An AI-Enhanced Bayesian Game Defense Framework for Electrical-Thermal Coupled Integrated Energy Systems

Bingjing Yan *[1], Chenhuan Cui *[2], Qiang Yang †[1], Shiming He *[3], Yaoxia Shao *[4] and Mengting Zhang *[5]
*School of Information and Electrical Engineering, Hangzhou City University, Hangzhou, China
[1]yanbj@zju.edu.cn, [2]cuich@hzcu.edu.cn, [3]hsm@hzcu.edu.cn, [4]shaoyx@hzcu.edu.cn, [5]mengtingzhang@hzcu.edu.cn
†College of Electrical Engineering, Zhejiang University, Hangzhou, China
[1]qyang@zju.edu.cn

***Abstract*—Integrated Energy Systems (IES) combine electricity, heat and natural gas through digital control to coordinate multi-energy operation. The resulting cyber-physical coupling improves flexibility but also enlarges the attack surface and accelerates cross-domain propagation of cyberattacks. This paper proposes a Bayesian game-theoretic defense framework for electrical-thermal coupled IES that captures attacker-defender interactions, asymmetric utilities and physical coupling constraints under incomplete information. On this basis, an adaptive defense module is designed by integrating Q-learning with dynamic state estimation, enabling online policy optimization and fast convergence under uncertain, time-varying conditions. The framework is validated on a micro gas turbine (MGT)-based IES platform using empirical electrical-thermal measurements, including exhaust temperature, thermal inertia and NO_x emissions, together with comparative simulations on a modified IEEE 33-bus test system. The results show that the proposed method significantly reduces attack-induced power and temperature deviations, improves the defender's expected utility and enhances overall system resilience, providing a scalable and experimentally verifiable active defense approach for digitalized electrical-thermal IES.**

***Index Terms*—AI-enabled defense, Bayesian game theory, integrated energy systems, cybersecurity, electrical-thermal coupling, reinforcement learning.**

I. Introduction

The rapid digitalization and intelligent transformation of global energy systems are driving the deep integration of cyber and physical domains, enabling more efficient monitoring, coordination, and optimization across electricity, heat, and gas networks. However, this convergence also reinforces the interdependencies between information infrastructures and physical assets, thereby expanding the potential attack surface of modern energy systems [1], [2]. Among these, Integrated Energy Systems (IES)—which coordinate the multiple energy subsystems through digital control [3]—represent a typical form of such coupling. While this architecture enhances energy management flexibility and cross-domain coordination, it simultaneously exposes IES to cascading disruptions triggered by cyber threats such as false data injection (FDI) and distributed denial-of-service (DDoS) attacks.

In recent years, numerous large-scale cyber incidents have revealed the fragility of energy cyber-physical systems. The 2015 cyberattack on Ukraine's power grid caused large-scale blackouts [4]; the Stuxnet malware compromised operations at Iran's nuclear facilities [5]; and in 2025, a cyberattack reportedly led by Pakistan paralyzed approximately 70% of India's national power grid [6]. These incidents underscore the escalating threats posed by cross-domain cyber intrusions: once malicious signals are injected into a single subsystem, they can propagate across coupled energy domains and result in cascading failures. Consequently, the secure operation of digitalized IES requires not only conventional intrusion detection and control recovery but also an intelligent defense strategy capable of adaptive decision-making under uncertainty.

Early cybersecurity studies mainly examined thermal or Heating, Ventilation, and Air Conditioning (HVAC) control loops, identifying vulnerabilities through man-in-the-middle and threat-injection attack analyses [7]–[9]. However, these works focused on isolated thermal subsystems and did not consider cross-domain interactions or the feedback effects of defense responses. With the rise of multi-energy coupling, cybersecurity analysis has expanded to IES. Recent efforts include resilience assessment and coordinated defense for electricity-heat systems [10], [11]. However, these models typically depend on simplified thermal assumptions and lack validation using realistic electrical-thermal interactions. In game-theoretic defense research, Bayesian methods have been applied to model decision-making under incomplete information [12]. Existing approaches, however, mainly address single-domain electrical networks and overlook the interdependent dynamics of electrical-thermal systems.

To address these limitations, this study proposes a **Bayesian game-theoretic defense framework for electrical-thermal coupled IES**. The framework characterizes attacker-defender strategic interactions and asymmetric utility trade-offs under incomplete information, allowing each side to consider both gains and associated costs. Specifically, the attacker's utility incorporates induced load deviations and operational perturbations, while the defender's cost includes recovery time, fluc-

979-8-3315-8138-1

tuation range, and control resource limitations—collectively capturing the thermal inertia and physical coupling characteristics of the system. Building on this formulation, an **adaptive strategy learning module** combining Q-learning and **dynamic state estimation** is developed to achieve online policy optimization and rapid convergence of defense strategies in uncertain and dynamic environments.

Experimental validation is performed using **empirical electrical-thermal data** from an MGT-based IES platform, where measurable indicators such as exhaust temperature, thermal inertia, and NO_x emissions are employed to evaluate disturbance sensitivity and defensive adaptability under operational perturbations. Additionally, comparative simulations on a modified IEEE 33-bus IES test system demonstrate that the proposed approach effectively mitigates attack-induced deviations, improves learning convergence, and enhances overall system resilience and defense efficiency—providing a scalable and data-driven pathway toward secure operation in the emerging *Digital Energy Network Era*.

The main technical contributions of this work are summarized as follows:

1) A **Bayesian game-theoretic defense framework** is proposed for IES, jointly considering electrical–thermal coupling and modeling attacker–defender interactions under incomplete information.
2) A **reinforcement learning-based adaptive strategy module** is developed by integrating Q-learning with dynamic state estimation, enabling efficient policy exploration and fast convergence of defense strategies in uncertain and dynamic environments.
3) The proposed framework is validated using **empirical electrical-thermal data** from an MGT-based IES platform and comparative simulations on a modified IEEE 33-bus system, demonstrating its effectiveness in mitigating attack-induced deviations, improving convergence, and enhancing overall system resilience.

The paper is organized as follows: Section II formulates the system model and problem, Section III presents the proposed algorithms, Section IV reports simulation and experimental results, and Section V concludes the paper.

II. System Design and Problem Formulation

A. System Dynamics and Attack-Induced Perturbation of States

The IES consists of an electrical subsystem and a thermal subsystem coupled through an energy conversion unit such as an MGT. The dynamic behavior of the system can be expressed by a set of coupled state equations describing both electrical and thermal interactions.

1) Electrical Subsystem: The electrical dynamics are governed by the power flow equations:

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

where P_i and Q_i denote the real and reactive power injections at bus i; V_i and θ_i are the voltage magnitude and phase angle; and G_{ij} and B_{ij} represent the conductance and susceptance between buses i and j, respectively.

During normal operation, system states $\mathbf{x} = [V_i, \theta_i]^T$ are estimated from measurement data:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{2}$$

where $\mathbf{e}$ represents Gaussian measurement noise. Under an FDI attack, a malicious vector $\mathbf{a}$ is injected into the measurement stream:

$$\mathbf{z}' = \mathbf{z} + \mathbf{a} \tag{3}$$

leading to a perturbed state estimate $\hat{\mathbf{x}}' = \mathbf{x} + \Delta\mathbf{x}$. The resulting power imbalance is approximated by the linearized relation:

$$\Delta P \approx J_P \Delta\mathbf{x} \tag{4}$$

where $J_P = \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}$ is the Jacobian matrix of the power-flow model. Hence, ΔP represents the sensitivity of power deviations to the injected attack vector.

2) Thermal Subsystem: The thermal subsystem is modeled by the first-order thermal inertia equation:

$$C_{th}\frac{dT}{dt} = Q_{\text{in}} - Q_{\text{out}} - H_{\text{loss}} \tag{5}$$

where C_{th} is the equivalent thermal capacitance, Q_{in} and Q_{out} denote the heat inflow and outflow, and H_{loss} accounts for thermal dissipation. In the case of an MGT-based IES, the heat inflow is proportional to the turbine's electrical power:

$$Q_{\text{in}} = \eta_{th} P_{\text{GT}} \tag{6}$$

where η_{th} is the thermal efficiency coefficient. When an FDI attack or denial-of-service event disturbs the electrical output, the resulting thermal response satisfies:

$$C_{th}\frac{d(\Delta T)}{dt} + \frac{\Delta T}{R_{th}} = \eta_{th}\Delta P \tag{7}$$

where R_{th} represents the equivalent thermal resistance of the heat network. This relationship describes how electrical disturbances propagate through the electrical-thermal coupling, producing measurable temperature deviations ΔT [13].

3) Coupled Perturbation Model: By combining the above formulations, the cyber-induced perturbations can be expressed as:

$$\Delta x(t) = \begin{bmatrix} \Delta P(t) \\ \Delta T(t) \end{bmatrix} \tag{8}$$

which jointly characterize the dynamic deviations of electrical and thermal domains under cyberattack conditions. These quantities serve as the state variables for evaluating the system's vulnerability, including the cross-domain propagation captured by ΔT, and form the basis for the attacker-defender game-theoretic model developed in Section II-C.

B. Bayesian Game Model under Incomplete Information

In an IES, both the attacker and defender operate under uncertainty due to the incomplete observability of system states and the stochastic nature of cyber-physical disturbances. To model this interaction, a Bayesian game framework is adopted, where each player maintains a probabilistic belief about the opponent's type and chooses actions accordingly.

1) Game Structure: The Bayesian game can be defined as:

$$G = \langle P, \mathcal{A}, \mathcal{D}, R, U \rangle \tag{9}$$

where:

- $P = \{P_A, P_D\}$ represents the set of players, with P_A denoting the attacker and P_D the defender.
- $\mathcal{A} = \{A_1, A_2, \ldots, A_I\}$ and $\mathcal{D} = \{D_1, D_2, \ldots, D_J\}$ are the finite sets of attack and defense actions, respectively.
- $R(A_i, D_j)$ denotes the reward or cost incurred by the interaction between strategies A_i and D_j, which is embedded into the subsequent utility.
- $U = \{U_A, U_D\}$ represents the expected utility functions of the attacker and defender.

Following Harsanyi's transformation [14], the incomplete-information static game is converted into a complete but imperfect-information game by introducing a fictitious player "Nature." Nature randomly selects each player's type $\tau_A \in \mathcal{T}_A$ and $\tau_D \in \mathcal{T}_D$ according to a joint probability distribution $\Pr(\tau_A, \tau_D)$, representing the likelihood of different attacker-defender type combinations. Here, τ_A and τ_D characterize the attacker's capability and the defender's resource availability, respectively. The joint probability $\Pr(\tau_A, \tau_D)$ can be estimated from historical operation data, intrusion records, or expert assessments [15]. Each player maintains a prior belief distribution $\mathbf{b} = \{b_A,\, b_D\}$ about the opponent's type, which can be initialized from empirical statistics or simulation results and iteratively updated through Bayesian inference using observed responses. This formulation captures the information asymmetry of real IES security scenarios, where attackers infer system vulnerabilities from limited signals, while defenders estimate threat levels from sparse intrusion data.

2) Utility Functions: The attacker's utility reflects the benefit gained from perturbing the system, while the defender's utility quantifies system stability and the efficiency of countermeasures. Let the utility functions be defined as:

$$\begin{aligned} U_A(A_i, D_j) &= \alpha_1 |\Delta P| + \alpha_2 |\Delta T| - C_A(A_i), \\ U_D(A_i, D_j) &= -\beta_1 |\Delta P| - \beta_2 |\Delta T| - C_D(D_j), \end{aligned} \tag{10}$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are weighting coefficients calibrated through sensitivity analysis and normalization [16], ensuring comparable influence between electrical and thermal deviations on system stability. $C_A(A_i)$ and $C_D(D_j)$ quantify the resource consumption or operational overhead associated with executing attack and defense actions, respectively. For instance, C_A may represent computational or bandwidth costs during an FDI attack, while C_D captures control reconfiguration costs or recovery delays due to defensive countermeasures. The system is modeled as a constrained non-zero-sum game, capturing the predominantly competitive nature of cyber conflicts in IES while still allowing for asymmetric costs on both sides.

3) Expected Utility and Nash Equilibrium: Set $\pi_A = [\pi_{A_1}, \ldots, \pi_{A_I}]$ and $\pi_D = [\pi_{D_1}, \ldots, \pi_{D_J}]$ as the mixed strategies of the attacker and defender, respectively. Their expected utilities are given by:

$$\begin{aligned} EU_A(\pi_A, \pi_D) &= \sum_{i=1}^{I} \sum_{j=1}^{J} \pi_{A_i} \pi_{D_j} U_A(A_i, D_j), \\ EU_D(\pi_A, \pi_D) &= \sum_{i=1}^{I} \sum_{j=1}^{J} \pi_{A_i} \pi_{D_j} U_D(A_i, D_j). \end{aligned} \tag{11}$$

The Nash equilibrium (π_A^*, π_D^*) represents a stable state where neither player can improve its expected utility by unilaterally deviating:

$$\begin{aligned} EU_A(\pi_A^*, \pi_D^*) &\geq EU_A(\pi_A, \pi_D^*), \quad \forall \pi_A, \\ EU_D(\pi_A^*, \pi_D^*) &\geq EU_D(\pi_A^*, \pi_D), \quad \forall \pi_D. \end{aligned} \tag{12}$$

At equilibrium, the defense strategy minimizes the expected deviations $\{|\Delta P|, |\Delta T|\}$ while optimizing resource allocation, achieving a balance between cyber-resilience and operational efficiency. To capture the adaptive evolution of strategies and belief updates under uncertainty, Section II-C introduces a reinforcement learning mechanism that dynamically adjusts mixed strategies and accelerates convergence toward the Bayesian equilibrium.

C. Adaptive Strategy Learning based on Q-learning and Dynamic State Estimation

To achieve real-time adaptability beyond the static Bayesian equilibrium, an adaptive defense mechanism is introduced by integrating Q-learning with dynamic state estimation, which approximates equilibrium behavior under uncertainties. The defender interacts with the environment to iteratively update its mixed strategy π_D. At each time t, the defender observes the system state s_t, performs action a_t, receives reward r_t, and updates the Q-value as:

$$Q_{t+1}(s_t, a_t) = (1-\lambda) Q_t(s_t, a_t) + \lambda [r_t + \gamma \max_{a'} Q_t(s_{t+1}, a')], \tag{13}$$

where λ and γ are the learning rate and discount factor. The reward is defined as

$$r_t = -(\beta_1 |\Delta P_t| + \beta_2 |\Delta T_t| + C_D(D_j)), \tag{14}$$

penalizing system deviations and resource usage. The system state $\mathbf{x}_t = [P_t, T_t, V_t, \ldots]$ is recursively estimated using an Extended Kalman Filter (EKF) [17], ensuring that policy updates reflect both cyber and physical variations:

$$\hat{\mathbf{x}}_{t|t} = \hat{\mathbf{x}}_{t|t-1} + K_t(\mathbf{z}_t - \mathbf{h}(\hat{\mathbf{x}}_{t|t-1})). \tag{15}$$

An ϵ-greedy policy ensures exploration during learning, and convergence is achieved when $\|Q_{t+1} - Q_t\| < \varepsilon$. This integration enables the defender to approximate the Bayesian equilibrium adaptively, achieving resilient and efficient decision-making under dynamic uncertainties in IES.

III. Game Model Solution and Algorithms

The proposed Bayesian game model is solved using a two-stage process combining data-driven state estimation and reinforcement learning. First, the pre-collected operational data are filtered using the EKF to remove noise and infer system deviations ΔP_t and ΔT_t caused by cyberattacks. Then, the Q-learning algorithm iteratively updates the defender's mixed strategy π_D toward the Bayesian equilibrium under uncertain and dynamic conditions.

Algorithm 1 Adaptive Q-learning-Based Defense Strategy

Require: Learning rate λ, discount factor γ, exploration rate ϵ

Ensure: Optimal defense policy π_D^* and equilibrium utilities EU_A, EU_D

1: Initialize $Q(A_i, D_j) = 0$ for all $(A_i, D_j) \in A \times D$
2: **repeat**
3: Observe state s_t via EKF, receive A_i, and select D_j using an ϵ-greedy rule
4: Compute instantaneous reward $r_t = -(\beta_1|\Delta P_t| + \beta_2|\Delta T_t| + C_D(D_j))$
5: Update Q-value:

$$Q_{t+1}(A_i, D_j) = (1-\lambda)Q_t(A_i, D_j) + \lambda\big[r_t + \gamma \max_{A', D'} Q_t(A', D')\big]$$

6: **until** $\|Q_{t+1} - Q_t\| < \varepsilon$
7: **return** $\pi_D^* = \arg\max Q(A_i, D_j)$

This approach allows the defender to approximate equilibrium strategies through online learning, while EKF-based estimation ensures that cyber-physical feedback is reflected in real time. Compared with traditional static optimization, the proposed algorithm enhances adaptability and convergence efficiency under time-varying attack environments.

IV. Experimental Validation and Performance Evaluation

A. Simulation Experiment Validation

Simulation experiments were conducted on a modified IEEE 33-bus system with an electrical-thermal coupling module, where an MGT unit fueled by compressed hydrogen (700 bar) was modeled as the core combined heat and power (CHP) device. The empirical MGT dataset, summarized in Table I, and the corresponding physical hydrogen-fueled micro gas turbine are shown in Fig. 1.

These parameters are directly derived from experimental measurements on the laboratory MGT platform and are employed to calibrate the thermal side of the coupled system and the thermal ΔT dynamics in (7). Specifically, the generation efficiency (26%) and output power (30 kW) define the steady-state reference operating point, while the total available heat energy (208 kWh) bounds the feasible energy conversion region. The runtime constraint (1.6 h) under two 80 L hydrogen bottles serves as a practical endurance limit and is used to verify the stability of control and defense algorithms during long-term operation.

TABLE I: Experimental Parameters of the Hydrogen-Fueled MGT

Parameter	Value
Lower heating value (LHV)	33.3 kWh/kg
Fuel density	39.1 kg/m^3
Total heat energy	208.1 kWh
Generation efficiency	26.0%
Electrical output power	30.0 kW
Thermal input power	115.4 kW
Actual runtime (2 bottles, 10% reserve)	1.6 h

Fig. 1: Hydrogen-fueled micro gas turbine and experimental parameters.

Electrical network simulations adopt MATPOWER 7.1, with SCADA measurement noise $\sigma_{SCADA} = 0.02$ and PMU noise $\{\sigma_V, \sigma_\theta\} = \{0.005, 0.002\}$. An EKF is employed for state estimation to track coupled electrical-thermal dynamics. All experiments are implemented in MATLAB R2021a on an i7-9700 CPU with 16 GB RAM.

B. Performance Evaluation

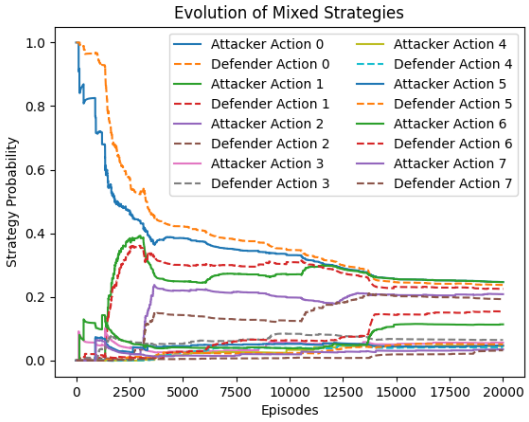
The proposed Bayesian defense framework is evaluated through both iterative game dynamics and its convergence behavior under multiple cyberattack scenarios. The attacker and defender strategy spaces are discretized into s levels, forming mixed strategies $\pi_A, \pi_D \in \{0, 1, \ldots, s-1\}$, where a larger s provides higher action granularity without compromising computational efficiency.

Fig. 2a illustrates the evolution of mixed strategies for both players. Initially, the attacker frequently alternates among high-impact actions, while the defender explores countermeasures of varying intensity. As learning progresses, feedback from electrical deviations ΔP and thermal variations ΔT gradually steers both players toward stable probability distributions. The curves eventually flatten, indicating that neither player can further increase its expected utility and that a Nash equilibrium is reached, corresponding to stabilized coupled electrical–thermal states.

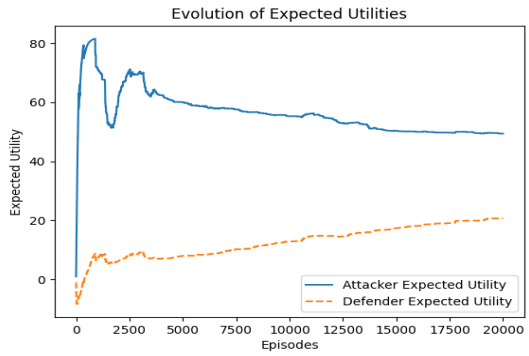
Fig. 2b presents the expected-utility trajectories. Early iterations exhibit sharp oscillations because small disturbances in ΔP or ΔT amplify utility changes. As Q-learning refines the defense policy and EKF improves state estimation, the defender's utility rises while the attacker's declines. Both eventually stabilize, confirming convergence to equilibrium and suppression of coupled electrical–thermal deviations.

Table II provides a quantitative comparison of five representative attack scenarios. A clear trend is observed: higher attack intensity results in larger electrical deviations ΔP, more pronounced thermal responses ΔT, and increased attacker utility. Notably, ΔT rises faster due to the thermal inertia captured from the MGT measurements.

Across all scenarios, the proposed defense converges within approximately 1.3×10^4 iterations. Mild FDI attacks converge the fastest, while hybrid attacks require more iterations due to



(a) Convergence of Mixed Strategies During Iterative Learning



(b) Convergence of Expected Utilities for Attacker and Defender

Fig. 2: Experimental Results: Convergence Behavior of Mixed Strategies and Expected Utilities

TABLE II: Cyber-Physical Impact Across Different Attack Scenarios

Scenario	$\Delta \mathbf{P}$ (kW)	$\Delta \mathbf{T}$ (°C)	$\mathbf{U_A}$	**Iter. to Conv.**
Mild FDI	2.4	3.1	5.8	11,950
Strong FDI	5.1	7.4	12.6	12,220
Mild DDoS	3.0	4.2	7.2	13,080
Strong DDoS	6.4	9.1	14.8	14,380
Hybrid FDI+DDoS	7.8	10.6	18.3	14,540

compounded disturbances. This consistent convergence behavior demonstrates the robustness of the reinforcement learning module and the effectiveness of the Bayesian decision-making framework under dynamic cyber-physical uncertainties.

Overall, the results show that the proposed approach effectively suppresses attack-induced deviations, stabilizes coupled electrical-thermal states, and achieves rapid convergence. The incorporation of empirical MGT thermal data further enhances situational awareness, providing a practical and scalable active defense solution for digitalized IES.

V. Conclusion

This paper presented a Bayesian game-theoretic defense framework for electrical-thermal coupled IES under incomplete cyber-physical information. By combining physical coupling constraints, MGT-based electrical-thermal measurements, and a Q-learning adaptive strategy module, the framework provides a unified and data-driven approach for defense optimization under uncertainty.

Simulation and experimental studies show that it suppresses attack-induced deviations, enhances system resilience, and achieves fast convergence to stable defense policies. Future work will consider coordinated multi-attacker scenarios, multi-agent reinforcement learning for distributed defense, and scalable deployment for real-time operation in IES control centers.

References

[1] Yingjun Wu, Hao Xu, and Ming Ni. Defensive resource allocation method for improving survivability of communication and information system in cpps against cyber-attacks. *Journal of Modern Power Systems and Clean Energy*, 8(4):750–759, 2020.

[2] Krishna Kumar, Neeraj Kumar Pandey, Filippo Verre, and Rachna Shah. Cybersecurity challenges in the digitization and integration of renewable energy systems: A review. *IEEE Transactions on Engineering Management*, 72:3042–3054, 2025.

[3] Jianzhnog Wu, Jinyue Yan, Hongjie Jia, Nikos Hatziargyriou, Ned Djilali, and Hongbin Sun. Integrated energy systems, 2016.

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

[5] Thomas M. Chen and Saeed Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[6] Guo Yuandan. Pak military says it 'paralyzed 70% of india's power grid,' further verification needed, but power facilities are vulnerable targets: expert. Global Times, May 10, 2025, 2025. Accessed: 2025-11-06.

[7] Kaveh Paridari, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, and Henrik Sandberg. A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. *Proceedings of the IEEE*, 106(1):113–128, 2017.

[8] Yiyuan Qiao, Dongyu Chen, Qun Zhou Sun, Guanyu Tian, and Wenyi Wang. Unveiling stealthy man-in-the-middle cyber-attacks on energy performance in grid-interactive smart buildings. *Energy Conversion and Management*, 319:118949, 2024.

[9] Yangyang Fu, Zheng O'Neill, Zhiyao Yang, Veronica Adetola, Jin Wen, Lingyu Ren, Tim Wagner, Qi Zhu, and Terresa Wu. Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings. *Applied Energy*, 303:117639, 2021.

[10] W. Ding, W. Gu, S. Lu, R. Yu, and L. Sheng. Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism. *Applied Energy*, 311:118650, 2022.

[11] W. Gu, W. Ding, S. Lu, P. Zhao, D. Zou, Y. Qiu, R. Yu, and L. Sheng. Coordinated heat and power cyber-attacks with time window matching strategy. *IEEE Transactions on Smart Grid*, 14(4):2747–2761, 2023.

[12] Hui Ge, Lei Zhao, Dong Yue, Xiangpeng Xie, Linghai Xie, Sergey Gorbachev, Iakov Korovin, and Yuan Ge. A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack. *Information Sciences*, 652:119759, 2024.

[13] Rafal Wrobel, Barrie Mecrow, and Maamar Benarous. Thermal evaluation of a short-operating-duty dual-lane fault-tolerant actuator for aerospace applications. *IEEE Transactions on Industry Applications*, 59(4):4083–4094, 2023.

[14] John C Harsanyi. Games with incomplete information played by "bayesian" players, i–iii part i. the basic model. *Management science*, 14(3):159–182, 1967.

[15] Mohamed R. Elkadeem, Kotb M. Kotb, Atif S. Alzahrani, and Mohammad A. Abido. Design and global sensitivity analysis of a power-to-hydrogen-to-power-based multi-energy microgrid under uncertainty. *IEEE Transactions on Industry Applications*, 61(2):1811–1827, 2025.

[16] Buxiang Zhou, Rui Su, Tianlei Zang, Chuangzhi Li, Xiaoning Tong, and Yahui Gong. Resilience assessment of power-thermal systems considering coordinated cyber and physical attacks. *IEEE Internet of Things Journal*, 12(19):40159–40175, 2025.

[17] Dezhi Yuan, Ting Luo, Chaochen Gu, and Kunpeng Zhu. The cyber-physical system of machine tool monitoring: A model-driven approach with extended kalman filter implementation. *IEEE Transactions on Industrial Informatics*, 19(9):9576–9585, 2023.