Game-theoretical Model for Dynamic Defense Resource Allocation in Cyber-physical Power Systems Under Distributed Denial of Service Attacks

Bingjing Yan, Pengchao Yao, Tao Yang, Boyang Zhou, and Qiang Yang, *Senior Member*, *IEEE*

***Abstract*—Electric power grids are evolving into complex cyber-physical power systems (CPPSs) that integrate advanced information and communication technologies (ICTs) but face increasing cyberspace threats and attacks. This study considers CPPS cyberspace security under distributed denial of service (DDoS) attacks and proposes a nonzero-sum game-theoretical model with incomplete information for appropriate allocation of defense resources based on the availability of limited resources. Task time delay is applied to quantify the expected utility as CPPSs have high time requirements and incur massive damage DDoS attacks. Different resource allocation strategies are adopted by attackers and defenders under the three cases of attack-free, failed attack, and successful attack, which lead to a corresponding consumption of resources. A multidimensional node value analysis is designed to introduce physical and cybersecurity indices. Simulation experiments and numerical results demonstrate the effectiveness of the proposed model for the appropriate allocation of defense resources in CPPSs under limited resource availability.**

***Index Terms*—Game theory, complex cyber-physical power system (CPPS), multidimensional evaluation, distributed denial of service (DDoS) attack.**

I. Introduction

THE modern power grid is evolving toward complex cyber-physical power systems (CPPSs) consisting of the production, transmission, and distribution of power energy, which is expected to achieve operational reliability, flexibility, and economy [1]. However, due to the massive integration of advanced information and communication technologies (ICTs) such as wide-area measurement systems (WAMSs), supervisory control and data acquisition (SCADA) systems, and advanced metering infrastructures (AMIs), CPPSs are increasingly vulnerable to emerging threats posed not only by the physical environment but also by cyberspace components [2]. In the case of the Ukraine power grid hack, the attackers used cyberattacks to hinder severely the system recovery procedure [3], indicating the vulnerability and importance of CPPSs.

It is agreed that cyberspace attacks such as distributed denial of service (DDoS) [4], authentication [5], and injection [6] attacks may significantly affect the reliable and safe operational process of physical systems or even lead to fatal failures [7]. The DDoS attack is currently one of the most prevalent threats to industry because of its low cost [8]. This confirms the consensus that security does not imply that an attack is impossible but that the price of an attack is greater than its expected reward. In addition, conventional defense strategies and tools such as firewalls, encryption algorithms, and physical isolation cannot ensure the security of power systems under cyberattacks [9].

To address these technical challenges, considerable research efforts have been made to exploit CPPS vulnerabilities from different aspects, including impact quantification of cyberattacks on the power grid [10], [11], attack models [12], and cyber-physical interdependence analysis based on co-simulation testbeds [13], [14]. However, these studies have mainly been conducted only from the attacker's perspective, and the effects of cyber attacks on CPPSs have been analyzed and quantified on the premise that the attacks are successful. To analyze the strategy choice problems among multiple parties, game theory is considered an efficient paradigm for the analysis of cyber-physical system (CPS) defense [15]-[20]. Although both the attacker and defender are considered, these studies mainly focus on communication systems, which means only the cyber layer is considered. However, physical and cyber components are deeply intertwined in a CPPS, which means that attackers and defenders must consider the physical components in the game process. Our previous study [21] proposed a dynamic cyber-physical security defensive strategy based on game theory.

Manuscript received: August 18, 2022; revised: December 9, 2022; accepted: March 31, 2023. Date of CrossCheck: March 31, 2023. Date of online publication: May 25, 2023.

This work was supported by the "Pioneer" and "Leading Goose" R&D Program of Zhejiang (No. 2022C01239), National Natural Science Foundation of China (No. 52177119), and Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform).

B. Yan, P. Yao, T. Yang, and Q. Yang (corresponding author) are with the College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: yanbj@zju.edu.cn; pcyao@zju.edu.cn; 21910107@zju.edu.cn; qyang@zju.edu.cn).

B. Zhou is with Zhejiang Lab, Hangzhou 311100, China (e-mail: zhouby@zhejianglab.com).

DOI: 10.35833/MPCE.2022.000524

Physical safety targets and cybersecurity indices were introduced, and the asset value was analyzed multidimensionally. However, the study did not fully consider the specific manifestations of the attacks and their adverse effects on CPSs.

Therefore, the motivation of this study is to analyze the node value from multidimensional factors based on the cyber-physical coupling characteristics of CPPSs while fully considering the interactions between the attacker and defender based on a game-theory framework.

Accordingly, this study proposes a game-theoretical model for dynamic defense resource allocation in CPPSs under DDoS attacks. The operations of CPPSs are time sensitive, and thus a physical system node such as a programmable logic controller (PLC) or an interchanger is considered depleted when its task time delay exceeds a certain threshold, which can be quantified as the impact of an attack. A nonzero-sum game model with incomplete information is established to calculate the expected utility of each player under rationality from the two perspectives of resource consumption and value of the physical system node. Different strategies are adopted by the players (i.e., attacker and defender) under various conditions of attack-free, failed attack, and successful attack, resulting in corresponding resource consumption. In the attack-free case, the system node operates in a normal state, and the defender consumes only maintenance resources while the attacker consumes no resources. In a failed attack, the system node continues to operate normally despite the resources used by the attacker, whereas the defender consumes additional resources for defense. In the case of a successful attack, the system node cannot operate normally, whereas the attacker and defender both consume resources based on their respective strategies.

The value of a node is calculated by integrating the physical and cybersecurity indices derived from multiple dimensions. The significance of the node itself and the influence of superiors and subordinates are among the node weights. The attack complexity is mainly influenced by the attack strategy (i.e., path complexity, concealment, and attack potential), which is described in the common vulnerability scoring system (CVSS) [22] as well as the series level, which is determined by the connected node devices. Security is measured by the three indicators of confidentiality, integrity, and reliability, which are represented by service unavailability, privacy violation, information manipulation, authority hijacking, and aberrant device performance. When a node functions appropriately, the resource allocation has the most significant effect on the intensity of the defense.

Simulation experiments are conducted to evaluate the proposed game-theoretical model for dynamic defense resource allocation, and numerical results confirm its effectiveness in identifying appropriate strategies. The main technical contributions of this study are as follows.

1) This study develops a game-theoretical model to support the decision-making of defense resource allocation in CPPSs under DDoS attacks, and the time delay reflected by the node state is applied to quantify the efficiency of the strategy.

2) The proposed solution fully considers defense resource consumption as a metric under three conditions (attack-free, failed attack, and successful attack) and multidimensional factors (node weight, attack complexity, security property, and defensive intensity).

3) The appropriate resource allocation is obtained dynamically by achieving the attacker-defender Nash equilibrium under limited defense resources.

The remainder of this paper is organized as follows. Section II presents related work in terms of CPS security. A detailed description of the proposed game-theoretical model is provided in Section III. The simulation experiments and the numerical results are presented in Section IV. Finally, concluding remarks are presented in Section V.

II. Related Work in Terms of CPS Security

In previous studies, considerable efforts have been made toward CPSs that integrate mutually interacting physical and cyber systems [23]. Cyberspace systems that rely on underlying information and communication systems support the comprehensive perception and timely management of physical systems and face growing cyberspace threats [24].

In [10], the effects of cyberattacks were exploited on power grid voltage management performance, proving the huge impact of cyberattacks on various areas from the cyber domain to the physical world and particularly in CPPSs. To exploit the correlation between the switching vulnerability and structure of the power grid, flexible co-simulation frameworks were provided to simulate cyber-physical switching problems [12], [13]. Reference [25] indicated that DDoS attacks can inexpensively flood a system. Several attack strategies emphasizing the increasing number and method diversity of DDoS attacks were proposed in [26], [27]. In [28], a representative system was developed to analyze security risks based on software-defined networking, and the cyberspace risks of denial of service (DoS) attacks on intelligent electronic devices and communication networks were calculated. In [29], a comprehensive study was presented to evaluate power grid resilience against DDoS attacks, thus providing a theoretical basis for quantifying the effects of DDoS attacks on CPPSs.

Game theory offers a quantifiable and understandable foundation for implementing active defensive strategies under uncertainty in several fields such as optimal energy demand analysis and Internet of Things networks [30]-[32]. In addition, game-theoretical research toward CPS security has been conducted. To acquire up-to-date attack response strategies and timely risk evaluation, [33] devised a finite-horizon semi-Markov game between the engineer and aggressor. In [16], a dynamic game paradigm was proposed to describe interactions in CPSs. In [20], a Bayesian game approach was formulated to schedule the energy consumption of residential communities in response to peak-load shifts. Reference [15] described a risk decision-making approach based on a stochastic game model to define the relationship between players in industrial cyber-physical systems (ICPSs). In [34], a defense technique based on a dynamic Bayesian game model was proposed to investigate false data injection attacks on power systems. In [19], the operational risks and vulnerabilities of CPPSs in two possible cyberattack scenarios were discussed.

Although extensive research efforts have been made in defense strategies for communication systems (i.e., in the insurance of cyberspace security), researchers generally agree that security of industrial power systems cannot be assured because of the operational couplings of CPSs. In addition, most existing studies have mainly focused on analyzing attacker behavior or defender strategies without fully considering their sophisticated interactions. The resource using of attackers and defenders as well as information gained from counterparties that significantly affects attack and defensive performances require further research.

III. Detailed Description of Proposed Game-theoretical Model

In this study, a three-layer CPPS structure and node characteristics are adopted, as suggested in [16] and [35]. The construction of the game-theoretical model and an update to the belief index are then presented. The overall architecture of the proposed game-theoretical model against DDoS attacks in terms of CPPSs is shown in Fig. 1.

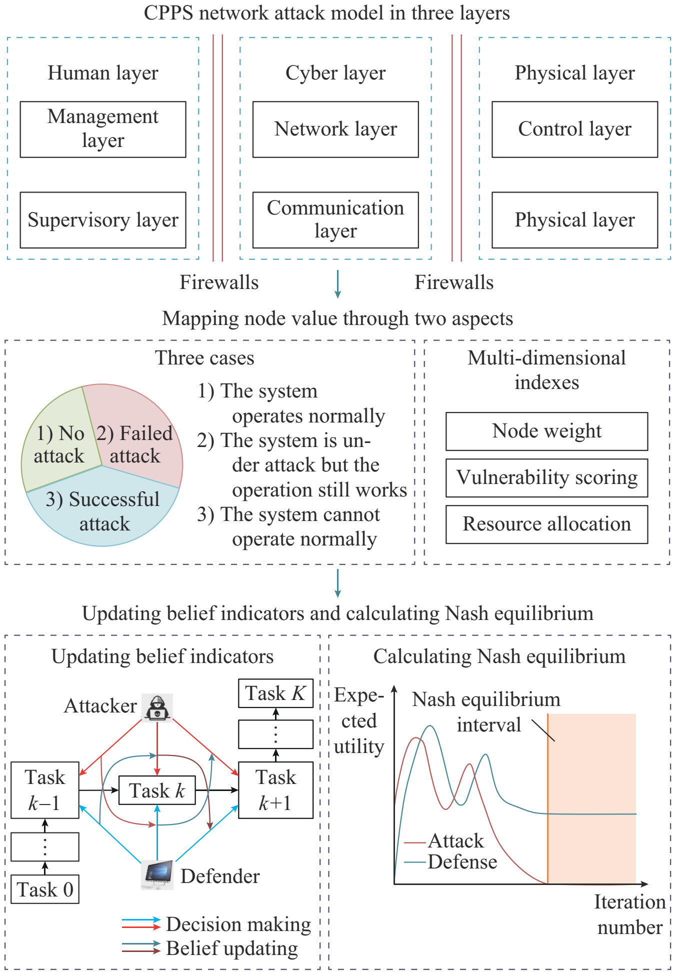


Fig. 1. Overall architecture of proposed game-theoretical model against DDoS attacks in terms of CPPSs.

A. DDoS Attack Model

Unlike traditional information and communication networks, complex CPPSs generally contain extensive physical devices with limited computing capacity, low memory, and insufficient storage capacity. Decisions related to specific tasks such as perception, measurement, and execution are generally made in the human layer and delivered through the cyber layer. The strict requirements for time delay and the presence of relay protection in the power system allow attackers to interrupt or otherwise affect information transmission through attacks such as DDoS, which may lead to contingencies in CPPS operations. Impact of DDoS attacks generally falls into the two categories of excessive delay and resource depletion [27]. Excessive delay occurs when extensive interference packets are injected to congest the network bandwidth such that legitimate commands cannot be delivered between nodes. Resource depletion occurs when the central processing unit (CPU) receives illegal commands, which exhausts the memory of nodes or causes the cores to be occupied and thus unable to provide corresponding services. Attackers can generate large-scale system disruptions with a minor cost when targeting the communication channel of a specific node, delaying the execution of tasks by the device, or obfuscating the device state. During an attack, a significant communication delay is added to all packets. The sensing equipment continues to use the previous data such that the bad input allows the application to give an incorrect response. Finally, the wrong control action is returned to the power system, leading to a severe accident such as the 2011 San Diego blackout.

The attack process can be considered a multistage process [36]. In the first step, the attacker performs reconnaissance of the system to obtain prior knowledge, including information about vulnerable devices, which is incomplete because of the protective measures of the defender. Some reconnaissance strategies such as hit list scanning, topological methods, permutation scanning, and local subnet scanning are popular or have the potential to deploy DDoS attacks [37]. The appropriate attack target is then selected through analysis based on this knowledge, and DDoS attack methods are used. Examples include the synchronize sequence number (SYN) flooding attack [38] and internet control message protocol (ICMP) attack [39]. References [40] and [41] described wired and wireless DDoS attack methods and demonstrated the feasibility of remote DDoS attacks that can be conducted at low rates even when the attacker cannot get close to the power grid or directly access a wired network. Finally, the attacker evaluates the utility after the initial malicious attack and begins the next round of reconnaissance.

The decision-making layer may isolate or directly cut off the faulty part due to relay protection when a signal is received from a node under attack. Researchers have investigated many efficient detection methods against DDoS attacks [8], [25], [42] and demonstrated that the essential issue of DDoS attacks and defense is resource competition between attackers and defenders.

B. Game-theoretical Model

Considering the uncertainty in attacker behavior and the complexity of CPPSs, a game-theoretical model based on incomplete information is established. A dynamic game for defense strategy (DGDS) G contains five elements of players, strategy profiles, tasks, expected utilities, and belief indices, which are denoted as M, Φ, K, U, and B, respectively.

$$G = \langle M, \Phi, K, U, B \rangle \tag{1}$$

Player a is the attacker and player d is the defender (i.e., control center). The finite sets Φ_a and Φ_d are used to encompass the selected strategies of the players, which can be mapped to resource consumption. K is the set of tasks k. The reward is adjusted, and the expected cumulative utility $(U_{a,k}^n; U_{d,k}^n)$ is established for each task k. For example, $\varphi_{a,k}^3$ refers to the strategy of the attacker in node 3 at task k based on the available information $(b_{a,k} \in B_{a,k}, b_{d,k} \in B_{d,k})$, which means that the attacker denotes the corresponding resource consumption $r_{a,k}^3$. $B_{a,k}$ and $B_{d,k}$ are the available information of attacker and defender, respectively. The specific strategies of attackers may include changing the DDoS attack methods (e.g., SYN flooding and ICMP attacks), increasing the attack intensity and attack surface [43]. As this study is based on the defender's perspective, the computing resources of the attacker are mapped to the attack traffic rate [18] because no universal standard exists for quantifying different attack methods. The specific strategies of defenders include bandwidth inflation, static blocking, and rate limiting [17], [27]. Accordingly, the computing resources of the defender are quantified as the resource budgets of the CPU, memory, and bandwidth of the user.

Players acquire greater knowledge as the game proceeds by assessing each other's strategies and rewards from previous tasks. Belief indices are formed to quantify the probability of other player's strategies. An initial distribution $(b_{a\to d,0}^n; b_{d\to a,0}^n)$ with a random variable is created as the other player's strategy at the beginning of the task and is updated at each task.

The resource consumption $(r_{a,k}^n; r_{d,k}^n)$ is normally assumed to be proportional to the strategies $(\varphi_{a,k}^n; \varphi_{d,k}^n)$. However, better results can be achieved with more appropriate strategies when sufficient prior knowledge $(b_{a\to d,k}^n; b_{d\to a,k}^n)$ is obtained.

C. Dynamic Game-based Solution

Because the CPPS is time-sensitive, a node is considered depleted when its task time delay exceeds a certain threshold. The attacker (i.e., the malicious device that attempts to disrupt the normal operational node) compromises as many nodes as possible at a favorable cost. By contrast, the defender (i.e., the control center) expects the system to operate normally to reduce system losses. A system is considered to have an exponential distribution of the service duration $\lambda_{d,k}$, and the duration of a task t_k depends on the service efficiency ς_e and resource consumption budget v_r [17].

Two types of operational modes are used in a network node: normal and risk. A node is considered to operate normally when its task time delay is below the time threshold t_{th}. The probability of the normal mode is calculated as:

$$P_{d,k} = P(t_k \le t_{th}) = \int_0^{t_{th}} \lambda_{d,k} \mathrm{e}^{-\lambda_{d,k} t_k} \mathrm{d}t_k \tag{2}$$

A node is considered attacked when its task time delay exceeds the time threshold t_{th}. The probability of the risk mode is calculated as:

$$P_{a,k} = P(t_{th} < t_k) = 1 - \int_0^{t_{th}} \lambda_{d,k} \mathrm{e}^{-\lambda_{d,k} t_k} \mathrm{d}t_k \tag{3}$$

Two states of attacks can occur under the normal mode: failed attack and attack-free. The probabilities of failed attack $P_{af,k}$ and attack-free $P_{nf,k}$ are calculated as:

$$P_{af,k} = P(t_k \le \delta) = \int_0^{\delta} \lambda_{af,k} \mathrm{e}^{-\lambda_{af,k} t_k} \mathrm{d}t_k \tag{4}$$

$$P_{nf,k} = P(\delta < t_k \le t_{th}) = \int_{\delta}^{t_{th}} \lambda_{nf,k} \mathrm{e}^{-\lambda_{nf,k} t_k} \mathrm{d}t_k \tag{5}$$

where δ is the balancing factor used to express these two states of attacks, which is similar to that used in [44]; $\lambda_{af,k}$ is the service duration rate when the device is under attack but the attack fails; and $\lambda_{nf,k}$ is the service duration rate when the device is not under attack.

In the case of a high task time delay, the node changes its defensive strategy and resource consumption budget r_d', and the corresponding task duration t_k' changes accordingly. The resource consumption budgets corresponding to the normal and risk modes are as follows:

$$\begin{cases} r_{d,k} = \displaystyle\int_0^{t_{d,k}} r_d \mathrm{d}t_k + \int_0^{t_{a,k}} r_d' \mathrm{d}t_k' \\ t_{d,k} = \displaystyle\sum_{t_i \in \{t_k | t_k < t_{th}\}} t_i \\ t_{a,k} = \displaystyle\sum_{t_i \in \{t_k | t_k \ge t_{th}\}} t_i \end{cases} \tag{6}$$

where $r_{d,k}$ is the resource consumption budget for a node at task k; r_d is the resource consumption budget for a node; $t_{a,k}$ is the period of the attacker acting; and $t_{d,k}$ is the period of the defender acting.

The attack resource consumption budget is r_0 for the period of the attack-free case. In addition, r_a and r_a' denote the attack resources when a trial attack is sent but fails and when the attack succeeds, respectively. The total consumed resource is calculated as:

$$\begin{cases} r_{a,k} = \displaystyle\int_0^{t_{nf,k}} r_0 \mathrm{d}t_k + \int_0^{t_{af,k}} r_a \mathrm{d}t_k + \int_0^{t_{a,k}} r_a' \mathrm{d}t_k' \\ t_{nf,k} = \displaystyle\sum_{t_i \in \{t_k | t_k < \delta\}} t_i \\ t_{af,k} = \displaystyle\sum_{t_i \in \{t_k | \delta \le t_k < t_{th}\}} t_i \\ t_{a,k} = \displaystyle\sum_{t_i \in \{t_k | t_k \ge t_{th}\}} t_i \end{cases} \tag{7}$$

where $t_{nf,k}$ is the period of attack-free; and $t_{af,k}$ is the period when a trial attack is sent but fails.

D. Update of Belief Index and Cumulative Utility

Traditional defensive strategies require historical data to establish blocklists [45]. In this study, a belief index is introduced to assume the information obtained from a counterparty and to simulate the behavior under an active defense. A higher belief index indicates that the attacker or the defender has obtained sufficient prior knowledge, and a better strategy is adopted with an excellent effect and low resource consumption.

Players establish the belief $(b^n_{a\to d,k}; b^n_{d\to a,k})$ at task k, which can be retrieved from the supplied knowledge at task $k-1$. Insufficient previous knowledge exists for obtaining a belief index in the initial task $k=0$, and therefore the belief distribution $(b^n_{a\to d,0}; b^n_{d\to a,0})$ is based on historical experiences or a stochastic strategy. The Bayesian rule is used to update the belief in each task.

The belief index update can be regarded as a Markov renewal process in which the belief at task k is dictated by the information at task $k-1$:

$$b^n_{a\to d,k}=\begin{cases}(1-\alpha)b^n_{a\to d,k-1}+\alpha\varphi^n_{d,k-1} & \Delta>0\\ b^n_{a\to d,k-1} & \Delta\leq 0\end{cases} \tag{8}$$

$$b^n_{d\to a,k}=\begin{cases}(1-\beta)b^n_{d\to a,k-1}+\beta\varphi^n_{a,k-1} & \Delta>0\\ b^n_{d\to a,k-1} & \Delta\leq 0\end{cases} \tag{9}$$

$$\Delta=P^n_{af,k}+P^n_{a,k} \tag{10}$$

where $P^n_{af,k}$ is the probability of the failed attack at task k of node n; $P^n_{a,k}$ is the probability of the risk mode at task k of node n; and the constants α and β represent the capabilities of the attacker and the defender, respectively. Higher α and β indicate that the players are more skilled and can be considered to have acquired more prior knowledge and offered a more efficient strategy [16].

The attacker wants to compromise as many nodes as possible with positive utilities, whereas the defender wants the system to operate normally, at least within a certain threshold, to reduce system losses under limited resources. For the attacker, the revenue $R^n_{a,K}$ is the aggregate of the values of node n that do not work properly:

$$R^n_{a,K}=\sum_{k=0}^{K}V^nP^n_{a,k} \tag{11}$$

where V^n is the value of node n, and its specific calculation is examined in Section III-E.

For the defender, the revenue $R^n_{d,K}$ is the aggregate of the values of node n working normally:

$$R^n_{d,K}=\sum_{k=0}^{K}V^nP^n_{d,k} \tag{12}$$

where $P^n_{d,k}$ is the probability of the normal mode at task k of node n. For each node n, the expected utilities of the defender and attacker $U^N_{a,K}$ and $U^N_{d,K}$ are the revenue minus resource consumption, which can be expressed as:

$$U^N_{a,K}=\sum_{n=1}^{N}(R^n_{a,K}-r^n_{a,K}) \tag{13}$$

$$U^N_{d,K}=R^n_{d,K}-r^n_{d,K} \tag{14}$$

The bimatrix game is thought to encompass nonzero-sum game circumstances in which the conclusion of a decision process does not always indicate the amount one player earns and the other loses [46].

For any $\varphi^n_{d,k}$, a fixed strategy $\tilde{\varphi}^n_{a,k}$ exists such that $\tilde{U}^N_{a,K}$ is the maximum value, and for any $\varphi^n_{a,k}$, a fixed strategy $\tilde{\varphi}^n_{d,k}$ exists such that $\tilde{U}^N_{d,K}$ is the maximum value:

$$\tilde{U}^N_{a,K}>U^N_{a,K}\quad \exists\tilde{\varphi}^n_{a,k},\forall\varphi^n_{d,k}\in\Phi^n_{d,k} \tag{15}$$

$$\tilde{U}^N_{d,K}>U^N_{d,K}\quad \exists\tilde{\varphi}^n_{d,k},\forall\varphi^n_{a,k}\in\Phi^n_{a,k} \tag{16}$$

where $\Phi^n_{a,k}$ is the total set of possible attack strategies; and $\Phi^n_{d,k}$ is the total set of possible defensive strategies.

Here, the pair $(\tilde{\varphi}^n_{a,k}, \tilde{\varphi}^n_{d,k})$ is classified as an equilibrium outcome of the bimatrix game in mixed strategies adopted when the pure strategy Nash equilibrium does not exist; that is, a probability is assigned to each pure strategy, as suggested in [47]. In [46], every bimatrix game is proven to have at least one Nash equilibrium solution for mixed strategies.

E. Multidimensional Evaluation

Considering the specific effects of DDoS attacks, we propose a multidimensional evaluation based on our previous study [21] from four perspectives: node weight, attack complexity, security property, and defensive intensity, as shown in Table I.

TABLE I
MULTIDIMENSIONAL EVALUATION

Perspective	Description	Example
Node weight	Value of node itself	Physical value Cyber value
	Effects of superiors and subordinates	
Attack complexity	Series level	
	Path complexity	
	Concealment	
	Attack potential	
Security property	Confidentiality	
	Integrity	
	Reliability	
Defensive intensity	Software defense	Firewall Block lists
	Hardware defense	Quick break protection Differential protection

Here, the node weight is calculated by considering the value of the node (physical and cyber values) quantified by the criticality level (CL) [48] and the effects of superiors and subordinates reflected by the node centrality degree. The more significant the expected direct and indirect effects of the risk mode of the node, the higher the CL. Attack complexity comprises a series level defined by the degree of network cohesiveness and the difficulty of the attack (i. e., attack path complexity, attack concealment, and attack potential). The attack difficulty is calculated by translating the exploitability metrics (e. g., attack vector, attack complexity, privileges required, and user interaction) in the CVSS. Several typical vulnerabilities in DDoS attacks are selected as examples and listed in Table II, where PC stands for personal computer; and DSC stands for digital signal controller. Security properties include the three indicators of confidentiality, integrity, and availability, which are considered the core underpinnings of information security [49]. Confidentiality can be defined as the access levels of information internally and externally. Integrity means that data or information in the system is maintained (e. g., the system uses Hash verifications or employs backups) so that the data or information is not modified or deleted by unauthorized parties. Availability requires the system to be available to authorized users through countermeasures such as providing hardware redundancy or data storage. With respect to the CVSS, the CIA is also used as a base metric. Defensive intensity is primarily influenced by defenses built into the device hardware such as quick-break protection and differential protection as well as the software defense strategy related to resource allocation.

TABLE II
TYPICAL VULNERABILITIES IN DDOS ATTACKS

Vulnerability	Equipment	Description
CVE-2021-0259	Interchanger	Due to a vulnerability in DDoS protection, instability may occur in the underlay network as a consequence of exceeding the default DDoS-protection aggregate threshold
CVE-2019-19922	PC	In the Linux kernel, a DoS against non-CPU-bound applications is caused when a CPU is used
CVE-2013-5211	PC, PLC, DSC	The monlist feature in a network time protocol (NTP) allows remote attackers to generate a DoS (traffic amplification)
CVE-2007-0086	PC, PLC, DSC	A DoS (network bandwidth consumption) is caused by remote attackers when accessed through a transmission control protocol (TCP) connection

F. Algorithmic Design

We consider a nonzero-sum game to explore the solution of the Nash equilibrium during resource consumption. In most cases, incomplete information places the sum of utilities in non-equilibrium. The corresponding choices of strategy pairs are listed in Table III.

TABLE III
CORRESPONDING CHOICES OF STRATEGY PAIRS

Mode	Attack intensity	Defend intensity
Successful attack	Constant	Up or down to 0
Failed attack	Up or down to 0	Down to normal level or constant
Attack-free	Up or constant	Constant

In addition, the attacker abandons the node when the expected utility becomes negative.

The knowledge that attackers and defenders have of each other is limited to t_{k-1}. Therefore, they can only use their own and others' current and historical information when calculating their strategies in t_k. Thus, the Q-learning algorithm has the reward values of

$$\Upsilon_{a,k}^{n}=R_{a,k-1}^{n}-r_{a,k}^{n}+V^{n}\cdot\Pr(b_{a\to d,k}^{n}\geq\varphi_{a,k}^{n}) \tag{17}$$

$$\Upsilon_{d,k}^{n}=R_{d,k-1}^{n}-r_{d,k}^{n}+V^{n}\cdot\Pr(b_{d\to a,k}^{n}>\varphi_{d,k}^{n}) \tag{18}$$

where $\Upsilon_{a,k}^{n}$ and $\Upsilon_{d,k}^{n}$ are the final reward values of the attacker and the defender, respectively; and $\Pr(\cdot)$ denotes the players' predicted probability of obtaining revenue through the historical belief index.

$\Upsilon_{a,k}^{n}$ and $\Upsilon_{d,k}^{n}$ are not equal to $U_{a,k}^{n}$ and $U_{d,k}^{n}$, respectively, and therefore some errors will occur due to the incomplete information model. This results in the inability of both parties to make optimal judgments.

Algorithm 1 provides a computational approach based on Q-learning algorithm to achieve the Nash equilibrium using the following procedure. The defender utilizes the strategy transformation function to set a resource allocation value $r_{d,0}^{n}$ to node n in the initial task k_0. The resource adapter conducts a defensive strategy $\varphi_{d,k}^{n}$ after performing and configuring the resource allocation $r_{d,k}^{n}$. The strategy reward $\Upsilon_{d,k}^{n}$ and belief index $b_{a\to d,k}^{n}$ are updated. After the corresponding expected utility for the interaction of strategy selection is calculated under this initial condition, the procedure is repeated for each node k until the initial strategy pair $(\varphi_{a,0}^{n},\varphi_{d,0}^{n})$ with the optimal expected utility is obtained.

Algorithm 1: computational approach based on Q-learning algorithm to achieve Nash equilibrium

```
Input: parameters in DGDS, task $K$, node $N$
Output: $\varphi_{a,k}^{n},\varphi_{d,k}^{n},U_{a,K}^{N},U_{d,K}^{N}$
Initialization: $U_{a,0}^{N},U_{d,0}^{N}$
Initialization: $k,n$
for each node $n\in N$ do
  for each $(\varphi_{a,0}^{n},\varphi_{d,0}^{n})\in(\Phi_{a,0}^{n},\Phi_{d,0}^{n})$ do
    while $k<K$ do
      if $\varphi_{a,k}^{n}>0$ then
        Update $b_{a\to d,k}^{n},b_{d\to a,k}^{n}$
      end if
      Update $Q$-function using (17) and (18)
      Select strategy pairs $(\varphi_{a,k}^{n},\varphi_{d,k}^{n})\in(\Phi_{a,k}^{n},\Phi_{d,k}^{n})$ using $\varepsilon$-greedy algorithm
      Update $U_{a,k}^{n},U_{d,k}^{n}$
      $k=k+1$
    end while
    Select initial strategy pair $(\varphi_{a,0}^{n},\varphi_{d,0}^{n})$ using mixed strategy
    Update $U_{a,K}^{n},U_{d,K}^{n}$
  end for
end for
```

IV. SIMULATION EXPERIMENTS AND NUMERICAL RESULTS

A. Experimental Setup

In this study, experiments are conducted on a testbed at Zhejiang University, China. A CPPS with topological connections and different devices is implemented as illustrated in Fig. 2.

Nodes 1-3 are PCs (Core i7, 8086K) equipped with Linux systems. Node 4 is an industrial switch that uses the Modbus/TCP protocol. Node 5 is a PLC manufactured by SIEMENS. Node 6 is a distributed control system (DCS) manufactured by SIEMENS. Node 7 is a remote terminal unit (RTU) manufactured by Schneider Electric. Finally, Nodes 7 and 8 are connected to traditional electrical devices.

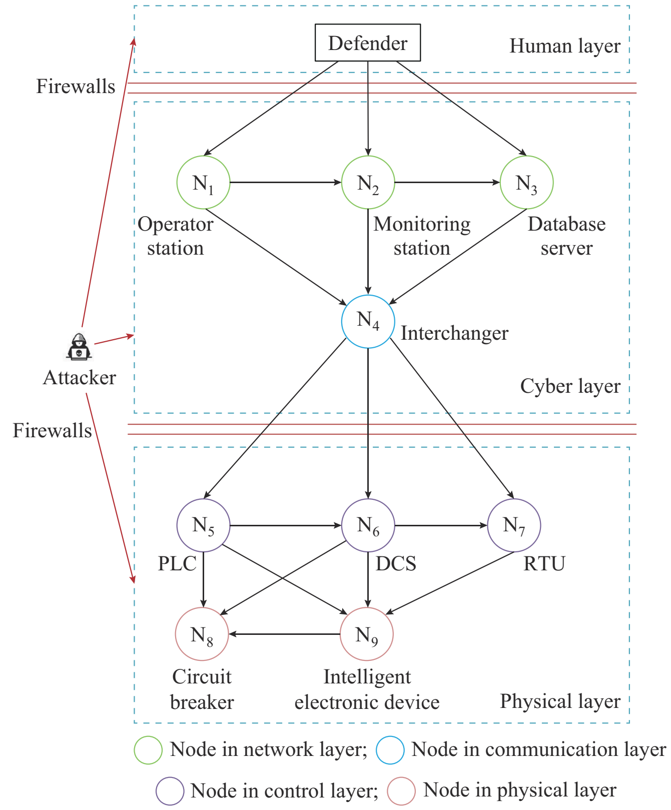


Fig. 2. CPPS structure in simulations.

Node 4 mainly transmits data; therefore, the CL of the cyber value is high, but it does not have a high value itself, and the CL of the physical value is low. As a key node, it is connected to many other nodes, and the effects of the upper and lower levels are very high. This node is in the second stage (communication layer); therefore, its series level is low. The attack difficulty is obtained as low by mapping AV: N/AC: L/PR: N/UI: N/S: U in vulnerability CVE-2019-16920. The security property is obtained by mapping C: H/I: H/A: H to be very high. The defensive intensity is medium. Additional details of the CVSS can be found in [22].

Similar to SCADA, the human layer is connected to the cyber layer via Ethernet. A local area network connects the computing and communication devices in the cyber layer internally and intelligent devices in the physical layer. In the physical layer, PLCs and controllers (e. g., circuit breakers) are expected to operate in real time, and communication can guarantee their time-sensitive performance [50].

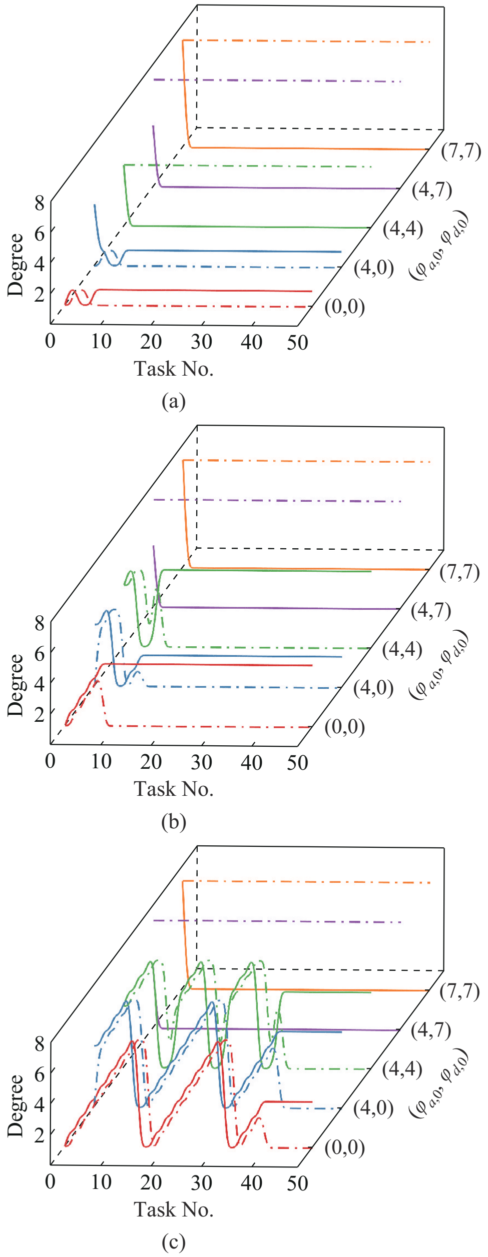
B. Performance Evaluation

The attacker's goal is a successful attack, which is evaluated based on [51], when more nodes are prevented from operating normally with positive expected utility. The goal of the defender is to protect more nodes with limited resources. The intensities of the attacker and defender are discretized into s degrees: $\varPhi_a = \varPhi_b = (0, 1, \ldots, s-1)$. The greater the value of s, the more complex is the game.

First, each task that is issued to a target node in a sampling interval is assumed to consume the same time and resources. However, task consumption may differ with different nodes because of the corresponding devices connected to the node. Thus, only a single attacker is considered in this study; that is, no cooperative attack occurs. In addition, a prior belief distribution based on past experiences with another player is assumed.

1) Values of Nodes

For nodes with different values, the strategies of the attacker and the defender change. Three typical nodes a, b, and c are selected as samples, as shown in Fig. 3. The solid and dashed lines denote the strategy change processes of the attacker and the defender, respectively. Initial strategy pairs of players s^2 are employed. Here, $s = 8$ with initial strategy pairs $(\varphi_{a,0}, \varphi_{d,0}) \in \{(0,0), (4,0), (4,4), (4,7), (7,7)\}$ are demonstrated to show the game processes from 64 strategy pairs.



(a)

(b)

(c)

Fig. 3. Sets of optimal strategy pairs under different initial strategy pairs for typical nodes. (a) Node a. (b) Node b. (c) Node c.

The results of nodes a, b, and c show that the higher the value of a node, the longer the game process continues. Finally, the optimal strategy pairs are found.

When the defender chooses a very low degree as the initial strategy (when only basic defensive measures based on local protection devices are available), for example, $(\varphi_{a,0},\varphi_{d,0})\in\{(0,0),(4,0)\}$, the following are possible:

1) For a low-value node, regardless of the initial strategy the attacker chooses, the attack strategy will fall back into the low-degree strategy after certain duration of the game process.

2) For a medium-value node, the initial strategy adopted by the attacker (i.e., heuristic attack) is important. When the attacker gradually increases the attack degree from zero, the defender quickly gives up. However, the attacker fails to obtain sufficient prior knowledge, and therefore the result is not as good as that under the situation starting from the medium degree.

3) For a high-value node, the attacker has obtained sufficient prior knowledge in the long game process, and the update of the belief index determines the initial defense degree. Therefore, the higher the initial defense degree, the higher the attack degree.

When the defender chooses a high degree as the initial strategy (e. g., $(\varphi_{a,0},\varphi_{d,0})\in\{(4,7),(7,7)\}$), regardless of the value of the node, the attacker will directly abandon the node. By contrast, when the attacker initially adopts a medium degree to conduct a heuristic attack (e. g., $(\varphi_{a,0},\varphi_{d,0})\in\{(4,0),(4,4),(4,7)\}$), the following are possible:

1) For a low-value node, the defender can choose a strategy above a medium degree to protect the node and force the attacker to give up.

2) For a medium-value node, the defender must select a high degree as the initial strategy to successfully defend against the attacker. Otherwise, the defender will give up after certain duration of the game process because of resource consumption.

3) For a high-value node, the defender spends significantly more time collecting the attacker's information. However, the defender will eventually give up because of resource consumption and aggressive attack strategy unless a high-degree defense strategy is initially chosen.

2) Mixed Strategy

For a high-value node c, strategy pairs exist with 64 initial degrees and the corresponding expected utilities for the Nash equilibrium solution. If no pure strategy pairs exist from the 64 expected utilities (i.e., the attacker takes the best utility and the defender does not), then a mixed strategy is adopted. The probabilities of the attacker and defender for the initial degree strategy are listed in Table IV. The corresponding expected utilities and changes in expected utilities are presented in Fig. 4.

3) Comparison of Cases with Complete and Incomplete Information

As Fig. 5 shows, in the complete information scenario, the optimal expected utility of the defender is much greater than that in the incomplete information scenario.

TABLE IV
PROBABILITIES OF ATTACKER AND DEFENDER FOR INITIAL DEGREE STRATEGY

Initial degree	Probability	
	Attack strategy	Defense strategy
0	4.49×10^{-1}	4.61×10^{-9}
1	2.54×10^{-2}	4.26×10^{-9}
2	3.63×10^{-1}	5.21×10^{-9}
3	4.62×10^{-7}	4.70×10^{-9}
4	1.14×10^{-1}	4.06×10^{-9}
5	1.09×10^{-7}	4.15×10^{-9}
6	8.61×10^{-9}	4.99×10^{-1}
7	4.94×10^{-2}	5.01×10^{-1}

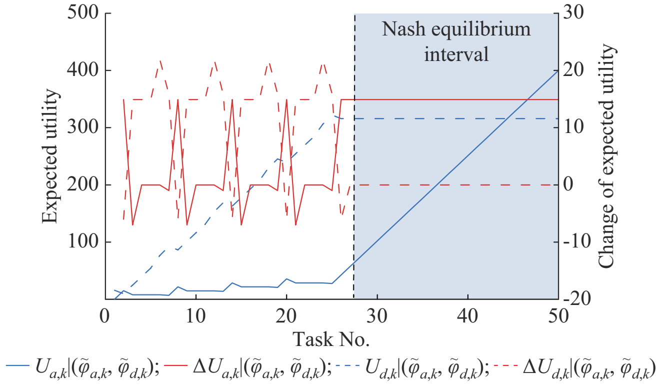
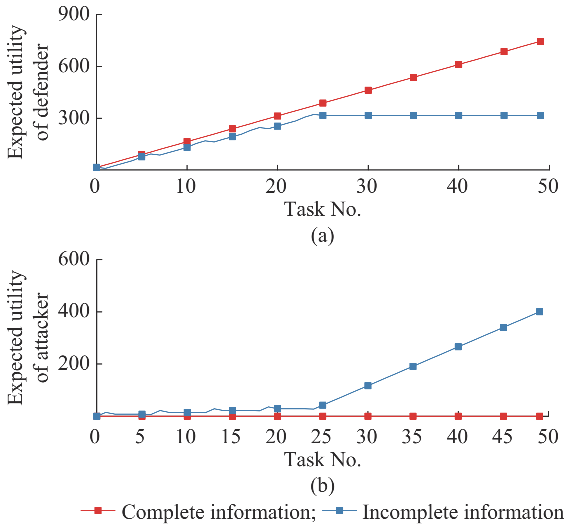


Fig. 4. Results of expected utilities and changes in expected utilities.



(a)

(b)

Fig. 5. Comparison of expected utilities of defenders and attackers in complete and incomplete information scenarios. (a) Expected utilities of defenders. (b) Expected utilities of attackers.

For an attacker, a heuristic attack consumes resources without any benefit. Note that the attacker's benefit is not affected by the defender's benefit loss in a nonzero-sum game.

4) Belief Index

The belief indices vary depending on the attacker's and defender's capabilities (e. g., trained players, hackers, and masters). For the high-value node c, the strategy pairs and expected utilities for players with different capabilities are examined. The initial strategy pairs are chosen randomly as $(\varphi_{a,0}, \varphi_{d,0})=(0,5)$, which is unrelated to the results. Figure 6 illustrates the strategy pairs and expected utilities when the attacker is stronger than the defender. Figure 7 illustrates the strategy pairs and expected utilities when the attacker is weaker than the defender.

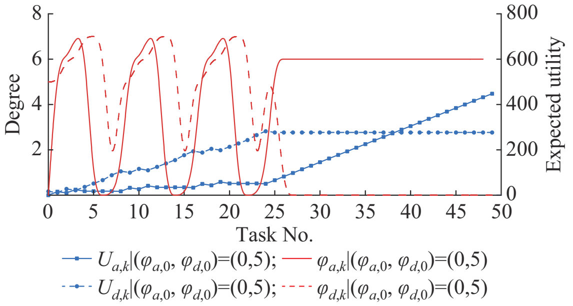


Fig. 6. Strategy pairs and expected utilities when attacker is stronger than defender.

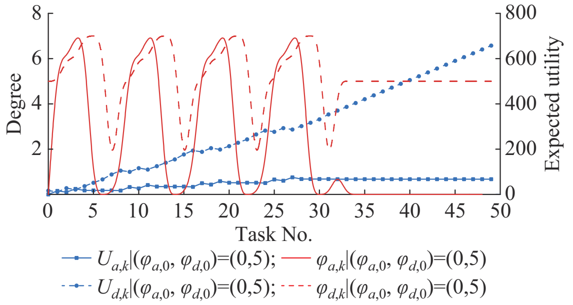


Fig. 7. Strategy pairs and expected utilities when attacker is weaker than defender.

It can be observed that when the attacker is stronger than the defender, even if the initial strategy is inferior, the attack is likely to succeed. When the defender is stronger than the attacker, the attacker has difficulties breaking through the defense unless the defender gives up. In Fig. 8, if both the attacker and defender do not obtain information from historical data (i.e., they ignore the influence of the belief index), they will cyclically adopt the same strategy pairs.

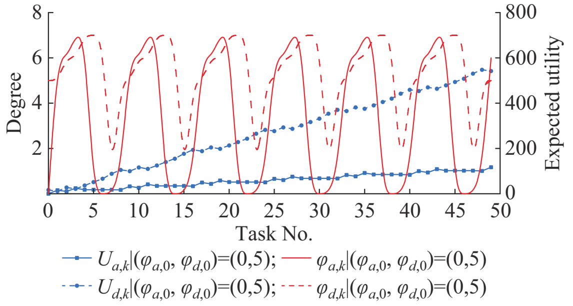


Fig. 8. Strategy pairs and expected utilities when no belief index exists.

Our study shows that the proposed solution can provide an appropriate allocation of defensive resources under limited resources. The initial strategy significantly affects the choice of strategy for both the attacker and the defender. For complete information scenario, the attacker has difficulties obtaining the utility. Experienced defenders can reduce system losses effectively.

V. Conclusion

This study exploited a game-theoretical model for a dynamic defense strategy under DDoS attacks with respect to CPPSs and developed a nonzero-sum game model with incomplete information. The effectiveness of the proposed solution was extensively evaluated through simulation experiments, and the numerical results confirmed its effectiveness in dynamically allocating defense resources. In the future study, machine-learning models can be incorporated into the design of game-theoretical defense strategies. The exploitation of a complex scenario with multiple game participants (i.e., a cooperative attack or cooperative defense) is worthy of further research.

References

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

[2] K. Tian, W. Sun, and D. Han, "Strategic investment in transmission and energy storage in electricity markets," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 179-191, Jan. 2022.

[3] O. Analytica. (2021, May). US pipeline hack to make ransomware risks a priority. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/OXAN-GA261470

[4] S. Yu, W. Zhou, R. Doss *et al*., "Traceback of DDoS attacks using entropy variations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 3, pp. 412-425, Mar. 2011.

[5] M. Cagalj, T. Perkovic, and M. Bugaric, "Timing attacks on cognitive authentication schemes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 584-596, Mar. 2015.

[6] H. T. Reda, A. Anwar, A. Mahmood *et al*., "Data-driven approach for state prediction and detection of false data injection attacks in smart grid," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 2, pp. 455-467, Mar. 2023.

[7] R. A. Jabr and Izudin Džafić, "Distribution management systems for smart grid: architecture, work flows, and interoperability," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 300-308, Mar. 2022.

[8] S. Yu, Y. Tian, S. Guo *et al*., "Can we beat DDoS attacks in clouds?," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245-2254, Sept. 2014.

[9] M. Ni, M. Li, J. Li *et al*., "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 3, pp. 477-484, May 2021.

[10] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proceedings of 2011 IEEE PES General Meeting*, Detroit, USA, Jul. 2011, pp. 1-6,.

[11] B. Chen, S. Mashayekh, K. L. Butler-Purry *et al*., "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proceedings of 2013 IEEE PES General Meeting*, Vancouver, Canada, Jul. 2013, pp. 1-5.

[12] S. Liu, S. Mashayekh, D. Kundur *et al*., "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273-285, Dec. 2013.

[13] J. H. Kazmi, A. Latif, I. Ahmad *et al*., "A flexible smart grid co-simulation environment for cyber-physical interdependence analysis," in *Proceedings of 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Vienna, Austria, Apr. 2016, pp. 1-6.

[14] V. Venkataramanan, A. Srivastava, and A. Hahn, "Real-time co-simulation testbed for microgrid cyber-physical analysis," in *Proceedings of 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Vienna, Austria, Apr. 2016, pp. 1-6.

[15] K. Huang, C. Zhou, Y. Qin *et al*., "A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 3, pp. 2371-2379, Mar. 2020.

[16] L. Huang and Q. Zhu, "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems," *Computers & Security*, vol. 89, p. 101660, Feb. 2020.

[17] J. Liu, X. Wang, S. Shen *et al*., "A Bayesian *Q*-learning game for dependable task offloading against DDoS attacks in sensor edge cloud," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7546-7561, May 2020.

[18] G. Yan, R. Lee, A. Kent *et al*., "Towards a Bayesian network game framework for evaluating DDoS attacks and defense," in *Proceedings of the 2012 ACM conference on Computer and Communications Security*, Raleigh, USA, Oct. 2012, pp. 553-566.

[19] B. Gao and L. Shi, "Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system," *IEEE Access*, vol. 8, pp. 30322-30331, Feb. 2020.

[20] X. Liu, D. Tang, and Z. Dai, "A Bayesian game approach for demand response management considering incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 492-501, Mar. 2022.

[21] B. Yan, P. Yao, J. Wang *et al*., "Game theoretical dynamic cybersecurity defense strategy for electrical cyber physical systems," in *Proceedings of 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2)*, Taiyuan, China, Oct. 2021, pp. 2392-2397.

[22] P. Mell, K. Scarfone, and S. Romanosky. (2007, Jul.). A complete guide to the common vulnerability scoring system version 2.0. [Online]. Available: https://www.nist.gov/publications/complete-guide-common-vulnerability-scoring-system-version-20

[23] L. Sha, S. Gopalakrishnan, X. Liu *et al*., "Cyber-physical systems: a new frontier," in *Proceedings of 2008 IEEE International Conference on Sensor Networks*, Taichung, China, Jun. 2008, pp. 1-9.

[24] H. Gill, "From vision to reality: cyber-physical systems," in *Proceedings of HCSS National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive, Aviation, and Rail*, Austin, USA, Nov. 2008, pp. 18-20.

[25] S. Yu, S. Guo, and I. Stojmenovic, "Can we beat legitimate cyber behavior mimicking attacks from botnets?," in *Proceedings of 2012 IEEE INFOCOM*, Orlando, USA, Mar. 2012, pp. 2851-2855.

[26] L. Garber, "Denial-of-service attacks rip the internet," *Computer*, vol. 33, no. 4, pp. 12-17, Apr. 2000.

[27] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol. 73, no. 1, pp. 3-25, Jul. 2020.

[28] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for SDN-enabled smart grids," *Computer Communications*, vol. 133, pp. 1-11, Jan. 2019.

[29] Y. Wadhawan, A. AlMajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, no. 10, p. 249, Sept. 2018.

[30] B. Gao, C. Chen, Y. Qin *et al*., "Evolutionary game-theoretic analysis for residential users considering integrated demand response," *Journal of Modern Power Systems and Clean Energy*, vol. 9, no. 6, pp. 1500-1509, Nov. 2021.

[31] X. Liu, D. Tang, and Z. Dai, "A Bayesian game approach for demand response management considering incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 492-501, Mar. 2022.

[32] Q. Jia, Y. Li, Z. Yan *et al*., "A reinforcement-learning-based bidding strategy for power suppliers with limited information," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 4, pp. 1032-1039, Jul. 2022.

[33] Y. Zhao, L. Huang, C. Smidts *et al*., "Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants," *Reliability Engineering & System Safety*, vol. 201, p. 106878, Sept. 2020.

[34] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: a dynamic Bayesian game-theoretic approach," *The International Society of Automation (ISA) Transactions*, vol. 115, pp. 108-123, Sept. 2021.

[35] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46-65, Feb. 2015.

[36] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5366-5380, Nov. 2021.

[37] O. Gasser, Q. Scheitle, P. Foremski *et al*., "Clusters in the expanse: understanding and unbiasing IPv6 hitlists," in *Proceedings of the Internet Measurement Conference 2018*, New York, USA, Oct. 2018, pp. 364-378.

[38] B. Al-Duwairi, E. Al-Quraan, and Y. Abdel-Qader, "ISDSDN: mitigating SYN flood attacks in software defined networks," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 1366-1390, Jun. 2020.

[39] S. Q. A. Shah, F. Z. Khan, and M. Ahmad, "The impact and mitigation of IMCP based economic denial of sustainability attack in cloud computing environment using software defined network," *Computer Networks*, vol. 187, p. 107825, Mar. 2021.

[40] S. B. Alaoui, T. El Houssaine, and C. Noreddine, "Modelling, analysis and design of active queue management to mitigate the effect of denial of service attack in wired/wireless network," in *Proceedings of 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Fez, Morocco, Oct. 2019, pp. 1-7.

[41] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 29-30, Jul. 2003.

[42] Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649-1662, Nov. 2007.

[43] A. Srivastava, B. B. Gupta, A. Tyagi *et al*., "A recent survey on DDoS attacks and defense mechanisms," in *Advances in Parallel Distributed Computing*. Heidelberg: Springer, Sept. 2011, pp. 570-580.

[44] R. Liu, C. Vellaithurai, S. S. Biswas *et al*., "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444-2453, Jun. 2015.

[45] M. Premkumar and T. Sundararajan, "DLDM: deep learning-based defense mechanism for denial of service attacks in wireless sensor networks," *Microprocessors and Microsystems*, vol. 79, p. 103278, Nov. 2020.

[46] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. Philadelphia: Society for Industrial and Applied Mathematics, 1998.

[47] I. Erev and A. E. Roth, "Predicting how people play games: reinforcement learning in experimental games with unique, mixed strategy equilibria," *American Economic Review*, vol. 88, no. 4, pp. 848-881, Sept. 1998.

[48] J. Watters, *Criticality Levels*. Berkeley: Apress, 2014, pp. 223-224.

[49] S. M. Dibaji, M. Pirani, D. B. Flamholz *et al*., "A systems and control perspective of CPS security," *Annual Reviews in Control*, vol. 47, pp. 394-411, May 2019.

[50] Q. Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, pp. 316-327, Aug. 2011.

[51] Y. Cao, X. Shi, Y. Li *et al*., "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4893-4905, Sept. 2017.

Bingjing Yan is currently pursuing the Ph.D. degree in the College of Electrical Engineering, Zhejiang University, Hangzhou, China. Her research interests include game-theoretic research toward cyber-physical power security against cyber attacks.

Pengchao Yao is currently pursuing the Ph.D. degree in the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include modeling and security analysis of industrial cyber-physical systems against cyber-attacks.

Tao Yang is currently pursuing the Ph.D. degree in the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include malware detection and adversarial malware generation.

Boyang Zhou received the Ph.D. degree in Computer Science and Technology from Zhejiang University, Hangzhou, China, in 2014. He is currently a Research Expert of Intelligent Networks Research Institute, Zhejiang Lab, Hangzhou, China. He was a Postdoctoral Researcher at College of Computer Science and Technology, Zhejiang University, from 2016 to 2019, and was also a Senior Engineer of State Grid Corporation of China, Beijing, China, from 2014 to 2019. His research interests include industrial Internet security, deterministic networks, future network architecture, and smart grid communications.

Qiang Yang received the Ph. D. degree in electronic engineering and computer science from Queen Mary, University of London, London, UK, in 2007, and worked in the Department of Electrical and Electronic Engineering, Imperial College London, London, UK, from 2007 to 2010. He visited the University of British Columbia, Vancouver, Canada and the University of Victoria Canada, British Columbia, Canada, as a visiting scholar in 2015 and 2016. He is currently a full Professor at the College of Electrical Engineering, Zhejiang University, Hangzhou, China. He is the Follow of British Computer Society (BCS), a Senior Member of IEEE, IET, and the Senior Member of China Computer Federation (CCF). He has published more than 220 technical papers, applied for 60 national patents, co-authored 2 books, and edited 2 books and several book chapters. His research interests include smart energy systems, large-scale complex network modeling, control and optimization, learning-based optimization and control.