energies

MDPI

Article

A Communication Encryption-Based Distributed Cooperative Control for Distributed Generators in Microgrids under FDI Attacks

Han Fu [1], Wenpei Li [2], Long Qiu [1], Yongheng Ai [1] and Zhixiong Liu [3,*]

[1] State Grid Wuhan Power Supply Company, Wuhan 430070, China; fuhan1@hb.sgcc.com.cn (H.F.); choul@hb.sgcc.com.cn (L.Q.); aiyh4@hb.sgcc.com.cn (Y.A.)
[2] State Grid Hubei Electric Power Research Institute, Wuhan 430062, China; liwp14@hb.sgcc.com.cn
[3] State Key Laboratory of Power Grid Environment Protection, School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China
* Correspondence: zxliu@whu.edu.cn

Abstract: To alleviate the hassle of false data injection (FDI) attacks on distributed generators (DGs) in microgrids, a communication encryption-based distributed cooperative control is proposed in this paper. Compared to the conventional distributed control strategies, the proposed control scheme is simpler with much less complex evaluation mechanism by upgrading the secondary control to a second-order control based on the finite-time control theory while combining an encryption strategy. The proposed algorithm provides constant injections to eliminate the impact of FDI attacks based on a robust communication system. The effectiveness and high efficiency of the proposed control scheme is validated in an IEEE 34 Node Test Feeder system with six DGs as a microgrid cyber-physical system (CPS) under different FDI attacks.

Keywords: microgrid; distributed cooperative control; FDI attack; Paillier homomorphic

Citation: Fu, H.; Li, W.; Qiu, L.; Ai, Y.; Liu, Z. A Communication Encryption-Based Distributed Cooperative Control for Distributed Generators in Microgrids under FDI Attacks. *Energies* **2023**, *16*, 7754. https://doi.org/10.3390/en16237754

Academic Editors: José Matas, Jorge El Mariachet and Sen Tan

Received: 29 October 2023
Revised: 19 November 2023
Accepted: 21 November 2023
Published: 24 November 2023

1. Introduction

With high penetrations of distributed generators (DGs), high-performance communication systems are increasingly accessed into the power grids to forge cyber-physical systems (CPSs) [1–4]. A microgrid is a major component of CPS that can operate in both grid-connected and grid-off modes. Self-commissioning operation is the most outstanding feature of microgrids [5–7]. To ensure the stability of microgrids, hierarchical control schemes, which generally consist of primary layer control, secondary layer control, and tertiary layer control are widely adopted [8–11]. On the basis of the primary stability concern, optimal power efficiencies and other objectives can also be set for hierarchical control.

The hierarchical control comprises centralized and distributed control. By considering communication delays, distributed control exhibits better flexibility and reliability [12,13]. However, distributed control may suffer from cyber-attack issues. The most striking feature of the distributed system is the information propagating and data update between neighbor DGs, which determines that all adjacent DGs are expected to be affected even if one DG is attacked. The distributed feature of DGs can result in the instability of entire microgrids if any one of the nodes in the system is attacked [14]. Network attacks prevent control algorithms from reaching the excepted goals and directly affecting the frequencies and voltages of the system. Attackers directly lead to the collapse of microgrids in more severe cases. Therefore, advanced distributed cooperative control with an anti-cyber-attack mechanism is desired to enhance the safety of microgrids.

False data injection (FDI) is a typical cyber attack that can destabilize the system without causing any tracking errors, since it can easily pass the largest normalized residual tests of the system compared to other types of attacks [15]. To this end, several strategies have been

proposed to enhance the stability of microgrids under FDI attacks [16–23]. In [16], an elastic distributed control algorithm is proposed. The algorithm first detects the existence of attacks, then gradually strips the attacked DG from the communication network. In [17–19], the influence of limited numbers of attackers on microgrids is regarded as interference. Striping the frequency information of the system from noise is investigated to solve the microgrid defense problem. However, this technology requires explicit expressions of disturbance to reflect prominent statistical characteristics. It becomes ineffective when the attack signals are deliberately designed by the attackers. To alleviate this hassle, a trust or confidence-based control strategy is proposed in [20] to reduce the attacks' impact on the systems to ensure the stability and reliability of microgrids. The weights of attacked DGs are reduced by establishing confidence factor strategy during data iteration, while the FDI attacks could destroy communication links and inject false data in the process of information propagating and update. Data encryption is an effective solution to address this issue. If the data is encrypted at the sending place and decrypted at the receiving place, the proceeding data remain correct even if falsified data are injected into the communication channel. In [21,22], an improved Dijk–Gentry–Halevi–Vaikutanathan style of fully homomorphic encryption are proposed. Parallel computation can be achieved via a k-means clustering scheme using fully homomorphic encryption with ciphertext packing technique without extra cost. In [23], a rakerski/Fan-Vercauteren scheme based on high-degree polynomial multiplication is proposed to enhance the computational efficiency in the encryption process. However, most studies on encryption are mainly focused on speed and efficiency, while practical applications of communication encryption technologies for microgrids are rarely considered [21–23].

This paper aims to bridge the research gap by proposing a new distributed cooperative control algorithm based on communication encryption. The main contributions of the paper are listed in the following points:

(1) A new cooperative control algorithm, which can eliminate the impact of FDI attacks to microgrids, is proposed. The frequency of each DGs in the microgrid can be restored to track the reference.
(2) An enhanced second-order control based on the finite-time control theory is proposed. The new higher-order control can restore the stability of the system faster.
(3) The proposed control algorithm is designed based on simple algorithm rather than conventional trust or confidential-based protocol, which can be implemented using inexpensive digital controllers.
(4) The communication protection algorithm used in this paper is based on the Paillier homomorphic encryption strategy, which has never been used for DGs in microgrids.

The rest of this paper is arranged as follows: Section 2 introduces the theoretical basis. The cooperative control strategy and finite time theory of the microgrid CPS are presented in Section 3. A new distributed cooperative control algorithm based on communication encryption is designed after analyzing the impact of attacks on the system in Section 4. Comparative studies under different attack conditions using the IEEE 34 Node Test Feeder system are presented in Section 5. The conclusions are drawn in Section 6.

2. Theoretical Basis

2.1. Priliminary of Graph Theory

We let $G = (V, E)$ signify the graph of the cyber network. There are a set of nodes $V = (v_1, v_{2,\ldots}, v_n)$ in the network topology diagram which represent the local DGs within the microgrid. A series of edges $E \subseteq V \times V$ denote the communication links between DGs. If node *vi* can receive information from node *vj*, node *vj* is named as the neighbor node to node *vi*. Laplacian matrix L of network graph G is defined as

$$L = \mathrm{diag}\left\{\sum_{j=1}^{n} d_{ij}\right\} - A, \quad (1)$$

where matrix $A = [a_{ij}]$ represents the adjacency matrix. $a_{ij} = 1$ if node vi can receive information from neighbor node vj. Otherwise, $a_{ij} = 0$. diag$(\cdot)$ is the diagonal function.

2.2. Priliminary of Lyapunov Stabiliy of DG Frequencies

Lemma 1 ([24]). *We choose a suitable Lyapunov function V (x) as*

$$\dot{V}(x) \leq -KV(X)^{\varphi}, \tag{2}$$

where $K > 0$ and $0 < \varphi < 1$. Then, the frequency of each DG in the microgrid is converged in a finite time T, as

$$T \leq T_{max} = \frac{v^{1-e}(0)}{K(1-\varphi)}. \tag{3}$$

3. Cooperative Control of DGs in Microgrids

3.1. Primary Droop Control

Droop control is mainly applied in power controllers to control the output active and reactive power of inverters in microgrid CPS. The underlying communication network model adopted by the primary control is shown in Figure 1, where the orange lines represent the communication links between DGs. The droop control exists in the DG i module, where $i = 1, 2, \ldots, n$.

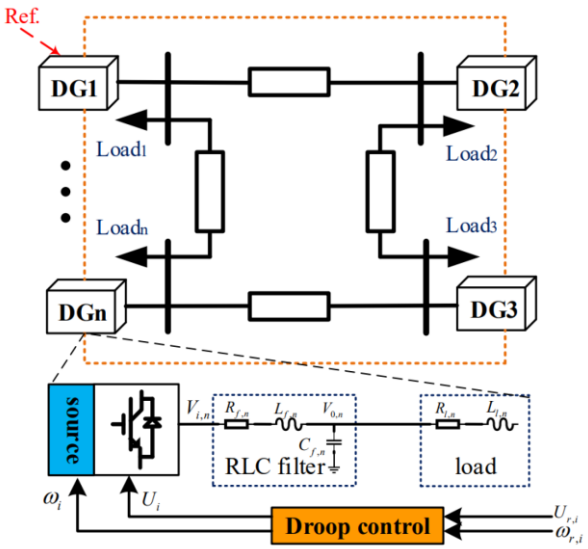


Figure 1. Electrical and communication networks for a typical microgrid CPS.

According to the operation law of the AC microgrid, the connection between active power-angular frequency and reactive power-voltage can be obtained as

$$\begin{cases} w_i = w_{r,i} - m_{p,i}P_i \\ U_i = U_{r,i} - n_{q,i}Q_i \end{cases}, \tag{4}$$

where w_i and U_i are the output angular frequency and voltage of inverter i, where $i = 1, 2, \ldots, n$. P_i and Q_i denote the active and reactive power of inverter i. $m_{p,i}$ and $n_{q,i}$ denote the active and reactive droop coefficients through the rating of inverter i. $w_{r,i}$ and $U_{r,i}$ are the primary control references.

3.2. Secondary Cooperative Control

Cooperative secondary control eliminates the frequency deviation due to droop control. In this paper, the main objective is to design a distributed secondary control scheme for

microgrid CPS under FDI attacks. The following condition needs to be satisfied when the microgrid CPS is stable.

$$\lim_{t\to\infty}\left|w_i - w_{raf}\right| = 0, \tag{5}$$

where $i = 1, 2, \ldots n$, w_{raf} represents reference frequency.

To achieve the above control objectives using distributed cooperative control, the microgrid frequency recovery problem containing n DGs can be converted to a tracking and synchronization problem for a first-order linear multi-intelligent. The inputs to the controller need to be designed by

$$u_i = \dot{w}_i = \dot{w}_{r,i} - m_{p,i}\dot{P}_i, \tag{6}$$

where u_i is the inputs to the controller, $\dot{w}_i$, $\dot{w}_{r,i}$, and $\dot{P}_i$ represent the differentials of w_i, $w_{r,i}$ and P_i. According to Lemma 1, when (6) satisfies Lyapunov stability, the stable point is zero of the function and (6) converges within a finite time.

4. Distributed Cooperative Control for DGs in Microgrids under FDI Attacks

It is critical to ensure the frequency stability of a microgrid with multiple DGs. The secondary frequency control is designed to ensure frequency stability. Unlike centralized control, distributed control lacks a relatively stable control center and relies on the cooperation among DGs to maintain system frequency. Constant FDI attacks fail the distributed control in achieving the objectives since the frequency of the microgrid is easy to be deviated. The size of the attack vectors can be arbitrary, and the attack paths are also uncertain. In this paper, a new distributed cooperative control algorithm is proposed to resist the attacks based on the models of consistent FDI attacks.

4.1. Attack Models

In microgrids, FDI attacks can be classified into two categories: (i) controller existing in the underlying model and (ii) communication links between the two DGs. Among them, controller attacks include two situations: the entire controller is hijacked by the attacker, and the controller inputs (actuators) are fabricated due to the falsified data.

The attacks on control inputs can be modeled as

$$u_i^c = u_i + \mu_i u_i^a, \tag{7}$$

where u_i^a is the FDI attack on actuator i. u_i^c is the control input. u_i is the corresponding control input based on (6). $\mu_i = 1$ represents the presence of attack, while $\mu_i = 0$ represents the absence of attack.

If the controller is hijacked, the frequency of the system is affected. Malicious damage to the controller can be modeled as

$$w_i^c = w_i + \eta_i w_i^a, \tag{8}$$

where w_i^a is the frequency deviation caused by the attacker in (6). w_i^c is fallacious frequency. $\eta_i = 1$ represents the presence of attack, while $\eta_i = 0$ represents the absence of attack.

If the communication links between two DGs is attacked, the controller receives false frequency data from the attackers. When the communication link is deliberately compromised, the system control input can be modeled as

$$w_i^{\dot{c}} = w_i + \eta_i w_i^{\beta}, \tag{9}$$

where w_i^{β} is the FDI attack caused by the attacker into the communication link. $w_i^{\dot{c}}$ is the frequency of DGs being transmitted on the communication link. $\eta_i = 1$ represents the communication link being under attack; otherwise, $\eta_i = 0$ represents the absence of attack.

4.2. Distributed Cooperative Control Algorithm Design and Stability Analysis under an FDI Attack

To remove negative results of an FDI attack on secondary control with constant injection, a second-order improved distributed cooperative control strategy based on finite-time control theory is adopted as

$$u_i = -\alpha \int [\sum_{i,j=1}^{n} a_{ij}\mathrm{sgn}(w_i - w_j)^{\varphi} + g_i\mathrm{sgn}(w_{ref} - w_i)^{\varphi}]dt - w_i, \tag{10}$$

where $\alpha > 1$, $0 < \varphi < 1$, $\mathrm{sgn}(l)^{\varphi}$ denotes function $\mathrm{sgn}(l)^{\varphi}|l|^{\varphi}$. $|l|$ represents the absolute value of l. $\mathrm{sgn}(\cdot)$ is the sign function, which is defined as

$$\mathrm{sgn}(l) = \begin{cases} 1, & l > 0 \\ 0, & l = 0 \\ -1, & l < 0 \end{cases}. \tag{11}$$

Lemma 2 ([24]). *For an undirected figure G, and if $a_{ij} = a_{ji}$ is an odd function,*

$$\sum_{i,j=1}^{n} a_{ij}\mathrm{sgn}(x_j - x_i) = -\frac{1}{2}\sum_{i,j=1}^{n} a_{ij}(x_i - x_j)\mathrm{sgn}(x_j - x_i). \tag{12}$$

Lemma 3 ([25]). *We let $\xi_1, \xi_2, \ldots, \xi_n \geq 0$, $0 < \theta < 1$; then,*

$$\sum_{i=1}^{n} \xi_i^{\theta} \geq \sum_{i=1}^{n} (\xi_i)^{\theta}. \tag{13}$$

Lemma 4 ([26]). *For an undirected graph G, the properties of Laplacian matrix $\hat{L} + diag\left(\hat{b}\right)$ are as follows:*

$$x^T\left(\hat{L} + \mathrm{diag}\left(\hat{b}\right)\right)x = \frac{1}{2}\sum_{i,j=1}^{n} a_{ij}(x_i - x_j)^2 + \sum_{i=1}^{n} b_{ij}(x_i)^2, \tag{14}$$

where x is the state variables of units. a_{ij} indicates whether node vi can receive information from neighbor node vj, as described in (1). b_{ij} indicates whether node vi can send information to neighbor node vj. L is the Laplacian matrix of network graph G.We donate the smallest eigenvalue of the Laplacian matrix by $\widetilde{\lambda}\left(\hat{L} + diag\left(\hat{b}\right)\right)$; then, we have

$$x^T\left(\hat{L} + \mathrm{diag}\left(\hat{b}\right)\right)x \geq \widetilde{\lambda}\left(\hat{L} + \mathrm{diag}\left(\hat{b}\right)\right)x^T x. \tag{15}$$

Theorem 1. *When Control algorithm (10) is adopted, the frequency of each DG in a microgrid is consistent within a finite time.*

Proof. The Lyapunov function is selected as follows:

$$V = \frac{1}{2}\delta_v^T\delta_v = \frac{1}{2}\sum_{i=1}^{n}\delta_{vi}^2. \tag{16}$$

The derivative function of the Lyapunov function can be expressed as

$$\dot{V} = \sum_{i=1}^{n}\delta_{vi}\dot{\delta}_{vi}. \tag{17}$$

By defining $\dot{\delta}_v = u_i + w_i$, the control algorithm can be rewritten as

$$\dot{\delta} = \frac{d(u_i + w_i)}{dt} = \propto \left[\sum_{j\in Ni} a_{ij}\mathrm{sgn}(w_i - w_j)^{\varphi} + g_i\mathrm{sgn}(w_{ref} - w_i)^{\varphi}\right]. \tag{18}$$

We define the new adjacency matrix of undirected graph G as $\hat{A} = [a_{vij}]_{n*n}$, where $a_{vij} = (\alpha a_{ij})^{\frac{2}{1+\varphi}}$. $\hat{L}$ represents the Laplacian matrix, and $\mathrm{diag}\left(\hat{b}\right) = [b_{vi}]_{m*n}$, where $b_{vi} = -(\alpha g_i)^{\frac{2}{1+\varphi}}$. Then, (18) can be reorganized as

$$\dot{\delta}_v = \sum_{ij=1}^{n} a_{vij}^{\frac{1+\varphi}{2}} \mathrm{sgn}(\delta_{vj} - \delta_{vi})^{\varphi} - b_{vij}^{\frac{1+\varphi}{2}} \mathrm{sgn}(\delta_{vi})^{\varphi}. \tag{19}$$

Based on (16)–(19), the derivative function of the Lyapunov function can be derived as

$$\dot{V} = \sum_{i=1}^{n} \delta_{vi} [\sum_{i,j=1}^{n} a_{vi}^{\frac{1+\varphi}{2}} \mathrm{sgn}(\delta_{vj} - \delta_{vi})^{\varphi} - b_{vi}^{\frac{1+\varphi}{2}} \mathrm{sgn}(\delta_{vi})^{\varphi}]. \tag{20}$$

Based on Lemma 2, (20) can be further simplified as

$$\dot{V} = -\frac{1}{2} [\sum_{i,j=1}^{n} a_{vj} \left(\delta_{vj} - \delta_{vi}\right) sig(\delta_{vj} - \delta_{vi})^{\frac{2\varphi}{1+\varphi}}]^{\frac{1+\varphi}{2}} - \left[\sum_{i=1}^{n} b_{vi} \delta_{vi} \mathrm{sgn}(\delta_{vi})^{\frac{2\varphi}{1+\varphi}}\right]^{\frac{1+\varphi}{2}}. \tag{21}$$

Based on Lemmas 3 and 4, the upper bound of (20) or (21) can be derived as

$$\begin{aligned} \dot{V} &\leq -\tfrac{1}{2} \left[\sum_{i,j=1}^{n} a_{vij} \left(\delta_{vj} - \delta_{vi}\right)^2 + 2\sum_{i=1}^{n} b_{vi} (\delta_{vi})^2\right]^{\frac{1+\phi}{2}} \\ &\leq -\left[\sum_{i,j=1}^{n} a_{vij} \left(\delta_{vj} - \delta_{vi}\right)^2 + \sum_{i=1}^{n} b_{vi} (\delta_{vi})^2\right]^{\frac{1+\varphi}{2}} \\ &\leq -\tfrac{1}{2} \left[2x_2 (L^v + \mathrm{diag}(b^v)) \delta_v^{\mathrm{T}} \delta_v\right]^{\frac{1+\varphi}{2}} \\ &\leq -\tfrac{1}{2} [4x_2 (L^v + \mathrm{diag}(b^v)) V]^{\frac{1+\varphi}{2}} \\ &\leq 0 \end{aligned}. \tag{22}$$

According to Lemma 1, $K = \frac{1}{2} 4x (L^v + \mathrm{diag}(b^v))]^{\frac{1+\varphi}{2}}$ can be defined. Then, the derivative of the Lyapunov function in (22) can be derived as

$$\dot{V} \leq -K[V]^{\frac{1+\varphi}{2}}. \tag{23}$$

Finally, the frequency of the DGs in the microgrid can reach an agreement in a finite time T_v as

$$T_v \leq \frac{2V^{\frac{1-\varphi}{2}}(0)}{K(1-\varphi)}. \tag{24}$$

□

4.3. Paillier Encryption Algorithm

Homomorphic cryptography allows certain arithmetic operations on the ciphertext. Paillier encryption is a cryptographic encryption that can be directly used to calculate the key without affecting the correctness of decryption [27]. Thus, it has been widely adopted in applications such as distributed optimizations, status estimations, etc. [28]. The Paillier Encryption Algorithm mainly comprises three parts, which can be described as follows:

We assume p and q are large prime numbers with the same length, while $\mathrm{lcm}(p-1)(q-1)$ represents the least common multiple of $p-1$ and $q-1$. We define function

$$\gamma(x) = \frac{x-1}{\hat{n}}, \tag{25}$$

where $\hat{n} = pq$ and x needs to satisfy

$$\forall x \in \left\{x < \hat{n}^2 \mid x = 1 \bmod \hat{n}\right\}. \tag{26}$$

Then, the mutually prime integers of $\hat{n}^2$ (i.e., g) and the control input (i.e., μ) can be obtained by calculating

$$\begin{cases} g = \hat{n} + 1 \\ \mu = \zeta(\hat{n})^{-1} \bmod \hat{n}' \end{cases} \tag{27}$$

where $\zeta(\hat{n}) = (p-1)(q-1)$.

It is worth noting that random primes p and q are continuously generated until g and μ being calculated from (25)–(27) satisfy the following conditions:

$$gcd\left(\gamma\left(g^{\lambda} \bmod \hat{n}^2\right),\ \hat{n}^2\right) = 1, \tag{28}$$

$$\mu = \left(\gamma\left(g^{\lambda} \bmod \hat{n}^2\right)\right)^{-1} \bmod \hat{n}, \tag{29}$$

where $gcd\left(\gamma\left(g^{\lambda} \bmod \hat{n}^2\right),\ \hat{n}^2\right)$ represents the greatest common divisor of $\gamma\left(g^{\lambda} \bmod \hat{n}^2\right)$ and $\hat{n}^2$. On this basis, the public key $(\hat{n}, g)$ and private key (λ, μ) can be obtained for the Paillier Encryption Algorithm.

We let the ciphertext be m and the encryption result be c, the encryption process can be expressed as

$$c = E_P(m, r) = g^m \cdot r^{\hat{n}} \bmod \hat{n}^2, \tag{30}$$

where r is a random integer, which is reciprocal with $\hat{n}$. It is worth noting that r is only a local variable for the sender of the message, since only the encryption process requires r, while the receiver does not use r in the decryption process. Even if the plaintexts are identical, the obtained ciphertexts are statistically indistinguishable due to the different random numbers used in each encryption. It is difficult for an attacker to perform collision attacks on the plaintexts by exhaustive enumeration.

After receiving the coded text, the decryption is calculated and obtained by

$$m = D_P(c) = \gamma\left(c^{\lambda} \bmod \hat{n}^2\right) \cdot (\mu \bmod \hat{n}). \tag{31}$$

During system communication, each node i requires the information about neighbor nodes being summarized in the following Algorithm 1.

Algorithm 1: Information Exchange in Networks

Preparation (node i)
Generate a bunch of public key $(\hat{n}, g)$ and private key (λ, μ) based on (25)–(30), then send $(\hat{n}, g)$ to all its neighbors (including node j).
Encryption and Transmission (node i)
Step 1 : Encrypt w_i as $E_p(w_i, r)$,
Step 2 : Transmit $E_p(w_i, r)$ to the neighbor: node j.
Calculation, and Transmission (node j)
Step 1: Decrypt $E_p(w_i, r)$ after the out-of-limit judgment, obtain the plaintext $D_p(w_i)$,
Step 2: Encrypt the kth calculation results of (10) as $E_p\left(w_{J+1}, r\right)$,
Step 3: Transmit $E_p\left(w_{J+1}, r\right)$ to node i.
Decryption (node i)
Repeat the above process and ensure the security of data during communication.

The zero-knowledge proof in [29] can be used to prove that node j decrypts the ciphertext correctly. Eventually, the secure and privacy-protected communication environment is proposed for the improved second-order attack-resistant algorithm based on the finite time theory.

5. Simulation Study

The proposed algorithm is verified on the IEEE 34 Node Test Feeder system (as shown in Figure 2), which has been widely adopted to evaluate high penetrations of DGs [30]. In

this paper, the system contains six DGs and four integrated loads (sum of load demands being connected to the same bus). The network communication topology among the six DGs is also presented in Figure 2b–e. The reference frequency of the microgrid is 50 Hz. The four integrated loads are load 1: 1.7 + 1.5j Ω, load 2: 1 + 1.2j Ω, load 3: 0.6 + 1.2 j Ω, and load 4: 1.5 + 1.5j Ω, respectively. The load impedances are referred from common load impedances in the IEEE 34 Node Test Feeder system by considering general electrical apparatus. The simulations are conducted in both MATLAB 2020a and PYTHON 3.9.2, which are common tools to investigate the stability of DGs in power systems under FDI attacks. For MATLAB 2020a, power system and power electronics blocks are well established.

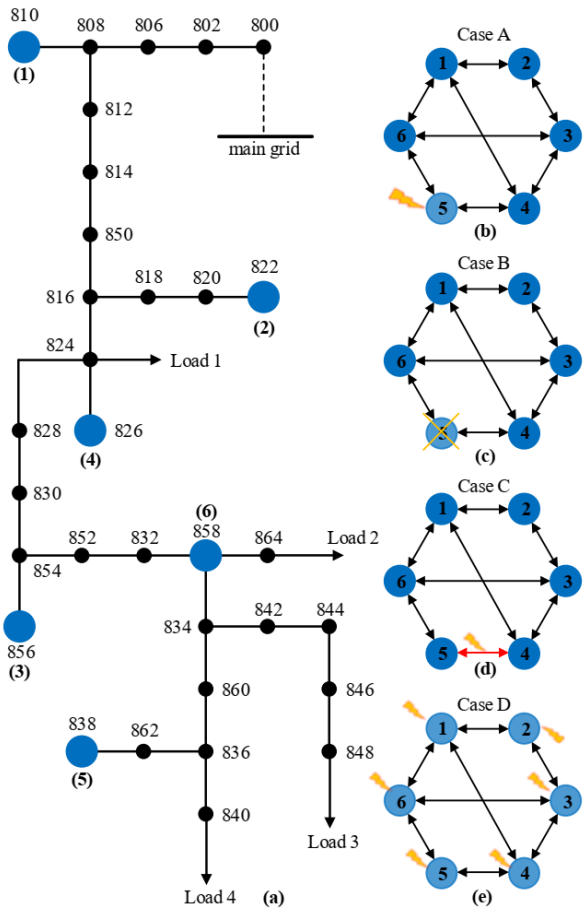


Figure 2. (**a**) Schematic diagrams of the studied IEEE 34 Node Test Feeder system with 6 DGs, (**b**) Case A: DG5′s actuator is under attack, (**c**) Case B: the controller of DG5 is destroyed, (**d**) Case C: the communication link between DG4 and DG5 is under attack, (**e**) Case D: all actuators in the system are under attacks.

The simulations are conducted in the following process: At t = 0 s, the IEEE 34 Node Test Feeder system disconnects from the main grid and operates stably. At t = 1 s, various FDI attacks are injected into the test feeder system. In Case A (Figure 2b), the FDI attack modelled in (7) is injected into the DG5 at 1 s. The effects of the FDI attacks on DG5 are embodied in the frequency change. Simulations are conducted based on the proposed control method and the algorithm in [20] for fair comparisons. The results are shown in Figure 3. Apparently, the frequencies of DGs, except the DG1, deviate from the rated 50 Hz when the conventional control algorithm in [20] is adopted. Their frequencies are converged at 50.2 Hz, which is not acceptable for the stability of a microgrid. The fundamental reason is that the FDI attack being modeled by (7) always exists, while the conventional algorithm is unable to compensate it. Alternatively, the proposed control method can ensure zero offsets and faster restoration.

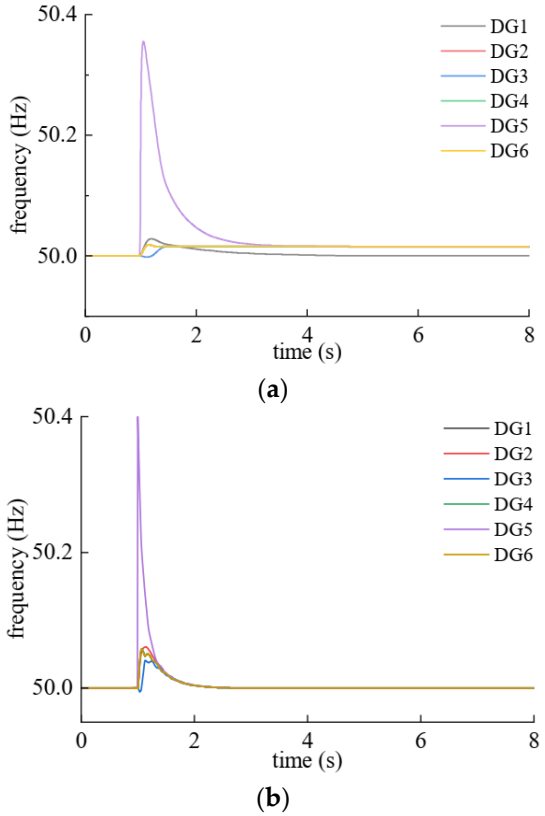


Figure 3. Frequencies of the six DGs with the (**a**) algorithm in [20] and (**b**) proposed algorithm when the DG5 is attacked by a constant FDI attack at 1 s.

In Case B (Figure 2c), the controller of DG5 is attacked to be nonfunctional during the period from 1 s to 2.5 s. As a result, the frequency of DG2 is changed to 50.2 Hz during that period, as shown in Figure 4. Figure 4a shows the frequencies of the six DGs controlled by the conventional algorithm in [20]. Obviously, the frequency of DG5 remains at 50.2 Hz during the period from 1 s to 2.5 s by using the state observer. At 2.5 s, the attack disappears, the conventional control method takes some time to settle steady states after a period of oscillations. In contrast, the proposed method can quickly compensate for the FDI attack; at about 2 s, the frequency of DG5 is already converged at 50 Hz even if the attack signal still exists. Consequently, the remaining DGs are also converged to 50 Hz. At 2.5 s, when the attack is cleared. Small overshoots can be observed, but they are quickly tamed for all the DGs. To further showcase the advantages of the proposed algorithm over the conventional algorithm, the attack signal is prolonged from a 1.5 s to a 4 s period.

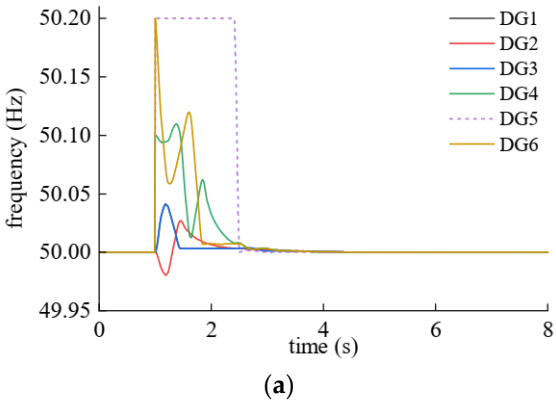
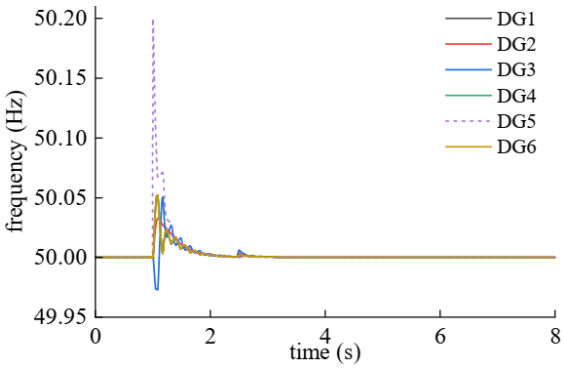


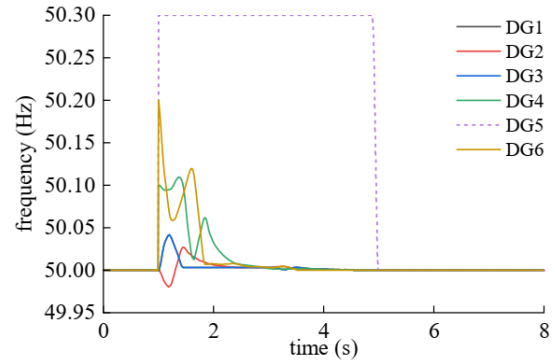
Figure 4. *Cont.*



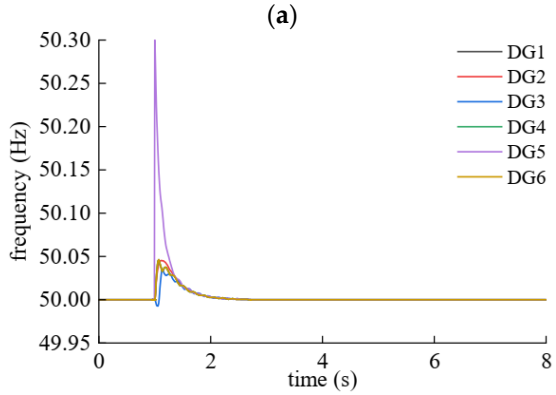
(**b**)

Figure 4. Frequencies of the six DGs with the (**a**) algorithm in [20] and (**b**) proposed algorithm when the DG5 is nonfunctional during the period from 1 s to 2.5 s.

In this case, the frequency of DG5 is attacked to be 50.3 Hz during the period from 1 s to 5 s, as shown in Figure 5a. Under the conventional control in [20], DG5 continuously brings disturbance to the system due to the introduction of the confidential factor. However, the proposed algorithm can detect and compensate for the attack in 2.691 s. The restoration time is significantly reduced, as shown in Figure 5b.



(**a**)



(**b**)

Figure 5. Frequencies of the six DGs with the (**a**) algorithm in [20] and (**b**) proposed algorithm when the DG5 is nonfunctional during the period from 1 s to 5 s.

In Case C (Figure 2d), the FDI signal attacks the communication link between the DG4 and DG5 at 1 s. As a result, both frequencies of DG4 and DG5 are seriously affected, as shown in Figure 6. With the conventional control method in [20], the DG4 and DG5 are subjected to a frequency deviation of +0.3 Hz and −0.3 Hz, respectively, as shown in Figure 6a. The restoration time is more than 2 s for both DG4 and DG5. By comparison,

both restoration times are less than 2 s for the proposed control method, as shown in Figure 6b. In addition, the proposed control method can also reduce the restoration time and fluctuations of other DGs during the attack period. It is worth noting that falsified data in the communication link are detected due to the existence of an encryption algorithm when there is an actual FDI attack against the communication link. Even if an attacker deliberately injects false data with the same bytes of encrypted data, the falsified data can be detected in the third part of Algorithm 1. The falsified data are not incorporated in the iteration process of the algorithm.

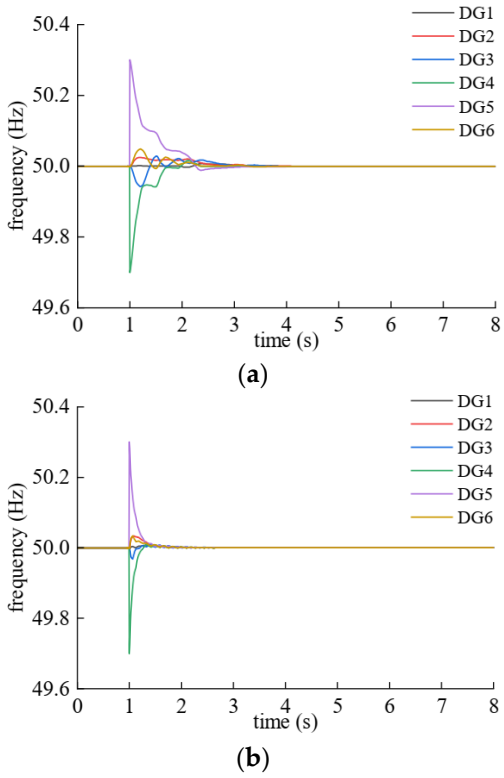


Figure 6. Frequencies of the six DGs with the (**a**) algorithm in [20] and (**b**) proposed algorithm when the communication link between the DG4 and DG5 is attacked at 1 s.

In Case D (Figure 2e), all the DGs are attacked by FDI attacks simultaneously at 1 s. The frequency deviations of the DGs are 0.1, 0.4, −0.2, −0.4, 0.2, and −0.9, respectively. Figure 7 shows the corresponding waveforms. For the conventional algorithm in Figure 7a, the settling time of all DGs is more than 1.5 s. Only DG1 and DG2 can be converged at the rated frequency, while the frequencies of other DGs have offsets. DG6 suffers from the most severe frequency deviation, which is more than 0.1 Hz. For the proposed control method, the restoration time of the DGs is less than 1.5 s. The steady-state tracking errors are almost zero, which means that the adverse effects of the FDI attacks can be eliminated by the proposed control.

Data transmission between the DGs is based on a 64-byte ciphertext, because of the communication protection algorithm being proposed in the algorithm. Table 1 shows the plaintext and the ciphertext of the frequency of each DG in the 22nd iteration of the communication link in Case B. The introduction of r in the encryption algorithm is random, so attackers cannot decipher the encrypted data. Table 2 shows the plaintext and ciphertext of the frequency of each DG in the 23rd iteration of the communication link in Case B. As can be seen from the comparisons of the encrypted frequency data of each DG in two adjacent iterations, the transmitted frequency data are purely random after the encryption. The attacker cannot obtain the system information even if part of the data is intercepted. In addition, even if the falsified data are introduced into the communication link, the

decryption process can detect the falsified data. The error data are be incorporated in the calculation process, such that the communication security of DGs in microgrids can be guaranteed.

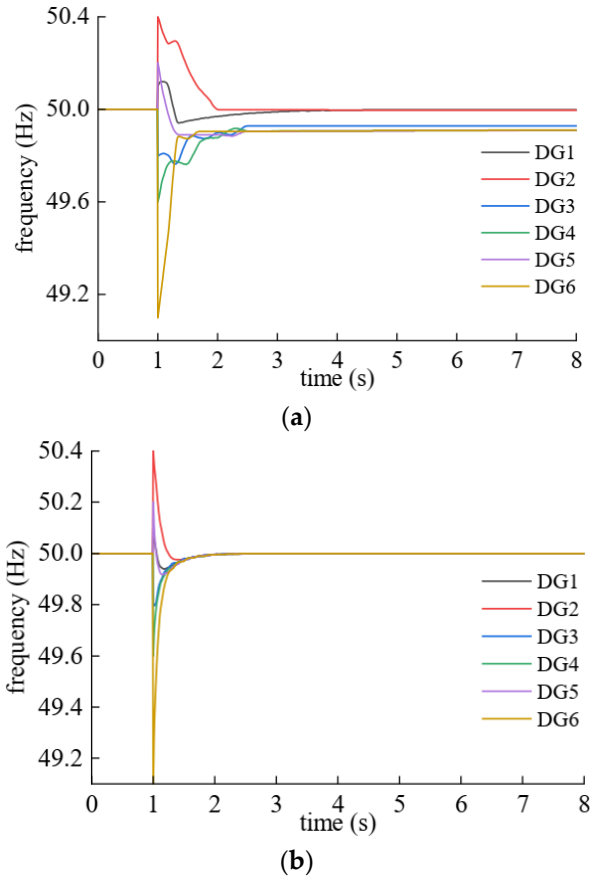


Figure 7. Frequencies of the six DGs with the (**a**) algorithm in [20] and (**b**) proposed algorithm when all the DGs are attacked at 1 s.

Table 1. Plaintext and Ciphertext of the Frequency in the 22nd Iteration of the Communication Link in Case B.

DG	Plaintext	Ciphertext
DG1	50.0032355670135	13962878293123695743 9242239157272820843
DG2	50.0026633037715	14406571166828568720 953973516366529545
DG3	50.0018906850775	60862867060801566833 099386705657357782
DG4	50.0032355670135	11225137299717172167 5466582369177460666
DG5	50.0022263829894	14023597620684394011 1984608615102968414
DG6	50.0032355670135	15775176166453180300 5257059011426352748

Table 2. Plaintext and Ciphertext of the Frequency in the 23rd Iteration of the Communication Link in Case B.

DG	Plaintext	Ciphertext
DG1	50.0020935573353	95041175951322109463 733745365162478020
DG2	50.0023534232178	17620672608558025515 504011146357424466
DG3	50.0026884404735	20223420227290324722 718693972073728424
DG4	50.0020935573353	40584764380985213406 764078574284625510
DG5	50.0025465624365	14635744288036751950 4011498137737930240
DG6	50.0020935573353	15924659508651567860 8601785411804554137525705 9

6. Conclusions and Future Work

Distributed generators (DGs) under false data injection (FDI) attacks affect the stability of entire microgrids. Various conventional cooperative control algorithms have been proposed to mitigate FDI attacks on the frequency deviation issue. However, most traditional cooperative control cannot completely remove the negative effects from the FDI attacks, since their data via the communication channels are not fully encrypted. To address this, a new cooperative control method based on the Paillier Encryption Algorithm is proposed. The Paillier Encryption Algorithm renders safe data spread in the communication links of the system, which significantly alleviates the hassle of penetrating falsified data into the secondary droop control for the DGs. The new cooperative control method is validated on the IEEE 34 Node Test Feeder system in simulation to better exhibit both dynamic and steady-state performance than a conventional cooperative control method for four difference cases, i.e., one DG is attacked, one DG is unfunctional, communication failure between the two DGs, and all DGs are attacked simultaneously. The results show that the frequency restoration time of the proposed control is faster than the conventional control in all the cases. The frequency deviations at the new steady states after the attack are almost zero for all the cases, while frequency deviations can be clearly observed for the conventional control. In future work, we will enhance the control algorithm by including additional nonlinear observers for other types of cyber attacks. In addition, the control objectives for the DGs could be power qualities and power efficiencies of microgrids.

Author Contributions: Conceptualization, Z.L.; methodology, H.F.; software, H.F.; validation, H.F.; formal analysis, H.F.; investigation, H.F.; resources, Z.L.; data curation, H.F.; writing—original draft preparation, H.F.; writing—review and editing, W.L.; visualization, L.Q.; supervision, Z.L.; project administration, Y.A.; funding acquisition, Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is unavailable due to privacy or ethical restrictions.

Conflicts of Interest: Authors Han Fu, Wenpei Li and Yongheng Ai were employed by the State Grid Wuhan Power Supply Company. The remaining 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.

References

1. Cao, G.; Gu, W.; Li, P.; Sheng, W.; Liu, K.; Sun, L.; Cao, Z.; Pan, J. Operational Risk Evaluation of Active Distribution Networks Considering Cyber Contingencies. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3849–3861. [CrossRef]
2. Yang, Y.; Tan, S.-C.; Hui, S.Y.R. Mitigating Distribution Power Loss of DC Microgrids with DC Electric Springs. *IEEE Trans. Smart Grid* **2018**, *9*, 5897–5906. [CrossRef]
3. Ding, D.; Han, Q.-L.; Ge, X.; Wang, J. Secure State Estimation and Control of Cyber-Physical Systems: A Survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 176–190. [CrossRef]
4. Yang, Y.; Qin, Y.; Tan, S.-C.; Hui, S.Y.R. Reducing Distribution Power Loss of Islanded AC Microgrids Using Distributed Electric Springs with Predictive Control. *IEEE Trans. Ind. Electron.* **2020**, *67*, 9001–9011. [CrossRef]
5. Abdi, F.; Chen, C.-Y.; Hasan, M.; Liu, S.; Mohan, S.; Caccamo, M. Preserving Physical Safety under Cyber Attacks. *IEEE Internet Things J.* **2019**, *6*, 6285–6300. [CrossRef]
6. Lu, X.; Yu, X.; Lai, J.; Wang, Y.; Guerrero, J.M. A Novel Distributed Secondary Coordination Control Approach for Islanded Microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 2726–2740. [CrossRef]
7. Yang, Y.; Ho, S.-S.; Tan, S.-C.; Hui, S.-Y.R. Small-Signal Model and Stability of Electric Springs in Power Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 857–865. [CrossRef]
8. Ding, D.; Han, Q.-L.; Wang, Z.; Ge, X. A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 2483–2499. [CrossRef]
9. Bidram, A.; Davoudi, A. Hierarchical Structure of Microgrids Control System. *IEEE Trans. Smart Grid* **2012**, *3*, 1963–1976. [CrossRef]
10. Yang, Y.; Tan, S.-C.; Hui, S.Y.R. Adaptive Reference Model Predictive Control with Improved Performance for Voltage-Source Inverters. *IEEE Trans. Control. Syst. Technol.* **2018**, *26*, 724–731. [CrossRef]
11. Shafiee, Q.; Guerrero, J.M.; Vasquez, J.C. Distributed Secondary Control for Islanded Microgrids—A Novel Approach. *IEEE Trans. Power Electron.* **2014**, *29*, 1018–1031. [CrossRef]
12. Yang, Y.; Mok, K.-T.; Tan, S.-C.; Hui, S.Y. Nonlinear dynamic power tracking of low-power wind energy conversion system. *IEEE Trans. Power Electron.* **2015**, *30*, 5223–5236. [CrossRef]
13. Zhang, G.; Li, C.; Qi, D.; Xin, H. Distributed Estimation and Secondary Control of Autonomous Microgrid. *IEEE Trans. Power Syst.* **2017**, *32*, 989–998. [CrossRef]
14. Chen, Y.; Qi, D.; Dong, H.; Li, C.; Li, Z.; Zhang, J. A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids. *IEEE Trans. Smart Grid* **2021**, *12*, 1929–1938. [CrossRef]
15. Zhao, Z.; Huang, Y.; Zhen, Z.; Li, Y. Data-Driven False Data-Injection Attack Design and Detection in Cyber-Physical Systems. *IEEE Trans. Cybern.* **2021**, *51*, 6179–6187. [CrossRef]
16. Yang, Y.; Qin, Y.; Tan, S.-C.; Hui, S.Y.R. Efficient Improvement of Photovoltaic-Battery Systems in Standalone DC Microgrids Using a Local Hierarchical Control for the Battery System. *IEEE Trans. Power Electron.* **2019**, *34*, 10796–10807. [CrossRef]
17. Jiao, Q.; Modares, H.; Lewis, F.L.; Xu, S.; Xie, L. Distributed L2-gain output-feedback control of homogeneous and heterogeneous systems. *Automatica* **2016**, *71*, 361–368. [CrossRef]
18. Shafiee, Q.; Nasirian, V.; Vasquez, J.C.; Guerrero, J.M.; Davoudi, A. A Multi-Functional Fully Distributed Control Framework for AC Microgrids. *IEEE Trans. Smart Grid* **2018**, *9*, 3247–3258. [CrossRef]
19. Abhinav, S.; Schizas, I.D.; Lewis, F.L.; Davoudi, A. Distributed Noise-Resilient Networked Synchrony of Active Distribution Systems. *IEEE Trans. Smart Grid* **2018**, *9*, 836–846. [CrossRef]
20. 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]
21. El-Yahyaoui, A.; El Kettani, M.D.E.-C. A verifiable fully homomorphic encryption scheme to secure big data in cloud computing. In Proceedings of the 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM), Rabat, Morocco, 1–4 November 2017; pp. 1–5.
22. Wu, W.; Liu, J.; Wang, H.; Hao, J.; Xian, M. Secure and Efficient Outsourced k-Means Clustering using Fully Homomorphic Encryption with Ciphertext Packing Technique. *IEEE Trans. Knowl. Data Eng.* **2021**, *33*, 3424–3437. [CrossRef]
23. Sutisna, N.; Jonatan, G.; Syafalni, I.; Mulyawan, R.; Adiono, T. Polynomial multiplication systolic array for homomorphic encryption in secure network communications. In Proceedings of the 2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Batam, Indonesia, 17–18 December 2020; pp. 390–394.
24. Wang, L.; Xiao, F. Finite-Time Consensus Problems for Networks of Dynamic Agents. *IEEE Trans. Autom. Control.* **2010**, *55*, 950–955. [CrossRef]
25. Pasqualetti, F.; Bicchi, A.; Bullo, F. Consensus Computation in Unreliable Networks: A System Theoretic Approach. *IEEE Trans. Autom. Control.* **2012**, *57*, 90–104. [CrossRef]
26. Pasqualetti, F.; Dorfler, F.; Bullo, F. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Trans. Autom. Control.* **2013**, *58*, 2715–2729. [CrossRef]
27. Rong-Bing, W.; Ya-Nan, L.; Hong-Yan, X.; Yong, F.; Yong-Gang, Z. Electronic Scoring Scheme Based on Real Paillier Encryption Algorithms. *IEEE Access* **2019**, *7*, 128043–128053. [CrossRef]
28. Chen, W.; Liu, L.; Liu, G.-P. Privacy-Preserving Distributed Economic Dispatch of Microgrids: A Dynamic Quantization-Based Consensus Scheme with Homomorphic Encryption. *IEEE Trans. Smart Grid* **2023**, *14*, 701–713. [CrossRef]

29. Ogunseyi, T.B.; Tang, B. Fast Decryption algorithm for paillier homomorphic cryptosystem. In Proceedings of the IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 28–30 July 2020; pp. 803–806.
30. Mwakabuta, N.; Sekar, A. Comparative study of the IEEE 34 node test feeder under practical simplifications. In Proceedings of the Presented at 39th American Power Symposium, Las Cruces, NM, USA, 30 September–2 October 2007; pp. 484–491.