This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI: 10.1109/ticps.2026.3705709, IEEE Transactions on Industrial Cyber-Physical Systems

Proactive Defence of Cyber-Physical Networks Against Coordinated Attacks With Optimal Resource Allocation

Min Du, *Member, IEEE*, Xin Zhang, *Senior Member*, David Flynn, *Senior Member*, Zidong Wang, *Fellow, IEEE*

***Abstract*—Cyber-physical power systems (CPPSs) are more vulnerable to coordinated attacks on cyber-physical networks. In this context, this paper first assesses the impact of coordinated attacks and reveals the interdependence of cyber-physical networks in amplifying system vulnerability. To address this issue, a tri-level cyber-physical network defence (CPND) model is proposed to enable proactive defence of cyber-physical networks through optimal protection resource allocation against coordinated attacks. This model considers the cyber and physical network properties as well as their interdependence in CPPSs. Meanwhile, it incorporates the optimal allocation of control centres, providing more practical defence strategies against coordinated attacks. Then, a Column-and-Constraint Generation (C&CG) with optimality cuts algorithm is developed to solve the proposed CPND model, thereby improving computational efficiency. Numerical simulation results verify the superiority of the proposed approach.**

***Index Terms*— Power systems, interdependent cyber-physical networks, coordinated attacks.**

NOMENCLATURE

Sets and Indices

KL	Physical line-node incidence matrix.
N	Set of physical nodes.
V	Set of cyber nodes.
$\boldsymbol{V}_0$	Set of control centres.
L	Set of physical lines.
L	Set of cyber lines.
C	Set of cyber-physical coupled link.
U	Set of attacked cyber links.
O	Set of attacked cyber-physical coupled links.
A	Set of attacked physical lines.
H	Set of protected cyber-physical coupled links.
n	Index of physical nodes.
v	Index of cyber nodes.
l	Index of physical lines.
ℓ	Index of cyber links.

Parameters

H^G	Resource for control centre allocation.
H^P	Protection resource for physical lines.
H^C	Protection resource for cyber links.
$\mathrm{N_V}$	Total information demand in the cyber network (p.u.).
N^O	Total number of cyber-physical coupled links.
K^O	Attack budget for cyber-physical coupled links.
H^O	Protection resource for cyber-physical coupled links.
N^P	Total number of physical lines.
N^C	Total number of cyber links.
K^P	Attack budget for physical lines.
K^C	Attack budget for cyber links.
H^P	Protection resource for physical lines.
H^C	Protection resource for cyber links.
ϖ	Degree of cyber-physical interdependence (p.u.).
$\bar{P}_n^G$	Maximum generation of thermal unit at physical node n (MW).
C_n^G	Generation cost for thermal unit at physical node n ($/MWh).
C_n^D	Penalty cost for load loss at physical node n ($/MWh).
C_l^P	Marginal cost of protecting physical line l ($/unit).
C_ℓ^C	Marginal cost of protecting cyber link ℓ ($/unit).
C_v^V	Marginal cost of allocating a control centre at cyber node v ($/unit).
b_l	Susceptance of physical line l (p.u.).
$\bar{P}_n^D$	Load at physical node n (MW).
$\bar{\theta}_n$	Maximum phase angle at physical node n (rad).
$\bar{F}_l^L$	Power flow capacity of physical line l (MW).

Variables

V_v^G	Information generated at control centre v, for $v \in \boldsymbol{V}_0$ (p.u.).
V_v^D	Information loss at cyber node v (p.u.).
F_ℓ	Information flow of cyber link ℓ (p.u.).
d_l	Binary defence variable for physical line l. If physical line l is protected, $d_l = 1$; otherwise $d_l = 0$.

This work was supported by the U.K. Research and Innovation Future Leaders Fellowship "Digitalisation of Electrical Power and Energy Systems Operation" under Grant MR/W011360/2. (*Corresponding author:* Xin Zhang.)

M. Du and X. Zhang are with the School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, S10 2TN United Kingdom (e-mail: m.du@sheffield.ac.uk; xin.zhang1@sheffield.ac.uk).

David Flynn is with the James Watt School of Engineering, University of Glasgow, G12 8QQ Glasgow, U.K. (e-mail: david. flynn@glasgow.ac.uk).

Zidong Wang is with the Department of Computer Science, Brunel University London, UB8 3PH Uxbridge United Kingdom (e-mail: zidong.wang@brunel.ac.uk).

z_ℓ Binary defence variable for cyber link ℓ. If cyber link ℓ is protected, $z_\ell = 1$; otherwise $z_\ell = 0$.

w_v Binary control centre allocation variable for cyber node v. If a control centre is allocated to cyber node v, $w_v = 1$; otherwise $w_v = 0$.

a_l Binary attack variable for physical line l. If physical line l is attacked, $a_l = 0$; otherwise $a_l = 1$.

u_ℓ Binary attack variable for cyber link ℓ. If cyber link ℓ is attacked, $u_\ell = 0$; otherwise $u_\ell = 1$.

F_l^L Power flow of physical line l (MW).

P_n^G Generation of thermal unit at physical node n (MW).

S_n^D Load loss at physical node n (MW).

θ_n Phase angle at physical node n (rad).

I. Introduction

A. Background

WIHE the advancement of information and communication technologies, power systems are transforming into cyber-physical power systems (CPPSs) consisting of interdependent cyber-physical networks [1-3]. While CPPSs enhance the efficiency and reliability of power transmission [4], their increasing size and complexity pose challenges to cyber-physical resilience under malicious attacks [5]. For example, in April 2013, a sniper attack on the Metcalf substation damaged 17 transformers and caused a significant blackout and financial loss [6]. In December 2015, a cyberattack targeted the Ukrainian grid, causing a massive outage affecting over 220,000 customers [7]. What's worse, coordinated attacks are able to combine cyber-attacks and physical attacks to significantly disrupt cyber and physical networks [8, 9]. Thus, it is of great importance to enhance the cyber-physical resilience of power systems against coordinated attacks, particularly through proactive defence strategies enabled by the optimal allocation of protection resources.

B. Related Works

At present, most research efforts have focused on enhancing the cyber-physical resilience of power systems to mitigate the impact of coordinated attacks. Specifically, a bilevel defence model was presented in [10] to identify vulnerable physical components subjected to coordinated attacks in power systems. Then, the authors in [11] proposed a tri-level defender-attacker-defender (DAD) model to obtain effective defence strategies, which considered proactive physical network defence strategies based on protecting physical lines. Motivated by this tri-level DAD model, a DAD-based network defence model was presented in [12] to minimise the attack damage. Recently, a tri-level proactive robust defence model was developed in [13] to determine defence decisions on distribution lines against malicious attacks. However, previous research has paid limited attention to the inherit interdependence of cyber-physical networks in power systems. Thus, the authors in [14] formulated a resilient network defence model to alleviate the impact of severe contingencies caused by coordinated attacks, while taking into account the interdependent properties of cyber-physical networks but without sufficiently considering the relevant physical laws of power systems.

Therefore, the authors in [15] further assessed the risk of coordinated attacks on power systems with interdependent networks, while taking physical laws into consideration. In reality, cyber and physical networks are equally important in CPPSs, since they are widely deployed and directly affect power system operations due to their interdependence. The authors in [16] further developed a network defence model against coordinated attacks by protecting cyber-physical networks. Nevertheless, this network defence model was still insufficient to characterise the detailed interdependence of cyber-physical networks with essential network properties. Thus, the authors in [17] developed a tri-level optimisation model incorporating a cyber network; however, they assumed that the physical and cyber networks are fully coupled. Meanwhile, the functional interdependence was neglected. In fact, the absence of comprehensive interdependence modelling may cause inadequate identification of critical networks, compromising defence strategies. Moreover, the lack of coordinated resource allocation across cyber and physical networks further limits the effectiveness of defence strategies.

Notably, the authors in [18] proposed a distributionally robust coordinated defence model against coordinated attacks, which considered the interdependent cyber-physical networks in power systems. Subsequently, an improved tri-level defence model was presented in [19] to enhance the cyber-physical resilience of power systems. However, this model ignored the need to protect cyber-physical networks and made an assumption that the interdependence of cyber-physical networks was based on cyber nodes being solely powered by the corresponding physical nodes. In practice, critical cyber nodes are typically equipped with a backup power supply such as a battery to adequately support their energy needs [20]. Meanwhile, another key aspect of cyber network properties is the optimal allocation of control centres when modelling cyber-physical interdependence, which is not considered in these research works.

C. Motivations and Contributions

To sum up, the main research gaps are identified as follows: *i)* Most of the reported studies have not adequately captured the interdependence between the cyber and physical networks of power systems. This underestimates the cyber-physical risks and vulnerabilities of coordinated attacks, thereby preventing effective defence of cyber-physical networks. *ii)* There remains a lack of comprehensive and detailed proactive defence models that explicitly characterise the interdependence between the cyber and physical networks. The absence of such models compromises the performance and robustness of defence strategies for CPPSs against coordinated attacks, particularly the optimal allocation of both cyber and physical protection resources. *iii)* Most of the existing works have not considered the optimal allocation of control centres as a key cyber network component, which leads to suboptimal defence decisions when protecting critical cyber network resources.

Motivated by the above gaps, a tri-level cyber-physical network defence (CPND) model is proposed to enable proactive defence for interdependent cyber-physical networks through the optimal allocation of protection resources. Compared with

traditional defence models that mainly focus on physical networks, the proposed model explicitly extends the defence framework to interdependent cyber-physical networks against coordinated attacks on both physical lines and cyber links. It further optimises protection resources for physical lines and cyber links and determines the optimal control centre location. The main contributions of this paper are listed as follows.

1) This paper first evaluates the operational risks of power systems with interdependent cyber-physical networks under coordinated attacks. The analysis reveals that the interdependence between the cyber and physical networks amplifies system vulnerability to coordinated attacks. To mitigate such risks, a tri-level CPND model is developed to enable proactive defence of cyber-physical networks and enhance the resilience of CPPSs.
2) The CPND model provides a comprehensive defence framework for CPPSs against coordinated attacks. It enables resilient defence decisions through the optimal allocation of protection resources, with features that consider the interdependence of cyber-physical networks. In addition, the optimal allocation of control centres is incorporated into the model to further enable the protection of critical cyber network resources.
3) To obtain the optimal solution, a Column-and-Constraint Generation (C&CG) with optimality cuts algorithm is developed to effectively solve the CPND model for the optimal resource allocation problem with a master and sub-problem scheme. Case studies validate the superiority of the proposed approach in enhancing the cyber-physical resilience of power systems against coordinated attacks.

The remainder of this paper is organised as follows: Section II presents a tri-level CPND framework and gives the mathematical formulation of the CPND model. Section III details the coordinated decomposition algorithm for solving the CPND model. Section IV discusses and analyses the case studies, and Section V concludes this paper.

II. Mathematical Formulation

A. Tri-level Modelling of the Proposed CPND Model

The CPND model can be depicted as a tri-level framework as illustrated in Fig. 1. The cyber-physical network defence strategy includes the protection of physical lines and cyber links, and the allocation of control centres. The three levels of proactive cyber-physical network defence, coordinated attack, and post-attack dispatch are as follows:

1) Upper-Level Proactive Defence Strategy: The proactive cyber-physical network defence strategy identifies critical cyber and physical networks that need to be protected and optimally allocates the control centre location, aiming to minimise the total cost of power system operations under the worst-case coordinated attack scenario. The network defence strategy is delivered to the mid- and lower-levels, and the control centre location allocation strategy is transferred to the lower-level strategy.

2) Mid-Level Coordinated Attack Strategy: The coordinated attack strategy aims to maximise the power system operational cost by attacking cyber and physical networks. More specifically, the attacker disrupts both physical lines and cyber links through coordinated attacks to achieve the maximum benefit. Then, the coordinated attack strategy is transmitted to the lower-level strategy.

3) Lower-Level Post-Attack Dispatch Strategy: Based on the coordinated attack scenario, the post-attack dispatch strategy aims to minimise the power system operational cost while ensuring the secure operation of the interdependent cyber-physical networks. It should be noted that the lower-level strategy interacts with the mid-level strategy to calibrate the optimal post-attack dispatch strategy under the worst-case coordinated attack scenario.

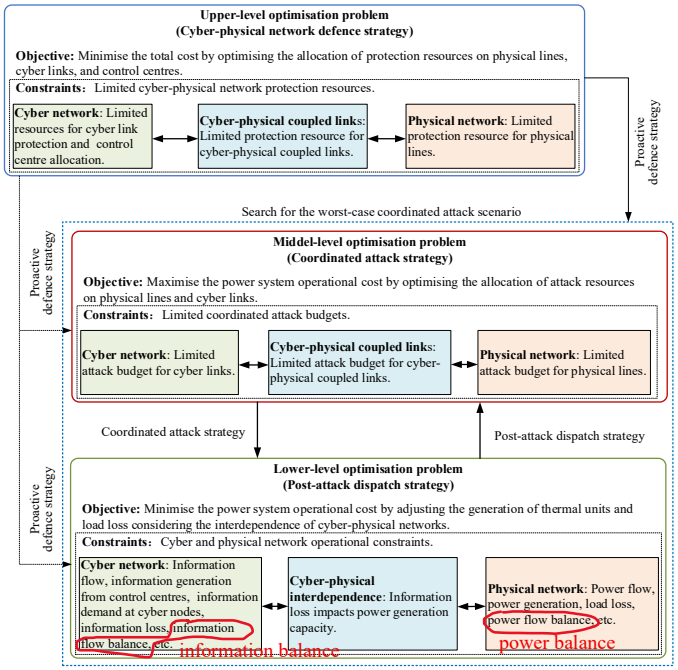

Fig. 1. Tri-level framework of the CPND model for proactive cyber-physical network defence and optimal resource allocation.

B. Mathematical Formulation of the Proposed CPND Model

The tri-level framework of the CPND model is mathematically formulated as three optimisation problems:

1) Upper-Level Optimisation Problem: The upper-level problem determines the optimal network defence decision to minimise the total cost of power system operation. The total cost is the sum of the defence cost and the power system operational cost. Note that the defence cost includes the costs of protecting physical lines, cyber links, and allocating control centres. Thus, this problem is modelled below:

$$\min_{\{d_l, z_\ell, w_v\}} \left[\sum_{l \in \boldsymbol{L}} C_l^P d_l + \sum_{\ell \in \boldsymbol{L}} C_\ell^C z_\ell + \sum_{v \in \boldsymbol{V}} C_v^V w_v + \max_{\{a_l, u_\ell\}} Q(a_l, u_\ell) \right] \tag{1}$$

subject to:

$$\sum_{l \in \boldsymbol{L}} d_l \le H^P \qquad d_l \in \{0,1\} \tag{2}$$

$$\sum_{\ell \in \boldsymbol{L}} z_\ell \le H^c \qquad z_\ell \in \{0,1\} \tag{3}$$

$$\mathbf{H} = \left\{ \begin{matrix} (d_l, z_\ell) \in \{0,1\} : \sum_{l \in \mathbf{C}} d_l \le H^O \\ , d_l = z_\ell, \ell \in \mathbf{C} \end{matrix} \right\} \tag{4}$$

$$\sum_{v\in\boldsymbol{V}} w_v \le H^G \qquad w_v \in \{0,1\} \tag{5}$$

where constraint (2) ensures that the number of protected physical lines is less than or equal to the available protection resource H^P. Constraint (3) ensures that the number of protected cyber links do not exceed H^C. Constraint (4) ensures that protection resources are allocated to cyber-physical coupled links within H^O. Notably, the physical line(s) and cyber link(s) belonging to the cyber-physical coupled link set $\mathbf{C}$ are protected simultaneously, and each cyber-physical coupled link requires only one protection resource. Constraint (5) means that the number of control centres is no more than H^G. In addition, it should be noted that $\max_{\{a_l,u_\ell\}} Q(a_l,u_\ell)$ is used to identify the worst-case coordinated attack scenario in order to maximise the power system operational cost at the mid-level problem, and $Q(a_l,u_\ell)$ minimises the power system operational cost after coordinated attacks at the lower-level problem.

2) Mid-Level Optimisation Problem: The mid-level problem determines the worst-case coordinated attack strategy to maximise the power system operational cost, which consists of the generation cost of thermal units and the load loss cost. Thus, this problem is formulated below:

$$\max_{\{a_l,u_\ell\}} \left(\sum_{n\in\boldsymbol{N}} C_n^G P_n^G + \sum_{n\in\boldsymbol{N}} C_n^D S_n^D \right) \tag{6}$$

subject to:

$$\boldsymbol{A} = \left\{ \begin{array}{l} \sum_{l\in\boldsymbol{L}} \left[1-(1-d_l)\cdot(1-a_l)\right] \\ \ge N^P - K^P, (d_l,a_l)\in\{0,1\} \end{array} \right\} \tag{7}$$

$$\boldsymbol{U} = \left\{ \begin{array}{l} \sum_{\ell\in\boldsymbol{L}} \left[1-(1-z_\ell)\cdot(1-u_\ell)\right] \ge \\ N^C - K^C, (z_\ell,u_\ell)\in\{0,1\} \end{array} \right\} \tag{8}$$

$$\boldsymbol{O} = \left\{ \begin{array}{l} (a_l,u_\ell)\in\{0,1\} : \sum_{l\in\boldsymbol{C}} \left[1-(1-d_l)\cdot \right. \\ \left. (1-a_l)\right] \ge N^O - K^O, a_l = u_\ell, \ell\in\boldsymbol{C} \end{array} \right\} \tag{9}$$

where constraint (7) guarantees that the number of attacked physical lines is less than or equal to K^P. Constraint (8) denotes that the number of attacked cyber links is no more than K^C. Constraint (9) ensures that the number of attacked cyber-physical coupled links within K^O. Notably, the physical lines and cyber links belonging to the cyber-physical coupled link set $\boldsymbol{C}$ are simultaneously interrupted, and therefore their attack statuses are the same. Cyber-physical coupled links characterise the topological interdependence between cyber and physical networks, as they are often supported by shared physical infrastructures such as OPGW cables [21]. Note that this paper considers specific coordinated attack scenarios with static attack budgets, which is consistent with operational practices and supported by prior works [22, 23]. In fact, the attack budgets can be reasonably estimated based on available data and expert knowledge, and this assumption does not limit the generality of the proposed model.

3) Lower-Level Optimisation Problem: The lower-level problem minimises both the generation cost of thermal units and the load loss cost after coordinated attacks, and this problem is formulated below:

$$Q(a_l,u_\ell) = \min_{V_v^G, V_v^D, F_\ell, P_n^G, S_n^D, F_l^L} \left(\sum_{n\in\boldsymbol{N}} C_n^G P_n^G + \sum_{n\in\boldsymbol{N}} C_n^D S_n^D \right) \tag{10}$$

The proposed CPND model operates on the energy dispatch timescales of minutes or hours, while the actual delay or congestion in cyber network is usually considered on milliseconds timescale, which does not impact the operational decisions of this modelling work. In addition, it is assumed that the transmission network is equipped with dedicated cyber links between control centres and substations, which significantly reduces the time delay and congestion considered in other cyber networks. Therefore, the delay or congestion in cyber network is not considered in this CPND model.

This post-attack dispatch problem is subject to cyber and physical network operational constraints. The cyber network is subject to the following operational constraints:

$$V_v^G - \sum_{\ell|o(\ell)=v} F_\ell + \sum_{\ell|d(\ell)=v} F_\ell + V_v^D = 1 \qquad \forall v\in\boldsymbol{V} \tag{11}$$

$$0 \le V_v^D \le 1 \qquad \forall v\in\boldsymbol{V} \tag{12}$$

$$0 \le V_v^G \le \mathrm{N_V}\cdot w_v \qquad \forall v\in\boldsymbol{V}_0 \tag{13}$$

$$-\left[1-(1-z_\ell)(1-u_\ell)\right]\mathrm{N_V} \le \mathrm{F}_\ell \qquad \forall \ell\in\boldsymbol{L} \tag{14}$$

$$\mathrm{F}_\ell \le \left[1-(1-z_\ell)(1-u_\ell)\right]\mathrm{N_V} \qquad \forall \ell\in\boldsymbol{L} \tag{15}$$

Control centres are assumed to be located at certain cyber nodes to generate and inject information into the cyber network. Therefore, V_v^G denotes the information generated locally at cyber node v when a control centre is allocated at this node. This means that V_v^G represents the local information injection at cyber node v. Thus, constraint (11) preserves the information flow balance at cyber node v. In addition, $o(\ell)$ and $d(\ell)$ are the "from" and "to" nodes of cyber link ℓ, respectively. Constraint (12) indicates the limits for information loss at cyber node v. Constraint (13) indicates that when $w_v = 1$, a control centre is located at cyber node v, and the information generated by the control centre should not exceed the total information demand. If $w_v = 0$, cyber node v is not equipped with a control centre, and this cyber node functions as either an information demand node or an information transmission node without generating information. Constraints (14)-(15) limit the information flow capacity of cyber link ℓ, which are associated with the protection and attack variables of cyber link ℓ (i.e., z_ℓ and u_ℓ).

In the physical network, the DC power flow model is adopted due to its high efficiency and sufficient accuracy, while AC models introduce significant nonlinearities and computational complexity [24]. The steady-state DC power flow model is assumed to be more compatible with this study of transmission-level energy dispatch problems, while power system dynamic and transient behaviours are not considered. In addition, the DC power flow model is more practical for integration with the

information flow-based cyber network model. Therefore, the physical network is subject to the following operational constraints:

$$P_n^G - \sum_{l \in \boldsymbol{L}} \mathbf{KL}_{l,n} F_l^L + S_n^D = \bar{P}_n^D \qquad \forall n \in \boldsymbol{N} \tag{16}$$

$$F_l^L = \left[1-(1-d_l)(1-a_l)\right] b_l \sum_{n \in \boldsymbol{N}} \mathbf{KL}_{l,n} \boldsymbol{\theta}_n \qquad \forall l \in \boldsymbol{L} \tag{17}$$

$$-\bar{F}_l^L \le F_l^L \le \bar{F}_l^L \qquad \forall l \in \boldsymbol{L} \tag{18}$$

$$0 \le P_n^G \le (1-\varpi V_v^D)\bar{P}_n^G \qquad \forall n \in \boldsymbol{N}, \forall v \in \boldsymbol{V} \tag{19}$$

$$0 \le S_n^D \le \bar{P}_n^D \qquad \forall n \in \boldsymbol{N} \tag{20}$$

$$-\bar{\theta}_n \le \theta_n \le \bar{\theta}_n \qquad \forall n \in \boldsymbol{N} \tag{21}$$

where constraint (16) represents the power balance at physical node n. Constraint (17) calculates the power flow of physical line l with physical line protection and attack variables, (i.e., d_l and a_l). Constraint (18) enforces the power flow limit for physical line l. Constraint (19) limits the minimum and maximum generation of the thermal unit at physical node n, which is affected by the information loss at cyber node v. Note here that each cyber node $v \in \boldsymbol{V}$ is associated with exactly one physical node $n \in \boldsymbol{N}$, forming a one-to-one mapping. It can be observed that the generation capacity of thermal units is influenced by the information loss at cyber node v, since the operation and control of the physical network in CPPSs rely heavily on information from cyber nodes in the cyber network. Specifically, the generation upper bound of thermal units is scaled by a factor $(1-\varpi V_v^D)$, where ϖ denotes the degree of cyber-physical interdependence, directly reflecting the impact of information loss on the generation capacity of physical node. Hence, the operability of the corresponding thermal unit generation capacity adjustment is constrained when the control function of cyber node v is compromised due to information loss. It effectively captures the functional interdependence between the cyber and physical networks. Constraint (20) limits the load loss. Constraint (21) limits the phase angle at physical node n.

III. C&CG With Optimality Cuts Algorithm

The C&CG with optimality cuts algorithm is developed with a master and sub-problem scheme to effectively solve the CPND model with the optimal solution. To facilitate the solution algorithm, the model compact form is shown below:

$$\min_{\boldsymbol{x}} \boldsymbol{A}^{\mathrm{T}} \boldsymbol{x} + \sup_{\boldsymbol{y}} Q(x, y) \tag{22}$$

$$\text{s.t.} \quad \boldsymbol{B}\boldsymbol{x} \le \boldsymbol{b} \tag{23}$$

$$\sup_{\boldsymbol{y}} Q(x, y) = \max_{\boldsymbol{y}} Q(x, y) \tag{24}$$

$$\text{s.t.} \quad \boldsymbol{C}\boldsymbol{x} + \boldsymbol{E}\boldsymbol{y} \le \boldsymbol{e} \tag{25}$$

$$Q(x, y) = \min_{\boldsymbol{p}} \boldsymbol{G}^{\mathrm{T}} \boldsymbol{p} \tag{26}$$

$$\text{s.t.} \quad \boldsymbol{L}\boldsymbol{x} + \boldsymbol{K}\boldsymbol{p} \le \boldsymbol{u} \qquad \boldsymbol{\varphi} \tag{27}$$

$$\boldsymbol{V}\boldsymbol{y} + \boldsymbol{U}\boldsymbol{p} \le \boldsymbol{f} \qquad \boldsymbol{\gamma} \tag{28}$$

$$\boldsymbol{F}\boldsymbol{x} + \boldsymbol{H}\boldsymbol{y} + \boldsymbol{Z}\boldsymbol{p} \le \boldsymbol{h} \qquad \boldsymbol{\pi} \tag{29}$$

where formulations (22)-(23) correspond to the upper-level optimisation problem (1)-(5). Formulations (24)-(25) refer to the mid-level optimisation problem (10)-(13). Formulations (26)-(29) represent the lower-level optimisation problem (10)-(21). Vector $\boldsymbol{x}$ represents the defence decision variables in the upper-level problem (i.e., d_l, z_ℓ and w_v). Vector $\boldsymbol{A}$ represents the marginal cost of the defence decisions. Vector $\boldsymbol{y}$ refers to the network attack decision variables in the mid-level problem (i.e., a_l and u_ℓ). Vector $\boldsymbol{p}$ corresponds to V_v^G, V_v^D, F_ℓ, P_n^G, S_n^D, θ_n and F_l^L which are the dispatch decision variables in the lower-level problem. Vector $\boldsymbol{G}$ represents the marginal cost of the dispatch decision. The vectors dual variables $\boldsymbol{\varphi}$, $\boldsymbol{\gamma}$, and $\boldsymbol{\pi}$ are associated with constraints (27)-(29), respectively. 'T' denotes the transpose.

A. Compact Form of the Sub-Problem Scheme

Based on the network defence strategy, duality theory is used to transform the max-min model described by formulations (24)-(29) into a single maximisation problem. Thus, the dualised problem is derived as follows:

$$\mathrm{T}(\boldsymbol{x}, \boldsymbol{y}) = \max_{\boldsymbol{\varphi}, \boldsymbol{\gamma}, \boldsymbol{\pi}} (\boldsymbol{u} - \boldsymbol{L}\hat{\boldsymbol{x}})^{\mathrm{T}} \boldsymbol{\varphi} + (\boldsymbol{f} - \boldsymbol{V}\boldsymbol{y})^{\mathrm{T}} \boldsymbol{\gamma} + (\boldsymbol{h} - \boldsymbol{F}\hat{\boldsymbol{x}} - \boldsymbol{H}\boldsymbol{y})^{\mathrm{T}} \boldsymbol{\pi} \tag{30}$$

subject to:

$$\boldsymbol{K}^{\mathrm{T}} \boldsymbol{\varphi} + \boldsymbol{U}^{\mathrm{T}} \boldsymbol{\gamma} + \boldsymbol{Z}^{\mathrm{T}} \boldsymbol{\pi} \le \boldsymbol{G} \tag{31}$$

$$\boldsymbol{\varphi} \le \boldsymbol{0}, \boldsymbol{\gamma} \le \boldsymbol{0}, \boldsymbol{\pi} \le \boldsymbol{0} \tag{32}$$

$$\boldsymbol{C}\boldsymbol{x} + \boldsymbol{E}\boldsymbol{y} \le \boldsymbol{e} \tag{33}$$

where (30) refers to the objective function of the dualised problem, defined as $\mathrm{T}(\boldsymbol{x}, \boldsymbol{y})$. Constraint (31) represents the dual constraint generated based on the vector $\boldsymbol{p}$, which is composed of the dispatch decision variables in the lower-level problem. Additionally, constraint (32) involves the declaration of dual variable vectors. Once the sub-problem is solved, to accelerate convergence, two types of cuts are iteratively generated and added to the master problem.

The first cut type consists of feasibility and optimality cuts derived from the system response, which ensure that the master problem remains consistent with the lower-level operational constraints. For any variable $\boldsymbol{x}$ from the upper-level problem, constraints (10)-(21) are always feasible due to the load loss allowed at the lower-level problem. Thus, the infeasibility of the upper-level problem does not need to be checked. This implies that we only need to generate the optimality cut and add this cut to the master problem. Let ω represent the objective function value of $\sup_{\boldsymbol{y}} Q(\boldsymbol{x}, \boldsymbol{y})$. If $\omega < \mathrm{T}(\boldsymbol{x}, \boldsymbol{y})$, the optimality cut is generated and added to the master problem. This cut can be described as follows:

$$\begin{aligned} \omega \ge & \left(\boldsymbol{u} - \boldsymbol{L}\boldsymbol{x}\right)^{\mathrm{T}} \hat{\boldsymbol{\varphi}}_k + \left(\boldsymbol{f} - \boldsymbol{V}\hat{\boldsymbol{y}}_k\right)^{\mathrm{T}} \hat{\boldsymbol{\gamma}}_k + \\ & \left(\boldsymbol{h} - \boldsymbol{F}\boldsymbol{x} - \boldsymbol{H}\hat{\boldsymbol{y}}_k\right)^{\mathrm{T}} \hat{\boldsymbol{\pi}}_k \end{aligned} \tag{34}$$

The second cut type corresponds to adversarial scenario cuts, which are generated based on worst-case coordinated attack strategies to progressively refine the solution space. After

obtaining the network attack strategy in the k-th iteration (i.e., $\hat{\boldsymbol{y}}_k$), if $\omega < \mathrm{T}(\boldsymbol{x}, \boldsymbol{y})$, constraints (35)-(38) will be added to the master problem. These constraints are used to enforce the feasibility of defence decisions under newly identified worst-case attack scenarios and to iteratively tighten the solution space.

$$\omega \geq \boldsymbol{G}^{\mathrm{T}} \boldsymbol{p}_k \tag{35}$$

$$\boldsymbol{L}\boldsymbol{x} + \boldsymbol{K}\boldsymbol{p}_k \leq \boldsymbol{u} \tag{36}$$

$$\boldsymbol{V}\hat{\boldsymbol{y}}_k + \boldsymbol{U}\boldsymbol{p}_k \leq \boldsymbol{f} \tag{37}$$

$$\boldsymbol{F}\boldsymbol{x} + \boldsymbol{H}\hat{\boldsymbol{y}}_k + \boldsymbol{Z}\boldsymbol{p}_k \leq \boldsymbol{h} \tag{38}$$

This C&CG algorithm with additional optimality cut generation mechanisms effectively shrink the feasible region and accelerates convergence to the optimal solution.

B. Compact Form of the Master Problem Scheme

Given the variable values obtained from the sub-problem, the master problem can be expressed below:

$$W(\boldsymbol{x}, \omega) = \min_{\boldsymbol{x}} \boldsymbol{A}^{\mathrm{T}} \boldsymbol{x} + \omega \tag{39}$$

subject to:

$$\boldsymbol{B}\boldsymbol{x} \leq \boldsymbol{b} \tag{40}$$

$$\begin{aligned} \omega \geq\ & (\boldsymbol{u} - \boldsymbol{L}\boldsymbol{x})^{\mathrm{T}} \hat{\boldsymbol{\varphi}}_k + \left(\boldsymbol{f} - \boldsymbol{V}\hat{\boldsymbol{y}}_k\right)^{\mathrm{T}} \hat{\boldsymbol{\gamma}}_k + \\ & \left(\boldsymbol{h} - \boldsymbol{F}\boldsymbol{x} - \boldsymbol{H}\hat{\boldsymbol{y}}_k\right)^{\mathrm{T}} \hat{\boldsymbol{\pi}}_k \end{aligned} \tag{41}$$

$$\omega \geq \boldsymbol{G}^{\mathrm{T}} \boldsymbol{p}_k \tag{42}$$

$$\boldsymbol{L}\boldsymbol{x} + \boldsymbol{K}\boldsymbol{p}_k \leq \boldsymbol{u} \tag{43}$$

$$\boldsymbol{V}\hat{\boldsymbol{y}}_k + \boldsymbol{U}\boldsymbol{p}_k \leq \boldsymbol{f} \tag{44}$$

$$\boldsymbol{F}\boldsymbol{x} + \boldsymbol{H}\hat{\boldsymbol{y}}_k + \boldsymbol{Z}\boldsymbol{p}_k \leq \boldsymbol{h} \tag{45}$$

Note that the C&CG with optimality cuts are successively added to the master problem in each iteration until the prescribed tolerance gap is met, thereby ensuring convergence to the optimal solution. The solution algorithm is as follows:

Algorithm 1: The C&CG with optimality cuts algorithm for solving the CPND model.

Step 1	Initialise protection strategy $\hat{\boldsymbol{x}}$ and let attack strategy set $\boldsymbol{A} = \varnothing$. Set $UB = +\infty$, $LB = -\infty$, and k=1. In addition, the tolerance gap ε is set to 0.01.
Step 2	Based on $\boldsymbol{A}$, solve the master problem (39)-(45) to update the protection strategy $\hat{\boldsymbol{x}}$ and obtain its optimal objective value $W(\hat{\boldsymbol{x}}, \hat{\omega})$. Update $LB = \max\{LB, W(\hat{\boldsymbol{x}}, \hat{\omega})\}$.
Step 3	Based on the updated $\hat{\boldsymbol{x}}$, solve the subproblem (30)-(33) to identify the worst-case attack strategy $\hat{\boldsymbol{y}}_k$ and obtain $\mathrm{T}(\hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}_k)$. Update $UB = \min\{UB, \mathrm{T}(\hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}_k)\}$ and update $\boldsymbol{A} = \boldsymbol{A} \cup \hat{\boldsymbol{y}}_k$.
Step 4	If $\lvert UB - LB \rvert / UB > \varepsilon$, the C&CG with optimality cuts (41)-(45) are added to the master problem. Subsequently, set k=k+1 and return to step 2. Otherwise, terminate and output the optimal defence strategy.

IV. Case Studies

In this section, the modified IEEE 24-bus and IEEE RTS-96 test systems are used for case studies. The CPND model is implemented in MATLAB R2019b and solved using CPLEX 12.4 on a desktop computer with an Intel i9-13900KS processor and 96 GB RAM, with a tolerance gap of 0.01. The protection costs for each physical line and cyber link are set to \$200 and \$100, respectively. The load loss penalty is \$150/MW, and the control centre allocation cost is \$50 per unit. These cost settings are subject to change according to the specific case study requirements; therefore, they do not affect the generality of the proposed model.

A. Vulnerability Analysis and Risk Assessment

This part studies the vulnerability of CPPSs and assesses the risk of coordinated attacks on the IEEE 24-bus system. The top 10 physical lines in terms of power capacity are designated as cyber-physical coupled links for illustrative purposes. This selection does not affect the generality of the proposed model, which remains applicable to other configurations of cyber-physical coupled links. It is considered that control centres are located at cyber nodes 9 and 15, respectively.

1) Vulnerability of Interdependent Cyber-physical Networks: This case study compares the cyber-physical attacker-defender (AD) model with the physical-only AD model developed in [25] to reveal the amplified vulnerability of interdependent cyber-physical networks to coordinated attacks. Here, the cyber-physical AD model is the CPND model without proactive network protection actions, and the control centre locations are randomly allocated. The attack budget is set to 3 (i.e., $K^P = 3$ and $K^C = 3$). The coordinated attack budget K^O is set to 2, and the degree of cyber-physical interdependence ϖ is set to 1.0 p.u. to enable the vulnerability analysis under strong cyber-physical interdependence.

TABLE I.
Vulnerability Analysis of Interdependent Cyber-Physical Networks

Vulnerability analysis	Cyber-physical AD model	Physical-only AD model in [25]
Attacked physical lines	11, 25*, 26*	25, 26, 28
Attacked cyber links	25*, 26*, 28	\
Load loss (MW)	720.00	212.00
Total cost (\$)	170601.57	103515.23

† "*" denotes the cyber-physical coupled link.

As shown in Table I, with the consideration of cyber-physical network interdependence, there is more load loss and a higher total cost. Also, a comparison of the two models in Table I confirms that the physical-only and coordinated attack strategies become different due to the interdependence of cyber-physical networks. If this interdependence of cyber-physical networks is ignored, the attacked physical lines are 25, 26, and 28 in [25]. However, when the interdependence of cyber-physical networks is modelled, the attacked physical lines change to 11, 25, and 26. Moreover, cyber links 25, 26, and 28 are also attacked due to coordinated attacks on the cyber-physical networks of the CPPSs. This suggests that the

interdependence of cyber-physical networks amplify system vulnerability and enables higher-impact coordinated attacks.

2) Risk Assessment of Coordinated Attacks: This case further assesses the risk of coordinated attacks on CPPSs by incorporating the interdependence of cyber-physical networks. The attack budget is set to vary from 3 to 7, with $K^P = K^C$. The coordinated attack budget is set to 2 (i.e., $K^O = 2$). Table II presents the comparison results for case studies with physical-only and cyber-physical networks.

As shown in Table II, an increase in the attack budget results in a higher total cost. For example, in the cyber-physical AD model, the total cost is \$170,601.57 when the attack budget is 3 (i.e., $K^P = 3$ and $K^C = 3$), while it increases to \$208,088.84 if the attack budget raises to 4. This difference in the total cost becomes more significant as the attack budget increases. In addition, it can be observed that coordinated attacks on interdependent cyber-physical networks can lead to more severe impacts. For example, the total cost is \$256,387.97 in the cyber-physical AD model when the attack budget is 5, compared to \$158,789.62 in the physical-only AD model [25]. Notably, Table II also shows the load loss under different attack budgets. The load loss caused by coordinated attacks in the cyber-physical AD model is always higher than that in the physical-only AD model [25]. Failure to consider the interdependence of cyber-physical networks may result in an underestimation of the coordinated attack impacts. These risk assessments highlight the importance of cyber-physical network defence strategies to protect CPPSs from coordinated attacks.

TABLE II.
RISK ASSESSMENT UNDER PHYSICAL-ONLY AND DIFFERENT ATTACK BUDGETS

Attack budget	Cyber-physical AD model				Physical-only AD model in [25]		
	Attacked physical lines	Attacked cyber links	Total cost ($)	Load loss (MW)	Attacked physical lines	Total cost ($)	Load loss (MW)
2	12, 13	1, 11	83500.66	296.00	19, 23	71680.19	194.00
3	11, 25*, 26*	25*, 26*, 28	170601.57	720.00	25, 26, 28	103515.23	212.00
4	11, 18*, 31, 38	15, 17, 18*, 29	208088.84	1171.00	7, 21, 22, 23	135317.73	516.00
5	7, 11, 18*, 23*, 29	15, 17, 18*, 23*, 29	256387.97	1591.00	15, 17, 18, 23, 27	158789.62	842.00
6	2, 7, 11, 24*, 28, 29	14, 15, 16, 17, 24*, 28	270149.14	1691.00	7, 11, 18, 20, 21, 23	177398.85	1017.00
7	7, 24*, 28, 30, 32, 33, 38	2, 8, 12, 14, 15, 24*, 28	335527.43	2200.00	21, 22, 25, 26, 28, 36, 37	194338.95	872.00

† "*" denotes the cyber-physical coupled link.

B. Proactive Defence of Coordinated Attacks

1) Risk Mitigation of the CPND Model: In this case study, the proactive defence strategies of the CPND model in mitigating coordinated attacks on CPPSs are analysed, considering the interdependence of cyber-physical networks. The attack budget is set to 3 (i.e., $K^P = 3$ and $K^C = 3$). The coordinated attack budget is $K^O = 2$. The protection resource is 3, (i.e., $H^P = 3$ and $H^C = 3$). Note that the coupled protection resource is $H^O = 1$, which is manually set to the maximum values of available coupled protection resources. The control centre resource is $H^G = 2$, and the degree of cyber-physical interdependence ϖ is 1.0 p.u.

As observed in Table III, based on the cyber-physical AD model, the attacked physical lines are 11, 25, and 26, and the attacked cyber links are 25, 26, and 28. Nevertheless, this model only identifies vulnerable cyber-physical networks and does not provide proactive network protection or the optimal allocation of control centres (i.e., the control centres are randomly allocated to cyber nodes 9 and 15). Conversely, the CPND model provides the proactive network defence strategy, suggesting that the protected physical lines should be 21, 28, and 29, and the protected cyber links should be 1, 21, and 33. The total cost obtained using the CPND model is \$73541.00, which is significantly less than the \$170,601.57 obtained using the cyber-physical AD model. This implies that the CPND model can provide an optimal allocation of cyber and physical defence resources to enhance the cyber-physical resilience against coordinated attacks. Cyber nodes 7 and 22 are selected as the optimal locations for control centres.

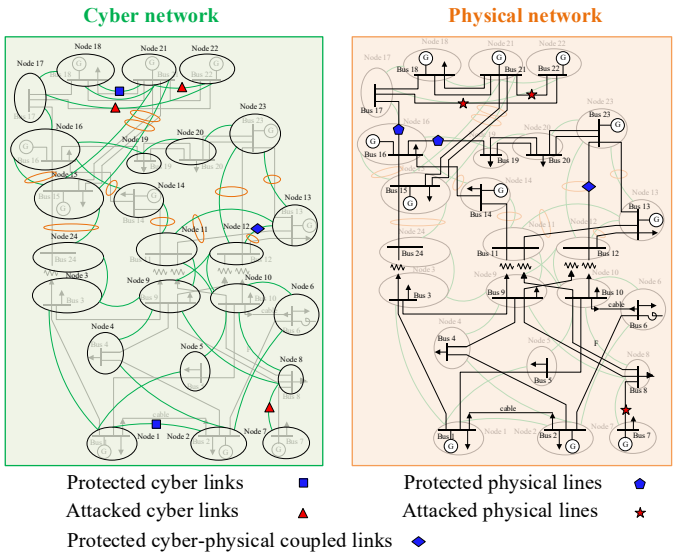

Fig. 2. Illustration of proactive defence strategies and coordinated attacks on the cyber-physical network topology of the IEEE 24-bus system.

In addition, the physical-only DAD model [11] is implemented for further comparison. As shown in Table III, the CPND model yields a total cost of \$73541.00, which is slightly higher than the \$70,860.32 obtained by the physical-only DAD model. This is because the CPND model considers a more comprehensive cyber-physical defence framework, including cyber link protection, cyber-physical interdependence, and control centre allocation, whereas the physical-only DAD only protects physical lines. Thus, the lower cost of the physical-only DAD model results from defending only the physical network and may underestimate cyber-physical operational risks, thereby limiting the applicability of the cyber-physical coordinated defence strategy to CPPSs.

TABLE III.
COMPARATIVE RESULTS OF VARIOUS PROACTIVE AND NON-PROACTIVE DEFENCE MODELS ON THE IEEE 24-BUS SYSTEM

Comparative analysis	Proposed CPND model	Cyber-physical AD model	Physical-only DAD model [11]
Protected physical lines	21*, 28, 29	\	23, 28, 29
Protected cyber links	1, 21*, 33	\	\
Attacked physical lines	11, 31, 38	11, 25*, 26*	2, 6, 27
Attacked cyber links	11, 31, 38	25*, 26*, 28	\
Control centre location	7, 22	9, 15	9, 15
Total cost ($)	73541.00	170,601.57	70860.32

† "*" denotes the cyber-physical coupled link.

2) Degree of Cyber-Physical Interdependence: To investigate the impact of cyber-physical network interdependence, case studies are conducted by varying the degree of cyber-physical interdependence ϖ from 0.1 to 1.0 p.u. with a step size of 0.2. The attack budget is set to 4 (i.e., $K^P = 4$ and $K^C = 4$), including coordinated attack budget $K^O = 2$. The protection resource is set to 3 (i.e., $H^P = 3$ and $H^C = 3$), and the coupled protection resource is $H^O = 2$. The control centre resource is $H^G = 2$. Table IV shows the simulation results.

It can be found that the total cost increases with the higher degree of cyber-physical interdependence under both the proposed CPND model and the cyber-physical AD model. These increased costs are attributed to greater impacts of information loss that can compromise the operability of the physical networks, requiring higher costs to defend against cyber-physical coordinated attacks. For the same degree of cyber-physical interdependence, for example, at $\varpi = 1.0$ p.u., the total cost under the CPND model is $112,926.31, which corresponds to a 45.73% reduction relative to the cyber-physical AD model. This reduced total cost stems from the ability of the CPND model to determine the optimal allocation of protection resources for cyber links and physical lines, and to optimise control centre locations according to different degrees of cyber-physical interdependence, thereby enhancing the cyber-physical resilience of CPPSs. Also, the optimal network defence strategies vary with the degree of cyber-physical interdependence ϖ. For instance, when $\varpi = 0.3$ p.u., physical lines 23, 28, and 31 are selected for protection, whereas for $\varpi = 0.7$ p.u., physical lines 7, 11, and 17 are protected as priorities. Note that protected physical lines and cyber links are dynamically adjusted. This suggests the adaptability of the CPND model in determining proactive defence strategies under varying degrees of cyber-physical interdependence. Overall, the proposed CPND model provides an adaptable and proactive defence strategy considering cyber-physical interdependence, ensuring cost-effective operation of CPPSs.

TABLE IV.
SIMULATION RESULTS UNDER DIFFERENT DEGREES OF CYBER-PHYSICAL INTERDEPENDENCE

Cyber-physical interdependence degree (ϖ)	Proposed CPND model				Cyber-physical AD model	Total cost reduction ratio (%)
	Protected physical lines	Protected cyber links	Control centre location	Total cost ($)	Total cost ($)	
0.1	23*, 28, 31	1, 11, 23*	7, 22	91581.86	122124.46	25.01%
0.3	23*, 28, 31	7, 23*, 28	1, 7	98697.50	122546.62	19.46%
0.5	23*, 28, 31	23*, 29, 31	7, 20	103869.28	132707.48	21.73%
0.7	7, 11, 17	11, 29, 31	7, 21	104515.23	162860.02	35.83%
0.9	7, 11, 36	2, 11, 12	18, 23	108797.97	193012.57	43.63%
1.0	7, 11, 36	2, 11, 12	21, 23	112926.31	208088.84	45.73%

† "*" denotes the cyber-physical coupled link.

3) Allocation of Control Centres: This case study investigates the impact of control centre allocation on the total operational cost of CPPSs. The protection resource for physical lines is set to 3 (i.e., $H^P = 3$), and the protection resource for cyber links is set to 4 (i.e., $H^C = 4$). In addition, the coupled protection resource is H^O=2. Similarly, the attack budget is set to $K^P = 3$ and $K^C = 4$, respectively. The coordinated attack budget is assumed to be 2 (i.e., $K^O = 2$). The degree of cyber-physical interdependence ϖ is set to 1.0 p.u.

It can be observed from Table V that the control centre allocation can significantly affect the total cost of CPPSs. For example, when the control centre resource is only 1 (i.e., $H^G = 1$), the total cost is $104,794.94 if the control centre is located at cyber node 3, while it is $111,540.48 when located at cyber node 14. This is because the location of the control centre may re-distribute the information flow in the cyber network and subsequently affect the interdependent operation of cyber-physical networks. Furthermore, it is observed that the optimal location for the control centre is allocated at cyber node 21, as determined by the proposed CPND model, with the total cost being reduced to $104,594.94. Similarly, when the control centre resource H^G increases to 2, the proposed CPND model allocates optimal locations for two control centres at cyber nodes 7 and 18, respectively. The corresponding total cost is $91,083.77, which is the lowest among other fixed control centre allocations. This implies that the proposed CPND model can provide a cost-effective strategy for control centre allocation.

TABLE V.
COMPARATIVE RESULTS OF CONTROL CENTRE ALLOCATION

Control centre resource	Fixed allocation		Optimal allocation	
	Location	Total cost ($)	Location	Total cost ($)
1	(3)	104794.94	(21)	104594.94
	(5)	110108.40		
	(14)	111540.48		
2	(7, 23)	103969.27	(7, 18)	91083.77
	(4, 17)	104644.94		
	(5, 12)	104565.23		
	(10, 15)	104844.94		

† "*" denotes the cyber-physical coupled link.

4) Proactive Defence under Various Protection Resources: To analyse the impact of the protection resources available for

proactive defence strategies, the protection resources are varied from 2 to 7, where $H^P = H^C$. To fully utilise the protection resources, the numbers of protected physical lines and cyber links are manually set to the maximum values of available protection resources (i.e. H^P and H^C). The protection costs for each physical line and cyber link are adjusted to \$2,000 and \$1,000, respectively, and the control centre allocation cost is adjusted to \$500 per unit. The attack budget is 4 (i.e., $K^P = 4$ and $K^C = 4$). The coordinated attack budget is $K^O = 2$, and the control centre resource is $H^G = 2$. Meanwhile, the coupled protection resource is $H^O = 2$. The degree of cyber-physical interdependence ϖ is 1.0 p.u. Table VI and Fig. 3 show the simulation results.

Fig. 3 illustrates the trend in total cost under different protection resources. It suggests that a protection resource of 6 provides the lowest total cost in this case study, offering a useful guidance to select an appropriate protection resource level. As shown in Fig. 3, as the protection resource increases, the total cost decreases, which consists of proactive defence, load loss, and power generation costs. More specifically, the total cost decreases from \$135,581.71 at the protection resource of 2 to \$96,156.85 at the protection resource of 6, indicating that increasing protection resources can effectively mitigate the impact of coordinated attacks within a certain range. This decrease occurs because higher-risk parts of cyber-physical networks are proactively protected as the protection resource increases. As shown in Table VI, when the protection resource is 4, physical line 28 is attacked. However, if the protection resource is increased to 5, the attacked physical line 28 will be protected, forcing the coordinated attacks to choose lower-risk lines. It is also observed that the total cost slightly increases when the protection resource further increases from 6 to 7. This is because the additional protection actions introduce extra proactive defence costs, while the additional protected components may bring limited marginal benefits in reducing load loss and power generation cost. Therefore, excessive protection resources may not necessarily lead to further cost reduction. These findings indicate that the proposed CPND model can provide adaptable and proactive defence strategies based on appropriate network protection resources.

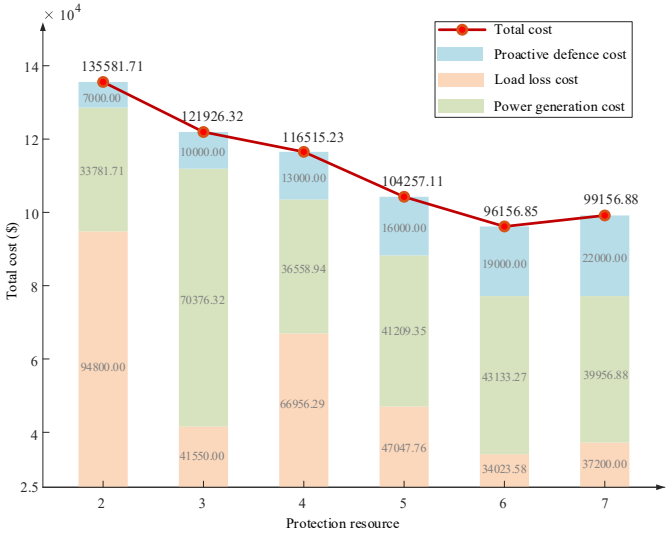

Fig. 3. Total cost under different protection resources.

TABLE VI.
SIMULATION RESULTS UNDER DIFFERENT NETWORK PROTECTION RESOURCES

Protection resource	Protected physical lines	Protected cyber links	Control centre locations	Attacked physical lines	Attacked cyber links
2	11, 36	11, 13	21, 23	15, 17, 34, 35	28, 32, 33, 38
3	7, 28, 36	2, 11, 12	18, 23	21*, 22*, 34, 35	21*, 22*, 31, 38
4	7, 11, 15, 22*	2, 11, 22*, 29	7, 18	6, 25*, 26*, 28	3, 25*, 26*, 28
5	7, 15, 28, 29, 31	1, 2, 11, 12, 38	18, 23	21*, 22*, 36, 37	21*, 22*, 32, 33
6	11, 17, 23*, 28, 30, 37	1, 2, 11, 12, 23*, 38	18, 23	14, 16, 20*, 21*	7, 20*, 21*, 28
7	10, 17, 21, 23*, 28, 29, 31	1, 2, 11, 12, 21, 23*, 38	18, 23	7, 14, 15, 16	4, 7, 15, 16

† "*" denotes the cyber-physical coupled link.

C. Large-Scale System Performance and Algorithm Comparison

In this section, additional comparative analyses on the IEEE RTS-96 system are performed to demonstrate the advantages of the proposed approach. The top 20 physical lines in terms of capacity are selected as the cyber-physical coupled links. The attack budget is set to 2 (i.e., $K^P = 2$ and $K^C = 2$), and the coordinated attack budget is K^O=1. The control centre resource is 3 (i.e., $H^G = 3$), and the degree of cyber-physical interdependence ϖ is set to 1.0 p.u. In addition, the protection resource is 4 (i.e., $H^P = 4$ and $H^C = 4$), and the coupled protection resource is $H^O = 2$.

1) Comparison with Cyber and Physical AD Models: This case study further investigates the performance of the CPND model and compares it with the cyber-physical and physical-only AD models. Table VII indicates that the total cost is \$175,689.76 in the physical-only AD model, while it increases to \$188,985.90 in the cyber-physical AD model. The increase in the total cost is due to the cyber-physical AD model incorporating cyber-physical network interdependence, which is vulnerable to coordinated attacks on both physical lines and cyber links. These coordinated attacks may cause greater operational risks, resulting in a higher total cost to mitigate attack impacts. This implies that coordinated attacks can pose higher risks to CPPSs due to cyber-physical interdependent networks. When the CPND model is employed to hedge against coordinated attacks, the total cost is reduced to \$169,807.43, and nodes 31, 59, and 59 are selected as the optimal locations for control centres. The protected physical lines are 47, 61, 80, and 104, and the protected cyber links are 1, 41, 73, and 119. In comparison, the CPND model offers a more comprehensive cyber-physical coordinated defence strategy, which is essential for securing modern CPPSs against coordinated attacks.

TABLE VII.
COMPARATIVE RESULTS ON THE IEEE RTS-96 SYSTEM

Comparative analysis	Proposed CPND model	Cyber-physical AD model	Physical-only AD model [25]
Protected physical lines	47, 61,80, 104	\	\
Protected cyber links	11, 41, 73, 119	\	\
Attacked physical lines	86, 91	54, 55	61, 65
Attacked cyber links	1, 54	53, 92	\
Control centre location	31, 55, 59	9, 38, 72	9, 38, 72
Total cost ($)	169807.43	188985.90	175689.76
Computation time (s)	3255.15	1503.83	32.35

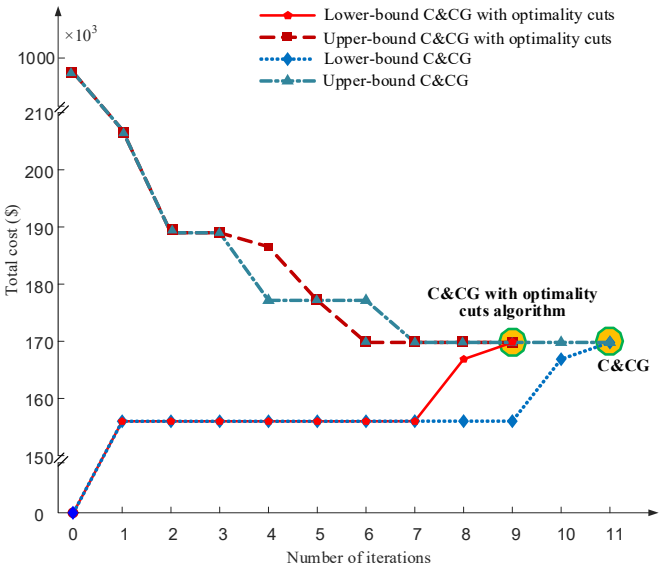

Fig. 4. Convergence comparison of the C&CG algorithms with and without optimality cuts.

2) Comparison with the C&CG Algorithm: To verify the computational efficiency of the C&CG with optimality cuts algorithm, this algorithm is compared with the traditional C&CG algorithm. As shown in Table VII, the proposed algorithm reduces the computational time to 3,255.15 seconds, demonstrating a significant improvement in solution efficiency. This improvement is mainly attributed to the optimality-cut generation mechanism, which tightens the feasible region and accelerates convergence. In comparison, the computational time based on the C&CG with optimality cuts is reduced by 20.57% compared with that of the C&CG algorithm. As illustrated in Fig. 4, the upper and lower bounds for the C&CG with optimality cuts converge within 9 iterations, whereas the C&CG algorithm requires 11 iterations to achieve convergence. These results further demonstrate that the C&CG with optimality cuts algorithm outperforms the C&CG algorithm in terms of iteration efficiency. This improvement can be attributed to the C&CG with the optimality cuts-generation mechanism, which effectively shrinks the feasible region and accelerates convergence to the optimal solution. For large-scale systems, high-performance computing platforms and machine learning-based variable reduction could be considered as future implementations to improve computational efficiency.

V. CONCLUSION

This paper develops a tri-level CPND model for CPPSs against coordinated attacks, considering the interdependence of cyber-physical networks. The proposed model enables proactive defence through the optimal allocation of protection resources, including the protection of physical lines, cyber links, and the allocation of control centres. In addition, this model accounts for the impact of cyber network failures and information loss on the operational constraints of physical network. Compared with physical-only DAD and cyber-physical AD models, the CPND model is more effective in enhancing the proactive defence strategy in both cyber and physical networks, while also being more cost-effective in mitigating against coordinated attacks. To obtain the optimal solution, a C&CG with optimality cuts algorithm is proposed, reducing the numbers of solution iterations and improving computational efficiency. Future work will extend the proposed CPND model to incorporate uncertainties into cyber-physical network defence strategies, including both multi-stage attack uncertainty and renewable energy uncertainty.

REFERENCES

[1] Y. Liu, A. Ştefanov, I. Semertzis, and P. Palensky, "GraphCCI: Critical Components Identification for Enhancing Security of Cyber-Physical Power Systems," *IEEE Transactions on Industrial Cyber-Physical Systems,* vol. 2, pp. 340-349, 2024.

[2] D. Qiu, M. Liu, R. Zhang, T. Luo, A. Griffo, and X. Zhang, "Cyber-Physical Real-Time Digital Simulation for Cybersecurity Analysis in Microgrids," *IEEE Transactions on Industrial Cyber-Physical Systems,* vol. 3, pp. 429-441, 2025.

[3] M. Liu *et al.*, "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," *IEEE Transactions on Smart Grid,* vol. 15, no. 5, pp. 4998-5030, 2024.

[4] M. Du, X. Zhang, J. Zhang, R. Zhang and J. Zhao, "Robust Resilience Enhancement Strategy Against Uncertain Cyber-Physical Coordinated Attacks Considering Power-Communication Network Interdependence," in *IEEE Transactions on Power Systems,* early access, 2026.

[5] X. Kong, Z. Lu, X. Guo, J. Zhang, and H. Li, "Resilience Evaluation of Cyber-Physical Power System Considering Cyber Attacks," *IEEE Transactions on Reliability,* vol. 73, no. 1, pp. 245-256, 2024.

[6] M. Du, X. Zhang, J. Zhang and S. Bu, "Bilevel Cyber-Induced Overloads Mechanism for False Data Injection Attacks Considering Post-Attack Economic Dispatch," in *IEEE Transactions on Information Forensics and Security*, vol. 21, pp. 2918-2932, 2026.

[7] C. Fei, J. Shen, H. Qiu, Z. Zhang, and W. Xing, "Learning Secure Control Design for Cyber-Physical Systems Under False Data Injection Attacks," *IEEE Transactions on Industrial Cyber-Physical Systems,* vol. 2, pp. 60-68, 2024.

[8] M. Ghaedi, H. Delkhosh, H. Seifi, and M. Shafie-Khah, "Two-Stage Direct and Bi-Level Indirect Coordinated Cyber-Physical Attacks Integrating Substation Outage," *IEEE Transactions on Power Systems,* vol. 40, no. 6, pp. 5057-5070, Nov. 2025.

[9] R. Zeng, X. Zhang, and R. Zhang, "Enhancing Resilience of Power Distribution Systems Under Cyber-Physical Hybrid Attacks: A Coordinated Localization and Restoration Strategy with Feeder Automation," *IEEE Transactions on Smart Grid,* early access, 2026.

[10] L. Wei, A. I. Sarwat, and W. Saad, "Risk assessment of coordinated cyber-physical attacks against power grids: A stochastic game approach," in *2016 IEEE Industry Applications Society Annual Meeting*, 2016, pp. 1-7.

[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, 2017.

[12] C. Qin, C. Zhong, B. Sun, X. Jin, and Y. Zeng, "A tri-level optimal defense method against coordinated cyber-physical attacks considering full substation topology," *Applied Energy,* vol. 339, p. 120961, 2023.

[13] D. Ma *et al.*, "Proactive Robust Hardening of Resilient Power Distribution Network: Decision-Dependent Uncertainty Modeling and Fast Solution Strategy," *IEEE Transactions on Automation Science and Engineering,* vol. 22, pp. 14953-14966, 2025.

[14] W. K. Chai, V. Kyritsis, K. V. Katsaros, and G. Pavlou, "Resilience of interdependent communication and power distribution networks against cascading failures," in *2016 IFIP Networking Conference (IFIP*

Networking) and Workshops, 2016, pp. 37-45: IEEE.
[15] M. Zeraati, Z. Aref, and M. A. Latify, "Vulnerability Analysis of Power Systems Under Physical Deliberate Attacks Considering Geographic-Cyber Interdependence of the Power System and Communication Network," *IEEE Systems Journal,* vol. 12, no. 4, pp. 3181-3190, 2018.
[16] M. Tian, Z. Dong, L. Gong, and X. Wang, "Line hardening strategies for resilient power systems considering cyber-topology interdependence," *Reliability Engineering & System Safety,* vol. 241, p. 109644, 2024.
[17] Z. Dong, M. Tian, M. Tang, J. J. I. J. o. E. P. Liang, and E. Systems, "Power generation allocation of cyber–physical power systems from a defense–attack–defense perspective," vol. 156, p. 109690, 2024.
[18] X. Li, Q. Xu, X. Lu, M. Lin, C. Chen, and X. Guan, "Distributionally Robust Coordinated Defense Strategy for Time-Sensitive Networking Enabled Cyber–Physical Power System," *IEEE Transactions on Smart Grid,* vol. 15, no. 3, pp. 3278-3287, 2024.
[19] Y. Guo, C. Guo, and J. Yang, "A tri-level optimization model for power systems defense considering cyber-physical interdependence," vol. 17, no. 7, pp. 1477-1490, 2023.
[20] S. Gharebaghi, N. R. Chaudhuri, T. He, and T. F. L. Porta, "Dynamic Modeling and Mitigation of Cascading Failures in Power Grids With Interdependent Cyber and Physical Layers," *IEEE Transactions on Smart Grid,* vol. 15, no. 3, pp. 3235-3247, 2024.
[21] M. Du, X. Zhang, G. Taylor, and V. Terzija, "Game theory-based vulnerability analysis of cyber-physical power systems under interdependent network attacks," *Cyber-Physical Energy Systems,* 2025.
[22] H. Lei, S. Huang, Y. Liu, and T. Zhang, "Robust Optimization for Microgrid Defense Resource Planning and Allocation Against Multi-Period Attacks," *IEEE Transactions on Smart Grid,* vol. 10, no. 5, pp. 5841-5850, 2019.
[23] X. Wang, Z. Li, M. Shahidehpour, and C. Jiang, "Robust Line Hardening Strategies for Improving the Resilience of Distribution Systems With Variable Renewable Resources," *IEEE Transactions on Sustainable Energy,* vol. 10, no. 1, pp. 386-395, 2019.
[24] M. Du, X. Zhang and J. M. Guerrero, "Adaptive Robust Planner-Attacker-Operator Model Against Multistage Uncertain Malicious Attacks for Power Systems With Volatile Wind Power," in *IEEE Transactions on Industrial Informatics*, vol. 22, no. 6, pp. 5378-5389, June 2026.
[25] J. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *Generation, Transmission & Distribution, IET,* vol. 4, pp. 178-190, 2010.