Game Theory based Optimal Defensive Resources Allocation with Incomplete Information in Cyber-physical Power Systems against False Data Injection Attacks

Bingjing Yan, Zhenze Jiang, Pengchao Yao, Qiang Yang, Wei Li, and Albert Y. Zomaya

***Abstract*—Modern power grid is fast emerging as a complex cyber-physical power system (CPPS) integrating physical current-carrying components and processes with cyber-embedded computing, which faces increasing cyberspace security threats and risks. In this paper, the state (i.e., voltage) offsets resulting from false data injection (FDI) attacks and the bus safety characterization are applied to quantify the attack consequences. The state offsets are obtained by the state estimation method, and the bus safety characterization considers the power network topology as well as the vulnerability and connection relationship of buses. Considering the indeterminacy of attacker's resource consumption and reward, a zero-sum game-theoretical model from the defender's perspective with incomplete information is explored for the optimal allocation of limited defensive resources. The attacker aims to falsify measurements without triggering threshold alarms to break through the protection, leading to load shedding, over-voltage or under-voltage. The defender attempts to ensure the estimation results to be as close to the actual states as possible, and guarantee the system's safety and efficient defensive resource utilization. The proposed solution is extensively evaluated through simulations using the IEEE 33-bus test network and real-time digital simulator (RTDS) based testbed experiments of the IEEE 14-bus network. The results demonstrate the effectiveness of the proposed game-theoretical approach for optimal defensive resource allocation in CPPS when limited resources are available when under FDI attacks.**

***Index Terms*—Optimal strategy, game theory, Nash equilibrium, CPPS, FDI attack.**

I. INTRODUCTION

The advance of information and communication technologies (ICT) has accelerated the traditional power system into a complex cyber-physical power system (CPPS) which promotes operational efficiency, reliability and flexibility [1]. However, it also creates additional security problems with the emerging threat not only by the physical environment but also by cyberspace components, despite many researches have already been carried out to support the comprehensive protection of the cyber system and timely management of the physical system [2]. The previous cyber attacks on different critical infrastructures, e.g., the Ukraine power grid hack [3] and Stuxnet [4], have demonstrated the vital importance of CPPS safety.

As one of the most malicious cyber attacks, the false data injection (FDI) attack targets state estimators and systematically alters analog measurement data [5], which can lead to cascading failure [6], bus voltage instability [7], and disruption of electricity markets [8]. To alleviate the negative impact of FDI attacks, the current countermeasures can be generally classified into two categories: protection methods by identifying critical measurements (e.g., [9]) or keeping the exact reactance (e.g., [10]), and detection solutions through the analysis of raw measurements (e.g., [11]).

In addition, there have been some efforts of game-theoretic research toward CPPS security against FDI attacks since the game theory can provide a quantifiable and understandable foundation for implementing active defensive strategies under different forms of system uncertainties [12], [13]. To improve the quality of monitoring and decision-making in smart grid, reference [14] specifies the effect of compromising each measurement on the price of electricity and defines the game model as a zero-sum game under complete information. In [15], a zero-sum game theoretical attack-defense model is suggested to describe interactions in cyber-physical systems, while the measurements are used as the attack and defense objects and load shedding

Received: March 2, 2023
Accepted: November 1, 2023
Published online: March 1, 2024

Qiang Yang (corresponding author) is with the College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: qyang@zju.edu.cn).

DOI: 10.23919/PCMP.2023.000138

is applied to quantify the attack consequences. Furthermore, reference [16] describes a model with multiple attackers and a single defender using a Stackelberg game model in which the defender acts as the leader with complete information. Similarly, a Stackelberg game model is investigated in [17] to analyze the optimal solutions under different budget constraints with the assumption of complete information. Reference [18] proposes a defense technique based on a dynamic Bayesian game model to investigate FDI attacks in power systems.

It is worth noting that the aforementioned solutions have not fully exploited the trade-off between the overall system's safety and defensive resource utilization efficiency, as well as the optimal resource allocation considering the limited availability based on CPPS vulnerability analysis. In addition, most studies have assumed a game model with complete information (e.g., the use of the Stackelberg game model requires the assumption of complete and perfect information), which is less realistic than a game model with incomplete information. In addition, only simulations have been used in previous studies to model the coupling behaviors between cyber and physical domains, which is insufficient to fully demonstrate the system characteristics.

This paper proposes a game-theoretical model for optimal defensive resource allocation strategy in a CPPS under FDI attacks with limited defensive resources availability. A zero-sum game model with incomplete information is established to calculate the expected utilities of rational players from two perspectives: the state offsets of the impacted buses and the bus safety characterization.

FDI attacks target the installed measurement devices, e.g., the phasor measurement units (PMU), and mislead the decision-making process of the defender (e.g., control center) by tampering with the estimation results to affect the normal operation of power systems. Accordingly, the weighted least squares (WLS) method, as a basic approach for state estimation, is applied to approximate the impacted buses' state offsets which reflect the adverse effect of the FDI attack in this paper. The design of bus safety characterization fully considers the topology of the power system (e.g., centrality degree, betweenness degree), the vulnerability of devices described in the common vulnerability scoring system (CVSS) [19], and the connection relationship on buses reflected with logic gates ('AND', 'OR'). From the defender's perspective, the game model is built considering that the attacker aims to falsify measurements without triggering threshold alarms to break through the protection, resulting in load-shedding, over-voltage or under-voltage. Additionally, the defender attempts to secure the estimation results close to the actual variables and guarantee the system's safety and efficient defensive resource utilization. The effectiveness of the proposed solution is validated through both simulations using the IEEE 33-bus test network and the real-time digital simulator (RTDS) based testbed experiments using the IEEE 14-bus network. Compared with the simulation results, the RTDS testbed experiments retain the necessary interactions of the cyber-physical domain. The main technical contributions made in this work are as follows:

1) An optimal game-theoretical model with incomplete information is presented considering that the strategy choices and behaviors of the attackers are not deterministic, which introduces the game model into the cyber-physical system, taking into account the characteristics of critical infrastructure.

2) The proposed solution identifies the optimal resource allocation by making the trade-off between the overall CPPS safety and defensive resource utilization efficiency based on the software vulnerability and the topology structure analysis.

The remainder of the paper is organized as follows. Section II overviews the system design and problem formulation. A detailed description of the game-theoretical model is presented in Section III. The simulation and testbed experiments are carried out and the numerical results are presented in Section IV. Finally, conclusions are given in Section V.

II. System Model and Problem Formulation

This section describes the FDI threat model and introduces the WLS minimization-based state estimation. The overall architecture of the proposed system model in CPPS under the FDI attack is illustrated in Fig. 1.

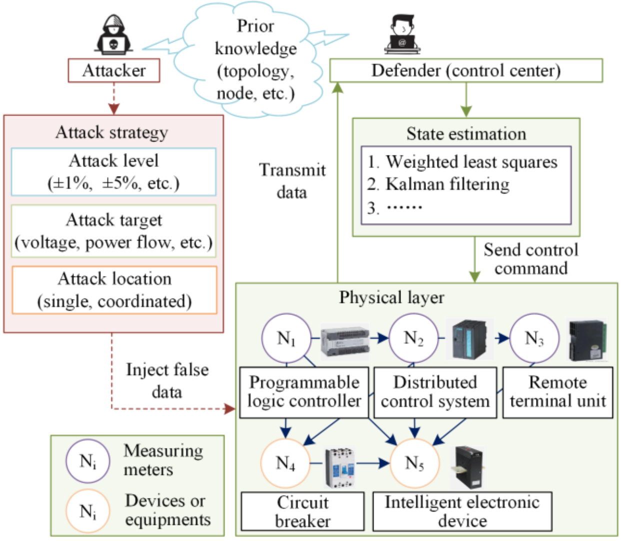
Attacker
Prior knowledge (topology, node, etc.)
Defender (control center)
Attack strategy
Attack level (±1%, ±5%, etc.)
Attack target (voltage, power flow, etc.)
Attack location (single, coordinated)
Transmit data
State estimation
1. Weighted least squares
2. Kalman filtering
3. ……
Send control command
Physical layer
N1
N2
N3
Programmable logic controller
Distributed control system
Remote terminal unit
Inject false data
N4
N5
Circuit breaker
Intelligent electronic device
Ni Measuring meters
Ni Devices or equipments

Fig. 1. Overall architecture of the proposed system model under the FDI attacks in the context of CPPSs.

As shown, the attacker with some prior knowledge acquired through techniques such as sniffing or social engineering launches an attack on the physical layer by appropriate attack strategies, causing anomalies in the monitored device status by the defender. This leads to erroneous actions by the defender and subsequently affects the normal operation of the entire system.

A. FDI Threat Model

Because of the coupling of the cyber-physical relationship, cyber attacks can significantly affect the operation of the grid system. An FDI attack, as one of the most prevalent cyber attacks, is established as the threat model. The FDI attackers with prior knowledge interfere with the estimation results (e.g., voltage, current and power measurements) by controlling meters, the communication networks and the master station. Specific attack strategies such as missing data encryption, operating system (OS) command injection and structured query language (SQL) injection, etc. use automated attacks or manually construct fake data targeting acquisition devices or monitoring systems [20]. Then the control center is induced to take emergency measures to trip critical buses and lines, resulting in load shedding, over-voltage or under-voltage tripping. For example, as one of the most publicly known malware, Stuxnet injected processes and registered services to modify data sent to or re-turned from the programmable logic controller (PLC) without the knowledge of the administrator in supervisory control and data acquisition (SCADA) systems, leading to the scrapping of one-fifth of the centrifuges in Iran's uranium enrichment plant, greatly delayed Iran's nuclear process [4].

For the attackers, there are generally two targets for the FDI into the state estimation, i.e., certain system state variables (e.g., bus phase angle, bus voltage magnitude) and certain measurements determined by system structure and at least two system variables [21]. The attacker needs to inject more false data into meters if one intends to change the multiple states simultaneously, which can be formulated by the following equations, as suggested in [22].

1) Real and reactive power injection at bus i:

$$\begin{cases} P_i = V_i \sum\limits_{j\in\Omega_i} V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \\ Q_i = V_i \sum\limits_{j\in\Omega_i} V_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \end{cases} \tag{1}$$

2) Real and reactive power flow from bus i to bus j:

$$\begin{cases} P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij}\cos\theta_{ij} + b_{ij}\sin\theta_{ij}) \\ Q_{ij} = -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij}\sin\theta_{ij} - b_{ij}\cos\theta_{ij}) \end{cases} \tag{2}$$

where V_i and θ_i are the respective voltage magnitude and phase angle at bus i; θ_{ij} is the angle difference between θ_i and θ_j; $G_{ij} + \mathrm{j}B_{ij}$ is line admittance between bus i and j; $g_{si} + \mathrm{j}b_{si}$ is the admittance of the shunt branch at bus i; and Ω_i is the set of buses connected to bus i. Also, the measurements that are affected by the manipulated state variables need to be considered in order to pass the bad data detection.

Recent studies have examined many specific attack methods [20], and confirm that attackers can implement FDI attacks at a low cost by falsifying the measurements without triggering the predefined threshold alarms [23]. Also, some topology identification methods based on measurements have been proposed [24], [25]. Therefore, this work mainly focuses on the impact of the attack without details of the specific implementation of the attacks.

B. State Estimation under FDI Attack

Real-time monitoring of power system is critical for maintaining system's safety and reliability [26]. Operators monitor system components and report meters' readings to the control center which estimates the state of the system and takes measures according to the defense strategy.

Considering a power system with s state variables is monitored by m meters ($m > s$, i.e. the system is observable) [27], state estimation is to estimate state variables $\boldsymbol{x}$ based on meter measurements $\boldsymbol{z}$ such as P_i, Q_i, V_i, etc. which are described in (1) and (2) under independent random measurement noises $\boldsymbol{e}$. The mathematical relation between them is given as:

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{3}$$

where $\boldsymbol{h}(\boldsymbol{x}) = [\boldsymbol{h}_1(\boldsymbol{x}), \cdots, \boldsymbol{h}_i(\boldsymbol{x}), \cdots, \boldsymbol{h}_m(\boldsymbol{x})]^{\mathrm{T}}$ are the measurement functions of $\boldsymbol{x}$, which depend on the specific measurement type and involve the network topology and parameters of the power system. The basic approach for state estimation is called the WLS method [28], which attempts to obtain the best fit such that the sum of squared errors is minimized.

If the error data is likely to be well-designed because the attacker is familiar with the CPPS, the FDI attack can be successfully launched and the security of the system can be compromised. The attack vector $\boldsymbol{a}$ is given as:

$$\boldsymbol{a} = \boldsymbol{h}(\boldsymbol{x} + \boldsymbol{c}) - \boldsymbol{h}(\boldsymbol{x}) \tag{4}$$

where $\boldsymbol{c}$ is the state vector error caused by the attack. In general, the largest normalized residual (LNR) is used to identify the anomalies [27], as:

$$\begin{aligned} \Delta = \|(\boldsymbol{z} + \boldsymbol{a}) - \boldsymbol{h}(\boldsymbol{x} + \boldsymbol{c})\|^2 \leqslant \\ \|(\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}))\|^2 + \|(\boldsymbol{a} + \boldsymbol{h}(\boldsymbol{x}) - \boldsymbol{h}(\boldsymbol{x} + \boldsymbol{c}))\|^2 \end{aligned} \tag{5}$$

In this case, the false data can be successfully injected into the system without triggering the alarm, which can effectively avoid the traditional detection.

C. CPPS Asset Analysis

Unlike our previous work [29], the bus safety characterization addressed in this work is more inclined towards the inherent characteristics of the power system architecture rather than device software vulnerabilities. The inherent characteristics of a complex CPPS can be better investigated by abstracting bus-to-edge connections from the degree of correlation between topologies.

In this work, the bus weight is designed considering four aspects, i.e., centrality degree, betweenness degree, network cohesion degree and value degree, described as follows.

1) Centrality Degree

D_i is the number of buses connected to the bus i, which is proportional to the importance. The comprehensive beneficial function is proposed to reflect the energy required for electric energy transmission by utilizing the electrical coupling distance in order to identify buses with the same number of connections, as:

$$d_{ij} = \frac{U_{ij}}{I_i} = Z_i + Z_j - 2Z_{ij} \tag{6}$$

where Z_i and Z_j denote the self-impedance of bus i and j, respectively; while Z_{ij} is the mutual impedance between buses i and j.

2) Betweenness Degree

B_i represents the number of the shortest paths that pass through bus i. A bus with a higher betweenness degree would have more control over the network because more vital buses are connected. The betweenness degree of bus i is given by:

$$g(i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \tag{7}$$

where σ_{st} denotes the total number of shortest paths between buses s and t; and $\sigma_{st}(i)$ denotes the number of those paths that pass through i. A normalization can be performed without sacrificing accuracy, as:

$$B_i = \text{normal}(g(i)) = \frac{g(i) - \min(g)}{\max(g) - \min(g)} \tag{8}$$

3) Network Cohesion Degree

K_i indicates the location of bus i in the power system topology. The more intersections, the higher the bus's relevance, which can be derived using the contraction method [30] by clustering bus i and buses near i.

4) Value Degree

C_i represents the asset value of bus i, including physical value (the device itself) and cyber value (the data contained in it), as measured by the criticality level (CL) [31]. The specific quantification method is described in detail in [29].

Based on subjective correction weight methods (e.g., hierarchical analysis method [32]) and objective correction weight methods (e.g., critic method [33]), different coefficients are set to combine multiple weight coefficients to obtain the integrated weight vector, which has been described in detail in [34]. Synthetically, the weight degree of bus i is defined as:

$$W_i = \sum_{j=1}^{4} A_{ji}\mu_{ji} \tag{9}$$

where A_{ji} denotes the *j*th weight indicator of bus i; and μ_{ji} denotes the composite weight vector of that indicator.

III. Game Model

A. Bayesian Game Model

The Bayesian game model is implemented, which widely utilized in incomplete information. Players in the Bayesian game model evaluate the decisions and information of other players based on prior knowledge and historical data, and subsequently formulate their own decisions. In CPPS scenarios, the prior knowledge includes the system's topological structure and available devices connected with network buses. However, the players lack insight into each other's decisions. The defenders formulate decisions (i.e., defense strategies and whether to carry out defense actions) continuously based on current information which does not include whether the attacker is launching an attack. Likewise, the attacker is in the same situation.

As CPPS is a critical infrastructure, the attacker can hardly carry out multiple trial attacks to gather sufficient information and modify the attack strategy. Hence the attacker generally has only one chance of attack in practice. When the attack fails, the defender (i.e., control center) will redeploy protection measures. As a result, the attack-defense interaction can be defined as a one-stage static simultaneous moves game. Harsanyi transformation is accomplished to convert a static game with incomplete information to an equivalent imperfect information game by introducing the concept of nature, providing a solution for subsequent calculations [35].

The static game model with incomplete information involves four elements: players, strategy pairs, actions and expected utilities, as explained in Table I. More details for the definition of game elements can be found in [36].

TABLE I
ELEMENTS IN STATIC GAME MODEL WITH INCOMPLETE INFORMATION

Element	Notation
Players	$P=\{P_A, P_D\}$. P_A is the attacker. P_D is the defender.
Actions	$A=\{A_1, A_2, \cdots, A_I\}$. $D=\{D_1, D_2, \cdots, D_J\}$.
Strategy pairs	$\pi_A=\{\pi_{A_1}, \pi_{A_2}, \cdots, \pi_{A_I}\}$. $\pi_D=\{\pi_{D_1}, \pi_{D_2}, \cdots, \pi_{D_J}\}$.
Expected utilities	$EU_A=\{EU_A(\pi_{A_1}, \pi_{D_1}), \cdots, EU_A(\pi_{A_I}, \pi_{D_J})\}$. $EU_D=\{EU_D(\pi_{A_1}, \pi_{D_1}), \cdots, EU_D(\pi_{A_I}, \pi_{D_J})\}$.

B. Actions and Probability of Successful Attack

The attacker has several actions in action set A: Idle denoting no-operation action while Attack denoting all the possible attacks. In the case of attack, the level (the range of injected data), the target (the measured value or state value, which has been introduced in Section II.A), and the location (single-point attack or multi-point coordinated attack) can be selected. Obviously, the attacker's resource consumption C_{A_i} is related to the action A_i.

On the other hand, the defender's action set D: Idle representing no-operation action and Defend describing the possible defense actions, including increasing the defense intensity (e.g., increasing monitor scanning frequency), modifying defensive measures (e.g., detection threshold level), and expanding the defensive location. Similarly, the defender's resource consumption C_{D_j} is allocated to accomplish the action D_j.

The probability of a successful attack $\Pr(A_i, D_j)$ is mainly determined by the actions of the attacker and defender. Also, it is affected by the vulnerability $V_{\Pr}^n$ of the device at bus n. Several typical vulnerabilities in FDI attacks are selected as examples in Table II.

TABLE II
TYPICAL VULNERABILITIES IN FDI ATTACK

Vulnerability	Equipment	Description
CVE-2020-5304	Dashboard	The dashboard allows log injection via a substring in the independent parameter (IDP) to the uniform resource identifier (URI).
CVE-2022-35942	PC	Improper input validation may allow for arbitrary SQL injection which may affect the confidentiality and integrity of data stored on the connected database.
CVE-2010-2729	PC, PLC	The Print Spooler service does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory.
CVE-2010-2568	PC, PLC	Windows Shell allows local users or remote attackers to execute arbitrary code via a crafted (1). LNK or (2). PIF shortcut file, which is not properly handled during icon display in Windows Explorer.

The vulnerability of the device is defined by the CVSS metric [19]:

$$V_{\Pr} = 2 \times S_{AV} \times S_{AC} \times S_{AU} \tag{10}$$

where S_{AV} is the access vector; S_{AC} is the access complexity; and S_{AU} is the authentication, which is also adopted as a measuring element in [37, 38]. The vulnerability of bus n originates from devices and their connection logic [39]. The logic 'OR' assumes that any of the vulnerabilities exploited will cause system abnormality (an intelligent attacker will target the most susceptible vulnerability), as:

$$V_{\Pr}^n = \max(V_{\Pr,p}^n), V_{\Pr,p}^n \in \left\{V_{\Pr,1}^n, \cdots, V_{\Pr,P}^n\right\} \tag{11}$$

where P is the total number of vulnerabilities of the devices at bus n. The logic 'AND' requires that all the vulnerabilities be corrupted, as:

$$V_{\Pr}^n = \prod_{p=1}^{P} V_{\Pr,p}^n, V_{\Pr,p}^n \in \left\{V_{\Pr,1}^n, \cdots, V_{\Pr,P}^n\right\} \tag{12}$$

C. Strategy Pairs

For bus n, the strategy of the attacker and the defender can be expressed as follows:

$$\begin{cases} \pi_A^n = \left\{\pi_{A_1}^n, \pi_{A_2}^n, \cdots, \pi_{A_I}^n\right\}, \\ \text{s.t.} \sum_{i=1}^{I} \pi_{A_i}^n = 1, \forall i \in I, 0 \leqslant \pi_{A_i}^n \leqslant 1 \\ \pi_D^n = \left\{\pi_{D_1}^n, \pi_{D_2}^n, \cdots, \pi_{D_J}^n\right\}, \\ \text{s.t.} \sum_{j=1}^{J} \pi_{D_j}^n = 1, \forall j \in J, 0 \leqslant \pi_{D_j}^n \leqslant 1 \end{cases} \tag{13}$$

where π_A^n and π_D^n are the sets of action probabilities that can be selected by the attacker and the defender at bus n, respectively. When $\exists i \in I, \pi_{A_i}^n = 1$, the attacker strategy is a pure strategy, whereas in others, it is a mixed strategy. Similarly, for the defender, the pure strategy is satisfied only if $\exists j \in J, \pi_{D_j}^n = 1$.

D. Expected Utilities and Rewards

Given the attacker and defender strategy pair (π_A^n, π_D^n) for bus n, the expected utilities are defined as:

$$\begin{cases} EU_A^n(\pi_A^n, \pi_D^n) = \sum_{i=1}^{I} \pi_{A_i}^n \sum_{j=1}^{J} \pi_{D_j}^n U_A^n(A_i^n, D_j^n) \\ EU_D^n(\pi_A^n, \pi_D^n) = \sum_{j=1}^{J} \pi_{D_j}^n \sum_{i=1}^{I} \pi_{A_i}^n U_D^n(A_i^n, D_j^n) \end{cases} \tag{14}$$

where $U_A^n(A_i^n, D_j^n)$ and $U_D^n(A_i^n, D_j^n)$ calculate the expected utilities with action (A_i^n, D_j^n), as listed in Table III.

TABLE III
SIMPLIFIED EXPECTED UTILITIES MATRIX FOR THE GAME MODEL

$U_A^n(A_i^n, D_j^n)$ $U_D^n(A_i^n, D_j^n)$	A_1^n	$\cdots$	A_I^n
D_1^n	Eq. (9)	$\cdots$	Eq. (10)
$\vdots$	$\vdots$		$\vdots$
D_J^n	Eq. (13)	$\cdots$	Eq. (14)

$$\begin{cases} U_A^n(A_1^n, D_1^n) = -R_A \\ U_D^n(A_1^n, D_1^n) = R_D \end{cases} \tag{15}$$

There is no depletion of resources when both attacker and defender select Idle, and the utility comes solely from the reward. When the defender accomplishes to guarantee the system's normal operation which includes no attack and attack failure, the reward R_D belongs to the defender. On the other hand, the attacker is rewarded with R_A when the system operates anomalously, i.e., an attack is launched successfully. R_D is obtained by the mapping of W_z, which was defined in Section II.C. It is difficult to quantify R_A as it is affected not only by W_z but also by other factors, e.g., personal retaliation [41], national political behavior [3]. Therefore, this paper assumes $R_A = R_D$ from the defender's perspective.

$$\begin{cases} U_A^n(A_I^n, D_1^n) = R_A + Y^n(A_I^n, D_1^n) - C_{A_I}^n \\ U_D^n(A_I^n, D_1^n) = -Y^n(A_I^n, D_1^n) - R_D \end{cases} \tag{16}$$

where $C_{A_I}^n$ denotes the resource consumption required by the attacker to adopt the attack action A_I^n. The probability of attack failure can be ignored when there is no defense.

$$Y^n(A_i^n, D_j^n) = \sum_{z=1}^{Z} \Delta\vec{V}_z^n(A_i^n, D_j^n) W_z \tag{17}$$

where $Y^n(A_i^n, D_j^n)$ is the total impacted buses' state offsets $\Delta\vec{V}_z^n(A_i^n, D_j^n)$ multiplied by the bus safety characterization W_z, i.e. the absolute payoff without considering resource consumption; $Y_A^n(A_i^n, D_j^n) = -Y_D^n(A_i^n, D_j^n)$, i.e., the attacker's payoff is equal to the defender's negative payoff; Z is the total number of buses affected when bus n is attacked.

$$\Delta\vec{V}_z^n(A_i^n, D_j^n) = \vec{V}_z^n(A_i^n, D_j^n) - \vec{V}_z \tag{18}$$

where $\Delta\vec{V}_z^n(A_i^n, D_j^n)$ denotes the state offset of bus z when bus n is attacked, i.e., the difference between the voltage state $\vec{V}_z^n(A_i^n, D_j^n)$ after attack and the voltage state $\vec{V}_z$ during normal operation, which is obtained by WLS. The details can be found in Section II.B.

$$\begin{cases} U_A^n(A_1^n, D_J^n) = -R_A \\ U_D^n(A_1^n, D_J^n) = R_D - C_{D_J}^n \end{cases} \tag{19}$$

When the attacker does not attack and the defender defends, the attacker loses the reward, and the defender gains the reward but lose the resource consumption $C_{D_J}^n$ for the action D_J^n.

$$\begin{cases} U_A^n(A_I^n, D_J^n) = \Pr(A_I^n, D_J^n)\left[R_A + Y^n(A_I^n, D_J^n)\right] - C_{A_I}^n \\ U_D^n(A_I^n, D_J^n) = \left[1 - \Pr(A_I^n, D_J^n)\right]\left[R_D + Y^n(A_I^n, D_J^n)\right] - C_{D_J}^n \end{cases} \tag{20}$$

When both the attacker and the defender take action, their expected utilities are the product of the probability of the successful attack and payoff of the successful attack minus the attack resource consumption, and the product of the probability of normal operation and payoff minus the defense resource consumption, respectively. Because there may not be a Nash equilibrium in a non-zero-sum game matrix and the defender cannot obtain the attacker's action under incomplete information, the zero-sum game matrix is constructed as shown in Table IV.

The utility of the attacker is proportional to the negative of the defender's utility, i.e.:

$$U_A^n(A_i^n, D_j^n) = -U_D^n(A_i^n, D_j^n) \tag{21}$$

TABLE IV
SIMPLIFIED EXPECTED UTILITIES MATRIX FOR THE GAME MODEL FROM THE PERSPECTIVE OF THE DEFENDER

	A_1^n	$\cdots$	A_I^n
U_1^n	$U_D^n(A_1^n, D_1^n) = R_D$	$\cdots$	$U_D^n(A_1^n, D_1^n) = -Y^n(A_1^n, D_1^n) - R_D + C_{A_I}^n$
$\vdots$	$\vdots$		$\vdots$
U_I^n	$U_D^n(A_1^n, D_J^n) = R_D - C_{D_I}^n$	$\cdots$	$U_D^n(A_I^n, D_J^n) = \left[1 - \Pr(A_I^n, D_J^n)\right]\left[R_D + Y^n(A_I^n, D_J^n)\right] - C_{D_I}^n + C_{A_I}^n$

In game problems, both attacker and defender aim to maximize their total utilities. The Nash equilibrium is reached when they find the optimal strategy pairs which will not be deviated [42]. If there exists an attacker strategy π_A^n that maximizes the attacker utility $EU_A^n(\pi_A^n, \pi_D^n)$ for any defender strategy π_D^n, and at the same time, there exists a defender strategy π_D^n that maximizes the defender utility $EU_D^n(\pi_A^n, \pi_D^n)$ for any attacker strategy π_A^n, then a mixed strategy pair (π_A^n, π_D^n) is a Nash equilibrium solution:

$$\begin{cases} \exists\pi_A^n, EU_A^n(\pi_A^n, \pi_D^n) > \forall EU_A^n(\pi_A^n, \pi_D^n), \forall\pi_D^n \\ \exists\pi_D^n, EU_D^n(\pi_A^n, \pi_D^n) > \forall EU_D^n(\pi_A^n, \pi_D^n), \forall\pi_A^n \end{cases} \tag{22}$$

where $EU_A^n(\pi_A^n, \pi_D^n)$ and $EU_D^n(\pi_A^n, \pi_D^n)$ calculate the expected utilities with the optimal strategy sets of the attacker and defender, respectively.

For a zero-sum game, the mixed strategy is classified as an equilibrium outcome of the bimatrix game which is adopted when a pure strategy Nash equilibrium does not exist, i.e., a probability is assigned to each pure strategy, as suggested in [43]. It is proven in [44] that every bimatrix game has at least one Nash equilibrium solution in mixed strategies.

E. Game Solution

There are three parts to the solution procedure, as shown in Fig. 2.

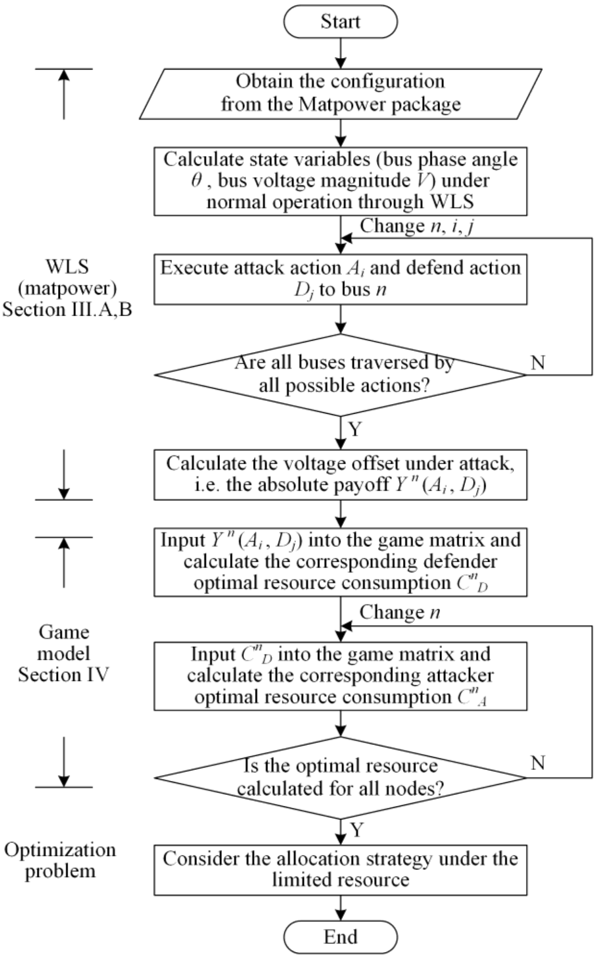
Start
Obtain the configuration from the Matpower package
Calculate state variables (bus phase angle θ, bus voltage magnitude V) under normal operation through WLS
Change n, i, j
Execute attack action A_i and defend action D_j to bus n
Are all buses traversed by all possible actions?
N
Y
Calculate the voltage offset under attack, i.e. the absolute payoff $Y^n(A_i, D_j)$
Input $Y^n(A_i, D_j)$ into the game matrix and calculate the corresponding defender optimal resource consumption C^n_D
Change n
Input C^n_D into the game matrix and calculate the corresponding attacker optimal resource consumption C^n_A
Is the optimal resource calculated for all nodes?
N
Y
Consider the allocation strategy under the limited resource
End
WLS (matpower) Section III.A,B
Game model Section IV
Optimization problem

Fig. 2. Procedure of the game solution.

The first part is to determine the system offset, i.e. absolute payoff $Y^n(A_i^n, D_j^n)$, caused by the attack in bus n, which has been presented in detail in Section II.B.

In the second part, the optimal strategy set pair (π_A^n, π_D^n) is selected based on $EU_A^n(\pi_A^n, \pi_D^n)$ and $EU_D^n(\pi_A^n, \pi_D^n)$. Here, the attacker's resource consumption C_{A_i} and the defender's resource consumption C_{D_j} vary. Their impact on the probability of successful attack $\Pr(A_i, D_j)$ is assumed as a known function that is associated with the bus vulnerability. This paper chooses the common experiment function relation as an example, and it should be noted that the function can be modified if there is enough prior knowledge or expert knowledge of the system so better results can be obtained. The Lemke-Howson Algorithm is used to solve this static single-stage game [44].

The third part involves resource allocation to each bus based on limited resources, with the knowledge of the optimal resource consumptions of the attacker C_{A_i} and the defender C_{D_j}. The resource allocation problem is an optimization issue, which can be solved by iteration [45], [46], deep learning [47], genetic algorithm [48] etc. The iteration method is utilized here, and the ORIGAMI algorithm is consulted to improve efficiency, as detailed in [45].

IV. Experimental Validation and Numerical Results

A. Simulation Experiment Validation

In this work, the IEEE 33-bus system [49] is adopted for the performance evaluation of the proposed solution. The configurations of the IEEE 33-bus system and the power flow calculation are based on MATPOWER (version 7.1). The Gaussian noises, the standard deviation of device measurement and measurement data are obtained from [50]. The solution is implemented using MATLAB (version R2021a) and executed on a computer equipped with a 3.20 GHz i7-97000 CPU and 16.00 G RAM.

The attacker's strategy means the level (the range of injected data), the target (the measured value or state value), and the location (single-point attack or multi-point coordinated attack). Figure 3 shows the network estimation (bus voltage amplitude and phase angle) in the attack-free condition and three network scenarios considering the attack action with the high level (30%) at different locations (buses 4, 8, and 12) on the specific measurement type (voltage amplitude), respectively.

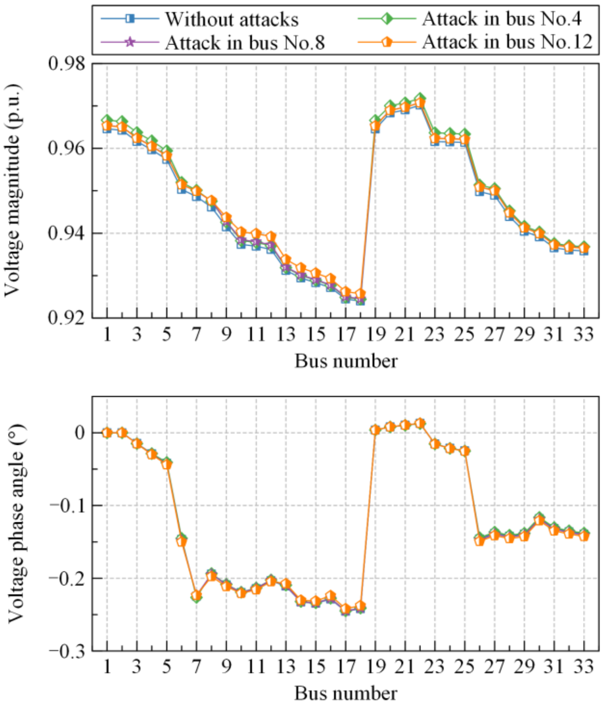

Fig. 3. Network estimation under different scenarios.

The estimated error caused by the attack can reach 0.5%, while such fluctuations will trigger alarms for some sensitive electrical equipment. The defender's strategy means configuring more defense methods including increasing the defense intensity (e.g., increasing monitor scanning frequency), modifying defensive measures (e.g., detection threshold level), and expanding the defensive location.

This section presents numerical results obtained from the simulations through a comparative study.

1) Defender's Resource Consumption

The analysis is conducted considering the impact of the defender's resource consumption C_{D_j} on the solution of the Nash equilibrium, while the impact of the attacker's resource consumption C_{A_i} is not considered. Figure 4 illustrates the relationship between the expected utility and the defender's resource consumption at bus 3.

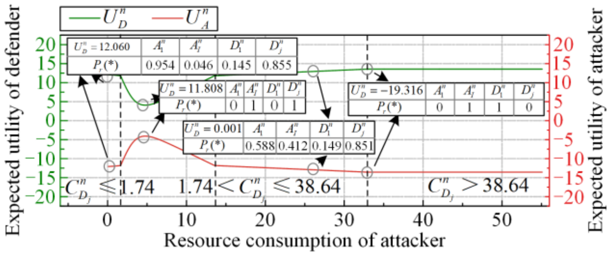

Fig. 4. Impact of defender's resource consumption.

As seen from Fig. 4, when $C_{D_J}\leqslant 1.74$, the pure strategy Nash equilibrium is selected such that the attacker and the defender both take action to occupy the reward because the attacker does not consider the resource consumption and the defender argues that the reward exceeds the resource consumption. Here, when the optimal defender's resource consumption $C_{D_j}=1.74$ is set, the expected utility $U_D^n(A_I^n,D_J^n)=11.808$ is the optimal solution for the defender.

When $1.74<C_{D_j}\leqslant 38.64$, the probability of a successful attack decreases with the increase of the defender's resource consumption, which leads the attacker to consider selecting Idle. Also, the defender hesitates to defend since the expected utility decreases as resource consumption increases. Obviously, the strategy matrix is a mixed strategy. Figure 5 is the game result when $C_{D_j}=15.93$, and the equilibrium point is (0.149, 0.588, 0.001), i.e., the saddle point of the game matrix.

When $C_{D_j}>38.64$, because it is expensive to take action for the defender, the attacker takes action in consideration that the rational defender will select Idle, even though the attack will definitely fail if the defender takes action. The defender concludes that the payoff cannot be sufficient to compensate for the resource consumption, so Idle is selected.

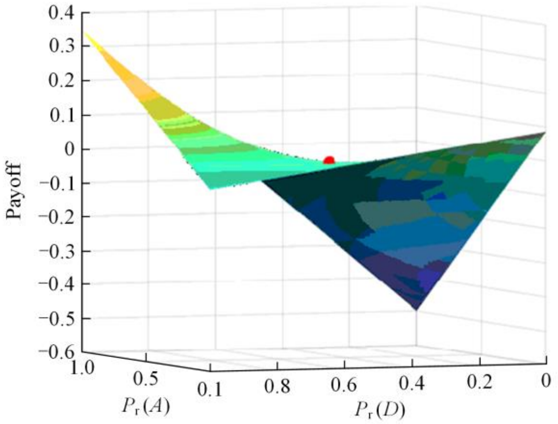

Fig. 5. Game result and the equilibrium point at $C_{D_j}=15.93$.

2) Attacker's Resource Consumption

Assume that the defender sets the optimal resource consumption according to the previous experiment, the impact of the attacker's resource consumption C_{A_i} is conducted. Figure 6 shows the relationship between the expected utility and the attacker's resource consumption at bus 3.

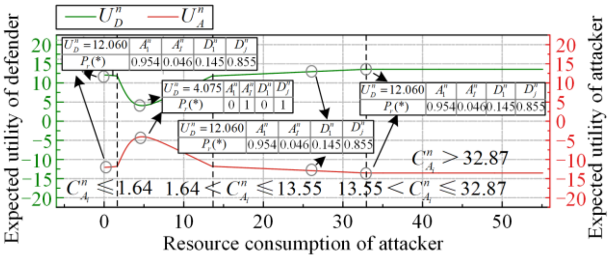

Fig. 6. Impact of attacker's resource consumption.

When $C_{A_i}\leqslant 1.64$, the rational attacker tends to select Idle in consideration of the low probability of a successful attack once the defender takes action, while the defender tends to take action because the payoff is greater than its resource consumption.

When $1.64<C_{A_i}\leqslant 13.55$, the probability of a successful attack is positively correlated with the attacker's resource consumption. Thus, the attacker concludes that the payoff outweighs the resource consumption and takes action. On the other hand, the defender selects defending to reduce the probability of a successful attack.

When $13.55<C_{A_i}\leqslant 32.87$, the attacker is more likely to give up attacking because of the high resource consumption, and the defender tends to select Idle in consideration of the poor payoff under the action.

When $C_{A_i}>32.87$, both the attacker and the defender select Idle because the attacker's resource consumption is too costly and the defender considers that the rational attacker will not take action. Thus, the defender may not allocate resource consumption when the difficulty of attacking the bus necessitates a considerable quantity of the attacker's resource consumption.

3) Summary

The analysis is conducted on the impact of the different buses which cause the value of rewards and the system offsets on the solution of optimal resource consumption. The attack action is unified as a low level (5%) on a specific measurement type (voltage amplitude). The optimal attacker's and defender's resource consumptions as well as the maximum and the minimum expected utilities of the defender (i.e., the minimum and the maximum expected utilities of the attacker) at buses 1-33 are presented in Fig. 7. Here, the optimal strategy is a mixed strategy under Nash equilibrium.

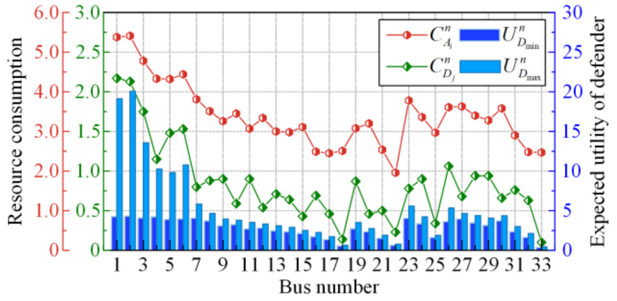

Fig. 7. The optimal resource consumption and the expected utility of the defender.

It can be observed that some buses are crucial but intensely competitive which require high resource consumption. Taking buses 1 and 2 as examples, if the attacker/defender can choose only one bus to take the attacking/defensive action, a rational attacker prefers to attack bus 2 as the expected utility is 5.58% higher than that of bus 1 at the price of 0.55% more resource consumption. Similarly, the defender prefers bus 2 as the expected utility is 5.58% higher than that of bus 1 with 1.88% less resource consumption. However, the cooperativity of multiple buses and uncertainty of the attacker require the defender to combine the relationship between resource consumption and expected utilities as shown in Figs. 4 and 6, and cannot directly assume a single-point defense to allocate resources. Therefore, further experiments are conducted for optimal resource allocation under limited resources considering the balance between efficiency and safety.

4) Limited Resources Allocation

Consider the optimal resource allocation strategy for the defender with limited resources and set the factor ϖ as the availability of resources: $R_{\text{lim}} = R_{\text{all}} \times \varpi$. Both the attacker and the defender are considered absolutely rational players, and the defender's action is quantified in five levels which denote the percentage of resource allocation in the optimal resource consumption, while the attacker is assumed to attack only one bus. Here, level 0 denotes 0%, i.e. Idle, level 1 denotes 25%, level 2 denotes 50%, level 3 denotes 75%, and level 4 denotes 100%. It should be noted that better results can be obtained with a higher quantity of levels but the computational complexity increases. Figure 8 shows the defender's optimal resource allocation strategy under the condition of different limited resources at buses 1-33.

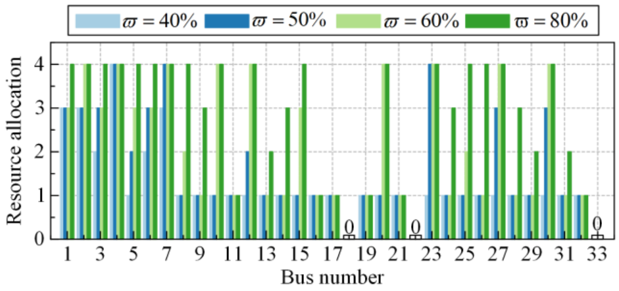

Fig. 8. Optimal allocation strategy with limited resources.

Compared with the results of no resource consumption and the results of resource consumption with vulnerability analysis based on [51], the proposed solution leads to 19.81% and 7.87% higher expected utilities, indicating that the proposed solution can provide appropriate allocations of defensive resources under limited resources.

B. RTDS Testbed Validation

The proposed solution is further assessed using the RTDS-based testbed for the IEEE 14-bus system [52] shown in Fig. 9(a) to demonstrate the effectiveness of the proposed method. Figures 9 (b) and (c) show the system model construction and the NovaCor hardware platform of RTDS, respectively. Assuming that only one bus is under attack and the defender has limited resources with the factor $\varpi = 40\%$, the maximum number of defensive resources (e.g., PMU) can be configured as 5. The attacker's resource consumption significantly increases if its target is configured with PMU. Figure 10 compares the bus voltage amplitudes under the original state without attack and three conditions under FDI attacks: without PMU configuration, PMU configuration with vulnerability analysis based on [53], and PMU configuration with the proposed method.

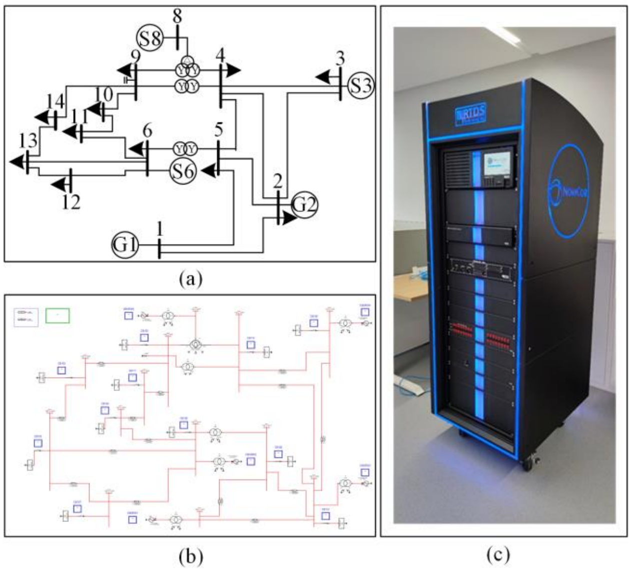

Fig. 9. IEEE 14-bus system and RTDS model. (a) IEEE 14-bus system. (b) System model construction. (c) NovaCor hardware platform of RTDS.

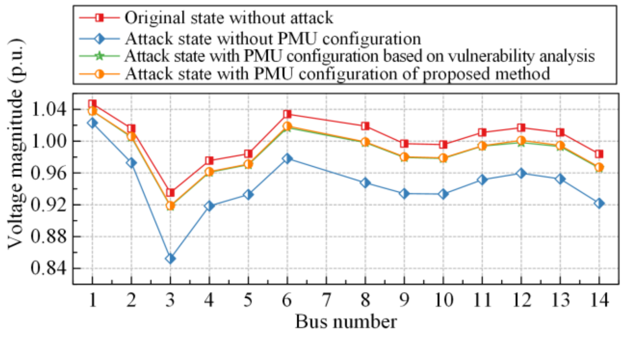

Fig. 10. Bus voltage amplitude under different conditions.

The numerical results obtained from the RTDS-based testbed experiments are consistent with the results from the previous simulations.

V. Conclusion

This paper investigates the game theory-based method for static defensive resource allocation strategy in the presence of FDI attacks in CPPS, and develops a zero-sum game model with incomplete information. In addition, an architecture is proposed including the threat model, state estimation method and bus safety characterization, which are improved based on existing researches to meet the requirements of the power system. Compared with the existing solutions, this work fully considers the trade-off between the overall system's safety and defensive resources utilization efficiency to adapt for more comprehensive development of CPPS in the future. The numerical results from the simulation and the RTDS-based testbed experiments demonstrate that the proposed solution is efficient and effective in identifying the optimal allocation of defensive resources with limited available defensive resources.

For future work, the situation of multiple game participants needs to be studied as more than one attacker may participate in the attacking process while multiple defenders need to carry out the collaborative defensive decision-making simultaneously. Also, this work has focused on the magnitude of changes in state variables, but their recovery time can significantly affect the system's stability in practice. In addition, the actual implementation and application of the game model require reliable data sets and expert knowledge, which require further investigation.

It can be observed that the reliable operation of the system is greatly affected by the FDI attack when no defensive measure is configured. PMU configurations with the vulnerability analysis and with the method proposed in this paper can effectively mitigate the impact on the grid system against the FDI attack by 71.94% and 73.76%, respectively. In addition, the result of PMU configuration with the proposed method is 6.93% better than that with the vulnerability analysis.

Acknowledgements

Not applicable.

Author's Contributions

Bingjing Yan: design the study, perform the research, and write the paper. Zhenze Jiang: analyze the data and design the study. Pengchao Yao and Qiang Yang: design the study and check English expression. Wei Li and Albert Y. Zomaya: perform research and check English expression. All authors read and approved the final manuscript.

Funding

This work is supported by the National Key Research and Development Program of China (No. 2023YFB 3107603), the "Pioneer" and "Leading Goose" R&D Program of Zhejiang (No. 2022C01239), the Special Support Plan for Zhejiang Province High-level Talents (No. 2022R52012), the National Natural Science Foundation of China (No. 52177119), and the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform).

Availability of Data and Materials

Not applicable.

Declarations

Competing interests: 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 article.

Authors' Information

Bingjing Yan is currently pursuing the PhD degree in the College of Electrical Engineering, Zhejiang University. Her research interests cover the game theory applications in cyber-physical systems.

Zhenze Jiang is currently pursuing the master degree in the College of Electrical Engineering, Zhejiang University. His research interests include the cyberspace security assessment and analysis in cyber-physical systems.

Pengchao Yao is currently pursuing the PhD degree in the College of Control Science and Engineering, Zhejiang University. His research interests include the active defense strategies of electric power infrastructures.

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

Wei Li received his PhD degree from the School of Information Technologies at The University of Sydney. He is currently a research fellow in center for distributed and high performance computing, the School of Computer Science, The University of Sydney. His research interests include internet of things, edge computing, sustainable computing, task scheduling, energy efficiency and optimization. He is the recipient of four IEEE or ACM conference best paper awards. He received the IEEE TCSC Award for Excellence in Scalable Computing for Early Career Researchers (2018) and the IEEE Outstanding Leadership Award (2018). He is a senior member of the IEEE Computer Society and the IEEE, and a member of the ACM.

Albert Y. Zomaya is currently the chair professor of high performance computing & networking in the School of Information Technologies, The University of Sydney. He is also the director of the center for distributed and high performance computing which was established in late 2009. He published more than 500 scientific papers and articles and is author, co-author or editor of more than 20 books. He served as the Editor in Chief of the IEEE Transactions on Computers (2011-2014). Currently, he serves as Editor in Chief of Springer's Scalable Computing and he is an associate editor for 22 leading journals, such as, the ACM Computing Surveys, IEEE Transactions on Computational Social Systems, IEEE Transactions on Cloud Computing, and Journal of Parallel and Distributed Computing. He is the recipient of the IEEE Technical Committee on Parallel Processing Outstanding Service Award (2011), the IEEE Technical Committee on Scalable Computing Medal for Excellence in Scalable Computing (2011), and the IEEE Computer Society Technical Achievement Award (2014). He is a chartered engineer, a fellow of AAAS, IEEE, IET (UK). His research interests are in the areas of parallel and distributed computing and complex systems.

References

[1] Z. Inayat, A. Gani, and N. B. Anuar *et al.*, "Intrusion response systems: foundations, design, and challenges," *Journal of Network and Computer Applications*, vol. 62. pp. 53-74, 2016.

[2] 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.

[3] Oxford Analytica. "Us pipeline hack to make ransomware risks a priority," *Emerald Expert Briefings*, (oxan-ga).

[4] T. M. Chen and Saeed Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4. pp. 91-93, Apr. 2011.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14. pp. 1-13, 2011.

[6] J. Ouyang, J. Yu, and X. Long *et al.*, "Coordination control method to block cascading failure of a renewable generation power system under line dynamic security," *Protection and Control of Modern Power Systems*, vol. 8, no. 1, pp. 194-204, Jan. 2023.

[7] J. Yang, G. Sun and J. Yin, "Coordinated cyber-physical attack considering false overload of lines," *Protection and Control of Modern Power Systems*, vol. 7, no. 4, pp. 670-682, Dec. 2022.

[8] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: worst-case robustness," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5710-5720, Nov. 2018.

[9] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326-333, Jun. 2011.

[10] S. Bi and Y. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1471-1485, Jul. 2014.

[11] S. K. Singh, K. Khanna, and R. Bose *et al.*, "Joint-transformation-based detection of false data injection attacks in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 89-97, Jan. 2017.

[12] Y. Dong, J. Yang, and Y. Zhu *et al.*, "Robust optimal dispatch of a power system based on a zero-sum game," *Power System Protection and Control*, vol. 50, no. 5, pp. 55-64, Mar. 2022. (in Chinese)

[13] C. T. Do, N. H. Tran, and E. Huh *et al.*, "Dynamics of service selection and provider pricing game in heterogeneous cloud market," *Journal of Network and Computer Applications*, vol. 69, pp. 152-165, 2016.

[14] M. Esmalifalak, G. Shi, and Z. Han *et al.*, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160-169, Jan. 2013.

[15] Q. Wang, W. Tai, and Y. Tang *et al.*, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169-177, 2019.

[16] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038-2049, Jul. 2016.

[17] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: a Stackelberg game analysis," *IEEE Transactions on Automatic Control*, vol.

63, no. 10, pp. 3503-3509, Oct. 2018.

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

[19] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," in *FIRST-Forum of Incident Response and Security Teams*, 2007, pp. 23-29.

[20] Q. Yang, J. Yang, and W. Yu *et al.*, "On false data-injection attacks against power system state estimation: modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, Mar. 2014.

[21] R. Deng, P. Zhuang, and H. Liang *et al.*, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871-2881, May 2019.

[22] C. Gu, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476-2483, Sep. 2015.

[23] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871-2881, May 2018.

[24] J. Zhao, L. Li, and Z. Xu *et al.*, "Full-scale distribution system topology identification using Markov random field," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4714-4726, Nov. 2020.

[25] Z. Xu, W. Jiang, and J. Xu *et al.*, "Distribution network topology identification using asynchronous transformer monitoring data," *IEEE Transactions on Industry Applications*, vol. 59, no. 1, pp. 323-331, Jan. 2023.

[26] T. Liu and T. Shu, "On the security of ANN-based AC state estimation in smart grid," *Computers & Security*, vol. 105, 2021.

[27] Y. Ju and Y. Huang, "State estimation for an AC/DC hybrid power system adapted to non-smooth characteristics," *Power System Protection and Control*, vol. 50, no. 2, pp. 141-150, Jan. 2023. (in Chinese)

[28] A. J. Monticelli, "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262-282, Feb. 2000.

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

[30] L. Devroye, "Nonuniform random variate generation," *Handbooks in Operations Research and Management Science*, vol. 13, pp. 83-121, 2006.

[31] J. Watters, "*Criticality levels,"* Berkeley, CA, USA: Apress, 2014, pp. 223-224.

[32] M. Zhao, R. V. Panda, and S. S. Sapatnekar *et al.*, "Hierarchical analysis of power distribution networks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 21, no. 2, pp. 159-168, Feb. 2002.

[33] D. Diakoulaki, G. Mavrotas, and L. Papayannakis, "Determining objective weights in multiple criteria problems: the critic method," *Computers & Operations Research*, vol. 22, no. 7, pp. 763-770, 1995.

[34] Y. Wang and Y. Luo, "Integration of correlations with standard deviations for determining attribute weights in multiple attribute decision making," *Mathematical and Computer Modelling*, vol. 51, no. 1-2, pp. 1-12, Jan. 2010.

[35] J. C Harsanyi, "Games with incomplete information played by "Bayesian" players, i–iii part i. the basic model," *Management Science*, vol. 14, no. 3, pp. 159-182, 1967.

[36] D. Fudenberg and J. Tirole, "*Game theory,"* Cambridge, MA, USA: MIT Press, 1991.

[37] X. Liu and L. Shi, "A dynamic game model for assessing risk of coordinated physical-cyber attacks in an AC/DC hybrid transmission system," *Frontiers in Energy Research*, vol. 10, 2023.

[38] J. Khoury and M. Nassar, "A hybrid game theory and reinforcement learning approach for cyber-physical systems security," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary, Apr. 2020, pp. 1-9.

[39] K. Huang, C. Zhou, and 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. 2019.

[40] N. Sayfayn and S. Madnick, "Cybersafety analysis of the maroochy shire sewage spill (preliminary draft)". 2017.

[41] M. Attia, H. Sedjelmaci, and S. M. Senouci *et al.*, "Game model to optimally combine electric vehicles with green and non-green sources into an end-to-end smart grid architecture," *Journal of Network and Computer Applications*, vol. 72, pp. 1-13, 2016.

[42] I. Erev, A. E. Roth, "Predicting how people play games: Reinforcement learning in experimental games with unique, mixed strategy equilibria," *American Economic Review*, pp. 848-881, 1998.

[43] T. Basar and G. J. Olsder, "Dynamic noncooperative game theory," *Society for Industrial and Applied Mathematics*, 1998.

[44] L. S. Shapley, "A note on the Lemke-Howson algorithm," in *Pivoting and Extension*, Springer, 1974, pp. 175-189.

[45] P. Lau, W. Wei, and L. Wang *et al.*, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4403-4414, Sep. 2020.

[46] A. Shahid, S. Aslam, and H. S. Kim *et al.*, "Distributed joint resource and power allocation in self-organized Femtocell networks: a potential game approach," *Journal of Network and Computer Applications*, vol. 46, pp. 280-292, 2014.

[47] M. Chen, W. Liu, and N. Zhang *et al.*, "Gpds: a multi-agent deep reinforcement learning game for anti-jamming secure computing in MEC network," *Expert Systems with Applications*, pp. 118394, 2022.

[48] M. Mejia, N. Pen˜a, and J. L. Mun˜oz *et al.*, "A game theoretic trust model for on-line distributed evolution of cooperation inmanets," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 39-51, Jan. 2011.

[49] S. H. Dolatabadi, M. Ghorbanian, and P. Siano *et al.*, "An enhanced IEEE 33 bus benchmark test system for

distribution system studies," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2565-2572, May 2020.

[50] Y. Wang, M. Xia, and Q. Yang *et al.*, "Augmented state estimation of line parameters in active power distribution systems with phasor measurement units," *IEEE Transactions on Power Delivery*, vol. 37, vol. 5, pp. 3835-3845, Oct. 2022.

[51] S. Zhang, H. Cheng, and K. Li *et al.*, "Optimal siting and sizing of intermittent distributed generators in distribu tion system," *IEEE Transactions on Electrical and Electronic Engineering*, vol. 10, 2015.

[52] P. K. Iyambo and R. Tzoneva, "Transient stability analysis of the IEEE 14-bus electric power system," in *AFRICON 2007*, Windhoek, South Africa, Sep. 2007, pp. 1-9.

[53] Q. Lai, C. Liu, and K. Sun, "Vulnerability assessment for voltage stability based on solvability regions of decoupled power flow equations," *Applied Energy*, vol. 304, pp. 117738, 2021.