Cyber-Resilient Strategy for Coupled Electric-Heating Distributed Energy Systems Management under Coordinated False Data Injection Attacks

Jiyuan Li[1,2], Xinyue Chang[1,2,*], Yixun Xue[1,2], Xiao Fan[3]
Taiyuan University of Technology
1. Key Laboratory of Cleaner Intelligent Control on Coal & Electricity, Ministry of Education
2. College of Electrical and Power Engineering
3. College of Electronic Information Engineering
Taiyuan, China

542658099@qq.com

Hongbin Sun[1,4]
Tsinghua University
4. Department of Electrical Engineering
Beijing, China

***Abstract*—With the increasing integration of cyber and communication technologies, coupled electric-heating energy systems have become more susceptible to cyberattacks. When multiple attack sources exist within the system, the coordinated effects among them are often overlooked. This paper first introduces a coordinated false data injection attack model targeting the dispatch process and further accounts for multiple coordination patterns among the attack sources. To effectively isolate malicious behaviors and ensure secure and economic system dispatch, a distributed energy management strategy based on communication link reputation is further proposed. The strategy incorporates the influence of each energy entity on its neighbors and introduces a multidimensional dynamic residual estimation method to fully capture the coordinated characteristics among the attack sources. Numerical case studies demonstrate both the detrimental impact of coordinated attacks and the effectiveness of the proposed defense strategy.**

***Index Terms*—distributed energy systems management, coordinated false data injection attacks, coupled electric-heating energy systems, dynamic residual estimation.**

I. INTRODUCTION

The development of combined heat and power (CHP) technology has enhanced the capacity efficiency of coupled electricity-heating energy systems (EHES), while strengthening the integration between electrical and district heating networks [1], [2]. Moreover, with the integration of information and communication technology, traditional EHES are evolving into a new type of coupled electricity-heating cyber-physical system (EHCPS) [3]. This transformation has significantly enhanced the energy management efficiency of the system, but it has also introduced corresponding cybersecurity risks.

The study of cyberattack patterns is a crucial prerequisite for ensuring the information security of the system. Among various types of attacks, false data injection attacks (FDIAs) have long been one of the most intensively studied subjects due to their diverse attack patterns and high concealment. In EHCPSs, attackers may launch FDIAs in different ways depending on the specific stage of the energy management process. The first type is the state-estimation attack, where adversaries construct injection vectors consistent with the system's measurement matrix to manipulate sensor data and mislead the state estimator; these attacks are highly stealthy. The second type is the control-layer attack, target actuator commands or feedback signals such as automatic voltage control (AVC) and automatic generation control (AGC) setpoints [4], potentially causing improper control actions or dynamic instability. The third type is the monitoring and protection-oriented FDIA, which alters the status or alarm signals of the monitoring system [5], potentially causing false tripping or denial of operation, thereby aggravating cascading failures. A typical example of this type is an attack targeting the supervisory control and data acquisition (SCADA) system. A fourth class, the optimization or dispatch attack, which falsifies load forecasts, power generation, or market price information to distort energy management, leading to issues such as mismatching, increased operational cost, and power limit violations of equipment. Such attacks are often more concealed and can trigger cascading physical effects, causing broader and more persistent damage to system security.

To address the issue of FDIAs in energy systems, researchers have conducted meaningful studies. Methods such as sliding time window strategy [6] and joint meter coding [7] are employed to detect FDIAs targeting state estimation in power systems. Sharshar et al. develop a deep learning model based on artificial neural networks to detect FDIAs against AGC systems [4]. In [5], a multilayer perceptron model is trained to detect joint FDIAs targeting both state estimation and gas pipeline monitoring systems in integrated power and gas systems. Existing studies on countermeasures against FDIAs have primarily focused on state estimation–oriented and control command–oriented attacks. However, research on dispatch-oriented FDIAs remains relatively limited. Moreover, most of the existing research tend to focus primarily on attacks

This work is supported by National Natural Science Foundation of China (52407133, 52321004), Key Research and Development Program of Shanxi Province (202402150301007).

Xinyue Chang (corresponding author, email: 542658099@qq.com)

979-8-3315-8138-1

initiated by a single adversary, while insufficient attention has been paid to the coordinated impacts of multi-adversary attacks.

This paper proposes a distributed energy management strategy against coordinated dispatch-oriented FDIAs for EHCPS. First, a structured FDIA model is established, in which adversaries exploit the communication topology of the EHCPS to construct forged nodes. Multiple compromised nodes then collaborate to falsify data or mutually corroborate the injected false information. Secondly, a fully distributed optimization framework based on collective neurodynamic optimization (CNO) is employed to enhance computational efficiency while improving cyber resilience. Moreover, a communication link reputation evaluation method combined with multidimensional dynamic residual detection is proposed for the first time to effectively identify slow and highly concealed FDIAs.

II. MODELLING OF THE EHCPS

A. Energy enetity Modelling

Fig.1 illustrates the structural composition of the EHCPS. The power transmission network (PTN) side consists of energy entities such as distributed generator units (DGs), wind turbines (WTs), photovoltaic systems (PV), energy storage units (ESs), and electric vehicles (EVs). The PTN and the district heating network (DHN) are coupled through electricity–heat conversion units such as the combined heat and power units (CHPs) and electric boilers (EBs). The DHN also includes other heating loads.

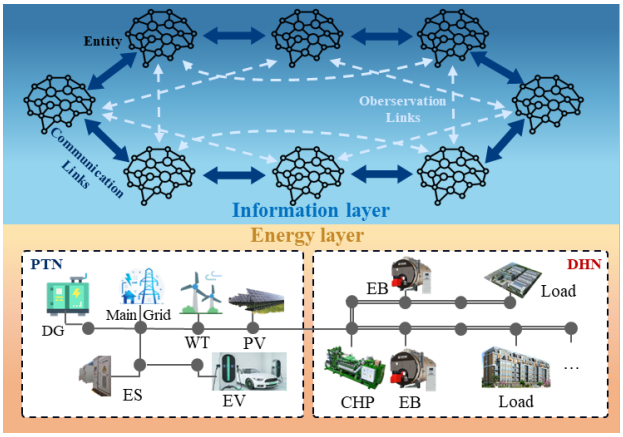

Fig.1. Physical and informational architecture of the EHCPS.

$$f_{i,t}^{\mathrm{DG}} = a_1^{\mathrm{DG}}\left(P_{i,t}^{\mathrm{DG}}\right)^2 + a_2^{\mathrm{DG}}P_{i,t}^{\mathrm{DG}} + a_3^{\mathrm{DG}} \tag{1}$$

$$f_{i,t}^{\mathrm{RG}} = a^{\mathrm{RG}}\left(P_{i,t}^{\mathrm{RG,max}} - P_{i,t}^{\mathrm{RG}}\right)^2 \tag{2}$$

$$f_{i,t}^{\mathrm{ES}} = a^{\mathrm{ES}}\left(P_{i,t}^{\mathrm{ES}}\right)^2 \tag{3}$$

$$C_{i,t}^{\mathrm{ES}} = d^{\mathrm{ES}}C_{i,t-1}^{\mathrm{ES}} + P_{i,t}^{\mathrm{ES}} \tag{4}$$

As shown in (1)-(3), the operational costs of DG, WT, PV, and ES units at time t are modeled as quadratic functions of their corresponding power. $P_{i,t}^{\mathrm{DG}}$ and $P_{i,t}^{\mathrm{ES}}$ denote the power outputs of DG i and ES i, respectively. $a_{1\sim3}^{\mathrm{DG}}$ and a^{ES} are both cost factors. Both WT and PV are renewable generator (RG), and their costs can be represented as renewable curtailment costs. a^{RG} denotes the penalty factor and $P_{i,t}^{\mathrm{RG,max}}$ represents the maximum achievable power output constrained by environmental conditions, including wind speed and the intensity of solar radiation. (4) characterizes the temporal evolution of stored electricity, in which the degradation coefficient d^{ES} is defined as a constant within the range [0, 1]. As a typical flexible load capable of providing adjustable capacity, the charging utility loss cost $f_{i,t}^{\mathrm{EV}}$ of EV i is expressed as shown in (5). a_i^{EV} denotes the utility factor. $P_i^{\mathrm{EV,ideal}}$ denotes the ideal charging/discharging power, which depends on the charging status, as shown in (6). C_i^{EV} is the battery capacity of EV i, η_i^{EV} denotes the charging efficiency, and $\mathcal{T}_i^{\mathrm{EV}}$ represents the maximum charging duration. $S_i^{\mathrm{EV,ini}}$ denotes the state of charge (SoC), and $[S_i^{\mathrm{EV,min}}, S_i^{\mathrm{EV,max}}]$ denotes the ideal SoC range.

$$f_{i,t}^{\mathrm{EV}} = a_i^{\mathrm{EV}}\left(P_{i,t}^{\mathrm{EV}} - P_i^{\mathrm{EV,ideal}}\right)^2 \tag{5}$$

$$P_i^{\mathrm{EV,ideal}} = -\frac{C_i^{\mathrm{EV}}\left(S_i^{\mathrm{EV,min}} + S_i^{\mathrm{EV,max}} - 2S_i^{\mathrm{EV,ini}}\right)}{\eta_i^{\mathrm{EV}}\mathcal{T}_i^{\mathrm{EV}}\Delta t} \tag{6}$$

$$\begin{aligned} f_{i,t}^{\mathrm{CHP}} = {} & a_1^{\mathrm{CHP}}\left(H_{i,t}^{\mathrm{CHP}}\right)^2 + a_2^{\mathrm{CHP}}H_{i,t}^{\mathrm{CHP}} + a_3^{\mathrm{CHP}} + \\ & a_4^{\mathrm{CHP}}H_{i,t}^{\mathrm{CHP}}P_{i,t}^{\mathrm{CHP}} + a_5^{\mathrm{CHP}}\left(P_{i,t}^{\mathrm{CHP}}\right)^2 + a_6^{\mathrm{CHP}}P_{i,t}^{\mathrm{CHP}} \end{aligned} \tag{7}$$

$$H_{i,t}^{\mathrm{CHP}} = \frac{a_{\mathrm{heat}}\left(1-\eta^{\mathrm{CHP}}-c^{\mathrm{loss}}\right)}{\eta^{\mathrm{CHP}}}\cdot P_{i,t}^{\mathrm{CHP}} \tag{8}$$

$$f_{i,t}^{\mathrm{EB}} = a^{\mathrm{EB}}H_{i,t}^{\mathrm{EB}}, H_{i,t}^{\mathrm{EB}} = \eta^{\mathrm{EB}}P_{i,t}^{\mathrm{EB}} \tag{9}$$

The operational cost of CHP is given in (7), where $a_{1\sim6}^{\mathrm{CHP}}$ denote the cost factors. (8) represents the electricity–heat conversion relationship of the CHP output power, where a_{heat} denotes the heat production coefficient, η^{CHP} is the operating efficiency of the unit, and c^{loss} represents the heat loss ratio. (9) defines the cost function of EB, where $H_{i,t}^{\mathrm{EB}}$ denotes the generated heating power and $P_{i,t}^{\mathrm{EB}}$ represents the consumed electrical power. Parameters a^{EB} and η^{EB} correspond to the cost coefficient and heat production efficiency, respectively.

B. Constrainsts of the EHCPS

The constraints include equipment operational constraints, network constraints, and power balance constraints.

$$P_i^{\mathrm{DG,min}} \le P_{i,t}^{\mathrm{DG}} \le P_i^{\mathrm{DG,max}} \tag{10}$$

$$-\Delta P_i^{\mathrm{DG,min}} \le P_{i,t}^{\mathrm{DG}} - P_{i,t-1}^{\mathrm{DG}} \le \Delta P_i^{\mathrm{DG,max}} \tag{11}$$

$$0 \le P_{i,t}^{\mathrm{RG}} \le P_i^{\mathrm{RG,max}} \tag{12}$$

$$P_i^{\mathrm{ES,min}} \le P_{i,t}^{\mathrm{ES}} \le P_i^{\mathrm{ES,max}} \tag{13}$$

$$C_i^{\mathrm{ES,min}} \le C_{i,t}^{\mathrm{ES}} \le C_i^{\mathrm{ES,max}} \tag{14}$$

$$P_i^{\mathrm{EV,min}} \le P_{i,t}^{\mathrm{EV}} \le P_{i,t}^{\mathrm{EV,max}} \tag{15}$$

$$S_i^{\mathrm{EV,min}} \le \frac{C_i^{\mathrm{EV}} S_i^{\mathrm{EV,ini}} + \sum_{t\in T} P_{i,t}^{\mathrm{EV}}}{C_i^{\mathrm{EV}}} \le S_i^{\mathrm{EV,max}} \tag{16}$$

$$P_{i,t}^{\mathrm{CHP}} > \mathcal{C}_i^{\mathrm{CHP}} H_{i,t}^{\mathrm{CHP}} + \eta_i^{\mathrm{CHP}} \tag{17}$$

$$P_{i,t}^{\mathrm{CHP}} < P_{i,t}^{\mathrm{CHP,max}} - c_i H_{i,t}^{\mathrm{CHP}} \tag{18}$$

$$-\Delta P_i^{\mathrm{CHP,min}} \le P_{i,t}^{\mathrm{CHP}} - P_{i,t-1}^{\mathrm{CHP}} \le \Delta P_i^{\mathrm{CHP,max}} \tag{19}$$

$$P_i^{\mathrm{EB,min}} \le P_{i,t}^{\mathrm{EB}} \le P_i^{\mathrm{EB,max}} \tag{20}$$

(10), (11), (12), (13), (15), (19), and (20) represent the output constraints of the corresponding devices. (14) and (16) represent the capacity limits of devices equipped with energy storage capability. (17) and (18) define the feasible operating region constraints of the CHP unit. The PTN model adopts a DC power flow formulation, and the transmission line capacity constraints are given in (21). $\kappa_{l,n}$ is the shift factor, $P_{i,t}^{\mathrm{G}}$ denotes the power output of all generation units, $L_{n,t}$ represents the power load connected to bus n at time t, and P_l^{limit} denotes the transmission capacity limit of line l in PTN. Constraint (22) ensures the power balance of the system.

$$\left| \sum_{n\in\Omega^{\mathrm{bus}}} \kappa_{l,n} \cdot \left(\sum_{i\in\Omega^{\mathrm{DG,RG,CHP}}} P_{i,t}^{\mathrm{G}} + \sum_{j\in\Omega^{\mathrm{ES}}} P_{j,t}^{\mathrm{ES}} + \sum_{g\in\Omega^{\mathrm{EV}}} P_{g,t}^{\mathrm{EV}} - P_{n,t}^{\mathrm{load}} \right) \right| \le P_l^{\mathrm{limit}}, \forall l \in \Omega^{\mathrm{line}} \tag{21}$$

$$\sum_{i\in\Omega^{\mathrm{DG,RG,CHP}}} P_{i,t}^{\mathrm{G}} + \sum_{j\in\Omega^{\mathrm{ES}}} P_{j,t}^{\mathrm{ES}} + \sum_{g\in\Omega^{\mathrm{EV}}} P_{g,t}^{\mathrm{EV}} = \sum_{n\in\Omega^{\mathrm{bus}}} L_{n,t} \tag{22}$$

$$H_{g,t}^{\mathrm{CHP}} + H_{g,t}^{\mathrm{EB}} - L_{g,t} = c^{\mathrm{water}} m_g \left(\tau_g^{\mathrm{s}} - \tau_g^{\mathrm{r}}\right), g \in \Omega_{\mathrm{H}} \tag{23}$$

$$\sum_{i\in\mathcal{P}_g^-} m_{i,g}^- = \sum_{i\in\mathcal{P}_g^+} m_{i,g}^+, g \in \Omega_{\mathrm{H}} \tag{24}$$

$$\sum_{i\in\mathcal{P}_g^-} m_{i,g}^- \cdot \tau_{i,g}^- = \sum_{i\in\mathcal{P}_g^+} \left(m_{i,g}^+ \tau_{i,g}^+\right) \tag{25}$$

$$\tau_i^{\mathrm{ed}} = T_{\mathrm{am}} + \left(\tau_i^{\mathrm{st}} - T_{\mathrm{am}}\right) e^{-\frac{\delta l_i}{c^{\mathrm{water}} m_i}}, i \in \Omega_{\mathcal{P}} \tag{26}$$

For the DHN, (23) describes the heating power balance at node g, where c^{water} denotes the specific heat capacity of water, m_g represents the mass flow rate of the heat source or load. τ_g^{s} and τ_g^{r} denote the supply and return water temperatures of the heat source. (24) and (25) denote the mass flow balance and heat balance at the node, where $m_{i,g}^-$ and $m_{i,g}^+$ is the mass flow rate of water injected into and flowing out from node g through pipelines, respectively. $\tau_{i,g}^-$ and $\tau_{i,g}^+$ denote the inlet and outlet water temperatures, respectively. (26) represents the temperature variation process of a single pipeline, where T_{am} denotes the ambient temperature.

III. Attack Modes and Defense Strategy

A. Coordinated FDIA Model

In the context of this paper, adversaries exfiltrate the identity information of legitimate entities within the EHCPS and create corresponding forged entities that share the same communication peers and communication modalities as their legitimate counterparts. The forged entities send falsified messages with injected biases to their communication peers, as shown in (27). k denotes the iteration step, x_i^{ori} denotes the original information, and $\tilde{x}_i^{\mathrm{f}}$ denotes the false information sent by the forged entities. β denotes the attack intensity, and ϵ represents the perturbation. Such attacks not only produce deceptive effects but also impose a substantial additional burden on system bandwidth.

$$\tilde{x}_i^{\mathrm{f}}(k) = x_i^{\mathrm{ori}}(k) + \beta \cdot \epsilon \tag{27}$$

$$\tilde{x}_{i,1}^{\mathrm{f}}(k) = x_i^{\mathrm{ori}}(k) + \beta \cdot \left(\epsilon_1 + A_1 \sin\left(\frac{2\pi\left(k - k^{\mathrm{attack}}\right)}{\mathcal{T}_1^{\mathrm{attack}}} \right) \right) \tag{28}$$

$$\tilde{x}_{i,2}^{\mathrm{f}}(k) = x_i^{\mathrm{ori}}(k) + \beta \cdot \epsilon_2, \quad i = \Omega_{\mathrm{f}} \left[\mathrm{mod}\left(\left\lfloor \frac{k - k^{\mathrm{attack}}}{\mathcal{T}_2^{\mathrm{attack}}} \right\rfloor, \left|\Omega_{\mathrm{f}}\right| \right) + 1 \right] \tag{29}$$

$$\tilde{x}_{i,3}^{\mathrm{f}}(k) = x_i^{\mathrm{ori}}(k) + d^{\mathrm{attack}}(k) \cdot \beta\left(\epsilon_3 + A_3\sigma\right) \tag{30}$$

$$d^{\mathrm{attack}}(k) = \begin{cases} 1, & \text{if } \mathrm{mod}\left(\left\lfloor \dfrac{k - k^{\mathrm{attack}}}{\mathcal{T}_3^{\mathrm{attack}}} \right\rfloor, 2 \right) = 0 \\ -1, & \text{otherwise} \end{cases} \tag{31}$$

When multiple forged entities are present in the system, they tend to coordinate their actions to maximize attack effectiveness while minimizing the likelihood of detection. Three coordinated attack modes are considered in this paper: synchronous attacks, sequential attacks, and directional attacks. (28) defines the synchronous attack mode, in which all forged entities launch attacks simultaneously by injecting sinusoidal bias signals. k^{attack} denotes the attack initiation step, A_1 represents the sinusoidal amplitude, and $\mathcal{T}^{\mathrm{attack}}$ denotes the attack period. (29) defines the sequential attack mode, in which forged entities launch attacks in turn. Ω_{f} denotes the set of forged entities. As shown in (30), directional attacks involve forged information that deviates consistently in a direction, with the direction of bias switching periodically. d^{attack} is the direction factor, A_3 denotes the fluctuation amplitude, and σ represents a uniformly distributed random variable within the interval [0, 1].

B. Fully Distributed CNO-Based Computation Method

The objective of energy management for EHCPS is to minimize the system's operational cost while maintaining energy supply–demand balance. To enhance computational efficiency while reducing the risk of global computation failure caused by single-point communication faults, a fully distributed optimization approach based on projection neural networks (PNNs) is adopted [8]. The local problem of each entity is solved by a set of PNNs, and neighboring PNNs synchronize with one another to achieve global consensus. The dynamic updating equation can be written in the form of (32). ϑ denotes the updating step size, and P_Ω represents the projection operator. L_p and L_q are obtained by taking the Kronecker product of the Laplacian matrix of the energy-entity communication graph with the p-dimensional and q-dimensional identity matrices, respectively. $\boldsymbol{x}_i$ denotes the state vector, and $\boldsymbol{\mu}_i$, $\boldsymbol{\lambda}_i$, $\boldsymbol{\nu}_i$, and $\boldsymbol{\gamma}_i$ are the corresponding Lagrange multipliers.

$$\begin{cases} \vartheta \dfrac{d\boldsymbol{x}_i}{dt} = -\boldsymbol{x}_i + P_\Omega\left(\boldsymbol{x}_i - \nabla f(\boldsymbol{x}_i) + A^T\boldsymbol{\mu}_i - \nabla G(\boldsymbol{x}_i)\boldsymbol{\nu}_i\right) \\ \vartheta \dfrac{d\boldsymbol{\mu}_i}{dt} = -L_p\boldsymbol{\mu}_i - L_p\boldsymbol{\lambda}_i - (A_i\boldsymbol{x}_i - b_i) \\ \vartheta \dfrac{d\boldsymbol{\lambda}_i}{dt} = L_p\boldsymbol{\mu}_i \\ \vartheta \dfrac{d\boldsymbol{\nu}_i}{dt} = -\boldsymbol{\nu}_i + \left(\boldsymbol{\nu}_i + G(\boldsymbol{x}_i) - L_q\boldsymbol{\gamma}_i - L_q\boldsymbol{\nu}_i\right)^+ \\ \vartheta \dfrac{d\boldsymbol{\gamma}_i}{dt} = L_q\boldsymbol{\nu}_i \end{cases} \tag{32}$$

C. Reputation Evaluation Mechanism Based on Multidimensional Dynamic Residuals

To identify and isolate FDIAs in the communication network, reputation evaluation of the communication links is performed after global consensus is reached among the PNNs in each iteration. An observation network structure [9] is adopted here. This network is used solely to exchange link evaluation results among 2-hop neighbors and does not participate in the physical dispatch process. Consequently, it imposes only minimal communication overhead on the system.

$$r_{i,1}(k) = \sum_{j\in N_i^-} \mathbf{1}\left[\left|x_j^+(k) - x_i(k)\right| > \theta_1\right] \tag{33}$$

$$r_{i,2}(k) = \mathrm{std}\left(\left\{x_{ji}^-(k) : j \in N_i^+\right\}\right) \tag{34}$$

$$r_{i,3}(k) = \left|x_i(k) - \mathrm{median}\left(\left\{x_j(k) : j \in \Omega_{i\_\mathrm{type}}\right\}\right)\right| \tag{35}$$

Considering both the impact of forged entities on their neighboring entities and the coordinated behaviors among forged entities, this paper proposes a multidimensional dynamic residual–based detection metric. (33) defines the neighbor influence residual, where $\mathbf{1}[\cdot]$ denotes the indicator function and θ represents the threshold. N_i^- denotes the in-neighbors of entity i in the communication graph, and N_i^+ denotes its out-neighbors. $x_j^+(k)$ denotes the information transmitted from entity j to its neighbors in iteration k. (34) presents the cross-validation residual, which is used to examine the consistency of the data that the same entity transmits to different neighbors. $x_{ji}^-(k)$ denotes the information received by entity j from entity i. As shown in (35), consensus outlier residual quantifies the deviation between the information transmitted by entity i and the median of the information transmitted by entities in the same category. Ω_{i_type} denotes the set of entities that belong to the same category as entity i, such as RG units and ES units.

$$S_i^{\mathrm{attack}}(k) = \omega_1 r_{i,1}(k) + \omega_2 r_{i,2}(k) + \omega_3 r_{i,3}(k) \tag{36}$$

$$u_i(k) = \begin{cases} 0, & S_i^{\mathrm{attack}}(k) > \theta_S \\ 1, & \text{else} \end{cases} \tag{37}$$

$$\mathcal{M}_{ji}(k) = \begin{cases} \mathcal{M}_{ji}(k-1) + 1, & u_i(k) = 1 \\ \mathcal{M}_{ji}(k-1), & u_i(k) = 0 \end{cases} \tag{38}$$

$$\mathcal{R}_{ji}(k) = \frac{\chi_k \mathcal{M}_{ji}(k) + 1}{\chi_k k + 1} \tag{39}$$

After iteration k, neighboring entities compute the residual score $S_i^{\mathrm{attack}}(k)$ for entity i. In (36), ω denotes the weighting coefficient. The detection result $u_i(k)$ is also updated and recorded in the counter $\mathcal{M}_{ji}$. θ_S denotes the score threshold. The reputation of the communication link between entities i and j is updated according to (39). If the score of entity i remains consistently high, the reputation of the link will continue to decrease. Once the reputation falls below the threshold, the corresponding communication link is disconnected, thereby achieving isolation.

IV. Case Studies

This section employs an EHCPS test system composed of a 30-bus PTN and a 32-node DHN to evaluate the computational performance and cyber resilience of the proposed energy management strategy. The communication network contains a total of 14 legitimate energy entities. All simulations below are conducted in MATLAB R2022b.

Case 1: Evaluation of the Dispatch-Oriented FDIA Effects.

To illustrate the destructive impact of FDIAs targeting the dispatch process, both centralized and distributed solution schemes without any defense strategies are employed. Three forged entities are introduced in the case. The attack intensity β is set to 50, and the injected perturbation ϵ is set to 20% of the original data. The computational performance under attack is shown in Table I. It can be observed that coordinated attacks intensify the influence of forged entities on system decision-making, thereby resulting in additional operational costs. The distributed scheme demonstrates higher resilience against single-point failures compared with the centralized scheme under non-coordinated attack scenarios. However, under coordinated attacks, the distributed decision-making

framework becomes more vulnerable to deception, resulting in greater operational cost losses.

TABLE I. COMPUTATIONAL PERFORMANCE WITHOUT DEFENSE STRATEGIES

Scenarios	Performance Evaluation Metrics		
	Time (s)	Cost ($)	Percentage Increase in Cost (%)
Centralized (No attack)	4.12	480.89	-
Centralized (Non-coordinated attack)	5.38	511.53	6.37
Distributed (Non-coordinated attack)	0.79	503.82	4.77
Centralized (Coordinated attack)	5.29	551.99	14.79
Distributed (Coordinated attack)	1.01	582.73	21.18

Case 2: Computational Performance Under Non-Coordinated FDIAs.

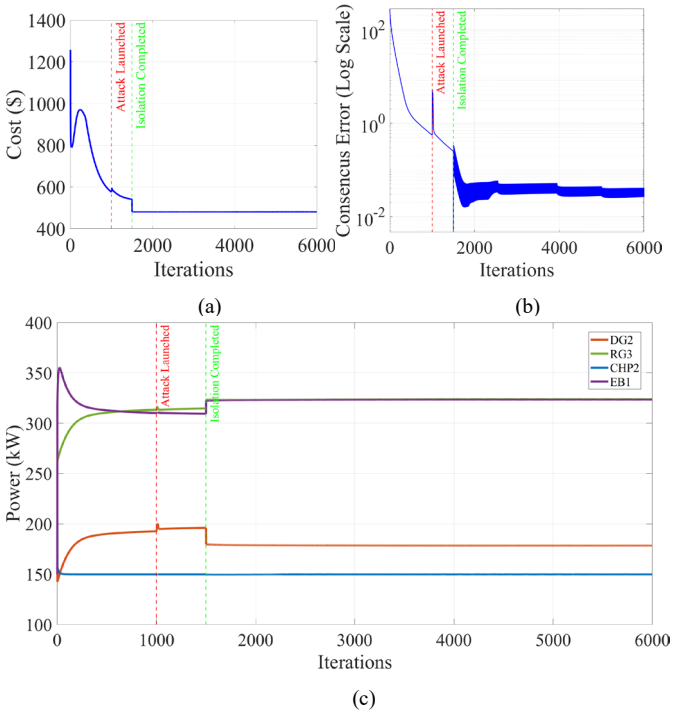

Fig.2. Computational Performance of the Proposed Algorithm Under Non-Coordinated Attacks. (a) Operational Cost of EHCPS. (b) Consensus Error of Entities. (c) Power Output of Representative Entities.

From the performance of the proposed energy management strategy illustrated in Fig.2, it can be observed that the system's decision results and the consensus among entities are noticeably affected once the attack is launched. Nevertheless, the overall convergence trend remains largely unchanged, demonstrating that the resilience of the communication network is effectively maintained. After isolating all FDIAs, a strong synchronization strategy is employed to accelerate the consensus-reaching process among the legitimate entities. Although slight fluctuations remain in the consensus error among the entities, the magnitude of the error is on the order of $O\left(10^{-2}\right)$. Moreover, the root mean squared error (RMSE) of the entities' power outputs is merely 0.09 kW.

Case 3: Computational Performance Under Coordinated FDIAs.

To better detect the temporal coordination among forged entities, a sliding time-window strategy is adopted, which dynamically records the attack initiation frequency over the preceding 20 iterations in each update step. The detection results for the coordinated attacks are presented in Table II. The link reputation values of the isolated forged nodes all fall below the threshold 0.5, indicating that the proposed strategy successfully achieves effective isolation of coordinated FDIAs.

TABLE II. COMPUTATIONAL PERFORMANCE UNDER COORDINATED FDIAS

Reputation of the Forged Links	Time (s)	RMSE (kW)	Relative Error of the Cost (%)
0.49, 0.49, 0.44	0.51	0.13	0.06

V. CONCLUSION

This paper proposes a distributed optimization strategy with enhanced cyber resilience for the energy management of the EHCPS. To address dispatch-oriented FDIAs, this paper first develops three coordinated false data injection models. Subsequently, a reputation evaluation strategy incorporating multidimensional dynamic residuals of entity information is proposed and integrated with a fully distributed computation method based on CNO, aiming to achieve efficient and secure energy management for the EHCPS. Finally, three case studies are conducted to demonstrate the threat posed by dispatch-oriented FDIAs and to verify the effectiveness of the proposed defense strategy.

REFERENCES

[1] H. Sun, Q. Guo, X. Shen, Y. Xue, M. Shahidehpour, and N. Hatziargyriou, "Energy Internet: Redefinition and categories," *Energy Internet*, vol. 1, no.1, pp. 3-8, Aug. 2024.

[2] Y. Du, Y. Xue, M. Shahidehpour, L. Zhao, X. Chang, J. Su, and H. Sun, "A Secure Distributed Computation of Combined Heat and Power Dispatch Based on Transformation Method," *IEEE Trans. Sustain. Energy*, vol. 16, no. 4, pp. 2903-2917, May 2025.

[3] W. Gu et al., "Coordinated heat and power cyber-attacks with time window matching strategy," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 2747–2761, Jul. 2023.

[4] M. Sharshar, A. M. Saber, D. Svetinovic, H. Zeineldin, and E. F. El-Saadany, "Accurate and Energy-Efficient Detection of Cyberattacks Against Non-Linear AGC Systems," *IEEE Trans. Smart Grid*, 2025.

[5] M. Zadsar, A. Abazari, A. Ameli, J. Yan, and M. Ghafouri, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4252-4268, Sep. 2023.

[6] J. Xu, Z. Wu, T. Zhang, Q. Hu, and Q. Wu, "A secure forecasting-aided state estimation framework for power distribution systems against false data injection attacks," *Appl. Energy*, vol. 328, Dec. 2022, Art. no. 120107.

[7] C. Liu, Y. Tang, R. Deng, M. Zhou, and W. Du, "Joint meter coding and moving target defense for detecting stealthy false data injection attacks in power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 20, no. 3, pp. 3371–3381, Mar. 2024.

[8] Z. Chen, J. Wang, and Q.-L. Han, "A collaborative neurodynamic optimization approach to distributed chiller loading," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 8, pp. 10950-10960, Aug. 2024.

[9] P. Li, Y. Liu, H. Xin, and X. Jiang, "A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks," *IEEE Trans. Ind. Inf.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.