frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 16 August 2022
DOI 10.3389/fenrg.2022.961488

OPEN ACCESS

EDITED BY
Xiao Wang,
Wuhan University, China

REVIEWED BY
Yue Wu,
Southwest Jiaotong University, China
Wang Lina,
China Jiliang University, China
Nannan Rong,
Tianjin Polytechnic University, China

*CORRESPONDENCE
Qihe Shan,
shanqihe@163.com
Jun Zhu,
zhu_j@aliyun.com

SPECIALTY SECTION
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

RECEIVED 04 June 2022
ACCEPTED 28 June 2022
PUBLISHED 16 August 2022

CITATION
Wang F, Shan Q, Zhu J and Xiao G (2022), Discrete-time resilient-distributed secondary control strategy against unbounded attacks in polymorphic microgrid.
Front. Energy Res. 10:961488.
doi: 10.3389/fenrg.2022.961488

Discrete-time resilient-distributed secondary control strategy against unbounded attacks in polymorphic microgrid

Fuzhi Wang[1], Qihe Shan[1]*, Jun Zhu[2]* and Geyang Xiao[2]

[1]Navigation College, Dalian Maritime University, Dalian, China, [2]Research Institute of Intelligent Networks, Zhejiang Lab, Hangzhou, China

This study proposes a polymorphic cooperative control system for microgrid consisting of a service layer, a control layer, a data layer, and a power layer to apply a resilient-distributed secondary control strategy to distributed generators (DGs) from different manufacturers more conveniently. Due to the improvement of network openness, external cyberattacks are more likely to tamper with the neighbor information transmitted in the cooperative control system. In this study, a discrete-time resilient-distributed secondary control strategy is designed to resist potential unbounded false data injection (FDI) attacks, which introduces a virtual network layer interconnecting the control network layer to form a layered network. The strategy can maintain the stability of voltage and frequency under unbounded attacks and then greatly suppress the state estimation difference of voltage and frequency. Meanwhile, the unbounded attack depending on voltage and frequency estimation difference is suppressed to a nearly bounded attack. Finally, a microgrid consisting of six inverter-based DGs is taken as an example to validate the effectiveness of the strategy against unbounded attacks.

KEYWORDS

unbounded attack sequence, discrete-time, polymorphic network, virtual layer, resilient distributed secondary control strategy

1 Introduction

With the rapid development of power electronic devices and new energy technology, the power system has gradually transitioned to the stage of a new electric power system characterized by a high proportion of new energy and power electronic devices (Zhou et al., 2020; Tang et al., 2022). As an important part of the new electric power system, microgrid integrates geographically dispersed, intermittent and random new energy, and internal energy storage devices can adjust the flow of electric energy flexibly (Zhou J. et al., 2021; Wang et al., 2021). With the increase of the proportion of new energy, a large number of power electronic devices, such as rectifiers and inverters, have

appeared in the microgrid to replace original generators with the rotor to generate power. Since power electronic devices cannot provide the inertia from generators with rotors, the frequency of microgrids is more susceptible to be disturbed. For microgrids with a high proportion of new energy and power electronic devices, distributed secondary control (Bidram et al., 2014) has attracted wide attention as an effective strategy to maintain voltage and frequency stability.

The distributed secondary control strategy relies on advanced communication facilities and network structure to exchange neighbor information. The development of the communication network structure of microgrid mainly includes three stages, i.e., IP-based network, software-defined network (SDN) (Nunes et al., 2014; Kreutz et al., 2015), and a polymorphic network with full-dimensional definition (Hu et al., 2020, 2022; Zhang et al., 2022). The IP-based network combines the function of the control layer and the data layer in the forwarding devices, which makes it difficult for researchers to test advanced control methods and hinders the innovation of network structure. SDN separates the function of the control layer and data layer. Network devices in the data layer only remain the function of forwarding data, and the function of calculating routes is centralized in the control layer. Due to the function separation, the control layer of SDN provides more programmable ports for microgrid managers to design and implement advanced control methods. In order to make the network requirements of various DGs produced by different manufacturers in microgrids can be realized on the same communication facilities in the data layer, a polymorphic network has been established which supports various network technology. A polymorphic network is integrated into a service layer, a control layer, and a data layer, where the control layer and the data layer still maintain the separated functions. A polymorphic network is an advanced network structure that can support a resilient distributed secondary control strategy applied in the microgrid. Neighbor information of various DGs can be exchanged on the same communication facilities, which benefits improving consensus performance of cooperative control among the DGs, and even microgrids.

The more advanced the network structure, the more open it will be. Both communication links and terminals are possibly subject to potential cyberattacks (Gao et al., 2022). Common attacks in the microgrid include denial of service (DoS) and FDI attacks. DoS attacks send a large number of packets to block the communication network to prevent information exchange between the neighbor DGs. Technologies such as firewalls (Salah et al., 2012) and gates (Condry and Nelson, 2016) can effectively defend against the threat of DoS attacks launched in the communication network of the microgrid. FDI attacks are characterized by tampering with the exchanged information between the neighbor DGs. The DG receives the tampered neighbor information but does not know it, and then transmits the tampered information to other neighboring DGs. In fact, it is difficult for us to defend FDI attacks by methods against DoS attacks because of their strong stealth. Therefore, how to design a proper distributed secondary control strategy against FDI attacks has been a noteworthy topic for researchers. At present, the solution to FDI attacks in the distributed secondary strategy mainly includes two scheme types. The first scheme is to design detection algorithms to isolate the attacked communication channels. The second scheme is to design resilient distributed secondary control strategies to mitigate the impact of FDI attacks in the microgrid. In such resilient strategies, FDI attacks exist together with the microgrid, and resilient distributed control strategies aim to minimize or even eliminate the impact of FDI attacks on consensus performance as much as possible. Liu et al. defined FDI attacks in state estimation of centralized power systems (Liu et al., 2009, 2011). After this, many algorithms emerged to detect FDI attacks in the microgrid. The work in Manandhar et al. (2014) shows that although the χ^2 detector can detect faults and DoS attacks, it cannot detect well-designed FDI attacks. In order to overcome this limitation, a Euclidean detector that can effectively detect FDI attacks is proposed. Yang et al. (2022) proposed a method for detecting bad data in power transformers based on artificial intelligence. Fawzi et al. (2014) studied the estimation problem of linear systems when some sensors or actuators are destroyed by attackers, and especially pointed out that if more than half of the sensors are attacked, it is impossible to accurately reconstruct the state of the system. Wang et al. (2020) proposed a local detection and isolation algorithm which can solve the problem of undetectable attacks through the combination of observable PMU or smart sensors. Chen et al. (2021) proposed an aperiodic intermittent control strategy with random switching frequency to detect and isolate the attacked communication channels. Hu et al. (2018) and Pang et al. (2022) studied the impact of stealthy FDI attacks on the communication channels and points out that if some key communication channels are well protected, the attack behaviors will be detected.

Such detection algorithms can effectively detect FDI attacks launched in the communication channels. When the DG exchanges information with its neighbors, detection algorithms will reduce the range of the attacked DGs through time iteration, and finally determine which DG has been attacked. The process is called computation response time that often requires the microgrid system to allocate resources to complete. Therefore, isolation measures will be delayed accordingly. The impact which FDI attacks can cause is serious during the detection time between attacks launched and eliminated. Researchers have become more interested in developing resilient distributed secondary control strategies against FDI attacks to address this problem. Zeng and Chow (2014) proposed a trust-based resilient distributed secondary control strategy, which embeds a recovery mechanism in the distributed control process and enhances the resilience against FDI attacks.

Abhinav et al. (2018) designed a trust-based resilient distributed secondary control strategy against FDI attacks launched in sensors, actuators, and communication channels. Under the condition that at least half of the neighbors of each DG are secure, this strategy can defend against time-independent constant FDI attacks. Gharesifard and Başar (2012) introduced a virtual network interconnecting with the original control network to make the overall dynamic network resilient against FDI attacks with linear dynamics by designing appropriate interconnection matrices. Gusrialdi et al. (2014) extended the work of Gharesifard and Başar (2012) to the case of strongly connected directed graphs. Abhinav et al. (2018) studied the case of directed graphs and attacks with nonlinear dynamics based on the work of Gharesifard and Başar (2012) and Gusrialdi et al. (2014).

Researchers introduced the layered network theory proposed by some studies (Gharesifard and Başar, 2012; Gusrialdi et al., 2014; Abhinav et al., 2018) to the FDI attack problem of networked microgrids, and Zhou Q. et al. (2021) and Chen et al. (2021) introduced the layered network theory into distributed secondary control strategy to deal with FDI attacks launched in the communication network. Liu et al. (2022) proposed a resilient distributed optimal frequency control scheme to deal with the impact of FDI attacks by introducing the layered network theory. Zuo et al. (2020) proposed a novel concept of the cooperative and adversarial multigroup system consisting of leaders, followers, and adversaries. Zuo and Yue (2022) designed a resilient containment control method against the unbounded FDI attacks occurring in the communication network of the multigroup system proposed by Zuo et al. (2020), and it is worth mentioning that the unbounded FDI attack in this study is modeled as a proportional function of time. Unbounded attacks modeled in this way are very destructive but can be easily perceived by detectors. A more realistic attack design method is to generate a destructive and stealthy attack sequence based on the matrix parameters of the microgrid (Hu et al., 2018). The attack sequence can make the state estimation difference of the microgrid go to ∞ without being perceived by the χ^2 detector. As mentioned previously, detection and isolation measures can cause a high computational burden for the microgrid. During the calculation process of detection and isolation measures, external FDI attacks will still cause irreparable impacts on the microgrid. Therefore, how to resist this kind of destructive and stealthy unbounded attack sequence has been a novel problem.

In this study, a discrete-time resilient distributed secondary control strategy is designed to resist the impact of unbounded attack sequences on the microgrid. The main contributions of this study are as follows.

1) A polymorphic cooperative control system for microgrids consisting of a service layer, a control layer, a data layer, and a power layer is established in this study, which can apply the resilient distributed secondary control strategy to DGs from different manufacturers.
2) Considering potential unbounded FDI attacks in the polymorphic cooperative control system, a discrete-time resilient distributed secondary control strategy is designed to maintain voltage and frequency stable against unbounded attacks.
3) The state estimation difference of voltage and frequency are suppressed by a large margin. Sufficient time is provided for the deployment of detection and isolation measures before the service layer of the polymorphic cooperative control system makes wrong decisions. Meanwhile, the unbounded attack depending on voltage and frequency estimation difference is suppressed to a nearly bounded attack, which is less threat to the microgrid.

The rest of this study is organized as follows. **Section 2** introduces the microgrid polymorphic cooperative control system and the function of each layer. **Section 3** describes the influence of unbounded FDI attack on the microgrid, then designs a resilient distributed secondary control strategy against attacks, and finally uses Lyapunov theory to prove the stability of the strategy. **Section 4** validates the effectiveness of the proposed strategy by a test microgrid with six inverter-based DGs. Finally, **Section 5** presents the summary of this study.

2 Structure of the polymorphic cooperative control system

A polymorphic network is an advanced network structure supporting the microgrid operation, which can change control strategy in real-time according to the operation characteristics of the microgrid. Moreover, various DGs produced by different manufacturers can transmit information in the data layer of the polymorphic network. The polymorphic cooperative control system established in this study is shown in **Figure 1**. The polymorphic cooperative control system consists of four layers: a service layer, a control layer, a data layer, and a power layer. The service layer, control layer, and data layer constitute the polymorphic network to support the cooperative control of DGs in the power layer. The service layer is the center of the polymorphic cooperative control system, which integrates data monitoring, resource allocation, control strategy design, and other functions; and is open to microgrid managers. Managers can design and deploy distributed secondary control strategies by obtaining matrix parameters of microgrids through the service layer. In the control layer, a polymorphic identification table is configured in the distributed controller, which supports the coexistence and collaboration of IP, content, identification, geospatial location, and other identities in the same data layer. In addition, the distributed secondary control strategy deployed through the service layer is also installed in the distributed

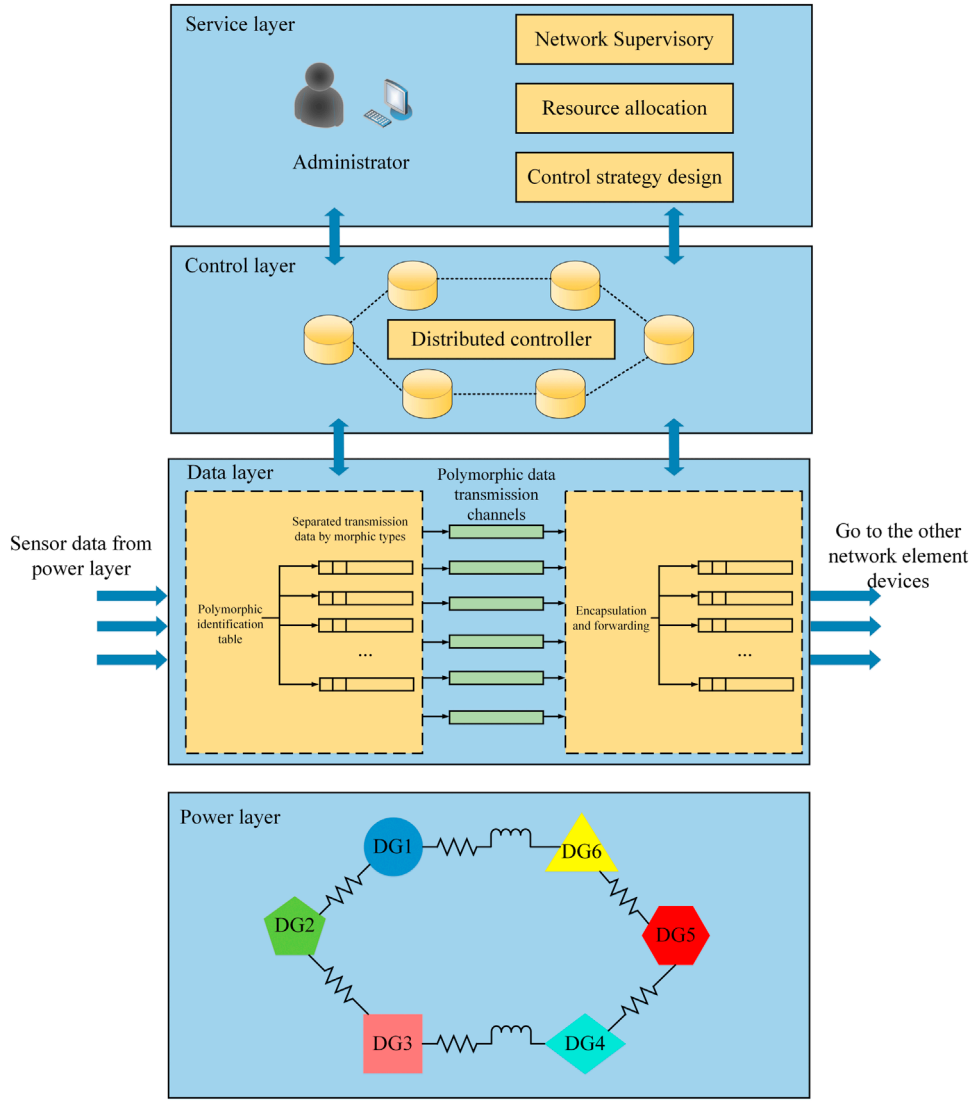

FIGURE 1
Microgrid polymorphic cooperative control system.

controller. According to the polymorphic identification table configured in the control layer, the data layer divides the polymorphic data packets uploaded through terminals in the power layer into corresponding polymorphic data transmission channels. These polymorphic packets are encapsulated and forwarded to the next network device to realize the resilient distributed secondary control strategy installed in the distributed controller. The interaction between the layers is realized through programmable ports. The upper layer transmits instructions to the lower layer, and the lower layer feeds back the collected information to the upper layer.

The service layer, control layer, and data layer of the microgrid polymorphic cooperative control system achieve the information transmission through programmable ports and separate the control function from the forwarding function. In fact, DGs in the microgrid are not provided by the same manufacturer and often support different network protocols and data package types. If a new control strategy is applied in the microgrid, managers need to manually adjust the configuration of DGs, which is undoubtedly not beneficial to the innovation of the control strategy. However, the polymorphic identification table configured in the control layer and the polymorphic data transmission channels in the data layer can make these various DGs plug and play in the same network environment. The control layer customizes the channels into processing units suitable for polymorphic data packets by programming FPGA. In this

way, the microgrid polymorphic cooperative control system can define the functions of each network layer to support the realization of distributed secondary control strategy applied in the large-scale heterogeneous DGs.

3 Resilient-distributed secondary control strategy against the unbounded FDI attack sequence

3.1 Graph preliminaries

The communication topology of microgrid discussed in this study is described as a directed graph ς including $N+m$ agents. $A_a = [a_{ij}] \in R^{N\times N}$ is the weighted adjacency matrix of ς, and a_{ij} denotes the weight value of the edge between the follower nodes, $a_{ij} > 0$ represents *DGi* that can receive information from *DGj*, otherwise $a_{ij} = 0$. $D = \mathrm{diag}(d_i) \in R^{N\times N}$ is the in-degree matrix for ς, where $d_i = \sum_{j=1}^{n} a_{ij}$. $L = D - A_a$ means the Laplace matrix of ς. Define $G_l = \mathrm{diag}(g_{li}) \in R^{nxn}, l = (1,2,\ldots,m)$, where g_{li} denotes the gain between the *l*th leader and *i*th follower. And a nomenclature containing sets, parameters, and abbreviations is shown in **Table 1**.

3.2 Problem formulation

The inherent distributed characteristics of DGs in microgrid make distributed control a more suitable secondary control strategy to adjust voltage and frequency. Microgrid managers can design proper distributed secondary control strategy to maintain voltage and frequency stable around the rated value. Only part of DGs can receive the reference information, and then complete the task in a cooperative manner through the communication network. For first-order linear multi agent systems (MASs), the distributed secondary control of microgrid with N DGs can be transformed into a synchronization problem. The local expression for the distributed secondary control strategy used to control voltage and frequency is

$$\frac{x_i(k+1)-x_i(k)}{T} = \sum_{j=1}^{n} a_{ij}\left(x_j(k)-x_i(k)\right) + \sum_{l=1}^{m} g_{li}\left(x_l(k)-x_i(k)\right), \quad (1)$$

where T is the sampling time of microgrid. $x_i(k) = \begin{bmatrix} V_i(k) \\ f_i(k) \end{bmatrix}$, $V_i(k)$ denotes the voltage of *DGi*, $f_i(k)$ denotes the frequency of *DGj*. $x_j(k) = \begin{bmatrix} V_j(k) \\ f_j(k) \end{bmatrix}$, $V_j(k)$ denotes the voltage of *DGj*, $f_j(k)$ denotes the frequency of *DGj*. $x_l(k) = \begin{bmatrix} V_l(k) \\ f_l(k) \end{bmatrix}$, $V_l(k)$ denotes the reference voltage of *DGs*, $f_l(k)$ denotes the reference frequency of *DGs*, $l = 1,2,\ldots,m$ denotes the number of leaders. Obviously, the influence caused by FDI attacks has not been considered in the distributed secondary control strategy. The neighbor information *DGi* received from *DGj* is $x_i^a(k) = x_j(k) + \Theta_{i,j}(k)$ when adversaries launched FDI attacks in the communication channels between *DGi* and *DGj*. $x_i^a(k)$ represents the neighbor information *DGi* received from *DGj* has been tampered by $\Theta_{i,j}(k)$. The local expression for the distributed secondary control strategy when the communication channels have been launched FDI attacks is

$$\frac{x_i(k+1)-x_i(k)}{T} = \sum_{j=1}^{n} a_{ij}\left(x_j(k)+\Theta_{i,j}(k)-x_i(k)\right) + \sum_{l=1}^{m} g_{li}\left(x_l(k)-x_i(k)\right). \quad (2)$$

Also, then the global form of **Eqn. 2** can be obtained as

$$\frac{x(k+1)-x(k)}{T} = \sum_{l=1}^{m}\left(G_l\otimes I_e\right)x_l^{'} - \left(\left(L\otimes I_e\right)x(k) + \sum_{l=1}^{m}\left(G_l\otimes I_e\right)x(k)\right) + \Theta(k), \quad (3)$$

where $x(k) = [x_1^T(k), x_2^T(k), \ldots, x_n^T(k)]^T$ denotes all the *DGs'* voltage and frequency state variable. Define $x_l^{'} = 1_n \otimes x_l$, and $\Theta(k) = [\Theta_1^T(k), \Theta_2^T(k), \ldots, \Theta_n^T(k)]^T$ denotes the global form of unbounded attack sequence. Define $\beta_l = 10L + G_l$, and $(L\otimes I_e)(1_n \otimes x_l) = 0$. **Eqn. 3** can be rewritten as

$$\frac{x(k+1)-x(k)}{T} = \sum_{l=1}^{m}\left(\beta_l\otimes I_e\right)x_l^{'} - \sum_{l=1}^{m}\left(\beta_l\otimes I_e\right)x(k) + \Theta(k). \quad (4)$$

TABLE 1 Nomenclature table.

Symbol	Description
Index and sets	
i,j	Index of DGs
$(\cdot)^T$	Transpose of the matrix
$\|\cdot\|$	Euclidean norm of the vector
$diag(\cdot)$	Diagonal matrix
Parameters	
N	Number of DGs
m	Number of leader DGs
a_{ij}	Gains between DGs
g_{li}	Gains between leader DGs and follower DGs
I_n	n dimensional identity matrix
$I_{N\times n}$	$N\times n$ dimensional identity matrix
I_e	Identity matrix of uncertain dimensions that aligns the dimensions of the equality matrix
$\Theta(k)$	Unbounded attack sequence
Σ_s	Control layer
Σ_h	Virtual layer
Abbreviations	
FDI	False data injection
DGs	Distributed generators
DoS	Denial of service
SDN	Software-defined network

When there exists no attacks in the communication channels, the voltage and frequency state variable $x(k)$ and measurement output $y(k)$ are shown as

$$\begin{cases} x(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)x(k) + T\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l', \\ y(k) = Cx(k) \end{cases} \tag{5}$$

The following state estimator is proposed for voltage and frequency state variable $x(k)$:

$$\begin{cases} \hat{x}(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\hat{x}(k) + T\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l' + Kz(k+1), \\ z(k) = y(k+1) - CA\hat{x}(k) \end{cases} \tag{6}$$

where $A = I_{N\times n} - T\sum_{j=1}^{n}(\beta_l \otimes I_e)$ and C is the measurement matrix, and $\hat{x}(k+1) = \left[\hat{V}_1^T(k+1), \hat{f}_1^T(k+1), \ldots, \hat{V}_1^T(k+1), \hat{f}_1^T(k+1)\right]^T$ denotes the state estimation value at time $k+1$. $z(k)$ denotes the estimation residual difference at time k, which is related to whether FDI attacks can be detected. If $z(k)$ is less than a constant value, the detector will not perceive the attacks. K denotes Kalman gain, although the standard Kalman filter is time-varying, the Kalman filter can rapidly enter steady state at exponential speed from any initial conditions (Huang et al., 2020). K can be obtained from **Eqs. 7**, **8**

$$P = APA^T + Q - APC^T\left(CPC^T + R\right)^{-1}CPA, \tag{7}$$

$$K = PC^T\left(CPC^T + R\right)^{-1}, \tag{8}$$

where Q and R commonly denote the covariance of the noise in Kalman filter, and they can also be used as parameters for strategy design in noiseless environment. The application of state estimation in noiseless environment is discussed in Rapp and Nyman (2004) and Dutta et al. (2019). In principle, they can be selected as any positive definite matrices. Combine with **Eqn. 4**, when attacks have been launched in the communication channels, the voltage and frequency state variable $x(k)$ and measurement output $y(k)$ are shown as

$$\begin{cases} x^a(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)x^a(k) + T\left(\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l' + \Theta(k)\right), \\ y^a(k) = Cx^a(k) \end{cases} \tag{9}$$

where $x^a(k+1)$ denotes the voltage and frequency state variable under attacks, and $y^a(k)$ denotes the measurement output under attacks. Accordingly, the state estimator for voltage and frequency under attacks can be shown as

$$\begin{cases} \hat{x}^a(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\hat{x}^a(k) + T\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l' + Kz^a(k+1), \\ z^a(k) = y^a(k+1) - C\left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\hat{x}^a(k) \end{cases} \tag{10}$$

where $\hat{x}^a(k+1) = \left[\hat{V}_1^a(k+1), \hat{f}_1^a(k+1), \ldots, \hat{V}_n^a(k+1), \hat{f}_n^a(k+1)\right]$ denotes$\hat{x}(k+1)$ under attacks at time $k+1$, and $z^a(k)$ denotes $z(k)$ under attacks at time k. Define $\Delta\hat{x}(k+1)$ and $\Delta z(k+1)$, which denote state estimation difference and the estimation residual difference, respectively. And the dynamic expression of $\Delta\hat{x}(k+1)$ and $\Delta z(k+1)$ can be obtained as

$$\begin{aligned} \Delta\hat{x}(k+1) &= \hat{x}^a(k+1) - \hat{x}(k+1) \\ &= \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\Delta\hat{x}(k) + K\Delta z(k+1) \\ &= \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\Delta\hat{x}(k) \\ &\quad - KC\left(I_n - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\Delta\hat{x}(k) \\ &\quad + KC(x^a(k+1) - x(k+1)) \\ &= (I_{N\times n} - KC)\left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\Delta\hat{x}(k) \\ &\quad + KC(x^a(k+1) - x(k+1)) \end{aligned} \tag{11}$$

$$\begin{aligned} \Delta z(k+1) &= z^a(k+1) - z(k+1) \\ &= -C\left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\hat{x}^a(k) \\ &\quad + C\left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\hat{x}(k) \\ &\quad + y^a(k+1) - y(k+1) \\ &= -C\left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\Delta\hat{x}(k) \\ &\quad + C(x^a(k+1) - x(k+1)) \end{aligned} \tag{12}$$

where $\hat{x}(k+1) = \left[\hat{V}_1^T(k+1), \hat{f}_1^T(k+1), \ldots, \hat{V}_1^T(k+1), \hat{f}_1^T(k+1)\right]^T$, and $x^a(k+1) - x(k+1) \neq 0$ represents the iteration process of $\Delta\hat{x}(k+1)$ and $\Delta z(k+1)$ has been affected by the unbounded attack sequence $\Theta(k)$. The attack sequence $\Theta(k)$ that depends on $\Delta\hat{x}(k)$ can satisfy $\lim_{k\to\infty}\|\Delta\hat{x}(k)\| \to \infty$ and $\lim_{k\to\infty}\|\Delta z(k)\| \leq M$ simultaneously, where M is a positive predetermined detection threshold. $\lim_{k\to\infty}\|\Delta\hat{x}(k)\| \to \infty$ represents that with the iteration of discrete time k, the voltage and frequency state estimation under unbounded attacks gradually deviates from the normal value. Since $\lim_{k\to\infty}\|\Delta\hat{x}(k)\| \to \infty$ and the generation process of $\Theta(k)$ depend upon $\Delta\hat{x}(k)$, $\lim_{k\to\infty}\|\Theta(k)\| \to \infty$ can be achieved. This study considers that $\Theta(0) = 0$ and the attack generation algorithm will be proposed later. $\lim_{k\to\infty}\|\Delta z(k)\| \leq M$ represents $\lim_{k\to\infty}\|\Delta\hat{x}(k)\| \to \infty$, the unbounded attack sequence $\Theta(k)$ will not trigger the traditional χ^2 detection.

The work of Hu et al. (2018) also inspires that protecting key communication channels can detect this stealthy unbounded attack sequence. Currently, phase measurement units (PMUs) are the most common equipment to protect communication channels (Mabaning et al., 2017; Tahabilder et al., 2017; Pei et al., 2020), which are more reliable than detectors. Algorithms detecting and isolating attacks often need to

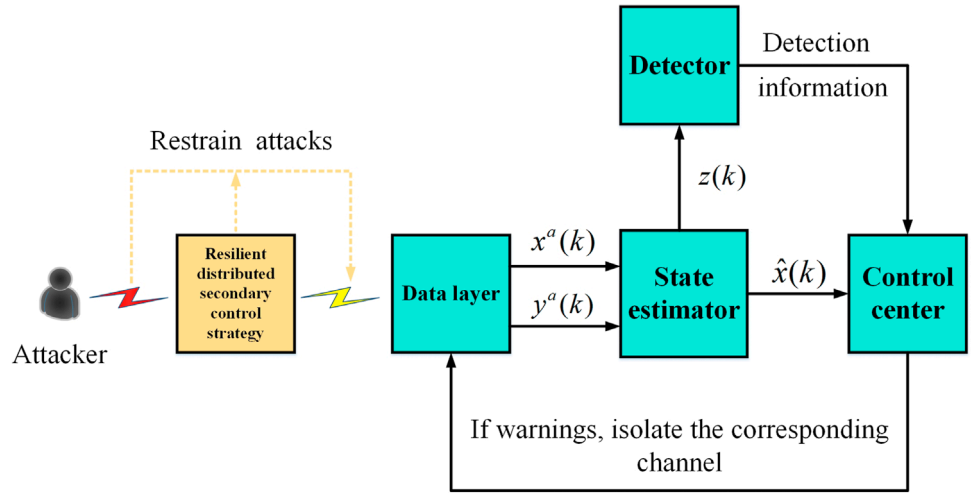

FIGURE 2
Function of the resilient-distributed control method proposed in this study in the process of unbounded attacks generation, state estimation, and detection.

consume a lot of computing resources, and the detection and isolation process that relies on the limited number of PMUs always has a certain time delay. The unbounded attack sequence which depends on $\Delta\hat{x}(k)$ will cause irreversible damage to the microgrid during the process. This study proposes a discrete-time resilient distributed secondary control strategy based on a layered network to greatly suppress the divergence degree of $\Delta\hat{x}(k)$ during the process, and the impact $\Theta(k)$ can cause will be equal to a bounded attack sequence accordingly. It can be seen from Eqn. 11 that although $x^a(k+1)$ and $x(k+1)$ are extremely close under the strategy proposed in this study, $x^a(k+1)-x(k+1)$ keeps accumulating during the iteration process of $\Delta\hat{x}(k+1)$, and $\Delta\hat{x}(k+1)$ still will tend to diverge after a long enough time. As shown in Figure 2, the strategy proposed in this study plays an essential role in the period from the beginning of FDI attack generation to the end of detection and isolation measures to enhance the resilience of the microgrid against attacks.

The following assumptions are made in this study:

Assumption 1: This monotonous unbounded attack sequence can generate at a limited rate, in other words, $\left\|\frac{a(k+1)-a(k)}{T}\right\| \le c$, where c is a positive scalar.

Assumption 2: FDI attacks cannot be launched on sensor devices directly, but only in sensor communication networks.

Assumption 3: The attacker has perfect knowledge about the system model, that is, information the attacks generation algorithm requires can be obtained by the attacker.

3.3 Resilient-distributed secondary strategy based on the layered communication network

This section introduces a virtual layer Σ_h based on the layered network (Gusrialdi et al., 2018) to interconnect with the original control layer Σ_s to form a layered communication network to enhance the resilience of the control layer Σ_s against unbounded FDI attacks, the layered network is shown in Figure 3, where the virtual layer Σ_h has no physical meaning, and it would be difficult for adversaries to associate the information in the virtual layer Σ_h with the measurements of voltage and frequency in the control layer Σ_s. There exist studies that have investigated attacks in the virtual layer Σ_h, but it is obvious that adversaries need more computing resources to launch attacks in the virtual layer Σ_h. Therefore, most work based on the layered network prefer to study attacks in the control layer Σ_s. The discrete-time resilient distributed secondary control strategy proposed in this study considers the unbounded attack sequence launched in the control layer Σ_s, and Lyapunov theory is used to validate the stability of the strategy in this section.

The layered network consisting of the control layer Σ_s and the virtual layer Σ_h can be shown in Figure 3. The control layer Σ_s and the virtual layer Σ_h have the same number of nodes, and the reference information is transmitted to the nodes in the control layer Σ_s and virtual layer Σ_h at the same time. After the unbounded attack sequence is launched in the control layer Σ_s, the layered network will generate a compensation sequence through the observer constituted by Eqs. 14, 15 so that the

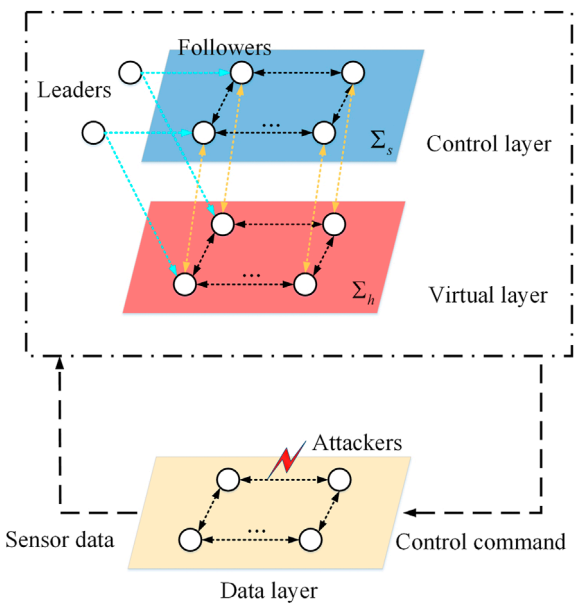

FIGURE 3
Structure of the layered communication network formed by introducing a virtual network layer.

control layer Σ_s as shown in Eqn. 13 can resist the impact of the unbounded attack sequence $\Theta(k)$.

$$x(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)x(k) + T\left(\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l' + \Theta(k) - \hat{\Theta}(k)\right), \quad (13)$$

$$\eta(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)\eta(k) + T\left(\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l'\right), \quad (14)$$

$$\hat{\Theta}(k+1) = T\left(\sum_{l=1}^{m}(\beta_l \otimes I_e)v(k) + \hat{\Theta}(k)\right), \quad (15)$$

where $\eta(k) = [\eta_1^T(k), \eta_2^T(k), \ldots, \eta_n^T(k)]^T$ denotes the state of nodes in the virtual network layer Σ_h, $v(k) = x(k) - \eta(k)$ denotes the difference between the control layer Σ_s and the virtual layer Σ_h at time k, and $\hat{\Theta}(k) = [\hat{\Theta}_1^T(k), \hat{\Theta}_2^T(k), \ldots, \hat{\Theta}_n^T(k)]^T$ denotes the compensation sequence. It can be seen that Eqs. 14, 15 together form an observer to generate a compensation sequence through which the impact of unbounded attack sequence in the control layer can be eliminated. Define errors between information in the leader node and that in the nodes of control layer Σ_s and virtual layer Σ_h as (16) and (17) respectively:

$$e_1(k) = x(k) - \left(\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)^{-1}\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l', \quad (16)$$

$$e_2(k) = \eta(k) - \left(\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)^{-1}\sum_{l=1}^{m}(\beta_l \otimes I_e)x_l'. \quad (17)$$

Theorem 1: When the unbounded attack sequence $\Theta(k)$ which depends on state estimation difference satisfying assumption 1 has been launched in the communication network of microgrid as shown in Eqn. 5, the resilient distributed secondary control strategy based on the layered network as shown in Eqs. 13–15 is designed to resist the impact $\Theta(k)$ can cause. If $e_1(k)$ in Eqn. 16 is stable, it can be said that the control layer Σ_s shown in Eqn. 13 can resist the unbounded attack sequence $\Theta(k)$ and maintain voltage and frequency stable.

Proof: Define $\tilde{\Theta}(k) = \Theta(k) - \hat{\Theta}(k) = [\tilde{\Theta}_1^T(k), \tilde{\Theta}_2^T(k), \ldots, \tilde{\Theta}_N^T(k)]^T$, and make the difference between Eqs. 13, 14 to obtain Eqn. 18:

$$v(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)v(k) + T\tilde{\Theta}(k). \quad (18)$$

Eqn. 19 can be obtained from Eqn. 15:

$$\begin{aligned}\frac{\tilde{\Theta}(k+1) - \tilde{\Theta}(k)}{T} &= \frac{\Theta(k+1) - \Theta(k)}{T} - \frac{\hat{\Theta}(k+1) - \hat{\Theta}(k)}{T} \\ &= -\sum_{l=1}^{m}(\beta_l \otimes I_e)v(k) + \hat{\Theta}(k+1) - \hat{\Theta}(k) \\ \tilde{\Theta}(k+1) - \tilde{\Theta}(k) &= \left(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e)\right)v(k) \\ &\quad + T\left(\hat{\Theta}(k+1) - \hat{\Theta}(k)\right)\end{aligned}. \quad (19)$$

Rewriting Eqs. 18, 19 in the following compact form yields

$$\begin{bmatrix} v(k+1) \\ \tilde{\Theta}(k+1) \end{bmatrix} = \begin{bmatrix} I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e) & I_{N\times n} \\ I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e) & 0_{N\times n} \end{bmatrix}\begin{bmatrix} v(k) \\ \tilde{\Theta}(k) \end{bmatrix} + \begin{bmatrix} 0_{(N\times n)\times 1} \\ T(\Theta(k+1) - \Theta(k)) \end{bmatrix}. \quad (20)$$

Define $m(k) = \begin{bmatrix}\tilde{\Theta}^T(k) & v^T(k)\end{bmatrix}^T$, $m(k+1) = \begin{bmatrix}\tilde{\Theta}^T(k+1) & v^T(k+1)\end{bmatrix}^T$, and $m(k+1) = A_2 m(k)$, where $A_2 = \begin{bmatrix} I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e) & I_{N\times n} \\ I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e) & 0_{N\times n} \end{bmatrix}$. Choose a Lyapunov function candidate as

$$V_d(k) = [T(\Theta(k+1) - \Theta(k))]^T[T(\Theta(k+1) - \Theta(k))]. \quad (21)$$

Given assumption 1, $\lim_{k\to\infty}\Theta(k) = \infty$ is a monotonous and limited-growth unbounded attack sequence, and $\Theta(0) = 0$. Therefore, $V_d(k) = T^2\|(\Theta(k+1) - \Theta(k))\|^2$ is positive-definite at arbitrary time k. Next, choose a Lyapunov function candidate to prove the stability of Eqn. 20:

$$V(k) = m^T(k) P_s m(k) + V_d(k). \tag{22}$$

where $P_s > 0$ is an arbitrary symmetric and positive-definite matrix, and $V_d(k) > 0$ is known from Eqn. 21. Therefore, $V(k)$ is positive-definite at arbitrary time k. The difference form of Eqn. 22 is can be obtained as

$$\begin{aligned} &V(k+1) - V(k) \\ &\quad = m^T(k+1) P_s m(k+1) - m^T(k) P_s m(k) \\ &\qquad + V_d(k+1) - V_d(k) \\ &\quad = (A_2 m(k))^T P_s (A_2 m(k)) - m^T(k) P_s m(k) \\ &\qquad + T^2 \|\Theta(k+2) - \Theta(k+1)\| - T^2 \|\Theta(k+1) - \Theta(k)\|. \\ &\quad = m^T(k) \left(A_2^T P_s A_2 - P_s\right) m(k) \\ &\qquad + T^2 \|\Theta(k+2) - \Theta(k+1)\| - T^2 \|\Theta(k+1) - \Theta(k)\| \\ &\quad = -m^T(k) Q m(k) + T^2 \left(\|\Theta(k+2) - \Theta(k+1)\|^2 \right. \\ &\qquad \left. - \|\Theta(k+1) - \Theta(k)\|^2\right) \end{aligned} \tag{23}$$

There exists a symmetric and positive-definite matrix P_s such that $A_2^T P_s A_2 - P_s < 0$ for an arbitrary symmetric and positive-definite matrix Q. Given assumption 1, $\|\Theta(k+2) - \Theta(k+1)\|^2 \le \|\Theta(k+1) - \Theta(k)\|^2$ can be obtained, that is, $\|\Theta(k+2) - \Theta(k+1)\|^2 - \|\Theta(k+1) - \Theta(k)\|^2 \le 0$. Through the aforementioned analysis, $V(k+1) - V(k) < 0$ can be obtained at arbitrary time k. Therefore, $v(k)$ and $\tilde{\Theta}(k)$ are stable. From Eqs. 16, 17, $e_1(k) = v(k) + e_2(k)$ can be obtained. In order to prove the stability of $e_1(k)$, the stability of $e_2(k)$ also should be proved. Combine with Eqn. 14, the difference form of Eqn. 17 can be obtained as

$$\begin{aligned} &\frac{e_2(k+1) - e_2(k)}{T} \\ &\quad = \frac{\eta(k+1) - \eta(k)}{T} - 0 \\ &\quad = -\sum_{l=1}^{m} (\beta_l \otimes I_e) \eta(k) + \sum_{l=1}^{m} (\beta_l \otimes I_e) x_l^{'} \\ &\quad = \left(\sum_{l=1}^{m} (\beta_l \otimes I_e)\right) \\ &\qquad \left(-\eta(k) + \left(\sum_{l=1}^{m} (\beta_l \otimes I_e)\right)^{-1} \sum_{l=1}^{m} (\beta_l \otimes I_e) x_l^{'}\right) \\ &\quad = -\sum_{l=1}^{m} (\beta_l \otimes I_e) e_2(k) \\ &e_2(k+1) = \left(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)\right) e_2(k) \end{aligned} \tag{24}$$

Choose a Lyapunov function candidate as $V^{'}(k) = e_2^T(k) P_h e_2(k)$, its difference form can be shown as

$$\begin{aligned} &V^{'}(k+1) - V^{'}(k) \\ &\quad = e_2^T(k+1) P_h e_2(k+1) - e_2^T(k) P_h e_2(k) \\ &\quad = e_2^T(k) \left(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)\right)^T \\ &\qquad P_h \left(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)\right) e_2(k) - e_2^T(k) P_h e_2(k) \\ &\quad = e_2^T(k) \left(\left(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)\right)^T \right. \\ &\qquad \left. P_h \left(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)\right) - P_h\right) e_2(k) \\ &\quad = -e_2^T(k) Q^{'} e_2(k) \end{aligned} \tag{25}$$

There exists a symmetric and positive-definite matrix Q' such that $(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e))^T P_h (I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e)) - P_h = -Q^{'} < 0$, that is, $V'(k+1) - V'(k) < 0$. Therefore, $e_2(k)$ is stable. Since $e_1(k) = v(k) + e_2(k)$, the stability of $e_1(k)$ can be proved. The proof of Theorem 1 has completed here, which indicates the distributed secondary strategy proposed in this study can defend attacks to maintain the voltage and frequency stable.

3.4 Design of the unbounded attack sequence

This section will introduce the generation process of the unbounded attack sequence $\Theta(k)$, and how it destroys the state estimation of microgrid. The specific design principle of parameters required in algorithm is shown in Hu et al. (2018), The generation algorithm of unbounded attack sequence is shown in Table 2. where the length of $I^s_{N\times n}$ is $N \times n$, and all its elements equal to 0 except the *sth* element equal to 1. How to select s can only be determined after the matrix parameters of microgrid are selected, which will be given in the next section. The unbounded attack sequence $\Theta(k) = \frac{1}{T}[(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e))\Delta\hat{x}(k) + \varphi(k) M I^s_{N\times n}]$ depends on the state estimation difference $\Delta\hat{x}(k)$ at time k, and $\varphi(k) M I^s_{N\times n}$ is a constant

TABLE 2 Algorithm for generating an unbounded attack sequence.

Algorithm for generating an unbounded attack sequence

Initialization parameter
Define $\Delta\hat{x}(0) = \hat{x}^a(0) - \hat{x}(0)$
Choose a arbitrary $\varphi \in (0,1)$, and the detection threshold $M = 2$
while $k \ge 0$ **do**
Set $\Delta\hat{x}(0) = 0$, $\varphi(0) = 0$
Calculate $\Theta(k) = \frac{1}{T}[(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e))\Delta\hat{x}(k) + \varphi(k) M I^s_{N\times n}]$
Calculate $\Delta\hat{x}(k+1) = [(I_{N\times n} - KC)(I_{N\times n} - T\sum_{l=1}^{m} (\beta_l \otimes I_e))\Delta\hat{x}(k)$
$+KC(x^a(k+1) - x(k+1))]$
$k = k + 1$
$\varphi(k) = \varphi$
end while

column vector. Since the existence of $\varphi(k)MI^s_{N\times n}$, $\Theta(k)$ will make $\|\Delta\hat{x}(k+1)\|$ be continuously increasing after time $k=1$, and $\Delta\hat{x}(k+1)$ will make $\|\Theta(k)\|$ be continuously increasing in turn. Finally, when $\lim_{k\to\infty}\|\Theta(k)\|=\infty$, $\lim_{k\to\infty}\|\Delta\hat{x}(k+1)\|=\infty$. The resilient distributed secondary control strategy proposed in this study, mitigating attacks rather than eliminating them, can restore $x^a(k+1)$ to $x(k+1)$, so that $x^a(k+1)-x(k+1)$ is close to 0. In this way, compared with the distributed secondary control strategy, the resilient strategy proposed in this study can suppress $\Delta\hat{x}(k+1)$ in **Eqn. 11** and $\Delta z(k+1)$ in **Eqn. 12**. Since the unbounded attack sequence $\Theta(k)$ depends on $\Delta\hat{x}(k)$ which is greatly suppressed before detection and isolation mearsures completed, the divergence trend of $\Theta(k)$ is also greatly suppressed. The impact of $\Theta(k)$ can be equaled to that caused by a bounded attack sequence, which greatly alleviates the threat to the microgrid. The resilient distributed secondary strategy proposed in this study only plays a role in the suppression process of $\Theta(k)$ and $\Delta\hat{x}(k)$, but cannot eliminate them completely. To eliminate the impact of this kind of unbounded attack sequence on microgrid, one should find a way to detect and isolate attacks is essential. How to protect key communication channels to detect stealthy unbounded attacks is an interesting topic, and authors will think about how to realize the idea in future research.

4 Case study

In this section, a test microgrid consisting of six inverter-based *DGs* is used to verify the effectiveness of the method proposed in this study against unbounded attack sequence $\Theta(k)$ (Bidram et al., 2013; Xu et al., 2019; Ge et al., 2021). The effectiveness of a resilient distributed secondary control strategy against unbounded attacks is that the voltage and frequency of each DG can still operate within the allowable fluctuation range near the rated value when the neighbor information has tampered. The influence of unbounded attack sequence on microgrids is analyzed by simulation when the elastic distributed secondary control strategy proposed in this study is adopted.

The power layer structure consisting of six inverter-based DGs illustrated in this study is shown in **Figure 4**. And the microgrid parameters are as follows:

$T=0.001s$, $a_{ij}=10$, $g_{li}=0.001$, $N=6$, $n=2,\mathrm{m}=2$, $C=I_{N\times n}=I_{12}$,

$Q=\mathrm{diag}\,(0.01,0.01,0.01,0.001,0.001,0.001,0.01,0.01,0.01,0.001,0.001,0.001)$,

$R=\mathrm{diag}(0.1,0.1,0.1,0.1,0.1,0.1,0.1,0.1,0.1,0.1,0.1,0.1)$,

In the unbounded attack generation algorithm, $\varphi=0.1$, $I^s_{N\times n}=[0,0,1,0,0,0,0,0,0,0,0,0]^T$. Define the reference information vector $x_1=x_2=\begin{bmatrix}380V\\50Hz\end{bmatrix}$, which represents all the DGs need to follow the reference voltage $380V$ and frequency $50Hz$.

First, the distributed secondary control strategy as shown in **Eqn. 4** is used to maintain voltage and frequency stability. Next, the unbounded attack sequence is launched into the communication channels. As shown in **Eqn. 9**, $\Theta(k)$ destroys the iterative process in the form of $T\Theta(k)$. As shown in **Figure 5A**, the unbounded attack sequence given by algorithm 1 can destroy the iterative process of $V_2(k)$, $V_3(k)$, $V_5(k)$, and $V_6(k)$, that is, the voltage consensus performance of DG2, DG3, DG5, and DG6 is destroyed. Information exchange under attacks will make all the DGs' voltage tend to ∞ with the iteration of the sampling time T. **Figure 5B** shows that the frequency of DGs has not been destroyed. Combine with **Figure 5A** and **Figure 5B**, the distributed secondary control strategy is still effective in the absence of $\Theta(k)$, but the voltage consensus performance will be destroyed under $\Theta(k)$.

Figure 6A shows the generation process of $\Theta(k)$ launched in **Figure 5A**. **Figure 6B** shows the voltage estimation difference of DGs under $\Theta(k)$. Since frequency has not been tampered, $\Theta_{i2}(k)=\Delta\hat{f}(k)=0$.

$T\Theta_{ex1}(k)$ denotes $T\Theta_1(k)$ and $T\Theta_4(k)$, and $\Delta\hat{V}_{\mathrm{ex1}}(k)$ denotes $\Delta\hat{V}_1(k)$ and $\Delta\hat{V}_4(k)$. **Figure 6** indicates the generation process of $\Theta_{i1}(k)$ depends on $\Delta\hat{V}(k)$ indeed. Also, then $\Theta_{i1}(k)$ will increase $\Delta\hat{V}(k)$ in turn. However, this phenomenon is profitless for voltage stability. During the period between the initialization of $\Theta(k)$ and completion of detection and isolation measures, the $\Theta(k)$ which diverges rapidly will cause irreversible effects on the microgrid. When the voltage exceeds the rated range allowed by the microgrid, the power circuit breakers inside the microgrid will act to disconnect the main circuit and stop operation. The renewable energy equipment inside the microgrid is expensive, which cannot stand the permanent damage such sudden breakdown causes. Obviously, it is not a wise choice to let such attacks diverge rapidly and put all hope in detection and isolation measures. The resilient distributed secondary control strategy proposed in this study can greatly suppress the divergence of $\Theta(k)$, and prevent the microgrid from being attacked to the point of crash before the completion of the whole process of detection and isolation measures.

It can be seen that $\Theta(k)$ is approximated into an attack sequence with minimal growth rate. Before completion of detection and isolation algorithms, relative to the original divergence, the impact of the suppressed $\Theta(k)$ can cause equal to a bounded attack sequence.

Figure 7 shows the performance of the resilient distributed secondary control strategy proposed in this study against the unbounded attack sequence $\Theta(k)$. It can be seen from **Figure 7A** that the voltage of DGs can still converge to the allowable range of the reference value 380 V under the impact of the unbounded attack sequence $\Theta(k)$. Moreover, **Figure 7B** shows the frequency of DGs can maintain stability, which indicates the resilient distributed secondary control strategy proposed in this study can also achieve the desired control objectives

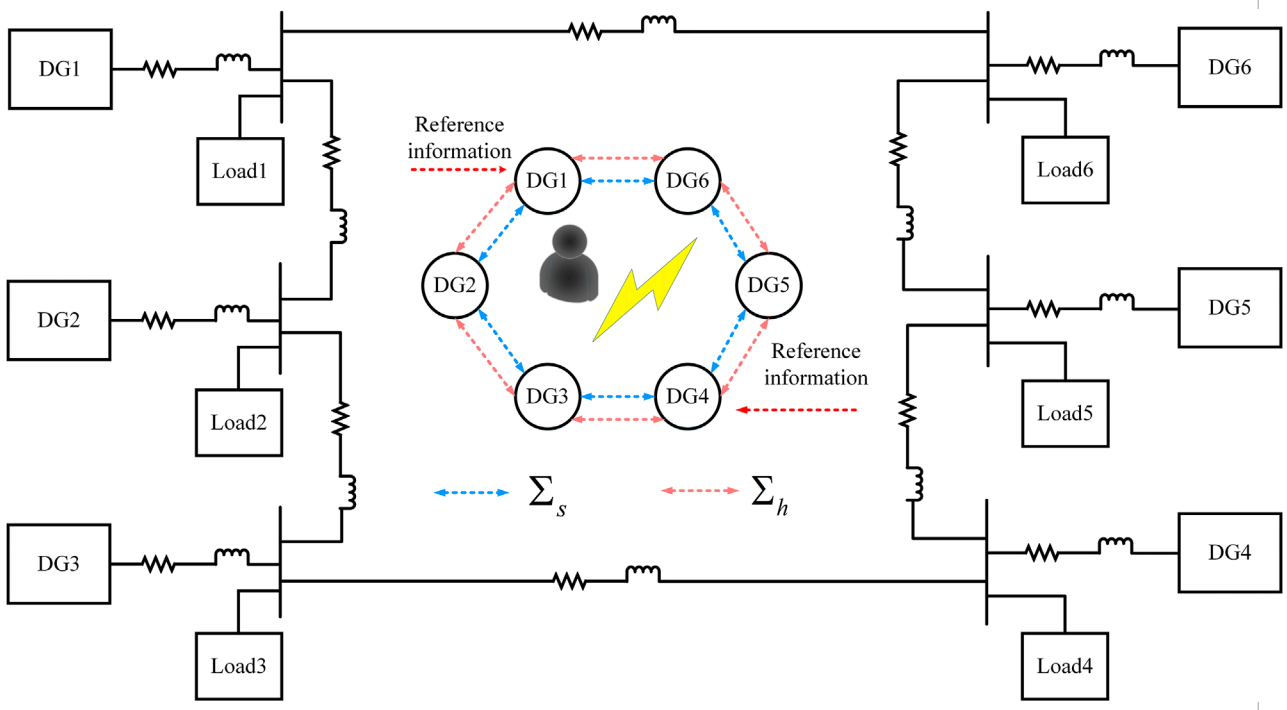

FIGURE 4
Physical structure and communication network topology of the microgrid illustrated in this study.

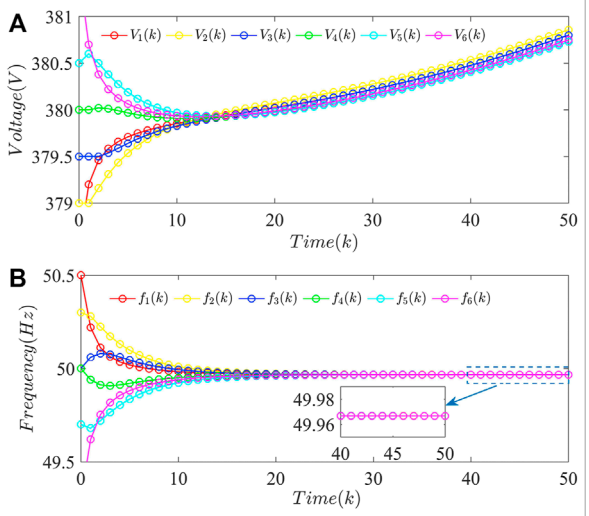

FIGURE 5
Performance of the distributed secondary control strategy against unbounded attack sequence $\Theta(k)$: **(A)** voltage; **(B)** frequency.

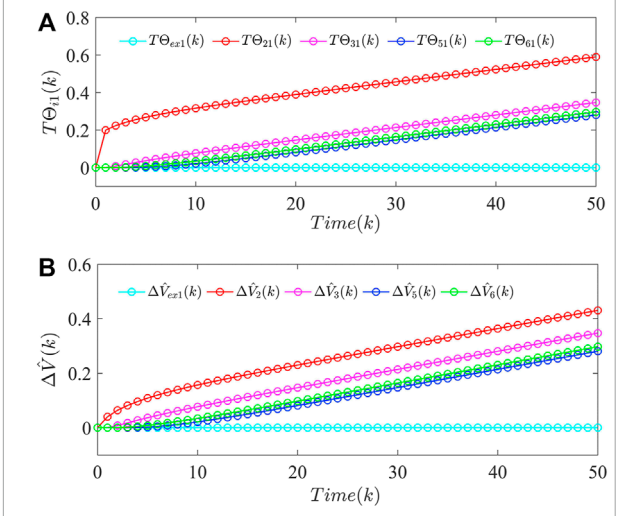

FIGURE 6
(A) Generation process of $\Theta(k)$ in **Figure 5**; **(B)** voltage estimation difference of DGs.

when there exist no attacks. It is worth mentioning that this strategy can make voltage under attacks $V^a(k)$ close to that without attacks $V(k)$, that is, $V^a(k) - V(k)$ is close to 0. Given Algorithm 1, if $\Delta\hat{x}(k)$ can be suppressed, and then $\Theta(k)$ also will be extremely suppressed. **Figure 8** shows the voltage estimation difference $\Delta\hat{V}(k)$ of DGs using the resilient distributed secondary control strategy proposed in this study. Combine with **Figure 6** and **Figure 8**, it is obvious that $\Delta\hat{V}(k)$ can be suppressed by

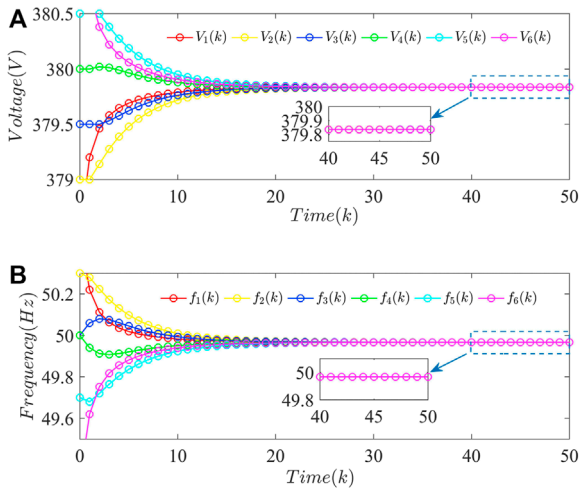

FIGURE 7
Performance of the resilient-distributed secondary control strategy proposed in this study against the unbounded attack sequence $\Theta(k)$: **(A)** voltage; **(B)** frequency.

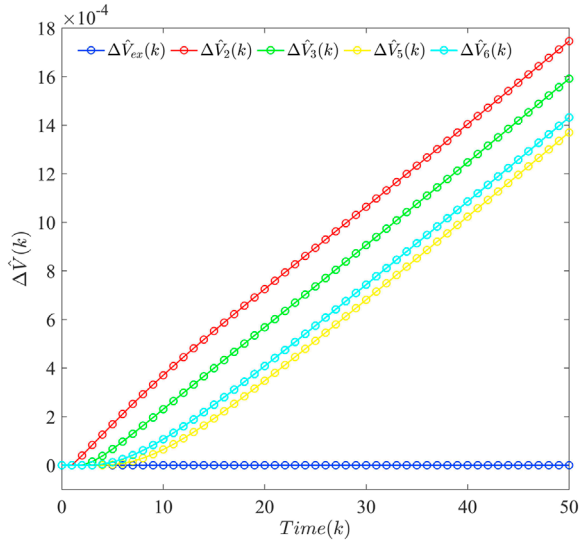

FIGURE 8
Voltage estimation difference using the resilient-distributed secondary control strategy proposed in this study.

the distributed secondary control strategy proposed in this study.

Figure 9 shows performance of the generation process of $\Theta(k)$ which depends on $\Delta\hat{V}(k)$ after the voltage estimation difference $\Delta\hat{V}(k)$ has been suppressed. As shown in Figure 9, the unbounded attack sequence $\Theta(k)$ is approximated into an bounded attack sequence with minimal growth rate under the resilient distributed secondary control strategy. From Eqn. 12, $\|\Delta z_{i1}(k+1)\| = \left\|-C(I_{N\times n} - T\sum_{l=1}^{m}(\beta_l \otimes I_e))\Delta\hat{x}(k) + C(x^a(k+1) - x(k+1))\right\|$ can be obtained. The resilient distributed secondary control strategy suppresses $\Delta\hat{x}(k)$ and $x^a(k+1) - x(k+1)$, which leads to $\|\Delta z_{i1}(k+1)\| < M$ as shown in Figure 10. However, it does not violate the original intention of the resilient distributed secondary control strategy, which is designed to mitigate attacks rather than detect them. It is acceptable to gain greater resilience against unbounded attack sequence at the cost of reducing $\|\Delta z_{i1}(k+1)\|$. The detection and isolation measures, such PMUs, will replace the traditional detectors by protecting key communication channels in the Σ_s to detect $\Theta(k)$. Face to well-designed unbounded attack sequence, how to deploy protection

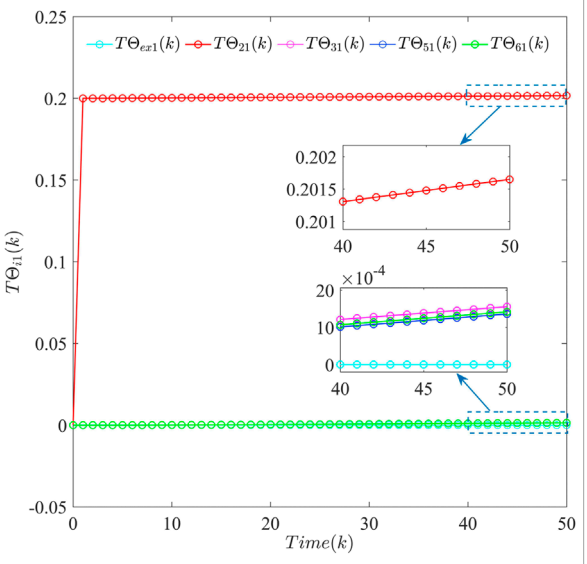

FIGURE 9
Unbounded attack sequence $\Theta(k)$ suppressed by the resilient-distributed secondary control strategy proposed in this study.

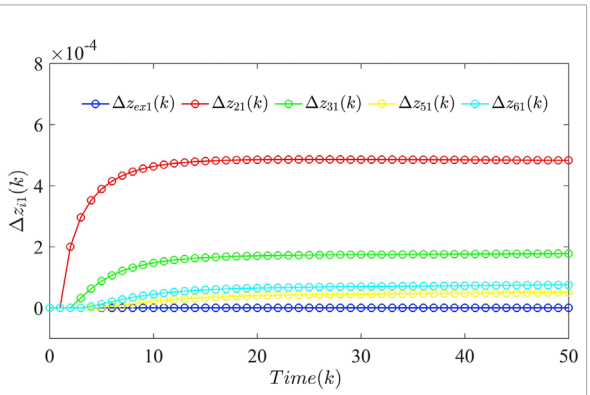

FIGURE 10
Voltage estimation residual difference $\Delta z_{i1}(k)$ of DGs using the resilient-distributed secondary control strategy proposed in this study.

devices in the minimum number of key communication channels has become an important topic in future research. One of authors' future work is how to integrate mitigation and detection processes to solve the problem of such unbounded attack sequence $\Theta(k)$ completely.

5 Conclusion

This study has studied the impact of a class of unbounded attack sequence $\Theta(k)$ launched in the polymorphic cooperative control system. A discrete-time resilient distributed secondary control strategy based on the layered network has been used to restore the voltage and frequency under attacks and suppress the divergence of state estimation difference. At the same time, $\Theta(k)$ depending on state estimation difference has also been suppressed, and its destructiveness has been limited to the level of a bounded attack sequence. The strategy proposed in this study is suitable for the process between the initialization of generating attacks and completion of detection and isolation measures to alleviate the irreversible impact on the microgrid. The effectiveness of a resilient distributed secondary control strategy against unbounded attacks has been validated by a test microgrid consisting of six inverter-based DGs. The authors will focus on how to integrate mitigation, detection, and isolation processes into a more complete and effective strategy against unbounded attacks.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

FW and QS designed the experiments and research methods. QS performed the format analysis. The tools analysis, data processing, and writing the original draft were carried out by JZ. GX solved the application problem of research methods. GX performed the writing—review on references. JZ and QS contributed to proofreading and organization management.

Funding

This work is supported in part by the National Key R&D Program of China (2019YFB1802501), the Key Research Project of Zhejiang Lab (2021LE0AC02), the High-Level Talents Innovation Support Plan of Dalian (Young Science and Technology Star Project) (under Grant No. 2021RQ058), the National Natural Science Foundation of China (under Grant Nos. 51939001, 61803064, 61751202, 61903092, 61976033, and U1813203), the Science and Technology Innovation Funds of Dalian (under Grant No. 2018J11CY022), the Liaoning Revitalization Talents Program (under Grant Nos. XLYC1908018 and XLYC1807046), the Natural Science Foundation of Liaoning (2019-ZD-0151 and 20170540098), and the Fundamental Research Funds for the Central Universities (under Grant Nos. 3132019345, 3132020103, and 3132020125).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abhinav, S., Modares, H., Lewis, F. L., Ferrese, F., and Davoudi, A. (2018). Synchrony in networked microgrids under attacks. *IEEE Trans. Smart Grid* 9, 6731–6741. doi:10.1109/TSG.2017.2721382

Bidram, A., Davoudi, A., Lewis, F. L., and Guerrero, J. M. (2013). Distributed cooperative secondary control of microgrids using feedback linearization. *IEEE Trans. Power Syst.* 28, 3462–3470. doi:10.1109/TPWRS.2013.2247071

Bidram, A., Lewis, F. L., and Davoudi, A. (2014). Distributed control systems for small-scale power networks: Using multiagent cooperative control theory. *IEEE Control Syst. Mag.* 34, 56–77. doi:10.1109/MCS.2014.2350571

Chen, Y., Qi, D., Dong, H., Li, C., Li, Z., Zhang, J., et al. (2021). A fdi attack-resilient distributed secondary control strategy for islanded microgrids. *IEEE Trans. Smart Grid* 12, 1929–1938. doi:10.1109/TSG.2020.3047949

Condry, M. W., and Nelson, C. B. (2016). Using smart edge iot devices for safer, rapid response with industry iot control operations. *Proc. IEEE* 104, 938–946. doi:10.1109/JPROC.2015.2513672

Dutta, R. G., Zhang, T., and Jin, Y. (2019). "Resilient distributed filter for state estimation of cyber-physical systems under attack," in 2019 American Control Conference (ACC), 5141–5147. doi:10.23919/ACC.2019.8815298

Fawzi, H., Tabuada, P., and Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Contr.* 59, 1454–1467. doi:10.1109/TAC.2014.2303233

Gao, S., Peng, Z., Liu, L., Wang, D., and Han, Q.-L. (2022). Fixed-time resilient edge-triggered estimation and control of surface vehicles for cooperative target tracking under attacks. *IEEE Trans. Intell. Veh.* 1, 1–10. doi:10.1109/TIV.2022.3184076

Ge, P., Zhu, Y., Green, T. C., and Teng, F. (2021). Resilient secondary voltage control of islanded microgrids: An eskbf-based distributed fast terminal sliding mode control approach. *IEEE Trans. Power Syst.* 36, 1059–1070. doi:10.1109/TPWRS.2020.3012026

Gharesifard, B., and Başar, T. (2012). Resilience in consensus dynamics via competitive interconnections. *IFAC Proc. Vol.* 45, 234–239. doi:10.3182/20120914-2-US-4030.00018

Gusrialdi, A., Qu, Z., and Simaan, M. A. (2018). Competitive interaction design of cooperative systems against attacks. *IEEE Trans. Autom. Contr.* 63, 3159–3166. doi:10.1109/TAC.2018.2793164

Gusrialdi, A., Qu, Z., and Simaan, M. A. (2014). "Robust design of cooperative systems against attacks," in 2014 American Control Conference, 1456–1462. doi:10.1109/ACC.2014.6858789

Hu, L., Wang, Z., Han, Q.-L., and Liu, X. (2018). State estimation under false data injection attacks: Security analysis and system protection. *Automatica* 87, 176–183. doi:10.1016/j.automatica.2017.09.028

Hu, Y., Cui, Z., Li, Z., Dong, Y., Cui, P., and Wu, J. (2022). Construction technologies of polymorphic network environment based on codesign of domain-specific software/hardware. *J. Commun.* 43, 3–13. doi:10.11959/j.issn.1000436x.2022086

Hu, Y., Li, D., Sun, P., Yi, P., and Wu, J. (2020). Polymorphic smart network: An open, flexible and universal architecture for future heterogeneous networks. *IEEE Trans. Netw. Sci. Eng.* 7, 2515–2525. doi:10.1109/TNSE.2020.3006249

Huang, J., Ho, D. W., Li, F., Yang, W., and Tang, Y. (2020). Secure remote state estimation against linear man-in-the-middle attacks using watermarking. *Automatica* 121, 109182. doi:10.1016/j.automatica.2020.109182

Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., Uhlig, S., et al. (2015). Software-defined networking: A comprehensive survey. *Proc. IEEE* 103, 14–76. doi:10.1109/JPROC.2014.2371999

Liu, Y., Li, Y., Wang, Y., Zhang, X., Gooi, H. B., Xin, H., et al. (2022). Robust and resilient distributed optimal frequency control for microgrids against cyber attacks. *IEEE Trans. Ind. Inf.* 18, 375–386. doi:10.1109/TII.2021.3071753

Liu, Y., Ning, P., and Reiter, M. K. (2009). "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 21–32. doi:10.1145/1653662.1653666

Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* 14, 1–33. doi:10.1145/1952982.1952995

Mabaning, A. A. G., Orillaza, J. R. C., and von Meier, A. (2017). "Optimal pmu placement for distribution networks," in 2017 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia), 1–6. doi:10.1109/ISGT-Asia.2017.8378415

Manandhar, K., Cao, X., Hu, F., and Liu, Y. (2014). Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Trans. Control Netw. Syst.* 1, 370–379. doi:10.1109/TCNS.2014.2357531

Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., and Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Commun. Surv. Tutorials* 16, 1617–1634. doi:10.1109/SURV.2014.012214.00180

Pang, Z.-H., Fan, L.-Z., Dong, Z., Han, Q.-L., and Liu, G.-P. (2022). False data injection attacks against partial sensor measurements of networked control systems. *IEEE Trans. Circuits Syst. Ii.* 69, 149–153. doi:10.1109/TCSII.2021.3073724

Pei, C., Xiao, Y., Liang, W., and Han, X. (2020). Pmu placement protection against coordinated false data injection attacks in smart grid. *IEEE Trans. Ind. Appl.* 56, 4381. doi:10.1109/TIA.2020.2979793

Rapp, K., and Nyman, P.-O. (2004). Stability properties of the discrete-time extended kalman filter. *IFAC Proc. Vol.* 37, 1377–1382. doi:10.1016/S1474-6670(17)31420-9

Salah, K., Elbadawi, K., and Boutaba, R. (2012). Performance modeling and analysis of network firewalls. *IEEE Trans. Netw. Serv. Manage.* 9, 12–21. doi:10.1109/TNSM.2011.122011.110151

Tahabilder, A., Ghosh, P. K., Chatterjee, S., and Rahman, N. (2017). "Distribution system monitoring by using micro-pmu in graph-theoretic way," in 2017 4th International Conference on Advances in Electrical Engineering (ICAEE), 159–163. doi:10.1109/ICAEE.2017.8255346

Tang, Z., Yang, Y., and Blaabjerg, F. (2022). Power electronics: The enabling technology for renewable energy integration. *CSEE J. Power Energy Syst.* 8, 39–52. doi:10.17775/CSEEJPES.2021.02850

Wang, X., Luo, X., Zhang, M., Jiang, Z., and Guan, X. (2020). Detection and isolation of false data injection attacks in smart grid via unknown input interval observer. *IEEE Internet Things J.* 7, 3214–3229. doi:10.1109/JIOT.2020.2966221

Wang, R., Sun, Q., Sun, C., Zhang, H., Gui, Y., and Wang, P. (2021). Vehicle-Vehicle Energy Interaction Converter of Electric Vehicles: A Disturbance Observer Based Sliding Mode Control Algorithm. *IEEE Trans. Veh. Technol* 70, 9910–9921. doi:10.1109/TVT.2021.3105433

Xu, Y., Guo, Q., Sun, H., and Fei, Z. (2019). Distributed discrete robust secondary cooperative control for islanded microgrids. *IEEE Trans. Smart Grid* 10, 3620–3629. doi:10.1109/TSG.2018.2833100

Yang, D., Qin, J., Pang, Y., and Huang, T. (2022). A novel double-stacked autoencoder for power transformers dga signals with an imbalanced data structure. *IEEE Trans. Ind. Electron.* 69, 1977–1987. doi:10.1109/TIE.2021.3059543

Zeng, W., and Chow, M.-Y. (2014). Resilient distributed control in the presence of misbehaving agents in networked control systems. *IEEE Trans. Cybern.* 44, 2038–2049. doi:10.1109/TCYB.2014.2301434

Zhang, R., Xiao, G., Shan, Q., Zou, T., Li, D., and Teng, F. (2022). Communication topology reconstruction method for multi-agent cooperative control in polymorphic networks. *J. Commun.* 43, 50–59. doi:10.11959/j.issn.1000436x.2022077

Zhou, J., Sun, H., Xu, Y., Han, R., Yi, Z., Wang, L., et al. (2021a). Distributed power sharing control for islanded single-/three-phase microgrids with admissible voltage and energy storage constraints. *IEEE Trans. Smart Grid* 12, 2760–2775. doi:10.1109/TSG.2021.3057899

Zhou, J., Xu, Y., Sun, H., Li, Y., and Chow, M.-Y. (2020). Distributed power management for networked ac–dc microgrids with unbalanced microgrids. *IEEE Trans. Ind. Inf.* 16, 1655–1667. doi:10.1109/TII.2019.2925133

Zhou, Q., Shahidehpour, M., Alabdulwahab, A., Abusorrah, A., Che, L., Liu, X., et al. (2021b). Cross-layer distributed control strategy for cyber resilient microgrids. *IEEE Trans. Smart Grid* 12, 3705–3717. doi:10.1109/TSG.2021.3069331

Zuo, S., and Yue, D. (2022). Resilient containment of multigroup systems against unknown unbounded fdi attacks. *IEEE Trans. Ind. Electron.* 69, 2864–2873. doi:10.1109/TIE.2021.3066941

Zuo, S., Lewis, F. L., and Davoudi, A. (2020). Resilient output containment of heterogeneous cooperative and adversarial multigroup systems. *IEEE Trans. Autom. Contr.* 65, 3104–3111. doi:10.1109/TAC.2019.2947620