Reliability Engineering and System Safety 264 (2025) 111417

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Robustness analysis of CPPS against malware attacks under malware incubation and attack–defense confrontation

Jinfu Zhang [a], Haicheng Tu [a,*], Yongxiang Xia [a], Xuetao Yang [b], Yibo Zhu [c]

[a] The School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, 310018, China
[b] Power System Department, China Electric Power Research Institute, Beijing, 100192, China
[c] Hangzhou Zhonhen Electric Co., Ltd, Hangzhou, 310053, China

ARTICLE INFO

Keywords:
Incubation period
Attack–defense confrontation
Limited information
Cyber-physical power system
Malware attacks

ABSTRACT

The integration of advanced technologies in Cyber-Physical Power System (CPPS) has increased the vulnerability to cyber threats. Consequently, many network science-based studies have sought to analyze the robustness of CPPS against Advanced Persistent Threats (APTs). Compared with previous studies, our framework incorporates the malware incubation period, incomplete attacker information, coupling patterns, and reconnaissance-evasion behavior, thereby covering a broader spectrum of scenarios. Based on our framework, we first quantify the tradeoff between incubation duration and attack success rate to identify the optimal attack launch time. Subsequently, we investigate how system robustness is affected by critical parameters across various scenarios. Simulation experiments reveal that the attackers' incomplete information delays the optimal launch time. Disassortative coupling patterns can mitigate malware impact and enhance CPPS robustness. Furthermore, results demonstrate two distinct defensive resource allocation strategies for optimal CPPS robustness. In the disassortatively coupled CPPS, defenders must continuously adjust the deployment of defensive assets as the relative attack–defense budget shifts, whereas under assortative coupling a quasi-static deployment of defensive assets suffices to attain optimal robustness. These insights provide cost-effective guidelines for strengthening the robustness of CPPS.

1. Introduction

Cyber-Physical Power System (CPPS) have become increasingly critical due to their ability to enhance the operational efficiency and reliability of traditional power system through the integration of advanced technologies [1]. By merging physical infrastructures with communication network, CPPS enable intelligent monitoring, control, and optimization, thereby playing a pivotal role in modern power system management [2]. This evolution has improved the performance of power system and generated significant scholarly interest, prompting extensive research efforts in the field [3,4]. However, this integration increases system's vulnerability to cyber threats [5–7]. These attacks partially include denial-of-service (DoS) attacks [8], false-data injection attacks (FDIAs) [9,10], advanced persistent threats (APTs) [11,12], large-scale coordinated attacks [13,14] and jamming attacks [15]. Among these, APTs are generally regarded as one of the most damaging attacks.

In APTs, malware can spread stealthily through the communication layer and it may remain undetected for long periods while preparing disruptive actions against the physical layer. The Ukrainian power grid blackout is a well-known illustration: a coordinated APTs campaign penetrated the supervisory control and data acquisition (SCADA) network and ultimately caused a regional outage affecting a large number of customers [16]. Since that event, APTs analysis and mitigation have become a focal research topic in CPPS robustness and resilience analysis [17].

Several studies adopt a reductionist modeling method to characterize every step of the APTs [11,12,18]. Presekal et al. proposed the Advanced Cyber-Physical Power System kill-chain framework, which enumerates and examines each stage of APTs that target CPPS [18]. Building on that framework, Ref. [19] developed a spatio-temporal correlation method for early APTs detection. Such reductionist modeling method describes each stage of the attack in communication network in detail, which offer granular insight into how attackers laterally move and persist within critical infrastructure corresponding to CPPS, enabling anomaly detection at early stages of the compromise. However, this emphasis on high realism and behavioral detail comes at a cost. Simulating the joint dynamics of the communication network and power grid in full detail is computationally intensive and does

* Corresponding author.
E-mail address: tuhc@hdu.edu.cn (H. Tu).

https://doi.org/10.1016/j.ress.2025.111417
Received 11 February 2025; Received in revised form 25 May 2025; Accepted 30 June 2025
Available online 16 July 2025

Table 1
Comparison of representative related works in terms of modeling paradigm and four specific scenarios.

Work	Modeling method	Attack type	Incubation	Incomplete information	Coupling	Reconnaissance
Our work	Holistic modeling	APTs	✓	✓	✓	✓
[21]	Holistic modeling	APTs	X	X	✓	X
[22]	Holistic modeling	APTs	X	✓	✓	X
[23]	Holistic modeling	APTs	X	X	✓	X
[24,25]	Holistic modeling	APTs	✓	X	✓	X
[27]	Holistic modeling	APTs	✓	✓	X	X
[18,19]	Reductionist modeling	APTs	–	–	–	–
[8]	Holistic modeling	DOS	–	–	–	–
[9]	Physics-informed modeling	FDIAs	–	–	–	–
[15]	Physics-informed modeling	Jamming attack	–	–	–	–
[13]	Holistic modeling	Coordinated attack	–	–	–	–

✓: scenario included, *X*: scenario not included

not scale easily to very large systems. Moreover, these works tend to focus on particular attacker paths and network-level steps, so they may overlook system-wide failure modes and are not fully captured the system-level interdependencies between the two layers.

By contrast, complex-network approach, which adopts holistic modeling method, treats the CPPS as coupled networks and focus on macro-level interdependencies and cascades. In this paradigm, the power grid and its communication infrastructure are modeled as interdependent layers, and an attack is represented as removal of nodes or links that can propagate through both networks. Buldyrev et al. [20] pioneered the representation of CPPS as interdependent networks, sparking considerable interest in the vulnerability of coupled infrastructures. Inspired by this pioneering work, the interdependent network model is widely used in later studies. Ref. [21] analyzed malware-triggered cascading failures using a stochastic state-transition model, while Lai et al. [22] identified critical cyber nodes whose compromise markedly degrades system robustness. The interplay between malware propagation in the cyber layer and fault propagation in the physical layer is further investigated in [23]. To move beyond the common assumption that malware launches an attack immediately after infecting a host, Xu et al. incorporated both an incubation period and the detection probability into their analytical framework [24,25]. However, when considering the incubation period and detection probability of the malware, those studies presuppose that attackers possess complete knowledge of the communication-network topology.

In practice, adversaries often act under incomplete topological information of the CPPS [26]. The joint impact of (i) a non-zero malware incubation period and (ii) the attacker's limited topological information on CPPS therefore remains insufficiently explored. Moreover, although previous studies [22,27] have explored the impact of critical parameters on the robustness of CPPS, such as optimal node protection strategies preventing nodes from direct attacks, the situation of preventing nodes from being detected by attackers has received comparatively limited attention [28,29].

Motivated by the aforementioned limitations, this paper develops a system-level simulation framework to evaluate the robustness of CPPS against malwares from a network science perspective. As shown in Table 1, unlike previous studies, which considered a relatively limited set of scenarios, our simulation framework comprehensively considers four proposed scenarios — (i) the malware incubation period, (ii) the attacker's incomplete topological knowledge, (iii) heterogeneous cyber–physical coupling patterns, and (iv) the reconnaissance-evasion behavior. Built upon this unified platform, we conduct extensive attack–defense simulations under a variety of protection strategies. The main contributions are summarized as follows:

1. We develop a network science–based simulation framework that simultaneously captures (i) the malware incubation period, (ii) the attacker's incomplete topological knowledge, (iii) heterogeneous cyber–physical coupling patterns, and (iv) reconnaissance-evasion behavior. This unification extends previous studies by considering more scenarios and embedding a dynamic attack–defense process within an interdependent network context.
2. Based on this framework, we investigate the tradeoff between the malware incubation duration and detection risk, considering different coupling patterns and attackers' incomplete information. Our study offers insight into how prior information and disassortative coupling patterns can systematically determine the optimal attack launch timing and enhance CPPS robustness.
3. Our study demonstrates two distinct defensive resource allocation strategies for optimal CPPS robustness. In the disassortatively coupled CPPS, defenders must continuously adjust the deployment of defensive assets as the relative attack–defense budget shifts, whereas under assortative coupling a quasi-static deployment of defensive assets suffices to attain optimal robustness.

The rest of the paper is organized as follows. Section 2 outlines the CPPS topological model, which serves as the foundation for our analysis. Section 3 presents the comprehensive simulation framework for robustness analysis of CPPS under malware attacks. In Section 4, we propose our defense strategies and methodologies used to evaluate their effectiveness. Section 5 provides case studies and results. Finally, Section 6 concludes the paper.

2. CPPS model

As shown in Fig. 1, a typical CPPS consists of a power network (the physical layer) and a communication network (the cyber layer which contains control layer and transmission layer) [30]. In this section, we describe the topological model of the power and communication networks and outline the coupling patterns between these two layers.

2.1. Power network model

Under malware attacks, the power grid experiences not only topological transformations but also functional changes, such as the redistribution of power flows. In CPPS, the DC power flow model [24,31] is commonly used to characterize the behavior of the power network. This model provides a simplified linear approximation of system dynamics, enabling effective analysis of power system behavior.

The power network in CPPS can be represented as a directed graph $G_p = (V_p, E_p)$, where V_p is the set of power nodes, and E_p represents the transmission lines between them. Considering a power network with m power nodes and n transmission lines, the vector of injected real power at the nodes, denoted as $P = [p_1, p_2, \ldots, p_m]^T$, can be calculated with the following equation:

$$P = B\Theta \tag{1}$$

where $\Theta = [\theta_1, \theta_2, \ldots, \theta_m]^T$ is the vector of nodal phase angles, and $p_i > 0$ for supply nodes such as generators and $p_i < 0$ for demand nodes

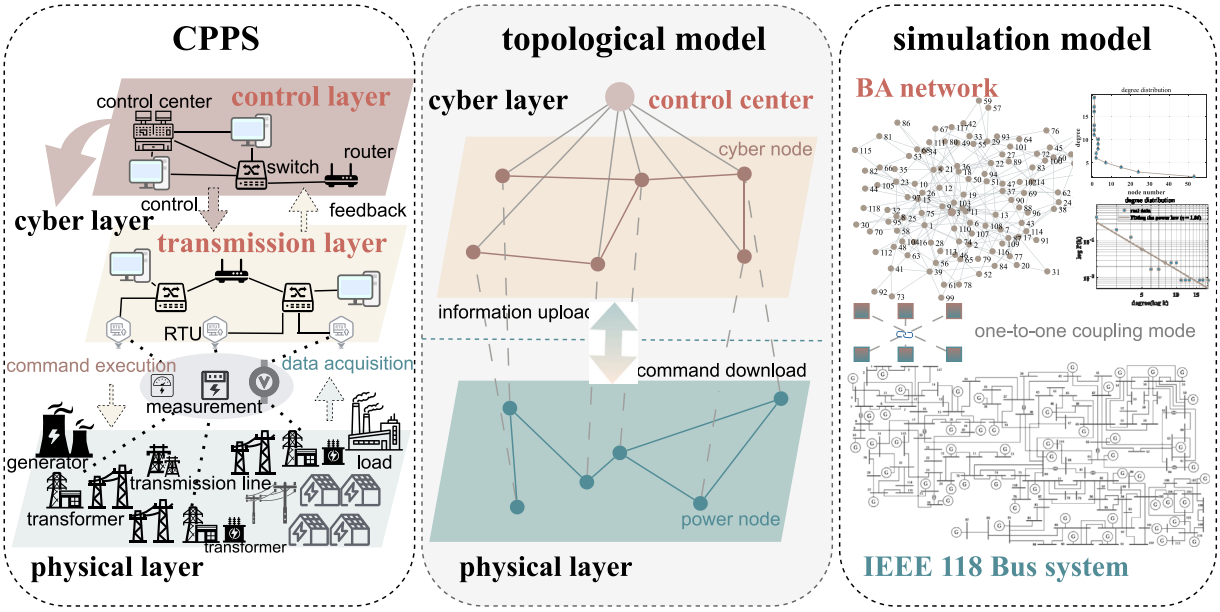

Fig. 1. CPPS and its topological & simulation models in our study.

such as loads. Here, B is the nodal admittance matrix, which is a $m \times m$ matrix whose entries are defined as:

$$B = \begin{bmatrix} \sum_{j \neq 1} b_{1j} & -b_{12} & -b_{13} & \cdots & -b_{1m} \\ -b_{21} & \sum_{j \neq 2} b_{2j} & -b_{23} & \cdots & -b_{2m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -b_{m1} & -b_{m2} & -b_{m3} & \cdots & \sum_{j \neq m} b_{mj} \end{bmatrix} \tag{2}$$

where b_{ij} is defined as follow:

$$b_{ij} = b_{ji} = \begin{cases} \frac{1}{x_{ij}}, & \text{if nodes } i, j \text{ is connected} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where x_{ij} being the admittance of transmission line between nodes i and j. The power flow equation can be expressed as

$$F = W^{-1} M^T \Theta, \tag{4}$$

where $F = [f_1, f_2, \ldots, f_l]^T$ is the vector of power flows in the grid. $W = \text{diag}(x_l)$ is an $n \times n$ diagonal matrix with entries x_l being the admittance of transmission line l. M is the $n \times m$ line-node incidence matrix with $M_{ij} = 1$ if node j is the origin of the ith transmission line, $M_{ij} = -1$ if node j is the ending and $M_{ij} = 0$ otherwise. In our case study, the power network is modeled using IEEE 118-Bus System.

2.2. Communication network model

As illustrated in Fig. 1, the communication network can similarly be modeled as a graph $G_c = (V_c, E_c)$, where V_c denotes the set of communication nodes, and E_c represents the communication links between them. In CPPS, communication nodes are Intelligent Electronic Devices (IEDs) controlled by the control center. These IEDs include sensors, routers, and actuators, which monitor the power network, communicate with other nodes, and execute control commands. The control center processes information from the IEDs and issues instructions to ensure grid stability and safety. In this study, we assume that the control center operates in a centralized form and has the capability to monitor all IEDs. Following Refs. [4,32], since the control center is modeled as the most critical component in the model, substantial defensive measures will be allocated to protect this hub node. We assume the control center is secure and not compromised.

In our case study, the communication network is modeled as a scale-free graph, reflecting empirical findings that power-grid communication topologies often exhibit heavy-tailed (power-law) degree distributions [33,34]. Accordingly, we employ the Barabási–Albert (BA) model to generate the communication topology [35]. We configure the BA process so that the final graph has the same size as the IEEE 118 Bus system. Specifically, following Refs. [4,32], we begin with $m_0 = 4$ connected nodes and attach each new node with $m = 2$ links, continuing until $N = 118$ nodes are reached. By construction, the resulting communication network has 118 nodes. This model yields a scale-free communication network and ensures that the communication network aligns with the power network.

2.3. Coupling patterns of CPPS

The coupling between power and communication networks in a CPPS is established through interdependence interfaces [36]. IEDs are connected to power buses, facilitating bidirectional communication: the IEDs collect data from the buses and relay it to the control center, which then issues operational directives back to the buses. This integrated structure highlights the potential for failures in one network to propagate to the other, potentially triggering cascading failures.

In this framework, we implement a one-to-one correspondence strategy [37], as illustrated in Fig. 1, to ensure that each power node is monitored and controlled by its corresponding linked IEDs. Additionally, given that most communication devices are equipped with Uninterruptible Power Supply systems [38], a unidirectional coupling model is employed. In this model, power nodes depend on their associated communication nodes for monitoring and regulatory purposes, whereas communication nodes operate independently and are not reliant on power nodes.

In addition, we present four distinct one-to-one coupling strategies between the communication and power networks, along with a random coupling strategy for comparison:

(1) **Coupling Pattern I — Degree-Degree Assortative Coupling (DDAC):** Communication nodes are paired with power nodes based on their degree, with both networks sorted in descending order of degree.

(2) **Coupling Pattern II — Degree-Degree Disassortative Coupling (DDDC):** Communication nodes, sorted in descending order of degree, are paired with power nodes sorted in ascending order of degree.
(3) **Coupling Pattern III — Degree-Capacity Assortative Coupling (DCAC):** Communication nodes, sorted in descending order of degree, are paired with power nodes sorted in descending order of power capacity.
(4) **Coupling Pattern IV — Degree-Capacity Disassortative Coupling (DCDC):** Communication nodes, sorted in descending order of degree, are paired with power nodes sorted in ascending order of power capacity.
(5) **Coupling Pattern V - Random Coupling (RC):** Nodes are paired randomly between the communication and power networks, without considering degree or power capacity.

3. Simulation framework of malware attacks in CPPS

This section analyzes the simulation framework for malware attacks in CPPS in a network science perspective, considering the attackers' incomplete information of the system's network topology and the presence of a malware incubation period. These constraints inherently shape the attackers' strategies, influencing the efficiency of malware propagation and the overall outcomes of the attack [32]. To address these dynamics, we develop mathematical models to characterize the stages of malware propagation, detection, the eventual launch of the attack, and the corresponding cyber protection measures, including load shedding and evaluation metrics. The section concludes with a comprehensive summary of the entire simulation process.

3.1. Limited CPPS topology information of attackers

In a more realistic scenario, attackers are unable to fully observe the structure of the CPPS [39], as illustrated in Fig. 2. Initially, the attacker can only observe a subset of communication nodes, which constrains their ability to select optimal attack node.

The attacker's objective is to maximize the power loss of the CPPS following the malware attack. To achieve this, after the malware spreads within the visible portion of the network, the attacker selects the node with the highest degree among the observed nodes for malware injection. This strategy ensures maximum disruption.

Mathematically, let V_{obs} represent the set of nodes observable by the attacker, and $d(i)$ denote the degree of node i. The attacker will initially inject malware into the node with the highest degree within V_{obs}:

$$i^* = \arg\max_{i \in V_{obs}} d(i) \tag{5}$$

where i^* represents the optimal initial infection node under limited information.

3.2. Advanced persistent threats in CPPS

APTs targeting CPPS are multi-stage attacks that traverse IT and OT domains to achieve strategic disruption [7,18]. A representative example is the Ukraine 2015 power grid cyberattack. The attackers began with initial penetration via spear-phishing emails carrying weaponized documents that installed malware on an IT workstation. This foothold established a command-and-control (C2) channel, enabling the attackers to remotely persist in the network and download additional tools. The attackers then performed internal reconnaissance to map the corporate network, logging keystrokes and collecting credentials and sensitive information. Using the stolen domain credentials, the adversaries moved laterally and bridged the IT–OT gap. They installed covert access proxies to evade detection and maintain stealthy access into the operational technology (OT) environment. Finally, the APT group executed the attack payload in multiple stages to maximize damage. They remotely took control of substation breakers via legitimate SCADA client software over the illicit VPN and opened them, causing immediate power loss.

3.3. Malware incubation, propagation, and detection

In line with previous studies [4,23,25], we treat the APTs as an equivalent network epidemic spreading across the CPPS. In our network-based model, the progress of malware follows a Susceptible–Infected (SI) epidemic process on a graph: initially one node is infected and able to propagate the malware, while the rest are still susceptible. Each stage of the real attack (whether phishing penetration, establishing C2, or an OT payload) ultimately results in newly compromised hosts, which in the model corresponds to the transmission of infection along network links. This SI abstraction captures key aspects of the attack lifecycle in an analytically tractable way: an incubation period during which malware resides undetected on infected nodes, an active propagation phase as the infection attempts to spread to adjacent nodes, and eventual detection which discovers infected nodes and defeats the attack [22,32].

In the simulation, once malware is injected into the system, it spreads silently through the communication network following the SI model [40]. In this model, nodes are categorized as either susceptible or infectious. A susceptible node becomes infected through interactions with its infectious neighbors. The probability that node k becomes infected at time t is given by:

$$P_k(t) = 1 - (1 - \lambda)^{M(k,t-1)} \tag{6}$$

where λ is the infection rate, and $M(k, t-1)$ denotes the number of infected neighbors of node k at time $t-1$.

As shown in Fig. 2, before launching an attack, the malware propagates stealthily without triggering any disruptions [40]. The attackers aim to infect as many communication nodes as possible before initiating the attack.

During each time step of the malware propagation, system operators have a chance to detect the infection [24,32]. Let β represent the detection probability per infected node. The probability of survival, $PS(t)$, that the malware remains undetected until time t is expressed as:

$$PS(t) = (1 - \beta)^{I(t)} PS(t-1) \tag{7}$$

where $I(t)$ is the number of infected nodes at time t. If the malware is detected before the attackers launch the attack – specifically, if even a single infected communication node is detected – the system operators will be alerted, ultimately causing the entire attack to fail.

3.4. Attack launch and load shedding

After the propagation period, at onset time T_{onset}, the attacker launches the attack by using the infected communication nodes to issue malicious commands to the power nodes under their control, forcibly disconnecting these power nodes from the power network, leading to cascading failures in the power network [32]. The attack strategy is formulated as:

$$A(T_{\text{onset}}) = \sum_{i \in V(T_{\text{onset}})} C_i \tag{8}$$

where $A(T_{\text{onset}})$ represents the attack vector at the time of onset T_{onset}, $V(T_{\text{onset}})$ denotes the set of infected communication nodes at T_{onset}, and C_i is the malicious command issued by node i to the power nodes under the attacker's control.

Before the cyber attack triggering widespread cascading failures across the power network, cyber control becomes crucial in controlling the propagation of these failures, ensuring that power distribution is optimized to limit the impact of malware-induced disruptions on system stability.

A common strategy to control cascading failures in the power network following a cyber–physical attack is load shedding. By shedding load, the power system reduces the burden on overloaded transmission

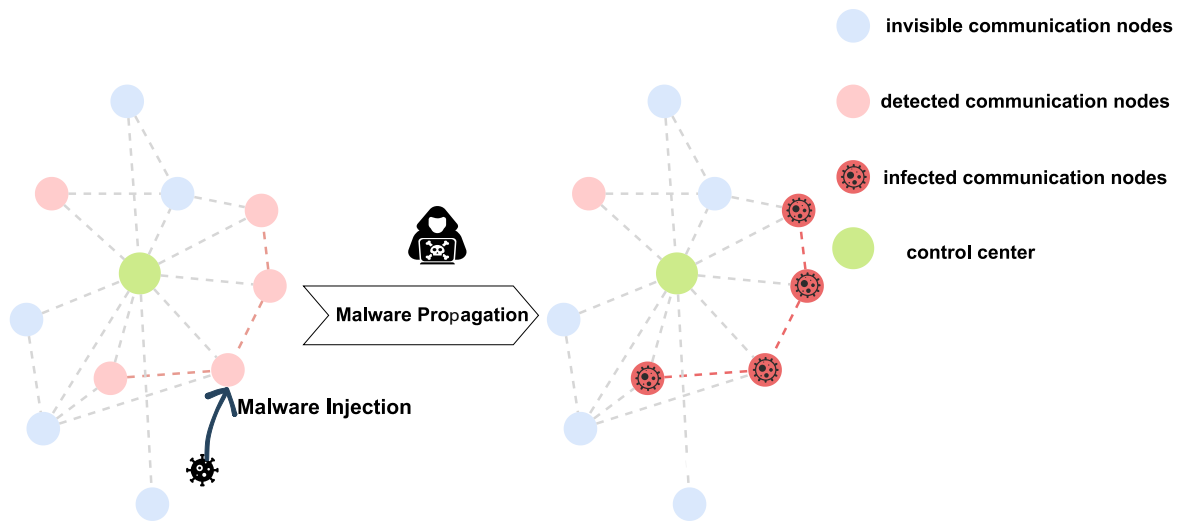

Fig. 2. Malware propagation in the CPPS communication network.

lines, ensuring that power flow is redistributed within the safety capacity of each bus and line. Using the DC power flow model, this load adjustment process can be mathematically formulated as the following optimization model [41]:

$$\max \quad \sum_{j\in V_D} \left|P_j\right| \tag{9a}$$

$$\text{s.t.} \quad P = B\Theta \tag{9b}$$

$$F = W^{-1}M^T\Theta \tag{9c}$$

$$\sum_{i\in V_G} |P_i| = \sum_{j\in V_D} |P_j| \tag{9d}$$

$$P_{dj} \le P_j \le 0, \quad \forall j \in V_D \tag{9e}$$

$$0 \le P_i \le P_{gi}^{\max}, \quad \forall i \in V_G \tag{9f}$$

$$|f_l| \le f_l^{\max}, \quad \forall l \in E_p \tag{9g}$$

Here, P represents the vector of power at each node that needs to be optimized. V_G and V_D denote the sets of generation and demand nodes, respectively. P_i represents for supply node and P_j is for demand node. $F = [f_1, f_2, \ldots, f_l]^T$ is the vector of power flows in the grid. $W = \text{diag}(x_l)$ is an $n \times n$ diagonal matrix with entries x_l being the admittance of transmission line l. M is the $n \times m$ line-node incidence matrix. The objective in Eq. (9a) aims to maximize the remaining load. The DC power flow constraints in Eqs. (9b) and (9c) capture the physical characteristics of the system and ensure that power flows respect the power network topology and operational limits, preventing overloads. Eq. (9d) enforces power balance between generation and consumption, ensuring energy conservation. Eq. (9e) restricts the load at each demand node to its initial demand, supporting demand-side management. Eq. (9f) ensures that generators operate within their safe capacity, and Eq. (9g) limits transmission line flows to prevent infrastructure overloads and potential failures. In this paper, the above optimization problem was formulated in Matlab using the YALMIP modeling toolbox [42] and subsequently solved with Gurobi Optimizer 11.0.2, invoking its built-in dual-simplex algorithm (Method = 1) [43].

3.5. Evaluation metrics

If the malware remains undetected during the propagation period, the attacker can launch the attack, disabling key power nodes and causing significant disruptions [32]. The effectiveness of the attack launched at T_{onset} is measured by the percentage of lost load (PLL), calculated as:

$$\text{PLL}(T_{\text{onset}}) = \frac{L_0 - L(T_{\text{onset}})}{L_0} \tag{10}$$

where L_0 is the initial load, and $L(T_{\text{onset}})$ represents the remaining load after the attack at time T_{onset}.

Malware with a longer propagation period generally leads to higher attack effectiveness, as indicated by an increased PLL. However, extending the propagation period also raises the likelihood of detection, thereby reducing the probability of survival PS and lowering the resulting PLL. Consequently, attackers must carefully balance the tradeoff between maximizing attack effectiveness and minimizing detection risk. This decision is influenced by the amount of available CPPS information and requires determining the optimal time to launch the attack.

To model this dynamic, we define the expected payoff for the attacker. For a successful attack launched at time T_{onset}, the payoff is given by $PLL(T_{\text{onset}})$. If the malware is detected before T_{onset} during the propagation period, the attack fails, and the attacker's payoff is zero. Thus, the expected payoff $EP(T_{\text{onset}})$ for launching the attack at time T_{onset}, can be expressed as:

$$\begin{aligned} EP(T_{\text{onset}}) &= PLL(T_{\text{onset}}) \cdot PS(T_{\text{onset}}) + 0 \cdot \left(1 - PS(T_{\text{onset}})\right) \\ &= PLL(T_{\text{onset}}) \cdot PS(T_{\text{onset}}), \end{aligned} \tag{11}$$

where $PS(T_{\text{onset}})$ is the probability that the malware remains undetected until time T_{onset}.

3.6. Summary of the malware attack process

The entire process of a malware-induced cyber attack in CPPS is summarized as follows:

Step 1. **Initialization and Malware Injection:** Due to the attacker's lack of global information, the system is initialized by randomly selecting a fixed proportion of the network as the observable part for the attacker. From this visible portion, the attacker selects a high-degree node and injects the malware.

Step 2. **Malware Propagation:** During the incubation period, the malware propagates silently within the communication network, following the SI model and infecting susceptible nodes.

Step 3. **Malware Detection:** At each time step, system operators attempt to detect the malware. If the malware is detected before T_{onset}, the attack fails, and the process ends.

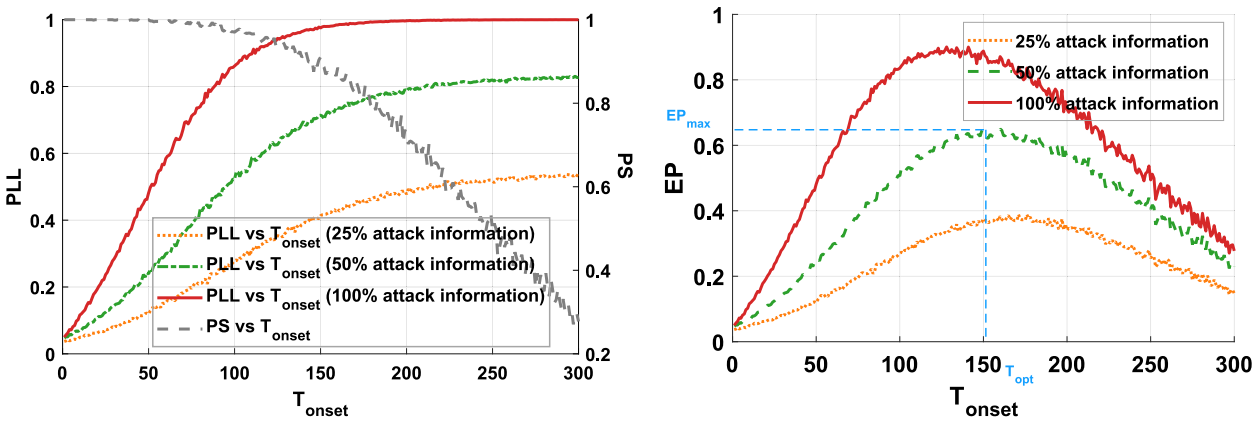

Fig. 3. Random coupling pattern: The results of PLL,PS and EP under different values of T_{onset}, considering various prior attack information.

Step 4. **Attack Launch at** T_{onset}: If the malware remains undetected beyond the propagation period, the attacker disables the power nodes linked to infected cyber nodes, causing cascading failures and widespread disruptions in the system.

Step 5. **Load Shedding:** Load shedding is employed to mitigate cascading failures and restore stability to the power network.

Step 6. **Damage Evaluation:** The PLL is calculated to quantify the impact of this attack.

4. Attack–defense costs and defense strategies

4.1. Introduction of attack–defense costs

Common antimalware methods typically require execution times on the order of milliseconds, making them technically infeasible for large-scale applications in time-critical industrial control systems such as CPPS [24,44]. Due to real-time constraints and cost considerations, it is impractical to equip every communication node with defense technologies to protect against malware infections. Attackers can often detect nodes with weaker defenses, while struggling to identify highly protected nodes employing strategies such as continuous moving target defense [28]. Therefore, in our simulation framework, we consider scenarios where defenders protect communication nodes from being detected by attackers under various defense costs. These protected communication nodes are not designated as attack injection nodes at the beginning of the attack and their corresponding power grid nodes will not be shut down during subsequent attacks.

Different attack and defense resources allocation may result in varying levels of effectiveness. These considerations can be quantified as attack and defense costs, defined as follows:

- **Attack Costs:** The attack costs represent the proportion of cyber nodes that the attacker attempts to detect.
- **Defense Costs:** The defense costs represent the number of cyber nodes that the defender seeks to protect from being detected by the attacker.

4.2. Description of defense strategies

Malware attacks on CPPS pose significant risks by exploiting vulnerabilities in communication and power networks, potentially leading to severe disruptions and catastrophic system failures. Protecting critical nodes from detection by attackers is essential, as undiscovered nodes play a vital role in maintaining system integrity. This approach includes techniques such as Moving Target Defense (MTD) [28] and IP randomization [29], which dynamically alter network configurations to reduce the likelihood of attackers identifying and targeting specific nodes, thereby enhancing overall system security.

Considering network degree and capacity, this research evaluates three distinct defense strategies, described as follows:

(1) **Defense Strategy I — Communication Degree-based Protection (CDP):** This strategy prioritizes the protection of communication nodes based on their degree, with higher-degree nodes receiving priority.

(2) **Defense Strategy II — Power Degree-based Protection (PDP):** This strategy prioritizes the protection of communication nodes that are coupled with high-degree power nodes.

(3) **Defense Strategy III — Capacity-based Protection (CP):** This strategy prioritizes the protection of communication nodes that are coupled with high-capacity power nodes.

5. Case study

This section presents case studies on a CPPS simulation model using the IEEE 118 Bus system coupled with a BA scale-free communication network, as shown on the right of Fig. 1. The simulations model malware-induced cyber attacks within these networks, analyzing the maximum potential payoff for attackers and evaluating the effectiveness of various defense strategies under different attack and defense cost scenarios. For simulation parameters, an infection rate ($\lambda = 0.01$) and a detection rate ($\beta = 0.00001$) are applied. To account for potential overload scenarios, the transmission line and generator node capacities are set to 1.5 times their normal operating power flow. For random coupling pattern, the coupling between the power and communication networks is varied across simulation runs. Each result represents the average of 1000 simulation runs, ensuring robust statistical evaluation.

5.1. Impact of incubation period on CPPS robustness with different prior information

We simulate cyber attacks launched at different T_{onset} within CPPS, where the two subnetworks are coupled according to specific coupling patterns. The simulation results for PLL and PS are presented in Fig. 3(a), with the two subnetworks randomly coupled under three levels of the attacker's limited information (25%, 50%, and 100%). Simulation results for all coupling patterns are shown in Fig. 4. The figures illustrate that malware with a longer propagation period generally leads to higher attack effectiveness (increased PLL), but this also heightens the risk of detection (decreased PS). As a result, attackers must carefully balance the tradeoff between maximizing attack effectiveness and minimizing detection risk. This balance is achieved by selecting the optimal T_{onset} based on the extent of available CPPS information.

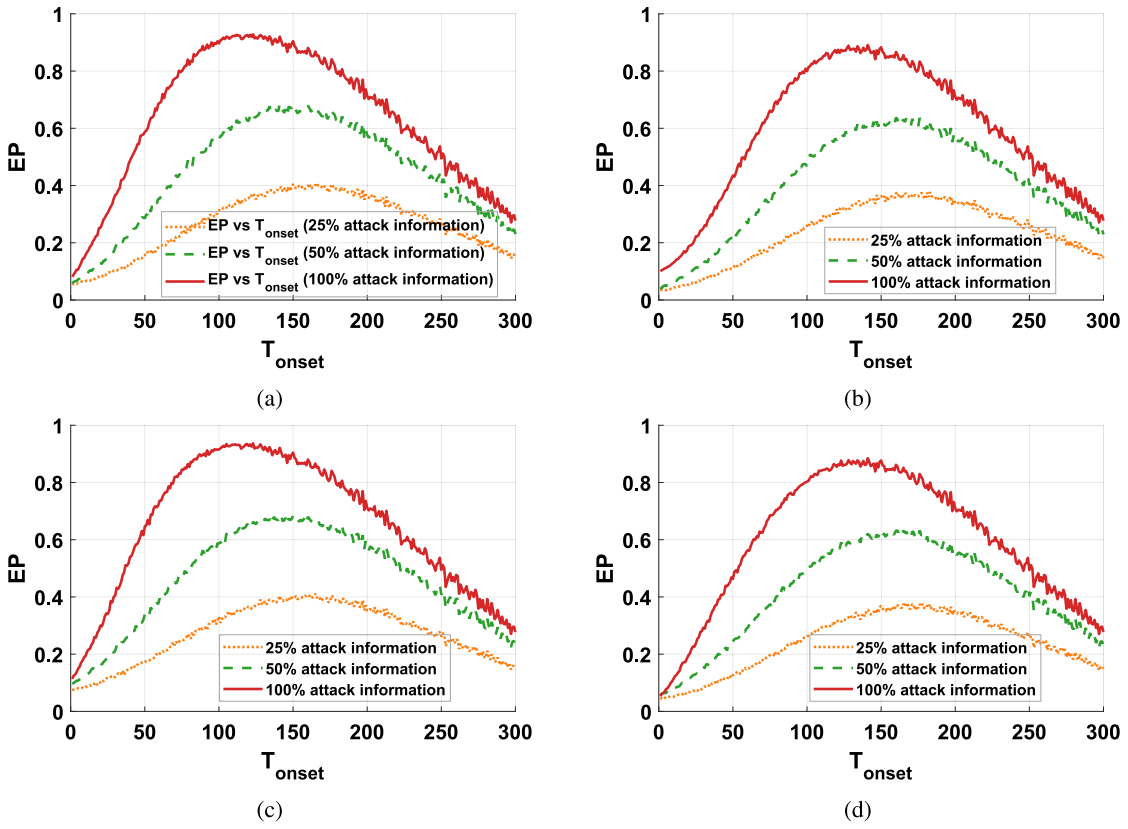

Fig. 4. Comparison of the percentage of EP as a function of T_{onset} under different coupling patterns and varying levels of the attack information. Subfigure (a) corresponds to coupling pattern DDAC, (b) to DDDC, (c) to DCAC, and (d) to DCDC.

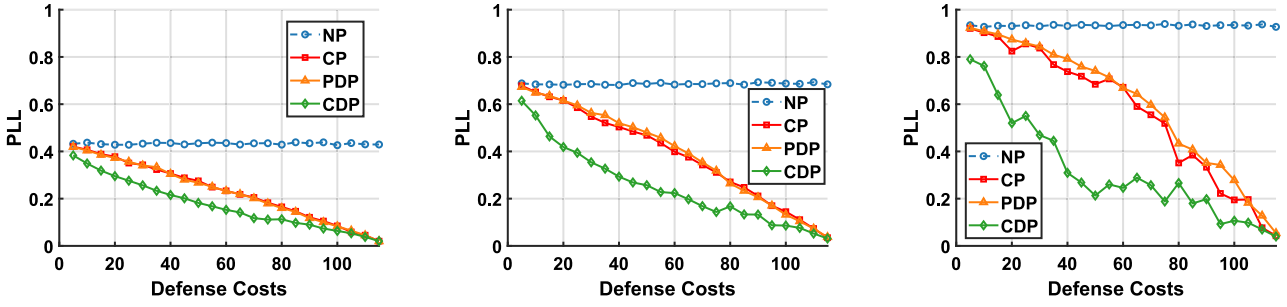

Fig. 5. Robustness comparison of different defense strategies under random coupling, considering various attack and defense costs. Subfigures (a), (b), and (c) correspond to attack costs representing 25%, 50%, and 100% of cyber nodes, respectively.

Table 2
Optimal attack timing and maximum attack payoff under different coupling patterns with varying prior attack information levels.

Coupling pattern	25% information		50% information		100% information	
	T_{opt}	EP_{max}	T_{opt}	EP_{max}	T_{opt}	EP_{max}
DDAC	161	0.40673	141	0.68744	**123**	**0.92825**
DDDC	**183**	**0.37697**	160	0.63768	141	0.89115
DCAC	161	0.41082	141	0.68835	**123**	**0.93709**
DCDC	**171**	**0.38561**	161	0.64026	141	0.88985
RC	171	0.38849	150	0.65012	128	0.90060

Fig. 3(b) shows the correlation between the attacker's expected payoff (EP) and the onset launch time (T_{onset}) for three levels of limited information (25%, 50%, and 100%) with randomly coupled subnetworks. As depicted, the relationship between EP and T_{onset} follows a non-monotonic pattern, suggesting the existence of an optimal attack time (T_{opt}) that yields the maximum expected payoff, denoted as EP_{max}. This peak EP_{max} represents the highest expected payoff achievable by the attacker. Moreover, simulation results reveal that all four coupling patterns exhibit a similar non-monotonic trend, with each pattern featuring its distinct T_{opt} and EP_{max}, as shown in Fig. 4. The specific values of T_{opt} and EP_{max} for different levels of observed information and coupling patterns are summarized in Table 2.

For a given coupling pattern, as the amount of information available to the attacker increases, T_{opt} decreases while EP_{max} increases. This indicates that more system information enables attackers to launch earlier and more effective attacks. This trend is particularly evident in assortative coupling patterns, DDAC and DCAC, which have smaller T_{opt} and larger EP_{max} compared to other patterns. These results suggest that these assortative coupling patterns make it more challenging for the power network to defend against attacks. In contrast, disassortative

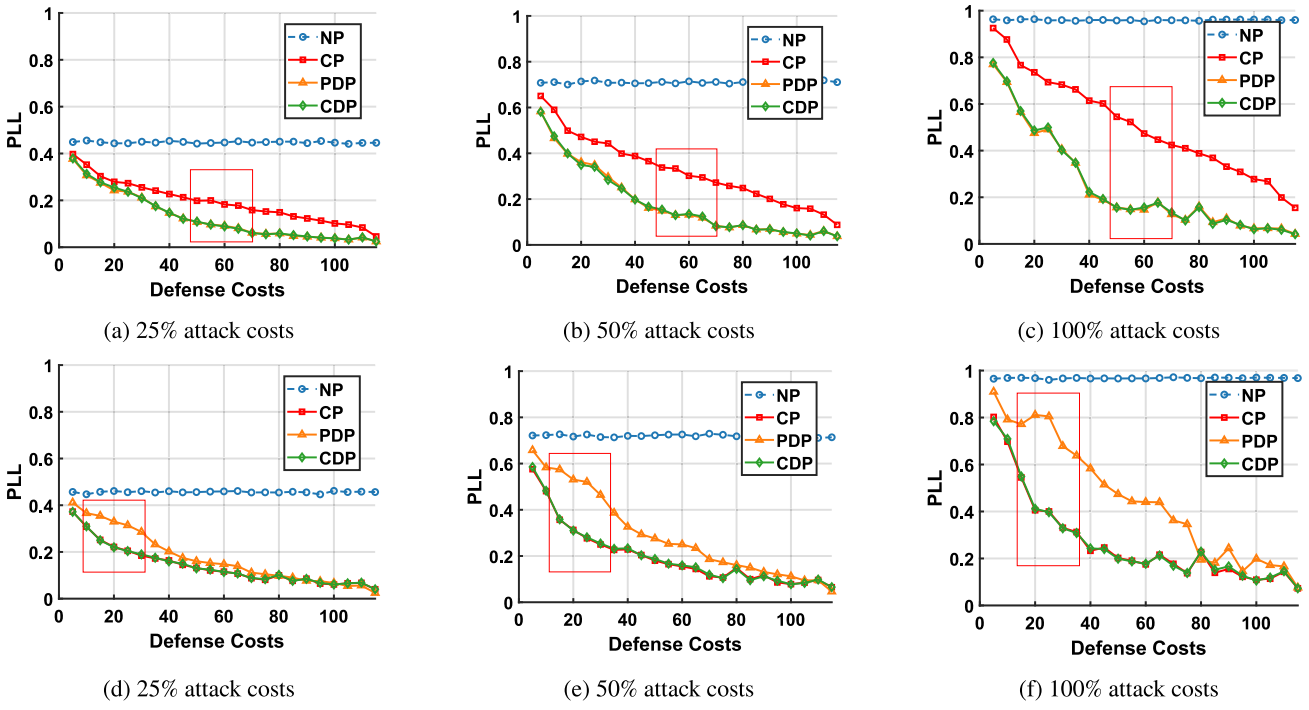

Fig. 6. Robustness comparison of different defense strategies under coupling patterns DDAC and DCAC, considering various attack and defense costs. Subfigures (a), (b), and (c) correspond to attack costs of 25%, 50%, and 100% in DDAC, while subfigures (d), (e), and (f) correspond to attack costs of 25%, 50%, and 100% in DCAC.

coupling patterns, DDDC and DCDC, exhibit larger T_{opt} and smaller EP_{max}, indicating that attackers are less effective in causing significant damage. The random coupling pattern, by comparison, lies between the assortative and disassortative patterns in terms of both T_{opt} and EP_{max}.

5.2. Attack and defense confrontation

As previously discussed, attackers rarely possess a complete view of the CPPS topology, and it is equally impractical for defenders to protect every node [24]. Given the variation in attack and defense costs (introduced in Section 4.1), this study investigates how resource allocation and coupling patterns influence the performance of three defense strategies in maintaining CPPS robustness. Specifically, we analyze the confrontation between attackers and defenders, focusing on the interplay of their respective costs.

For this purpose, both attack and defense costs are classified into three categories. Attack costs are categorized as light, moderate, and heavy, corresponding to prior attack information proportions of 25%, 50%, and 100%, respectively. Similarly, defense costs are divided into light, moderate, and heavy, based on the protection of 20, 60, and 100 nodes, respectively.

The full set comprises three different proportions of attack costs and five coupling patterns, resulting in 15 individual games, as shown in Figs. 5, 6, and 7. Specifically, each game simulates a scenario where the defender and attacker engage in a battle with varying defense costs and strategies – CDP, PDP, CP, and a no-protection strategy for comparison – corresponding to a specific coupling pattern and a particular proportion of attack costs. Additionally, the attacker launches the attack from the communication network at T_{opt}, which is determined based on the coupling pattern and the attacker's limited information, as discussed in Section 5.1. This represents the optimal attack time in the given scenario, ensuring the simulations are convincing.

Fig. 5 illustrates the effectiveness of three defense strategies and the no-protection strategy under attack costs where the attacker observes 25%, 50%, or 100% of prior CPPS information according to the random coupling pattern. The results show that, for the RC pattern, all protection strategies significantly outperform having no protection. Furthermore, the CDP strategy consistently demonstrates superior performance compared to other listed defense strategies, regardless of the defense cost.

These findings indicate that protecting high-degree communication nodes is more effective than protecting high-degree or high-capacity power nodes when the two networks are randomly coupled. Theoretically, because the cyber layer is approximately scale-free, a tiny set of hub nodes simultaneously (i) controls the majority of cyber reachability and (ii) is most likely to be coupled to high-capacity physical assets. Targeted protection of these hubs therefore raises the epidemic threshold in the cyber layer and removes the primary gateways into the physical layer. In comparison, protecting high-capacity or high-degree power nodes provides only localized defense, as malware can still propagate freely through the communication network and subsequently infiltrate the power layer via unprotected communication nodes.

5.3. Effect of critical parameters

The effectiveness of the three defense strategies varies significantly with changes in critical parameters such as coupling patterns and the resource allocation within CPPS.

From Fig. 6, it can be observed that for the DDAC coupling pattern, the effectiveness of PDP and CDP is equivalent. Notably, although both DDAC and DCAC are assortative coupling patterns, they exhibit distinct differences. In the DDAC pattern, protecting high-degree communication nodes yields the most significant improvement in enhancing CPPS robustness when defense costs are light. In contrast, for DCAC, the greatest improvement is observed when defense costs are moderate.

This phenomenon reveals that CPPS robustness is highly sensitive to the way the cyber and physical networks are coupled.

For disassortative coupling, as shown in Fig. 7, the choice of defense strategy becomes more nuanced. To analyze defense strategies against malware attacks in CPPS under disassortative coupling patterns, we first define two critical concepts:

- **Critical Point:** These critical points mark a kind of phase transition in the system's response: for example, in one coupling regime

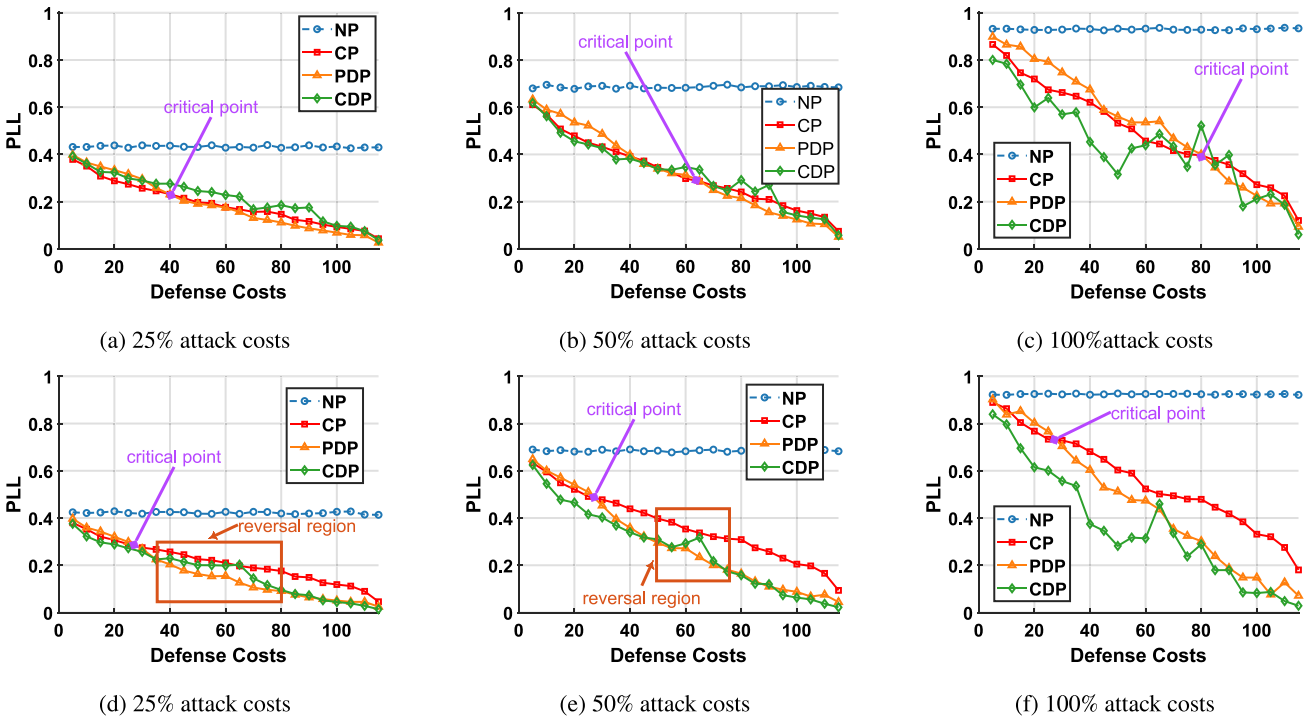

Fig. 7. Robustness comparison of different defense strategies under coupling patterns DDDC and DCDC, considering various attack and defense costs. Subfigures (a), (b), and (c) correspond to attack costs of 25%, 50%, and 100% in DDDC, while subfigures (d), (e), and (f) correspond to attack costs of 25%, 50%, and 100% in DCDC.

a minimal defense budget favors protecting high-capacity nodes (CP), but beyond a threshold, protecting nodes associated with high-degree power nodes (PDP) becomes more effective.

- **Reversal Region:** The reversal region was identified under certain coupling (DCDC) where the rank order of defense strategies flips over a range of intermediate resource levels. This counterintuitive phenomenon implies that adding more defense resources can momentarily make a previously suboptimal strategy (like PDP) outperform the strategy that was optimal at both lower and higher resource levels.

In Figs. 7(a)–7(c), corresponding to the DDDC coupling pattern, a critical point emerges. Specifically, when defense costs are light, CP outperforms PDP. However, beyond the critical point – when defense costs reach moderate or heavy levels – PDP becomes more effective than CP. Furthermore, as attack costs increase from light to moderate or heavy, the critical point shifts, occurring only at higher defense costs. In Figs. 7(d)–7(f), corresponding to the DCDC coupling pattern, both a critical point and a reversal region are observed. As shown in Figs. 7(d) and 7(e), the reversal region typically appears when attack costs are light or moderate and shrinks as attack costs approach heavy levels. This region also arises at higher defense costs (i.e., moderate or heavy). Unlike the DDDC pattern, the critical point for DCDC occurs at relatively light defense costs and remains relatively stable across different attack cost levels.

The existence of such critical points and reversal regions highlights a deeply nonlinear and non-monotonic response in the CPPS: the system's robustness does not improve uniformly with additional defense investment, but rather depends on the distribution of that investment across different node types in subtle ways. These insights contribute to theory by revealing how resource allocation ratios (attack vs. defense) interact with network topology to produce emergent behavior. Specifically, CPPS exhibits tipping-point behavior common in complex networks, where defense measures have diminishing returns until a pivotal amount is reached, after which the marginal benefit can change dramatically. The result also emphasizes that protecting seemingly less obvious targets (e.g. communication nodes linked to high-degree power nodes in certain scenarios) can be more beneficial than intuitively critical ones (high-degree communication nodes), under specific conditions, thus exposing the mechanistic interplay between cyber–physical network structure and adaptive attack–defense dynamics.

6. Conclusion

This study presents a comprehensive simulation framework for systematically analyzing the robustness of CPPS under malware attacks in a network science perspective. In contrast to previous studies that considered limited scenarios, the proposed framework incorporates the influences of the malware's incubation period, incomplete information, coupling patterns and the reconnaissance-evasion behavior. Using this framework, we evaluate the tradeoff between the malware incubation duration and the attack success rate to determine the optimal attack timing. Additionally, we investigate the impact of system parameters on CPPS robustness across different attack–defense scenarios.

Our findings indicated that disassortative coupling patterns were identified as a promising approach to mitigate the impact of malware and enhance overall system robustness. Moreover, our experimental results reveal some interesting phenomena: protecting seemingly less obvious targets can be more beneficial than intuitively critical ones. The defender must dynamically adjust the resource allocation as the relative attack–defense budget evolves, whereas in an assortatively coupled CPPS a nearly static allocation of defensive resources achieves optimal robustness. These insights provide concrete, cost-effective guidelines for strengthening the robustness of CPPS. As future work, we plan to incorporate finer-grained communication layer modeling to improve realism while preserving the core architecture of our prior work.

CRediT authorship contribution statement

Jinfu Zhang: Writing – original draft, Methodology, Data curation, Software, Formal analysis. **Haicheng Tu:** Writing – original draft, Supervision, Funding acquisition, Writing – review & editing, Validation, Methodology, Conceptualization. **Yongxiang Xia:** Visualization, Supervision, Writing – review & editing, Validation. **Xuetao Yang:** Writing – review & editing, Validation. **Yibo Zhu:** Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was supported by National Natural Science Foundation of China under Grant No. 62403174 and the Hangzhou Key Scientific Research Program Project [Grant No. 2024SZD1A24] for "Research and Application of Key Technologies for Intelligent Decision-Making Based on Industry Big Data—A Power Big Data Approach".

Data availability

Data will be made available on request.

References

[1] Ding X, Wang H, Zhang X, Ma C, Zhang H-F. Dual nature of cyber–physical power systems and the mitigation strategies. Reliab Eng Syst Saf 2024;244:109958.
[2] Alvarez-Alvarado MS, Apolo-Tinoco C, Ramirez-Prado MJ, Alban-Chacón FE, Pico N, Aviles-Cedeno J, Recalde AA, Moncayo-Rea F, Velasquez W, Rengifo J. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Comput Electr Eng 2024;116:109149.
[3] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proc IEEE 2011;100(1):210–24.
[4] Zhao T, Tu H, Jin R, Xia Y, Wang F. Improving resilience of cyber–physical power systems against cyber attacks through strategic energy storage deployment. Reliab Eng Syst Saf 2024;252:110438.
[5] Tu H, Gu F, Zhang X, Xia Y. Robustness analysis of power system under sequential attacks with incomplete information. Reliab Eng Syst Saf 2023;232:109048.
[6] Yohanandhan RV, Elavarasan RM, Manoharan P, Mihet-Popa L. Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. IEEE Access 2020;8:151019–64.
[7] Presekal A, Rajkumar VS, Ştefanov A, Pan K, Palensky P. Cyberattacks on power systems. In: Smart cyber-physical power systems: fundamental concepts, challenges, and solutions. Vol. 1, Wiley Online Library; 2025, p. 365–403.
[8] Zhang Y, Fei M, Du D, Hu Y. Security state assessment in cyber-physical systems post-DoS attack based on cyber layer partitioning. IEEE Trans Ind Inform 2025;21(3):2204–13.
[9] Lu K-D, Wu Z-G, Huang T. Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems. IEEE/ASME Trans Mechatronics 2022;28(2):1137–48.
[10] Lu K-D, Wu Z-G. Constrained-differential-evolution-based stealthy sparse cyber-attack and countermeasure in an AC smart grid. IEEE Trans Ind Inform 2021;18(8):5275–85.
[11] Singh NK, Mahajan V. Analysis and evaluation of cyber-attack impact on critical power system infrastructure. Smart Sci 2021;9(1):1–13.
[12] Sreejith A, Shanti Swarup K. MITRE ATT&CK for smart grid cyber-security. In: Cyber-security for smart grid control: vulnerability assessment, attack detection, and mitigation. Springer; 2024, p. 59–73.
[13] Li X, Xu Q, Lu X, Lin M, Chen C, Guan X. Distributionally robust coordinated defense strategy for time-sensitive networking enabled cyber–physical power system. IEEE Trans Smart Grid 2024;15(3):3278–87.
[14] Xu Q, Li X, Jiang Y, Zhu S, Chen C, Yang B, Guan X. Transportation-energy-communication integrated management of ship cyber-physical systems against cyber attacks. IEEE Trans Smart Grid 2025;16(3):2518–28.
[15] Yuan H, Yuan Y, Zhong Y, Xia Y. Incomplete information-based resilient strategy design for cyber-physical systems under stochastic communication protocol. IEEE Trans Ind Electron 2024;71(11):14967–76.
[16] Whitehead DE, Owens K, Gammel D, Smith J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In: 2017 70th annual conference for protective relay engineers. CPRE, IEEE; 2017, p. 1–8.
[17] Kong X, Lu Z, Guo X, Zhang J, Li H. Resilience evaluation of cyber-physical power system considering cyber attacks. IEEE Trans Reliab 2023.
[18] Presekal A, Ştefanov A, Rajkumar VS, Semertzis I, Palensky P. Advanced persistent threat kill chain for cyber-physical power systems. IEEE Access 2024;12:177746–71.
[19] Presekal A, Ştefanov A, Semertzis I, Palensky P. Spatio-temporal advanced persistent threat detection and correlation for cyber-physical power systems using enhanced GC-LSTM. IEEE Trans Smart Grid 2025;16(2):1654–66.
[20] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010;464(7291):1025–8.
[21] Xi Z, Liu D, Zhan C, Tse CK. Effects of cyber coupling on cascading failures in power systems. IEEE J Emerg Sel Top Circuits Syst 2017;7(2):228–38.
[22] Lai R, Qiu X, Wu J. Robustness of asymmetric cyber-physical power systems against cyber attacks. IEEE Access 2019;7:61342–52.
[23] Wang T, Wei X, Huang T, Wang J, Valencia-Cabrera L, Fan Z, Pérez-Jiménez MJ. Cascading failures analysis considering extreme virus propagation of cyber-physical systems in smart grids. Complexity 2019;2019(1):7428458.
[24] Xu S, Xia Y, Shen H-L. Cyber protection for malware attack resistance in cyber-physical power systems. IEEE Syst J 2022;16(4):5337–45.
[25] Xu S, Tu H, Xia Y. Resilience enhancement of renewable cyber–physical power system against malware attacks. Reliab Eng Syst Saf 2023;229:108830.
[26] Qi Y, Gu Z, Li A, Zhang X, Shafiq M, Mei Y, Lin K. Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems. Comput Electr Eng 2023;108:108660.
[27] Zhao T, Tu H. Impact analysis of diverse prior information and protection cost on attack efficiency in cyber-physical power system. In: 2024 IEEE 7th advanced information technology, electronic and automation control conference. IAEAC, Vol. 7, IEEE; 2024, p. 1540–4.
[28] Zhang T, Xu C, Shen J, Kuang X, Grieco LA. How to disturb network reconnaissance: a moving target defense approach based on deep reinforcement learning. IEEE Trans Inf Forensics Secur 2023.
[29] Xu X, Hu H, Liu Y, Tan J, Zhang H, Song H. Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack. Digit Commun Netw 2022;8(3):373–87.
[30] Zang T, Wang Z, Wei X, Zhou Y, Wu J, Zhou B. Current status and perspective of vulnerability assessment of cyber-physical power systems based on complex network theory. Energies 2023;16(18):6509.
[31] Powell L. Power system load flow analysis. 2005, (No Title).
[32] Xu S, Xia Y, Shen H-L. Analysis of malware-induced cyber attacks in cyber-physical power systems. IEEE Trans Circuits Syst II: Express Briefs 2020;67(12):3482–6.
[33] Xiang M, Qu Q. A congestion control strategy for power scale-free communication network. Appl Sci 2017;7(10):1054.
[34] Cai Y, Cao Y, Li Y, Huang T, Zhou B. Cascading failure analysis considering interaction between power grids and communication networks. IEEE Trans Smart Grid 2015;7(1):530–8.
[35] Barabási A-L, Albert R. Emergence of scaling in random networks. Science 1999;286(5439):509–12.
[36] Li ZS, Wu G, Cassandro R, Wang H. A review of resilience metrics and modeling methods for cyber-physical power systems (CPPS). IEEE Trans Reliab 2024;73(1):59–66. http://dx.doi.org/10.1109/TR.2023.3339388.
[37] Chen Z, Du W-B, Cao X-B, Zhou X-L. Cascading failure of interdependent networks with different coupling preference under targeted attack. Chaos Solitons Fractals 2015;80:7–12.
[38] Cai Y, Li Y, Cao Y, Li W, Zeng X. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. Int J Electr Power Energy Syst 2017;89:106–14.
[39] Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S, Adhikari U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans Smart Grid 2013;4(1):235–44.
[40] Wang Y, Wen S, Xiang Y, Zhou W. Modeling the propagation of worms in networks: A survey. IEEE Commun Surv Tutor 2013;16(2):942–60.
[41] Aminifar F, Fotuhi-Firuzabad M, Shahidehpour M, Safdarian A. Impact of WAMS malfunction on power system reliability assessment. IEEE Trans Smart Grid 2012;3(3):1302–9.
[42] Löfberg J. YALMIP: A Toolbox for Modeling and Optimization in MATLAB. In: Proceedings of the CACSD conference. Taipei, Taiwan; 2004, URL: https://yalmip.github.io.
[43] Gurobi Optimization, LLC. Gurobi optimizer reference manual. 2024, URL: https://www.gurobi.com.
[44] Falco JA, Hurd S, Teumim D. Using host-based anti-virus software on industrial control systems: Integration guidance and a test methodology for assessing performance impacts. Washington, DC, USA: U.S. Dept. Commerce, National Inst. Stand. Technol.; 2006, http://dx.doi.org/10.6028/nist.sp.1058.