Hindawi
Complexity
Volume 2022, Article ID 5995281, 15 pages
https://doi.org/10.1155/2022/5995281

Research Article

Distributed Energy Management for Port Power System under False Data Injection Attacks

Qihe Shan,[1] **Xin Zhang**,[1] **Qiongyue Zhang**,[1] **and Qiuye Sun**[2]

[1]*Navigation College, Dalian Maritime University, Dalian 116026, China*
[2]*School of Information Science and Engineering, Northeastern University, Shenyang 110819, China*

Correspondence should be addressed to Qiuye Sun; sunqiuye@ise.neu.edu.cn

Received 30 April 2021; Revised 9 December 2021; Accepted 24 December 2021; Published 31 January 2022

Academic Editor: Ning Cai

This paper investigates a distributed energy management strategy for the port power system under false data injection attacks. The attacker can tamper with the interaction information of energy equipment, penetrate the boundary between port information system and port power system, and cause serious operation failure of port energy equipment. Firstly, a hierarchical topology is proposed to allocate the security resources of the port power system. Secondly, by reconstructing the topological structure of the port information system, the robustness of the information system is improved, and the impact of false data injection attacks on the port power system is reduced, which realizes secure distributed energy management of the port power system. Finally, the simulation results show the effectiveness of the proposed strategy, and the defense capability of the port power system is improved.

1. Introduction

With the development of the shipping industry [1], the types and quantities of energy equipment in port are increasing, and the port has become an energy-intensive region that relies on fossil energy; pollutant emissions are also increasing year by year [2]. In order to achieve effective pollution control, the interaction of multiple stakeholders in the maritime shore power system is required [3]. Port enterprises should speed up the realization of the strategy of "implementing shore power," and the government should actively supervise pollution emissions and encourage the use of clean energy [4]. Optimizing the utilization rate of renewable energy is the breakthrough point to solve the problem of high energy consumption and high emission in ports, but as the penetration rate of renewable energy becomes higher and higher, its randomness and volatility bring uncertainty to the port power system [5, 6]. More noteworthy, the Port of Barcelona was the target of a cyberattack that affected some of its servers and systems on the morning of September 20, 2018, forcing the organization to launch the contingency plan designed specifically for these incidents [7]. An Israeli cyber attack on the Iranian port setup caused serious chaos in the port's waterways and roads according to the Washington Post reported in May 2020 [8]. A study by Lloyd's of London showed that a cyberattack affecting major ports in the Asia-Pacific could cost $110 billion [9]. Therefore, how to carry out port energy management has become a key issue in order to make full use of the renewable energy of the port, reduce the environmental pollution caused by the redundant power supply, and ensure the normal run of the port power system.

At present, the energy management of port mainly draws on the experience and methods of the distribution grid, and it is actually an optimization problem of the complex system considering various practical constraints [10]. It aims to realize the balance of supply and demand and to maximize the operation benefit of the port power system when meeting the physical constraints of energy equipment [11, 12]. At the same time, the ports that implement wind power generation and photovoltaic power generation have the characteristics of distribution and uncertainty, which brings difficulties to the traditional centralized energy management strategy [13, 14]. Port energy management is gradually transformed into a distributed management method with the advantages of

flexibility, high reliability, and scalability [15–17]. A number of studies concerned about energy management have been proposed for power systems, including hierarchical decentralized energy management, multiagent system-based coordinated operation strategy, and hybrid energy management [18–20]. To solve the energy management problem of the energy Internet, the work in [18] proposed a completely distributed algorithm, in which each participant can realize the estimation of the optimal energy price and the calculation of the optimal energy output by only interacting with the neighbors. The large-scale connected inverter (CI) networks increase the reliability and resilience for the power grid, which may also cause grievous adventure to the reliable and stable operation of the main grid if the control of multiple CIs could not enable good cooperation [21, 22]. Lu et al. proposed a master-slave cluster cooperation strategy over the two-layer switching cyber network topologies to realize the economic distribution among multiple clusters [23]. There have been many studies on ports in different directions. The literature [24–26] reduces the peak load in the port by excavating the peak cutting and valley filling capacity of port freezers, terminal cranes, and electric vehicles. In reference [27], aiming at the problem that a large number of flexible loads such as reefers, ships, and electric vehicles are difficult to be highly coordinated, the port load management optimization is realized by using multiagent system with electricity price as the regulation signal. A novel decentralized power management method for a large port-based multiagent system (MAS) is proposed in [28].

It is specially mentioned that the information interaction process is vulnerable to malicious network attacks among the calculation and analysis of energy supply equipment due to the strong distributed characteristics of the current port power system [29]. In the next place, owing to the rapid development of information technology, there is a strong coupling characteristic between port cyber system and its power system [30, 31], which determines that the secure operation of information communication network is a basic foundation for the normal operation of its power system obviously [32]. Considering the increasing degree of dependence between information flow and power flow, the threat on information communication flow within the port power system will influence the normal operation of the power system, which will penetrate the boundary between the above two systems and have several negative impacts on disturbance, system instability, and collapse of the energy system [33, 34]. Thus, in order to ensure the reliable operation of the port power system under the above situations, it is necessary to strengthen the security defense of its information and communication system, so as to ensure the normal operation of its internal equipment [35–37]. It is noted that the operations security and efficiency of energy utilization are the most significant requirements within the port cyber-physical system [38]. Therefore, ports must make cyber security a top priority to ensure its security, compliance, and commercial competitiveness. The direct target of network attacks is the information flow in the information layer. It is common that cyberattacks include denial of service attacks, packet loss attacks, false data injection attacks (FDIAs), malicious software viruses, and so on [39]. Among them, the false data injection attack approach is easy to implement and has the characteristics of strong concealment and interference, which have attracted widespread attention from researchers in related fields. Literature [40] mainly treats the perturbation term in FDI attacks as a constant. In Literature [41], to verify the robustness of the proposed technique, four cases of FDI attacks across attacker injection signals were considered that are non-periodic attack, non-periodic replacement attack, periodic attack, and simultaneous attack. All of the above attack types will be within our consideration. In the next place, we need to focus on existing ways to resist attacks, a method for detecting FDIA in DC microgrid current measurement based on distributed control strategy control is introduced in [42]. The authors study fault identification using SVM, decision trees, and random forests in [43, 44]. The detection method of FDIA was studied in the above literature. The work in [45] proposes an antioffensive cooperative control strategy, which can adjust the power of the virtual power plant under a specific scheduling command. References [46, 47] proposed a trust-based antiattack resilient cooperative distributed control method and designed a resilient synchronization protocol to solve the problem of sensor attacks and reduce the adverse effects of attacks on communication links and hijacking of controllers. The author analyzed the relationship of the maximum amount of tolerable attacks and the number of total agents, and connected number has been provided for consensus under adversarial attacks, and a sequence of resilient consensus algorithms were developed in [48, 49].

However, the existing defense mechanisms rely mainly on the means of detecting attacks, and the effectiveness of those is still restricted by the maximum amount of tolerable attacks. To actively defend and relax the assumption on the maximum amount of tolerable attacks, this article was completed inspired by [50]. This paper proposes a distributed energy management strategy for the port power system based on hierarchical topology reconstruction of communication networks in order to reduce the impact of false data injection attacks on port energy management within limited defense resources to ensure the safe run of the system with lower security defense cost.

The main contributions of this paper are summarized as follows:

(1) This paper investigates the problem of distributed port energy management when the network of the port power system is under attack, where the tolerable number of attack nodes is unknown and can be arbitrarily large.

(2) To increase the security capacity of the port power system under false data injection attacks, this paper proposes a hierarchical topology reconstruction method of the port information system, which can reduce the impact of false data injection attacks on the port power system during the whole operation condition.

The rest of the paper is organized in the following. Section 2 presents the main types of port power facilities and energy management. The secure distributed energy management under FDIAs is detailed given in Section 3. In Section 4, the proposed method is simulated for port power system, and the obtained results are presented and evaluated. Finally, Section 5 draws a general conclusion.

2. Distributed Energy Management of Port Power System

2.1. Port Power System Configuration. In the port information energy system, there are multiple energy supply, energy demand, and energy storage entities [51]. In terms of energy supply, the port is particularly suitable for converting natural resources such as wind energy, tidal energy, and solar energy into electrical energy; in terms of energy use, the port uses a large number of cranes, gantry cranes, bridge cranes, plug-in electric vehicles, and so on [52]. In terms of energy storage, it is necessary to alleviate the uncertainty of port load and absorb intermittent and fluctuating renewable energy; energy storage equipment needs to be considered in the port power system.

2.1.1. Renewable Generator. Solar and wind energy are the main renewable energy sources. Considering the intermittency and volatility of renewable energy, it is unable to participate in the energy management process of the port, so according to the dispatch forecast curve before the day, the average value is used as a reference. Taking renewable power generation equipment as an example, its power generation can be expressed as follows:

$$\widetilde{P}_i = \frac{\int_t^{t+T} P_i dt}{T}, \tag{1}$$

where $\widetilde{p}_i$ is the power generation predicted by the renewable energy equipment i according to the day-ahead dispatch period T. Assuming that the prediction error described by the probability density function obeys the Gaussian distribution, it can be expressed as follows:

$$f_i(\Delta P_i) = \frac{1}{\sqrt{2\pi}\delta_i} e^{-\left(\Delta P_i/2\delta_i\right)^2}. \tag{2}$$

Choose an appropriate confidence level to get the confidence interval of the prediction error $[\Delta P_i^{\min}, \Delta P_i^{\max}]$. Thus, the power generation of renewable energy equipment i can be expressed as follows:

$$\begin{aligned} &\underline{P}_i \le P_i \le \overline{P}_i, \\ &P_i = \widetilde{P}_i + \Delta P_i. \end{aligned} \tag{3}$$

To sum up, considering the actual operation effect, the operation cost function of renewable energy equipment i can be expressed as follows:

$$C_i(P_i) = a_i {P_i}^2 + b_i P_i + c_i, \tag{4}$$

where b_i and c_i are the coefficients of the operating cost function; the optimality and possibility of renewable energy equipment operation can be balanced to take renewable energy into energy management.

2.1.2. Fuel Generator. The use of alternative clean energy in port equipment and buildings can effectively reduce environmental pollution and greenhouse gas emissions in the port area, which is in line with the development concept of green port [48]. The choice of alternative clean energy fuels plays an important role in the sustainable development of ports and the improvement of the port environment. The local optimization problem of fuel energy equipment can be transformed into

$$\min C_i(P_i) = a_i(P_i)^2 + b_i P_i + c_i + \tau_i \exp(\eta_i P_i), \tag{5}$$

$$P_i^{\min} \le P_i \le P_i^{\max}, \tag{6}$$

$$-P_i^{\text{ramp}} \le P_i(k) - P_i(k-1) \le P_i^{\text{ramp}}. \tag{7}$$

2.1.3. Shore-Ship Power Supply. In order to effectively promote the development of energy-saving and low-carbon emission reduction, the use of shore-based power supply by ships calling at ports is one of the key tasks of the port industry for energy conservation and emission reduction. When the ship is at the berth, the ship's auxiliary generator runs in parallel with the shore power source to ensure the ship's reliable operation. The operating cost of the auxiliary engine (only fuel is considered) is approximated by the second-order polynomial of the power generated by the generator [28]:

$$U_i(P_i) = a_i(P_i)^2 + b_i P_i + c_i. \tag{8}$$

2.1.4. Plugged in Electric Vehicle. Electronic transportation in the port improves energy efficiency and reduces greenhouse gas emissions. The use of electric vehicles instead of port internal combustion engine operating vehicles (such as automobiles, forklifts, etc.) will effectively reduce carbon emissions in the port. In the future, large ports can charge and discharge electric vehicles through charging piles, thereby increasing the flexibility of providing port energy requirements. The cost function of PEV can be modeled as follows [27]:

$$\max U_i(P_i) = -a_i(P_i + b_i)^2. \tag{9}$$

Electric vehicles are constrained by battery charging efficiency and battery capacity as follows:

$$E_r(k) - E_r(k-1) = \begin{cases} \varsigma^{ch} P_i T \\ \dfrac{1}{\varsigma^{\text{ds}}} P_i T \end{cases}. \tag{10}$$

2.1.5. Distributed Power Storage Device. Distributed renewable energy generation has the characteristics of intermittent and volatility. Large-scale access to distributed power generation equipment increases the adjustment difficulty of the grid and is likely to cause a lot of waste of resources such as abandoning light and wind; When a large number of short-cycle loads are connected, it will cause large fluctuations in the frequency or voltage of the grid, which will affect the stability of other electrical equipment. The addition of energy storage system in the power grid will not only help to reduce the abandonment of new energy and make up for the instability of new energy power generation but also reduce the demand pressure at the peak of power consumption by releasing the stored energy. On the energy-consuming side, it meets the rapid response requirements of frequency and voltage regulation and provides high-quality electric energy. The cost of energy storage equipment i can be defined as follows:

$$C_i(P_i) = a_i(P_i + b_i)^2, \tag{11}$$

where p_i represents the charge and discharge power of the energy storage device i, and its symbol represents the state of charge and discharge (the discharge state is positive, and the charge state is negative). Energy storage equipment cannot work in charging and discharging at the same time and needs to meet multiple restricted operating conditions:

$$-P_i^{ch,\max} \le P_i \le P_i^{\mathrm{ds},\max}, \tag{12}$$

$$SoC(k) - SoC(k-1) = \begin{cases} \varsigma^{ch} P_i T, & p_i \le 0 \\ \dfrac{1}{\varsigma^{\mathrm{ds}}} P_i T, & p_i > 0 \end{cases}, \tag{13}$$

where P_i should be between the maximum charging power $P_i^{ch,\max}$ and the maximum discharging power $P_i^{\mathrm{ds},\max}$, ς^{ch} and ς^{ds} are positive numbers between 0 and 1, and represents the energy loss during the charging and discharging process of the energy storage device i.

3. Distributed Energy Management Scheme of Port Power System

The goal of energy management of the port power system is to maximize the operation benefit or minimize the operation cost on the basis of ensuring the safe operation of port power equipment and the balance of supply and demand of the port power system.

We assume that the port power system can be represented by an undirected graph $G = (V, E, A)$, where $V = \{v_1, v_2, \ldots, v_n\}$ is a vertex set, $E \subseteq V \times V$ is the set of undirected edges, and A is weighted and non-negative adjacency matrix [50]. It assumed that there are n power devices in the port power system, whose cost function of device i can be denoted by $C_i(P_i)$, where P_i is the output power of device i. The energy management problem can be expressed as follows:

$$\max \sum_{i=1}^{n} -C_i(P_i), \tag{14}$$

subject to the following constraints:

(a) Device constrains

$$p_i^{\min} \le p_i \le p_i^{\max}, \tag{15}$$

$$P_4^* = 40.0000\,\mathrm{MW}, \tag{16}$$

where $P_i^{\min}, P_i^{\max}$ are the minimum and maximum power output of the device i, respectively, and P_i^{ramp} is the ramp rate constraint of the power facility.

(b) Supply-demand balance constraints

$$\sum_{i=1}^{n} P_i = \sum_{i=1}^{n} d_i, \tag{17}$$

where d_i is load. It is assumed that the energy management problem is solvable; the following conditions are satisfied:

$$\sum_{i=1}^{n} P_i^{\min} \le \sum_{i=1}^{n} d_i \le \sum_{i=1}^{n} P_i^{\max}. \tag{18}$$

Assumption 1. For each $i \in \{1, 2, \ldots, N\}$, the cost function $C_i(P_i)$: $R_+ \longrightarrow R_+$ is strictly convex and continuously differentiable, where R_+ denotes the set of non-negative real numbers.

The Lagrangian function of problem (14) and constraints (15) is as follows:

$$\begin{aligned} L(P, \lambda) &= \sum_{i=1}^{n} \left(-C_i(P_i)\right) - \lambda \left(\sum_{i=1}^{n} d_i - \sum_{i=1}^{n} P_i \right) \\ &= \sum_{i=1}^{n} \left(-C_i(P_i) + \lambda P_i\right) - \lambda \sum_{i=1}^{n} d_i, \end{aligned} \tag{19}$$

where λ is the dual variable. By decoupling P_i from $L(P, \lambda)$, we get

$$P_i^* = \arg\max \left(-C_i(P_i) + \lambda P_i\right). \tag{20}$$

Assumption 2. The Lagrangian function $L(P, \lambda)$ has a saddle point, that is, there exists an optimal solution (P^*, λ^*) such that

$$L(P^*, \lambda) \le L(P^*, \lambda) \le L(P^*, \lambda). \tag{21}$$

holds for all $P_i \in \Omega$, $\lambda \in R_+$.

With Assumption 2, problem (14) is a convex optimization problem, and the duality gap is 0; it can be transformed into its dual problem, which can be expressed as follows:

$$\min D(\lambda) = \min L(P^*, \lambda), \\ = \min\left(\sum_{i=1}^{n}\left(-C_i(P_i^*) + \lambda P_i^*\right) - \lambda\sum_{i=1}^{n} d_i\right). \tag{22}$$

Using the gradient descent method to solve, the update of $\lambda(k)$ can be described as follows:

$$\lambda(k+1) = \lambda(k) - \alpha\frac{\partial D}{\partial \lambda}(\lambda(k)), \tag{23}$$

where $\alpha > 0$ is a constant that represents the step size. The energy management based on the gradient descent method can be expressed as follows:

$$P_i(k) = \max\left\{P_i^{\min}, \min\left\{\arg\max\left(-C_i(P_i) + \lambda(k)P_i\right), P_i^{\max}\right\}\right\}, \tag{24}$$

$$\lambda(k+1) = \lambda(k) - \alpha\left(\sum_{i=1}^{n} P_i(k) - \sum_{i=1}^{n} d_i\right). \tag{25}$$

It is worth noting that the above energy management method is centralized and $\lambda(k)$ is a global variable, which requires the centralized control center to collect the information of all devices in the system and greatly increases the computing burden and communication burden of the control center. In this case, once the control center fails, the energy management process of the port power system will collapse, and the safe operation of the system will be seriously threatened. In [54], a distributed estimator $\lambda_i(k)$ is introduced to evaluate global variables $\lambda(k)$, and a distributed energy management algorithm is designed through a finite number of consensus protocol calculations, which alleviates the communication burden and computing burden of the scheduling center (Algorithm 1).

Here, $w_{ij} > 0$ is the weight assigned by node i to node j.

Assumption 3. The existence of a double random matrix $W = [w_{ij}]_{n\times n}$ which satisfies $W = W^T$ and for $(v_i, v_i) \notin E \cup (v_i, v_i)$, $w_{ij} \neq 0$.

Lemma 1. *Under the above assumptions, the iteration number of consensus updates meets* $\sigma \geq (\log\beta - \log(4n(\beta + \alpha l))/\log\gamma$, *and the initial value* $\lambda_i(0)$ *satisfies* $|\lambda_i(0) - \overline{\lambda}(0)| \leq \beta$; *sequence* $\{\lambda_i(k)\}$ *can be achieved consensus; and* $\{P(k)\}$ *can arbitrarily approach the optimal solution* P^*.

Remark 1. The above algorithm does not need centralized scheduling and decentralize the computation burden of the scheduling center. Each node only needs to exchange information with its neighbors to alleviate the communication burden of the central nodes. In this case, distributed scheduling method assumes that the network environment is benign, and if there are intruders in the information network, it is very likely that the consensus between nodes cannot be achieved.

4. Distributed Energy Management under FDIAs

With the deep fusion of information flow and energy flow in the port power system, the safe operation of the port power system is facing many challenges. More and more energy devices with communication abilities are connected to the port power system, and the information transmitted by energy equipment is threatened by network attacks [55].

4.1. Energy Management Problem under FDIAs. Considering the features of concealment and interference, false data injection attacks (FDIAs) have been regarded as one of the most popular attacks of the communication system in the port power system [56]. Furthermore, the attacker can track the configuration of the port power system, tamper with the sensing data of the sensor or tamper with the command signal sent by the controller, which will lead to the error of the state estimation process, and finally make the power system unable to operate normally [57]. As mentioned above, the false data injection attack model is as follows:

$$\lambda_i(k+1) = \zeta_i(\lambda_i(k)), \tag{26}$$

where $\lambda_i(k)$ denotes the information of device i exchanged with other devices and $\zeta_i(\lambda_i(k))$ represents arbitrary update function.

Without losing generality, we assume that node $i = 1, 2, \ldots, n_0$ is not attacked by false data injection attacks and node $i = n_0 + 1, n_0 + 2, \ldots n$ is attacked by false data injection attacks. The interaction of $\lambda_i(k)$ in information layer can be rewritten as follows:

Initialization: Each node i initializes $\lambda_i(0)$, step size α and calculation times σ
Iteration: $(k \geq 0)$
(1) Each node i updates $P_i(k)$ according to (24)
(2) Each node i updates $v_i^0(k+1)$ based on the gradient descent method, $v_i^0(k+1) = \lambda_i(k) - \alpha(P_i(k) - d_i)$
(3) Each node i interacts with its neighbors, until reached consensus. $v_i^1(k+1) = \sum_{v_j^0 \in S_i} w_{ij} v_j^0(k)$, $v_i^2(k) = \sum_{v_j^1 \in S_i} w_{ij} v_j^1(k)$, $v_i^\sigma(k) = \sum_{v_i^{\sigma-1} \in S_i} w_{ij} v_i^{\sigma-1}(k)$
(4) Each node i estimates $\lambda_i(k+1)$. $\lambda_i(k+1) = v_i^\sigma(k)$
Let $k = k+1$, turn to 1.

Algorithm 1: Distributed energy management scheme.

$$\begin{bmatrix} \lambda_1(k+1) \\ \lambda_2(k+1) \\ \vdots \\ \lambda_{n_0}(k+1) \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n_0} & w_{1(n_0+1)} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n_0} & w_{2(n_0+1)} & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ w_{n_01} & w_{n_02} & \cdots & w_{n_0n_0} & w_{n_0(n_0+1)} & \cdots & w_{n_0n} \end{bmatrix} \begin{bmatrix} v_1^{\sigma-1}(k) \\ v_2^{\sigma-1}(k) \\ \vdots \\ v_{n_0}^{\sigma-1}(k) \\ v_{n_0+1}^{\sigma-1}(k) \\ \vdots \\ v_n^{\sigma-1}(k) \end{bmatrix}, \tag{27a}$$

$$\begin{bmatrix} \lambda_{n_0+1}(k+1) \\ \vdots \\ \lambda_n(k+1) \end{bmatrix} = \begin{bmatrix} \zeta_{n_0+1}\left(v_{n_0+1}^{\sigma-1}(k)\right) \\ \vdots \\ \zeta_n\left(v_n^{\sigma-1}(k)\right) \end{bmatrix}. \tag{27b}$$

The goal of energy management of the port power system under FDIAs is to maximize the operation benefit of non-attacked devices. The energy management problem can be expressed as follows:

$$\max \sum_{i=1}^{n_0} -C_i(P_i), \tag{28}$$

subject to the following constraints:

(a) Device constrains

$$p_i^{\min} \leq p_i \leq p_i^{\max}, \tag{29}$$

$$-P_i^{\text{ramp}} \leq P_i(k) - P_i(k-1) \leq P_i^{\text{ramp}}, \tag{30}$$

where $P_i^{\min}, P_i^{\max}$ are the minimum and maximum power output of the device i, respectively, and P_i^{ramp} is the ramp rate constraint of the power facility.

(b) Supply-demand imbalance constraints

$$\left| \sum_{i=1}^{n_0} P_i - \sum_{i=1}^{n_0} d_i \right| \leq P_{\text{thres}}^{\text{im}}, \tag{31}$$

where $P_{\text{thres}}^{\text{im}}$ is the constant threshold of power mismatch under false data injection attacks.

4.2. Secure Distributed Energy Management Based on Topology Reconfiguration. The topology of the information

network is the key factor to realize the coordinated operation of port power devices and energy management of port power systems [53]. It is noted that the reliable transmission of information is a necessary condition to ensure the safe, stable, and economic operation of the port energy system. Information networks can provide different services and guarantees for energy equipment in different regions. In order to build a safe information network environment, we consider changing the port information network from a flat topology to a hierarchical topology. The hierarchical topology is as Figure 1.

Hierarchical topology divides n nodes into m layers and marks the layers as 1 to m from top to bottom. The nodes in the first layer only send information to the second layer, and the nodes in the i layer at least send messages to one node in the $i+1$ layer. In each layer, the information interaction between nodes can be bidirectional. Using hierarchical topology, it is realized that when false data injection attacks occur in the port information network, we should divide the attacked node and the non-attacked node into different topology layers and reduce the weight of the non-attacked node assigned to the attacked node, so as to reduce the impact of network attacks on the port information network.

Inspired by the literature [50], we protect some nodes in the port power system from being invaded by attack nodes. By expanding the influence of these protected nodes in the network, to suppress the impact of false data injection attacks on the port information and energy system, the protection measures include: (1) improving the firewall security level of the protected nodes, and make redundant resources of the protected nodes to ensure that the protected nodes get real and reliable information; (2) Using the digital signature and data encryption technology, to the protected nodes the real information sent cannot be tampered. Before introducing a secure distributed energy management strategy, we introduce the following definitions and assumptions.

For the convenience of description, we regard the vertex set $T = \{v_i | i = 1, 2, \ldots n_1\}$ as the set of protected nodes, and the vertex set $A = \{v_i | i = n_0 + 1, \quad n_0 + 2, \ldots, n\}$ as the set of attacked nodes. The other vertex is ordinary nodes.

Remark 2. Topology reconstruction from communication network due to attack does not mean that the operation of the attacked node stops completely. The isolated node does not mean that its corresponding unit stops power output. It will continue to supply local load demand because the attack action of an isolated node only occurs at the communication layer. The physical layer topology of the actual power supply unit will not change due to the occurrence of a network attack.

The Lagrangian function of problem (28) and constraints (31) is as follows:

$$\begin{aligned} L(P, \widetilde{\lambda}) &= \sum_{i=1}^{n_0} \left(-C_i(P_i)\right) - \widetilde{\lambda}\left(\sum_{i=1}^{n_0} d_i - \sum_{i=1}^{n_0} P_i - P_{\text{thres}}^{\text{im}}\right), \\ &= \sum_{i=1}^{n_0} \left(-C_i(P_i) + \widetilde{\lambda} P_i\right) - \widetilde{\lambda}\left(\sum_{i=1}^{n_0} d_i - P_{\text{thres}}^{\text{im}}\right), \end{aligned} \tag{32}$$

where $\widetilde{\lambda}$ is the dual variable. By decoupling P_i from $L(P, \widetilde{\lambda})$, we get:

$$P_i^* = \arg\max\left(-C_i(P_i) + \widetilde{\lambda} P_i\right). \tag{33}$$

Remark 3. The above Lagrange function assumes that the supply is in short demand in the port power system. It can also assume that the supply exceeds the demand in the port power system. Owing to the port power system containing energy storage equipment, it can provide or store electric energy in time to reduce the negative pressure of power imbalance in case of emergency.

Assumption 4. The Lagrangian function $L(P, \widetilde{\lambda})$ has a saddle point, that is, there exists an optimal solution $(\widetilde{P}^*, \widetilde{\lambda}^*)$ such that

$$L\left(P, \widetilde{\lambda}^*\right) \le L\left(\widetilde{P}^*, \widetilde{\lambda}^*\right) \le L\left(P^*, \widetilde{\lambda}\right), \tag{34}$$

holds for all $P_i \in \Omega$, $\widetilde{\lambda} \in R_+$.

With Assumption 4, problem (14) is a convex optimization problem, and the duality gap is 0; it can be transformed into its dual problem, which can be expressed as follows:

$$\begin{aligned} \min D(\widetilde{\lambda}) &= \min L\left(P^*, \widetilde{\lambda}\right) \\ &= \min\left(\sum_{i=1}^{n_0}\left(-C_i(P_i^*) + \widetilde{\lambda} P_i^*\right) - \widetilde{\lambda}\left(\sum_{i=1}^{n_0} d_i - P_{\text{thres}}^{\text{im}}\right)\right) \\ &= \min \sum_{i=1}^{n_0} g_i(\widetilde{\lambda}). \end{aligned} \tag{35}$$

Before introducing a secure distributed energy management strategy, we introduce the following definitions and assumptions.

Definition 1. G_d is a connected dominating set of $G = (V, E, A)$ if each node i, which does not belong to the subset G_d, has at least one neighbor in the subset G_d and all nodes in G_d can form a connected graph.

Assumption 5. The protected nodes induce a connected dominating set of $G = (V, E, A)$.

Thus, a secure distributed energy management strategy based on topology reconfiguration is as follows (Algorithm 2,):

$\{\alpha(0), \ldots, \alpha(\infty)\}$ is the sequence of step sizes, which meets $\sum_{k=0}^{\infty} \alpha(k) = \infty$, $\sum_{k=0}^{\infty} \alpha^2(k) < \infty$, and $\alpha(k+1) \le \alpha(k)$.

The convergence of secure distributed energy management schemes under FDIAs topology reconstruction algorithm is given below.

According to the secure distributed energy management scheme under FDIAs, each node i determines the maximum threshold $\chi_i^M(k)$ and minimum threshold $\chi_i^m(k)$. And then, the set $R_i(k)$ can be obtained by threshold filtering. During the k iteration of node i, $R_i(k)$ can be divided into three

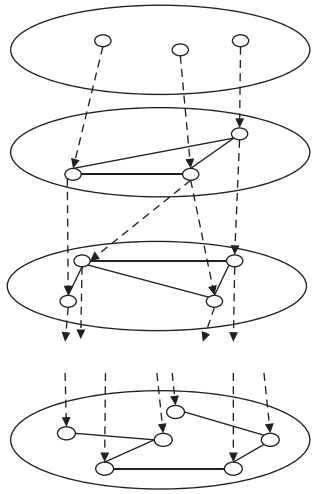

Figure 1: Hierarchical topology of information network.

Initialization: Each node i initializes $\lambda_i(0)$
Iteration: $(k \geq 0)$
(1) Each node i updates $P_i(k)$ according to (24)
(2) Each node i updates $\chi_i(k)$ based on the gradient descent method, $\chi_i(k) = \widetilde{\lambda}_i(k) - \alpha(k)(P_i(k) - d_i)$
(3) Each node i receives information, formulates the set $S_i(k) = \{\chi_i(k) | i \in N_i\}$
(4) Node i identifies the information of the protected node, compares with its own information, and then determines the maximum threshold $\chi_i^M(k)$ and minimum threshold $\chi_i^m(k)$
(5) Node i filters information between $\chi_i^m(k)$ and $\chi_i^M(k)$ and then formulates the set $R_i(k) = \left\{\chi_j(k) | \chi_i^m(k) \leq \chi_j(k) \leq \chi_i^M(k), \quad j \in N_i\right\}$
(6) Each node i updates $\chi_i(k+1)$, $m_{ij}(k) = 1/|R_i(k)|, \chi_j(k) \in R_i(k), \chi_i(k+1) = \sum_{\chi_j \in R_i(k)} m_{ij}(k)\chi_j(k)$
(7) Each node i estimates $\widetilde{\lambda}_i(k+1)$ and $\widetilde{\lambda}_i(k+1) = \chi_i(k+1)$
Let $k = k+1$, until $|\lambda_i(k) - \lambda_j(k)| < \varepsilon, \ j = 1, 2, \ldots, n_1$

Algorithm 2: Secure distributed energy management scheme under FDIAs.

types: from the set of protected nodes $R_i^T(k)$, itself $\chi_i(k)$, and the set of the other nodes $R_i^{\overline{T}}(k)$. Equation in Algorithm 2, can be rewritten as follows

$$\begin{aligned} \widetilde{\lambda}_i(k+1) &= \frac{1}{\left|R_i(k)\right|} \sum_{\chi_j(k) \in R_i(k)} \chi_j(k) \\ &= \frac{1}{\left|R_i(k)\right|} \left(\sum_{\chi_j(k) \in R_i^T(k)} \chi_j(k) + \chi_i(k) + \sum_{\chi_j(k) \in R_i^{\overline{T}}(k)} \chi_j(k) \right), \end{aligned} \tag{36}$$

where $\forall \chi_j(k) \in R_i^{\overline{T}}(k)$; it can be expressed as $\chi_j(k) = \rho_j \chi_i^m(k) + (1 - \rho_j)\chi_i^M(k), \quad 0 < \rho_j < 1$. Thus, equation in Algorithm 2, can be further rewritten as follows:

$$\begin{aligned}\widetilde{\lambda}_i(k+1) &= \frac{1}{\left|R_i(k)\right|}\left(\sum_{\chi_j(k)\in R_i^T(k)}\chi_j(k)+\chi_i(k)+\sum_{\chi_j(k)\in R_i^{\overline{T}}(k)}\chi_j(k)\right)\\ &= \frac{1}{\left|R_i(k)\right|}\left(\sum_{\chi_j(k)\in R_i^T(k)}\chi_j(k)+\sum_{\chi_j(k)\in R_i^{\overline{T}}(k)}\left(\rho_j\chi_i^m(k)+\left(1-\rho_j\right)\chi_i^M(k)\right)\right)\\ &= \sum_{\chi_j(k)\in R_i^T(k)\cup\chi_i(k)} m_{ij}\chi_j(k).\end{aligned} \tag{37}$$

Then, we have

$$\begin{bmatrix}\widetilde{\lambda}_1(k+1)\\ \vdots\\ \widetilde{\lambda}_{n_1}(k+1)\\ \vdots\\ \widetilde{\lambda}_{n_0}(k+1)\end{bmatrix}=\begin{bmatrix}m_{11} & \cdots & m_{1n_1} & \cdots & 0\\ \vdots & \ddots & \vdots & \cdots & \vdots\\ m_{n_11} & \cdots & m_{n_1n_1} & \cdots & 0\\ \vdots & \cdots & \vdots & \ddots & \vdots\\ m_{n_01} & \cdots & m_{n_0n_1} & \cdots & m_{n_0n_0}\end{bmatrix}\begin{bmatrix}\chi_1(k)\\ \vdots\\ \chi_{n_1}(k)\\ \vdots\\ \chi_{n_0}(k)\end{bmatrix}. \tag{38}$$

Compared with (27a), after topology reconstruction, the links from ordinary nodes to protected nodes and the links from attacked nodes to protected nodes are weakened, and the connection between attacking node and common node is also weakened. Equation (38) can be expressed as:

$$M(k)=\begin{bmatrix}M_{n_1\times n_1} & 0\\ M_{n_2\times n_1} & M_{n_2\times n_2}\end{bmatrix}_{n_0\times n_0}, \tag{39}$$

where $M_{n_1\times n_1}$ is the interaction between protected nodes, $M_{n_2\times n_1}$ denotes the interaction between protected node and ordinary nodes, and $M_{n_2\times n_2}$ is the interaction of itself. The nodes of the communication network can be divided into three layers by hierarchical topology reconstruction algorithm: layer 1 of trusted nodes, layer 2 of common nodes, and layer 3 containing attack nodes.

Furthermore, equation (38) can be written as follows:

$$\begin{aligned}\widetilde{\lambda}(k+1) &= M(k)\chi_i(k),\\ &= M(k)\left(\widetilde{\lambda}(k)-\alpha(k)\frac{\partial g}{\partial\widetilde{\lambda}}(\widetilde{\lambda}(k))\right),\\ &= M(k)\cdots M(0)\widetilde{\lambda}(0)-\sum_{t=0}^{k}M(k)\\ &\quad\cdots M(t+1)\alpha(t)\frac{\partial g}{\partial\widetilde{\lambda}}(\widetilde{\lambda}(t)),\\ &= \Psi(k,0)\widetilde{\lambda}(0)-\sum_{t=1}^{k+1}\Psi(k,t)\alpha(t-1)\frac{\partial g}{\partial\widetilde{\lambda}}(\widetilde{\lambda}(t-1)).\end{aligned} \tag{40}$$

Under Assumption 5 and Algorithm 2, $\Psi(k,t)$ have the following property: for any fixed t, n_2 non-zero entries in ψ(t) are lower bounded by φ^d.

To estimate $\widetilde{\lambda}(k)$, define the set as follows:

$$C(\mu,\eta)=\left\{h(\lambda)\middle|h(\lambda)=\sum_{i=1}^{n_1}\gamma_i g_i(\lambda),\sum_{i=1}^{n_1}\gamma_i=1,\sum_{i=1}^{n_1}I\{\gamma_i\geq\mu\}=\eta\right\}, \tag{41}$$

and define the solution set as follows:

$$Y(\mu,\eta)=\cup_{h(\lambda)\in C(\mu,\eta)}\arg\min_{\lambda}h(\lambda). \tag{42}$$

By choosing $\mu=\varphi^d$ and $\eta=n_1$, it is easy to obtain $Y(\mu,\eta)$ is a convex set. According to reference [38], when $\alpha(k)$ meets $\lim_{k\longrightarrow\infty}\alpha(k)=0$, the $\lambda_i(k)$ of all protected nodes and ordinary nodes is convergent from (40), and converges to the set $Y(\mu,\eta)$ of optimal solutions of a weighted average of local cost functions $g_i(\widetilde{\lambda})$ belonging to all protected nodes and ordinary nodes.

Remark 4. Compared with literature [50], this paper focuses on secure energy management under FDIAs, which is a constrained optimization problem with coupling characteristics. By decoupling P_j from $L(P,\widetilde{\lambda})$, the dual problem is simplified, which make $\widetilde{\lambda}$ can achieve consensus.

5. Numerical Results

Consider port power system shown in Figure 2 and network topology under FDIAs shown in Figure 3; there are eight nodes in the port information network; the set of attacked nodes is $\{v_6,v_7,v_8\}$. The FDIA models are formed as

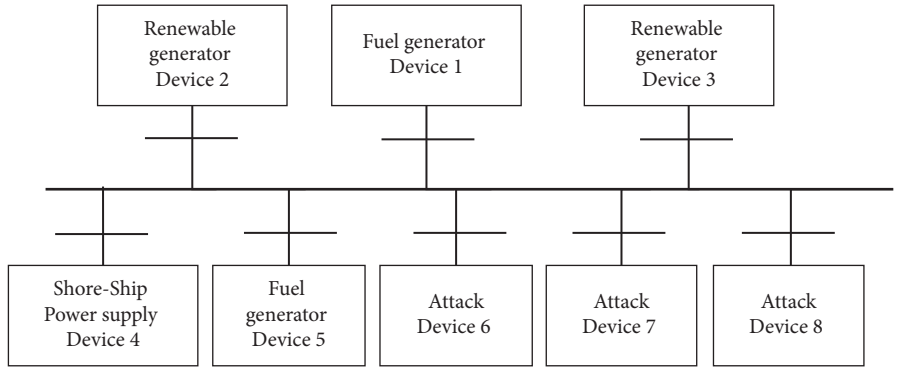

Figure 2: Port power system configuration.

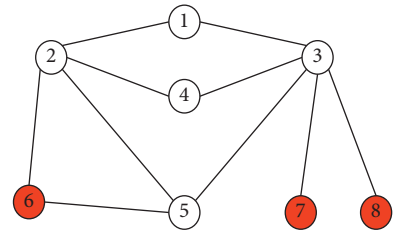

Figure 3: Network topology under FDIAs.

Table 1: The parameters of port power devices.

	Device 1	Device 2	Device 3	Device 4	Device 5
$a_i\,(\$/MW^2)$	0.040	0.032	0.023	0.054	0.040
$b_i\,(\$/MW)$	25	32	28	27	25
$c_i\,(\$)$	99	150	110	50	99

$\lambda_6(k+1) = 8\sin(0 \cdot 0025\pi\lambda_2(k+1)) + 35$, $\lambda_7(k+1) = (k/100)^2$, and $\lambda_8(k+1) = 40$.

We set cost function $C_i(P_i) = a_i{P_i}^2 + b_iP_i + c_i$ of devices i, with different parameters shown in Table 1. The loads are set as 85 MW, 50 MW, 105 MW, 85 MW, 77 MW, 30 MW, 33 MW, and 40 MW. According to Algorithm 1, set the initial value of the dual variable be 0, and the number of calculations is 40.

Figure 4(a) shows that when the nodes in the information network are attacked, the existing distributed energy management cannot guarantee the asymptotic consistency of the dual variable, and it leads to the outputs of power equipment fluctuating significantly, and the safe operation of the equipment is not realized as shown in Figure 4(b). As a result, the power mismatch of distributed energy management strategy cannot converge, and the imbalance constraint between supply and demand cannot be satisfied shown in Figure 4(c). It can be seen that the distributed energy management strategy loses effectiveness under FDIAs.

There are a total of eight nodes in the network of the information energy system: $\{v_1, v_2, v_3\}$ are protected nodes, $\{v_4, v_5\}$ are ordinary nodes, and $\{v_6, v_7, v_8\}$ are the nodes that are attacked. The network after topology reconstruction is shown in Figure 5, which divided nodes into two layers: the protected nodes are in the first layer and the other nodes are in the second layer. The information transfer from the first layer to the second layer in the topology is directed.

In the case of a network attack, the dual variables of nodes 1–5 are asymptotically consistent by topology reconstruction shown in Figure 6(a). Furthermore, Figure 6(b) shows that the output of all energy equipment tends to be safe run with small fluctuations, indicating that the energy strategy after topology reconstruction basically guarantees the safe run of the system. The energy management solution is given by $P_1^* = 73.8660$ MW, $P_2^* = 40.0000$ MW, $P_3^* = 62.9363$ MW, $P_4^* = 40.0000$ MW, and $P_5^* = 73.8660$ MW.

Power mismatches for secure distributed energy management fluctuate around −20 as shown in Figure 6(c), which greatly reduces the degree of energy mismatch compared with before the topology reconstruction. Although the energy mismatch still fluctuates to a small extent due to the direct transmission of information between nodes of the layered network after topology reconstruction, it is acceptable because it is safer than before topology reconstruction. In summary, the distributed optimization scheduling strategy has been topologically restructured to increase the robustness of the network and strengthen the active defense capability of the network.

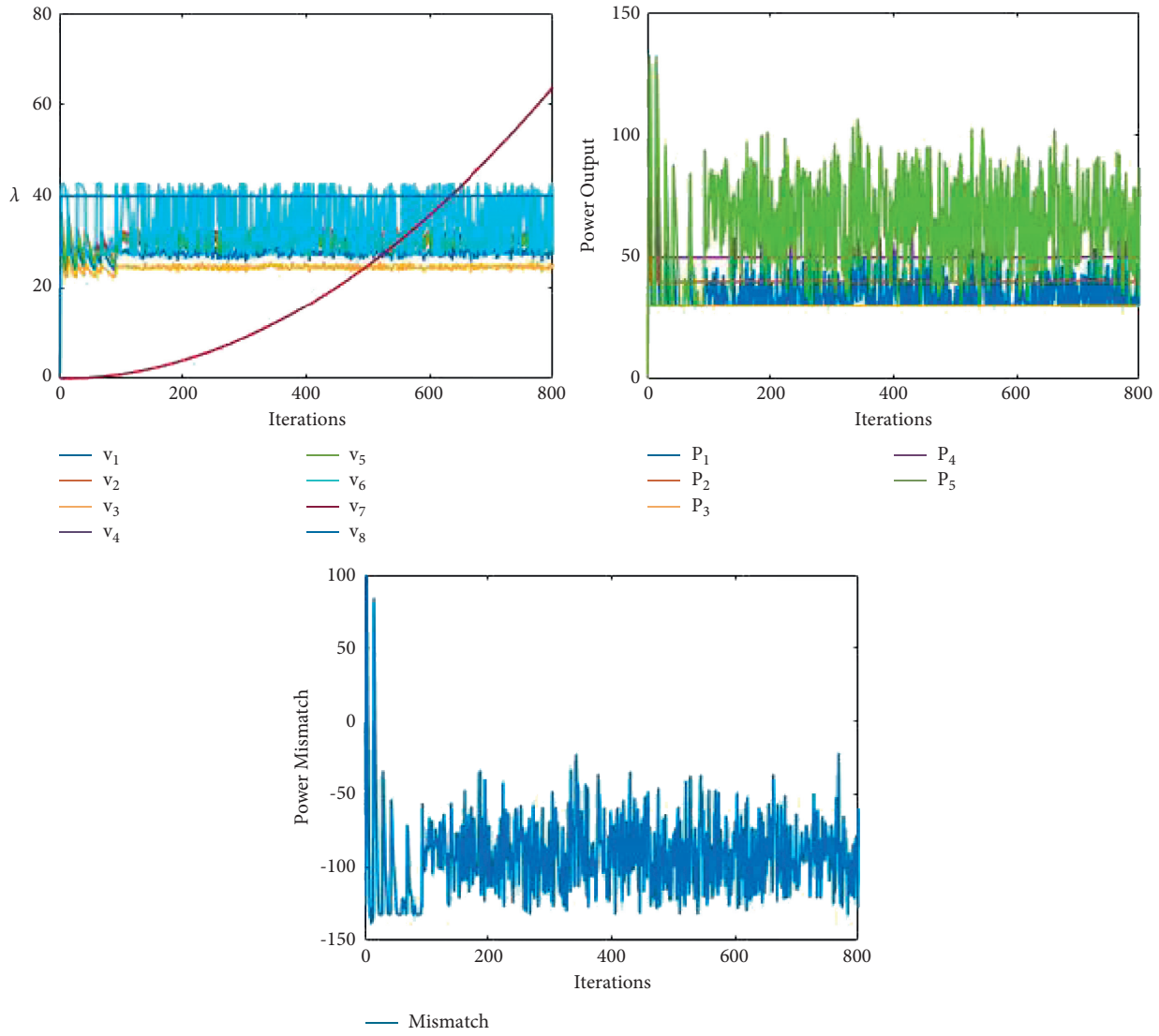

Figure 4: Variables of distributed energy management under FDIAs: (a) dual variables, (b) power output, and (c) power mismatch.

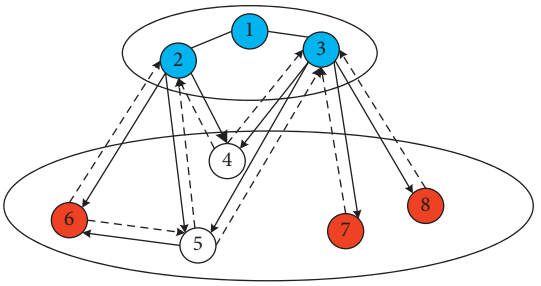

Figure 5: Reconfigurable network topology under FDIAs.

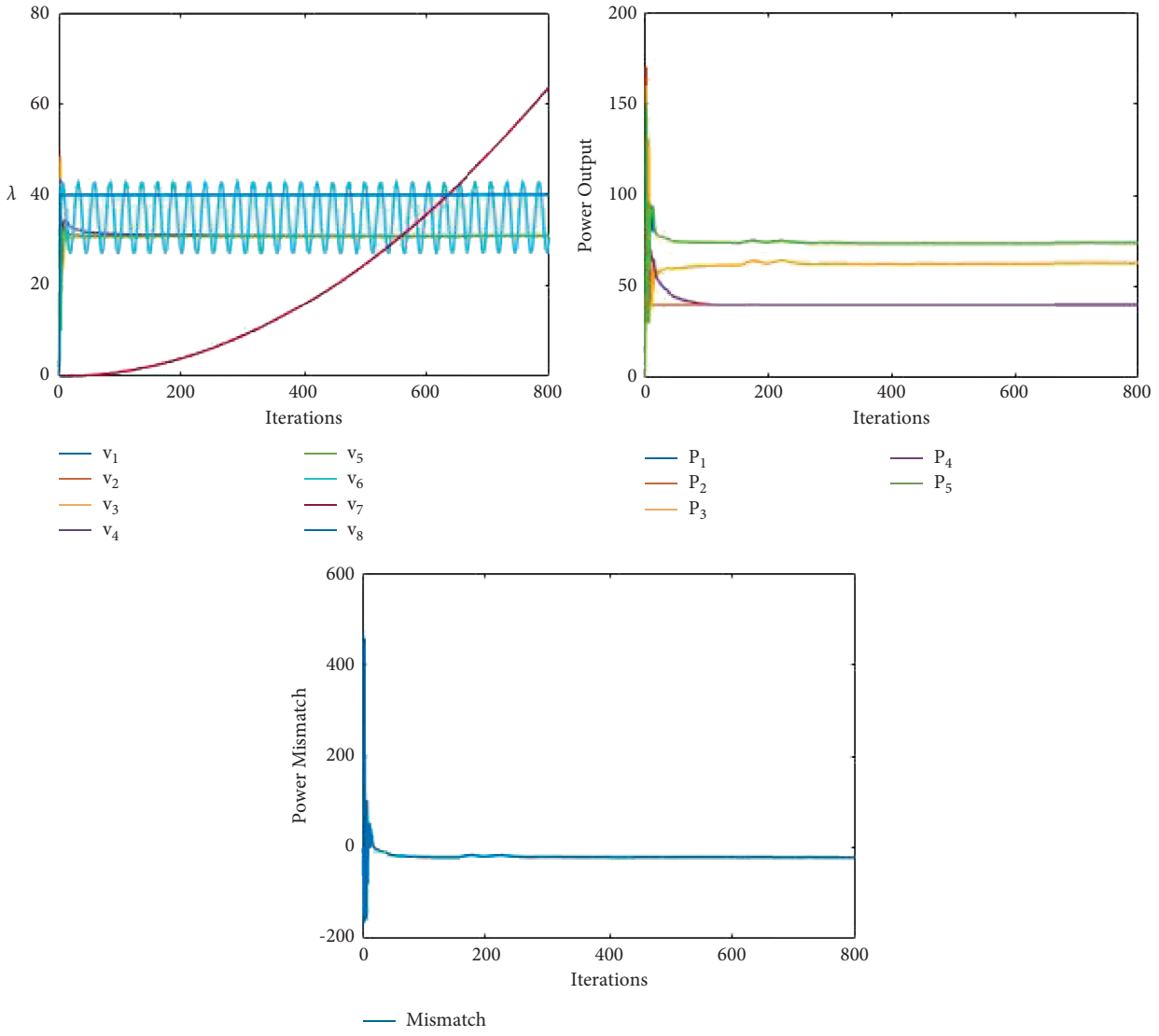

Figure 6: Variables of secure distributed energy management under FDIAs: (a) dual variables, (b) power output, and (c) power mismatch.

6. Conclusions

In this paper, a distributed energy management strategy for the port power system has been proposed under false data injection attacks. First of all, we proposed a hierarchical topology to allocate the security resources of the port power system. Then, by reconstructing the topological structure of the port information network, the robustness of the information network is improved; the impact of false data injection attacks on the port power system is reduced; and thus, the secure distributed energy management of the port energy system is realized. We have relaxed the assumption of the maximum tolerable number of attack nodes (F) while increasing the maximum number of tolerable attack nodes in the network. By protecting a portion of the nodes in the network, the normal operation of all the attacked nodes is ensured. Finally, the effectiveness of the proposed energy management was investigated by simulation results, and the defense capability of the port power system has been improved. It is important to note that our study still has some limitations. The method of topological reconstruction using the threshold changes the interactions between agents; although it is safer after topological reconstruction, there are still small fluctuations leading to energy mismatch, and it is acceptable. So the topological reconstruction algorithm still needs to be improved; This paper only studies the FDIA attacks; more types of attacks and attacks with a wider range can be considered in future work.

Nomenclature

$\tilde{p}_i$:	Power generation predicted by the renewable energy equipment i
T:	Dispatch period
$[\Delta P_i^{\min}, \Delta P_i^{\max}]$:	Confidence interval of the prediction error
a_i, b_i c_i:	Coefficients of the cost function
$P_i^{ch,\max}$:	The maximum charging power
$P_i^{ds,\max}$:	The maximum discharging power

ς^{ch}: The energy loss during the charging process
ς^{ds}: The energy loss during the discharging process
$P_i^{\min}$: The minimum power output of the device i
$P_i^{\max}$: The maximum power output of the device i
P_i^{ramp}: The ramp rate constraint
d_i: Load
$\alpha > 0$: A constant that represents the step size
$\lambda_i(k)$: The information of device i exchanged with other devices
$\zeta_i(\lambda_i(k))$: Arbitrary update function
$\chi_i^M(k)$: The maximum threshold
$\chi_i^M(k)$: The minimum threshold
$M_{n_1 \times n_1}$: The interaction between protected nodes
$M_{n_2 \times n_1}$: The interaction between protected node and ordinary nodes
$M_{n_2 \times n_2}$: The interaction of itself.

Data Availability

The data used to support this study are obtained by contacting the first author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Z. Peng, J. Wang, and D. Wang, "Distributed maneuvering of autonomous surface vehicles based on neurodynamic optimization and fuzzy approximation," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 3, pp. 1083–1090, 2018.

[2] J. Chen, T. Huang, X. Xie, P. T. W. Li, and C. Hua, "Constructing governance framework of a green and smart port," *Journal of Marine Science and Engineering*, vol. 7, no. 4, 2019.

[3] X. Lang, D. Zhongjie, and C. Jihong, "Evolutionary game of inland shipping pollution control under government co-supervision," *Marine Pollution Bulletin*, vol. 7, no. 21, 2021.

[4] L. Xu, Z. J. Di, J. H. Chen, J. Shi, and C. Yang, "Evolutionary game analysis on behavior strategies of multiple stakeholders in maritime shore power system," *Ocean & Coastal Management*, vol. 3, no. 1, 2021.

[5] 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 Transactions on Smart Grid*, vol. 11, no. 6, pp. 5339–5356, 2020.

[6] W. Rui, S. Qiuye, M. Dazhong, and H. Xuguang, "Line impedance cooperative stability region identification method for grid-tied inverters under weak grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 2856–2866, 2020.

[7] L. Ionut, "Port of Barcelona Suffers Cyberattack," 2018, https://www.bleepingcomputer.com/news/security/port-of-barcelona-suffers-cyberattack/.

[8] C. Sam, "Middle East Ports and Logistics Tech," 2020, https://m.sohu.com/a/396758697_433360.

[9] M. R. Colbie, "Cyber Attack on Asia-Pacific Ports Could Cost $110B, Hitting Global Supply Chains," 2019, https://www.insurancejournal.com/news/international/2019/10/30/546983.htm.

[10] T. Fei, S. Qihe, and L. Tieshan, "Intelligent ship integrated energy system and its distributed optimal scheduling algorithm," *ACTA AUTOMATICA SINICA*, vol. 46, pp. 1809–1817, 2020.

[11] Y. Li, H. Zhang, X. Liang, and B. Huang, "Event-triggered based distributed cooperative energy management for multienergy systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 14, pp. 2008–2022, 2019.

[12] L. Olatomiwa, S. Mekhilef, M. S. Ismail, and M. Moghavvemi, "Energy management strategies in hybrid renewable energy systems: a review," *Renewable and Sustainable Energy Reviews*, vol. 62, pp. 821–835, 2016.

[13] C. Deng, C. Wen, J. Huang, X.-M. Zhang, and Y. Zou, "Distributed observer-based cooperative control approach for uncertain nonlinear MASs under event-triggered communication," *IEEE Transactions on Automatic Control*, p. 1, 2021.

[14] Y. Wu and J. Dong, "Local stabilization of continuous-time T-S fuzzy systems with partly measurable premise variables and time-varying delay," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, 2018.

[15] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for is landed microgrids—a novel approach," *IEEE Transactions on Power Electronics*, vol. 29, no. 2, pp. 1018–1031, 2013.

[16] H. XIn, Z. Qu, J. Seuss, and M. Ali, "A self-organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1462–1473, 2010.

[17] G. Zhang, C. Li, D. Qi, and H. Xin, "Distributed estimation and secondary control of autonomous microgrid," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 989–998, 2016.

[18] F. Guo, C. Wen, J. Mao, J. Chen, and Y.-D. Song, "Hierarchical decentralized optimization architecture for economic dispatch: a new approach for large-scale power system," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 523–534, 2018.

[19] S. Hu, Y. Xiang, J. Liu et al., "Agent-based coordinated operation strategy for active distribution network with distributed energy resources," *IEEE Transactions on Industry Applications*, vol. 55, no. 4, pp. 3310–3320, 2019.

[20] J. Yu, C. Dou, and X. Li, "MAS-based energy management strategies for a hybrid energy generation system," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 6, pp. 3756–3764, 2016.

[21] J. Lai and X. Lu, "Resilient distributed voltage synchronization of CI networks under denial of service attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs, Nov.*vol. 24, 2020.

[22] J. Lai, X. Lu, Z. Dong, and S. Cheng, "Resilient Distributed Multiagent Control for AC Microgrid Networks Subject to Disturbances," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 1, 2022.

[23] X. Lu, J. Lai, and L. Guo-Ping, "Master-Slave Cooperation for Multi-DC-MGs via Variable Cyber Networks," *IEEE transactions on cybernetics*, pp. 1–14, 2021.

[24] J. H. R. van Duin, H. Geerlings, A. Verbraeck, and T. Nafde, "Cooling down: a simulation approach to reduce energy peaks of reefers at terminals," *Journal of Cleaner Production*, vol. 193, pp. 72–86, 2018.

[25] G. Parise, L. Parise, A. Malerba, F. M. Pepe, A. Honorati, and P. B. Chavdarian, "Comprehensive peak-shaving solutions for

port cranes," *IEEE Transactions on Industry Applications*, vol. 53, no. 3, pp. 1799–1806, 2017.

[26] N. Ihle, S. Runge, and N. Grundmeier, "An IT-architecture to support energy efficiency and the usage of flexible loads at a container terminal," in *Proceedings of the 28th EnviroInfo 2014 Conference*Oldenburg,Germany, September, 2014.

[27] F. D. Kanellos, "Multiagent-system-based operation scheduling of large ports' power systems with emissions limitation," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1831–1840, 2019.

[28] F. D. Kanellos, E.-S. M. Volanis, and N. D. Hatziargyriou, "Power management method for large ports with multi-agent systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1259–1268, 2019.

[29] Q. Sun, N. Zhang, S. You, and J. Wang, "The dual control with consideration of security operation and economic efficiency for energy hub," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 5930–5941, 2019.

[30] Z. Liu, A. Saberi, A. A. Stoorvogel, and D. Nojavanzadeh, "H∞ almost state synchronization for homogeneous networks of non-introspective agents: a scale-free protocol design," *Automatica*, vol. 122, Article ID 109276, 2020.

[31] J. Zhang, X. Chen, and G. Gu, "State Consensus for Discrete-Time Multi-Agent Systems over Time-Varying Graphs," *IEEE Transactions on Automatic Control*, vol. 66, 2020.

[32] Q. Guo, S. Xin, J. Wang, and H. Sun, "Comprehensive security assessment of information energy system from the blackout in Ukraine," *Power system automation*, vol. 40, no. 05, pp. 145–147, 2016, in Chinese.

[33] Y. Li, D. W. Gao, W. Gao, H. Zhang, and J. Zhou, "A Distributed Double-Newton Descent Algorithm for Cooperative Energy Management of Multiple Energy Bodies in Energy Internet," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, 2020.

[34] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 880–890, 2022.

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

[36] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber Security Analysis of State Estimators in Electric Power Systems," in *Proceedings of the IEEE 49th Conf. Decis. Control (CDC)*, pp. 5991–5998, Atlanta, GA, USA, December, 2010.

[37] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[38] J. Zhang, H. Zhang, and T. Feng, "Distributed optimal consensus control for nonlinear multiagent system with unknown dynamic," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3339–3348, 2018.

[39] Y. Tang, C. Qian, M. Li, and Q. Wang, "Overview on cyber-attacks against cyber physical power system," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 59–69, 2016, in Chinese.

[40] M. R. Habibi, H. R. Baghaee, T. Dragicevic, and F. Blaabjerg, "False data injection cyber-attacks mitigation in parallel DC/DC converters based on artificial neural networks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, 2021.

[41] A. A. Khan, O. A. Beg, and M. Alamaniotis, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electric Power Systems Research*, vol. 193, 2021.

[42] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative DC microgrids-A discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2020.

[43] S. Kar, S. R. Samantaray, and M. D. Zadeh, "Data-mining model based intelligent differential microgrid protection scheme," *IEEE Systems Journal*, vol. 11, no. 2, pp. 1161–1169, 2017.

[44] E. Casagrande, W. L. Woon, H. H. Zeineldin, and D. Svetinovic, "A differential sequence component protection scheme for microgrids with inverter-based distributed generators," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 29–37, 2014.

[45] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2923–2932, 2016.

[46] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, 2019.

[47] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2018.

[48] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[49] W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Resilient consensus protocol in the presence of trusted node," *Proc. 7th Int. Symp. Resilient Control Syst.*, pp. 1–7, 2014.

[50] C. Zhao, J. He, and Q.-G. Wang, "Resilient distributed optimization algorithm against adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4308–4315, 2020.

[51] M. Acciaro, T. Vanelslander, C. Sys et al., "Environmental sustainability in seaports: a framework for successful innovation," *Maritime Policy & Management*, vol. 41, no. 5, pp. 480–500, 2014.

[52] G. Harry and V. Duin Ron, "A new method for assessing CO2-emissions from container terminals: a promising approach applied in Rotterdam," *Journal of Cleaner Production*, vol. 19, no. 6-7, pp. 657–666, 2011.

[53] D. Ma, X. Hu, H. Zhang, Q. Sun, and X. Xie, "A hierarchical event detection method based on spectral theory of multi-dimensional matrix for power system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 4, pp. 2173–2186, 2021.

[54] K. Ma, Y. Q. Yu, S. Y. Zhu, J. Yang, and X. Guan, "Distributed algorithm for economic dispatch based on gradient descent and consensus in power grid," *Sci Sin Inform*, vol. 48, pp. 1364–1380, 2018, in Chinese.

[55] S. Mei, A. Xue, and X. Weng, "Summary on Risk of Blackouts in Complex Interconnected Power Grids and Prospects of its Preventive control," in *Proceedings of the the 24th Chinese Control Conference*, China Automation Society, Guangzhou, China, August, 2006, in Chinese.

[56] L. Yao, N. Peng, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[57] Q. Sun, R. Fan, Y. Li, B. Huang, and D. Ma, "A distributed double-consensus algorithm for residential we-energy," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 8, pp. 4830–4842, 2019.