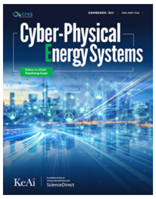
Cyber-Physical Energy Systems 1 (2025) 116–124

Contents lists available at ScienceDirect

Cyber-Physical Energy Systems

journal homepage: www.elsevier.com/locate/cpes



# Game theory-based vulnerability analysis of cyber-physical power systems under interdependent network attacks

Min Du[a], Xin Zhang[a,*], Gareth Taylor[b], Vladimir Terzija[c]

[a] School of Electrical and Electronic Engineering, University of Sheffield, Sheffield S10 2TN, United Kingdom
[b] Department of Electronic and Electrical Engineering, Brunel University of London, London UB8 3PH, United Kingdom
[c] School of Engineering, Newcastle University, Newcastle upon Tyne NE1 7RU, United Kingdom

## ARTICLE INFO

*Keywords:*
Cyber-physical power systems
Coordinated cyber-physical network attacks
Vulnerability analysis
Attack-defence game model

## ABSTRACT

Cyber-physical power systems (CPPSs) have gained widespread adoption worldwide, driven by the growing need for enhanced power system security. The convergence of digital technologies with traditional power systems has facilitated significant enhancements in system monitoring, control, and power transmission. However, due to the interdependence of cyber-physical networks, CPPSs significantly increase their vulnerability to security risks under coordinated cyber-physical network attacks that can simultaneously compromise the transmission lines and communication links. In this paper, we develop a bilevel game theory-based attack-defence (GTAD) model that considers both functional and topological interdependence between the cyber and physical networks to assess the vulnerability of CPPSs under coordinated cyber-physical network attacks. Specifically, the upper-level problem aims to maximise load loss in the power system through coordinated cyber-physical network attacks; the lower-level problem aims to minimise load loss to the power system through corrective generation dispatch actions. Then, a strong duality-based method and a big-*M* method are employed to reformulate the GTAD model into a single-level mixed-integer linear programming (MILP) model. Finally, case studies are conducted on the IEEE RTS 24-bus system and a practical 36-zone Great Britain power transmission system to demonstrate the validity and rationality of our proposed GTAD method in analysing interdependent network vulnerability and more coordinated cyber-physical network attack strategies.

## 1. Introduction

IN recent years, modern power systems have evolved into cyber-physical power systems (CPPSs) that exhibit the deep interdependence between the cyber and physical networks in terms of functionality and topology [1]. This evolution has significantly enhanced the operational flexibility, monitoring accuracy, and control efficiency of electric power transmission [2]. However, the increasing interdependence between the cyber and physical networks also makes CPPSs more vulnerable to various network attacks [3–5].

These network attacks typically include cyberattacks and human-made physical attacks. Such attacks mainly disrupt the networks of CPPSs, which can pose substantial threats to the cyber-physical system security [6–8]. Historical incidents also provide supporting evidence of such cyber or physical threats. For example, in December 2015, a cyberattack damaged the Ukrainian power system, resulting in a severe power service disruption and affecting over 220000 customers for several hours [9]. In September 2023, a deliberate physical attack on transmission lines in Nigeria led to the loss of over 90 % of Nigeria's electricity supply [10]. These events strongly illustrate that load loss becomes a significant consequence of cyber and physical attacks. Thus, it is crucial to analyse the vulnerability of CPPSs under cyber and physical attacks, in order to better assess the load loss impacts and determine resilience enhancement strategies.

Particularly in CPPSs, coordinated cyber-physical attacks which combine both cyber and physical attacks have attracted increasing attention, as such attack coordination is expected to cause more severe impacts on system security than either single cyber or physical attack due to the cyber-physical interdependence. Most existing studies have focused on analysing the vulnerability of CPPSs under coordinated cyber-physical attacks using multi-level and multi-stage optimisation programs. For example, the authors proposed a bilevel optimisation model in [11] to analyse the impact of coordinated cyber-physical attacks on power systems, aiming to maximise total power flow deviations across transmission lines, subject to a limited attack budget that includes both transmission line disruptions and load measurement manipulations. In [12], two typical coordinated cyber-physical attacks were introduced and analysed within a bilevel optimisation framework, aiming to capture the adversarial interaction between the attacker maximising load loss and the system operator minimising it. Recently, a two-stage direct attack and bilevel indirect coordinated attack model was developed in [13] to assess the potential risk of CPPSs under com-

[*] Corresponding author.
*E-mail address:* xin.zhang1@sheffield.ac.uk (X. Zhang).

https://doi.org/10.1016/j.cpes.2025.08.001
Received 26 June 2025; Received in revised form 7 August 2025; Accepted 18 August 2025

## Nomenclature

| | |
|---|---|
| *Indices and Sets* | |
| $b$ | Index of power nodes. |
| $\mathcal{v}$ | Index of communication nodes. |
| $X_{ij}$ | Reactance of transmission line $(i,j)$. |
| $(i,j)$ | Index of transmission lines, where $i$ and $j$ denote the sending and receiving power nodes, respectively. |
| $(v,w)$ | Index of communication links, where $v$ and $w$ denote the sending and receiving communication nodes, respectively. |
| **KP** | Power node- generation unit incidence matrix. |
| **KD** | Power node-load incidence matrix. |
| **KL** | Power node-transmission line incidence matrix. |
| $\boldsymbol{\mathcal{V}}/\boldsymbol{B}/\boldsymbol{\mathcal{V}}_0$ | Set of communication nodes/ power nodes/ control centres. |
| $\boldsymbol{\mathcal{L}}/\boldsymbol{L}$ | Set of communication links/transmission lines. |
| $\boldsymbol{\ell}$ | Set of coupled transmission lines-communication links. |
| $\boldsymbol{\mathcal{C}}$ | Set of attacked coupled lines. |
| *Parameters* | |
| $\mathcal{H}_c$ | Budget of coordinated cyber-physical network attacks on communication links. |
| $\mathcal{H}_p$ | Budget of coordinated cyber-physical network attacks on transmission lines. |
| $\mathcal{H}_o$ | Budget of coordinated cyber-physical network attacks on coupled lines. |
| $\alpha$ | Functional interdependence coefficient. |
| card($\boldsymbol{\mathcal{V}}$) | Total number of communication nodes. |
| $P_b^{\rm Dmax}$ | Load demand at power node $b$. |
| $F_{ij}^{\rm Lmax}$ | Power flow capacity of transmission line $(i,j)$. |
| $\theta_b^{\rm max}$ | Voltage phase angle limit at power node $b$. |
| *Variables* | |
| $C_{\mathcal{v}}^G$ | Information output at control centre $\mathcal{v}$. |
| $\Delta C_{\mathcal{v}}^D$ | Communication data loss at communication node $\mathcal{v}$. |
| $\mathcal{L}_{vw}^{\rm L}$ | Information flow of communication link $(v,w)$. |
| $P_b^{\rm G}$ | Generation unit output at power node $b$. |
| $\Delta P_b^{\rm D}$ | Load loss at power node $b$. |
| $F_{ij}^{\rm L}$ | Power flow of transmission line $(i,j)$. |
| $\theta_b$ | Voltage phase angle at power node $b$. |
| $\Delta \boldsymbol{P}^{\rm D}$ | Load loss vector which consists of load loss $\Delta P_b^{\rm D}$ at each power node. |
| $\boldsymbol{P}^{\rm G}$ | Generation unit output vector which consists of generation unit output $P_b^{\rm G}$ at each power node. |
| $\boldsymbol{F}^{\rm L}$ | Power flow vector which consists of power flow $F_{ij}^{\rm L}$ of transmission line $(i,j)$. |
| $c_{vw}$ | Status of communication link $(v,w)$, where it is equal to 0 if this link attacked, being 1 otherwise. |
| $p_{ij}$ | Status of transmission line $(i,j)$, where it is equal to 0 if this line attacked, being 1 otherwise. |

bined false data injection and substation outage attacks. In practice, a sophisticated attacker may exploit both cyber-physical attack coordination and the combined use of availability and integrity attacks within the field of cyberattacks. Thus, the authors in [14] studied the combined impact of physical attacks and Denial-of-Service (DoS) attacks, which were considered more realistic and destructive attacks in CPPS environments. Meanwhile, the authors in [15] also pointed out that DoS attacks can severely degrade the performance of distributed control schemes in microgrids due to the interdependence of the cyber and physical networks.

However, previous studies have primarily focused on the operational problem of the physical network, with limited attention given to the deep interdependence between cyber and physical networks, particularly their functional and topological interdependence of the networks. As a result, the potential risk posed to CPPSs under interdependent network attacks has not been adequately explored. Such attacks can disrupt both transmission lines and communication links in interdependent cyber-physical networks, which are typically implemented through coordinated cyber-physical network attacks. This coordinated mechanism leverages the interdependent infrastructure to maximise system disruption and forms the analytical foundation of the proposed model. In fact, the impact of physical attacks may be further amplified due to the topological interdependence between the cyber and physical networks, which often share parts of the physical infrastructure. For example, in power transmission networks of 110 kV and above, optical fibre composite overhead ground wire (OPGW) cables are commonly used in China, India, and the United Kingdom, among others, as communication links. These communication links are co-installed with transmission lines on the same transmission towers, sharing the same transmission routes to improve communication stability and security [16]. However, if a transmission tower is physically damaged, both the transmission lines and their associated communication links can be simultaneously disrupted. A notable example occurred in 2008, when a severe ice storm in southern China caused widespread failures of transmission lines and their associated OPGW cables, ultimately leading to a large-scale power system collapse. This event has been recognised as a representative example of coordinated failure between the cyber and physical networks [17]. To assess such interdependent cyber-physical network risks, the authors in [18] proposed a bilevel optimisation model to analyse the vulnerability of CPPSs under physical attacks considering the geographic-cyber interdependence of cyber-physical networks. Then, the authors in [19] proposed a tri-level line hardening model for improving the resilience of CPPSs considering cyber-topological interdependence. However, these efforts still ignored the functional interdependence between the cyber and physical networks, where cyber and physical networks interdependently rely on each other to support control and operation of CPPSs.

In CPPSs, the cyber network acquires real-time operational data through sensors to support system monitoring and control, which leads to a strong functional interdependence between the cyber and physical networks. For example, power nodes supply power to their associated communication nodes, while these communication nodes, in turn, perform monitoring and control functions for corresponding components in the physical network. This bidirectional cyber-physical interdependence enhances operational efficiency but also increases the vulnerability of CPPSs to coordinated cyber-physical network attacks. To capture this interaction, the authors in [20] proposed a cyber-constrained optimal power flow model based on energy-supply relationships. Then, the authors in [21,22] modelled the interdependent mechanism of cyber-physical networks in tri-level defence models. However, these studies [20–22] primarily modelled the functional interdependence between the cyber and physical networks through power supply relationships, rather than capturing the detailed functionalities such as information exchange, monitoring, and control enabled by the interdependent cyber-physical networks.

In practice, CPPSs are typically equipped with backup battery systems to ensure uninterrupted power supply for communication nodes, even during blackouts. Thus, functional interdependence based on power supply does not accurately reflect the practical operational behaviour of CPPSs. In contrast, functional interdependence is more accurately characterised by the reliability of information exchange between the cyber and physical networks to monitor or control the components in the physical network. More specifically, communication node failures or packet losses in the cyber network can impair the monitoring or control capabilities over components (e.g., generation unit output) in the physical network. Since the normal functionality of these components relies on control signals transmitted from the control centre by communication nodes, it is more appropriate to model functional interdependence in terms of control signal availability, rather than solely the power supply.

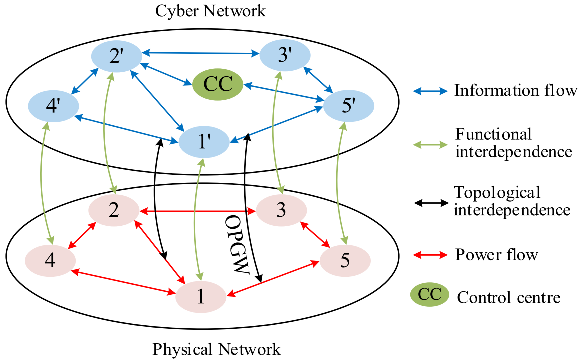


**Fig. 1.** Interdependent cyber-physical networks in CPPSs.

Accordingly, we propose a novel bilevel model based on game theory that incorporates both functional and topological interdependence between the cyber and physical networks of CPPSs in order to analyse their vulnerability to coordinated cyber-physical network attacks. Specifically, the attacker at the upper-level aims to maximise the load loss through coordinated cyber-physical network attacks, while the defender at the lower-level aims to minimise the load loss by corrective generation dispatch actions. The proposed model uncovers the potential vulnerabilities and risks of CPPSs under coordinated cyber-physical network attacks considering the functional and topological interdependence between the cyber and physical networks, thereby providing theoretical insights for ensuring the operational security of CPPSs. The main contributions are summarised as follows:

(1) We explicitly model both the functional and topological interdependence between cyber and physical networks in CPPSs by introducing mathematically defined interdependent constraints. Through this formulation, we demonstrate that such interdependence amplifies system vulnerability under coordinated cyber-physical network attacks, revealing hidden risks that are overlooked in conventional models.
(2) We propose a novel bilevel game-theoretic attack-defence (GTAD) model that quantifies the vulnerability of CPPSs under coordinated cyber-physical network attacks. The model captures the interdependence of the cyber and physical networks, particularly the impact of disrupted communication links on component control capabilities in physical networks, thereby identifying critical vulnerabilities beyond the scope of existing approaches.
(3) To ensure computational feasibility, we reformulate the proposed GTAD model into an equivalent single-level mixed-integer linear programming (MILP) problem using strong duality theory and the big-$M$ method. Extensive case studies on the IEEE RTS 24-bus system and the practical 36-zone Great Britain power transmission system demonstrate the effectiveness, scalability, and superiority of the proposed approach.

The remainder of this paper is structured as follows. Section 2 intro duces interdependent cyber-physical networks of CPPSs. Section 3 presents the proposed GTAD model framework along with its corresponding mathematical formulation. Section 4 reformulates the proposed model into a single-level MILP problem. Section 5 conducts case studies based on the IEEE RTS 24-bus system and the practical 36-zone Great Britain power transmission system. Section 6 summarises the conclusions and outlines directions for future research.

## 2. Interdependent cyber-physical networks

As shown in Fig. 1, a typical CPPS consists of interdependent cyber and physical networks, which are characterised by both functional and topological interdependence. Specifically, the cyber network provides essential control signals and system observability, while relying on a continuous power supply from the physical network for operational continuity. Moreover, the cyber and physical networks often share physical routes or infrastructure, such as OPGW cables that are co-installed on transmission towers, which are considered as coupled lines. This is due to the fact that only the communication links that share physical infrastructure with transmission lines (e.g., mounted on the same towers) are subject to identical attack states. For simplicity and without loss of generality, we assume that the cyber network and the physical network share the same topology, with a one-to-one correspondence between communication nodes and power nodes. This simplification is widely adopted in recent literature (e.g., [19–22]) as a baseline modelling assumption to facilitate analysis of interdependent network behaviours in CPPSs.

### 2.1. Functional interdependence of cyber-physical networks

In CPPSs, the cyber network and the physical network are functionally interdependent. More specifically, measurements from electrical components in the physical network are gathered by local communication nodes and forwarded through communication links to the control centre. Based on these inputs, the control centre issues control commands to communication nodes, which then transmit them back to actuators in the physical network. If a communication link is disrupted, the observability and controllability of components in the physical network may be compromised, potentially leading to the inability of monitoring and control systems to respond to contingencies.

Furthermore, the cyber network also relies on a stable and continuous power supply from the physical network to sustain its operational functions. For example, base stations, routers, and relay devices embedded in cyber network require reliable power supply from the physical network. Any disconnection or blackout in the physical network may cause the cyber equipment to shut down, further disrupting the information transmission of monitoring and control signals.

### 2.2. Topological interdependence of cyber-physical networks

Topological interdependence primarily captures the spatial and structural co-location between the cyber and physical networks. A prominent example is the use of OPGW cables, which integrate communication fibres within the shield wires installed on transmission towers, as shown in Fig. 2. While this architecture can effectively reduce infrastructure cost and improve communication coverage, it also introduces potential security risks to CPPSs. Specifically, a deliberate physical attack on a transmission tower or line may simultaneously disrupt both power delivery and communication connectivity. This topological interdependence of cyber-physical networks causes failures in one system component to inherently affect the other. Accordingly, if a transmission line is disrupted by deliberate attacks, the communication link embedded within the associated tower will also become unavailable.

## 3. Game theory-based attack-defence model

This section presents the GTAD model for evaluating the vulnerability of CPPSs under coordinated cyber-physical network attacks. Section 3.1 outlines the overall framework of the GTAD model, while Section 3.2 presents its mathematical formulation in detail.

### 3.1. Framework of the proposed GTAD model

The proposed GTAD model is formulated as a game interaction between an attacker and a defender in terms of load loss, as illustrated in Fig. 3. This model aims to analyse the vulnerability of CPPSs under interdependent network attacks. Such attacks are typically implemented as coordinated cyber-physical network attacks. Given that the cyber and physical networks are interdependent, and that transmission

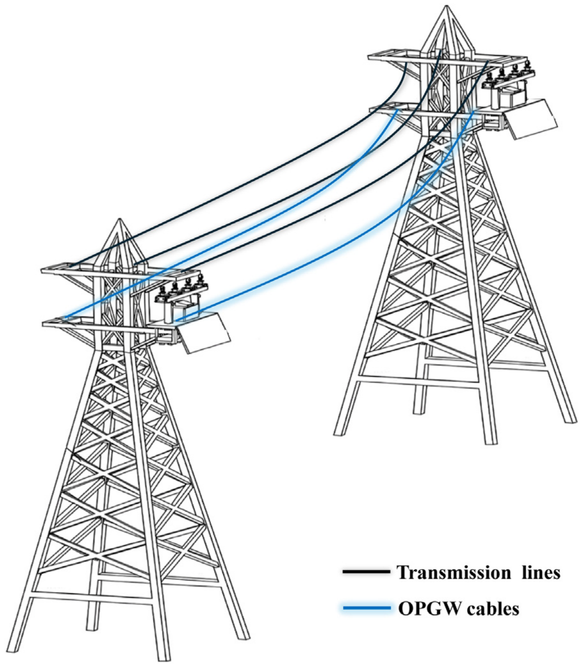


**Fig. 2.** Transmission lines and OPGW cables on the power tower.

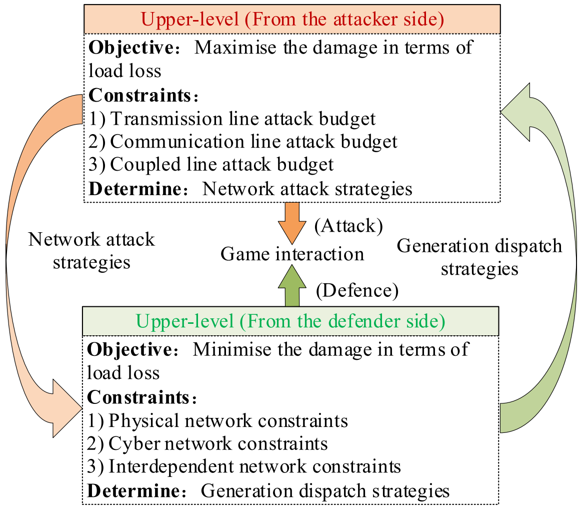

Upper-level (From the attacker side)
Objective: Maximise the damage in terms of load loss
Constraints:
1) Transmission line attack budget
2) Communication line attack budget
3) Coupled line attack budget
Determine: Network attack strategies
(Attack)
Network attack strategies
Game interaction
Generation dispatch strategies
(Defence)
Upper-level (From the defender side)
Objective: Minimise the damage in terms of load loss
Constraints:
1) Physical network constraints
2) Cyber network constraints
3) Interdependent network constraints
Determine: Generation dispatch strategies

**Fig. 3.** Overall framework of the proposed GTAD model.

lines are typically more vulnerable than other components in power systems, this paper focuses on coordinated cyber-physical network attacks targeting transmission lines and communication links. To this end, the bilevel game theory-based optimisation framework is detailed as follows:

- At the upper level, the attacker aims to maximise the load loss of the power system by launching coordinated cyber-physical network attacks on both transmission lines and communication links. The attack strategy can be achieved by leveraging both the topological and functional interdependence between cyber and physical networks in CPPSs. Here, topological interdependence captures the physical co-location of transmission lines and communication links; functional interdependence refers to the control dependency of generation units on their corresponding communication nodes.
- At the lower level, the defender reacts to such a disruption by corrective actions to minimise load loss and ensure the operational security of the power system. The corrective actions include generation unit redispatch and load shedding, all subject to the constraints of the physical network. The defender also considers the reduced controllability of components in the physical network due to the communication data loss at communication nodes.

This framework employs a game-theoretic perspective to capture the strategic interaction between the attacker and the defender, enabling the identification of optimal attack and generation dispatch strategies. In the proposed GTAD model, the DC power flow is adopted to represent the characteristics of the power system in the physical network. The DC power flow model is widely used in vulnerability assessment models due to its linearity [18]. Note that the proposed GTAD model extends the traditional model introduced by [23], which does not consider the impact of the communication network on generation dispatch decisions.

### 3.2. Game theory-based attack-defence model

Based on the above description of the framework for the proposed GTAD model, the corresponding mathematical formulation of this model is given as follows:

$$\max_{c_{vw},p_{ij}} \sum_{b\in \boldsymbol{B}} \Delta P_b^{\mathrm{D}} \tag{1}$$

$$\sum_{(v,w)\in \boldsymbol{\mathcal{L}}} \left(1-c_{vw}\right) \le \mathcal{H}_c,\ \forall (v,w)\in \boldsymbol{\mathcal{L}} \tag{2}$$

$$\sum_{(i,j)\in \boldsymbol{L}} \left(1-p_{ij}\right) \le \mathcal{H}_p,\ \forall (i,j)\in \boldsymbol{L} \tag{3}$$

$$\boldsymbol{\mathcal{C}} = \left\{ \begin{array}{l} \sum\limits_{(i,j)\in \boldsymbol{\ell}} \left(1-p_{ij}\right) \le \mathcal{H}_o \\ p_{ij} = c_{vw},\ \forall (i,j)\in \boldsymbol{\ell} \\ \forall (v,w)\in \boldsymbol{\mathcal{L}},\ \forall \boldsymbol{\ell}\in \boldsymbol{L} \end{array} \right\} \tag{4}$$

where the objective function (1) is to maximise the damage to the CPPSs under coordinated cyber-physical network attacks in terms of load loss. This represents the impact of coordinated cyber-physical network attacks disrupting both transmission lines and communication links. Here, constraint (2) limits the number of communication links that can be attacked by the attacker. Constraint (3) ensures that the total number of attacked transmission lines does not exceed the specified attack budget. Constraint (4) models the topological interdependence between the cyber and physical networks, which also limits the number of attacked coupled lines. Here, coupled lines refer to transmission lines that are co-located with communication links on the same tower. In our work, topological interdependence refers to the physical co-location of communication links and transmission lines, where damage to one component (i.e., a transmission line) can simultaneously disable its associated communication link. Thus, for the coupled lines, the state of the transmission line is consistent with that of the corresponding communication link.

$$\min_{\left\{P_b^{\mathrm{G}},\Delta P_b^{\mathrm{D}},F_{ij}^{\mathrm{L}},\theta_b,C_v^G,\Delta C_v^D,\mathcal{L}_{vw}^{\mathrm{L}}\right\}} \sum_{b\in \boldsymbol{B}} \Delta P_b^{\mathrm{D}} \tag{5}$$

$$\sum_{v\in \boldsymbol{\mathcal{V}}_0} C_v^G - \sum_{w\in \boldsymbol{\mathcal{L}}_v(v,\cdot)} \mathcal{L}_{vw}^{\mathrm{L}} + \sum_{w\in \boldsymbol{\mathcal{L}}_v(\cdot,v)} \mathcal{L}_{vw}^{\mathrm{L}} = \left(1-\Delta C_v^D\right)\ \forall v\in \boldsymbol{\mathcal{V}}, \forall (v,w)\in \boldsymbol{\mathcal{L}} \tag{6}$$

$$0 \le C_v^G \le \mathrm{card}(\boldsymbol{\mathcal{V}}), \forall v\in \boldsymbol{\mathcal{V}}_0 \tag{7}$$

$$0 \le \Delta C_v^D \le 1,\ \forall v\in \boldsymbol{\mathcal{V}} \tag{8}$$

$$-c_{vw}\mathrm{card}(\boldsymbol{\mathcal{V}}) \le \mathcal{L}_{vw}^{\mathrm{L}} \le c_{vw}\mathrm{card}(\boldsymbol{\mathcal{V}}), \forall (v,w)\in \boldsymbol{\mathcal{L}} \tag{9}$$

$$\mathbf{KP} \cdot \boldsymbol{P}^{\mathrm{G}} - \mathbf{KL} \cdot \boldsymbol{F}^{\mathrm{L}} = \mathbf{KD} \cdot \left(\boldsymbol{P}^{\mathrm{Dmax}} - \Delta \boldsymbol{P}^{\mathrm{D}}\right) \tag{10}$$

$$F_{ij}^{\mathrm{L}} = p_{ij} \frac{\theta_i - \theta_j}{X_{ij}}, \ \forall (i,j) \in \boldsymbol{L} \tag{11}$$

$$0 \le P_b^{\mathrm{G}} \le \left(1 - \alpha \Delta C_{\mathscr{v}}^{D}\right) P_b^{\mathrm{Gmax}}, \ \forall b \in \boldsymbol{B}, \forall \mathscr{v} \in \boldsymbol{\mathcal{V}} \tag{12}$$

$$0 \le \Delta P_b^{\mathrm{D}} \le P_b^{\mathrm{Dmax}}, \ \forall b \in \boldsymbol{B} \tag{13}$$

$$-F_{ij}^{\mathrm{Lmax}} \le F_{ij}^{\mathrm{L}} \le F_{ij}^{\mathrm{Lmax}}, \ \forall (i,j) \in \boldsymbol{L} \tag{14}$$

$$-\theta_b^{\max} \le \theta_b \le \theta_b^{\max}, \ \forall b \in \boldsymbol{B} \tag{15}$$

where the objective function (5) is to minimise load loss by taking corrective actions to ensure the operational security of the CPPS under coordinated cyber-physical network attacks. For the constraints of the cyber network, constraint (6) ensures the balance of the information flow at each communication node $v$, which includes the unserved communication demand due to cyber disruptions. Constraint (7) limits the information capacity generated by each control centre $\mathscr{v}$. Constraint (8) limits the communication data loss at each communication node $\mathscr{v}$, which can reflect its degree of disconnection from the corresponding component in the physical network. Note that each communication node is set to a communication demand of 1 p.u. Constraint (9) limits the information flow of communication link $(v, w)$, which integrates the attack decision $c_{vw}$ on communication link $(v, w)$. For the constraints of physical networks, constraint (10) is a power flow balance constraint. Constraint (11) calculates the power flow of transmission line $(i, j)$, which integrates the attack decision $p_{ij}$ on transmission line $(i, j)$. Constraint (12) models the functional interdependence between cyber and physical networks. If the communication node is partially or fully disconnected from the corresponding generation unit, the associated generation unit output capacity is proportionally reduced according to the fraction of unserved communication demand. This indicates that the communication data loss at communication nodes will degrade the control capabilities of the system operator on the corresponding generation unit outputs, thereby amplifying the effects of coordinated cyber-physical network attacks. In constraint (12), $\alpha$ denotes the functional interdependence coefficient, which quantifies how the control capacity of generation unit output is affected by the communication data loss of its associated communication node. Note that a higher value of $\alpha$ indicates stronger functional interdependence between the cyber and physical networks. Constraint (13) limits the load loss at each power node. Constraint (14) limits the power flow on transmission line $(i, j)$. Constraint (15) restricts the voltage phase angle of each power node.

## 4. Solution methodology

To facilitate the solution, this section transforms the proposed GTAD model into a MILP problem by applying the strong duality theory and the big-$M$ method. For simplicity and without loss of generality, the GTAD model can be expressed in the following matrix form.

$$\max_{\boldsymbol{x}} \ \ \boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} \tag{16}$$

$$\text{s.t. } \boldsymbol{C x} \le \boldsymbol{b}, \ \boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}\} \tag{17}$$

$$\min_{\boldsymbol{x}} \ \boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} \tag{18}$$

$$\text{s.t. } \boldsymbol{D y} + \boldsymbol{E x} \le \boldsymbol{d} \tag{19}$$

$$\boldsymbol{y} \ge \mathbf{0} \tag{20}$$

where the objective function (16) corresponds to the above objective function (1). Constraint (17) corresponds to constraints (2)–(4). Here, vector $\boldsymbol{x}$ refers to binary attack decision variables, i.e., $c_{vw}$ and $p_{ij}$; vector $\boldsymbol{y}$ denotes generation dispatch decision variables, i.e., $C_{\mathscr{v}}^{G}$, $\Delta C_{\mathscr{v}}^{D}$, $\mathcal{L}_{vw}^{\mathrm{L}}$, $P_b^{\mathrm{G}}$, $\Delta P_b^{\mathrm{D}}$, $F_{ij}^{\mathrm{L}}$, and $\theta_b$. The objective function (18) corresponds to the above objective function (5). Constraints (19)–(20) correspond to constraints (6)–(15). Vectors $\boldsymbol{C}$ and $\boldsymbol{b}$ correspond to the coefficient and constant matrices of constraints (2)–(4); vectors $\boldsymbol{D}$, $\boldsymbol{E}$, and $\boldsymbol{d}$ correspond to the coefficient and constant matrices of constraints (6)–(15).

The compact form of the lower-level problem is described as:

$$\min_{\boldsymbol{y}} \ \boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} \tag{21}$$

$$\text{s.t. } \boldsymbol{D y} \le \boldsymbol{d} - \boldsymbol{E x}, \ (\lambda) \tag{22}$$

$$\boldsymbol{y} \ge \mathbf{0} \tag{23}$$

where $\lambda$ denotes the dual variable vector associated with constraint (22). Since the lower-level model is a linear program with convex constraints and a continuous objective function that satisfies strong duality, it can be replaced with its equivalent dual constraints. Thus, its dual problem can be formulated as:

$$\max_{\boldsymbol{y}} \ \lambda^{\mathrm{T}}(\boldsymbol{d} - \boldsymbol{E x}) \tag{24}$$

$$\text{s.t. } \boldsymbol{D}^{\mathrm{T}} \lambda \le \boldsymbol{A} \tag{25}$$

$$\lambda \le \mathbf{0} \tag{26}$$

The strong duality condition has:

$$\boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} = \lambda^{\mathrm{T}}(\boldsymbol{d} - \boldsymbol{E x}) \tag{27}$$

Thus, the equivalent single-level problem can be formulated as:

$$\min_{\boldsymbol{x},\boldsymbol{y}} \ \boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} \tag{28}$$

$$\text{s.t. } \boldsymbol{C x} \le \boldsymbol{b}, \ \boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}\} \tag{29}$$

$$\boldsymbol{D y} \le \boldsymbol{d} - \boldsymbol{E x} \tag{30}$$

$$\boldsymbol{y} \ge \mathbf{0} \tag{31}$$

$$\boldsymbol{D}^{\mathrm{T}} \lambda \le \boldsymbol{A} \tag{32}$$

$$\boldsymbol{A}^{\mathrm{T}} \boldsymbol{y} = \lambda^{\mathrm{T}}(\boldsymbol{d} - \boldsymbol{E x}) \tag{33}$$

$$\lambda \le \mathbf{0} \tag{34}$$

In addition, we can observe that a nonlinear term appears in (33), which involves the multiplication of the continuous dual variable vector $\lambda$ and the binary attack decision variable vector $\boldsymbol{x}$. Thus, this nonlinear term can be linearised using the big-$M$ method, which is detailed as follows:

$$\boldsymbol{t} = \lambda - \boldsymbol{h} \tag{35}$$

$$-M\boldsymbol{x} \le \boldsymbol{t} \le M\boldsymbol{x} \tag{36}$$

$$-M(\mathbf{1} - \boldsymbol{x}) \le \boldsymbol{h} \le M(\mathbf{1} - \boldsymbol{x}) \tag{37}$$

where $\boldsymbol{t}$ and $\boldsymbol{h}$ are auxiliary variable vectors. Ultimately, our proposed model is reformulated as a tractable single-level MILP problem. Note that we set $M$=100000 based on empirical bounds of the relevant variables [24], ensuring constraint validity and maintaining solver performance under both the IEEE RTS 24-bus and practical 36-zone Great Britain power transmission systems.

**Table 1**

Simulation results with and without consideration of network functional and topological interdependence.

| Models | $\mathcal{H}_p$ | Attacked transmission lines | Attacked communication links | Attacked coupled lines | Load loss (MW) |
|---|---|---|---|---|---|
| Ref. [23] | 2 | 19, 23 | \ | \ | 204.21 |
| | 3 | 25, 26, 28 | \ | \ | 344.47 |
| | 4 | 7, 21, 22, 23 | \ | \ | 610.26 |
| This paper | 2 | 25, 26 | 25, 26, 28 | 25, 26 | 695.00 |
| | 3 | 11, 25, 26 | 25, 26, 28 | 25, 26 | 863.42 |
| | 4 | 11, 15, 25,26 | 25, 26, 28 | 25, 26 | 863.42 |

## 5. Numerical results

This section conducts case studies based on two test systems: a modified IEEE RTS 24-bus network and a practical 36-zone power transmission system representing the Great Britain grid. All simulations are carried out using MATLAB R2019 with CPLEX 12.4 on a personal computer with an Intel Core i7-8700 processor (3.20 GHz) and 16 GB RAM. In addition, it should be emphasised that to characterise the worst-case vulnerability of CPPSs under coordinated cyber-physical network attacks, the functional interdependence coefficient is set to $\alpha$=1.0, which represents the maximum interdependence between cyber and physical networks, fully exposing the impact of disruptions. Nevertheless, the proposed GTAD model supports the flexible adaptation of $\alpha$ to reflect time-varying or asset-specific cyber-physical network interdependence, such as control sensitivity or communication reliability. This flexibility enhances the applicability of the GTAD model in practical settings and facilitates more targeted defence strategies based on empirical vulnerability assessment.

(1) IEEE RTS 24-bus system: We first conduct case studies on the IEEE Reliability Test System (RTS) 24-bus system, which is widely adopted for analysing the vulnerability of power systems under coordinated cyber-physical network attacks. This test system comprises 24 buses, 10 generation units, 38 transmission lines, and 17 loads. The total system demand is set to 3000 MW. For more information on this system, interested readers can refer to [25]. Moreover, we assume that two control centres are deployed at communication nodes 7 and 15. The top 10 transmission lines based on their power flow capacities are assumed to be coupled lines, such as in the case of OPGW cables.

### 5.1. Vulnerability analysis of CPPSs

In this case, we analyse the vulnerability of CPPSs to coordinated cyber-physical network attacks considering the functional and topological interdependence between the cyber and physical networks. The attack budget of the communication link $\mathcal{H}_c$ is set to 3, and the attack budget of the coupled line $\mathcal{H}_o$ is set to 2. Furthermore, the functional interdependence coefficient $\alpha$ is set to 1.0. A detailed comparison between the proposed GTAD model and the traditional model developed in [23] is conducted in this case study. Table 1 shows the corresponding simulation results.

Under the same attack budget for transmission lines, the inclusion of communication link disruptions in the cyber network leads to increased load loss in all cases. For instance, when the attack budget of transmission line $\mathcal{H}_p$ is set to 3, the load loss is 863.42 MW in the proposed GTAD model, whereas it is only 344.47 MW in [23]. It can be calculated that this increase in load loss amounts to 150.65 %. In fact, this increase in load loss is due to the disruption of communication links (e.g., links 25, 26, and 28) that are critical for the operation and control of the associated components in the physical networks. Once these communication links are disrupted, the affected components become less observable or less controllable, enlarging the instability of the power system. More specifically, the failure of communication links caused by coordinated cyber-physical network attacks can directly affect the communication demand at certain communication nodes, which can further affect the generation unit output in the physical network, as shown in (12). This means that when the functional and topological interdependence between the cyber and physical networks is considered in CPPSs, the coordinated attack effects are no longer limited to physical networks but also propagate through the cyber networks. In summary, the attacker can exploit the interdependence between the cyber and physical networks to cause more significant consequences in CPPSs, and failure to consider this interdependence may lead to a significant underestimation of the potential vulnerabilities and risks posed to CPPSs under coordinated cyber-physical network attacks.

In addition, we can further observe that the difference in load loss between the proposed GTAD model and the traditional model proposed in [23] tends to decrease as the attack budget for transmission lines increases. This is because a portion of the total system load demand can be fully supplied by local generation units connected directly to the corresponding load buses in the physical network. As a result, even though more transmission lines are compromised under a higher attack budget, the marginal impact of the cyber-physical interdependence diminishes, leading to a reduced difference in load loss between the two models.

### 5.2. Impact of the attack budget

This case examines the impact of the attack budget in terms of both transmission lines and communication links. The functional interdependence coefficient $\alpha$ is set to 0.8. The load level is set at 0.8 times the total system demand. Table 2 shows the corresponding simulation results.

Based on rows 1-5 in Table 2, we analyse the impact of the transmission line attack budget on load loss under a fixed setting of $\mathcal{H}_c$=3 and $\mathcal{H}_o$=2. We can observe that the load loss increases as the transmission line attack budget increases. Specifically, the load loss is only 56.82 MW when the transmission line attack budget $\mathcal{H}_p$ is 1, whereas it reaches 620.79 MW if $\mathcal{H}_p$ is 5. This is because as the number of transmission line disruptions increases, the power delivery capability is progressively reduced, limiting the ability to deliver power to meet load demand. Thus, greater amounts of load loss are required to maintain power balance and prevent system instability. Similarly, we can find from rows 6-10 that the load loss also increases with the increase in the attack budget of the communication link under a fixed setting of $\mathcal{H}_p$=3 and $\mathcal{H}_o$=2. However, when the attack budget of the communication link $\mathcal{H}_c$ is 1, the load loss is only 266.95 MW, and it reaches 1280.69 MW if $\mathcal{H}_c$ is 5. By comparison, the impact of attacked communication links on load loss is more significant than that of attacked transmission lines. This is because the disruption of critical communication links can compromise the control and observability of multiple components in the physical network, thereby degrading the ability of the system operator to execute effective generation dispatch strategies. These results fully reveal the potential risks to CPPSs under coordinated cyber-physical network attacks considering the interdependent cyber and physical networks. In addition, the coordinated attack strategies significantly vary under different attack budgets. It also paves the way for the system defender to determine relevant defence strategies.

In addition, it can be observed that increasing the attack budget on communication links results in significantly more load loss than an

**Table 2**
Simulation results under different attack budgets.

| Setting | | Attack budget | Attacked transmission lines | Attacked communication links | Attacked coupled lines | Load loss (MW) |
|---|---|---|---|---|---|---|
| $\mathcal{H}_c = 3$ | $\mathcal{H}_p$ | 1 | 26 | 26, 30, 36 | 26 | 56.82 |
| $\mathcal{H}_o = 2$ | | 2 | 19, 23, | 19, 23, 29 | 19, 23 | 163.37 |
| | | 3 | 29, 36, 37 | 11, 28, 33 | \ | 260.21 |
| | | 4 | 5, 7, 27 | 6, 27, 33 | 27 | 388.21 |
| | | 5 | 7, 15, 17, 18, 23 | 18, 23, 32 | 18, 23 | 620.79 |
| $\mathcal{H}_p = 3$ | $\mathcal{H}_c$ | 1 | 5, 10, 37 | 35 | \ | 266.95 |
| $\mathcal{H}_o = 2$ | | 2 | 10, 29, 37 | 16, 33 | \ | 266.95 |
| | | 3 | 29, 36, 37 | 11, 28, 33 | \ | 260.21 |
| | | 4 | 24, 27, 28 | 11, 24, 27, 28 | 24, 27 | 1214.37 |
| | | 5 | 11, 24, 28 | 7, 11, 24, 30, 31 | 11, 24 | 1280.69 |

**Table 3**
Simulation results under different load levels.

| Load level | $\mathcal{H}_p = 2$ | | $\mathcal{H}_p = 3$ | |
|---|---|---|---|---|
| | Load loss (MW) | Load loss ratio | Load loss (MW) | Load loss ratio |
| 0.8 | 163.37 | 6.81 % | 260.21 | 10.84 % |
| 0.9 | 292.74 | 12.20 % | 356.58 | 13.21 % |
| 1.0 | 475.00 | 15.83 % | 643.42 | 21.54 % |
| 1.1 | 775.00 | 23.48 % | 930.26 | 28.19 % |
| 1.2 | 1075.00 | 29.86 % | 1217.11 | 33.81 % |

equivalent increase in the attack budget on transmission lines. This asymmetry arises from the functional interdependence between cyber and physical networks, explicitly modelled in constraint (12). Unlike transmission line outages, which locally restrict power delivery capacity, the disruption of communication links undermines the observability and controllability of multiple generation units in the physical network even if those components remain physically intact. In particular, affected generation units may become unreachable for generation redispatch, effectively reducing available generation and forcing the system to shed load to maintain balance. These effects are further amplified under strong interdependence (i.e., high $\alpha$ values), where generation unit output is directly constrained by communication availability. Thus, cyber-side attacks exhibit a stronger marginal effect by degrading the control capability of the system, and neglecting this cyber-physical interdependence may significantly underestimate system vulnerability under coordinated cyber-physical network attack scenarios.

### 5.3. Sensitivity analysis of the load level

This case further examines the impact of load level on load loss in the CPPSs. The attack budget of the communication link $\mathcal{H}_c$ is set to 3. The attack budget of the coupled line $\mathcal{H}_o$ is set to 2. The functional interdependence coefficient $\alpha$ is set to 0.8. The load level varies from 0.8 to 1.2, and the corresponding simulation results are shown in Table 3.

It can be observed that as the system load level increases, the load loss and its ratio to the total demand both increase significantly across all scenarios. For instance, in the case with a transmission line attack budget $\mathcal{H}_p = 2$, the load loss rises from 163.37 MW (6.81 %) at 0.8 load level to 1075.00 MW (29.86 %) at 1.2 load level in the physical network. A similar trend is also observed for $\mathcal{H}_p = 3$, where load loss increases from 260.21 MW (10.84 %) to 1217.11 MW (33.81 %). This trend is attributed to the reduced system resilience under higher load demand stress. As the total load demand increases in the physical network, the system becomes more sensitive to the loss of controllability and transfer capability caused by coordinated cyber-physical network attacks. This is due to the fact that, under a higher load level, there is limited spare capacity available to meet the load demand, especially when communication links are attacked and functional interdependence degrades generation unit control. Thus, the system needs to shed more load to ensure the operational security of CPPSs.

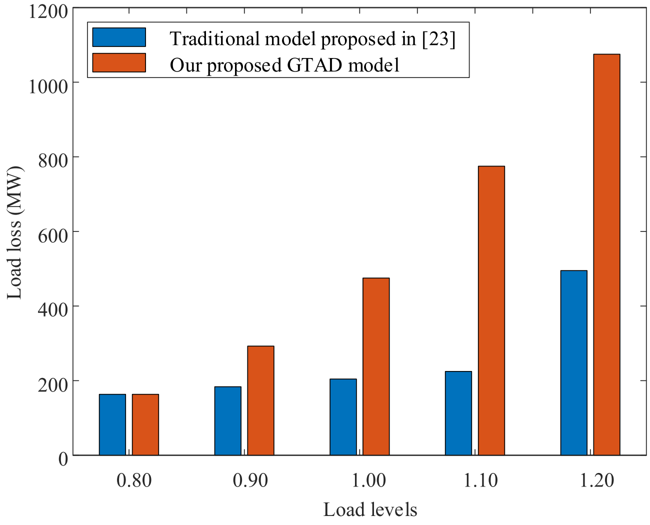


**Fig. 4.** Load loss under different load levels when the attack budget of the transmission line $\mathcal{H}_p$ is set to 2.

Additionally, Fig. 4 shows the load loss obtained in our proposed GTAD model and the traditional model proposed in [23] under different load levels. We can observe that the proposed GTAD model consistently yields significantly higher load loss compared to the model proposed in [23], across all load levels except at 0.8. For example, when the load level is set to 1.0, our proposed GTAD model reports 475.00 MW of load loss, whereas the model proposed in [23] remains well below 300 MW, specifically at 204.21 MW. This gap further widens when the load level is set to 1.2. This demonstrates that our model more effectively captures the impact of cyber-physical interdependence under a higher load level, whereas the traditional model proposed in [23] underestimates the vulnerability of CPPSs to coordinated cyber-physical network attacks. These results emphasise the necessity of dynamic protection schemes and resilient operation strategies tailored to different load levels.

### 5.4. Sensitivity analysis of the functional interdependence coefficient

In this case, we analyse the impact of the functional interdependence coefficient $\alpha$ on CPPSs. Two control centres are deployed at communication nodes 9 and 18. The attack budget for transmission lines $\mathcal{H}_p$ is set to 4, while the attack budgets for communication links $\mathcal{H}_c$ and coupled lines $\mathcal{H}_o$ are set to 3 and 2, respectively. The coefficient is set to vary from 0.5 to 1, which characterises the degree of functional interdependence between the cyber and physical networks. The corresponding simulation results are shown in Table 4.

It is clear that the load loss increases monotonically with the growth of the functional interdependence coefficient $\alpha$. When $\alpha$=0.5, the load loss is 512.89 MW, whereas it increases to 644.47 MW if $\alpha$=1.0, marking

**Table 4**
Simulation results under different functional interdependence coefficients.

| $\alpha$ | Attacked transmission lines | Attacked communication links | Attacked coupled lines | Load loss (MW) |
|---|---|---|---|---|
| 0.5 | 11, 25, 26, 28 | 4, 25, 26 | 25, 26 | 512.89 |
| 0.6 | 1, 25, 26, 28 | 11, 25, 26 | 25, 26 | 524.47 |
| 0.7 | 25, 26, 28, 37 | 11, 25, 26 | 25, 26 | 554.47 |
| 0.8 | 7, 24, 28, 37 | 11, 15, 24 | 24 | 587.12 |
| 0.9 | 25, 26, 28, 31 | 11, 25, 26 | 25, 26 | 614.47 |
| 1.0 | 7, 25, 26, 28 | 11, 25, 26 | 25, 26 | 644.47 |

a 25.65 % increase. This trend reflects that a higher functional interdependence amplifies the vulnerability of CPPSs under coordinated cyber-physical network attacks, as the failure of communication links more directly leads to the loss of control functions in associated components in the physical network (e.g., generation units). In contrast, at lower values of $\alpha$, the functional interdependence between the cyber and physical networks is weaker, allowing some physical assets to effectively operate, thereby reducing the impact of coordinated cyber-physical network attacks. These results emphasise the importance of functional interdependence in analysing the vulnerability of CPPSs to coordinated cyber-physical network attacks. Ignoring such interdependence may lead to a significant underestimation of the potential vulnerabilities and risks to CPPSs under coordinated cyber-physical network attacks.

In addition, we can further observe that transmission lines 25, 26, and 28, along with communication links 25 and 26, are the most frequently selected in the optimal attack strategies across different values of the interdependence coefficient and can be identified as high-risk components. This means that these high-risk components play a critical role in CPPSs in terms of delivering power and transmitting information, and their disruptions may amplify the vulnerability of CPPSs to coordinated cyber-physical network attacks. Therefore, identifying such high-risk components can provide valuable guidance for the system defender to develop targeted defence strategies. In summary, our proposed method not only provides a more accurate and comprehensive framework for assessing the potential vulnerabilities and risks of CPPSs but also offers targeted defence strategies against coordinated cyber-physical network attacks.

(2) Practical 36-zone Great Britain Power Transmission System: To further validate the scalability of our proposed GTAD model, additional case studies are conducted on a practical 36-zone Great Britain power transmission system. This system, with a peak load demand of 40000 MW, features 36 zones interconnected by 69 transmission lines operating at the 400 kV voltage level. The GB power transmission system used in this study is a reduced network initially developed by National Grid in 2012 based on publicly available, non-confidential data. In 2020, the system was further extended and improved, making it particularly suitable for the analysis of large-scale scalability applications. The corresponding topology of the 36-zone power transmission system is shown in Fig. 5. Similarly, the top 15 transmission lines based on power flow capacity are assumed to be coupled lines.

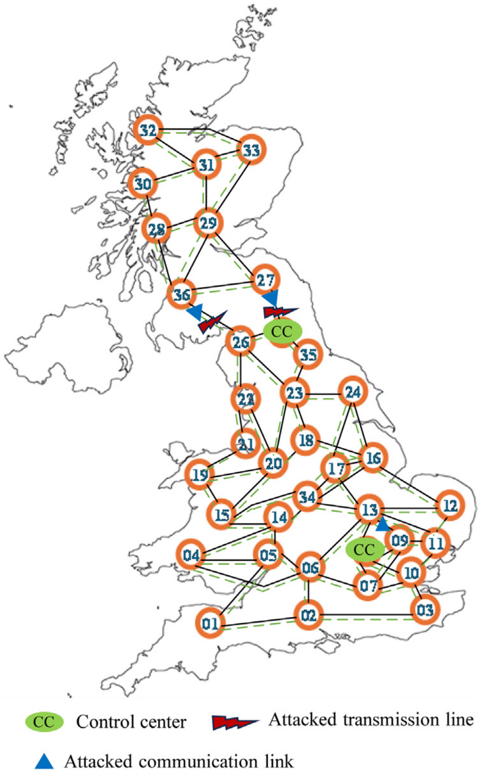


**Fig. 5.** Attacked transmission lines and communication links when the attack budget of transmission line $\mathcal{H}_p$ is set to 2.

In this case, the attack budget of the communication link $\mathcal{H}_c$ is set to 3, and the attack budget of the coupled line $\mathcal{H}_o$ is set to 2. The functional interdependence coefficient $\alpha$ is set to 1. Two control centres are deployed at communication nodes 8 and 25. Table 5 shows the corresponding simulation results under different attack budgets for the transmission line. As can be observed, when the functional and topological interdependence between the cyber and physical networks is considered, larger load loss is caused in all cases due to coordinated cyber-physical network attacks. That is to say, the load loss and the attack strategy are strongly affected by the interdependent cyber and physical networks compared to those obtained in [23]. Taking the case of $\mathcal{H}_p$ =3 as an example, the traditional model proposed in [23] yields a load loss of 2205.91 MW, whereas our proposed GTAD model leads to a load loss of 4793.05 MW, marking a 117.28 % increase. This is because our proposed model considers the effects caused by communication link disruptions and the consequent loss of controllability over critical components i.e., generation units, which are neglected in [23].

In addition, Table 5 shows the computation times under different attack budgets for transmission lines. It can be observed that as the attack resources increase, the calculation time will increase. For example, when the attack budget $\mathcal{H}_p$ increases from 2 to 4, the calculation time of the proposed model rises from 56.42 s to 132.55 s. The calculation time re-

**Table 5**
Simulation results based on a practical 36-zone Great Britain power transmission system.

| Models | $\mathcal{H}_p$ | Attacked transmission lines | Attacked communication links | Attacked coupled lines | Load loss (MW) | Calculation time (s) |
|---|---|---|---|---|---|---|
| Ref. [23] | 2 | 17, 19 | \ | \ | 1515.77 | 1.17 |
| | 3 | 15, 17, 19 | \ | \ | 2205.91 | 5.26 |
| | 4 | 11, 15, 17,19 | \ | \ | 2708.80 | 11.65 |
| This paper | 2 | 51, 52 | 50, 51, 52 | 51, 52 | 4417.49 | 56.42 |
| | 3 | 18, 51, 52 | 18, 51, 52 | 51, 52 | 4793.05 | 88.21 |
| | 4 | 17, 19, 51,52 | 46, 49, 51 | 51 | 5404.85 | 132.55 |

mains acceptable for off-line analysis or scenario evaluation, especially considering the enhanced attack impact achieved through more comprehensive modelling. This confirms that the model exhibits promising computational efficiency and scalability, further supporting its potential for near real-time deployment even in large-scale practical systems.

Meanwhile, a detailed observation of the attack strategy reveals that our proposed GTAD model consistently targets transmission lines and communication links that are cyber-physically coupled and topologically critical, such as lines 51 and 52, as shown in Fig. 5. In contrast, the traditional model proposed in [23] tends to select targeted components based solely on the physical network. This difference demonstrates the capability of our proposed model to uncover hidden vulnerabilities stemming from the interdependence between the cyber and physical networks under coordinated cyber-physical network attacks. That is to say, neglecting the impact of the functional and topological interdependence between the cyber and physical networks may result in significant inaccuracies in analysing the vulnerability of CPPSs. These results illustrate that our proposed GTAD model not only provides a more accurate assessment of system vulnerability under coordinated cyber-physical network attacks but also offers valuable insights for determining defence strategies to enhance the resilience of CPPSs.

## 6. Conclusion

In this paper, we propose a bilevel game theory-based attack-defence (GTAD) model for vulnerability analysis of cyber-physical power systems (CPPSs) under coordinated cyber-physical network attacks, considering both functional and topological interdependence between cyber and physical networks. Case studies on IEEE 24-bus system and a realistic 36-zone Great Britain power transmission system demonstrate that ignoring the interdependence between cyber and physical networks can significantly underestimate the potential risks to CPPSs under coordinated cyber-physical network attacks, both in terms of load loss and attack strategies. Overall, the proposed GTAD model can determine higher-risk coordinated cyber-physical attack strategies compared with the traditional method. In future work, we will investigate how to further determine optimal defence strategies to enhance the resilience of CPPSs against coordinated cyber-physical network attacks. In addition, we will incorporate full AC power flow constraints to capture voltage-dependent vulnerabilities and reactive power effects that may be overlooked by DC-based models.

## CRediT authorship contribution statement

**Min Du:** Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Xin Zhang:** Writing – original draft, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Gareth Taylor:** Supervision, Resources, Funding acquisition, Conceptualization. **Vladimir Terzija:** Supervision, Project administration, Investigation, Conceptualization.

## Funding

This work was supported by the U.K. Research and Innovation Future Leaders Fellowship “Digitalisation of Electrical Power and Energy Systems Operation” (MR/W011360/2).

## Declaration of competing interests

Xin Zhang is an associate editor for Cyber-Physical Energy Systems, Vladimir Terzija is an advisory board member for Cyber-Physical Energy Systems, they were both not involved in the editorial review or the decision to publish this article. All authors declare that there are no competing interests.

## References

[1] M.S. Alvarez-Alvarado, C. Apolo-Tinoco, M.J. Ramirez-Prado, F.E. Alban-Chacón, N. Pico, J. Aviles-Cedeno, A. A. Recalde, F. Moncayo-Rea, W. Velasquez, J. Rengifo, Cyber–physical power systems: a comprehensive review about technologies drivers, standards, and future perspectives, Comput. Electr. Eng. 116 (2024) 109149.

[2] P. Li, J. Fu, K. Xie, B. Hu, Y. Wang, C. Shao, Y. Sun, W. Huang, A defense planning model for a power system against coordinated cyber–physical attack, Prot. Control Mod. Power Syst. 9 (5) (2024) 84–95.

[3] S. Paul, F. Ding, K. Utkarsh, W. Liu, M.J. O’Malley, J. Barnett, On vulnerability and resilience of cyber–physical power systems: a review, IEEE Syst. J. 16 (2) (2022) 2367–2378.

[4] R. He, H. Xie, J. Deng, T. Feng, L.L. Lai, M. Shahidehpour, Reliability modeling and assessment of cyber space in cyber–physical power systems, IEEE Trans. Smart Grid 11 (5) (2020) 3763–3773.

[5] Y. Shen, Q. Zhou, Y. Wen, Z. Shuai, Z.J. Shen, Integrated satellite-Terrestrial network framework for Next generation Smart grid, IEEE Trans. Smart Grid 15 (5) (2024) 5249–5252.

[6] B. Ti, G. Li, M. Zhou, J. Wang, Resilience assessment and improvement for cyber—physical power systems under typhoon disasters, IEEE Trans. Smart Grid 13 (1) (2022) 783–794.

[7] T. Zhou, K. Xiahou, L.L. Zhang, Q.H. Wu, Real-time detection of cyber–physical false data injection attacks on power systems, IEEE Trans. Ind. Inform. 17 (10) (2021) 6810–6819.

[8] B. Yan, Z. Jiang, P. Yao, Q. Yang, W. Li, A.Y. Zomaya, Game theory based optimal defensive resources allocation with incomplete information in cyber–physical power systems against false data injection attacks, Prot. Control Mod. Power Syst. 9 (2) (2024) 115–127.

[9] M. Du, X. Liu, Z. Li, H. Lin, Robust mitigation strategy against dummy data attacks in power systems, IEEE Trans. Smart Grid 14 (4) (2023) 3102–3113.

[10] N. Stephanie, J.A. Abubakar, O.F. Ademola, The impact of stand-alone systems in Nigeria’s energy distribution sector and present-day challenges faced, IOP Conference Series: Earth and Environmental Science, IOP Publishing, 2024, pp. 012010.

[11] Z. Li, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, Bilevel model for analyzing coordinated cyber–physical attacks on power systems, IEEE Trans. Smart Grid 7 (5) (2016) 2260–2272.

[12] Y. Xiang, L. Wang, N. Liu, Coordinated attacks on electric power systems in a cyber–physical environment, Electr. Power Syst. Res. 149 (2017) 156–168.

[13] M. Ghaedi, H. Delkhosh, H. Seifi, M. Shafie-Khah, Two-stage direct and bi-level indirect coordinated cyber-physical attacks integrating substation outage, IEEE Trans. Power Syst. [Online](2025). Available: https://ieeexplore.ieee.org/document/10963701. doi:10.1109/TPWRS.2025.3560084.

[14] J. Tian, B. Wang, T. Li, F. Shang, K. Cao, Coordinated cyber–physical attacks considering DoS attacks in power systems, Int. J. Robust Nonlinear Control 30 (11) (2020) 4345–4358.

[15] Z. Lian, Y. Zhu, F. Guo, C. Peng, Q. Zhou, Distributed cyber resilient control strategy for remote DC microgrids under integrated satellite terrestrial networks, IEEE Trans. Ind. Inform. 21 (3) (2025) 2363–2372.

[16] K. Jiang, Networking analysis of power communication networks, China Electric Power Press, Beijing, 2014.

[17] M. Xin, C. Xi, in: Natural disasters prevention of power communications system, 2010 International Conference on Power System Technology, IEEE, 2010, pp. 1–6.

[18] M. Zeraati, Z. Aref, M.A. Latify, Vulnerability analysis of power systems under physical deliberate attacks considering geographic-cyber interdependence of the power system and communication network, IEEE Syst. J. 12 (4) (2018) 3181–3190.

[19] M. Tian, Z. Dong, L. Gong, X. Wang, Line hardening strategies for resilient power systems considering cyber-topology interdependence, Reliab. Eng. Syst. Saf. 241 (2024) 109644.

[20] G. Huang, J. Wang, C. Chen, C. Guo, Cyber-constrained optimal power flow model for smart grid resilience enhancement, IEEE Trans. Smart Grid 10 (5) (2019) 5547–5555.

[21] Y. Guo, C. Guo, J. Yang, A tri-level optimization model for power systems defense considering cyber–physical interdependence, IET Gener. Transm. Distrib. 17 (7) (2023) 1477–1490.

[22] Y. Guo, C. Guo, J. Yang, A resilience-oriented restoration model against attacks on cyber–physical power systems, CSEE J. Power Energy Syst. [Online] Available: https://ieeexplore.ieee.org/document/10436609. doi:10.17775/CSEEJPES.2022.08550.

[23] J.M.J.I.G. Arroyo, transmission and distribution, Bilevel programming applied to power system vulnerability analysis under multiple contingencies, IET Gener. Transm. Distrib. 4 (2) (2010) 178–190.

[24] Z. Song, The evaluation of parameter m in the big m method of linear programming, in: International Conference on Materials Engineering and Information Technology Applications (MEITA 2015), Atlantis Press, 2015, pp. 37–40.

[25] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, C. Singh, The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee, IEEE Trans. Power Syst. 14 (3) (1999) 1010–1020.