Preventing Outages under Coordinated Cyber-Physical Attack with Secured PMUs

Yudi Huang, Ting He, Nilanjan Ray Chaudhuri, and Thomas La Porta
Pennsylvania State University, University Park, PA 16802, USA
Email: {yxh5389, tzh58, nuc88, tfl12}@psu.edu

***Abstract*—Due to the severe consequences of the coordinated cyber-physical attack (CCPA), the design of defenses has gained a lot of attention. A popular defense 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* in order to reduce the required number of secured PMUs. To this end, we formulate the problem of *PMU Placement for Outage Prevention (PPOP)* as a tri-level non-linear optimization and transform it into a bi-level mixed-integer linear programming (MILP) problem. Then, we propose an alternating optimization algorithm to solve it optimally. Finally, we evaluate our algorithm on IEEE 30-bus, 57-bus, and 118-bus systems, which demonstrates the advantage of the proposed approach in significantly reducing the required number of secured PMUs.**

I. Introduction

The *coordinated cyber-physical attack (CCPA)* [1] has gained a lot of attention due to its stealthiness and potential for severe damage on smart grid. The danger of CCPA is that its physical component damages the grid while its cyber component masks such damage from the control center (CC) for prolonged outages. For instance, in the Ukrainian power grid attack [2], 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 roughly categorized into *detection* and *prevention*. Attack detection mechanisms aim at detecting attacks that are otherwise undetectable by traditional bad data detection (BDD) by exploiting knowledge unknown to the attacker [3]. 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, who 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. While attack prevention traditionally aims at eliminating undetectable attacks by deploying enough secured PMUs to achieve full observability [4], this approach can require a large number of PMUs. To address this issue, we lower the goal 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 further line tripping (other than those disconnected by the physical attack). The key novelty of our approach is that we allow undetectable attacks to exist but prevent them from causing any outage, hence potentially requiring fewer secured PMUs.

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

A. Related Work

Attacks: False data injection (FDI) is widely adopted to launch cyber attacks in CCPA for bypassing the traditional BDD [1]. A typical form of FDI is load redistribution attack [5], which together with physical attacks [6] aims to mislead SCED by injecting false data for economic loss or severe physical consequences such as sequential outages [7].

Defenses: To eliminate the existence of FDI with minimal cost, different strategies have been studied, such as directly protecting meters [8] or deploying secured PMUs [9], [10]. Different from the aforementioned works, our work only aims to prevent attacks from causing outages, which can significantly reduce the required number of secured PMUs.

Tri-level optimization is widely adopted for modeling interactions among the defender, the attacker, and the operator. In [11], a tri-level model is proposed to find the optimal lines to protect from physical attacks to minimize load shedding. In [12], a similar problem is studied in distribution networks. To minimize the load curtailment, a budget-constrained equipment protection strategy is proposed in [13], while [14] additionally considers the uncertainties regarding the attacking resource. The work closest to ours is [15], which aims to minimize the number of overloaded lines by securing sensor measurements under a budget constraint. Besides the different objectives, [15] also differs from our work in that: (i) their physical attack is limited to a single line and is not optimized; (ii) their defender selects individual meters to protect instead of locations for PMU placement. In contrast, we consider physical attacks that can disconnect multiple lines at optimized locations, and our defense is via deploying secured PMUs that offer protection at the granularity of one-hop neighborhoods. These differences make our problem more challenging while enabling our solution to defend against stronger attacks.

B. Summary of Contributions

We summarize our contributions as follows:

1) Instead of eliminating the existence of CCPA, we investigate an optimal secured PMU placement problem to prevent outages due to CCPA, where we consider a powerful attacker with full knowledge and capability to attack multiple links. As a byproduct, our solution can identify critical measurements for outage prevention.
2) We convert the proposed problem into a bi-level mixed-integer linear programming problem, and propose an alternating optimization algorithm to solve it optimally based on the generation of "no-good" constraints.
3) We evaluate the proposed solution on IEEE 30-bus system, IEEE 57-bus system, and IEEE 118-bus system. Our results demonstrate that the proposed solution requires substantially fewer secured PMUs than the state-of-the-art solution based on achieving full observability.

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 $C_1 \leftrightarrow C_2$ indicates that C_2 is true if and only if C_1 is true. Similarly, logical expression $C_1 \rightarrow C_2$ indicates that C_2 is true if C_1 is true. When the operators $\geq, \leq, =$ are applied to two vectors, they indicate element-wise operations.

A. Power Grid Modeling

We model the power grid as a connected undirected graph $G = (V, E)$, where E denotes the set of links (lines) and V the set of nodes (buses). Under the DC power flow approximation, which is widely adopted for studying security issue on grid [4], [5], [7], each link $e = (s, t)$ is characterized by reactance $r_e = r_{st} = r_{ts}$. The network state is phase angles $\boldsymbol{\theta} := (\theta_u)_{u \in V}$, which are related to active powers $\boldsymbol{p} = (p_u)_{u \in V}$ by

$$\boldsymbol{B}\boldsymbol{\theta} = \boldsymbol{p}, \tag{1}$$

where the *admittance matrix* $\boldsymbol{B} \in \mathbb{R}^{|V| \times |V|}$ is defined as:

$$B_{uv} = \begin{cases} 0 & \text{if } u \neq v, (u,v) \notin E, \\ -1/r_{uv} & \text{if } u \neq v, (u,v) \in E, \\ -\sum_{w \in V \setminus \{u\}} B_{uw} & \text{if } u = v. \end{cases} \tag{2}$$

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:

$$D_{ij} = \begin{cases} 1 & \text{if link } e_j \text{ comes out of node } v_i, \\ -1 & \text{if link } e_j \text{ goes into node } v_i, \\ 0 & \text{otherwise,} \end{cases} \tag{3}$$

where the orientation of each link 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 power flow over links can be represented as $\boldsymbol{f} = \boldsymbol{\Gamma}\boldsymbol{D}^T\boldsymbol{\theta} \in \mathbb{R}^{|E|}$.

The CC will periodically conduct state estimation, whose results will be used for SCED to re-plan the power generation [5], [7]. Formally, let $\boldsymbol{z} = [\boldsymbol{z}_N^T, \boldsymbol{z}_L^T]^T \in \mathbb{R}^m$ denote the 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) links. 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

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

where $\boldsymbol{H}$ is the measurement matrix based on the reported breaker status, and $\boldsymbol{\epsilon}$ is the measurement noise. Suppose $\bar{\boldsymbol{\theta}}$ is the estimated phase angle given $\boldsymbol{z}$ and $\boldsymbol{H}$, BDD will raise alarm if $\|\boldsymbol{z} - \boldsymbol{H}\bar{\boldsymbol{\theta}}\|$ is greater than a predefined threshold.

Given $\bar{\boldsymbol{\theta}}$, 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 $\boldsymbol{p}_0$ as the estimated power injection before SCED, $\hat{\boldsymbol{\theta}}$ 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 [7] as follows:

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

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

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

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

where $\boldsymbol{f}_{max} \in \mathbb{R}^{|E|}$ indicates the 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 load redistribution attacks [5] that aim at causing the maximum outages. The defense against this attack model is formulated to prevent outage under any attack under the same constraints. In the following, "ground truth" means the estimated value based on unmanipulated measurements, which may contain noise.

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

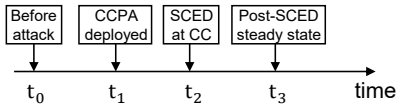

Figure 1. Time sequence of an instance of CCPA

- 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, which changes 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 $\tilde{\boldsymbol{\theta}}_3$ is the associated predicted phase angles.
- At t_3, the new dispatch takes effect and reaches steady state, with the true phase angles $\boldsymbol{\theta}_3$.

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.

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	—	—	$\tilde{\boldsymbol{z}}_2$	—

First, we model the influence of attacks on SCED. We define $\boldsymbol{a}_c \in \mathbb{R}^m$ as the cyber-attack vector, which changes the measurements received by the CC to $\tilde{\boldsymbol{z}}_2 = \boldsymbol{z}_2 + \boldsymbol{a}_c$. Following [1], [6], [7], we define $\boldsymbol{a}_p \in \{0,1\}^{|E|}$ as the physical-attack vector, where $a_{p,e} = 1$ indicates that link e is disconnected by the physical attack. As the physical attack changes the topology, we use $\tilde{\boldsymbol{B}}, \tilde{\boldsymbol{D}}, \tilde{\boldsymbol{H}}$ to 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 $\boldsymbol{H} = \tilde{\boldsymbol{H}} - [(\boldsymbol{\Lambda}_p\tilde{\boldsymbol{D}}\boldsymbol{\Gamma}\text{diag}(\boldsymbol{a}_p)\tilde{\boldsymbol{D}}^T)^T, (\boldsymbol{\Lambda}_f\tilde{\boldsymbol{D}}\text{diag}(\boldsymbol{a}_p))^T]^T$. The falsified information in $\tilde{\boldsymbol{z}}_2, \tilde{\boldsymbol{H}}$ will mislead the CC to an incorrect state estimation and possibly insecure 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 [1]. Considering that $\tilde{\boldsymbol{z}}_2 = \boldsymbol{z}_2 + \boldsymbol{a}_c$, $\boldsymbol{a}_c$ should be constructed such that

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

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

$$\boldsymbol{a}_c = \boldsymbol{z}_0 - \boldsymbol{z}_2 + \tilde{\boldsymbol{H}}(\tilde{\boldsymbol{\theta}}_2 - \boldsymbol{\theta}_0) \quad (8)$$

Besides (8), there may be additional constraints on $\boldsymbol{a}_c$ to avoid causing suspicion. Specifically, following [5], we assume that all the power injections at generator buses are measured and not subject to attacks, i.e.,

$$\boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2 = \boldsymbol{\Lambda}_g\boldsymbol{B}\boldsymbol{\theta}_2 = \boldsymbol{\Lambda}_g\boldsymbol{p}_0, \quad (9)$$

recalling that $\boldsymbol{\Lambda}_g$ is the row selection matrix corresponding to generator buses. Moreover, the magnitude of $\boldsymbol{a}_c$ needs to be constrained, which can be modeled by

$$-\alpha\boldsymbol{\Lambda}_p|\boldsymbol{p}_0| \le \boldsymbol{\Lambda}_N\boldsymbol{a}_c \le \alpha\boldsymbol{\Lambda}_p|\boldsymbol{p}_0|, \quad (10)$$

where α is a constant representing the maximum normal load fluctuation determined by the CC. Note that (9) makes (10) redundant for generator buses. Meanwhile, as the total generation is known to the CC, the falsified loads must preserve the total load in the ground truth, i.e., $\boldsymbol{1}^T\boldsymbol{\Lambda}_N\boldsymbol{a}_c = 0$. Following the convention in [5], [16], the attack is constrained by a predefined constant ξ_p denoting the maximum number of attacked links and another constant ξ_c denoting the maximum number of manipulated measurements, i.e.,

$$\|\boldsymbol{a}_p\|_0 \le \xi_p, \quad \|\boldsymbol{a}_c\|_0 \le \xi_c. \quad (11)$$

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 [7]. 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

$$\tilde{\boldsymbol{D}}_u\boldsymbol{f}_{con} = \begin{cases} |V| - 1, & \text{if } u = u_0, \\ -1, & \text{if } u \in V \setminus \{u_0\}, \end{cases} \quad (12a)$$

$$-|V| \cdot (1 - a_{p,e}) \le f_{con,e} \le |V| \cdot (1 - a_{p,e}). \quad (12b)$$

With links oriented as in $\tilde{\boldsymbol{D}}$, (12a) (flow conservation constraint) and (12b) (link 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 link and $f_{con,e} < 0$ otherwise.

As shown in [7], attacks can cause overload at t_3 since SCED is conducted with falsified information. Moreover, initial overload can cause cascading outages at other links since significantly overloaded links will be automatically tripped by protective relays and the associated power flow will be re-distributed. Specifically, let $\boldsymbol{f}_{max} \in \mathbb{R}^{|E|}$ be the maximum power flows over links under normal conditions. Define γ_e as the threshold of automatic self-disconnection for link e [7], i.e., e will automatically trip itself (i.e., having an outage) if

$$|f_e| > \gamma_e f_{max,e}. \quad (13)$$

C. Modeling Optimal PMU Placement

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; $\Omega(\boldsymbol{\beta}) := \{u|\beta_u = 1\}$. Let $\mathcal{N}_u$ be the node set containing neighbors of node u (including u) and E_u be the link set composed of links incident on u. According to [9], by measuring both voltage and current phasor, a PMU on node u can guarantee the correctness of phase angles in $\mathcal{N}_u$ and protect links in E_u from both cyber and physical attacks. Formally, we define $\boldsymbol{x}_N \in \{0,1\}^{|V|}$ such that $(x_{N,u} = 1) \leftrightarrow (\exists v \in \mathcal{N}_u \text{ such that } \beta_v = 1)$, which can be modeled as

$$\boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} \le \boldsymbol{x}_N \le \boldsymbol{\Delta}^{-1}\underline{\boldsymbol{A}}\boldsymbol{\beta} + (\|\boldsymbol{\Delta}\|_\infty - 1)/\|\boldsymbol{\Delta}\|_\infty, \quad (14)$$

where $\boldsymbol{\Delta} \in \mathbb{Z}^{|V|\times|V|}$ is a diagonal matrix with $\Delta_{uu} = |\mathcal{N}_u|$, 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 $\boldsymbol{x}_L \in \{0,1\}^{|E|}$ such that $(x_{L,e} = 1) \leftrightarrow (\exists v \text{ with } e \in E_v \text{ and } \beta_v = 1)$, which

can be modeled as

$$\frac{1}{2}|\boldsymbol{D}|^T\boldsymbol{\beta} \le \boldsymbol{x}_L \le \frac{1}{2}|\boldsymbol{D}|^T\boldsymbol{\beta} + \zeta, \tag{15}$$

where ζ can be any constant within $[0.5, 1)$. Thus, the constraints on $\boldsymbol{a}_c$ and $\boldsymbol{a}_p$ due to a given $\boldsymbol{\beta}$ can be modeled by (14)-(15) and the following logical expressions:

$$x_{N,u} = 1 \to \tilde{\boldsymbol{\theta}}_{2,u} = \boldsymbol{\theta}_{2,u}, \forall u \in V, \tag{16a}$$

$$x_{L,e} = 1 \to a_{p,e} = 0, \quad \forall e \in E. \tag{16b}$$

Note that (14)-(16) implicitly protect the power flow measurements on links 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 (14)-(15). By (16), it is guaranteed that $\tilde{z}_{2,e} := \frac{\tilde{\theta}_{2,s} - \tilde{\theta}_{2,t}}{r_{st}} = \frac{\theta_{2,s} - \theta_{2,t}}{r_{st}} =: z_{2,e}$.

Now, we are ready to formulate our main problem named *PMU Placement for Outage Prevention (PPOP)*, which aims at placing the minimum number of secured PMUs so that no undetectable CCPA can cause self-tripping (interchangeably used to imply protective tripping due to line overload). To achieve this, we model the problem as a tri-level optimization problem. The *upper-level* optimization is the PMU placement problem over the decision variable $\boldsymbol{\beta} \in \{0,1\}^{|V|}$, formulated as

$$\min \quad \|\boldsymbol{\beta}\|_0 \tag{17a}$$

$$\text{s.t.} \quad \psi_a(\boldsymbol{\beta}) = 0, \tag{17b}$$

where $\psi_a(\boldsymbol{x})$ defined in (18) denotes the maximum number of links that will be tripped according to (13) at t_3. The *middle-level* optimization is the attacker's problem, which defines $\psi_a(\boldsymbol{\beta})$ based on the optimal attack strategy:

$$\psi_a(\boldsymbol{\beta}) := \max \quad \|\boldsymbol{\pi}\|_0 \tag{18a}$$

$$\text{s.t.} \quad (6), (8)-(11), (14)-(16), \tag{18b}$$

$$\boldsymbol{\Gamma}\tilde{\boldsymbol{D}}^T\tilde{\boldsymbol{\theta}}_2 \in [-\boldsymbol{f}_{max}, \boldsymbol{f}_{max}], \tag{18c}$$

$$\boldsymbol{\Lambda}_d\boldsymbol{B}\boldsymbol{\theta}_3 = \boldsymbol{\Lambda}_d\boldsymbol{p}_0, \tag{18d}$$

$$\boldsymbol{\Lambda}_g\boldsymbol{B}\boldsymbol{\theta}_3 = \boldsymbol{\Lambda}_g\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3, \tag{18e}$$

$$\boldsymbol{\theta}_{i,u_0} = 0, \tilde{\boldsymbol{\theta}}_{i,u_0} = 0, \quad i \in \{2,3\}, \tag{18f}$$

$$\boldsymbol{p}_0 = \boldsymbol{B}\boldsymbol{\theta}_2, \tag{18g}$$

$$\tilde{\boldsymbol{\theta}}_3 = \psi_s(\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_2, \tilde{\boldsymbol{D}}), \tag{18h}$$

$$\frac{|\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3|}{f_{max,e}} > \gamma_e \leftrightarrow \pi_e = 1, \forall e \in E. \tag{18i}$$

The binary decision variables are $\boldsymbol{\pi}, \boldsymbol{a}_p, \boldsymbol{x}_N, \boldsymbol{x}_L$, and $\boldsymbol{B}, \boldsymbol{D}, \boldsymbol{\theta}_2, \tilde{\boldsymbol{\theta}}_2, \boldsymbol{\theta}_3, \tilde{\boldsymbol{\theta}}_3$ are continuous variables. Here, $\pi_e = 1$ if and only if link e is overloaded to cause self-tripping, which is ensured by (18i). Thus, the objective of (18) is to maximize the number of links facing self-tripping due to the attack (besides those directly failed by the attack). The constraints (18b)-(18c) are used by the attacker to avoid detection, while (18d)-(18g) are used to enforce the power flow equation (1) for $\tilde{\boldsymbol{\theta}}_3$, $\boldsymbol{\theta}_3$, and $\boldsymbol{\theta}_2$, respectively. Here, $\tilde{\boldsymbol{B}}\tilde{\boldsymbol{\theta}}_3$ in (18e) indicates the new generation computed by SCED, and (18f) fixes the phase angle at the reference node, denoted as node u_0. Constraint (18h) incorporates the *lower-level* optimization of SCED (5) by specifying the post-SCED generation, determined by $\tilde{\boldsymbol{\theta}}_3$. Note that although (18) does not explicitly contain $\boldsymbol{a}_c$, $\boldsymbol{a}_c$ is implicitly specified as a function of $\tilde{\boldsymbol{\theta}}_2$ and $\boldsymbol{\theta}_2$ via (8). In the following, we call $(\boldsymbol{a}_p, \boldsymbol{a}_c, \boldsymbol{\pi}, \boldsymbol{\beta})$ an *attack tuple* since it determines other variables. An attack tuple is called "successful" if $\|\boldsymbol{\pi}\|_0 \ge 1$. The above formulation treats $\boldsymbol{p}_0$ as a constant, which can be easily extended to handle the fluctuations in loads. The detail is illustrated in Appendix A of [17].

III. Solving PPOP

The PPOP problem formulated in (17)-(18) is a tri-level non-linear mixed-integer optimization problem. In this section, we first formally prove that the problem is NP-hard, then transform it into a *bi-level mixed-integer linear programming (MILP)* problem, and finally present an alternating optimization algorithm to solve the problem optimally.

A. Hardness

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 by a reduction from the dominating set problem that PPOP is NP-hard (See proof in Append B of [17].).

Theorem III.1. *The PPOP problem* (17)-(18) *is NP-hard.*

B. Conversion into a Bi-Level MILP

We first transform (18) into a single-level problem. To achieve this, we first transform (5) into its dual problem by using the strong duality of linear programming (LP), which forms a linear system. We refer readers to [5] for the details.

Then, we show how to reformulate (18) as a MILP. In the following, the big-M modeling technique will be frequently applied for linearization by introducing sufficiently large constants denoted as $M_{(\cdot)}$. The calculation of $M_{(\cdot)}$ is given in Appendix C of [17]. To reformulate (16) and (18i) into linear constraints, we introduce M_θ such that (16a) for node u holds if and only if the following inequalities hold:

$$-M_\theta \cdot (1 - \boldsymbol{x}_{N,u}) \le \tilde{\theta}_{2,u} - \theta_{2,u} \le M_\theta \cdot (1 - \boldsymbol{x}_{N,u}), \tag{19}$$

and similar conversion applies to (16b). As for (18i), by defining a sufficiently large constant M_π and two binary auxiliary variables $\pi_{n,e}, \pi_{p,e}$ to get rid of the absolute operation, (18i) is transformed into

$$-M_{\pi,e} \cdot (1 - \pi_{p,e}) < \frac{\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3}{f_{max,e}} - \gamma_e \le M_{\pi,e} \cdot \pi_{p,e}, \tag{20a}$$

$$-M_{\pi,e} \cdot (1 - \pi_{n,e}) < -\frac{\Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3}{f_{max,e}} - \gamma_e \le M_{\pi,e} \cdot \pi_{n,e}. \tag{20b}$$

We claim that $\pi_e = \pi_{n,e} + \pi_{p,e}$. To see this, suppose that $f_{e,3} := \Gamma_e\boldsymbol{d}_e^T\boldsymbol{\theta}_3 \ge 0$. Then, we must have $-\frac{f_{e,3}}{f_{max,e}} - \gamma_e \le 0$ and thus $\pi_{n,e} = 0$, while $\frac{|f_{e,3}|}{f_{max,e}} - \gamma_e = \frac{f_{e,3}}{f_{max,e}} - \gamma_e$ and thus $\pi_{p,e} = \pi_e$. Notice that we must have $\pi_e = 1$ if $|f_{e,3}| - \gamma_e \cdot f_{max,e} > 0$, while $|f_{e,3}| - \gamma_e \cdot f_{max,e} \le 0$ leads to $\pi_e = 0$.

Another challenge is the bilinear terms $a_{p,e}\boldsymbol{\theta}_3$ ($e \in E$) in (18d), (18e), (18i) and $a_{p,e}\boldsymbol{\theta}_2$ ($e \in E$) in (18g). One standard approach to handle such non-linearity is McCormick relaxation. Specifically for $a_{p,e}\boldsymbol{\theta}_3$, we introduce another variable $w_{3,u,e}$ ($\forall u \in V, e \in E$) with linear constraints:

$$-M_w \cdot a_{p,e} \le w_{3,u,e} \le M_w \cdot a_{p,e}, \tag{21a}$$

$$-M_w \cdot (1 - a_{p,e}) \le w_{3,u,e} - \theta_{3,u} \le M_w \cdot (1 - a_{p,e}), \tag{21b}$$

where M_w is a sufficiently large constant such that $-M_w \le \theta_{3,u} \le M_w, \forall u \in V$. It is easy to see that constraints (21) ensure $w_{3,u,e} = a_{p,e}\theta_{3,u}$. Similar trick applies to $a_{p,e}\theta_{2,u}$.

Finally, by introducing binary variables $w_{c,i} \in \{0,1\}, i = 1, \cdots, m$ (recall that m is the number of measurements), the constraint $\|\boldsymbol{a}_c\|_0 \le \xi_c$ in (11) is equivalent to $(a_{c,i} \neq 0) \leftrightarrow (w_{c,i} = 1), \forall i$ with $\sum_{i=1}^{m} w_{c,i} \le \xi_c$, where the logical expression can be linearlized by introducing a sufficiently large constant $M_{a,i}$ as follows:

$$-M_{a,i} w_{c,i} \le a_{c,i} \le M_{a,i} w_{c,i}. \tag{22}$$

Together, the above techniques transform (18) into a MILP, the detail of which is given in Appendix D of [17].

C. An Alternating Optimization Algorithm for PPOP

After transforming (18) into MILP, PPOP becomes a bi-level MILP, which is still difficult to solve due to the integer variables. In [15], a similar problem is solved by enumerating all possible combinations of the upper-level integer variables, which is not scalable. In this section, we propose an alternating optimization algorithm to solve the bi-level MILP obtained in Section III-B by iteratively adding "no-good" constraints to refine the feasible region. The algorithm is motivated by the following simple observation:

Lemma III.1. *Given $\hat{\boldsymbol{\beta}}$ and $\Omega(\hat{\boldsymbol{\beta}})$ (nodes with PMUs under placement $\hat{\boldsymbol{\beta}}$) such that there exists a successful attack tuple $(\boldsymbol{a}_p, \boldsymbol{a}_c, \boldsymbol{\pi}, \hat{\boldsymbol{\beta}})$, 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 $\Omega(\boldsymbol{\beta}) \subseteq \Omega(\hat{\boldsymbol{\beta}})$, $(\boldsymbol{a}_p, \boldsymbol{a}_c, \boldsymbol{\pi}, \boldsymbol{\beta})$ 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 through the following iterative procedure: during each iteration, we first find a solution $\hat{\boldsymbol{\beta}}$ to (17) omitting constraints (17b) (initially, the solution is $\hat{\boldsymbol{\beta}} = \mathbf{0}$), and then solve (18) to obtain $\psi_a(\hat{\boldsymbol{\beta}})$. If $\psi_a(\hat{\boldsymbol{\beta}}) = 0$, $\hat{\boldsymbol{\beta}}$ is the optimal solution; otherwise, we will add the following "no-good" constraint

$$\sum_{i:\hat{\beta}_i = 0} \beta_i \ge 1 \tag{23}$$

to (17) for the next iteration to rule out the infeasible solution $\hat{\boldsymbol{\beta}}$. However, the above procedure will converge 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 further narrow down candidate solutions. This can be achieved by solving the following problem:

$$\max \quad \|\hat{\boldsymbol{\beta}}'\|_0 \tag{24a}$$

$$\text{s.t.} \quad \psi_a(\hat{\boldsymbol{\beta}}') \ge 1, \tag{24b}$$

$$\hat{\beta}'_u = 1, \quad \forall u \in V \text{ with } \hat{\beta}_u = 1. \tag{24c}$$

Then, we can add $\sum_{i:\hat{\beta}'_i = 0} \beta_i \ge 1$ to (17), which subsumes (23). The details of the algorithm is given in Alg. 1, which solves PPOP optimally, as proved in Appendix E of [17].

Theorem III.2. *Algorithm 1 converges in finite time to an optimal solution to* (17)*.*

Algorithm 1: Alternating Optimization

```
Initialization: β̂ = 0, C = ∅;
while True do
    Solve (18) under given β̂ to obtain ψ_a(β̂);
    if ψ_a(β̂) > 0 then
        Solve (24) to obtain β̂', and C ← C ∪ {β̂'};
        Solve min ‖β‖_0 s.t. Σ_{i:β'_i=0} β_i ≥ 1, ∀β' ∈ C
          to update β̂;
    else
        break;
Return β̂, indicators of the selected PMU placement;
```

IV. Numerical Experiments

Simulation Settings: We evaluate our solution against benchmarks in several standard systems: IEEE 30-bus system, IEEE 57-bus system, and IEEE 118-bus system, where the system parameters as well as load profile are obtained from [18]. *The parameters for our evaluation are set as follows unless specified otherwise:* We assume that $\boldsymbol{H}$ has full column rank to support state estimation. We assume all nodes are measured ($m_N = |V|$) and $\alpha = 0.25$ following the the convention in [7]. In addition, 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 $\xi_p = 1$, $\xi_c = \infty$ (no constraint on the number of manipulated meters). We set the self-tripping threshold to $\gamma_e = 1.2, \forall e \in E$, which is slightly smaller than the one used in [7] to make the solution more robust.

Importance of Placing Secured PMUs: We first demonstrate the physical consequence of the attack formulated in (18). With no secured PMUs, the attack can result in self-tripping of 2, 1, and 11 lines for IEEE 30-bus, 57-bus, and 118-bus systems, respectively. In addition, the re-distribution of power flows on the tripped lines can cause further cascading outages. This highlights the importance of deploying secured PMUs.

Saving in the Number of PMUs: In Table II, we compare the number of secured PMUs required by Alg. 1 with what is required to achieve full observability as proposed in [19] under the nominal operating point [18]. The number of PMUs

required by our algorithm, denoted by $\|\boldsymbol{\beta}\|_0^*$, is significantly smaller than what is required by the existing approach, thanks to the lowered goal in PPOP.

Table II
COMPARISON OF THE REQUIRED NUMBER OF PMUS

	30-bus	57-bus	118-bus
$\|\boldsymbol{\beta}\|_0^*$ (PPOP)	1	2	8
Full observability	10	17	32

Impact of System Parameters: Now we evaluate the impact of various parameters on $\|\boldsymbol{\beta}\|_0^*$. First, to study the impact of power injection measurements modeled in (10), we evaluate two extreme cases: $m_N = |V|$ (all nodes are measured) and $m_N = |V_g|$ (only generator nodes are measured). The results in Table III show that measuring more (load) nodes can reduce the required number of PMUs since it reduces the feasible region of the attacker.

Table III
$\|\boldsymbol{\beta}\|_0^*$ UNDER VARYING m_N

	30-bus	57-bus	118-bus
$m_N = \|V_g\|$	2	3	25
$m_N = \|V\|$	1	2	8

Next, we study the effect of α introduced in (10), 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 small α while it is not very sensitive to α.

Table IV
$\|\boldsymbol{\beta}\|_0^*$ UNDER VARYING α

	30-bus	57-bus	118-bus
$\alpha = 0.25$	1	2	8
$\alpha = 0.5$	1	2	9
$\alpha = 0.75$	2	3	10

Finally, we increase ξ_p to evaluate the impact of stronger attacks. As shown in Table V, (i) defending against a stronger attacker requires more PMUs as expected, and (ii) PPOP still requires much fewer PMUs than "Full observability" when the attacker can disconnect multiple lines, which is stronger than the attack model considered in [7], [15].

Table V
$\|\boldsymbol{\beta}\|_0^*$ UNDER VARYING ξ_p

	30-bus	57-bus	118-bus
$\xi_p = 1$	1	2	8
$\xi_p = 2$	2	3	9

V. CONCLUSION

We formulate a multi-level optimization problem to find the optimal secured PMU placement to defend against the coordinated cyber-physical attack (CCPA) in 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 mixed-integer linear programming problem and then propose an alternating optimization algorithm based on "no-good" constraint generation. Our solution can also identify critical measurements for outage prevention. Our experimental results on standard test systems demonstrate the great promise of the proposed approach in reducing the requirement of PMUs.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, 2014.

[9] 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.

[10] F. Aminifar, A. Khodaei, M. Fotuhi-Firuzabad, and M. Shahidehpour, "Contingency-constrained pmu placement in power networks," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 516–523, 2009.

[11] 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.

[12] 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.

[13] 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.

[14] ——, "An improved defender–attacker–defender model for transmission line defense considering offensive resource uncertainties," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2534–2546, 2018.

[15] 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.

[16] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, 2016.

[17] Y. Huang, T. He, N. R. Chaudhuri, and T. L. Porta, "Preventing outages under coordinated cyber-physical attack with secured PMUs," Technical Report, September 2021, https://sites.psu.edu/nsrg/files/2021/09/YudiSGCReport.pdf.

[18] 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.

[19] 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.