{f_{3,e}}{f_{\max,e}} - \gamma_e \le 0$ and thus $\pi_{n,e} = 0$, while $\frac{|f_{3,e}|}{f_{\max,e}} - \gamma_e = \frac{f_{3,e}}{f_{\max,e}} - \gamma_e$ and thus $\pi_{p,e} = \pi_e$. Notice that we must have $\pi_e = 1$ if $|f_{3,e}| - \gamma_e \cdot f_{\max,e} > 0$, while $|f_{3,e}| - \gamma_e \cdot f_{\max,e} \le 0$ leads to $\pi_e = 0$.

To linearize (20g), we introduce binary variables $\boldsymbol{w}_f \in \{0,1\}^{|m_L|}$ and $\boldsymbol{w}_p \in \{0,1\}^{|m_N|}$ for data injection on line measurements and node measurements, respectively. Then, (20g) can be transformed into (see definitions of $M_{c,f}$, $M_{c,p}$ in Appendix B)

$$-M_{c,f}\boldsymbol{w}_f \le \boldsymbol{\Lambda}_f \left(\tilde{\boldsymbol{f}}_2 - \boldsymbol{f}_2\right) \le M_{c,f}\boldsymbol{w}_f, \tag{40a}$$

$$-M_{c,p}\boldsymbol{w}_p \le \boldsymbol{\Lambda}_p \left(\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{p}_0\right) \le M_{c,p}\boldsymbol{w}_p, \tag{40b}$$

$$\mathbf{1}^T\boldsymbol{w}_f + \mathbf{1}^T\boldsymbol{w}_p \le \xi_c. \tag{40c}$$

Together, the above techniques transform (23) into a MILP. Specifically, the binary decision variables are $\{\boldsymbol{\pi}_n, \boldsymbol{\pi}_p, \boldsymbol{a}_p, \boldsymbol{w}_f, \boldsymbol{w}_p\}$, continuous variables are $\{\tilde{\boldsymbol{\theta}}_2, \tilde{\boldsymbol{\theta}}_3, \boldsymbol{\theta}_2, \boldsymbol{\theta}_3, \boldsymbol{f}_2, \boldsymbol{f}_3, \tilde{\boldsymbol{f}}_2, \boldsymbol{f}_{con}\}$, where $\boldsymbol{w}_f, \boldsymbol{w}_p$ are introduced auxiliary variables. Then, the full formulation without considering the optimality of (5) is given as follows.

$$\max \quad \|\boldsymbol{\pi}_p + \boldsymbol{\pi}_n\|_0 \tag{41a}$$

s.t.

$$\boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} \le \boldsymbol{x}_N \le \boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} + \frac{\|\boldsymbol{\Delta}\|_\infty - 1}{\|\boldsymbol{\Delta}\|_\infty}, \tag{41b}$$

$$\frac{1}{2}|\boldsymbol{D}|^T\boldsymbol{\beta} \le \boldsymbol{x}_L \le \frac{1}{2}|\boldsymbol{D}|^T\boldsymbol{\beta} + \zeta, \tag{41c}$$

$$-(\mathbf{1} - \boldsymbol{a}_p) \le \operatorname{diag}(\boldsymbol{\gamma} \odot \boldsymbol{f}_{\max})^{-1} \boldsymbol{f}_2 \le \mathbf{1} - \boldsymbol{a}_p, \tag{41d}$$

$$\tilde{\boldsymbol{D}}\boldsymbol{f}_2 = \boldsymbol{p}_0, -M_{2,f}\boldsymbol{a}_p \le \boldsymbol{\Gamma}\boldsymbol{D}\boldsymbol{\theta}_2 - \boldsymbol{f}_2 \le M_{2,f}\boldsymbol{a}_p, \tag{41e}$$

$$-\boldsymbol{f}_{\max} \le \tilde{\boldsymbol{f}}_2 \le \boldsymbol{f}_{\max}, \ \boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\tilde{\boldsymbol{\theta}}_2 - \tilde{\boldsymbol{f}}_2 = 0, \tag{41f}$$

$$-\alpha|\boldsymbol{p}_0| \le \tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 - \boldsymbol{p}_0 \le \alpha|\boldsymbol{p}_0|, \tag{41g}$$

$$\boldsymbol{\Lambda}_g\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2 = \boldsymbol{\Lambda}_g\boldsymbol{p}_0, \tag{41h}$$

$$-M_{c,f}\boldsymbol{w}_f \le \boldsymbol{\Lambda}_f \left(\tilde{\boldsymbol{f}}_2 - \boldsymbol{f}_2\right) \le M_{c,f}\boldsymbol{w}_f, \tag{41i}$$

$$-M_{c,p}\boldsymbol{w}_p \le \tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{p}_0 \le M_{c,p}\boldsymbol{w}_p, \tag{41j}$$

$$\mathbf{1}^T\boldsymbol{w}_f + \mathbf{1}^T\boldsymbol{w}_p \le \xi_c, \ \|\boldsymbol{a}_p\|_0 \le \xi_p, \tag{41k}$$

$$\tilde{\theta}_{2,u} - \theta_{2,u} \le M_{2,\theta} \cdot (1 - \boldsymbol{x}_{N,u}), \tag{41l}$$

$$\tilde{\theta}_{2,u} - \theta_{2,u} \ge -M_{2,\theta} \cdot (1 - \boldsymbol{x}_{N,u}), \tag{41m}$$

$$\boldsymbol{p}_{g,min} \le \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 \le \boldsymbol{p}_{g,max}, \tag{41n}$$

$$-\boldsymbol{f}_{\max} \le \boldsymbol{\Gamma}\boldsymbol{D}^T\tilde{\boldsymbol{\theta}}_3 \le \boldsymbol{f}_{\max}, \tag{41o}$$

$$\boldsymbol{\Lambda}_d\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 = \boldsymbol{\Lambda}_d\tilde{\boldsymbol{D}}\tilde{\boldsymbol{f}}_2, \tag{41p}$$

$$-M_{3,a}(\mathbf{1} - \boldsymbol{a}_p) \le \boldsymbol{f}_3 \le M_{3,a}(\mathbf{1} - \boldsymbol{a}_p), \tag{41q}$$

$$\boldsymbol{\Lambda}_d\tilde{\boldsymbol{D}}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_d\boldsymbol{p}_0, \quad \boldsymbol{\Lambda}_g\tilde{\boldsymbol{D}}\boldsymbol{f}_3 = \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3, \tag{41r}$$

$$-M_{3,f}\boldsymbol{a}_p \le \boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\boldsymbol{\theta}_3 - \boldsymbol{f}_3 \le M_{3,f}\boldsymbol{a}_p, \tag{41s}$$

$$\theta_{2,u_0} = \theta_{3,u_0} = \tilde{\theta}_{2,u_0} = \tilde{\theta}_{3,u_0} = 0, \tag{41t}$$

$$-\cdot(1 - \pi_{p,e}) < \frac{f_{3,e}}{M_{\pi,e}f_{\max,e}} - \frac{\gamma_e}{M_{\pi,e}} \le \cdot\pi_{p,e}, \forall e, \tag{41u}$$

$$-\cdot(1 - \pi_{n,e}) < \frac{-f_{3,e}}{M_{\pi,e}f_{\max,e}} - \frac{\gamma_e}{M_{\pi,e}} \le \cdot\pi_{n,e}, \forall e, \tag{41v}$$

$$\tilde{\boldsymbol{D}}_u\boldsymbol{f}_{con} = \begin{cases} |V| - 1, & \text{if } u = u_0, \\ -1, & \text{if } u \in V \setminus \{u_0\}, \end{cases} \tag{41w}$$

$$-|V| \cdot (1 - a_{p,e}) \le f_{con,e} \le |V| \cdot (1 - a_{p,e}) \tag{41x}$$

The constraints (41b)-(41c) correspond to (16)-(17), (41d)-(41e) correspond to (19a)-(19c), (41f)-(41k) correspond to (20), (41l)-(41m) correspond to (38), (41n)-(41s) correspond to (21), (41t) corresponds to (23c), (41u)-(41v) correspond to (23e), (41w)-(41x) correspond to (14).

If we do not relax the optimality requirements in (5), we need to introduce additional binary variables $\{\boldsymbol{r}_{fl}, \boldsymbol{r}_{fu}, \boldsymbol{r}_{gl}, \boldsymbol{r}_{gu}\}$ and continuous dual variables $\{\boldsymbol{\mu}_b, \boldsymbol{\mu}_c, \boldsymbol{\mu}_d, \boldsymbol{\mu}_e, \boldsymbol{\mu}_g\}$ to transform (5) into a linear system by using its KKT conditions [9]. Specifically, we add the following linear system into (41) for the completeness of KKT conditions of (5):

$$\tilde{\boldsymbol{B}}\boldsymbol{\Lambda}_d^T\boldsymbol{\mu}_b + \tilde{\boldsymbol{D}}\boldsymbol{\Gamma}\boldsymbol{\mu}_c + \tilde{\boldsymbol{D}}\boldsymbol{\Gamma}\boldsymbol{\mu}_d + \tilde{\boldsymbol{B}}\boldsymbol{\Lambda}_g^T\boldsymbol{\mu}_e - \tilde{\boldsymbol{B}}\boldsymbol{\Lambda}_g^T\boldsymbol{\mu}_g = -\tilde{\boldsymbol{B}}\boldsymbol{\Lambda}_g^T\boldsymbol{\phi} \tag{42a}$$

$$\boldsymbol{\mu}_c - M\boldsymbol{r}_{fl} \le \mathbf{0}, \tag{42b}$$

$$\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\tilde{\boldsymbol{\theta}}_3 + M\boldsymbol{r}_{fl} \le M - \boldsymbol{f}_{\max} \tag{42c}$$

$$\boldsymbol{\mu}_d - M\boldsymbol{r}_{fu} \le \mathbf{0}, \tag{42d}$$
$$-\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\tilde{\boldsymbol{\theta}}_3 + M\boldsymbol{r}_{fl} \le M - \boldsymbol{f}_{\max} \tag{42e}$$
$$\boldsymbol{\mu}_e - M\boldsymbol{r}_{gl} \le \mathbf{0}, \tag{42f}$$
$$\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 + M\boldsymbol{r}_{gl} \le \boldsymbol{p}_{g,min} + M\mathbf{1} \tag{42g}$$
$$\boldsymbol{\mu}_g - M\boldsymbol{r}_{gu} \le \mathbf{0}, \tag{42h}$$
$$-\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3 + M\boldsymbol{r}_{gu} \le -\boldsymbol{p}_{g,max} + M\mathbf{1} \tag{42i}$$
$$\boldsymbol{r}_{gl} + \boldsymbol{r}_{gu} \le \mathbf{1} \tag{42j}$$
$$\boldsymbol{r}_{fl} + \boldsymbol{r}_{fu} \le \mathbf{1} \tag{42k}$$
$$\boldsymbol{\mu}_c, \boldsymbol{\mu}_d, \boldsymbol{\mu}_e, \boldsymbol{\mu}_g \ge \mathbf{0} \tag{42l}$$

Compared to the attacker's formulations in [1], [13] that also optimize the location of physical attacks, the key advantage of (23) is avoiding McCormick's relaxation for bilinear terms (22) and reducing the numbers of variables and constraints. Specifically, McCormick's relaxation in [1] will introduce $2|E||V|$ additional continuous variables and $8|E||V|$ additional constrains. The cost of avoiding bilinear term in (23) is the additional variables $\boldsymbol{f}_2, \boldsymbol{f}_3, \tilde{\boldsymbol{f}}_2$ and the associated constraints, although the benefit usually outweighs the cost. For example, for the IEEE 118-bus system, the formulation in [1] has 44436 continuous variables and $178,596$ constraints, while (23) only has 1216 continuous variables and $5,802$ constraints.

APPENDIX B
CALCULATION OF BIG-M

In this section, we will explain how to calculate $M_{2,a,e}$ in (19a), $M_{2,f}$ in (19c), $M_{3,a}$ in (21d), $M_{2,\theta}$ in (38), $M_{3,f}$ in (21f), $M_{\pi,e}$ in (39), $\overline{M}_F, \underline{M}_F$ in (33), $M_{c,f}, M_{c,p}$ in (40) and M_q in (34c). In this section, we denote $\mathcal{N} = (V, E)$ as the graph before physical attack while $\mathcal{N}' = (V, E')$ as the graph after attack.

We first show how to calculate $M_{2,a}$, $M_{2,f}$ and $M_{2,\theta}$. Suppose that the power grid is designed to be robust to $N-k$ contingency. Then, the value of $M_{2,a}$ depends on $\xi_p - k$. If $\xi_p - k \le 0$, then we can set $M_{2,a,e} := f_{\max,e}$ or $M_{2,a,e} := \gamma_e f_{\max,e}$, since no $\boldsymbol{a}_p$ can cause overloading. Otherwise, we set $M_{2,a,e} := C_{2,a}\gamma_e f_{\max,e}$ with a parameter $C_{2,a} > 1$. In our simulations, we find that $C_{2,a} := 3$ suffices since $\xi_p - k$ is usually small. Next, we bound $|\boldsymbol{\theta}_2|$ by defining $M_{\theta_2,u} \ge \max_{\boldsymbol{a}_p} |\theta_{2,u}|$ and $M_{\theta_2} \ge \max_{\boldsymbol{a}_p} \max_u |\theta_{2,u}|$ since the value of $\boldsymbol{\theta}_2$ depends on $\boldsymbol{a}_p$. An intuitive way of obtaining $M_{\theta_2,u}$ is enumerating all possible values of $\boldsymbol{a}_p$, whose time complexity is polynomial in $|E|$ and $|V|$ if $\xi_p = \mathcal{O}(1)$. Here we provide another way of bounding $M_{\theta_2,u}$. Due to our assumption of the connected $\mathcal{N}$, there exists at least one path in $\mathcal{N}$ connecting the reference node u_0 to each node $u \in V$. Moreover, for each path connecting u_0 and u, say $Pa(u_0, u) := (e_0, e_1, \cdots, e_J)$ where $e_0 = (u_0, v_1)$, $e_j = (v_j, v_{j+1})$ and $e_J = (v_J, u)$, we have $\theta_{2,u} - \theta_{2,u_0} = \theta_{2,s} - \theta_{2,v_1} + \theta_{2,v_1} - \cdots + \theta_{2,v_J} - \theta_{2,t}$, which leads to

$$\begin{aligned}\max_{\boldsymbol{a}_p} |\theta_{2,u}| &= \max_{\boldsymbol{a}_p} |\theta_{2,u} - \theta_{2,u_0}| \\ &\le \sum_{j=0}^{J} r_{e_j} M_{2,a,e_j} := M_{Pa}(\theta_{2,u})\end{aligned} \tag{43}$$

since $\theta_{2,u_0} = 0$ in our assumption and $|\theta_{2,v_j} - \theta_{2,v_{j+1}}| \le r_{e_j} M_{2,a,e_j}$ due to (19a). Denote n_p as the number of different paths connecting u and u_0. Then, since the physical attack will disconnect at most ξ_p lines, we set $M_{\theta_2,u} := \max\{M_{Pa_i}(\theta_{2,u})\}_{i=1}^{\min\{\xi_p+1, n_p\}}$.

Equipped with $M_{\theta_2,u}, u \in V$, we can calculate $M_{2,f}$ and $M_{2,\theta}$. We define an intermediate constant $M_{2,f,e}$ for each line such that $M_{2,f} = \max_{e\in E} M_{2,f,e}$. Then, for $e = (u, v)$ we can set $M_{2,f,e} := r_e(M_{\theta_2,u} + M_{\theta_2,v})$ since $|\Gamma_e \tilde{\boldsymbol{d}}_e^T \boldsymbol{\theta}_2 - f_{2,e}| > 0$ only if $a_{p,e} = 1$ and $f_{2,e} = 0$.

To obtain $M_{2,\theta}$, we first bound $M_{\tilde{\theta}_2,u} \ge \max_{\boldsymbol{a}_p, \boldsymbol{a}_c} |\tilde{\theta}_{2,u}|, u \in V$ in a similar way as that in (43). Specifically, since $\tilde{\boldsymbol{\theta}}_2$ is estimated by CC based on the topology $\mathcal{N}$, we can arbitrarily choose one path $(e_0, e_1, \cdots, e_J)$ in $\mathcal{N}$ that connects u and u_0 and set

$$M_{\tilde{\theta}_2,u} := \sum_{j=0}^{J} r_{e_j} f_{max,e_j} \ge \max_{\boldsymbol{a}_p, \boldsymbol{a}_c} |\tilde{\theta}_{2,u}|. \tag{44}$$

Then, we can set $M_{2,\theta} := \max_{u\in V}(M_{\tilde{\theta}_2,u} + M_{\theta_2,u})$.

Now, we are ready to demonstrate the calculation of $M_{3,a}$ and $M_{3,f}$. As for $M_{3,a}$, we only require $M_{3,a,e} > \gamma_e f_{\max,e}$ and $M_{3,a} \ge \max_{e\in E} \gamma_e f_{\max,e}$ so that the attacker can cause outages over any lines. In practice, we can set $M_{3,a} := c \max_{e\in E} \gamma_e f_{\max,e}$ with $c > 1$. As for $M_{3,f}$, we again first show that we can bound $|\theta_{3,u}| \le M_{\theta_3,u}$ without hurting the attacker's objective. We notice that the topology of grid at t_3 before lines facing outage automatically disconnect themselves is still $\mathcal{N}'$. Thus, we can set $M_{\theta_3,u}$ similarly as $M_{\theta_2,u}$, except that (43) becomes:

$$\max_{\boldsymbol{a}_p} |\theta_{3,u}| \le \sum_{j=0}^{J} r_{e_j} M_{a,e_j} := M_{Pa}(\theta_{3,u}). \tag{45}$$

Then, we can set $M_{\theta_3,u} := \max\{M_{Pa_i}(\theta_{3,u})\}_{i=1}^{\min\{\xi_p+1, n_p\}}$, $M_{3,f,e} := r_e(M_{\theta_3,u} + M_{\theta_3,v})$ for $e = (u, v) \in E$, and $M_{3,f} = \max_{e\in E} M_{3,f,e}$.

Equipped with $M_{3,a,e}$, $M_{\pi,e}$ can be easily set as $c \cdot (\frac{M_{3,a,e}}{f_{\max,e}} + \gamma_e)$ with any constant $c > 1$.

We can set $\overline{M}_F$ as 0 since $\boldsymbol{q}_2 \ge \mathbf{0}$ and $F_{3,i,u} \in \{0, -M_{2,\theta}\}$, $\forall i, u$. There is no simple guidelines for $\underline{M}_F$ in (33) since it is the bound for dual variables. In practice, we can initialize $\underline{M}_F$ to a given value and solve (31) for each attack pair separately. Then, we iteratively decrease $\underline{M}_F$ until (31) is feasible under each attack pair separately. In our simulations, we set $\underline{M}_F := -M_{2,\theta}^2$. Equipped with $\underline{M}_F$, we can set $M_q := \frac{2M_F}{M_{2,\theta}}$.

Finally, we demonstrate how to set $M_{c,f}$ and $M_{c,p}$. Due to (19a) and (20a), we have $|\tilde{f}_{2,e} - f_{2,e}| \le (1 + \gamma_e) f_{\max,e}$, which implies that we can set $M_{c,f} := \max_{e\in E}(1 + \gamma_e) f_{\max,e}$. Similarly, we can set $M_{c,p} := \alpha\|\boldsymbol{p}_0\|_\infty$ due to (20e).

APPENDIX C
EFFICIENCY ANALYSIS OF "NO-GOOD" CONSTRAINTS

We have the following observations about AONG:

1) *Cold start*. The efficiency of (27) can be characterized by the number of infeasible $\boldsymbol{\beta}$'s that are cut out. Let $\{\hat{\boldsymbol{\beta}}^{(k)}\}_{k=1}^{K}$ be the PMU placements obtained in the first

K iterations of Alg. 1 and $\{\hat{\boldsymbol{\beta}}^{'(k)}\}_{k=1}^{K}$ the corresponding augmented placements obtained from (26). Then, the number of feasible $\boldsymbol{\beta}$'s for the next iteration is at least

$$\left(2^{|\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c|}-1\right)\cdot 2^{|V|-|\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c|} \tag{46}$$

if $\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c\neq\emptyset$, as placing at least one PMU in $\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c$ will satisfy (27) for every placement in $\{\hat{\boldsymbol{\beta}}^{'(k)}\}_{k=1}^{K}$. This implies that the number of $\boldsymbol{\beta}$'s that are cut out is at most $2^{|V|-|\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c|}$. Therefore, the first K "No-Good" constraints (27) added in Alg. 1 will be inefficient if $|\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c|$ is large. We observe that $|\bigcap_{k=1}^{K}\Omega(\hat{\boldsymbol{\beta}}^{'(k)})^c|$ is large at the beginning of Alg. 1 and decreases quickly as $\|\hat{\boldsymbol{\beta}}^{(k)}\|_0$ increases.

2) *Repeated successful attacks*. Another cause of inefficiency is that for many PMU placements enumerated by AONG, there exist successful attacks based on the same attack pair $(\boldsymbol{a}_p, e)$, indicating that new constraints are needed to better defend against identified attacks.

APPENDIX D
THE DETAILS OF COEFFICIENTS IN ATTACKER'S PROBLEM

The linear system (28a) is the composition of (20f), (21e) and (21c), which can be expanded into:

$$\begin{bmatrix}\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \boldsymbol{\Lambda}_d\boldsymbol{B}\\ \mathbf{0} & -\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}} & \boldsymbol{\Lambda}_g\boldsymbol{B}\\ \boldsymbol{\Lambda}_d\tilde{\boldsymbol{B}} & -\boldsymbol{\Lambda}_d\tilde{\boldsymbol{B}} & \mathbf{0}\end{bmatrix}\begin{bmatrix}\tilde{\boldsymbol{\theta}}_2\\ \tilde{\boldsymbol{\theta}}_3\\ \boldsymbol{\theta}_3\end{bmatrix}=\begin{bmatrix}\boldsymbol{\Lambda}_g\boldsymbol{p}_0\\ \boldsymbol{\Lambda}_d\boldsymbol{p}_0\\ \mathbf{0}\\ \mathbf{0}\end{bmatrix} \tag{47}$$

as well as $\tilde{\theta}_{2,u_0}=\tilde{\theta}_{3,u_0}=\theta_{3,u_0}=0$. For a given attack pair $(\boldsymbol{a}_p, e)$ and the corresponding $\boldsymbol{\theta}_2$, the expansion of (28b) is

$$\begin{bmatrix}\tilde{\boldsymbol{\theta}}_2 & \tilde{\boldsymbol{\theta}}_3 & \boldsymbol{\theta}_3 & \boldsymbol{s}_2+\boldsymbol{F}_3\boldsymbol{x}_N\\ \tilde{\boldsymbol{B}} & \mathbf{0} & \mathbf{0} & \boldsymbol{p}_0+\alpha|\boldsymbol{p}_0|\\ -\tilde{\boldsymbol{B}} & \mathbf{0} & \mathbf{0} & -\boldsymbol{p}_0+\alpha|\boldsymbol{p}_0|\\ \boldsymbol{I}_{|V|} & \mathbf{0} & \mathbf{0} & \boldsymbol{\theta}_2+M_\theta(1-\boldsymbol{x}_N)\\ -\boldsymbol{I}_{|V|} & \mathbf{0} & \mathbf{0} & -\boldsymbol{\theta}_2+M_\theta(1-\boldsymbol{x}_N)\\ 0 & 0 & -\Gamma_e\boldsymbol{d}_e^T & -\gamma_e f_{\max,e}\\ \mathbf{0} & \tilde{\boldsymbol{D}}^T\boldsymbol{\Gamma} & \mathbf{0} & \boldsymbol{f}_{\max}\\ \mathbf{0} & -\tilde{\boldsymbol{D}}^T\boldsymbol{\Gamma} & \mathbf{0} & \boldsymbol{f}_{\max}\\ \mathbf{0} & \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}} & \mathbf{0} & \boldsymbol{p}_{g,max}\\ \mathbf{0} & -\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}} & \mathbf{0} & -\boldsymbol{p}_{g,min}\\ \tilde{\boldsymbol{D}}^T\boldsymbol{\Gamma} & \mathbf{0} & \mathbf{0} & \boldsymbol{f}_{\max}\\ -\tilde{\boldsymbol{D}}^T\boldsymbol{\Gamma} & \mathbf{0} & \mathbf{0} & \boldsymbol{f}_{\max}\end{bmatrix} \tag{48}$$

Specifically, the first two rows of (48) correspond to (20e), the next two rows correspond to (38), the 5-th row indicates the outage at the target line, the 6-th and 7-th rows correspond to (21b), the 8-th and 9-th rows correspond to (21a), and the last two rows correspond to (20a).

APPENDIX E
DETAILS OF THE ATTACKER'S PROBLEM UNDER AC POWER FLOW MODEL

For completeness, we summarize the necessary notations for presenting AC power flow model in Table VII. Specifically, we denote $\boldsymbol{C}_f$ as the *From* end incidence matrix, in which $C_{f,e,i}=1$ if and only if we have $e=(i,k)\in E$. The *To* end incidence matrix $\boldsymbol{C}_t$ is defined similarly, where $C_{t,e,k}=1$ if and only if we have $e=(i,k)\in E$.

Table VII
NOTATIONS FOR AC POWER FLOW

Notation	Description
$\boldsymbol{p}/\boldsymbol{q}\in\mathbb{C}^{\lvert V\rvert}$	Active/reactive power injection
$\vec{v}_u=v_u e^{j\cdot\theta_u}$	node voltage
$\tilde{\boldsymbol{Y}}_{bus}=\tilde{\boldsymbol{G}}_{bus}+j\tilde{\boldsymbol{B}}_{bus}$	Bus admittance matrix
$\tilde{\boldsymbol{Y}}_f/\tilde{\boldsymbol{Y}}_t\in\mathbb{C}^{\lvert E\rvert\times\lvert V\rvert}$	*From/to* end admittance matrix
$\boldsymbol{C}_f/\boldsymbol{C}_t\in\{0,1\}^{\lvert E\rvert\times\lvert V\rvert}$	*From/to* end incidence matrix
$\boldsymbol{p}_f/\boldsymbol{p}_t\in\mathbb{C}^{\lvert E\rvert}$	*From/to* end active power flow
$\boldsymbol{q}_f/\boldsymbol{q}_t\in\mathbb{C}^{\lvert E\rvert}$	*From/to* end reactive power flow
$\lvert\boldsymbol{I}_f\rvert^2/\lvert\boldsymbol{I}_t\rvert^2\in\mathbb{C}^{\lvert E\rvert}$	Square of *from/to* end current magnitude
$\boldsymbol{I}_{max}\in\mathbb{R}^{\lvert E\rvert}$	Limit on line current magnitude
$\hat{\boldsymbol{I}}_{max}\in\mathbb{R}^{\lvert E\rvert}$	Threshold for line tripping
$\tilde{\boldsymbol{Y}}_c=\tilde{\boldsymbol{G}}_c+j\tilde{\boldsymbol{B}}_c\in\mathbb{C}^{\lvert E\rvert}$	line charging
$\tilde{\boldsymbol{Z}}=\tilde{\boldsymbol{Z}}_R+j\tilde{\boldsymbol{Z}}_I\in\mathbb{C}^{\lvert E\rvert}$	line impedance
$\tilde{\boldsymbol{Y}}_L=\tilde{\boldsymbol{G}}_L+j\tilde{\boldsymbol{B}}_L\in\mathbb{C}^{\lvert E\rvert}$	line admittance
$\boldsymbol{V}_{max}/\boldsymbol{V}_{min}\in\mathbb{R}^{\lvert V\rvert}$	Limit on node voltage magnitude
$\boldsymbol{\theta}_{max}/\boldsymbol{\theta}_{min}\in\mathbb{R}^{\lvert E\rvert}$	Limit on phase angle difference for lines
$\hat{\boldsymbol{p}}_3/\hat{\boldsymbol{q}}_3\in\mathbb{R}^{\lvert V\rvert}$	approximated power injections at t_3
$\hat{\boldsymbol{p}}_{f,3}/\hat{\boldsymbol{q}}_{f,3}\in\mathbb{R}^{\lvert E\rvert}$	approximated line power flow at t_3

To begin with, we demonstrate the basics on QC relaxation for AC power flow equations. Recall from Table VII that the complex voltage on node i is $\vec{v_i}:=v_i e^{j\cdot\theta_i}$. Then, we introduce auxiliary variables c_{ii}, c_{ik} and s_{ik} in the hope that

$$c_{ii}=v_i^2, \tag{49a}$$
$$c_{ik}=v_i v_k\cos\theta_{ik} \tag{49b}$$
$$s_{ik}=v_i v_k\sin\theta_{ik}, \tag{49c}$$

where $\theta_{ik}=\theta_i-\theta_k$. As proposed in [40], we first introduce the notation $\langle x\rangle^{\breve{}}$, which indicates an auxiliary variable as well as the associated constraints with x as input. Concretely, $\langle x^2\rangle^T$ indicates the auxiliary variable $\breve{x}$ together with the following constraints:

$$\langle x^2\rangle^T\equiv\begin{cases}\breve{x}\geqslant x^2\\ \breve{x}\leqslant(x_u+x_l)\,x-x_u x_l\end{cases}, \tag{50}$$

where $x\in[x_l,x_u]$ is pre-assigned bound. Similarly, we have

$$\langle xy\rangle^M:=\begin{cases}\breve{xy}\geqslant x_l y+y_l x-x_l y_l\\ \breve{xy}\geqslant x_u y+y_u x-x_u y_u\\ \breve{xy}\leqslant x_l y+y_u x-x_l y_u\\ \breve{xy}\leqslant x_u y+y_l x-x_u y_l\end{cases} \tag{51a}$$

$$\langle\sin x\rangle^S:=\begin{cases}\breve{sx}\leqslant\cos\left(\frac{x_u}{2}\right)\left(x-\frac{x_u}{2}\right)+\sin\left(\frac{x_u}{2}\right)\\ \breve{sx}\geqslant\cos\left(\frac{x_u}{2}\right)\left(x+\frac{x_u}{2}\right)-\sin\left(\frac{x_u}{2}\right)\end{cases} \tag{51b}$$

$$\langle\cos x\rangle^C:=\begin{cases}cx\leqslant 1-\frac{1-\cos(x_u)}{(x_u)^2}x^2\\ \breve{cx}\geqslant\cos(x_u)\end{cases} \tag{51c}$$

Equipped with (50) and (51), the QC relaxation-based constraints on c_{ii} for each $i \in V$ can be written as $c_{ii} \in \left\langle v_i^2 \right\rangle^T$, while the constraints on c_{ik} and s_{ik} for each $e = (i,k) \in E$ are

$$c_{ik} = c_{ki}, \tag{52a}$$
$$s_{ik} = -s_{ki}, \tag{52b}$$
$$c_{ik}^2 + s_{ik}^2 \leq c_{ii} c_{kk}, \tag{52c}$$
$$c_{ik} \in \left\langle \langle v_i v_k \rangle^M \cdot \langle \cos\theta_{ik} \rangle^C \right\rangle^M, \tag{52d}$$
$$s_{ik} \in \left\langle \langle v_i v_k \rangle^M \cdot \langle \sin\theta_{ik} \rangle^S \right\rangle^M. \tag{52e}$$

For simplicity, we will omit the auxiliary variables and the associated constraints for modeling (52d) and (52e). We assume that (52d) and (52e) are imposed when QC relaxation is adopted. For (36b), the decision variables we focus are $\tilde{c}_{2,ii}, \forall i \in V, \tilde{c}_{2,ik}, \tilde{s}_{2,ik}, \forall e = (i,k) \in E, e = (k,i) \in E$, $\tilde{\boldsymbol{\theta}}_2, \tilde{\boldsymbol{v}}_2$ and $|\tilde{\boldsymbol{I}}_{2,f}|^2, |\tilde{\boldsymbol{I}}_{2,t}|^2$. Then, the constraints (36b) can be written as

$$\boldsymbol{\Lambda}_g(\tilde{\boldsymbol{p}}_2 - \boldsymbol{p}_0) = 0, \boldsymbol{\Lambda}_g(\tilde{\boldsymbol{q}}_2 - \boldsymbol{q}_2) = 0 \tag{53a}$$
$$\boldsymbol{\Lambda}_g(\tilde{\boldsymbol{v}}_2 - \boldsymbol{v}_2) = \boldsymbol{0}, \tag{53b}$$
$$\tilde{c}_{2,ii} = v_{2,i}^2, \forall i \in V_g, \tag{53c}$$
$$-\boldsymbol{\Lambda}_d|\tilde{\boldsymbol{p}}_0| \leq \alpha\boldsymbol{\Lambda}_d(\tilde{\boldsymbol{p}}_{2,i} - \tilde{\boldsymbol{p}}_0) \leq \alpha\boldsymbol{\Lambda}_d|\tilde{\boldsymbol{p}}_0|, \tag{53d}$$
$$-\boldsymbol{\Lambda}_d|\tilde{\boldsymbol{q}}_0| \leq \alpha\boldsymbol{\Lambda}_d(\tilde{\boldsymbol{q}}_{2,i} - \tilde{\boldsymbol{q}}_0) \leq \alpha\boldsymbol{\Lambda}_d|\tilde{\boldsymbol{q}}_0|, \tag{53e}$$
$$(1-\eta)\boldsymbol{V}_{min} \leq \tilde{\boldsymbol{v}}_2 \leq (1+\eta)\boldsymbol{V}_{max} \tag{53f}$$
$$(1-\eta)\theta_{min,e} \leq \tilde{\theta}_{2,e} \leq (1+\eta)\theta_{max,e}, \forall e \in E \tag{53g}$$
$$|\tilde{\boldsymbol{I}}_{2,f}| \leq \boldsymbol{I}_{max}, |\tilde{\boldsymbol{I}}_{2,t}| \leq \boldsymbol{I}_{max} \tag{53h}$$
$$\tilde{p}_{2,i} = \sum_{k=1,\ldots,n} \tilde{G}_{ik}\tilde{c}_{2,ik} - \tilde{B}_{ik}\tilde{s}_{2,ik}, \tag{53i}$$
$$\tilde{q}_{2,i} = \sum_{k=1,\ldots,n} -\tilde{B}_{ik}\tilde{c}_{2,ik} - \tilde{G}_{ik}\tilde{s}_{2,ik}, \tag{53j}$$
$$\tilde{p}_{2,f,e} = \tilde{G}_{f,e,i}\tilde{c}_{2,ii} + \tilde{G}_{f,e,k}\tilde{c}_{2,ik} - \tilde{B}_{f,e,k}\tilde{s}_{2,ik}, \tag{53k}$$
$$\tilde{q}_{2,f,e} = -\tilde{B}_{f,e,i}\tilde{c}_{2,ii} - \tilde{B}_{f,e,k}\tilde{c}_{2,ik} - \tilde{G}_{f,e,k}\tilde{s}_{2,ik}, \tag{53l}$$
$$\tilde{p}_{2,t,e} = \tilde{G}^*_{t,e,k}\tilde{c}_{2,kk} + \tilde{G}_{t,e,i}\tilde{c}_{2,ik} + \tilde{B}_{t,e,i}\tilde{s}_{2,ik}, \tag{53m}$$
$$\tilde{q}_{2,t,e} = -\tilde{B}^*_{t,e,k}\tilde{c}_{2,kk} - \tilde{B}_{t,e,i}\tilde{c}_{2,ik} + \tilde{G}_{t,e,i}\tilde{s}_{2,ik}, \tag{53n}$$
$$\tilde{p}_{2,i} = \boldsymbol{c}_{f,i}^T\tilde{\boldsymbol{p}}_{f,2} + \boldsymbol{c}_{t,i}^T\tilde{\boldsymbol{p}}_{t,2} + \mathcal{R}(Y_{sh,i}\tilde{c}_{2,ii}) \tag{53o}$$
$$\tilde{q}_{2,i} = \boldsymbol{c}_{f,i}^T\tilde{\boldsymbol{q}}_{f,2} + \boldsymbol{c}_{t,i}^T\tilde{\boldsymbol{q}}_{t,2} - \mathcal{I}(Y_{sh,i}\tilde{c}_{2,ii}) \tag{53p}$$
$$\tilde{c}_{2,ii} = v_{2,i}^2, \tilde{v}_{2,i} = v_{2,i}, \tilde{\theta}_{2,i} = \theta_{2,i}, \forall i \text{ with } x_{N,i} = 1, \tag{53q}$$
$$\tilde{c}_{2,ik} = v_{2,i}v_{2,k}\cos\theta_{ik}, \forall e = (i,k) \text{ with } x_{L,e} = 1, \tag{53r}$$
$$\tilde{p}_{2,e} = p_{2,e}, \tilde{q}_{2,e} = q_{2,e}, \forall e = (i,k) \text{ with } x_{L,e} = 1, \tag{53s}$$
$$\tilde{I}_{2,f,e} = I_{2,f,e}, \tilde{I}_{2,t,e} = I_{2,t,e}, \forall e = (i,k) \text{ with } x_{L,e} = 1, \tag{53t}$$

where $\boldsymbol{p}_0$ and $\boldsymbol{q}_0$ indicates the ground-truth power injections at t_0, (53i)-(53j) are imposed for each node $i \in V$, (53k)-(53n) are imposed for all $e = (i,k) \in E$, $\boldsymbol{c}_{f,i}/\boldsymbol{c}_{t,i}$ is the i-th column of $\boldsymbol{C}_f/\boldsymbol{C}_t$, $\boldsymbol{Y}_{sh}$ denotes the diagonal matrix of node shunt, $\mathcal{R}(x)/\mathcal{I}(x)$ denotes the real/imaginary part of x, (53q)-(53t) indicates the protection effect of PMUs, and $\eta \in [0,1)$ is a manually assigned factor for $\tilde{v}_2$ and $\tilde{\theta}_2$ not to raise alarms in control center. Besides (53), we impose the following constraints according to [42, Chapter 5] for each $e = (i,k) \in E$ into (36b) :

$$|\tilde{\boldsymbol{I}}_{2,f,e}|^2 = \frac{1}{|Z_e|^2}(\tilde{c}_{2,ii} + \tilde{c}_{2,kk} - 2\tilde{c}_{2,ik}) + 2\tilde{G}_{c,e}\tilde{p}_{2,f,e} - 2\tilde{B}_{c,e}\tilde{q}_{2,f,e} - |\boldsymbol{Y}_{c,e}|^2\tilde{c}_{2,ii}, \tag{54a}$$
$$\tilde{p}_{2,f,e} + \tilde{q}_{2,f,e} = \tilde{Z}_{R,e}\big(|\tilde{\boldsymbol{I}}_{2,f,e}|^2 - 2(\tilde{G}_{c,e}\tilde{p}_{2,f,e} - \tilde{B}_{c,e}\tilde{q}_{2,f,e}) + |\boldsymbol{Y}_{c,e}|^2\tilde{c}_{2,ii}\big) + \tilde{G}_{c,e}(\tilde{c}_{2,ii} + \tilde{c}_{2,kk}), \tag{54b}$$
$$\tilde{p}_{2,f,e} + \tilde{q}_{2,f,e} = \tilde{Z}_{I,e}\big(|\tilde{\boldsymbol{I}}_{2,f,e}|^2 - 2(\tilde{G}_{c,e}\tilde{p}_{2,f,e} - \tilde{B}_{c,e}\tilde{q}_{2,f,e}) + |\boldsymbol{Y}_{c,e}|^2\tilde{c}_{2,ii}\big) - \tilde{B}_{c,e}(\tilde{c}_{2,ii} + \tilde{c}_{2,kk}), \tag{54c}$$
$$\Big(1 + 2\tilde{Z}_{R,e}\tilde{G}_{c,e} - 2\tilde{Z}_{I,e}\tilde{B}_{c,e}\Big)\tilde{c}_{2,ii} - \tilde{c}_{2,kk} = 2(\tilde{Z}_{R,e}\tilde{p}_{2,f,e} + \tilde{Z}_{I,e}\tilde{q}_{2,f,e}) - |\tilde{Z}_e|^2\big(|\tilde{\boldsymbol{I}}_{2,f,e}|^2 - 2(\tilde{G}_{c,e}\tilde{p}_{2,f,e} - \tilde{B}_{c,e}\tilde{q}_{2,f,e}) + \Big|\tilde{Y}_{c,e}\Big|^2\tilde{c}_{2,ii}\big) \tag{54d}$$

All equations in (54) should hold simultaneously.

Similarly, the decision variables we will focus on in (36c) are $\tilde{c}_{3,ii}, \forall i \in V, \tilde{3}_{2,ik}, \tilde{s}_{3,ik}, \forall e = (i,k) \in E, e = (k,i) \in E$, $\tilde{\boldsymbol{\theta}}_3, \tilde{\boldsymbol{v}}_3$ and $|\tilde{\boldsymbol{I}}_{3,f}|^2, |\tilde{\boldsymbol{I}}_{3,t}|^2$. Then, the constraints (36c) are similar to (53) and (54), with (53a)-(53h) changed into

$$\boldsymbol{p}_{g,min} \leq \boldsymbol{\Lambda}_g\tilde{\boldsymbol{p}}_3 \leq \boldsymbol{p}_{g,max}, \boldsymbol{q}_{g,min} \leq \boldsymbol{\Lambda}_g\tilde{\boldsymbol{q}}_3 \leq \boldsymbol{q}_{g,max}, \tag{55a}$$
$$\boldsymbol{\Lambda}_d(\tilde{\boldsymbol{p}}_{3,i} - \tilde{\boldsymbol{p}}_{2,i}) = 0, \quad \boldsymbol{\Lambda}_d(\tilde{\boldsymbol{q}}_{3,i} - \tilde{\boldsymbol{q}}_{2,i}) = 0, \tag{55b}$$
$$\boldsymbol{\Lambda}_g(\tilde{\boldsymbol{p}}_{3,i} - \tilde{\boldsymbol{p}}_{2,i}) = 0 \tag{55c}$$
$$\boldsymbol{V}_{min} \leq \tilde{\boldsymbol{v}}_3 \leq \boldsymbol{V}_{max}, \theta_{min,e} \leq \tilde{\theta}_{3,e} \leq \theta_{max,e}, \forall e \in E, \tag{55d}$$
$$|\tilde{\boldsymbol{I}}_{3,f}| \leq \boldsymbol{I}_{max}, |\tilde{\boldsymbol{I}}_{3,t}| \leq \boldsymbol{I}_{max}. \tag{55e}$$

Following [33], the decision variables in (36d) are $\hat{v}_{3,i}^2, \hat{\theta}_{3,i}, \hat{p}_{3,i}, \hat{q}_{3,i}, \forall i \in V$, $\hat{\boldsymbol{p}}_{f,3} \in \mathbb{R}^{|E|}, \hat{\boldsymbol{q}}_{f,3} \in \mathbb{R}^{|E|}$ and $|\hat{\boldsymbol{I}}_3|^2 \in \mathbb{R}^{|E|}$. Next, we define $p_{f,3,e}^L$ and $q_{f,3,e}^L$ for $e = (i,k) \in E$ with $a_{p,e} = 0$ as follows:

$$p_{f,3,e}^L = \tilde{G}_{L,e}\bigg(\hat{\theta}_{ik,0}\hat{\theta}_{3,ik} - \frac{\hat{\theta}_{ik,0}^2}{2} + \frac{\hat{v}_{i,0} - \hat{v}_{k,0}}{\hat{v}_{i,0} + \hat{v}_{k,0}}(\hat{v}_{3,i}^2 - \hat{v}_{3,k}^2) - \frac{(\hat{v}_{i,0} - \hat{v}_{k,0})^2}{2}\bigg) + \mathcal{R}(\tilde{Y}_{c,e})\hat{v}_{3,i}^2 \tag{56a}$$
$$q_{f,3,e}^L = -\tilde{B}_{L,e}\bigg(\hat{\theta}_{ik,0}\hat{\theta}_{3,ik} - \frac{\hat{\theta}_{ik,0}^2}{2} + \frac{\hat{v}_{i,0} - \hat{v}_{k,0}}{\hat{v}_{i,0} + \hat{v}_{k,0}}(\hat{v}_{3,i}^2 - \hat{v}_{3,k}^2) - \frac{(\hat{v}_{i,0} - \hat{v}_{k,0})^2}{2}\bigg) - \mathcal{I}(\tilde{Y}_{c,e})\hat{v}_{3,i}^2, \tag{56b}$$

where $\hat{v}_{ik,0}$ and $\hat{\theta}_{ik,0}$ are obtained from any base case system operating condition. In our work, we set it as $\hat{v}_{ik,0} = v_{2,ik}$ and $\hat{\theta}_{ik,0} = \theta_{2,ik}$ for each given $(\boldsymbol{a}_p, e_t)$. Then, we have three types of constraints in (36d). Specifically, by appropriately setting $\eta_{3,p,i}$ and $\eta_{3,q,i}$ (see proof of Theorem IV.1 for details) to tolerate the approximation error, for each $i \in V$, we have

$$-\eta_{3,p,i} \leq \boldsymbol{D}_i\hat{\boldsymbol{p}}_{3,f} + \hat{v}_{3,i}^2\sum_{k=1}^{|V|}\tilde{G}_{ik} - p_{0,i} \leq \eta_{3,p,i}. \tag{57}$$

For each $i \in V_d$, we have

$$-\eta_{3,q,i} \leq \boldsymbol{D}_i\hat{\boldsymbol{q}}_{3,f} - \hat{v}_{3,i}^2\sum_{k=1}^{|V|}\tilde{B}_{ik} - \tilde{q}_{3,i} \leq \eta_{3,q,i},. \tag{58}$$

For each $e=(i,k)\in E$ with $a_{p,e}=0$, we have

$$p_{f,3,e}=\tilde{G}_{L,e}\frac{\hat{v}_{3,i}^2-\hat{v}_{3,k}^2}{2}-\tilde{B}_{L,e}\hat{\theta}_{ik}+p_{f,3,e}^L, \tag{59a}$$

$$q_{f,3,e}=-\tilde{B}_{L,e}\frac{\hat{v}_{3,i}^2-\hat{v}_{3,k}^2}{2}-\tilde{G}_{L,e}\hat{\theta}_{ik}+q_{f,3,e}^L, \tag{59b}$$

$$\begin{aligned}\left(1+2\tilde{Z}_{R,e}\tilde{G}_{c,e}-2\tilde{Z}_{I,e}\tilde{B}_{c,e}\right)\hat{v}_{3,i}^2-\hat{v}_{3,k}^2=2(\tilde{Z}_{R,e}\hat{p}_{3,f,e}\\ +\tilde{Z}_{I,e}\hat{q}_{3,f,e})-|\tilde{Z}_e|^2\big(|\hat{\boldsymbol{I}}_{3,f,e}|^2-2(\tilde{G}_{c,e}\hat{p}_{3,f,e}\\ -\tilde{B}_{c,e}\hat{q}_{3,f,e})+\left|\tilde{Y}_{c,e}\right|^2\hat{v}_{3,i}^2\big)\end{aligned} \tag{59c}$$

APPENDIX F
DETAILS OF PMU LOCATIONS OBTAINED IN PPOP

Here, we present the location of PMUs obtained in the proposed PPOP. First, in Table VIII, we give the PMU locations according to the best proposed solution Ω_{PPOP} to PPOP, which is consistent with Table II.

Table VIII
PMU LOCATIONS OF PPOP UNDER DC MODEL

	Location of PMUs
IEEE 30-bus system	15, 23
IEEE 57-bus system	12,13,25
IEEE 118-bus system	17,34,37,42,49,72,85,100,118
IEEE 300-bus system	8,20,22,34,38,43,44,48,49,54,64,68, 74,77,79,89,90,94,99,109,119,132, 138,152,185,190,203,216,221,270,271

Then, in Table IX, we present the PMU locations of the solution that can pass the test of Alg. 4 under AC power flow model, obtained by Alg. 5.

Table IX
PMU LOCATIONS OF PPOP UNDER AC MODEL

	Location of PMUs
IEEE 30-bus system	5,15,23
IEEE 57-bus system	12,13,25
IEEE 118-bus system	17,34,37,42,49,62,72,85,100,118
IEEE 300-bus system	8,20,22,34,38,43,44,48,49,54,64,68, 74,77,79,81,89,90,94,99,109,119,132, 138,152,175,185,190,197,203,216, 221,270,271

APPENDIX G
MORE DISCUSSION OF RELATED WORKS

Different defense techniques against CCPA/FDI: Following [6], we classify defense techniques against CCPAs into the following categories:

1) **Prevention:** Due to the requirements of network information and measurements, prevention methods defend against CCPAs by reducing or postponing the information leakage. Moving target defense (MTD) approach [10] is a typical technique in this category. Specifically, MTD methods will strategically impose random change to network components (such as line admittance) to mislead the attacker. The CCPAs with falsified network parameters have a higher chance to be detected. Another typical method in this category is dynamic watermarking [43], which shares a similar spirit of MTD.
2) **Detection:** The methods in this category manage to detect the existence of attacks under some assumption on information exposure and attack capability. Traditional BDD is one of the approaches in this category. There are some advanced detection techniques, such as low rank-based detection [44]. Securing measurements or deploying PMUs can also be used for detection. Specifically, an attack that tries to alter the measurements secured by PMUs will be detected by the control center. However, to achieve full detection, full observability by PMUs is required.
3) **Resilience:** It is critical to keep the system stable when there exist CCPAs that can bypass the detection. In other words, resilience approaches aim at limiting the impact of the attacks. Game-theoretic methods can be regarded as typical ones, such as the budget-constrained formulations in [18], [22]–[24], [27]. Our solution lies in this category.

APPENDIX H
ADDITIONAL PROOFS

Theorem III.1. We will reduce the dominating set problem to PPOP. Given a graph $\mathcal{N}=(V,E)$, the dominating set problem aims to find a minimum set of vertices $V_1\in V$ such that $\forall u\in V\setminus V_1$, u has at least one neighbor in V_1. The dominating set problem is known to be NP-hard. Notice that given the grid $\mathcal{N}=(V,E)$ the parameters for the proposed problem (24)-(23) are $\boldsymbol{p}_0,\boldsymbol{\Gamma},\xi_p,\xi_c,\boldsymbol{\alpha}$ and $\{\gamma_e\}_{e\in E}$. We will prove for any given connected grid and the associated dominating set problem, there exists a parameter setting for the proposed problem such that V_1 is a minimal dominating set if and only if V_1 is an optimal solution to (24), i.e., $\forall u\in V, x_{N,u}=1$.

Given any $\boldsymbol{p}_0$, suppose that $\boldsymbol{\theta}_0$ is the associated phase angle without attack, i.e., $\boldsymbol{p}_0=\tilde{\boldsymbol{B}}\boldsymbol{\theta}_0$, and $\hat{\boldsymbol{\theta}}_0$ is the the solution to (5), i.e., $\hat{\boldsymbol{\theta}}_0=\psi_s(\boldsymbol{p}_0,\tilde{\boldsymbol{D}})$, which gives $\hat{\boldsymbol{f}}_0:=\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\hat{\boldsymbol{\theta}}_0$.

Then, we set $\boldsymbol{p}_0=\boldsymbol{0}$, $\xi_p=0$, $\xi_c=\infty$, $\alpha=\infty$ and $\boldsymbol{\Gamma}$ as identity matrix, which results in $\boldsymbol{\theta}_0=\hat{\boldsymbol{\theta}}_0=\boldsymbol{0}$ and $\hat{\boldsymbol{f}}_0=\boldsymbol{0}$. In addition, we set $\gamma_e=0,\forall e\in E$, which transform (23e) to

$$|\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3|=0\leftrightarrow\pi_e=0. \tag{60}$$

Next, we show by contradiction that $|\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3|=0$ holds for all $e\in E$ only if $\tilde{\boldsymbol{\theta}}_2=\boldsymbol{0}=\boldsymbol{\theta}_0$. Suppose $\tilde{\boldsymbol{\theta}}_2\neq\boldsymbol{0}$, we must have $\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2\neq\boldsymbol{0}$, which leads to $\boldsymbol{0}\neq\tilde{\boldsymbol{\theta}}_3=\psi_s(\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2,\tilde{\boldsymbol{D}})$ and thus $\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3\neq\boldsymbol{0}$ due to the constraint (23c). The non-zero $\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3$ implies that $\exists e\in E$ such that $\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3\neq 0$. That is to say, the constraint (24b) holds only when $\tilde{\boldsymbol{\theta}}_2=\boldsymbol{\theta}_0=\boldsymbol{0}$, which indicates that the defender has to place PMUs to guarantee that the only feasible solution to (23) is $\boldsymbol{a}_c=\boldsymbol{0}$. In another word, $\boldsymbol{\beta}$ needs to satisfy $\forall u\in V, x_{N,u}=1$, which completes the proof. □

Theorem III.2. First, we introduce some definitions: $\mathcal{B}:=\{\boldsymbol{\beta}|\psi_a(\boldsymbol{\beta})=0\}$ denotes the set of feasible solutions, $\mathcal{B}^c:=\{\boldsymbol{\beta}|\psi_a(\boldsymbol{\beta})\geq 1\}$ the infeasible solutions, $\mathcal{M}(\mathcal{B}^c):=\{\boldsymbol{\beta}|(\boldsymbol{\beta},\boldsymbol{\beta}'\in\mathcal{B}^c)\wedge(\boldsymbol{\beta}'\geq\boldsymbol{\beta})\rightarrow(\boldsymbol{\beta}'=\boldsymbol{\beta})\}$ the maximal infeasible solutions, and $\mathcal{P}:=\{\check{\boldsymbol{\beta}}\in[0,1]^{|V|}|\forall\boldsymbol{\beta}\in\mathcal{M}(\mathcal{B}^c):$

$\sum_{u:\beta_u=0} \check{\beta}_u \geq 1\}$ the polytope excluding all the maximal infeasible solutions.

Then, based on the results in [45], we have the following characterization:

Lemma H.1. *The following statements hold: (i)* $\mathcal{P} \cap \{0,1\}^{|V|} = \mathcal{B}$*; (ii)* $\forall \boldsymbol{\beta}' \in \mathcal{M}(\mathcal{B}^c)$, $\sum_{u:\beta'_u=0} \beta_u \geq 1$ *defines a facet of* $\mathcal{P}$.

Proof. To prove statement (i), we first prove that $\mathcal{B} \subseteq (\mathcal{P} \cap \{0,1\}^{|V|})$ by contradiction. Suppose $\exists \boldsymbol{\beta}_1 \in \mathcal{B}$ but $\boldsymbol{\beta}_1 \notin \mathcal{P}$. Then by definition of $\mathcal{P}$, there must exist $\boldsymbol{\beta}'_1 \in \mathcal{B}^c$ such that $\sum_{u:\beta'_{1,u}=0} \beta_{1,u} = 0$, which implies $\Omega(\boldsymbol{\beta}_1) \subseteq \Omega(\boldsymbol{\beta}'_1)$. By Lemma III.1, we must have $\boldsymbol{\beta}_1 \in \mathcal{B}^c$, which contradicts with the assumption that $\boldsymbol{\beta}_1 \in \mathcal{B}$. Thus, $\mathcal{B} \subseteq (\mathcal{P} \cap \{0,1\}^{|V|})$. Then, we prove $(\mathcal{P} \cap \{0,1\}^{|V|}) \subseteq \mathcal{B}$ by contradiction. Suppose there exists $\check{\boldsymbol{\beta}} \in (\mathcal{P} \cap \{0,1\}^{|V|})$ but $\check{\boldsymbol{\beta}} \notin \mathcal{B}$, which implies that $\check{\boldsymbol{\beta}} \in \mathcal{B}^c$. That is to say, $\exists \check{\boldsymbol{\beta}}' \geq \check{\boldsymbol{\beta}}$ such that $\check{\boldsymbol{\beta}}' \in \mathcal{M}(\mathcal{B}^c)$. Then by definition of $\mathcal{P}$, we have $\sum_{u:\check{\beta}'_u=0} \check{\beta}_u \geq 1$. However, since $\check{\boldsymbol{\beta}}' \geq \check{\boldsymbol{\beta}}$, $\forall u : \check{\beta}_u = 0$, we must have $\check{\beta}_u = 0$ and leads to $\sum_{u:\check{\beta}'_u=0} \check{\beta}_u = 0$, which introduces contradiction. In summary, $\mathcal{P} \cap \{0,1\}^{|V|} = \mathcal{B}$.

We then prove statement (ii) by contradiction, i.e., $\exists \check{\boldsymbol{\beta}}' \in \mathcal{M}(\mathcal{B}^c)$ such that when we remove the inequality $\sum_{u:\check{\beta}'_u=0} \beta_u \geq 1$ from $\mathcal{P}$, we still have $\mathcal{P}$. By definition of $\mathcal{M}(\mathcal{B}^c)$, we must have $\check{\boldsymbol{\beta}}' \in \mathcal{B}^c$, which implies $\sum_{u:\check{\beta}'_u=0} \check{\beta}'_u = 0$, i.e., $\check{\boldsymbol{\beta}}' \notin \mathcal{P}$. That is to say, there exists some inequality to cut $\check{\boldsymbol{\beta}}'$ out from $\mathcal{P}$, i.e., $\exists \check{\boldsymbol{\beta}}'' \in \mathcal{M}(\mathcal{B}^c)$ and $\check{\boldsymbol{\beta}}'' \neq \check{\boldsymbol{\beta}}'$ such that $\sum_{u:\check{\beta}''_u=0} \check{\beta}'_u = 0$. Notice that $\forall u : (\check{\beta}''_u = 0) \rightarrow (\check{\beta}'_u = 0)$, which implies $\Omega(\check{\boldsymbol{\beta}}') \subseteq \Omega(\check{\boldsymbol{\beta}}'')$. By definition of $\mathcal{M}(\mathcal{B}^c)$, we must have $\check{\beta}''_u = \check{\beta}'_u$, which contradicts with $\check{\beta}''_u \neq \check{\beta}'_u$ and completes the proof. □

We now prove Theorem III.2 based on Lemma H.1. First notice that each $\hat{\boldsymbol{\beta}} \in \mathcal{B}^c$ will be enumerated at most once in Alg. 1 due to the "no-good" constraints, and hence the algorithm will converge in finite time. Then, consider an arbitrary $\hat{\boldsymbol{\beta}}'$ obtained through (26). The generated "no-good" constraint $\sum_{i:\hat{\beta}'_i=0} \beta_i \geq 1$ must be satisfied by all the feasible solutions in $\mathcal{B}$, as any PMU placement violating this constraint must be infeasible according to Lemma III.1. Finally, for any $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \in \mathcal{B}$ with $\|\boldsymbol{\beta}_1\|_0 < \|\boldsymbol{\beta}_2\|_0$, $\boldsymbol{\beta}_1$ will be found by Alg. 1 before $\boldsymbol{\beta}_2$, since each guess of PMU placement is obtained by minimizing $\|\boldsymbol{\beta}\|_0$ in (24), which completes the proof. □

Theorem III.3. As Alg. 1 always returns a feasible solution that defends against all attack pairs, we only need to prove that the solution $\boldsymbol{\beta}_1$ returned by AODC requires the minimum number of PMUs. We will prove this by contradiction. Suppose that there exists $\boldsymbol{\beta}_2$ such that $\|\boldsymbol{\beta}_2\|_0 < \|\boldsymbol{\beta}_1\|_0$ and $\psi_a(\boldsymbol{\beta}_2) = 0$. Then $\boldsymbol{\beta}_2$ must be feasible to the instance of (31) constructed based on the attack pairs $\{(\boldsymbol{a}_p^{(k)}, e^{(k)})\}_{k=1}^K$ and the maximal infeasible solutions $\{\hat{\boldsymbol{\beta}}'^{(k)}\}_{k=1}^K$ found by AODC as it defends against all attacks. This contradicts with the fact that $\boldsymbol{\beta}_1$ is optimal to (31). □

Lemma III.2. We first observe that $\boldsymbol{x}_N$ and $\boldsymbol{x}_L$ are unique under the constraints (16)-(17). Thus, we will use $\boldsymbol{x}_N(\boldsymbol{\beta})$ and $\boldsymbol{x}_L(\boldsymbol{\beta})$ to denote the values of $\boldsymbol{x}_N$ and $\boldsymbol{x}_L$ satisfying (16)-(17) for a given $\boldsymbol{\beta} \in \{0,1\}^{|V|}$.

For a given attack pair $(\boldsymbol{a}_p, e)$, $(\check{\boldsymbol{q}}_1, \check{\boldsymbol{q}}_2, \check{\boldsymbol{\beta}})$ can be feasible to (34) in two different cases. The first case is that

$$\sum_{a_{p,e}=1} x_{L,e}(\lceil \check{\boldsymbol{\beta}} \rceil) \geq 1, \tag{61}$$

which makes $(\boldsymbol{q}_1 = \boldsymbol{0}, \boldsymbol{q}_2 = \boldsymbol{0}, \lceil \check{\boldsymbol{\beta}} \rceil, \boldsymbol{x}_N(\lceil \check{\boldsymbol{\beta}} \rceil), \boldsymbol{x}_L(\lceil \check{\boldsymbol{\beta}} \rceil))$ feasible for (30) with $w_a = 1$.

The second case is that $x_{L,e}(\lceil \check{\boldsymbol{\beta}} \rceil) = 0$ for all e with $a_{p,e} = 1$, in which case we must have $(\check{\boldsymbol{q}}_1, \check{\boldsymbol{q}}_2, \lceil \check{\boldsymbol{\beta}} \rceil, \boldsymbol{x}_N(\lceil \check{\boldsymbol{\beta}} \rceil), \boldsymbol{x}_L(\lceil \check{\boldsymbol{\beta}} \rceil))$ feasible to (30) with $w_a = 0$. To prove this, we only need to show that

$$\left(\boldsymbol{F}_3 \boldsymbol{x}_N(\lceil \check{\boldsymbol{\beta}} \rceil)\right)^T \check{\boldsymbol{q}}_2 \leq \boldsymbol{F}_3 \check{\boldsymbol{q}}_2. \tag{62}$$

According to (48), $F_{3,i,u}$ is either 0 or $-M_\theta$, which together with the fact that $\boldsymbol{x}_{N,u}(\lceil \check{\boldsymbol{\beta}} \rceil) \geq 0$ and $\check{q}_{2,i} \geq 0$ implies that

$$\left(\boldsymbol{F}_3 \boldsymbol{x}_N(\lceil \check{\boldsymbol{\beta}} \rceil)\right)^T \check{\boldsymbol{q}}_2 = \sum_{u \in V} \boldsymbol{x}_{N,u}(\lceil \check{\boldsymbol{\beta}} \rceil) \left(\sum_{i=1}^{m_2} F_{3,i,u} \check{q}_{2,i} \right) \tag{63}$$

$$\leq \sum_{u \in V} \boldsymbol{1} \left(\sum_{i=1}^{m_2} F_{3,i,u} \check{q}_{2,i} \right) = \boldsymbol{F}_3 \check{\boldsymbol{q}}_2, \tag{64}$$

which completes the proof. □

Theorem III.4. Under the assumption of $\xi_p = \mathcal{O}(1)$, the number of possible attack pairs is $|E| \left(\sum_{i=1}^{\xi_p} \binom{|E|}{i} \right) \leq \xi_p |E|^{\xi_p+1} = \mathcal{O}\left(|E|^{\xi_p+1}\right)$. Therefore, the time complexity of solving (23) for a given $\boldsymbol{\beta}$ is polynomial in $|E|$ and $|V|$, since in the worst case (23) can be solved by checking the feasibility of (28) for all the $\mathcal{O}\left(|E|^{\xi_p+1}\right)$ attack pairs.

We first characterize the complexity of Alg. 3. Since each candidate placement Ω_i either has one more node or can defend against all attack pairs in $\mathcal{A}$ after one iteration of the while loop, Alg. 3 converges within $|V|$ iterations. Each iteration of Alg. 3 is dominated by solving (35) (Line 8) for at most K_c times. Since the numbers of variables and constraints of (35) are both $\mathcal{O}((|E| + |V|)|\mathcal{A}|)$ and $|\mathcal{A}| = \mathcal{O}\left(|E|^{\xi_p+1}\right)$, the complexity of solving (35) is polynomial [3] in $|V|$ and $|E|$. In summary, the complexity of Alg. 3 is polynomial in $|V|$, $|E|$, and K_c since it solves a polynomial-sized LP for at most $K_c|V|$ times. It is worth noting that the effect of K_A and K_L in Alg. 3's complexity is dominated by $|V|$ and $|E|$. To see this, we note that K_L only appears in Line 7 of Alg. 3, in which we must have $K_L \leq |E|$. Then, K_A only appears in Line 9 of Alg. 3, in which we must have $K_A \leq |V|$. Thus, we do not consider the effect of K_A and K_L in Alg. 3's computational complexity.

The complexity of Alg. 2 comes from: (i) solving (23) $\mathcal{O}(|E|^{\xi_p+1})$ times (Line 3 and Line 12); (ii) solving (35) for $|\mathcal{A}_0| = \mathcal{O}(|E|^{\xi_p+1})$ times (Line 5), each of which deals with an LP containing $\mathcal{O}((|E|+|V|)|\mathcal{A}_0|)$ variables and constraints and thus takes polynomial time; (iii) calling Alg. 3 at Line 8 for 1 time and at Line 14 for $\mathcal{O}(|E|^{\xi_p+1})$ times, whose complexity is polynomial in $|V|$, $|E|$, and K_c. In summary, Alg. 2 is a polynomial-time algorithm in terms of $|V|$, $|E|$, and K_c. □

[3] The exact order depends on the specific algorithm used to solve LP [46].

Theorem IV.1. According to [33], [42] and (59), we have

$$|\hat{I}_{3,f,e}|^2 = \frac{1}{|Z_e|^2}\big(2(\tilde{Z}_{R,e}\hat{p}_{3,f,e} + \tilde{Z}_{I,e}\hat{q}_{3,f,e}) + \hat{v}_k^2 - (1 + 2\tilde{Z}_{R,e}\tilde{G}_{c,e} - 2\tilde{Z}_{I,e}\tilde{B}_{c,e})\hat{v}_i^2\big) + 2(\tilde{G}_{c,e}\hat{p}_{3,f,e} - \tilde{B}_{c,e}\hat{q}_{3,f,e}) - |\tilde{Y}_{c,e}|^2\hat{v}_i^2 \tag{65}$$

for each $e = (i,k) \in E$ with $a_{p,e} = 0$. Based on (65) and the assumption on $\boldsymbol{\epsilon_\theta} = (\epsilon_{\theta,u})_{u\in V}$, $\boldsymbol{\epsilon_v} = (\epsilon_{v,u})_{u\in V}$, $\boldsymbol{\epsilon_p} = (\epsilon_{p,e})_{e\in E}$ and $\boldsymbol{\epsilon_q} = (\epsilon_{q,e})_{e\in E}$, we can easily derive an upperbound $\epsilon_{I,e} \geq ||\hat{I}_{3,e}| - |I_{3,e}||, \forall e \in E$. Specifically, we can set

$$\epsilon_{I,e} := \frac{1}{|Z_e|^2}\big(2(|\tilde{Z}_{R,e}|\epsilon_{p,e} + |\tilde{Z}_{I,e}|\epsilon_{q,e}) + \epsilon_{v,i}^2 + |1 + 2\tilde{Z}_{R,e}\tilde{G}_{c,e} + 2\tilde{Z}_{I,e}\tilde{B}_{c,e}|\epsilon_{v,i}^2\big) + 2(|\tilde{G}_{c,e}|\epsilon_{p,e} + |\tilde{B}_{c,e}|\epsilon_{q,e}) + |\tilde{Y}_{c,e}|^2\epsilon_{v,i}^2. \tag{66}$$

If there exists an successful attack pair $(\boldsymbol{a}_p, e)$ that cannot be found by Alg. 4 for a given PMU placement, we must have one of the following cases:

1) There exists $\tilde{\boldsymbol{v}}_2, \tilde{\boldsymbol{\theta}}_2$ such that $|I_{3,e}| > \gamma_e I_{max,e}$. In the meantime, at least one of (57) and (58) are violated.
2) Let $|\hat{I}^*_{3,f,e}|$ be the optimal solution of (36). There exists $\tilde{\boldsymbol{v}}_2^{(1)}, \tilde{\boldsymbol{\theta}}_2^{(1)}, \tilde{\boldsymbol{v}}_3^{(1)}, \tilde{\boldsymbol{\theta}}_3^{(1)}$ such that $|I_{3,e}^{(1)}| > \gamma_e I_{max,e}$. Let $|\hat{I}_{3,f,e}^{(1)}|$ be the corresponding approximated solution for $\tilde{\boldsymbol{v}}_2^{(1)}, \tilde{\boldsymbol{\theta}}_2^{(1)}, \tilde{\boldsymbol{v}}_3^{(1)}, \tilde{\boldsymbol{\theta}}_3^{(1)}$. Then we must have $\hat{I}_{max,e} \geq |\hat{I}^*_{3,f,e}| \geq |\hat{I}^{(1)}_{3,f,e}|$.

We first show that the case one can be avoided if we properly set $\eta_{3,p,i}$ in (57) and $\eta_{3,q,i}$ in (58). Specifically, according to (57), we must have

$$\boldsymbol{D}_i\hat{\boldsymbol{p}}_{3,f} + \hat{v}_{3,i}^2\sum_{k=1}^{|V|}\tilde{G}_{ik} - p_{0,i} \leq \eta_{3,p,i} \tag{67}$$

if we set

$$\eta_{3,p,i} \geq (\Delta_{ii} - 1)\epsilon_{p,i} + |\sum_{k=1}^{|V|}\tilde{G}_{ik}|\epsilon_{v,i}, \tag{68}$$

where $(\Delta_{ii} - 1)$ denotes the number of neighbors of node i as defined in (16). Similarly, we can define $\eta_{3,q,i}$ to avoid the first case. Then, we will show how to set $\hat{I}_{max,e}$ so that the second case will not happen. In case two, we must have

$$\hat{I}_{max,e} \geq |\hat{I}^*_{3,f,e}| \geq |\hat{I}^{(1)}_{3,f,e}| \geq |I^{(1)}_{3,e}| - \epsilon_{I,e} > \gamma_e I_{max,e} - \epsilon_{I,e} \tag{69}$$

Thus, if we set $\hat{I}_{max,e} \leq \gamma_e I_{max,e} - \epsilon_{I,e}$, (69) cannot hold, which rules out the possibility of case two. In summary, by properly setting $\eta_{3,p,i}, \eta_{3,q,i}$ and set $\hat{I}_{max,e} \leq \gamma_e I_{max,e} - \epsilon_{I,e}$, a PMU placement that can pass the test of Alg. 4 will achieve our defense goal. □