Journal of
Marine Science and Engineering

Article

Resilient Distributed Secondary Control Strategy for Polymorphic Seaport Microgrid against Estimation-Dependent FDI Attacks

Fuzhi Wang [1], Fei Teng [2,*], Geyang Xiao [3,*], Yuanhao He [3] and Qian Feng [4]

[1] Navigation College, Dalian Maritime University, Dalian 116026, China
[2] Marine Electrical Engineering College, Dalian Maritime University, Dalian 116026, China
[3] Research Institute of Intelligent Networks, Zhejiang Lab, Hangzhou 311121, China
[4] School of Statistics, Beijing Normal University, Beijing 100875, China
* Correspondence: brenda_teng@163.com (F.T.); xgyalan@outlook.com (G.X.)

Abstract: This paper investigates the resilient distributed secondary control problem against FDI attacks for the seaport microgrid with a high proportion of renewable energy. Firstly, the polymorphic seaport microgrid containing a power layer, a control layer, a data layer and a service layer is constructed. It can achieve a software-defined function for control strategies based on a layered network and allows heterogeneous distributed generators (DGs) to exchange various types of data packets. Secondly, considering the unbounded attack generated by stolen estimator parameters can rapidly cause a large-scale power outage of the seaport microgrid, an estimation-dependent attack is designed from the perspective of attackers. Furthermore, a resilient distributed secondary control strategy using the virtual network is proposed to defend against the estimation-dependent attack. The virtual layer interconnects with the original control layer in the polymorphic network to generate an attack compensation vector, which can suppress the attack in the control layer. Furthermore, the stability analysis is completed by using the Lyapunov theory. Finally, the effectiveness of the proposed strategy is validated by a seaport microgrid test model with six DGs.

Keywords: polymorphic seaport microgrid; resilient distributed secondary control; unbounded FDI attacks; state estimator; cooperative control

check for updates

Citation: Wang, F.; Teng, F.; Xiao, G.; He, Y.; Feng, Q. Resilient Distributed Secondary Control Strategy for Polymorphic Seaport Microgrid against Estimation-Dependent FDI Attacks. *J. Mar. Sci. Eng.* **2022**, *10*, 1668. https://doi.org/10.3390/jmse10111668

Academic Editors: Rafael Morales and Eva Segura

Received: 9 October 2022
Accepted: 1 November 2022
Published: 5 November 2022

1. Introduction

The increasing logistics demand of the world maritime industry has led to higher energy consumption and carbon emissions [1]. To reduce carbon emissions, the proportion of clean energy of the maritime industry is increasing. As an important part of the maritime industry, the seaport microgrid undertakes the task of shaping the green and low-carbon maritime transportation. A seaport microgrid has a higher proportion of renewable energy compared with a conventional microgrid [2], which easily causes voltage and frequency deviations due to a strong randomness. Therefore, it is essential to investigate the distributed secondary control problem for a seaport microgrid to maintain its stability [3].

A seaport microgrid is actually a multiagent system (MAS) [4]. The distributed secondary control of the seaport microgrid relies on the communication network between the DGs. However, the traditional single-IP carrier communication network cannot support various types of data packets exchange between the heterogeneous DGs from different manufacturers. A polymorphic network [5] can support the coexistence and collaboration of multiple communication modes by programmable hardware, which can break the restraint of an IP network for information exchange between the heterogeneous DGs. Therefore, how to construct a seaport microgrid under a polymorphic environment is crucial to the distributed secondary control for the heterogeneous DGs. As a crucial node in the port's Internet of things (IoT) [6–8], the seaport microgrid attracts potential adversaries because of its public network. When the attacks are launched into the communication network, the consensus performance of the DGs is destroyed. The seaport microgrid faces the risk of a power outage [9,10]. Once a power outage occurs, the electric-driven devices (such as cranes, handing machines and belt-conveying machines) are not able to maintain normal operation, causing huge economic losses. Therefore, how to defend against potential attacks on the seaport microgrid has been widely focused on.

The false data injection (FDI) attack [11] on the microgrid is noteworthy; it destroys the consensus performance of the DGs by tampering with the neighboring information. The existing methods to defend against FDI attacks include two categories, one is to use detection and isolation algorithms to check whether the communication channels are attacked, and the other one is to use resilient control strategies to suppress attacks. The detection algorithms [12–14] generally need enough time to check each node in the communication network due to limited computing resources. That is, these detection methods cannot guarantee the stability of seaport microgrids during the detection process. As a result, researchers have developed resilient control strategies by using the virtual layer to suppress attacks [15–19]. Ref. [15] used a virtual network to interconnect with the original one to defend against linear dynamics FDI attacks. Ref. [16] proposed a resilient strategy in the case of directed graphs. For the microgrid, a resilient strategy makes the number of DGs under FDI attacks unlimited [17–19]. Ref. [17] designed the resilient strategy to defend against time-dependent and state-dependent FDI attacks on the multiple communication components. Ref. [18] indicated a resilient strategy could resist not only FDI attacks, but also DoS attacks by using the virtual layer. Ref. [19] proposed a resilient distributed method against unbounded time-dependent attacks for MASs. The above-mentioned attack types are time-dependent and state-dependent. For a seaport microgrid, the state estimator is applied to improve the measurement accuracy in complex weather environment [20]. The potential adversaries can choose to steal the state estimator parameters to design estimation-dependent attacks rather than time-dependent and state-dependent attacks [21]. It is noteworthy that compared with other FDI attacks, estimation-dependent attacks can change with the estimation results dynamically rather than with a fixed growth trajectory. The estimation-dependent attacks can destroy the state estimator function for making control decisions, causing a large-scale power outage of the seaport microgrid.

In conclusion, to defend against an estimation-dependent attack, this paper proposes a resilient distributed secondary control strategy for a polymorphic seaport microgrid. The contributions of this paper are as follows:

(1) The polymorphic seaport microgrid is constructed including a power layer, a data layer, a control layer and a service layer. The heterogeneous DGs can exchange information through the data layer. Furthermore, software-defined functions can be achieved by the control layer.

(2) A unbounded estimation-dependent attack from the perspective of attackers is designed. It can be generated by stolen estimator parameters of the seaport microgrid to cause a large-scale power outage due to the error estimation results. Furthermore, the characteristics of the estimation-dependent attack is analyzed to model the attack launched on the seaport microgrid.

(3) A resilient distributed secondary control strategy is proposed to defend against the estimation-dependent attack for the seaport microgrid. The virtual layer is used to interconnect with the control layer to generate an attack compensation vector, which can suppress the attack injected into the control layer.

The rest of this paper is organized as follows. Section 2 establishes a polymorphic seaport microgrid. Section 3 proposes a resilient distributed secondary strategy to suppress the estimation-dependent attack and completes a stability analysis. Section 4 gives simulation cases to validate the effectiveness of the proposed strategy. Finally, Section 5 summarizes this paper.

2. Framework of the Polymorphic Seaport Microgrid

The structure [22–24] of a seaport microgrid consists of DGs, power loads and control systems, as shown in Figure 1. To reduce carbon emissions, various renewable energy devices (such as wind turbines, photovoltaic panels, etc.) are integrated into the seaport microgrid. Since the seaport is an important link between the sea and the land, the power loads generally contain land-based electrical equipment (electric vehicles, port cranes, etc.) and cold ironing facilities providing power to the ships. In addition, the seaport microgrid is equipped with control systems to analyze data and make decisions. The SCADA system is responsible for collecting the measurement results uploaded by sensors in the channels between the DGs. The state estimator using the measurement results provides estimation results to the EMS.

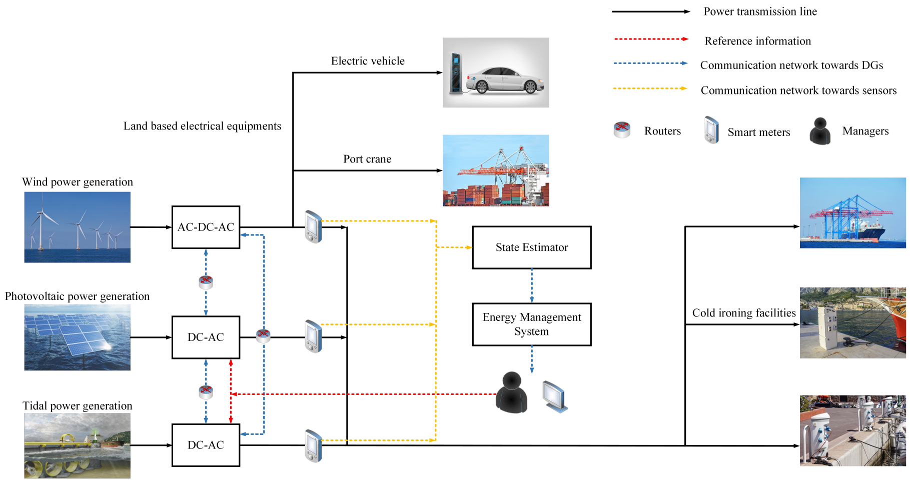

Figure 1. The typical structure of a seaport microgrid.

To break the restraint of traditional IP carrier network, a polymorphic seaport microgrid is established to exchange information between the heterogeneous DGs from different manufacturers in Figure 2. The manager-oriented service layer contains the state estimator and the EMS. That is, the control systems of the seaport microgrid shown in Figure 1 are included into the service layer. The control layer ensures the software-defined functions are compatible with various control strategies. Furthermore, the data layer configures the polymorphic identification table to exchange various types of data packets between the neighboring DGs through different transmission channels (such as FPGA, etc.). The power layer contains the whole DGs and loads, from which all the measurements are obtained. Thus, the polymorphic seaport microgrid can not only exchange information between the heterogeneous DGs, but also design and implement a resilient strategy using the virtual layer against estimation-dependent attacks.

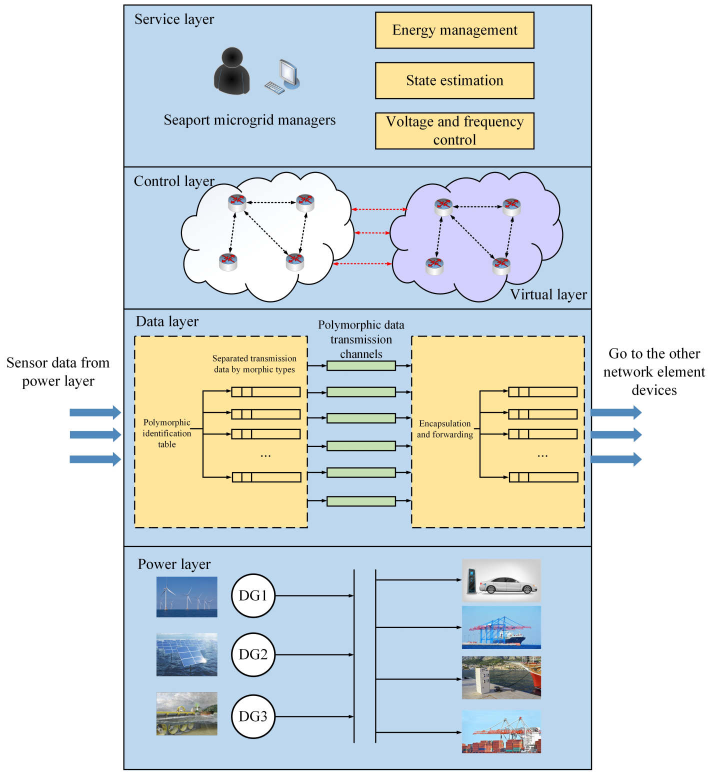
Service layer
Seaport microgrid managers
Energy management
State estimation
Voltage and frequency control
Control layer
Virtual layer
Data layer
Sensor data from power layer
Polymorphic data transmission channels
Separated transmission data by morphic types
Polymorphic identification table
...
Encapsulation and forwarding
...
Go to the other network element devices
Power layer
DG1
DG2
DG3

Figure 2. Illustrated framework of polymorphic seaport microgrid.

3. Resilient Distributed Secondary Control Strategy for the Seaport Microgrid

In this section, the impact of an estimation-dependent attack on the seaport microgrid is analyzed, and a resilient distributed secondary control strategy is proposed to defend against the estimation-dependent attack.

3.1. Graph Theory

The communication topology of the seaport microgrid considered is a directed graph ς containing a leader and N followers. The weighted adjacency matrix of ς can be described as $A = [a_{ij}] \in R^{N\times N}$, where a_{ij} is the weight between nodes. If $a_{ij} > 0$, the agent i can receive neighboring information from agent j, otherwise, $a_{ij} = 0$. The in-degree matrix of ς can be described as $D = diag(d_i) \in R^{N\times N}$, and $d_i = \sum\limits_{j=1}^{N} a_{ij}$. The Laplace matrix of ς can be described as $L = D - A$. In addition, $G_l = diag(g_{li}) \in R^{N\times N}$ is the matrix of gains from the leader to the ith follower. For a better expression, the notations involved in this paper are shown in Notations.

3.2. Problem Formulation

The droop mechanisms of the ith DG in the seaport microgrid can be shown as

$$\omega_i = \omega_{ni} - m_i P_i \tag{1}$$

$$V_i = V_{ni} - n_i Q_i \tag{2}$$

where ω_i is the angular frequency of the ith DG, V_i is the output voltage of the ith DG, ω_{ni} and V_{ni} are the set points for the droop mechanisms, m_i and n_i are droop coefficients chosen according to the power rating of the ith DG and P_i and Q_i are the active and reactive output power of the ith DG, respectively.

To maintain the consensus performance of the DGs, ω_{ni} and V_{ni} are exchanged between the neighboring DGs. Differentiating (1) and (2) yields

$$\dot{\omega}_{ni} = \dot{\omega}_i + m_i\dot{P}_i = u_{wi} \tag{3}$$

$$\dot{V}_{ni} = \dot{V}_i + n_i\dot{Q}_i = u_{vi} \tag{4}$$

where u_{wi} and u_{vi} are auxiliary control inputs.

Based on the leader–follower information, u_{wi} and u_{vi} at each DG can be shown as

$$\dot{\omega}_{ni} = u_{wi} = \sum_{j=1}^{N} a_{ij}(\omega_j - \omega_i) + g_{li}(\omega_{ref} - \omega_i) + \sum_{j=1}^{N} a_{ij}(m_jP_j - m_iP_i) \tag{5}$$

$$\dot{V}_{ni} = u_{vi} = \sum_{j=1}^{N} a_{ij}(V_j - V_i) + g_{li}(V_{ref} - V_i) + \sum_{j=1}^{N} a_{ij}(n_jQ_j - n_iQ_i) \tag{6}$$

where ω_{ref} and V_{ref} are the frequency and voltage reference information, respectively. Then, (5) and (6) can be reformulated as

$$\begin{aligned} \dot{\omega}_{ni} = u_{wi} = & \sum_{j=1}^{N} a_{ij}((\omega_j + m_jP_j) - (\omega_i + m_iP_i)) \\ & + g_{li}((\omega_{ref} + m_iP_i) - (\omega_i + m_iP_i)) \\ = & \sum_{j=1}^{N} a_{ij}(\omega_{nj} - \omega_{ni}) + g_{li}(\omega_{nref} - \omega_{ni}) \end{aligned} \tag{7}$$

$$\begin{aligned} \dot{V}_{ni} = u_{vi} = & \sum_{j=1}^{N} a_{ij}((V_j + n_jQ_j) - (V_i + n_iQ_i)) \\ & + g_{li}((V_{ref} + n_iQ_i) - (V_i + n_iQ_i)) \\ & \sum_{j=1}^{N} a_{ij}(V_{nj} - V_{ni}) + g_{li}(V_{nref} - V_{ni}) \end{aligned} \tag{8}$$

where $\omega_{nref} = \omega_{ref} + m_iP_i$, $V_{nref} = V_{ref} + n_iQ_i$ and the power sharing mechanisms m_iP_i and n_iQ_i are included in the distributed secondary control laws (7) and (8).

The frequency and the voltage of each DG can converge steadily due to the relationship between the active power/reactive power of each DG and its angular frequency/output voltage [25]. That is, to synchronize ω_i and m_iP_i / V_i and n_iQ_i, we can directly synchronize ω_{ni}/V_{ni}. For convenience, ω_i/V_i is used to denote ω_{ni}/V_{ni}. We consider the local form of discrete-time distributed secondary control laws as

$$\frac{\omega_i(k+1) - \omega_i(k)}{T} = \sum_{j=1}^{N} a_{ij}(\omega_j(k) - \omega_i(k)) + g_{li}(\omega_{ref} - \omega_i(k)) \tag{9}$$

$$\frac{V_i(k+1) - V_i(k)}{T} = \sum_{j=1}^{N} a_{ij}(V_j(k) - V_i(k)) + g_{li}(V_{ref} - V_i(k)) \tag{10}$$

The compact form combining (9) and (10) is shown as

$$\frac{\boldsymbol{v_i(k+1) - v_i(k)}}{T} = \sum_{j=1}^{N} a_{ij}(\boldsymbol{v_j(k)} - \boldsymbol{v_i(k)}) + g_{li}(\boldsymbol{v_l(k)} - \boldsymbol{v_i(k)}) \tag{11}$$

where $\boldsymbol{v_i(k)} = [V_i(k), \omega_i(k)]^T$ is the voltage and frequency of the ith DG and $\boldsymbol{v_l(k)} = [V_{ref}, \omega_{ref}]^T$ is the reference voltage and frequency of each DG. T is the sample time of the seaport microgrid. Then, the global form of (11) can be shown as

$$\boldsymbol{v(k+1)} = (-T(\beta_l \otimes I_e))\boldsymbol{v(k)} + T(\beta_l \otimes I_e)\boldsymbol{v_{wef}} \tag{12}$$

where $\boldsymbol{v_{wef}} = \mathbf{1_N} \otimes \boldsymbol{v_l}$, $\beta_l = L + G_l$, and $I_e = diag(1,1)$. In addition, to improve the measurement accuracy of the seaport microgrid, the state estimator is proposed as

$$\begin{cases} \boldsymbol{\hat{v}(k+1)} = (-T(\beta_l \otimes I_e))\boldsymbol{\hat{v}(k)} + T(\beta_l \otimes I_e)\boldsymbol{v_{wef}} + K\boldsymbol{r(k+1)} \\ \boldsymbol{r(k+1)} = \boldsymbol{y(k+1)} - C(-T(\beta_l \otimes I_e))\boldsymbol{\hat{v}(k)} \end{cases} \tag{13}$$

where $\boldsymbol{\hat{v}(k+1)}$ is the estimation result at time $k+1$, $\boldsymbol{y(k+1)}$ is the measurement vector, C is a $2N$-dimensional identity observation matrix. Define $\boldsymbol{r(k)}$ as the estimation residual, which aims to measure whether FDI attacks can be detected by the χ^2 detector. K is the Kalman gain, which can reach the steady state at an exponential speed from any original state [26]. Therefore, K can be solved by (14) and (15)

$$\begin{aligned} P = &-T(\beta_l \otimes I_e)P(-T(\beta_l \otimes I_e))^T + Q \\ &+T(\beta_l \otimes I_e)PC^T(CPC^T + R)^{-1}CP(-T(\beta_l \otimes I_e)) \end{aligned} \tag{14}$$

$$K = PC^T(CPC^T + R)^{-1} \tag{15}$$

where Q and R are both $2N$-dimensional positive definite matrices. They represent the covariance of the noise in the seaport microgrid, which can also be used for designing a control strategy without considering noise factors [27].

The strategy shown in (12) can keep the stability of the seaport microgrid. However, considering potential attacks, the strategy changes from (12) to (16):

$$\boldsymbol{v^a(k+1)} = (-T(\beta_l \otimes I_e))\boldsymbol{v^a(k)} + T((\beta_l \otimes I_e)\boldsymbol{v_{wef}} + \boldsymbol{\delta(k)}) \tag{16}$$

where $\boldsymbol{v^a(k+1)}$ is the voltage and frequency of DGs under FDI attacks. $\boldsymbol{\delta(k)}$ is the FDI attack vector. Accordingly, the dynamic expression of the state estimator (13) under FDI attacks is shown as

$$\begin{cases} \boldsymbol{\hat{v}^a(k+1)} = (-T(\beta_l \otimes I_e))\boldsymbol{\hat{v}^a(k)} + T(\beta_l \otimes I_e)\boldsymbol{v_{wef}} + K\boldsymbol{r^a(k+1)} \\ \boldsymbol{r^a(k+1)} = \boldsymbol{y^a(k+1)} - C(-T(\beta_l \otimes I_e))\boldsymbol{\hat{v}^a(k)} \end{cases} \tag{17}$$

where $\boldsymbol{\hat{v}^a(k+1)}$ is the estimation result under FDI attacks, $\boldsymbol{y^a(k+1)}$ is the measurement vector under FDI attacks and $\boldsymbol{r^a(k)}$ is the estimation residual under FDI attacks. From (17), the estimation results will deviate from the ones under normal operation under attacks. In order to reflect the deviation more clearly, we define $\boldsymbol{\Delta\hat{v}(k+1)}$ and $\boldsymbol{\Delta r(k+1)}$ as the estimation difference and the residual difference, respectively. Combining with (12), (13), (16) and (17), the expression of (17) can be given as

$$\begin{aligned} \boldsymbol{\Delta\hat{v}(k+1)} &= \boldsymbol{\hat{v}^a(k+1)} - \boldsymbol{\hat{v}(k+1)} \\ &= -KC(-T(\beta_l \otimes I_e))\boldsymbol{\Delta\hat{x}(k)} + KC(\boldsymbol{v^a(k+1)} - \boldsymbol{v(k+1)}) \end{aligned} \tag{18}$$

$$\begin{aligned} \boldsymbol{\Delta r(k+1)} &= \boldsymbol{r^a(k+1)} - \boldsymbol{r(k+1)} \\ &= -C(-T(\beta_l \otimes I_e))\boldsymbol{\Delta\hat{v}(k)} + C(\boldsymbol{v^a(k+1)} - \boldsymbol{v(k+1)}) \end{aligned} \tag{19}$$

where $\boldsymbol{v^a(k+1)} - \boldsymbol{v(k+1)}$ reflects the impact on the voltage and frequency of DGs caused by FDI attacks.

3.3. The Estimation-Dependent FDI Attack on the Seaport Microgrid

In existing works, potential FDI attacks on the microgrid are usually modeled as time-dependent sinusoidal and proportional functions, such as $\boldsymbol{\delta(k)} = f + b\sin(ck)$. f and b are both constants, and c is a positive integer. Obviously, there exists a arbitrary constant Con which can achieve $\|\boldsymbol{\delta(k)}\| \le Con$. Specially, if the FDI attack is modeled as $\boldsymbol{\delta(k)} = f + bk$, it becomes an unbounded attack. Such time-dependent attack modeling methods are indeed reasonable. However, potential adversaries can choose to steal the state estimator parameters to design estimation-dependent attacks. To illustrate the impact of estimation-dependent attack, this subsection designs an algorithm to generate an estimation-dependent FDI attack from the perspective of adversaries, as shown in Algorithm 1. It should be noted that Algorithm 1 needs to satisfy the following assumptions.

Algorithm 1 The estimation-dependent attack for the seaport microgrid

```
**Initialization parameters:**
Define $\boldsymbol{\Delta\hat{x}(0)} = \boldsymbol{\hat{x}^a(0)} - \boldsymbol{\hat{x}(0)}$.
Choose an arbitrary $\phi \in (0,1)$ and a detection threshold $M = 2$.
**while** $k \ge 0$ **do**
    Set $\boldsymbol{\Delta\hat{x}(0)} = 0$, $\phi(0) = 0$;
    Calculate $\boldsymbol{\delta(k)} = \frac{1}{T}[(-T(\beta_l \otimes I_e))\boldsymbol{\Delta\hat{x}(k)} + \phi(k)M\boldsymbol{I^s_{2N}}]$;
    Calculate $\boldsymbol{\Delta\hat{v}(k+1)} = -KC(-T(\beta_l \otimes I_e))\boldsymbol{\Delta\hat{v}(k)}$
                  $+KC(\boldsymbol{v^a(k+1)} - \boldsymbol{v(k+1)})]$;
    $k = k + 1$;
    $\phi(k) = 0.1$;
**end while**
```

Assumption 1. *Attackers have perfect knowledge of the communication topology inside the seaport microgrid.*

It should be noted that attackers cannot change the attack abruptly during the generation process due to limited resources [28]. In this case, it is reasonable to consider that $\boldsymbol{\delta(k)}$ is energy-bounded. That is, the attack grows at a steady or decaying rate. In existing works, the attack is believed to be proportional to the time or the state of the system [19,21,29]. Obviously, unbounded attacks [19,21,29] satisfy the nonstrict convexity. Therefore, we propose Assumption 2 to describe the general characteristic of unbounded attacks.

Assumption 2. *The estimation-dependent attack satisfies the nonstrictly convex function characteristic* $2\boldsymbol{\delta(k+1)} \le \boldsymbol{\delta(k)} + \boldsymbol{\delta(k+2)}$ *after several steps of initialization.*

Algorithm 1 generates the estimation-dependent attack as

$$\boldsymbol{\delta(k)} = \frac{1}{T}[(-T(\beta_l \otimes I_e))\boldsymbol{\Delta\hat{v}(k)} + \phi(k)M\boldsymbol{I^s_{2N}}] \tag{20}$$

where $\boldsymbol{I^s_{2N}}$ is the sth column of a $2N$-dimensional identity matrix. To be more precise, the selection principle of s is given by [21]. As Algorithm 1 shows, the estimation difference of voltage and frequency is set to zero at $k = 0$. Since $\phi(k)M\boldsymbol{I^s_{2N}} \neq 0$, $\boldsymbol{\delta(k)}$ will be a nonzero vector in the iterative process, which indicates $\boldsymbol{\delta(k)}$ can affect the seaport microgrid all the time. When the stability of the seaport microgrid is destroyed, $\boldsymbol{v^a(k+1)} - \boldsymbol{v(k+1)}$ has a nonzero value, which leads to the divergence of $\boldsymbol{\Delta\hat{v}(k+1)}$. The diverging $\boldsymbol{\Delta\hat{v}(k+1)}$ will generate $\delta(k+1)$ at the next time k, which leads to the divergence of $\delta(k+1)$. Thus, both $\delta(k)$ and $\Delta\hat{v}(k)$ will diverge to ∞ eventually.

In fact, when $\Delta\hat{v}(k)$ diverges to a certain degree, the seaport microgrid manager will make an outage decision to avoid causing great economic losses. Therefore, to defend against the estimation-dependent attack illustrated in Algorithm 1, a resilient strategy should be proposed.

3.4. Resilient Distributed Secondary Control Strategy Based on a Layered Network

This subsection introduces a virtual network Σ_h, which interconnects with the original network Σ_c to defend against an estimation-dependent attack. Since the virtual network Σ_h has no physical meanings, it has a pretty high level of security. The attackers can achieve the goal of destabilizing the seaport microgrid only by injecting limited resources. Therefore, a resilient distributed secondary control strategy using a virtual network is proposed to defend against an estimation-dependent attack on Σ_c.

As shown in Figure 3, both networks have the same number of nodes, and these nodes can accept reference information. The resilient strategy (21)–(23) is proposed to suppress the estimation-dependent attack launched on the original network Σ_c.

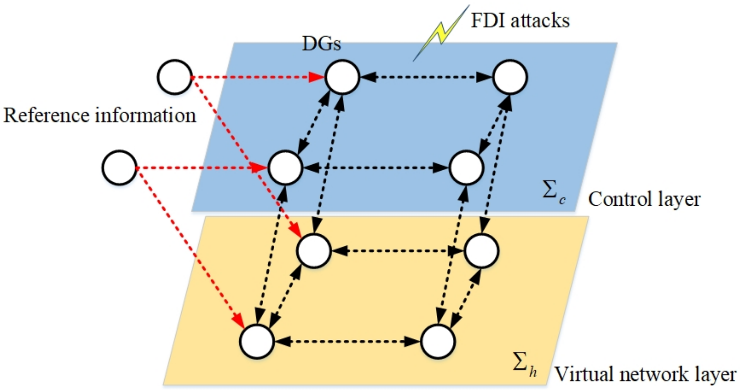

Figure 3. The layered network includes an original network Σ_c and a virtual network Σ_h.

$$v^a(k+1) = -T(\beta_l \otimes I_e)v^a(k) + T((\beta_l \otimes I_e)v_{wef} + \delta(k) - \hat{\delta}(k)) \tag{21}$$

$$\varphi(k+1) = -T(\beta_l \otimes I_e)\varphi(k) + T(\beta_l \otimes I_e)v_{wef} \tag{22}$$

$$\hat{\delta}(k+1) = T((\beta_l \otimes I_e)d(k) + \hat{\delta}(k)) \tag{23}$$

where $\varphi(k) = [\varphi_1^T(k), \varphi_2^T(k), ..., \varphi_{2N}^T(k)]^T$ is the state vector of Σ_h, $d(k) = v^a(k) - \varphi(k)$ is the difference of the state vectors between Σ_c and Σ_h and $\hat{\delta}(k)$ is the attack-compensation vector generated by (21) and (22). Define the error between $v^a(k)$ in Σ_c and the reference information x_{wef} as $d_1(k)$, and the error between $\varphi(k)$ in Σ_h and the reference information x_{wef} as $d_2(k)$.

$$d_1(k) = v^a(k) - x_{wef} \tag{24}$$

$$d_2(k) = \varphi(k) - x_{wef} \tag{25}$$

Assumption 3. *If there is a path to each other node, the direct graph ς has a spanning tree.*

Lemma 1 (see [30]). *Suppose Assumption 3 holds, β_l is a positive-definite and nonsingular matrix.*

Lemma 2 (see [19]). *If $X \in R^{N\times N}$ is a Hurwitz matrix, then $\begin{bmatrix} X & I_N \\ X & 0_N \end{bmatrix} \in R^{2N\times 2N}$ is also Hurwitz.*

Theorem 1. *Suppose the estimation-dependent attack (20) satisfying Assumption 1 and Assumption 2, and Assumption 3 holds. The synchronization of DGs under the estimation-dependent attack (20) can be maintained by using the proposed resilient distributed secondary control strategy (21)–(23).*

Proof of Theorem 1. For the resilient distributed secondary control strategy (21)–(23) against the estimation-dependent attack in Algorithm 1, the stability of the original control layer Σ_c (21) should be proven. Since $\boldsymbol{d_1(k)} = \boldsymbol{d(k)} + \boldsymbol{d_2(k)}$, we prove the stability of $\boldsymbol{d(k)}$ and $\boldsymbol{d_2(k)}$ in two steps and finally show the stability of the original control layer Σ_c.

Step 1: From Assumption 1, the estimation-dependent attack can be generated by Algorithm 1. Define $\boldsymbol{\tilde{\delta}(k)} = \boldsymbol{\delta(k)} - \boldsymbol{\hat{\delta}(k)} = [\tilde{\delta}_1^T(k), \tilde{\delta}_2^T(k), ..., \tilde{\delta}_{2N}^T(k)]^T$, which is the difference between the estimation-dependent attack vector and the attack-compensation vector (23). Then, the expression of $\boldsymbol{d(k+1)}$ can be obtained from (21) and (22) as

$$\boldsymbol{d(k+1)} = -T(\beta_l \otimes I_e)\boldsymbol{d(k)} + T\boldsymbol{\tilde{\delta}(k)} \tag{26}$$

From (23), the differential relationship between $\boldsymbol{\tilde{\delta}(k+1)}$ and $\boldsymbol{\tilde{\delta}(k)}$ is

$$\boldsymbol{\tilde{\delta}(k+1)} - \boldsymbol{\tilde{\delta}(k)} = -T(\beta_l \otimes I_e)\boldsymbol{d(k)} + T(\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)}) \tag{27}$$

To be more convenient, integrate (26) and (27) into a compact matrix form as

$$\begin{bmatrix} \boldsymbol{d(k+1)} \\ \boldsymbol{\tilde{\delta}(k+1)} \end{bmatrix} = \begin{bmatrix} -T(\beta_l \otimes I_e) & I_{2N} \\ -T(\beta_l \otimes I_e) & 0_{2N} \end{bmatrix} \begin{bmatrix} \boldsymbol{d(k)} \\ \boldsymbol{\tilde{\delta}(k)} \end{bmatrix} + \begin{bmatrix} 0_{2N} \\ T(\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)}) \end{bmatrix} \tag{28}$$

Define $\boldsymbol{r(k)} = [\tilde{\delta}^T(k), d^T(k)]^T$. The relationship between $\boldsymbol{r(k+1)}$ and $\boldsymbol{r(k)}$ is $\boldsymbol{r(k+1)} = \Phi\boldsymbol{r(k)} + \begin{bmatrix} 0_{2N} \\ T(\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)}) \end{bmatrix}$, where $\Phi = \begin{bmatrix} -T(\beta_l \otimes I_e) & I_{2N} \\ -T(\beta_l \otimes I_e) & 0_{2N} \end{bmatrix}$. A Lyapunov function is chosen as

$$V_1(k) = [T(\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)})]^T[T(\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)})] \tag{29}$$

From Assumption 2, $\Delta V_1 = \|\boldsymbol{\delta(k+2)} - \boldsymbol{\delta(k+1)}\|^2 - \|\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)}\|^2 \leq 0$. A Lyapunov function is chosen as

$$V_2(k) = \boldsymbol{r^T(k)}P_s\boldsymbol{r(k)} + V_1(k) \tag{30}$$

where $P_s > 0$ is a symmetric matrix. The differential form of (30) is shown as

$$\begin{aligned} V_2(k+1) - V_2(k) &= \boldsymbol{r^T(k+1)}P_s\boldsymbol{r(k+1)} - \boldsymbol{r^T(k)}P_s\boldsymbol{r(k)} + V_1(k+1) - V_1(k) \\ &= (\Phi\boldsymbol{r(k)})^T P_s(\Phi\boldsymbol{r(k)}) - \boldsymbol{r^T(k)}P_s\boldsymbol{r(k)} \\ &\quad + T^2\|\delta(k+2) - \delta(k+1)\|^2 - T^2\|\delta(k+1) - \delta(k)\|^2 \\ &= \boldsymbol{r^T(k)}(\Phi^T P_s\Phi - P_s)\boldsymbol{r(k)} \\ &\quad + T^2\|\delta(k+2) - \delta(k+1)\|^2 - T^2\|\delta(k+1) - \delta(k)\|^2 \\ &= -\boldsymbol{r^T(k)}Q_s\boldsymbol{r(k)} \\ &\quad + T^2(\|\delta(k+2) - \delta(k+1)\|^2 - \|\delta(k+1) - \delta(k)\|^2) \end{aligned} \tag{31}$$

From Assumption 3 and Lemma 1, since β_l is positive-definite, $-T(\beta_l \otimes I_e)$ is Hurwitz. From Lemma 2, $\Phi = \begin{bmatrix} -T(\beta_l \otimes I_e) & I_{2N} \\ -T(\beta_l \otimes I_e) & 0_{2N} \end{bmatrix}$ is also Hurwitz. Thus, there exists a symmetric positive matrix P_s, which makes $\Phi^T P_s\Phi - P_s = -Q_s < 0$ for any symmetric positive matrix Q_s. From Assumption 2, $\|\boldsymbol{\delta(k+2)} - \boldsymbol{\delta(k+1)}\|^2 - \|\boldsymbol{\delta(k+1)} - \boldsymbol{\delta(k)}\|^2 \leq 0$. Therefore, $\Delta V_2 < 0$ can be given after the initial time.

Step 2: To prove the stability of the virtual layer Σ_v (22), the differential form of $\boldsymbol{d_2(k)}$ can be written as $\boldsymbol{d_2(k+1)} = -T(\beta_l \otimes I_e)\boldsymbol{d_2(k)}$. Let $V(k) = \boldsymbol{d_2^T(k)}P_h\boldsymbol{d_2(k)}$, and the differential form is shown as

$$\begin{aligned} \Delta V &= \boldsymbol{d_2^T(k+1)}P_h\boldsymbol{d_2(k+1)} - \boldsymbol{d_2^T(k)}P_h\boldsymbol{d_2(k)} \\ &= \boldsymbol{d_2^T(k)}(-T(\beta_l \otimes I_e))^T P_h(-T(\beta_l \otimes I_e))\boldsymbol{d_2(k)} \\ &\quad -\boldsymbol{d_2^T(k)}P_h\boldsymbol{d_2(k)} \\ &= \boldsymbol{d_2^T(k)}((-T(\beta_l \otimes I_e))^T P_h(-T(\beta_l \otimes I_e)) - P_h)\boldsymbol{d_2(k)} \\ &= -\boldsymbol{d_2^T(k)}Q_h\boldsymbol{d_2(k)} \end{aligned} \tag{32}$$

Since $-T(\beta_l \otimes I_e)$ is Hurwitz, the positive symmetric matrix P_h can achieve $-Q_h < 0$. As a result, $\Delta V < 0$. The stability of the virtual layer Σ_h can be proven.

Step 1 and **Step 2** show that the original control layer Σ_c (21) and the virtual layer Σ_h (22) are both stable under the estimation-dependent attack. Thus, the resilient strategy (21)–(23) can defend against the estimation-dependent attack effectively. This completes the proof of Theorem 1. □

4. Case Study

The test seaport microgrid with six DGs and loads in Figure 4 was used to validate the effectiveness of the proposed resilient strategy to suppress attacks. The transmission lines between the inverter-based DGs were considered to be inductive, and the loads connected to the seaport microgrid through the AC bus. The DGs exchanged neighboring information through communication networks, and the relationship between the layered network and attackers is shown in Figure 4. The rated parameters of the test microgrid were the parameters in [23], as shown in Table 1.

Table 1. Setting of the test seaport microgrid and Algorithm 1.

Symbol	Parameters
DG1,DG2,DG3	9 kVA
DG4,DG5,DG6	7 kVA
Lines	$R = 0.23\ \Omega, L = 318\ \mu\text{H}$
Loads	$R = 3\ \Omega, L = 0.0064\ \text{H}$
T	0.001 s
N	6
M	2
σ	0.1
a_{ij}	10
g_{li}	1
I_{2N}^s	$[0,0,1,0,0,0,0,0,0,0,0,0]^T$
v_{wef}	$[380\ \text{V}, 50\ \text{Hz}]^T$
C	I_{12}
Q	$diag(0.001,0.001,0.001,0.01,0.01,0.01,0.001,0.001,0.001,0.01,0.01,0.01)$
R	$diag(0.1,0.1,0.1,0.2,0.2,0.2,0.1,0.1,0.1,0.2,0.2,0.2)$

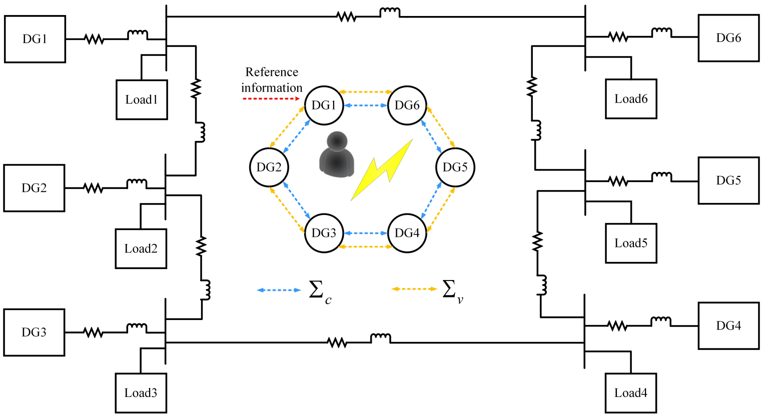

Figure 4. The test seaport microgrid with 6 DGs in this paper.

4.1. Case 1: The Effectiveness of the Proposed Strategy under Load Disturbance and No Attacks

This case study provides simulation cases to illustrate the applicability of the proposed strategy when there exists a load disturbance and no attacks. As shown in Figure 4, loads 1–5 of the seaport microgrid are connected to the seaport microgrid at the initial time, while load 6 is disconnected. When $k = 20$, load 6 is connected to the seaport microgrid, and load 5 is disconnected from the seaport microgrid when $k = 60$. The voltage performance of each DG during this period is shown in Figure 5. From the simulation results, it can be seen that the proposed strategy can maintain the voltage stability after a short period of fluctuation, regardless of whether the load is connected or disconnected. Obviously, it shows that the proposed strategy is also applicable under the normal operation of load disturbance and no attacks.

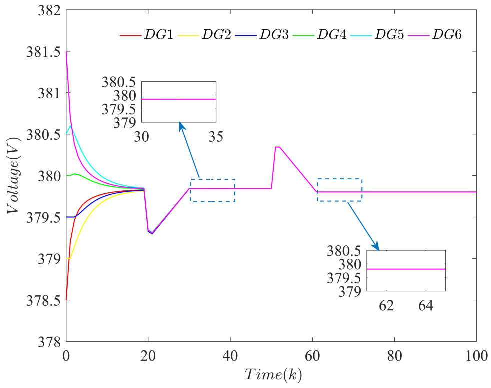

Figure 5. Performance of the proposed strategy under load disturbance and no attacks.

4.2. Case 2: The Impact of Designed Estimation-Dependent Attack

This case study provides simulation cases to show the impact of an estimation-dependent attack on the seaport microgrid using the state-of-art resilient strategy in [17]. For this purpose, the generation process of the designed estimation-dependent attack is shown in Figure 6. It can be observed that the unbounded attack initializes at $k = 20$ and then diverges to ∞ rapidly.

Before the estimation-dependent attack is launched on the control layer, the voltage trajectories converge to the reference voltage of 380 V. When the estimation-dependent attack initializes in the control layer at $k = 20$, the voltage trajectories diverge to 400 V gradually, as shown in Figure 7. Obviously, the voltage amplitude exceeds the allowable range 380 V $\times(1 \pm 5\%)$. This implies the estimation-dependent attack launched on the control layer destroys the consensus performance of DGs, and the resilient strategy in [17] cannot suppress the impact caused by the attack.

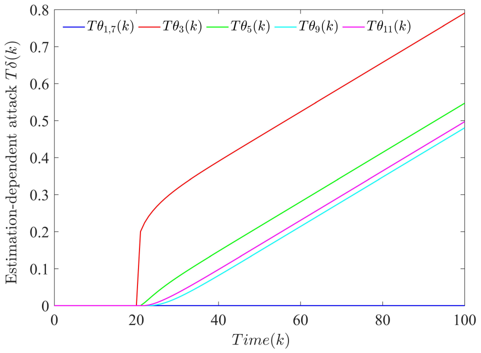

Figure 6. Dynamic generation process of the estimation-dependent attack given by Algorithm 1.

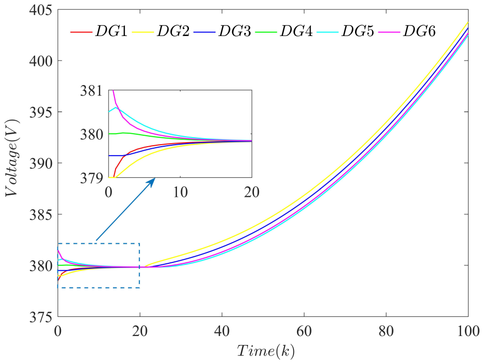

Figure 7. Consensus performance of the DGs using the strategy in [17] under the estimation-dependent attack.

Furthermore, it can be observed from Figure 8 that the voltage estimation difference also diverges to ∞ with increasing iterations due to the abnormal consensus performance shown in Figure 7. This is because $v^a(k) - v(k) \neq 0$ in (18) makes the iteration process of $\Delta\hat{v}(k)$ diverge.

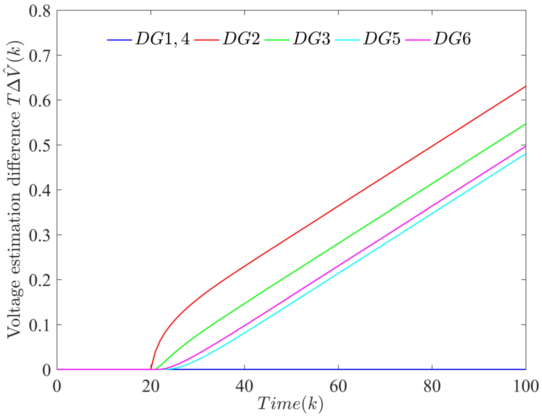

Figure 8. Estimation difference of the DGs using the strategy in [17] under the estimation-dependent attack.

The diverged voltage estimation at time k accelerates the divergence of the estimation-dependent attack at time $k+1$. Then, the diverged estimation-dependent attack at time $k+1$ accelerates the divergence of $\Delta\hat{v}(k)$ at time $k+2$. In this way, both the estimation-dependent attack and $\Delta\hat{v}(k)$ diverge to ∞ with the increasing number of iterations.

The results show that the estimation-dependent attack can be generated dynamically by the diverging voltage estimation difference, which has a stronger destructiveness compared with time-dependent and state-dependent attacks. Furthermore, the strategy in [17] cannot maintain the consensus performance of the DGs under the estimation-dependent attack.

4.3. Case 3: The Effectiveness of Proposed Strategy Against the Estimation-Dependent Attack

This case study prefers to focus on the effectiveness of the proposed strategy (21)–(23) against the estimation-dependent attack. As shown in Figure 9, the voltage of each DG still converges to 380 V under the estimation-dependent attack by using the proposed strategy. Compared with the strategy in [17], this shows the proposed strategy can suppress the impact caused by the estimation-dependent attack.

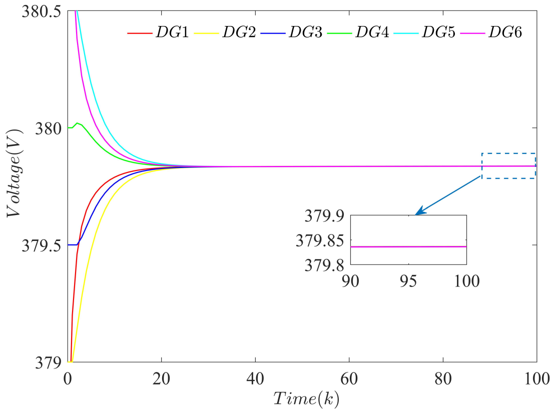

Figure 9. Consensus performance of the DGs using the proposed strategy under the estimation-dependent attack.

Furthermore, since $v^a(k+1) - v(k+1)$ in (18) is close to zero after the estimation-dependent attack initializes at $k = 20$, the estimation difference $\Delta\hat{v}(k)$ can be suppressed greatly during the iterative process in Figure 10. This implies that the proposed strategy can not only suppress the impact of the estimation-dependent attack on the consensus performance, but also protect the state estimator in the seaport microgrid.

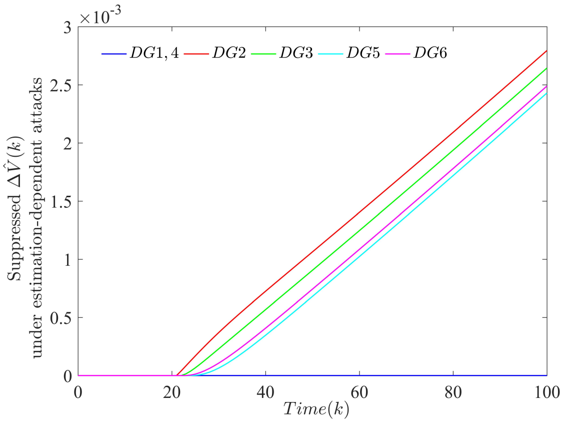

Figure 10. Estimation difference of the DGs using the proposed strategy under the estimation-dependent attack.

In addition, Figure 11 shows both the amplitude and divergence speed of the unbounded estimation-dependent attack are greatly suppressed. This is because the estimation difference $\Delta\hat{v}(k)$ is suppressed greatly by using the proposed strategy.

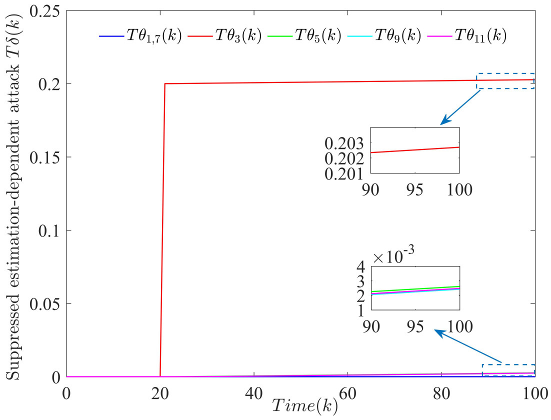

Figure 11. The suppressed estimation-dependent attack using the proposed strategy.

As a result, the proposed strategy can maintain the consensus performance of the DGs. Then, the estimation function of the state estimator is guaranteed due to the normal consensus performance. Finally, the estimation-dependent attack generated by estimation difference $\Delta\hat{v}(k)$ is greatly suppressed.

4.4. Case 4: The Effectiveness of the Proposed Strategy under a Time-Dependent Attack

To validate the generality of the proposed strategy against FDI attacks, this case study takes a time-dependent attack as an example. The time-dependent attack can be modeled as

$$\boldsymbol{\theta(k)} = [20\mathrm{sin(2k)}, 0, 20\mathrm{sin(k)}, 0, 20\mathrm{sin(k)}, 0, 20\mathrm{sin(k)}, 0, 20\mathrm{sin(2k)}, 0, 20\mathrm{sin(k)}, 0]^T \quad (33)$$

When large enough bounded time-dependent attacks initialize in the control layer at $k = 20$ using the strategy in [17], the additional sinusoidal attack signal is reflected in the voltage performance of the DGs shown in Figure 12A, which makes the voltage amplitude close to 400 V beyond the allowable fluctuation range 380 V $\times(1 \pm 5\%)$.

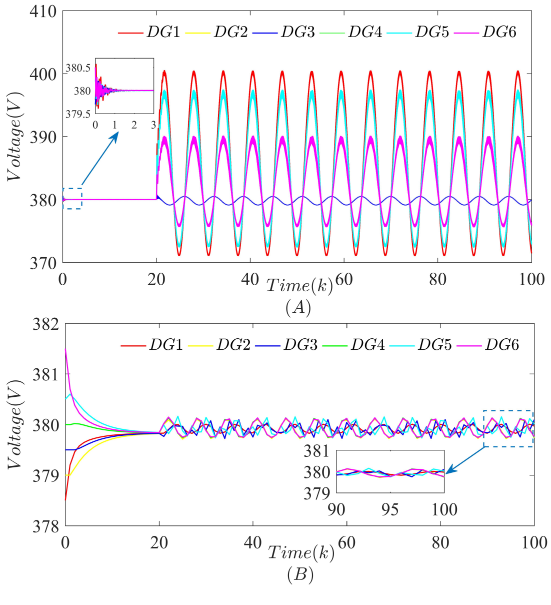

Figure 12. Consensus performance of the DGs using different resilient strategies under a time-dependent attack: (**A**) the strategy in [17]; (**B**) the proposed strategy.

When using the proposed strategy, the voltage can be maintained within the allowable fluctuation range 380 V $\times(1 \pm 5\%)$, as shown in Figure 12B. Compare with the strategy in [17], the proposed strategy is superior to defend against the large-enough bounded time-dependent attack, which can suppress the voltage fluctuation in the allowed range.

Accordingly, when using the strategy in [17], the estimation results under the bounded time-dependent attack deviate from the normal results by nearly 20 V, as shown in Figure 13A. Furthermore, the deviations using the proposed strategy can be suppressed to nearly 0.02 V, as shown in Figure 13B. Since the strategy in [17] cannot defend against the impact of bounded time-dependent attacks on the state estimator, it directly provides a vulnerability for attackers to design estimation-dependent attacks.

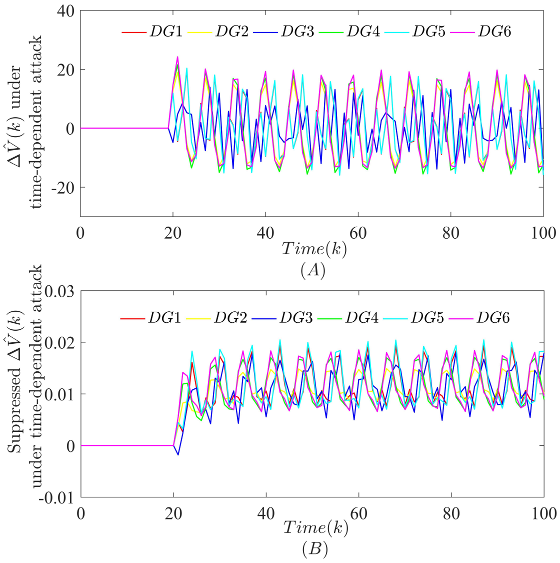

Figure 13. Estimation difference of the DGs using different resilient strategies under the time-dependent attack: (**A**) the strategy in [17]; (**B**) the proposed strategy.

In conclusion, all the simulation cases validated that the proposed strategy had better performance than the one in [17] when facing with estimation-dependent and time-dependent FDI attacks. Compared with the strategy in [17], the proposed strategy could maintain the seaport microgrid's stability under an estimation-dependent attack and suppress the voltage fluctuation within the rated range under a time-dependent attack. That is, the proposed strategy had a general ability to defend against various FDI attacks.

5. Conclusions

This paper proposed a distributed resilient secondary control strategy against estimation-dependent FDI attacks on a seaport microgrid. A polymorphic seaport microgrid was established to exchange various types of data packets for the heterogeneous DGs. Considering that the state estimator was essential to improve the measurement accuracy for the seaport microgrid under complex weather environment, an estimation-dependent attack generated by stolen estimator parameters was designed from the perspective of attackers. To defend against an estimation-dependent attack dynamically changing with the estimation results, the proposed strategy made the control layer interconnect with the virtual layer to generate an attack compensation vector. The proposed resilient strategy could make the tracking error $d_1(k)$ asymptotically stable under the estimation-dependent attack. Finally, simulation cases were used to validate the effectiveness of the proposed strategy compared with the strategy in [17].

Author Contributions: F.W. proposed the idea, completed the experiments and finished the final manuscript; F.T. modified the idea, edited the final manuscript and provided the seaport operational information; G.X. completed the experiments and analyzed the formulas; Y.H. revised the grammar of the final manuscript and summarized the references; Q.F. provided guidance for the structure of the article manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China (2019YFB1802501); the Key Research Project of Zhejiang Lab (2021LE0AC02); the National Natural Science Foundation of China (under grant nos. 52201407, 62203403, 51939001 and 61803064).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Notations

The following abbreviations are used in this manuscript:

Symbol	Description
i, j	Index of DGs
$(\cdot)^T$	Transpose of the matrix
$\|\cdot\|$	Euclidean norm of the vector
$diag(\cdot)$	Diagonal matrix
$\otimes$	Kronecker product
1_N	Vector whose all components are ones
A	Weighted adjacency matrix
D	In-degree matrix
L	Laplace matrix
G_l	Leader gain matrix
T	Sampling time
ω_i	Angular frequency of the ith DG
V_i	Voltage of the ith DG
ω_{ni}, V_{ni}	Secondary control setting points
m_i, n_i	Droop coefficients
P_i, Q_i	Active and reactive power
$\delta(k)$	FDI attack
v_i	Compact vector containing angular frequency and voltage
v_i^a	Compact vector under the FDI attack
v_l	Compact vector containing reference information
$\hat{v}_i$	State estimation results of angular frequency and voltage
φ	Compact vector of the virtual layer
y	Measurement vector
K	Kalman gain
Q, R	Covariance matrix of noise
$\hat{\delta}$	Attack-compensation vector

References

1. Fang, S.; Wang, C.X.; Liao, R.J.; Zhao, C.H. Optimal power scheduling of seaport microgrids with flexible logistic loads. *IET Renew. Power Gener.* **2022**, *16*, 2711–2720. [CrossRef]
2. Tazaki, T.; Harada, E.; Gotoh, H. Numerical investigation of sediment transport mechanism under breaking waves by DEM-MPS coupling scheme. *Coast. Eng.* **2022**, *175*, 104146. [CrossRef]
3. Bidram, A.; Davoudi, A. Hierarchical Structure of Microgrids Control System. *IEEE Trans. Smart Grid.* **2012**, *3*, 1963–1976. [CrossRef]
4. Zhang, J.L.; Chen, Z.Y.; Zhang, H.W.; Feng, T. Coupling effect and pole assignment in trajectory regulation of multi-agent systems. *Automatica.* **2021**, *125*, 109465. [CrossRef]
5. Hu, Y.X.; Li, D.; Sun, P.H.; Yi, P.; Wu, J.X. Polymorphic smart network: An open, flexible and universal architecture for future heterogeneous networks. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 2515–2525. [CrossRef]
6. Rana, M.M.; Xiang, W.; Wang, E. IoT-Based State Estimation for Microgrids. *IEEE Internet Things J.* **2018**, *5*, 1345–1346. [CrossRef]
7. Li, Y.S.; Gao, D.W.Z.; Gao, W.; Zhang, H.G.; Zhou, J.G. A Distributed Double–Newton Descent Algorithm for Cooperative Energy Management of Multiple Energy Bodies in Energy Internet. *IEEE Trans. Ind. Inf.* **2021**, *17*, 5993–6003. [CrossRef]
8. Chen, K.; Ma, Z.Z.; Bai, L.B.; Sheng, H.M.; Cheng, Y.H. Emergence of bipartite flocking behavior for Cucker-Smale model on cooperation-competition networks with time-varying delays. *Neurocomputing.* **2022**, *507*, 325–331. [CrossRef]
9. Iosif, P.; Paul, R.; Nikitas, N. Cyber Physical Systems Security for Maritime Assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384.

10. Teng, F.; Sun, Q.Y.; Xie, X.P.; Zhang, H.G.; Ma, D.Z. A disaster-triggered life-support load restoration framework based on Multi-Agent Consensus System. *Neurocomputing* **2015**, *170*, 339–352. [CrossRef]
11. Liu, Y.; Ning, P.; Reiter, M.K.False data injection attacks against state estimation in electric power grids. In Proceedings of the the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
12. Sahoo, S.; Mishra, S.; Peng, J.C.-H.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
13. Abhinav, S.; Modares, H.; Lewis, F.L.; Ferrese, F; Davoudi, A. Synchrony in Networked Microgrids Under Attacks. *IEEE Trans. Smart Grid.* **2018**, *9*, 6731–6741. [CrossRef]
14. Shi, X.Y.; Shi, L.; Zhou, Q.; Chen, K.; Cheng, Y.H. Bipartite Flocking for Cucker-Smale Model on Cooperation-Competition Networks Subject to Denial-of-Service Attacks. *IEEE Trans Circuits Syst I Regul Pap.* **2022**, *69*, 3379–3390. [CrossRef]
15. Gusrialdi, A.; Qu, Z.H.; Simaan, M.A. Robust design of cooperative systems against attacks. In Proceedings of the 2014 American Control Conference (ACC), Portland, OR, USA, 4–6 June 2014.
16. Gusrialdi, A.; Qu, Z.H.; Simaan, M.A. Competitive Interaction Design of Cooperative Systems Against Attacks. *IEEE Trans. Automat. Contr.* **2018**, *63*, 3159–3166. [CrossRef]
17. Chen, Y.L.; Qi, D.L.; Dong, H.Q.; Li, C.Y.; Li, Z.M.; Zhang, J.L. A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids. *IEEE Trans. Smart Grid.* **2021**, *12*, 1929–1938. [CrossRef]
18. Zhou, Q.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A.; Che, L.; Liu, X. Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids. *IEEE Trans. Smart Grid.* **2021**, *12*, 3705–3717. [CrossRef]
19. Zuo, S.; Yue, D. Resilient Containment of Multigroup Systems Against Unknown Unbounded FDI Attacks. *IEEE Trans. Ind. Electron.* **2022**, *69*, 2864–2873. [CrossRef]
20. Li, C.B.; Tan, Y.; Cao, Y.J.; Shao, S.N.; Zhou, H.J.; Liu, Y.; Qi, G.G.; Zhang, R.S. Energy management system architecture for new energy power supply system of islands. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012.
21. Hu, L.; Wang, Z.D.; Han, Q.-L.; Liu, X.H. State estimation under false data injection attacks: Security analysis and system protection. *Automatica.* **2018**, *87*, 176–183. [CrossRef]
22. Wang, R.; Sun, Q.Y.; Sun, C.H.; Zhang, H.G.; Gui, Y.H.; Wang, P. Vehicle-Vehicle Energy Interaction Converter of Electric Vehicles: A Disturbance Observer Based Sliding Mode Control Algorithm. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9910–9921. [CrossRef]
23. Bidram, A.; Lewis, F.L.; Davoudi, A. Distributed Control Systems for Small-Scale Power Networks: Using Multiagent Cooperative Control Theory. *IEEE Trans. Control Syst. Mag.* **2014**, *34*, 56–77.
24. Peng, Z.H.; Liu, L.; Wang, J. Output-Feedback Flocking Control of Multiple Autonomous Surface Vehicles Based on Data-Driven Adaptive Extended State Observers. *IEEE Trans Cybern.* **2021**, *51*, 4611–4622. [CrossRef] [PubMed]
25. Bidram, A.; Davoudi, A.; Lewis, F.L. A Multiobjective Distributed Control Framework for Islanded AC Microgrids. *IEEE Trans. Industr. Inform.* **2014**, *10*, 1785–1798. [CrossRef]
26. Zuo, S.; Beg, O.A.; Lewis, F.L.; Davoudi, A. Resilient Networked AC Microgrids Under Unbounded Cyber Attacks. *IEEE Trans. Smart Grid.* **2020**, *11*, 3785–3794. [CrossRef]
27. Huang, J.; Ho, D.W.; Li, F.; Yang, W.; Tang, Y. Secure remote state estimation against linear man-in-the-middle attacks using watermarking. *Automatica* **2020**, *121*, 109182. [CrossRef]
28. Dutta, R.G.; Zhang, T.; Jin, Y.E. Resilient Distributed Filter for State Estimation of Cyber-Physical Systems Under Attack. In Proceedings of the 2019 American Control Conference (ACC), Philadelphia, PA, USA, 10–12 July 2019.
29. Zhou, J.; Chen, B.; Yu, L. Intermediate-Variable-Based Estimation for FDI Attacks in Cyber-Physical Systems. *IEEE Trans. Circuits Syst. II-Express Briefs.* **2020**, *67*, 2762–2766. [CrossRef]
30. Zuo, S.; Song, Y.D.; Lewis, F.L.; Davoudi, A. Output Containment Control of Linear Heterogeneous Multi-Agent Systems Using Internal Model Principle. *IEEE Trans Cybern.* **2017**, *47*, 2099–2109. [CrossRef]