

A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks

Bonan Huang, Yushuai Li , *Member, IEEE*, Fengnan Zhan , Qiuye Sun , *Senior Member, IEEE*, and Huaguang Zhang , *Fellow, IEEE*

Abstract—Distributed algorithms are increasingly being used to solve the economic dispatch problem of integrated energy systems (IESs) because of their high flexibility and strong robustness, but those algorithms also bring more risk of cyber-attacks in IESs. To solve this problem, this article investigates the distributed robust economic dispatch problem of IESs under cyber-attacks. First, as the first line of defense against attacks, a privacy-preserving protocol is designed for covering up some vital information used for economic dispatch of IESs. On this basis, a distributed robust economic dispatch strategy is presented to achieve the energy management of IESs in the presence of misbehaving units, which consists of a neighbor-observe-based detection process and a reputation-based isolation process. The proposed strategy is implemented in a fully distributed fashion and possesses strong robustness against various colluding and noncolluding attacks. In addition, the strategy can not only ensure the reliability of information transmission among energy units, but also solve the problem of incorrect measurement of distributed local load data caused by cyber-attacks. Finally, the effectiveness of the proposed strategy is illustrated by simulation cases on a 39-bus 32-node power-heat IES.

Index Terms—Cyber-attacks, economic dispatch (ED), fully distributed control, integrated energy system (IES), noncolluding attacks.

I. INTRODUCTION

WITH the aggravation of environmental pollution and energy crisis, the research on integrated energy systems

(IESs) has received extensive attention from the scholars and governments around the world [1]. In recent years, various fundamental problems of IESs have been extensively investigated, one of which is the economic dispatch (ED) problem [2]–[5]. It studies how to allocate multienergy units under the premise of meeting system safety constraints and operating constraints, so as to minimize the system operation cost [6]. In the past decade, two categories of methods have been proposed to solve the ED problem of the IES, i.e., centralized and distributed methods. The centralized methods have the certain advantage in solving efficiency. However, these kinds of methods suffer from high communication cost [7], single-point failure sensitivity [8], and poor privacy [9].

As a promising way, the distributed methods can use the sparse communication network structure to realize the decentralized cooperation of each component in the network with better robustness [10], flexibility [11], and privacy [12]. However, these methods may increase the vulnerability of communication networks caused by attackers as well as the lack of central authority, which monitors the behaviors of all the units. Furthermore, with the increase in the number of distributed sensors and controllers, the transmission of measurement information and decision information in communication networks has become more frequent; meanwhile, the degree of cyber-physical integration of the IES has gradually deepened. If the communication network of the IES is maliciously attacked, it may cause a chain reaction of its physical network to affect the normal operation of the IES [13]–[15].

Recently, there has been increasing interest in studying the effects of different cyber-attacks within the context of power systems, which mainly contain denial of service (DoS) attacks, false data injection (FDI) attacks, and replay attacks [16]. Those malicious attacks spreading in the communication network may damage the economic and safe operation of the system and even result in crippled energy supply [17]. To address this issue, various strategies have been proposed to protect the distributed energy management of the system from cyber-attacks [18]–[28]. For example, with regard to FDI attacks, its effect on ED was investigated in [18]. On the basis of [18], the attack detection and solution strategy were proposed in [19]. Literature [20] investigated a technique for dynamic FDI attack detection, which integrates spiking neurons with the delayed feedback

Manuscript received January 8, 2021; revised April 10, 2021; accepted April 21, 2021. Date of publication May 4, 2021; date of current version October 27, 2021. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFA0702200, in part by the Fundamental Research Funds for the Central Universities under Grant N2104017 and Grant N2004005, and in part by the National Natural Science Foundation of China under Grant U20A20190. Paper no. TII-21-0086. (*Corresponding author: Yushuai Li.*)

Bonan Huang, Yushuai Li, Fengnan Zhan, and Qiuye Sun are with the School of Information Science and Engineering, Northeastern University, Shenyang 110004, China (e-mail: huangbonan@ise.neu.edu.cn; yushuai@ieee.org; yy11081003@163.com; sunqiuye@ise.neu.edu.cn).

Huaguang Zhang is with the State Key Laboratory of Synthetical Automation for Process Industries and the School of Information Science and Engineering, Northeastern University, Shenyang 110004, China (e-mail: hgzhang@ieee.org).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TII.2021.3077509>.

Digital Object Identifier 10.1109/TII.2021.3077509

reservoir computing. This technique can achieve a significantly better performance compared to existing techniques. Moreover, literature [21] integrated a physical model that captures ideal measurements with a generative adversarial network, which captures the deviations from ideal measurements to accurately recover the state estimation data manipulated by FDI attacks. For DoS attacks, a model based on machine learning to detect smart grid DoS attacks was proposed in [22], and the principal component analysis and support vector machine algorithms are used to improve the accuracy of attack detection. In addition, a robust method based on mixed-integer linear programming was investigated in [23] to mitigate the effect of DoS attacks. In recent years, event-triggered control [24], self-triggered control [25], and other robust control strategies have also been gradually applied to resist DoS attacks. Regarding replay attacks, a detection method based on causal countermeasures against replay attacks was proposed in [26]. A conceptual layered framework to protect the power system from replay attacks without compromising the availability of control and signal data was proposed in [27]. Furthermore, Li *et al.* [28] proposed a statistical process monitoring approach based on five statistical metrics to realize the detection and differentiation of replay attacks and equipment faults in SCADA systems.

It is worth noting that the above research only considered the noncolluding attacks but not the colluding attacks. Under the colluding attack mode, the detected misbehaving units can collaborate with some undetected “well-behaving” units by a special protocol. This protocol can ensure that aforementioned ordinary methods cannot isolate these abnormal units. Obviously, colluding attacks are much more difficult to be defended than noncolluding attacks. Recently, a robust method based on the distributed confidence level manager (DCLM) to detect and eliminate colluding attacks has been proposed in [29]. Although the designed robust method has gained some satisfactory results on dealing with the noncolluding attacks and colluding attacks, this method needs to be further improved. First, the DCLM-based method is developed based on a leader–follower consensus algorithm, which cannot be implemented in a fully distributed fashion. Second, the privacy-preserving aggregation algorithm used in [29] is not sufficiently reliable, since it only protects some information passed among the followers, but not the global information received by the leader. Third, in [29], the isolation process against misbehaving units is established based on the “confidence level.” However, the definition of the “confidence level” is unclear, whose value range is unknown. Last but not least, the DCLM-based method cannot deal with the scenario that the measurement of load data is attacked maliciously. This flaw can be exploited by attackers to destroy the energy supply–demand balance of the system. In addition, the methods proposed in [18]–[29] are mainly suitable for mitigating the impact of malicious cyber-attacks on the ED problem for power systems. However, for the IES, more energy resources from different energy networks are integrated, which is more difficult to be analyzed under diversified cyber-attacks. Until now, little research has been documented to develop fully distributed robust ED strategies for the IES against both noncolluding and colluding attacks.

Mainly with the aforementioned inspirations, we design a privacy-preserving protocol embedded into a well-developed distributed algorithm, which can effectively prevent vital information leakage. On this basis, we present a distributed robust ED strategy to ensure the economic and stable operation of the IES in the presence of various noncolluding and colluding attacks. The main contributions of this article are shown as follows.

- 1) This article, for the first time, presents a fully distributed robust ED strategy for the IES, which can resist both colluding and noncolluding attacks. The proposed strategy fits well with the strong coupling characteristic of the IES and possesses better dependability and less communication burden.
- 2) A privacy-preserving protocol is proposed to reduce the potential of information leakage. It covers up some vital updating information used for ED by injecting the time-varying noise items, which further enhances the safety and reliability of the ED process of the IES in a fully distributed fashion.
- 3) The isolation process based on the reputation values of communication links can effectively isolate the misbehaving units from the communication network. At the same time, by using a time-varying reputation coefficient, this isolation process can dynamically adjust its tolerance to transient network fluctuations to avoid misoperation or inaction of the isolation mechanism.
- 4) By embedding the detection and correction mechanism for local estimated energy mismatches, the proposed strategy can defend against a special type of FDI attack, which interferes with the execution of the distributed ED algorithm by manipulating the measured load data, thereby disrupting the multienergy supply–demand balance of the system.

II. PRELIMINARIES

The IES can be regarded as a kind of multiagent system, where each energy device is regarded as an agent. The energy devices can be classified into three types: power-only device (POD), combined heat and power device (CHP), and heat-only device (HOD).

The objective function of the ED problem of the IES can be expressed as follows:

$$\min F = F_P + F_C + F_H \quad (1)$$

$$F_P = \sum_{i \in N_P} F_i^P(p_i^P) = \sum_{i \in N_P} \alpha_i (p_i^P)^2 + \beta_i p_i^P + \gamma_i \quad (2)$$

$$F_C = \sum_{i \in N_C} F_i^C(p_i^C, h_i^C) = \sum_{i \in N_C} \alpha_i (p_i^C)^2 + \beta_i p_i^C + \theta_i (h_i^C)^2 + \delta_i h_i^C + \varepsilon_i p_i^C h_i^C \quad (3)$$

$$F_H = \sum_{i \in N_H} F_i^H(h_i^H) = \sum_{i \in N_H} \alpha_i (h_i^H)^2 + \beta_i h_i^H + \gamma_i \quad (4)$$

where F is the total operation cost of the IES; F_i^P , F_i^C , and F_i^H denote the cost functions of the i th POD, CHP, and HOD, respectively; p_i^P , p_i^C , h_i^C , and h_i^H denote the power generation

of the i th POD, power generation of the i th CHP, heat output of the i th CHP, and heat output of the i th HOD, respectively; N_P , N_C , and N_H represent the sets of PODs, CHPs, and HODs, respectively; and α_i , β_i , γ_i , θ_i , δ_i , and ε_i are the cost coefficients.

The ED problem of the IES is subject to a set of system security constraints and operating constraints [30], which can be further expressed as follows.

- 1) The power/heat supply–demand balance constraints

$$\Delta P = \sum_{i \in V} P_{Di} - \sum_{i \in N_P} p_i^P - \sum_{i \in N_C} p_i^C = 0 \quad (5)$$

$$\Delta H = \sum_{i \in V} H_{Di} - \sum_{i \in N_H} h_i^H - \sum_{i \in N_C} h_i^C = 0 \quad (6)$$

where P_{Di} denotes the local electrical load consumption measured by the i th POD and CHP for some particular districts, H_{Di} denotes the local heat load consumption measured by the i th HOD and CHP for some particular districts, ΔP is the total power mismatch, and ΔH is the total heat mismatch.

- 2) The upper and lower output limits of the i th POD and HOD

$$\underline{p}_i^P \leq p_i^P \leq \bar{p}_i^P \quad (7)$$

$$\underline{h}_i^H \leq h_i^H \leq \bar{h}_i^H \quad (8)$$

where the output of POD is limited by physical capacity limits $p_{i,\min}^P$ and $p_{i,\max}^P$, and due to the limited ramp rate $p_{i,\text{ramp}}$, the lower and upper output limits of the i th POD can be expressed as $\underline{p}_{i,t}^P = \max\{p_{i,\min}^P, p_{i,t-1}^P - p_{i,\text{ramp}}\}$ and $\bar{p}_{i,t}^P = \min\{p_{i,\max}^P, p_{i,t-1}^P + p_{i,\text{ramp}}\}$, respectively; $\underline{h}_i^H$ and $\bar{h}_i^H$ denote the lower and upper bounds of heat output of the i th HOD, respectively.

- 3) The power–heat operable domain constraints and ramp rate constraint of the i th CHP

$$\underline{p}_i^C(h_i^C) \leq p_i^C \leq \bar{p}_i^C(h_i^C) \quad (9)$$

$$\underline{h}_i^C(p_i^C) \leq h_i^C \leq \bar{h}_i^C(p_i^C) \quad (10)$$

$$-p_{i,\text{ramp}}^C \leq p_{i,t}^C - p_{i,t-1}^C \leq p_{i,\text{ramp}}^C \quad (11)$$

where $\underline{p}_i^C(h_i^C)$, $\bar{p}_i^C(h_i^C)$, $\underline{h}_i^C(p_i^C)$, and $\bar{h}_i^C(p_i^C)$ specify the power–heat operable domain for the i th CHP with the form of linearized functions; $p_{i,\text{ramp}}^C$ is the ramp rate limit of the i th CHP.

- 4) The physical transmission limits

$$\underline{p}_{l,\text{line}} \leq p_{l,\text{line}} \leq \bar{p}_{l,\text{line}} \quad (12)$$

$$\underline{h}_{l,\text{line}} \leq h_{l,\text{line}} \leq \bar{h}_{l,\text{line}} \quad (13)$$

where $l \in N_L$, and N_L is a set of the physical transmission lines; $\underline{p}_{l,\text{line}}$ and $\bar{p}_{l,\text{line}}$ denote the lower and upper bounds of power transmission of the l th transmission line, respectively; and $\underline{h}_{l,\text{line}}$ and $\bar{h}_{l,\text{line}}$ denote the lower and upper bounds of heat transmission of the l th transmission line, respectively.

The ED problem of the IES can be solved by using the Lagrange multiplier method [6]. To be specific, the Lagrange function is constructed as follows:

$$L = F + \lambda_p \Delta P + \lambda_h \Delta H \quad (14)$$

where λ_p and λ_h represent the Lagrange multipliers corresponding to the equality constraints (5) and (6), respectively.

The optimal operation point of the IES is determined according to the Karush–Kuhn–Tucker (KKT) conditions (see [Appendix A] [35]), from which we can obtain that λ_p is equal to the power incremental costs (ICs). Similarly, λ_h is equal to the heat ICs. In the following paragraphs, we directly use λ_p and λ_h to represent the power ICs and heat ICs, respectively.

III. PROBLEM DESCRIPTION

A. Fully Distributed ED Algorithm

According to the knowledge of graph theory (see [Appendix B] [35]), we define two matrices $M, N \in \mathbb{R}^{n \times n}$ associated with the communication network topology $G = \{V, E, A\}$ as follows:

$$m_{ij} = \begin{cases} \frac{a_{ij}}{d_i^+ + 1}, & j \in N_i^+ \text{ and } j \neq i \\ \frac{1}{d_i^+ + 1}, & j = i \\ 0, & \text{otherwise} \end{cases} \quad (15)$$

$$n_{ij} = \begin{cases} \frac{a_{ij}}{d_j^- + 1}, & i \in N_j^- \text{ and } j \neq i \\ \frac{1}{d_j^- + 1}, & i = j \\ 0, & \text{otherwise} \end{cases} \quad (16)$$

where $d_i^+ = \sum_{j \in N_i^+} a_{ij}$ denotes the sum of weights of the edges between unit i and its in-neighbors, and $d_i^- = \sum_{j \in N_i^-} a_{ji}$ denotes the sum of weights of the edges between unit j and its out-neighbors.

Assumption 1: The nonzero elements of the matrix M satisfy $\sigma \leq m_{ij} \leq 1$, where $0 \leq \sigma \leq \min_i \{1/(d_i^+ + 1)\}$. The nonzero elements of the matrix N satisfy $\varrho_{\min} \leq n_{ij} \leq \varrho_{\max}$, where $0 \leq \varrho_{\min} \leq \min_j \{1/(d_j^- + 1)\}$ and $\varrho_{\max} \leq 1$.

It is not very difficult to verify that M is a row-stochastic matrix and N is a column-stochastic matrix.

In this article, a well-developed fully distributed ED algorithm in [31] is expanded to the form of (17)–(19). By embedding the vector representing the power–heat coupling characteristics of the IES, two sets of consensus protocols with four consensus variables are established in (17) and (19), respectively. These consensus protocols are used to calculate the power and heat ICs and obtain the coupled power generation and heat output, thereby further estimating the local power and heat mismatches. Moreover, by using these consensus protocols, each unit only needs to exchange updating information with its neighbors. In this way, the dynamics (17)–(19) can be specifically expressed as follows:

- 1) The first consensus protocol

$$\lambda(k+1) = M\lambda(k) + \eta\gamma(k) \quad (17)$$

where $\lambda = [\lambda_p^P, \lambda_p^C, \lambda_h^C, \lambda_h^H]^T$ represents the column stack vector of all the ICs; $\lambda_p = [\lambda_p^P, \lambda_p^C]^T$ represents the power ICs

of PODs and CHPs, $\lambda_h = [\lambda_h^C, \lambda_h^H]^T$ represents the heat ICs of CHPs and HODs, η is the convergence coefficient, which is a sufficiently small positive constant, $M = \begin{bmatrix} \tilde{M} & \mathbf{0} \\ \mathbf{0} & \tilde{M} \end{bmatrix}$ is a consensus update weighting matrix, where $\hat{M} = \begin{bmatrix} \hat{M}_{n_1}^{n_1} & \hat{M}_{n_1}^{n_2} \\ \hat{M}_{n_2}^{n_1} & \hat{M}_{n_2}^{n_2} \end{bmatrix}$ and $\tilde{M} = \begin{bmatrix} \tilde{M}_{n_1}^{n_1} & \tilde{M}_{n_1}^{n_2} \\ \tilde{M}_{n_2}^{n_1} & \tilde{M}_{n_2}^{n_2} \end{bmatrix}$, where subscript/superscript n_1 refers to PODs, n_2 refers to CHPs, and n_3 refers to HODs (e.g., $\hat{M}_{n_1}^{n_2}$ represents the connection information of the edges between PODs and CHPs).

2) The power generation and heat output

$$x(k+1) = Z\lambda(k+1) + B(p^C, h^C) \quad (18)$$

where $x = [p^P, p^C, h^C, h^H]^T$ represents the column stack vector of the energy outputs; $Z = \begin{bmatrix} \hat{Z} & \mathbf{0} \\ \mathbf{0} & \tilde{Z} \end{bmatrix} = \text{diag}(Z_p^P, Z_p^C, Z_h^C, Z_h^H)$ is a block matrix consisting of cost coefficients; it can be further defined as $Z_p^P = \text{diag}(1/2\alpha_i), i \in N_P$, $Z_p^C = \text{diag}(1/2\alpha_i), i \in N_C$, $Z_h^C = \text{diag}(1/2\theta_i), i \in N_C$, $Z_h^H = \text{diag}(1/2\alpha_i), i \in N_H$; $B(p^C, h^C) = [B_p^P, B_p^C(h^C), B_h^C(p^C), B_h^H]^T$ is the vector representing the power-heat coupling characteristics of the IES, where B_p^P is the column vector form of $\beta_i/2\alpha_i, i \in N_P$, $B_p^C(h^C)$ is the column vector form of $(\varepsilon_i h_i^C + \beta_i)/2\alpha_i, i \in N_C$, $B_h^C(p^C)$ is the column vector form of $(\varepsilon_i p_i^C + \delta_i)/2\theta_i, i \in N_C$, and B_h^H is the column vector form of $\beta_i/2\alpha_i, i \in N_H$.

3) The second consensus protocol

$$y(k+1) = Ny(k) - (x(k+1) - x(k)) \quad (19)$$

where $y = [y_p^P, y_p^C, y_h^C, y_h^H]^T$ represents the column stack vector of the local estimated energy mismatches; $N = \begin{bmatrix} \hat{N} & \mathbf{0} \\ \mathbf{0} & \tilde{N} \end{bmatrix}$ is a consensus update weighting matrix, where $\hat{N} = \begin{bmatrix} \hat{N}_{n_1}^{n_1} & \hat{N}_{n_1}^{n_2} \\ \hat{N}_{n_2}^{n_1} & \hat{N}_{n_2}^{n_2} \end{bmatrix}$ and $\tilde{N} = \begin{bmatrix} \tilde{N}_{n_1}^{n_1} & \tilde{N}_{n_1}^{n_2} \\ \tilde{N}_{n_2}^{n_1} & \tilde{N}_{n_2}^{n_2} \end{bmatrix}$.

The composite system of (17)–(19) can be rewritten as

$$\begin{bmatrix} \lambda(k+1) \\ y(k+1) \end{bmatrix} = \begin{bmatrix} M & \eta I \\ Z(I-M) & N-\eta Z \end{bmatrix} \begin{bmatrix} \lambda(k) \\ y(k) \end{bmatrix} - \begin{bmatrix} \mathbf{0} \\ \Delta B(k) \end{bmatrix} \quad (20)$$

where $\Delta B(k) = [\mathbf{0} \ \Delta p^C(k) \ \Delta h^C(k) \ \mathbf{0}]^T$ is a time-varying vector satisfying $\lim_{k \rightarrow \infty} \Delta B(k) = \mathbf{0}$, and there exists a constant ρ such that $\sum_{k=0}^{\infty} \|\Delta B(k)\| \leq \rho$.

In this article, the initial values of ICs and energy outputs are capable to be any feasible values, and the local estimated energy mismatches are initialized as follows:

$$\begin{cases} y_{p,i}^P(0) = P_{Di} - p_i^P(0), & i \in N_P \\ y_{p,i}^C(0) = P_{Di} - p_i^C(0), & i \in N_C \\ y_{h,i}^C(0) = H_{Di} - h_i^C(0), & i \in N_C \\ y_{h,i}^H(0) = H_{Di} - h_i^H(0), & i \in N_H \end{cases} \quad (21)$$

Theorem 1: If the communication topology is strongly connected, and the initial values of variables satisfy (21), then

the convergence point of the algorithm (20) satisfies the KKT optimality conditions. The consensus of Lagrangian variables λ_p and λ_h are reached, respectively. Furthermore, the variable x converges to the optimal solution of the ED problem (1) under the constraints (5)–(13) (see [Appendix C] [35] for proof).

As a result, on the premise that the conditions in Theorem 1 are satisfied, the algorithm (17)–(19) can be applied to solve the ED problem of the IES.

B. Privacy-Preserving Protocol

The execution of the distributed ED algorithm requires the exchange of updating information among units, which may increase the risk of private information leakage, because this information is usually transmitted over unprotected communication links. Generally speaking, malicious attackers can prepare for their further attacks according to this private information collected. To solve this problem, as the first line of defense against attacks, a privacy-preserving protocol is proposed in this section. The time-varying noise items $r^\lambda(k)$ and $r^y(k)$ are added into the algorithm (20) to conceal the vital updating information used in the ED process of the IES. Then, the algorithm integrated with the privacy-preserving protocol can be reformulated as follows:

$$\begin{bmatrix} \lambda(k+1) \\ y(k+1) \end{bmatrix} = \begin{bmatrix} M & \eta I \\ Z(I-M) & N-\eta Z \end{bmatrix} \begin{bmatrix} \lambda(k) \\ y(k) \end{bmatrix} - \begin{bmatrix} \mathbf{0} \\ \Delta B(k) \end{bmatrix} + \begin{bmatrix} r^\lambda(k) \\ r^y(k) \end{bmatrix} \quad (22)$$

Theorem 2: As long as the added noise terms and a sufficiently small constant $\tau > 0$ satisfy the following conditions:

$$\sum_{k=0}^{\infty} \|r_i^\lambda(k)\| \leq \tau, \sum_{k=0}^{\infty} \|r_i^y(k)\| \leq \tau, \lim_{k \rightarrow \infty} \sum_{t=0}^k \sum_{i \in V} r_i^y(t) = 0$$

then we can obtain that the convergence point of the algorithm (22) satisfies the KKT optimality conditions (see [Appendix D] [35] for proof).

Remark 1: It is worth noting that the added noise items satisfying certain conditions will not affect the final convergence results of the distributed algorithm (22). Moreover, according to Assumption 2 (see [Appendix D] [35]), the above conditions always hold. As a result, the distributed units can carry out this distributed algorithm to solve the ED problem without deciphering the critical information amongst added noises. By embedding the privacy-preserving protocol, this distributed algorithm can enhance the safety and reliability of the ED process of the IES.

C. Attack Effect on the ED of the IES

In this section, we use the noncolluding replay attack as an example to describe the harmful effect of cyber-attacks on the ED of the IES.

Because the implementation of replay attacks is to make compromised units repeatedly send wrong information to the whole communication network, the term on the left-hand side and the first term on the right-hand side in (22) can be reformulated as

follows:

$$\begin{bmatrix} \lambda_m(k+1) \\ \lambda_w(k+1) \\ y_m(k+1) \\ y_w(k+1) \end{bmatrix} = T \begin{bmatrix} \lambda_m(k) \\ \lambda_w(k) \\ y_m(k) \\ y_w(k) \end{bmatrix} \quad (23)$$

$$\text{where } T = \begin{bmatrix} I_m & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ M_m & M_w & \mathbf{0} & \eta I_w \\ \mathbf{0} & \mathbf{0} & I_m & \mathbf{0} \\ (Z(I-M))_m & Z_w(I_w-M_w) & (N-\eta Z)_m & N_w-\eta Z_w \end{bmatrix}$$

and the vectors and matrices with subscript m refer to the misbehaving units caused by attacks, the vectors and matrices with subscript w refer to the well-behaving units, and I represents the identity matrix with appropriate dimension.

The convergence result of (22) under replay attacks depends on the convergence result of (23), which is analyzed and presented as follows:

$$\begin{aligned} \lambda_m^* &= \lambda_m, y_m^* = y_m \\ \lambda_w^* &= A_w^{-1}[\eta B_w^{-1}\{(Z(I-M))_m + Z_w M_m\} \\ &+ M_m - \eta B_w^{-1}(N - \eta Z)_m][\lambda_m^* \ y_m^*]^T \\ y_w^* &= B_w^{-1}[(Z(I-M))_m + Z_w M_m - (N - \eta Z)_m][\lambda_m^* \ y_m^*]^T \end{aligned}$$

where $A_w = I_w - M_w$, $B_w = I_w - N_w$.

The above convergence results mean that the ICs and local estimated power/heat mismatches of well-behaving units converge to the stable vector space spanned by $[\lambda_m^* \ y_m^*]^T$, i.e., the power/heat supply–demand balance constraints cannot be satisfied, and the consensus of variables λ associated with the well-behaving units cannot be achieved.

The above analysis uncovers the purposes of cyber-attacks in the IES. It is easy to conclude that the convergence point of the distributed ED algorithm under replay attacks is altered. In other words, the operation point of the IES is no longer the most economical, i.e., each energy device cannot keep the optimal output that minimizes the total operation cost of the system. More importantly, the power/heat supply–demand balance is destroyed, which undermines the stability of IES operation. Similarly, the economic and stable performance of the IES is damaged under DoS attacks [23] and FDI attacks [18]. To solve this problem, it is necessary to propose a robust ED strategy to mitigate the effect of attacks on the system performance.

IV. DISTRIBUTED ROBUST ED STRATEGY AGAINST CYBER-ATTACKS FOR THE IES

A. Detection Process

Detection of cyber-attacks needs to introduce the observation subnetwork, which is added to the communication network, as shown in Fig. 1. Inspired by the neighborhood watch mechanism [32], the observation subnetwork is established on the basis of the communication network. It worth noting that the communication network engages in the ED by transmitting the updating information in (17) and (19), but the observation subnetwork only transmits the attack detection results and monitors the behavior of neighbor units. Thus, the observation subnetwork does not engage in the ED of the IES.

Let the graph $G' = \{V, E'\}$ model the observation subnetwork topology, where the edge set E' depends on the topology

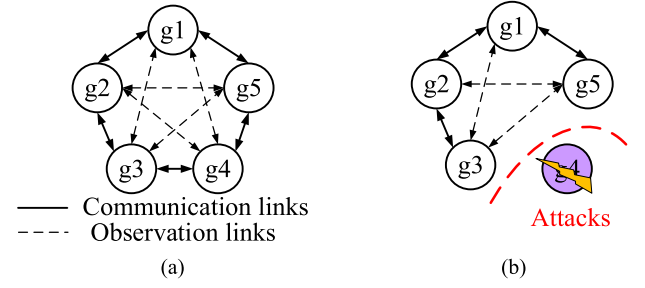


Fig. 1. Topologies of the communication network integrated with the observation subnetwork. (a) Ideal communication network. (b) Isolating misbehaving unit g4.

of the communication network as follows:

$$E' = \{(i, j) | \forall j \in N_v^+, \forall i \in N_v^-, \forall v \in V\}. \quad (24)$$

According to the definitions of graphs G and G' , it can be deduced that other than sending its own updating information, each unit also relays all the updating information of its in-neighbors to its out-neighbors. Thus, each unit can receive the information of its two-hop neighbors and utilize these information to detect cyber-attacks. Furthermore, for each unit v , $v \in V$, the detection results can be delivered from any of its out-neighbors to any of its in-neighbors through the observation subnetwork.

To describe the neighbor-observe-based detection process proposed in this article, we use units i , j , and v as an example. According to Assumption 1 and algorithm (20), unit i , $i \in N_v^-$, can estimate the rational bounds of the updating information of unit v in the next iteration, which can be further expressed as follows.

1) The rational bounds of the local estimated energy mismatches of unit v in the next iteration

$$y_v^{\text{up}}(k+1) = \sum_{l \in N_v^+} Y^+(y_l(k)) + \Upsilon(k, R) \quad (25)$$

$$y_v^{\text{low}}(k+1) = \sum_{l \in N_v^+} Y^-(y_l(k)) - \Upsilon(k, R) \quad (26)$$

where $\Upsilon(k, R)$ is a detection threshold function, which is determined by the iterations k and R , where R is a public parameter denoting the maximum value of the ramp rate limits of various energy equipment. The function satisfies $\Upsilon(k, R) \geq 0$ and $\lim_{k \rightarrow \infty} \Upsilon(k, R) = 0$. The function $Y^+(a)$ is defined as $Y^+(a) = \varrho_{\max} a$ when $a \geq 0$, otherwise $Y^+(a) = \varrho_{\min} a$. While $Y^-(a)$ is defined as $Y^-(a) = \varrho_{\min} a$ when $a \geq 0$, otherwise $Y^-(a) = \varrho_{\max} a$.

2) The rational bounds of the ICs of unit v in the next iteration

$$\begin{aligned} \lambda_v^{\text{up}}(k+1) &= \sigma \sum_{l \in N_v^+ - L_v^{\max}(k)} \lambda_l(k) + [1 - \sigma(|N_v^+| \\ &- |L_v^{\max}(k)|)] \lambda_v^{\max}(k) + \eta y_v(k) \end{aligned} \quad (27)$$

$$\begin{aligned} \lambda_v^{\text{low}}(k+1) &= \sigma \sum_{l \in N_v^+ - L_v^{\min}(k)} \lambda_l(k) + [1 - \sigma(|N_v^+| \\ &- |L_v^{\min}(k)|)] \lambda_v^{\min}(k) + \eta y_v(k) \end{aligned} \quad (28)$$

where $\lambda_v^{\max}(k) = \max\{\lambda_l(k) | \forall l \in N_v^+\}$ and $\lambda_v^{\min}(k) = \min\{\lambda_l(k) | \forall l \in N_v^+\}$; $L_v^{\max}(k) = \{l | \lambda_l(k) = \lambda_v^{\max}(k)\}$ and $L_v^{\min}(k) = \{l | \lambda_l(k) = \lambda_v^{\min}(k)\}$.

Based on this, the general idea of the detection process is expounded as follows.

Step 1: At iteration k , unit i estimates the rational bounds of $y_v(k+1)$ according to (25) and (26).

Step 2: Unit i compares the estimated feasible range of $y_v(k)$ with the received actual value of that. If $y_v^{\text{low}}(k) \leq y_v(k) \leq y_v^{\text{up}}(k)$ is satisfied, go to step 3; otherwise, unit v is judged to be misbehaving; go to step 5.

Step 3: Unit i estimates the rational bounds of $\lambda_v(k+1)$ according to (27) and (28).

Step 4: Unit i compares the estimated rational range of $\lambda_v(k)$ with the actual values of that. If $\lambda_v^{\text{low}}(k) \leq \lambda_v(k) \leq \lambda_v^{\text{up}}(k)$ is satisfied, unit v is judged to be well-behaving; otherwise, it is judged to be misbehaving. In particular, if the estimates $\lambda_v^{\text{low}}(k)$ and $\lambda_v^{\text{up}}(k)$ are absent, unit v is judged to be misbehaving directly.

Step 5: Update the detection result variable $d_v(k)$ of unit v as follows:

$$d_v(k) = \begin{cases} 1, & \text{unit } v \text{ is well-behaving} \\ 0, & \text{otherwise} \end{cases}. \quad (29)$$

Then, $d_v(k)$ is delivered from unit i to unit $j, j \in N_v^+$ through the observation subnetwork, and all the neighbors of unit v will activate the isolation process (the details are shown in the following sections).

Step 6: Let $k = k + 1$; repeat steps 1–5.

Remark 2: The detection process proposed above needs to detect variables y and λ . Thus, more computation burden arises from calculating the estimations and performing the validation, it is necessary to consider the tradeoff between additional burden and security requirements. To solve this problem, a conditional discrimination mechanism is introduced in this detection process. Note that each unit detect y first according to (25) and (26), and λ will be detected according to (27) and (28) if and only if y is considered to be safe. This detection mechanism reduces the computation burden and saves the memory space of system. Compared with literature [29], where only variable λ is selected to detect, the detection process proposed in this article is more comprehensive and implemented in a fully distributed fashion.

B. Isolation Process of the Misbehaving Units Caused by Noncolluding Attacks

In this section, an isolation process against the misbehaving units is proposed. First, a counting rule is defined as follows:

$$T_{iv}(k) = \begin{cases} T_{iv}(k-1) + 1, & d_v(k) = 1 \\ T_{iv}(k-1), & \text{otherwise} \end{cases} \quad (30)$$

where $T_{iv}(k)$ denotes a counter, and its initial value is set to $T_{iv}(0) = 0$. Simultaneously, unit j also update the counter $T_{vj}(k)$ with (30) according to the detection result $d_v(k)$.

Then, an auxiliary variable named reputation value is defined, which is used to adapt the distributed ED algorithm. The reputation value $\text{rep}_{iv}(k)$ is calculated as follows:

$$\text{rep}_{iv}(k) = \frac{\omega_k T_{iv}(k) + 1}{\omega_k k + 1} \quad (31)$$

where $\omega_k > 0$ is a time-varying parameter named reputation coefficient, which is used to dynamically adjust the rate of adaptation. The reputation value $\text{rep}_{iv}(k)$ satisfies $0 \leq \text{rep}_{iv}(k) \leq 1$.

If a unit is always well-behaving, its reputation value will be equal to 1; otherwise, the reputation value will gradually decrease from 1. We assume that the existence of communication links among the units depends on their reputation values. Consequently, the elements of M used in the distributed ED algorithm (20) vary with the principle as follows:

$$m_{iv}(k) = \frac{[\text{rep}_{iv}(k)]_{\text{rep}_{iv}}^+}{\sum_{l \in N_i^+} [\text{rep}_{il}(k)]_{\text{rep}_{il}}^+} \quad (32)$$

where rep_{iv}' is the threshold of reputation value satisfying $\sigma(|N_i^+| - 1)/(1 - \sigma) \leq \text{rep}_{iv}' \leq 1$. Combined with ω_k , rep_{iv}' is introduced to tolerate transient miscommunication of information caused by network fluctuations. It worth noting that this isolation process can dynamically adjust its tolerance to transient network fluctuations to avoid misoperation or inaction of the isolation mechanism. Similarly, the elements of N used in (20) vary with the reputation value rep_{vj} . The function $[a]_b^+$ is defined as

$$[a]_b^+ = \begin{cases} a, & a \geq b \\ 0, & \text{otherwise} \end{cases}. \quad (33)$$

When the reputation values of all the communication links connected to the misbehaving units drop below the threshold, the misbehaving units are isolated from the communication network, as shown in Fig. 1(b).

Remark 3: By setting the variable $d_v(k)$, although the in-neighbors of the misbehaving unit are not engaged in the attack detection, they can also identify the misbehaving unit and activate the isolation process. It means that the detected misbehaving units can be isolated from the communication network completely, which also prevents attackers from sniffing crucial information through the medium of misbehaving units. The safety and reliability of the system are further improved.

Remark 4: It is worth noting that the isolation process (30)–(32) cannot physically disconnect the misbehaving units from the physical network, which only occurs on the communication network. It means that the misbehaving units continue to supply local power/heat demand although they are isolated from the communication network entirely at iteration k ; meanwhile, their local estimated power/heat mismatches are set to zero. Then, the well-behaving units remeasure the load consumption for some particular districts and re-estimate the local energy mismatches with the correction rules (21). Therefore, the remaining well-behaving units continue to implement the ED process, and the multienergy supply–demand balance of the IES can be satisfied ultimately. It means that the detection and correction mechanism for local estimated energy mismatches can avoid the possibility

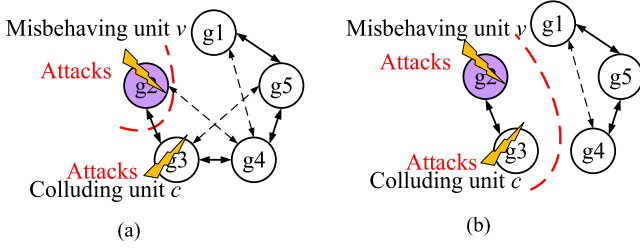


Fig. 2. Diagrams of the isolation of colluding attacks. (a) Misbehaving unit g2 colludes with g3. (b) Isolating misbehaving unit g2 and g3.

that the attackers use the damaged load data to disrupt the multienergy supply–demand balance of the system.

C. Isolation Process of the Misbehaving Units Caused by Colluding Attacks

The isolation process in the previous section can effectively prevent the further impact of noncolluding attacks on communication. However, the colluding attacks cannot be isolated by the above process because of their special trait. Under the colluding attack mode, for example, the misbehaving unit v sends the colluding request to its out-neighbor c , $c \in N_v^-$, an undetected “well-behaving” unit. Then, the colluding unit c deliberately deactivates the isolation process even if the abnormal behavior of unit v has been detected, as shown in Fig. 2(a). If the misbehaving units are still connected with their colluding units, the false information can be propagated to the whole communication network. Therefore, we propose an additional isolation process against the colluding attacks as follows:

Step 1: When the misbehaving unit v has been isolated by its neighbors with the isolation process (30)–(32), update the matrix $F(k) = [f_{ij}(k)]^{n \times n}$ to record the connection information in the observation subnetwork as follows:

$$f_{ij}(k) = \begin{cases} 1, & (j, i) \in E' \\ 0, & \text{otherwise} \end{cases}. \quad (34)$$

Step 2: If there is at least one nonzero element in the v th row of the matrix $F(k)$, it means that the misbehaving unit v is not completely isolated, i.e., there are colluding attacks in the communication network. Unit c can be judged to be the colluding unit of v easily, and it is considered to be a misbehaving unit.

Step 3: The result of the judgment on unit c is sent by its out-neighbors to its in-neighbors, and the isolation process (30)–(32) is carried out to isolate it.

Step 4: Repeat steps 1–3 until all the misbehaving units caused by colluding attacks are isolated from the communication network, as shown in Fig. 2(b).

Remark 5: The proposed isolation process can effectively prevent the further impact of colluding attacks and noncolluding attacks on communication. In addition, we assume that once cyber-attacks disappear, any disconnected communication link caused by the isolation process will be recovered into connected state by a restoration process. The restoration process is the inverse process of the isolation process; it will not be detailed here for the sake of convenience.

The distributed robust ED strategy proposed in this article includes the detection and isolation process, which is applicable to mitigating the impact of various cyber-attacks on the ED of the IES. If the communication network topology is still strongly connected, Theorem 1 still holds, and the consensus of variables λ and y associated with the remaining well-behaving units can be reached ultimately. As a result, the acceptable suboptimal solution can be obtained for the ED problem of the IES under various cyber-attacks, and the multienergy supply–demand balance can be guaranteed.

V. SIMULATION EXAMPLES

Simulation examples are performed on a power–heat IES inspired by the Barry Island case studied in [2]. The simulation test platform is built in the MATLAB environment. The proposed distributed robust ED strategy is implemented on a computer with Intel Xeon E-2186M (Six Core Xeon 2.90 GHz, 4.80-GHz Turbo, 12 MB 45 W) and 64-GB memory. This test system consists of a 39-bus power system and a 32-node heating system; its configuration and communication are shown in [Fig. E1, Appendix E] [35]. The communication mode adopted in this article is point-to-point mode. Meanwhile, multiple communication protocols are available, such as the Ethernet TCP/IP, ZigBee over IEEE 802.15.4, and Bluetooth over IEEE 802.15.1. The parameters of the energy units that make up this test system are listed in [Tables E1– E4, Appendix E] [35]. The total power demand is set to 600 kW, and the total heat demand is set to 700 kW. The convergence coefficient η in (20) is set to 0.005. Moreover, the thresholds of the reputation value of communication links are shown in [Table E5, Appendix E] [35]. In the interval $k \in [0500]$, the reputation coefficient ω_k in (31) is set to the following form:

$$\omega_k = \begin{cases} 0.1, & k \in [0, 20] \\ 0.085, & k \in [20, 100] \\ 0.05, & \text{otherwise} \end{cases}.$$

A. ED Under Ideal Communication Conditions

The convergence results of the dispatch system under ideal communication conditions are shown in Fig. 3. Without the interference of cyber-attacks, the power ICs of all the devices converge to $\lambda_p = 33.7240\$/\text{kWh}$ and the heat ICs converge to $\lambda_h = 22.8513\$/\text{kWh}$, as shown in Fig. 3(b). Furthermore, the power/heat supply–demand balance of the IES is achieved ultimately, as shown in Fig. 3(a). Obviously, the optimal solution of the ED problem can be obtained under the ideal communication conditions. This simulation case serves as a reference for the following simulation examples.

B. ED Under Noncolluding Attacks

This case investigates the scenario that the ED of the IES is performed under noncolluding attacks. Assume that at iteration $k = 20$, units 3 and 9 are subject to noncolluding replay attacks simultaneously.

The convergence results of the dispatch system without any robust strategy are shown in Fig. 4. As shown in Fig. 4(b), the

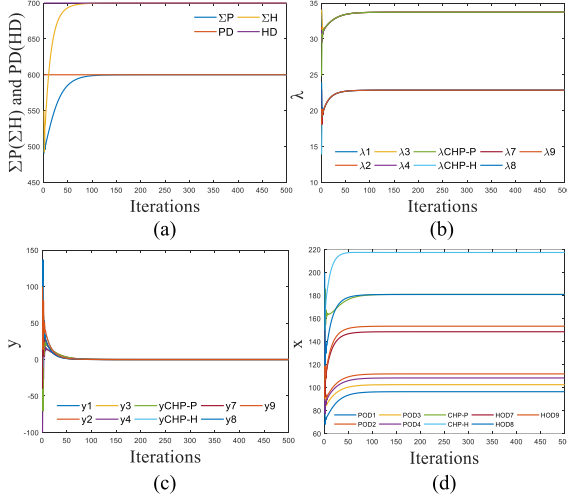


Fig. 3. Convergence results of the dispatch system under ideal communication conditions. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

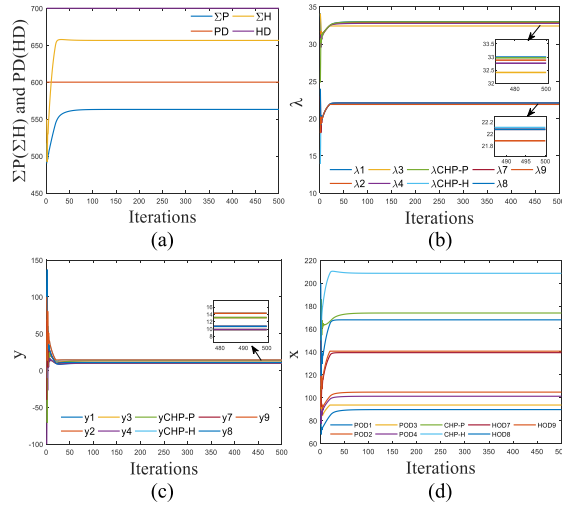


Fig. 4. Convergence results of the dispatch system without any robust strategy under noncolluding attacks. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

power/heat ICs cannot reach consensus. As shown in Fig. 4(a) and (c), the local estimated energy mismatches cannot converge to zero, and the multienergy supply–demand balance of the IES is destroyed by noncolluding attacks. The correctness of theoretical results with respect to the effect of attacks on ED is verified. In comparison, the convergence results of the dispatch system with the proposed robust strategy are shown in Fig. 5. It can be obtained that the misbehaving units 3 and 9 have been isolated at iteration $k = 40$, and the remaining well-behaving units continue to execute the distributed ED algorithm. As shown in Fig. 5(c), the trajectories of y fluctuate at iteration $k = 40$. It is not difficult to infer that this is because the local estimated energy mismatches of units 3 and 9 are set to zero, while the remaining well-behaving units re-estimate their power/heat mismatches for some particular districts. Ultimately, the power ICs of remaining

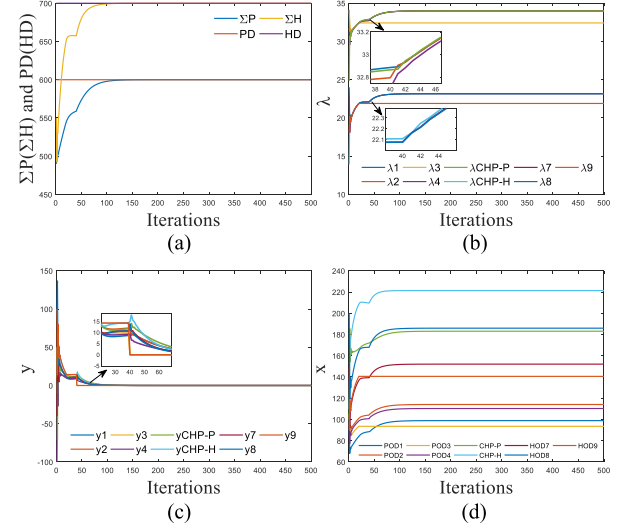


Fig. 5. Convergence results of the dispatch system with robust strategy under noncolluding attacks. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

well-behaving units converge to $\lambda_p = 33.9946\$/\text{kWh}$ and the heat ICs converge to $\lambda_h = 23.1570\$/\text{kWh}$ as shown in Fig. 5(b), which is an acceptable suboptimal solution of the ED problem of the IES. Furthermore, the power/heat supply–demand balance of the IES can be achieved under noncolluding attacks, as shown in Fig. 5(a). The above analyses show the effectiveness of the proposed robust strategy in mitigating the impact of noncolluding attacks on ED of the IES.

C. ED Under Colluding Attacks

This case investigates the ED problem of the IES under non-colluding attacks. Two methods of attack isolation are adopted: one is an ordinary isolation strategy in [17], and the other is the robust strategy proposed in this article. Assume that at iteration $k = 20$, unit 3 is subject to replay attacks, and it colludes with unit 2.

Fig. 6 shows the convergence results of the dispatch system with the ordinary isolation strategy; it can be observed that misbehaving unit 3 cannot be entirely isolated from the communication network. As a result, attacks continue to affect the ED of the IES. By contrast, Fig. 7 shows the convergence results of the dispatch system with the robust strategy proposed in this article. It is not difficult to observe that unit 3 has been partly isolated at iteration $k = 40$. Then, at iteration $k = 50$, units 2 and 3 have been both entirely isolated, and their local estimated energy mismatches are set to zero while the remaining well-behaving units re-estimate their power/heat mismatches for some particular districts, as shown in Fig. 7(c). Ultimately, the power ICs of remaining well-behaving units converge to $\lambda_p = 34.1700\$/\text{kWh}$ and the heat ICs converge to $\lambda_h = 22.9199\$/\text{kWh}$, as shown in Fig. 7(b). The power/heat supply–demand balance of the IES is achieved, as shown in Fig. 7(a). In other words, the impact of colluding attacks on the economic and stable performance of the IES is mitigated, and an acceptable suboptimal solution of

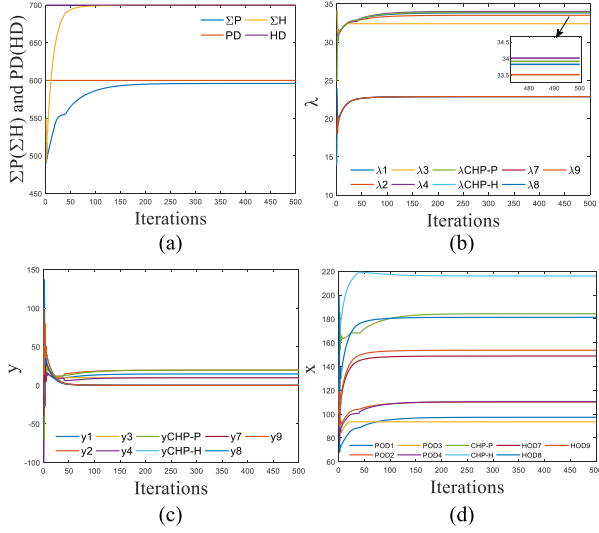


Fig. 6. Convergence results of the dispatch system with the ordinary strategy under colluding attacks. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

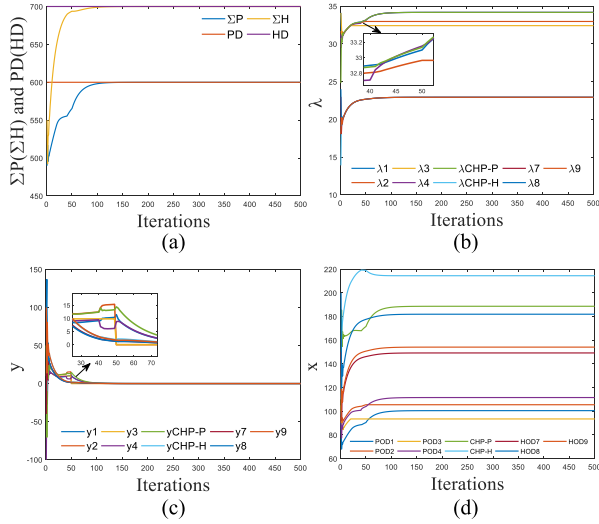


Fig. 7. Convergence results of the dispatch system with robust strategy under colluding attacks. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

the ED problem can be obtained. The above analyses show the effectiveness of the robust ED strategy against colluding attacks. Furthermore, according to Fig. 7(d) and the convergence point of heat ICs, it can be observed that energy changes in the power system can also affect the heating system. The strong coupling characteristic of the IES can be reflected in the implementation of the robust strategy proposed in this article.

D. Attackers Use the Damaged Load Data to Disrupt the ED

In this case, a special type of FDI attack is considered. Instead of directly damaging the communication links or disturbing the

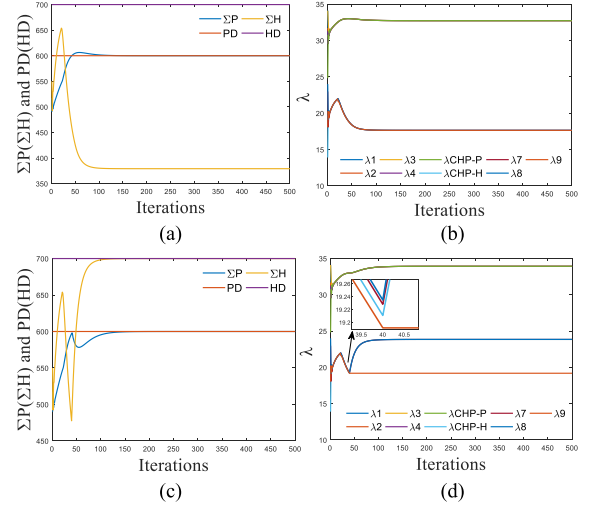


Fig. 8. Convergence results of the dispatch system with robust strategy under FDI attacks. (a) Total power/heat output and load demand. (b) Power/heat IC of each unit. (c) Power/heat mismatch of each unit. (d) Power/heat output of each unit.

data transmitted on them, this attack affects the local variables of a unit, i.e., the measured load data. Assume that unit 9 is subject to FDI attacks at iteration $k = 20$ until $k = 50$, during which the false load measurement value continuously uploaded by unit 9 is 80 kW. This causes the local estimated heat mismatch of unit 9 to be updated with $y_{h,9}^H(k) = 80 - h_9^H(k)$.

The convergence results of the dispatch system without any robust strategy is shown in Fig. 8(a) and (b). As shown in Fig. 8(b), the consensuses of power ICs and heat ICs are reached, respectively. However, as shown in Fig. 8(a), the heat supply–demand balance of the IES is destroyed by attacks, and there is a big gap between the heat supply and demand. By contrast, the convergence results of the dispatch system with the proposed robust strategy are shown in Fig. 8(c) and (d). It can be obtained that misbehaving unit 9 has been isolated at iteration $k = 40$; then, its local estimated heat mismatch has been set to zero, and the remaining well-behaving units re-estimate their power/heat mismatches. Ultimately, the power ICs of remaining well-behaving units converge to $\lambda_p = 33.9152\$/\text{kWh}$, and the heat ICs converge to consensus $\lambda_h = 23.8473\$/\text{kWh}$, as shown in Fig. 8(d). Moreover, the power/heat supply–demand balance of the IES is satisfied, as shown in Fig. 8(c). It means that an acceptable suboptimal solution of the ED problem can be obtained. The intention of attacks is destroyed, and the impact of attacks on the economic and stable performance of the IES is mitigated. The above analyses show the effectiveness of the robust ED strategy against the special type of FDI attack.

VI. CONCLUSION

This article proposed a fully distributed ED strategy for the IES, which is robust against various noncolluding and colluding attacks. First, a privacy-preserving protocol was designed for covering up some vital information used for ED of the IES. On this basis, by using the neighbor-observe-based detection

process, the misbehaving units caused by cyber-attacks can be effectively detected. Then, the misbehaving units were isolated by their neighbors with the reputation-based isolation process, so that the remaining well-behaving units can still accomplish the ED. Finally, the effectiveness of the proposed strategy was illustrated by the simulation cases implemented on a power-heat IES. Research on robust ED strategies against cyber-attacks is of great significance to enhance the stability and guarantee the economic operation of the system.

Based on the above analyses, the robust strategy proposed in this article can be abstracted as an attack-robust framework, which includes the detection and isolation process. In the future, we would like to take into account nonconvex and more physical limits and more distributed algorithms and further extend the application of this attack-robust framework in other multiagent systems. In addition, we will further study the ED problem of the IES with multi-time-scale characteristic under cyber-attacks, which possesses more practical values and more challenging theoretical difficulty.

REFERENCES

- [1] Y. Li, W. Gao, G. Wei, H. Zhang, and J. Zhou, "A distributed double-newton descent algorithm for cooperative energy management of multiple energy bodies in energy internet," *IEEE Trans. Ind. Informat.*, to be published, doi: [10.1109/TII.2020.3029974](https://doi.org/10.1109/TII.2020.3029974).
- [2] X. Liu, J. Wu, N. Jenkins, and A. Bagdanavicius, "Combined analysis of electricity and heat networks," *Appl Energy*, vol. 162, pp. 1238–1250, Jan. 2016.
- [3] C. Zhang, Y. Xu, Z. Y. Dong, and L. F. Yang, "Multi-timescale coordinated adaptive robust operation for industrial multienergy microgrids with load allocation," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3051–3063, May 2020.
- [4] Z. Lv, W. Kong, X. Zhang, D. Jiang, H. Lv, and X. Lu, "Intelligent security planning for regional distributed energy internet," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3540–3547, May 2020.
- [5] Y. Zhou, Z. Wei, and G. Sun, "A robust optimization approach for integrated community energy system in energy and ancillary service markets," *Energy*, vol. 148, pp. 1–15, Apr. 2018.
- [6] B. Huang, L. Liu, and H. Zhang, "Distributed optimal economic dispatch for microgrids considering communication delays," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1634–1642, Aug. 2019.
- [7] H. Li, Z. Wang, G. Chen, and Z. Y. Dong, "Distributed robust algorithm for economic dispatch in smart grids over general unbalanced directed networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4322–4332, Jul. 2020.
- [8] W. Yan, L. Cheng, S. Yan, W. Gao, and D. W. Gao, "Enabling and evaluation of inertial control for PMSG-WTG using synchronverter with multiple virtual rotating masses in microgrid," *IEEE Trans. Sustain. Energy*, vol. 11, no. 2, pp. 1078–1088, Apr. 2020.
- [9] R. Han *et al.*, "Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded AC microgrids," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5187–5199, Nov./Dec. 2017.
- [10] Y. Li, H. Zhang, and X. Liang, "Event-triggered-based distributed cooperative energy management for multienergy systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2008–2022, Apr. 2019.
- [11] R. Han, L. Meng, J. M. Guerrero, and J. C. Vasquez, "Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in dc microgrids," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 6416–6433, Jul. 2018.
- [12] G. Xie, K. Yang, H. Luo, R. Li, and S. Hu, "Reliability and confidentiality co-verification for parallel applications in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 6, pp. 1353–1368, Jan. 2021.
- [13] J. Huang, Y. Tang, W. Yang, and F. Li, "Resilient consensus-based distributed filtering: Convergence analysis under stealthy attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4878–4888, Jul. 2020.
- [14] Q. Zhang, F. Li, Q. Shi, K. Tomovic, J. Sun, and L. Ren, "Profit-oriented false data injection on energy market: Reviews, analyses and insights," *IEEE Trans. Ind. Informat.*, to be published, doi: [10.1109/TII.2020.3036104](https://doi.org/10.1109/TII.2020.3036104).
- [15] A. Sawas, H. Khani, and H. Farag, "On the resiliency of power and gas integration resources against cyber-attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3099–3110, May 2021, doi: [10.1109/TII.2020.3007425](https://doi.org/10.1109/TII.2020.3007425).
- [16] E. Mousavinejad, F. Yang, Q. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.
- [17] W. Zeng, Y. Zhang, and M. Y. Chow, "Resilient distributed energy management subject to unexpected misbehaving generation units," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 208–216, Feb. 2017.
- [18] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, Dec. 2016.
- [19] W. Zhang and X. He, "Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem," *Int. J. Elect. Power Energy Syst.*, vol. 103, pp. 233–246, Dec. 2018.
- [20] K. Hamedani, L. Liu, S. Hu, J. Ashdown, J. Wu, and Y. Yi, "Detecting dynamic attacks in smart grids using reservoir computing: A spiking delayed feedback reservoir based approach," *IEEE Trans. Power Del.*, vol. 4, no. 3, pp. 253–264, Aug. 2020.
- [21] Y. Li, Y. Wang, and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2031–2043, Mar. 2020.
- [22] W. Zhe, C. Wei, and L. Chunlin, "DoS attack detection model of smart grid based on machine learning method," in *Proc. IEEE Int. Conf. Power, Intell. Comput. Syst.*, Shenyang, China, 2020, pp. 735–738.
- [23] Z. Zhang, D. Yue, and C. Dou, "A robust consensus-based economic dispatch strategy under DoS attack," in *Proc. IEEE Int. Conf. Ind. Cyber Phys. Syst.*, Taipei, Taiwan, 2019, pp. 127–132.
- [24] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019.
- [25] W. Xu *et al.*, "Event/Self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 10, pp. 3137–3149, Jan. 2019.
- [26] D. Shi, Z. Guo, K. Johansson, and L. Shi, "Causality countermeasures for anomaly detection in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 63, no. 2, pp. 386–401, Feb. 2018.
- [27] D. Wei, Y. Lu, and M. Jafari, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.
- [28] D. Li, N. Gebräel, and K. Paynabar, "Detection and differentiation of replay attack and equipment faults in SCADA systems," *IEEE Trans. Autom. Sci. Eng.*, to be published, doi: [10.1109/TASE.2020.3013760](https://doi.org/10.1109/TASE.2020.3013760).
- [29] P. Li, Y. Liu, and H. Xin, "A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4343–4352, Oct. 2018.
- [30] Q. Sun, R. Fan, Y. Li, B. Huang, and D. Ma, "A distributed double-consensus algorithm for residential we-energy," *IEEE Trans. Ind. Informat.*, vol. 15, no. 8, pp. 4830–4842, Aug. 2019.
- [31] S. Yang, S. Tan, and J. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4416–4426, Nov. 2013.
- [32] J. Duan and M. Chow, "A novel data integrity attack on consensus-based distributed energy management algorithm using local information," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1544–1553, Mar. 2019.
- [33] Y. Li, D. W. Gao, W. Gao, H. Zhang, and J. Zhou, "Double-mode energy management for multi-energy system via distributed dynamic event-triggered Newton-Raphson algorithm," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5339–5356, Nov. 2020.
- [34] J. He, M. Zhou, C. Peng, S. Ling, and J. Chen, "Consensus under bounded noise in discrete network systems: An algorithm with fast convergence and high accuracy," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 1–11, Nov. 2016.
- [35] [Online]. Available: https://www.researchgate.net/publication/351221752_APPENDIX_A_KARUSH-KUHN-TUCKER_CONDITIONS April 2021.



Bonan Huang received the B.S. degree in electronic information engineering from Tianjin University, Tianjin, China, in 2005, and the M.A.Sc. and Ph.D. degrees in control theory and control engineering from Northeastern University, Shenyang, China, in 2008 and 2014, respectively.

He is currently an Associate Professor with the School of Information Science and Engineering, Northeastern University. His research interests include the collaborative control and operation optimization of energy Internet and multienergy systems, and cyber-physical security analysis of smart energy systems.



Qiuye Sun (Senior Member, IEEE) received the B.S. degree in power system and its automaton from the Northeast Dianli University of China, Jilin City, China, in 2000, and the M.S. degree in power electronics and drives and the Ph.D. degree in control theory and control engineering from Northeastern University, Shenyang, China, in 2004 and 2007, respectively.

Since 2014, he has been a Full Professor with the School of Information Science and Engineering, Northeastern University. He has authored or coauthored more than 280 journal and conference papers, six monographs, and co-invented 90 patents. His main research interests include optimization analysis technology of power distribution network, network control of distributed generation system, microgrids, and energy Internet.



Yushuai Li (Member, IEEE) received the B.S. degree in electrical engineering and automation and the Ph.D. degree in control theory and control engineering from Northeastern University, Shenyang, China, in 2014 and 2019, respectively.

From 2019 to 2020, he was a Postdoctoral Research Scholar with the Department of Electrical and Computer Engineering, University of Denver, Denver, CO, USA. He is currently a Lecturer with the School of Information Science and Engineering, Northeastern University. His main research interests include distributed modeling, control, energy management and optimization of energy Internet and multienergy systems, and distributed machine learning algorithm with applications in microgrids.

Dr. Li is the Section Chair for the IEEE 4th Conference on Energy Internet and Energy System Integration.



Huaguang Zhang (Fellow, IEEE) received the B.S. and M.S. degrees in control engineering from the Northeast Dianli University of China, Jilin City, China, in 1982 and 1985, respectively, and the Ph.D. degree in thermal power engineering and automation from Southeast University, Nanjing, China, in 1991.

In 1992, he joined the Department of Automatic Control, Northeastern University, Shenyang, China, as a Postdoctoral Fellow for two years. Since 1994, he has been a Professor and Head of the Institute of Electric Automation, School of Information Science and Engineering, Northeastern University. He has authored or coauthored more than 280 journal and conference papers, six monographs, and co-invented 90 patents. His main research interests include fuzzy control, stochastic system control, neural-network-based control, nonlinear control, and their applications.

Dr. Zhang is the E-letter Chair of the IEEE Computational Intelligence Society and the former Chair of the Adaptive Dynamic Programming and Reinforcement Learning Technical Committee on the IEEE Computational Intelligence Society. He is an Associate Editor for *Automatica*, *IEEE TRANSACTIONS ON NEURAL NETWORKS*, *IEEE TRANSACTIONS ON CYBERNETICS*, and *Neurocomputing*. He was an Associate Editor for *IEEE TRANSACTIONS ON FUZZY SYSTEMS* from 2008 to 2013. He received the Outstanding Youth Science Foundation Award from the National Natural Science Foundation Committee of China in 2003. He was named the Cheung Kong Scholar by the Education Ministry of China in 2005. He is a recipient of IEEE TRANSACTIONS ON NEURAL NETWORKS 2012 Outstanding Paper Award.



Fengnan Zhan received the B.S. degree in electrical engineering and automation from North China Electric Power University, Beijing, China, in 2018. She is currently working toward the master's degree in electric power system and automation with Northeastern University, Shenyang, China.

Her current research interests include distributed control and optimization of integrated energy systems and cyber-attacks in cyber-physical systems.