

A Privacy-Preserving Distributed Optimal Scheduling for Interconnected Microgrids

Authors:

Nian Liu, Cheng Wang, Minyang Cheng, Jie Wang

Date Submitted: 2019-02-27

Keywords: optimal scheduling, cybersecurity, distributed optimization, microgrid

Abstract:

With the development of microgrids (MGs), interconnected operation of multiple MGs is becoming a promising strategy for the smart grid. In this paper, a privacy-preserving distributed optimal scheduling method is proposed for the interconnected microgrids (IMG) with a battery energy storage system (BESS) and renewable energy resources (RESs). The optimal scheduling problem is modeled to minimize the coalitional operation cost of the IMG, including the fuel cost of conventional distributed generators and the life loss cost of BESSs. By using the framework of the alternating direction method of multipliers (ADMM), a distributed optimal scheduling model and an iteration solution algorithm for the IMG is introduced; only the expected exchanging power (EEP) of each MG is required during the iterations. Furthermore, a privacy-preserving strategy for the sharing of the EEP among MGs is designed to work with the mechanism of the distributed algorithm. According to the security analysis, the EEP can be delivered in a cooperative and privacy-preserving way. A case study and numerical results are given in terms of the convergence of the algorithm, the comparison of the costs and the implementation efficiency.

Record Type: Published Article

Submitted To: LAPSE (Living Archive for Process Systems Engineering)

Citation (overall record, always the latest version):

LAPSE:2019.0341

Citation (this specific file, latest version):

LAPSE:2019.0341-1

Citation (this specific file, this version):

LAPSE:2019.0341-1v1

DOI of Published Version: <https://doi.org/10.3390/en9121031>

License: Creative Commons Attribution 4.0 International (CC BY 4.0)

Article

A Privacy-Preserving Distributed Optimal Scheduling for Interconnected Microgrids

Nian Liu *, Cheng Wang, Minyang Cheng and Jie Wang

State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing 102206, China; wangcheng@ncepu.edu.cn (C.W.); cmyoung@ncepu.edu.cn (M.C.); wangjie1526@ncepu.edu.cn (J.W.)

* Correspondence: nianliu@ncepu.edu.cn; Tel.: +86-10-80790940

Academic Editor: Paras Mandal

Received: 20 October 2016; Accepted: 29 November 2016; Published: 7 December 2016

Abstract: With the development of microgrids (MGs), interconnected operation of multiple MGs is becoming a promising strategy for the smart grid. In this paper, a privacy-preserving distributed optimal scheduling method is proposed for the interconnected microgrids (IMG) with a battery energy storage system (BESS) and renewable energy resources (RESs). The optimal scheduling problem is modeled to minimize the coalitional operation cost of the IMG, including the fuel cost of conventional distributed generators and the life loss cost of BESSs. By using the framework of the alternating direction method of multipliers (ADMM), a distributed optimal scheduling model and an iteration solution algorithm for the IMG is introduced; only the expected exchanging power (EEP) of each MG is required during the iterations. Furthermore, a privacy-preserving strategy for the sharing of the EEP among MGs is designed to work with the mechanism of the distributed algorithm. According to the security analysis, the EEP can be delivered in a cooperative and privacy-preserving way. A case study and numerical results are given in terms of the convergence of the algorithm, the comparison of the costs and the implementation efficiency.

Keywords: microgrid; distributed optimization; cybersecurity; optimal scheduling

1. Introduction

Microgrids (MGs) are self-controlled entities, which facilitate the penetration of renewable energy and distributed energy resources (DERs) for economic and reliability purposes. Generally, the MG can be operated in either grid-connected [1] or island mode [2]. With the development of MGs, a new typical approach is to consider where several MGs exchange energy with one another even when the MGs are isolated from the utility grid. In other words, there exist energy flows within a group of physically-connected MGs, but not between the MGs and the main grid. One promising application of interconnected MGs (IMG) is for the service restoration in a self-healing distribution system to improve the dynamic performance when islanding occurs and to extend the power supply during the system outages [3,4]. Another important application is to ensure the full utilization of renewable energy resources (RESs) and improve the economic benefit and reliability in isolated areas [5]. Consequently, the interconnected operation of multi-MGs is becoming a promising strategy for the smart grid.

Considering the type of MGs, the interconnection among autonomous MGs can be realized via an AC [6,7], DC [8] or AC-DC hybrid architecture [9]. As a newly-emerging topic of the smart grid, there are still limited research works focused on the related problems of IMGs. The studies can be roughly divided into two categories: (1) coordinated control and (2) energy management. For the coordinated control, the feasibility (benefits) and basic controls of IMGs via AC connections were studied in [6,7]. Moreover, in [5,9,10], considering that the AC MGs may be operated at different voltages and frequencies, hybrid AC/DC links and coordinated control schemes were studied for

maintaining the autonomy of each MG during interconnections. For the interconnection of DC MGs, several control methods were proposed, such as the control strategy for two DC MGs [11], distributed hierarchical control [12] and distributed two-level tertiary control [13] for a cluster of DC MGs.

Energy management is another category of study for the IMG. To ensure the full utilization of RES and to minimize the operation cost, effective scheduling of the DERs and battery energy storage systems (BESS) [14] is highly necessary. Generally, if all of the MGs could share the information on their respective load data, generation data and parameters and grid parameters, the optimal scheduling could be easily realized based on the traditional centralized optimization [15], such as optimal power flow (OPF). However, for security considerations, it is not desirable for each MG to do so because the shared information could compromise the privacy of each MG. Thus, this is the basic driving force of the distributed optimization of IMG scheduling. For instance, a distributed convex optimization framework was developed for energy trading between islanded MGs [16]. The problem consists of several islanded MGs that exchange energy flows by means of an arbitrary topology. In [17], the authors studied the self-organization and decentralized energy management of an MG cluster islanded from the main grid after a disruptive event.

However, even with applying distributed optimization, there are still weak points in these works. First, for privacy preserving, the algorithms require the MGs to share enough data with others during the optimization. For instance, the trading prices and corresponding trading energy should be shared between the neighboring MGs in [16], and the expected power exchange of each MG should be shared with all other MGs in [17]. After long-term operation, the generation details and energy consumption patterns of one MG can be gradually inferred by other MGs using data mining [18], which could gradually affect the confidentiality and privacy [19]. In the smart grid, data perturbation and aggregation are the two main privacy-preserving approaches that have been applied to avoid the inference of sensitive information from the metering data [20]. For privacy preserving, the assumed attacks are mainly based on non-intrusive monitoring of energy usage traces. Typical solutions rely on battery-based load hiding [21,22], on noise injection [23] or on a multi-party computation cryptosystem [24,25]. However, in the distributed optimization framework, the shared data are tightly coupled with the local optimization and circulated during the execution of the scheduling horizon. In this regard, the solutions of battery-based hiding and noise injection are difficult to apply. Second, the modeling of BESS is not considered in the optimization of IMG. For the MGs consisting of wind, solar and diesel generations, the BESS is an important component to increase the utilization of RES [26,27]. With suitable sizing [26,28] and coordinated control [29], BESS could have great influence on the optimal scheduling of MGs.

To this end, this paper proposes a privacy-preserving distributed optimal scheduling method for energy management of IMG, with the consideration of BESS and RES. The main contributions of the paper are as follows: (1) based on the relationship between charging-discharging features and the battery life cost, the cost model of BESS is formulated as a quadratic polynomial; (2) by using the framework of the alternating direction method of multipliers (ADMM), a distributed optimal scheduling model and iterative algorithm is proposed; (3) based on the multi-party computation cryptosystem, a privacy-preserving strategy to protect the sharing of expected exchanging power (EEP) between MGs is designed to work with the iterative algorithm.

2. System Model

In this section, we describe the system model for the distributed optimal scheduling of IMG. In the MG, we take RESs, conventional distributed generation, and BESS into consideration. RESs, such as wind turbines (WT) and photovoltaics (PV), are non-dispatchable, and conventional distributed generation such as diesel, is dispatchable. BESS can be regarded as dispatchable resources for discharging and controllable load for charging.

2.1. Renewable Energy Resources

A RES unit, such as WT and PV, is not dispatchable, and its output power depends on the availability of the primary sources (i.e., solar irradiance or wind speed). Therefore, forecasting is required in order to consider them in the optimal operation of IMG [30]. In the optimization, we can assume that the complex power of an RES over the scheduling horizon is given, and there is no generation cost for RES [31].

2.2. Diesel Generation

Diesel generation (DG) is a dispatchable source, which plays the role of a supplement source when there is a shortage of RES power. Diesel fuel is necessary for generation, and the relationship between cost and output power can be expressed as:

$$C_{gen}(P_{gen}) = c_{fuel} \cdot (a_g P_{gen} + b_g P_{gen}^2 + c_g) \quad (1)$$

where c_{fuel} is the unit price of diesel fuel (CYN/L); P_{gen} is the output power of the diesel generation; a_g, b_g, c_g are the coefficients of the fuel demand of the generation to its output power [32].

2.3. BESS

The lifetime of the battery will be depleted after a certain number of charging and discharging cycles. The relationship of the BESS' lifetime loss can be described as:

$$L_{loss} = \frac{A_c}{A_{total}} \quad (2)$$

where L_{loss} is the life loss percentage of BESS; A_c is the effective cumulative capacity in a certain period, kWh. A_{total} is the total effective cumulative capacity of the full life cycles, kWh. According to the manufacturing manual of the lead acid battery, it will deliver 390Q effective kWh over its lifetime with the capacity of Q [33].

Furthermore, A_c is decided by the battery's state of charge (SOC) and the actual capacity A'_c , and the relationship is described as:

$$A_c = \lambda_{SOC} \cdot A'_c \quad (3)$$

where λ_{SOC} is an effective weight. When the SOC of BESS takes the value from 0.5 to 1.0, we can approximately assume that λ_{SOC} has a linear relation with SOC [33].

$$\lambda_{SOC} = a \cdot SOC + b \quad (4)$$

where a and b are two coefficients.

When BESS' SOC changes from SOC_{init} to SOC_{end} during the operation of discharging, the effective capacity is described as:

$$A_c = \int_{SOC_{end}}^{SOC_{init}} \lambda_{SOC} Q dSOC \quad (5)$$

With the consideration of the relationship between discharging power P and its duration ΔT , SOC_{end} can be further described as:

$$SOC_{end} = SOC_{init} - P \cdot \Delta T / Q \quad (6)$$

and the equivalent accumulative capacity is

$$A_c = -\frac{a}{2Q} P^2 \Delta T^2 + P \Delta T (a \cdot SOC_{init} + b) \quad (7)$$

Integrating (2) and (7), the lifetime cost can be described as a function of P :

$$C_{BS}(P) = I \frac{-aP^2 \Delta T^2 + 2P \Delta T Q (aSOC_{init} + b)}{2QA_{total}} \quad (8)$$

where I is the investment of BESS.

2.4. Optimal Scheduling Model of MGs

Given the forecasted power of WT, PV and loads, the MG operator can schedule the dispatchable resources' output power to minimize the total operation cost. Generally, the MG-n's optimal scheduling problem can be formulated as:

$$\min \quad h_n(\mathbf{x}_n) = f_n(\mathbf{x}_n) + \gamma(x_n^{in}) = C_{DG_n}(x_{DG_n}) + C_{BS_n}(x_{BS_n}) + \gamma(x_n^{in}) \quad (9)$$

$$\text{s.t.} \quad d_n - P_{uc_n} - x_{DG_n} - x_{BS_n} = x_n^{in} \quad (10)$$

$$0 \leq x_{DG_n} \leq P_{DG_n}^{max} \quad (11)$$

$$P_{charge}^{max} \leq x_{BS_n} \leq P_{discharge}^{max} \quad (12)$$

$$SOC_{min} \leq SOC_n \leq SOC_{max} \quad (13)$$

where $\mathbf{x}_n = [x_{DG}, x_{BS}]$ is composed by the dispatchable sources' output power, in which x_{DG_n} and x_{BS_n} are DG and BESS's output power, respectively. x_n^{in} is the expected exchange power of MG-n. If MG-n imports power from IMG, x_n^{in} is positive; otherwise, if MG-n exports power to IMG, x_n^{in} is negative. $\gamma(\cdot)$ is the cost of trading x_n in the IMG, which can be charged by the network investor considering the investment of power lines and network losses. d_n is the MG-n's total power demand, and P_{uc_n} is the total non-dispatchable output power. Considering that the energy efficiency of BESS in charging/discharging is less than 100%, when the BESS' scheduling power is x_{BS_n} , the actual charging power should be $x_{BS_n} \cdot \eta$, whereas the actual discharging power should be x_{BS_n} / η . As shown in (1) and (8), the cost function of DG and BS is convex, which indicates that the cost function $h_n(\mathbf{x})$ is convex, as well.

As for the constraints, (10) is set to keep the power balance of MG; (11) ensures that the output power of DG is in the range of rated capacity; (12) is used to limit the output power of the BESS, according to the fact that the charging/discharging power should not exceed the maximum power of the bi-directional inverter; (13) sets the maximum and minimum SOC of BESS in operation.

2.5. Optimal Scheduling Model of the IMG

In the environment of interconnected operation, all participating MGs are trying to lower their total operation cost by considering the cost efficiency of DERs and scheduling in a cooperative way. For an IMG containing N MGs, its optimization problem can be formulated as [16]:

$$\begin{aligned} \min \quad & \sum_{n=1}^N (f_n(\mathbf{x}_n) + \gamma_n(\mathbf{x}_n)) \\ \text{s.t.} \quad & \sum_{n=1}^N \mathbf{1}^T \mathbf{x}_n = \sum_{n=1}^N (d_n - P_{uc_n}) \end{aligned} \quad (14)$$

where $\mathbf{1}^T$ is the unit row vector.

It is noted that in (14), all of the participating MGs are assumed to work as a coalition [34], in which they will aim to minimize the global operation cost of the IMG.

In general, there are two methods to solve this optimal scheduling problem: centralized optimization and distributed optimization. In the centralized method, all private information of each MG needs to be collected by the control center (CC), and the optimal scheduling result will be distributed to each MG after optimization, as shown in Figure 1.

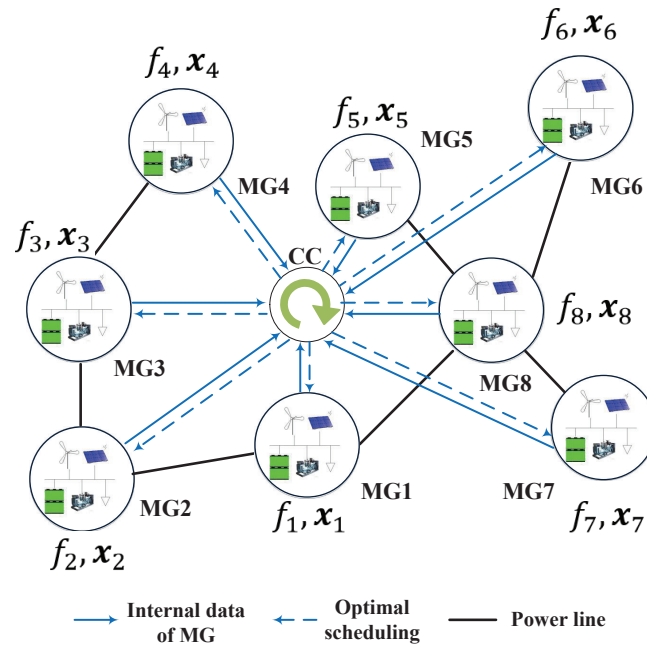


Figure 1. Centralized optimal scheduling of the interconnected microgrids (IMG).

3. Distributed Optimization

3.1. ADMM

ADMM was proposed by Gabay in the 1970s and has been widely used in large-scale distributed computing and optimization [35]. With the excellent performance in convergence and robustness, the method has drawn great attention in recent years. In the field of power system optimization, ADMM has also been used to solve the distributed optimization problem [36,37]. The basic form can be described as:

$$\begin{aligned} \min \quad & s(\mathbf{x}) + g(\mathbf{z}) \\ \text{s.t.} \quad & \mathbf{Ax} + \mathbf{Bz} = \mathbf{c} \end{aligned} \tag{15}$$

where $\mathbf{x} \in \mathbb{R}^n$; $\mathbf{z} \in \mathbb{R}^m$; $\mathbf{A} \in \mathbb{R}^{p \times n}$; $\mathbf{B} \in \mathbb{R}^{p \times m}$; $\mathbf{c} \in \mathbb{R}^p$. Functions s and g are all convex. When function s is $\mathbb{R}^n \rightarrow \mathbb{R} \cup \{+\infty\}$ and g is $\mathbb{R}^m \rightarrow \mathbb{R} \cup \{+\infty\}$, the algorithm can converge to the optimized solution [35].

3.2. Decentralizing the Problem

To decentralize objective Function (14), we define the following function according to the standard ADMM form [35]:

$$\begin{aligned} g(\mathbf{z}) &= \begin{cases} 0, & \mathbf{z} \in \mathbb{R}^N \\ +\infty & \mathbf{z} \notin \mathbb{R}^N \end{cases} \\ \mathbb{C} &= \{\mathbf{z} \in \mathbb{R}^N | z_1 + z_2 + \dots + z_N = 0\} \end{aligned} \tag{16}$$

To make the equation simple, we can express x^{in} as:

$$x_n^{in} = \mathbf{1}^T \mathbf{x}_n - (d_n - P_{uc_n}), n = [1, 2, \dots, N] \tag{17}$$

Combined with (9), Function (14) can be further described as:

$$\begin{aligned} \min \quad & \sum_{n=1}^N h_n(\mathbf{x}_n) + g(\mathbf{z}) \\ \text{s.t.} \quad & \mathbf{x}^{in} - \mathbf{z} = 0 \end{aligned} \tag{18}$$

where $\mathbf{x}^{in} = [x_1^{in}, x_1^{in}, \dots, x_N^{in}]$ indicates the EEP vector of MGs in IMG. Through variable \mathbf{z} , objective function (18) can be solved in a distributed manner.

According to the standard iteration form of ADMM, the problem's iteration process can be described as:

$$\begin{aligned} \mathbf{x}_n^{k+1} &= \arg \min_{\mathbf{x}} h_n(\mathbf{x}) + \frac{\rho}{2} \|\mathbf{x}_n^{in} - \mathbf{z}_n^k + \mathbf{u}_n^k\|_2^2 \\ \mathbf{z}^{k+1} &= \arg \min_{\mathbf{z}} g(\mathbf{z}) + \frac{\rho}{2} \sum_n \|\mathbf{z}_n - \mathbf{x}_n^{in^{k+1}} - \mathbf{u}_n^k\|_2^2 \\ \mathbf{u}_n^{k+1} &= \mathbf{u}_n^k + \mathbf{x}_n^{in^{k+1}} - \mathbf{z}_n^{k+1} \end{aligned} \tag{19}$$

where $\rho > 0$ is a given penalty coefficient; k is the number of iterations; u_n is the Lagrange multiplier for the equation constraint of (18). In the process of updating \mathbf{z} , all x_n^{in} should be collected. To enhance the privacy-preserving ability and simplify the iteration, we can have:

$$\bar{z} = \frac{1}{N} \sum_{n=1}^N z_n \tag{20}$$

and then, (16) can be transformed as:

$$\begin{aligned} \tilde{g}(\bar{z}) &= \begin{cases} 0, & \bar{z} \in \mathbb{Q} \\ +\infty, & \bar{z} \notin \mathbb{Q} \end{cases} \\ \mathbb{Q} &= \{\bar{z} | \bar{z} = 0\} \end{aligned} \tag{21}$$

For any \mathbf{z} , its update in (19) is equivalent to:

$$\begin{aligned} \min \quad & \tilde{g}(\bar{z}) + \frac{\rho}{2} \sum_{n=1}^N \|z_n - x_n^{in^{k+1}} - u_n^k\|_2^2 \\ \text{s.t.} \quad & \bar{z} = \frac{1}{N} \sum_{n=1}^N z_n \end{aligned} \tag{22}$$

For any constant \bar{z} , the Lagrange equation of (22) can be described as:

$$L(\mathbf{z}, \mu) = \tilde{g}(\bar{z}) + \frac{\rho}{2} \sum_{n=1}^N \|z_n - x_n^{in^{k+1}} - u_n^k\|_2^2 + \mu \cdot (\bar{z} - \frac{1}{N} \sum_{n=1}^N z_n) \tag{23}$$

where μ is the Lagrange multiplier for the constraint in (22). As (22) is a convex function, the necessary and sufficient condition is:

$$\nabla_{\mathbf{z}} L(\mathbf{z}, \mu) = 0 \quad \text{and} \quad \bar{z} = \frac{1}{N} \sum_{n=1}^N z_n \tag{24}$$

For any constant \bar{z} , $\tilde{g}(\bar{z})$ is a scalar, and the condition $\nabla_{\mathbf{z}} L(\mathbf{z}, \mu) = 0$ translates to:

$$\rho(z_n - x_n^{in^{k+1}} - u_n^k) - \frac{1}{N} \mu = 0, n = [1, 2, \dots, N] \tag{25}$$

After some manipulation, (24) and (25) collectively imply:

$$z_n - x_n^{in^{k+1}} - u_n^k = \bar{z} - \bar{x}^{in^{k+1}} - \bar{u}^k \tag{26}$$

where we have used the same overline-notation for $x^{in^{k+1}}$ and u^k :

$$\bar{x}^{in^{k+1}} = \frac{1}{N} \sum_{n=1}^N x_n^{in^{k+1}}, \bar{u}^k = \frac{1}{N} \sum_{n=1}^N u_n^k \tag{27}$$

By employing (26) in (22), the \mathbf{z} -update introduced in (19) can be equivalently formulated as:

$$\bar{z}^{k+1} = \arg \min_{\bar{z}} \tilde{g}(\bar{z}) + \frac{N \cdot \rho}{2} \|\bar{z} - \bar{x}^{in^{k+1}} - \bar{u}^k\|_2^2 \tag{28}$$

After being simplified, it is only needed to update \bar{z} , and the Lagrange multiplier u_n can be expressed as:

$$u^{k+1} = u^k + \bar{x}^{in^{k+1}} - \bar{z}^{k+1} \tag{29}$$

Combining (28) and (29), replace z_n^k in the updating process of x_n , and then, the simplified distributed iteration form is:

$$\begin{aligned} x_n^{k+1} &= \arg \min_x h_n(x) + \frac{\rho}{2} \|x_n^{in} - x_n^{in^k} + \bar{x}^{in^k} - \bar{z}^k + u^k\|_2^2 \\ \bar{z}^{k+1} &= \arg \min_{\bar{z}} \tilde{g}(\bar{z}) + \frac{N\rho}{2} \|\bar{z} - \bar{x}^{in^{k+1}} - u^k\|_2^2 \\ u^{k+1} &= u^k + \bar{x}^{in^{k+1}} - \bar{z}^{k+1} \end{aligned} \tag{30}$$

According to (21), the result of update \bar{z} would be:

$$\bar{z}^{k+1} = 0 \tag{31}$$

The final form of the distributed iteration can be described as:

$$\begin{aligned} x_n^{k+1} &= \arg \min_x h_n(x) + \frac{\rho}{2} \|x_n^{in} - x_n^{in^k} + \bar{x}^{in^k} + u^k\|_2^2 \\ u^{k+1} &= u^k + \bar{x}^{in^{k+1}} \end{aligned} \tag{32}$$

From (32), we can know that only the average EEP in IMG is required in the optimization, and the Lagrange multiplier's updating can be calculated within each MG.

As shown in Figure 2, by using the distributed optimization, each MG solves its own optimal scheduling and can finally reach the global optimal solution by informing its EEP to other MGs during the iterations.

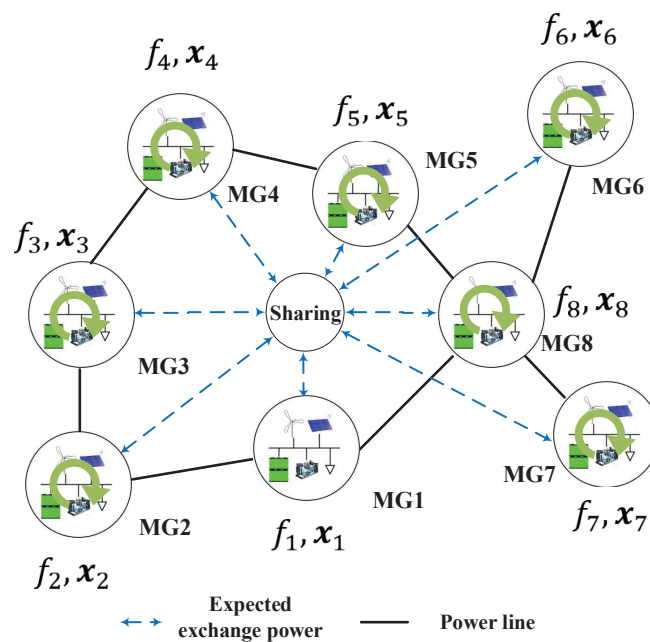


Figure 2. Distributed optimal scheduling of the IMG.

Furthermore, the dual residual can be used as the stopping criteria for the iteration convergence.

$$r_k = \frac{1}{N} \sum_{n=1}^N x_n^{in^k} \tag{33}$$

When the residual satisfies the following conditions, it is considered to achieve convergence, and the iteration is stopped.

$$\|r_k\|_2^2 \leq \varepsilon \tag{34}$$

in which ε is the convergence error. The calculation process of the distribution optimal scheduling is described in Algorithm 1.

Algorithm 1 Distributed scheduling algorithm

```

1: procedure DISPATCHING( $x_n, n = [1, 2, \dots, N]$ )
2:   Initiate  $u, \rho, k$ 
3:   while  $\|r\|_2^2 > \varepsilon$  do
4:      $x_n^{k+1} = \arg \min_x h_n(x) + \frac{\rho}{2} \|x_n^{in} - x_n^{in^k} + \bar{x}^{in^k} + u^k\|_2^2$ 
5:      $\bar{x}^{in^{k+1}} = \frac{1}{N} \sum_{n=1}^N x_n^{in^{k+1}}$ 
6:      $u^{k+1} = u^k + \bar{x}^{in^{k+1}}$ 
7:      $r_{k+1} = \frac{1}{N} \sum_{n=1}^N x_n^{in^{k+1}}$ 
8:      $k = k + 1$ 
9:   end while
10: end procedure

```

4. Privacy-Preserving Strategy

As shown in (27) and Algorithm 1, each MG should share its own EEP. After that, the average EEP will be calculated and sent back to all of the participating MGs. Considering the privacy, each MG should share its own EEP, but does not want to show it to the other MGs. By coincidence, as the Paillier cryptosystem has the features of homomorphic addition, indistinguishability and self-blinding, it is feasible to transfer the addition of plaintext EEPs to the multiplication of ciphertext EEPs, which makes it quite suitable for privacy preserving in the sharing of EEPs [38].

4.1. Basic Theory of the Paillier Cryptosystem

The Paillier cryptosystem is widely used in a distributed environment and can protect users' privacy in the collaboration process [39]. The basic schema of Paillier includes three parts, which are described as follows [38].

4.1.1. Key Generation

Select two prime numbers p and q , and calculate $N_k = pq$ and λ_k :

$$\lambda_k = \text{lcm}(p-1, q-1) \quad (35)$$

where lcm means the operation of calculating the lowest common multiple. We denote Euler's totient function $\phi(n)$ taken on N_k , i.e., $\phi(N_k) = (p-1)(q-1)$ in the present case. Recall that $|\mathbb{Z}_{N_k}^*| = \phi(N_k)$, then a random number $g_k \in \mathbb{Z}_{N_k}^*$ is needed and should satisfy:

$$\text{gcd}(L(g_k^{\lambda_k} \bmod N_k^2), N_k) = 1 \quad (36)$$

where $L(x) = (x-1)/N_k$ and gcd is the operation of calculating the greatest common divisor. The Paillier public key and private key are $\langle N_k, g_k \rangle$ and λ_k .

4.1.2. Encryption

Assume that $m_c \in \mathbb{Z}_N$ is plaintext, $w \in \mathbb{Z}_N$ is a random number and $E(\cdot)$ is the encryption operation.

$$E(m_c \bmod N_k, w \bmod N_k) = g_k^{m_c} w^{N_k} \bmod N_k^2 \quad (37)$$

4.1.3. Decryption

Assume that $c \in \mathbb{Z}_{N_k}^*$ is ciphertext and $D(\cdot)$ is the decryption operation with the private key λ_k .

$$D(c) = \frac{L(c^{\lambda_k \bmod N_k^2})}{L(g_k^{\lambda_k \bmod N_k^2})} \bmod N_k \tag{38}$$

To secure the Paillier cryptosystem’s privacy, parameter N_k and g_k should be big enough. $\forall m_{c1}, m_{c2}, w_1, w_2 \in \mathbb{Z}_N$, the formula holds:

$$E(m_{c1}, w_1)E(m_{c2}, w_2) = E(m_{c1} + m_{c2}, w_1w_2) \bmod N_k^2 \tag{39}$$

which indicates that the result of the multiple operation of two ciphertexts is equal to the encryption result of the sum of two plaintexts, and this is Paillier’s homomorphic addition characterization.

As can be seen, the plaintext should be an integer in the process of encryption, but the information exchanged might be decimals in actual applications. To make this cryptosystem useful, a constant multiple is used to amplify the plaintext.

4.2. Protocol of EEP Sharing

Firstly, an authority entity for the IMG is required, which is denoted as AU . The public key and private key of the AU are denoted as $\langle N_{AU}, g_{AU} \rangle$ and λ_{AU} . The public key $\langle N_{AU}, g_{AU} \rangle$ is known to every MG participating in the IMG, and the private key λ_{AU} is only known by the AU itself.

Secondly, the sharing for the EEP of every MG is implemented in a series manner. The route of information delivery must be fixed and known to every MG for each iteration.

As we know, x_n^{in} is the private data of $MG n$, and its ciphertext encrypted by the public key of AU can be denoted as $E(x_n^{in})$, which is transmitted from $MG n$ to $n + 1$. After each step, AU is the last receiver of the ciphertext and uses its private key to decrypt and broadcast the data to all of the MGs . The detailed information exchange procedure is listed as follows (see Figure 3).

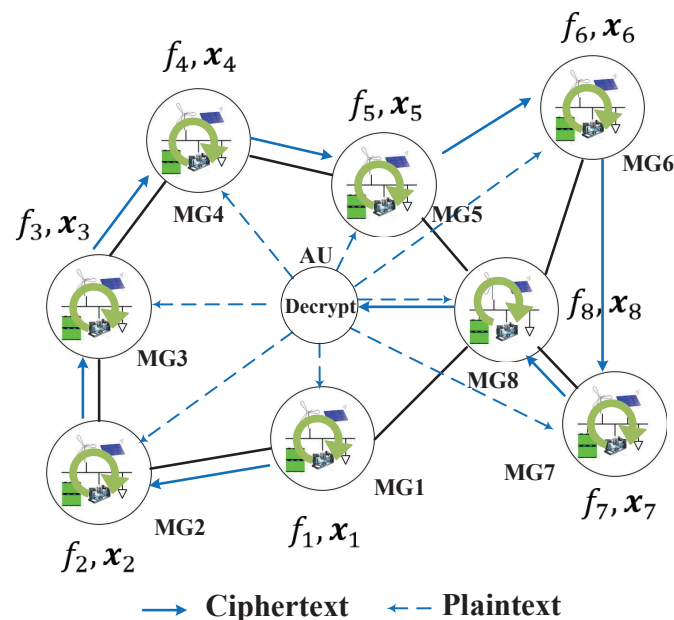


Figure 3. Information transmission process of the privacy-preserving strategy.

Step 1: Every MG optimizes its own EEP x_n^{in} , encrypts the plaintext by using AU 's public key and gets the ciphertext $E(x_n^{in})$.

Step 2: MG 1 transmits $E(x_1^{in})$ to MG 2, and then MG 2 should calculate as:

$$E(x_1^{in} + x_2^{in}) = E(x_1^{in})E(x_2^{in}). \quad (40)$$

After calculation, $E(x_1^{in} + x_2^{in})$ is transferred to the next MG and does the same operation until the last MG.

$$E(\sum_{n=1}^N x_n) = \prod_{n=1}^N E(x_n^{in}) \quad (41)$$

Step 3: The last MG N sends the cipher data to AU , and AU has the private key to perform the decryption process. Finally, the average EEP for distributed optimization is broadcast to all MGs.

$$\bar{x}^{in} = \frac{1}{N} \sum_{n=1}^N x_n^{in} \quad (42)$$

4.3. Security Analysis of the Protocol

We use the semi-honest security model to analyze the protocol [40]. This model assumes that the involved parties, in our case MG 1 to MG N and the AU , perform the protocol steps properly, but are also allowed to store the messages from previous steps in an attempt to deduce more information than they are entitled to. Based on the semi-honest model, we can enumerate three different attack scenarios: (1) all of the MGs are trustful, but the AU is untrustful; (2) some of the MGs are untrustful and collusive, but the AU is trustful; (3) some of the MGs are untrustful and collusive, and the AU is also untrustful.

- For the first scenario, the sensitive data of each MG x_n^{in} are encrypted and delivered on a fixed path. The AU can receive the ciphertext of summing EEP $E(\sum_{n=1}^N x_n)$. Although the plaintext can be decrypted as $\sum_{n=1}^N x_n$, the actual data of arbitrary MGs cannot be deduced.
- For the second scenario, as the EEP of each MG is encrypted by the public key of AU $E(x_n^{in})$, even if there are a number of collusive MGs, the plaintext of any MGs cannot be obtained without the private key of AU .
- For the third scenario, we assume that there are N_c collusive MGs. (a) When $N_c = N - 1$, that is only one non-collusive MG exists (denoted as MG-a), then, the MG-a is the target of the collusive MGs. In this case, if all of the collusive MGs can share their own plaintexts with the AU or set their EEPs to zero, the AU can get the privacy data of MG-a. Otherwise, the privacy of MG-a still can be guaranteed. However, this condition is difficult to achieve, since it would also affect the privacy of the collusive MGs or make it easy to be detected by MG-a. (b) When $N_c < N - 1$, that is the number of non-collusive MGs is not less than two. Similar to the condition of $N_c = N - 1$, the untrustful AU can only get the sum of EEPs from the non-collusive MGs (e.g. $\sum_{n=1}^{N-N_c} x_n$) even with the worst conditions.

Therefore, the privacy-preserving protocol can guarantee the privacy of every MG under the check of the semi-honest model.

5. Case Study

5.1. Basic Data

As shown in Figure 4, an IMG composed of three MGs is used to test the proposed distributed scheduling method. The parameters of DERs and BESS are listed in Tables 1 and 2, respectively.

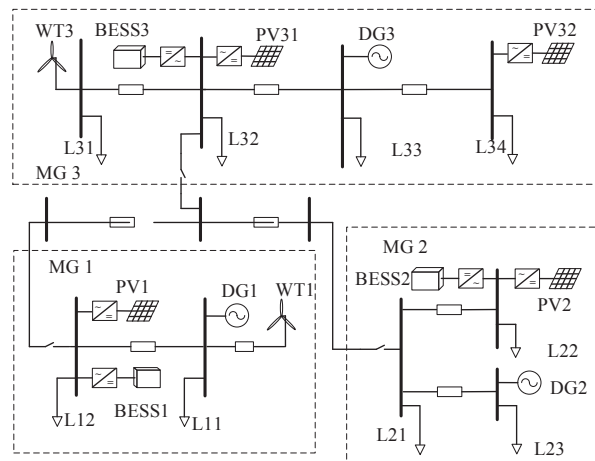


Figure 4. Structure of the IMG.

Table 1. Parameters of the distributed energy resources (DERs). WT, wind turbine.

DER	Rated Capacity (kW)	DER	Rated Capacity (kW)
MG1.WT1	500	MG3.PV3	800
MG1.PV1	500	MG1.DG1	500
MG2.PV2	800	MG2.DG2	800
MG3.WT3	500	MG3.DG3	1000

Table 2. Parameters of the battery energy storage systems (BESSs).

BESS	Rated Power (kW)	Rated Energy (kWh)	I (CYN)
MG1.BESS1	250	800	800,000
MG2.BESS2	350	1000	1,000,000
MG3.BESS3	400	1200	1,200,000

In the case study, 15 min is set as the length of a time slot. That is, there are 96 time slots in a day. The optimization is solved in a distributed manner by using the short-term forecasted power of PVs, WTs and loads, and only the encrypted information of the EEP should be delivered during the process of optimization. The net load curves of the MGs and the total net load curve of the IMG are shown in Figure 5.

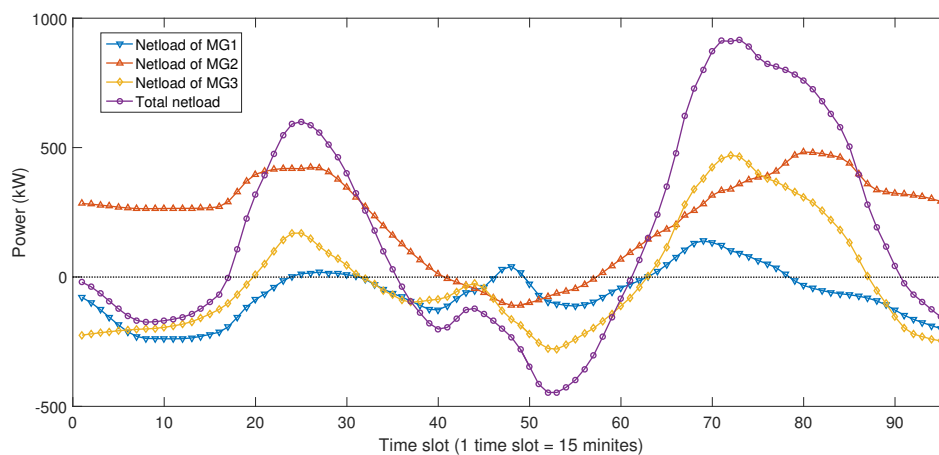


Figure 5. Net power curves of the MGs.

Apparently, these MGs have different net load profiles. The IMG has negative net load in Time Slots 1–17, 33–61 and 91–96. In these time slots, BESSs need to store the excess renewable energy. While in other time slots, BESSs or DGs should discharge or generate power to satisfy the load demand, considering their operation costs.

5.2. Result and Analysis of the Distributed Optimal Scheduling

The convergence of the distributed algorithm in each time slot is shown in Figure 6. The algorithm can achieve convergence in 40–50 iterations for almost every time slot, which indicates that the ADMM has good performance on solving this problem. Moreover, to analyze the evolution of the internal variables of three MGs, the 26th time slot in the scheduling horizon is chosen as an example, as shown in Figure 7. During the iteration process, the results show that each MG has decided its own scheduling scheme with the interaction of the shared EEP values, and all of the MGs finally approach the global optima without any changes for their solutions.

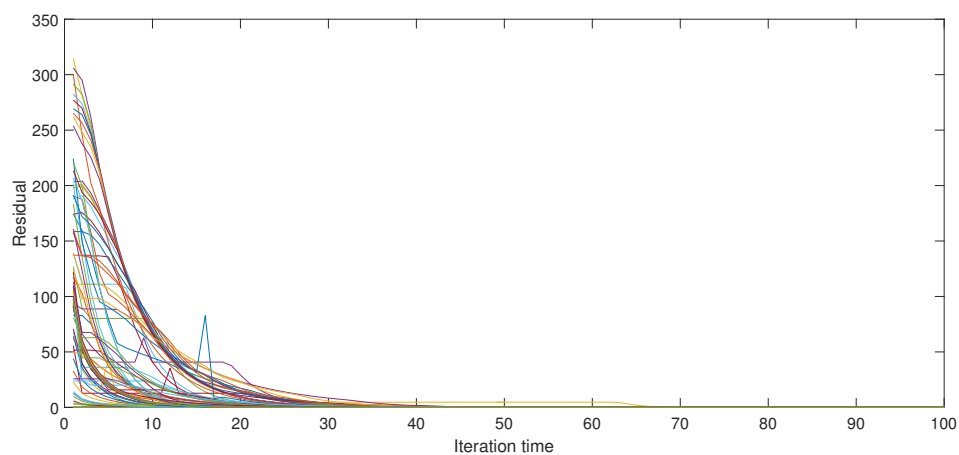


Figure 6. Convergence of the distributed optimization algorithm.

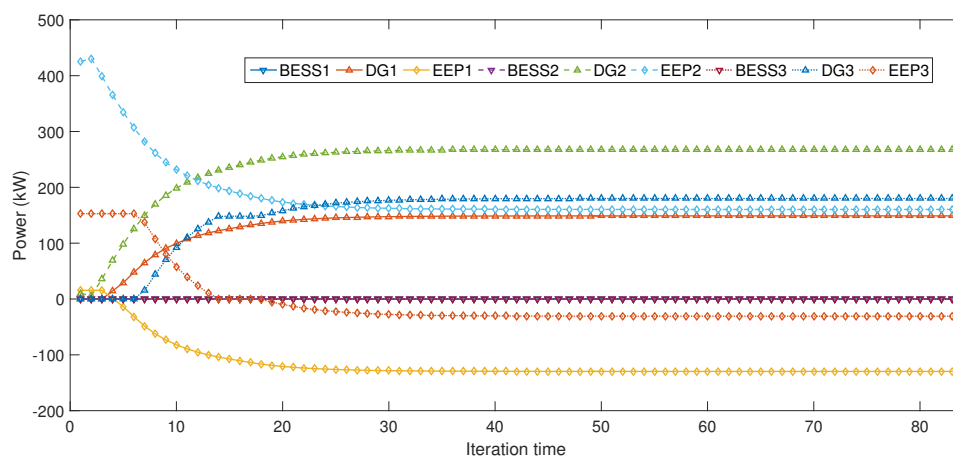


Figure 7. Evolution of the internal variables for the 26th time slot.

The output power curves of all of the controllable DERs are shown in Figure 8, and the curves of power exchanged via the connecting tie lines are shown in Figure 9. In Time Slots 1–17, 33–61 and 91–96, the total power of PVs and WTs is much higher than the load demand, so the BESSs are working in charging mode to store the surplus RES energy (the values are negative in Figure 8).

When the PVs and WTs cannot satisfy the load demand, the BESSs and DGs are scheduled to discharge or generate power and, thus, secure the IMG's operation. The output power of each controllable energy resource is decided by the cost characteristics. In Figure 8, we can find out that the energy of BESSs is utilized as first priority when there is a shortage of RES (i.e., Time Slots 15–25 and 61–71). After that, the DGs are scheduled to generate the remaining shortages (i.e., Time Slots 25–35 and 71–91). Furthermore, Figure 9 shows the curves of the decided exchanging power of different tie lines in the IMG. Combined with Figures 5, 8 and 9, the results show that the distributed optimal scheduling is reasonable for the operation of the IMG.

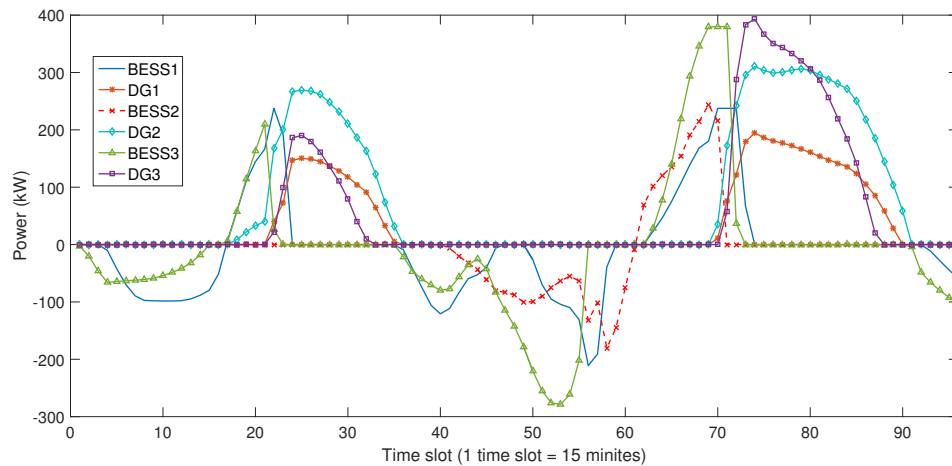


Figure 8. Scheduling results of the controllable DERs using the distributed optimization.

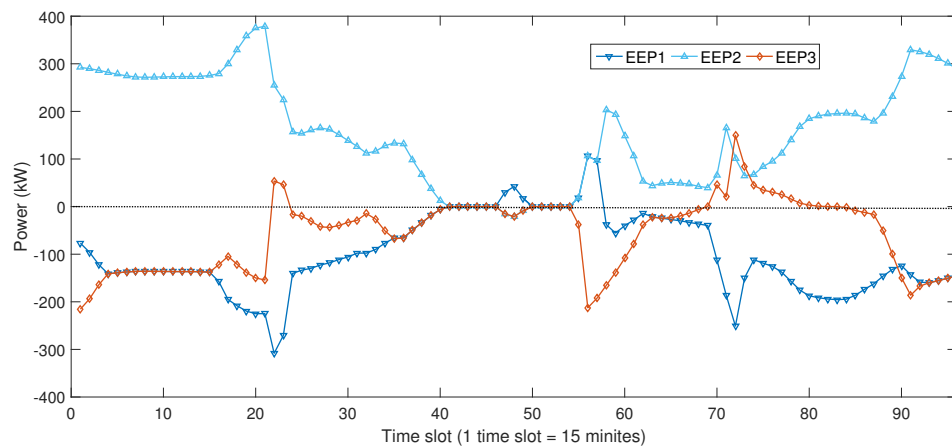


Figure 9. Decided exchanging power among MGs.

5.3. Comparison with the Centralized Optimization

The operation costs of the IMG are respectively obtained by using the centralized optimization and the distributed optimization, shown in Figure 10 and Table 3. The results show that the distributed optimal scheduling method is approximately the same as the centralized optimization; there are only minor errors in several time slots, which are mainly because of the rounding errors in the calculation.

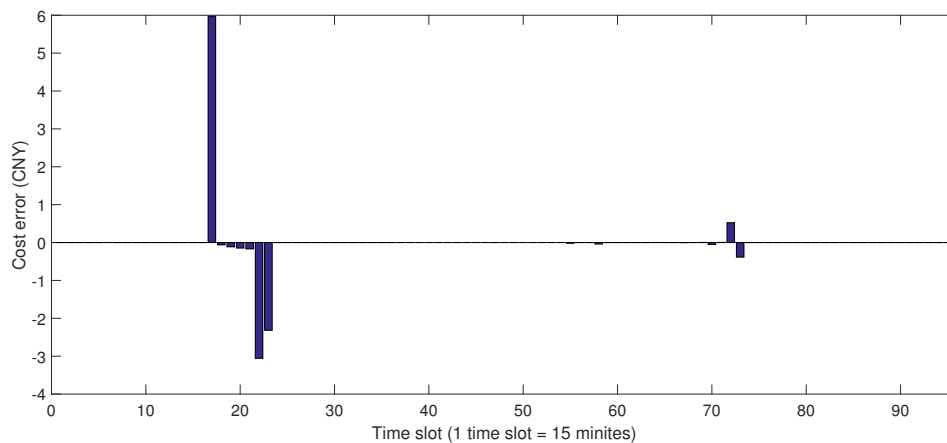


Figure 10. Errors between the operation cost of centralized optimization and distributed optimization.

Table 3. Comparison of the operation cost by using the centralized and distributed optimization.

MGs	Centralized Optimization (CNY)	Distributed Optimization (CNY)
MG1	3211.63	3213.14
MG2	6754.12	6747.35
MG3	5515.76	5520.88
Total	15,481.52	15,481.37

5.4. Comparison of Operation Cost between the Isolated Mode and Interconnected Mode

Assuming that all of the MGs can be operated in the isolated or interconnected mode, the operation cost of both modes are given in Table 4.

Table 4. Cost and discarded renewable energy resources (RES) energy in isolated and interconnected operation.

MGs	Cost of Isolated Operation (CNY)	Discarded RES Energy of Isolated Operation (kWh)	Cost of Interconnected Operation (CNY)	Discarded RES Energy of Interconnected Operation (kWh)
MG1	190.21	1128.13	2815.83	0
MG2	18,616.30	0	5856.92	0
MG3	4622.87	846.46	5307.43	0
Total	23,429.38	1974.59	15,481.37	0

In the isolated operation mode, the results show that there is discarded RES energy in MG1 and MG3. Due to the low load requirements and limited BESS in these two MGs, the RES energy cannot be fully utilized. Finally, the discarded energy has a great influence on the operation cost of MGs. As for the comparison, in the interconnected mode, the results show that the MGs are highly complementary in RES energy consumption, which has significantly decreased the overall cost of IMG.

5.5. Operation Cost Analysis for the Different Configured Capacities of BESS

Assuming that the BESS capacity has been changed from 0.7–1.2-times the original capacity in Table 1, the sensitivity analysis of the overall operation costs with different capacities of the BESS in MGs is shown in Figure 11. The results show that the cost change tendency can be categorized as two stages. First, from 0.7–0.9, the operation cost of IMG is reduced in this stage. This is mainly due to the discarded power of RESs having been decreased with the increasing of the BESS capacity, which eventually saves the cost of DGs. Second, from 0.9–1.2, the operation cost of IMG is increased with

the increasing of the BESS capacity. Considering that no more discarded RES power can be saved, the overall cost of IMG has been increased with the investment of BESS.

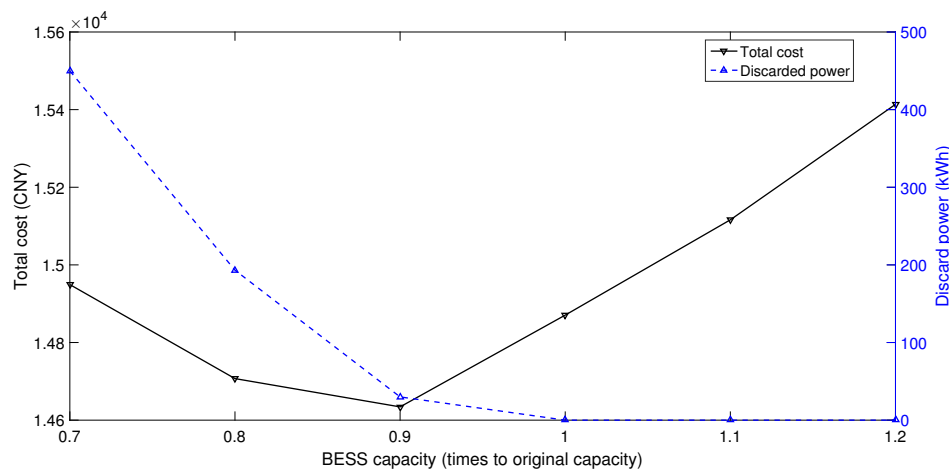


Figure 11. Sensitivity analysis for the different capacities of BESS.

5.6. Analysis for the Impact of Forecasting Errors

In the optimal scheduling, the solutions are obtained based on the short-term forecasting of RES power and load. In fact, the forecasting errors may cause unbalance between the generations and loads. Thus, in the interconnected operation, we assume that all of the MGs are working in the fixed power control of interconnection tie-lines. In this regard, all of the forecasting errors of load and RES could result in the autonomous power regulation of BESS or diesel generators in each MG, to keep the power balance and possible cost deviations by the MG itself. The detail of this control model can be found in [15]. Moreover, to analyze the influence of operation cost caused by the uncertain forecasting errors, we assume that the forecasting errors are randomly located in $[-10\%, 10\%]$ [30]. By using the control model [15], the final operation cost with balance regulations is shown in Table 5.

Table 5. Operation cost of the MGs considering the forecasting errors.

MGs	Distributed Scheduling (CNY)	Considering Forecasting Error (CNY)	Cost Errors (%)
MG1	3213.14	3040.24	−5.38
MG2	6747.35	6758.25	+0.16
MG3	5520.88	5396.10	−2.2
Total	15,481.37	15,194.60	−1.85

The results show that the forecasting errors have very limited influence on the total cost of IMG, in which the costs of MG1 and MG3 are reduced and the cost of MG2 is increased. It is apparent that the forecasting errors have the largest impact on the cost of MG1. Considering that MG1 has the largest capacity of RES, this is reasonable in the operation.

5.7. Efficiency Analysis of the Privacy-Preserving Protocol

As the privacy-preserving strategy is implemented as a series procedure in a wide area distributed environment, it is important to test the time requirement to finish the whole process of the distributed optimization. Therefore, we construct an experimental platform consisting of several computers and 3G communication networks. After complete implementation of one day's 96 time slot optimization, the execution time for each procedure is listed in Table 6, including the objection function solution, encryption, communication and decryption.

Table 6. Execution time of the experiment.

	Scheduling (s)	Encryption (s)	Transmission (s)	Decryption (s)
Average	0.0269	0.0042	1.887	0.0039
Minimize	0.0146	0.0032	1.33	0.0036
Maximize	0.0617	0.0098	3.15	0.0052

As shown in Figure 6, almost all of the scheduling of every time slot can be converged in around 50 iterations. Combined with the privacy-preserving protocol and the results of Table 6, the time requirement for one scheduling time slot can be finished in around 10 min. The result means that the minimum length of one time slot for the scheduling should be more than 10 min. Therefore, the method is suitable for the IMG's optimal scheduling problem of day ahead, hour ahead and even 15 min ahead.

6. Conclusions

A privacy-preserving distributed scheduling method for IMG with battery storage and renewable energy resources is proposed. According to the case study and experiment results, the method has almost the same optimization result with the centralized optimization, and the privacy of each MG can also be guaranteed. The processes of the iteration algorithm and privacy-preserving have delayed the implementation time of optimal scheduling, but still can be accepted for the condition with the minimum time slot longer than 10 min, which is suitable for the optimal scheduling problem of IMG.

The proposed method can be extended in several ways. Firstly, one interesting problem is the involvement of flexible loads (i.e., shiftable appliances, controllable heating, ventilation and air conditioning loads, etc.). In this scenario, the MG operator can choose to adjust the load, the generation of DGs or trade with other MGs, with the comprehensive consideration of the generation cost, trading price, load characteristic and demand response cost. Secondly, another interesting problem is the time horizon of optimization. In energy management that includes multiple time periods, the intertemporal constraint for remaining energy of BESS should be further considered. This constraint may have an influence on the distributed model, which needs further study. Finally, as the participating MGs are assumed to work as a coalition, the basic principle for forming a coalition and the related re-distribution strategy of cooperative benefits by using the IMG still need further research.

Acknowledgments: This work was supported in part by the National High-tech R&D Program of China (863 Program) (No. 2014AA052001) and in part by the Fundamental Research Funds for the Central Universities (No. 2015ZD02).

Author Contributions: The paper was a collaborative effort between the authors. Nian Liu, Cheng Wang, Minyang Cheng and Jie Wang contributed collectively to the theoretical analysis, modeling, simulation and manuscript preparation.

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

References

1. Liu, N.; Chen, Q.; Liu, J.; Lu, X. A Heuristic Operation Strategy for Commercial Building Microgrids Containing EVs and PV System. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2560–2570.
2. Ourelidis, K.O.; Bakirtzis, E.A.; Demoulias, C.S. Frequency-based control of islanded microgrid with renewable energy sources and energy storage. *J. Mod. Power Syst. Clean Energy* **2016**, *4*, 1–9.
3. Resende, F.; Gil, N.; Lopes, J. Service restoration on distribution systems using Multi-MicroGrids. *Eur. Trans. Electr. Power* **2011**, *21*, 1327–1342.
4. Shahnia, F.; Chandrasena, R.P.; Rajakaruna, S.; Ghosh, A. Primary control level of parallel distributed energy resources converters in system of multiple interconnected autonomous microgrids within self-healing networks. *IET Gener. Transm. Distrib.* **2014**, *8*, 203–222.

5. Nutkani, I.U.; Loh, P.C.; Blaabjerg, F. Distributed operation of interlinked AC microgrids with dynamic active and reactive power tuning. *IEEE Trans. Ind. Appl.* **2013**, *49*, 2188–2196.
6. Kamel, R.M.; Chaouachi, A.; Nagasaka, K. Analysis of transient dynamic response of two nearby micro-grids under three different control strategies. *Low Carbon Econ.* **2010**, *1*, 39.
7. Pashajavid, E.; Shahnia, F.; Ghosh, A. Interconnection of two neighboring autonomous microgrids based on small signal analysis. In Proceedings of the 2015 9th International Conference on Power Electronics and ECCE Asia (ICPE-ECCE Asia), Seoul, Korea, 1–5 June 2015; pp. 213–220.
8. Werth, A.; Kitamura, N.; Tanaka, K. Conceptual Study for Open Energy Systems: Distributed Energy Network Using Interconnected DC Nanogrids. *IEEE Trans. Smart Grid* **2015**, *6*, 1621–1630.
9. Koyanagi, K.; Hida, Y.; Yokoyama, R.; Nagata, S.; Nakao, K.; Hirai, T. Electricity cluster-oriented network: A grid-independent and autonomous aggregation of micro-grids. In Proceedings of the 2010 International Symposium Modern Electric Power Systems (MEPS), Wroclaw, Poland, 20–22 September 2010; pp. 1–6.
10. Che, L.; Shahidehpour, M.; Alabdulwahab, A.; Al-Turki, Y. Hierarchical Coordination of a Community Microgrid with AC and DC Microgrids. *IEEE Trans. Smart Grid* **2015**, *6*, 3042–3051.
11. Kumar, M.; Srivastava, S.C.; Singh, S.N.; Ramamoorthy, M. Development of a control strategy for interconnection of islanded direct current microgrids. *IET Renew. Power Gener.* **2014**, *9*, 284–296.
12. Shafiee, Q.; Dragicevic, T.; Vasquez, J.C.; Guerrero, J.M. Hierarchical control for multiple dc-microgrids clusters. *IEEE Trans. Energy Convers.* **2014**, *29*, 922–933.
13. Moayed, S.; Davoudi, A. Distributed Tertiary Control of DC Microgrid Clusters. *IEEE Trans. Power Electron.* **2016**, *31*, 1717–1733.
14. Zhao, H.; Qiuwei, W.U.; Wang, C.; Cheng, L.; Rasmussen, C.N. Fuzzy logic based coordinated control of battery energy storage system and dispatchable distributed generation for microgrid. *J. Mod. Power Syst. Clean Energy* **2015**, *3*, 422–428.
15. Li, Y.; Liu, N.; Zhang, J. Jointly optimization and distributed control for interconnected operation of autonomous microgrids. In Proceedings of the 2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA), Pathumwan Bangkok, Thailand, 3–6 November 2015; pp. 1–5.
16. Gregoratti, D.; Matamoros, J. Distributed Energy Trading: The Multiple-Microgrid Case. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2551–2559.
17. He, M.; Giesselmann, M. Reliability-constrained self-organization and energy management towards a resilient microgrid cluster. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2015; pp. 1–5.
18. Das, K.; Kargupta, H.; Bhaduri, K. A local distributed peer-to-peer algorithm using multi-party optimization based privacy preservation for data mining primitive computation. In Proceedings of the 2009 IEEE Ninth International Conference on Peer-to-Peer Computing, P2P'09, Seattle, WA, USA, 9–11 September 2009; pp. 212–221.
19. Liu, N.; Chen, J.; Zhu, L.; Zhang, J.; He, Y. A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. *IEEE Trans. Ind. Electron.* **2013**, *60*, 4746–4756.
20. Rottondi, C.; Barbato, A.; Chen, L.; Verticale, G. Enabling Privacy in a Distributed Game-Theoretical Scheduling System for Domestic Appliances. *IEEE Trans. Smart Grid* **2016**, doi:10.1109/TSG.2015.2511038.
21. Chen, Z.; Wu, L. Residential Appliance DR Energy Management with Electric Privacy Protection by Online Stochastic Optimization. *IEEE Trans. Smart Grid* **2013**, *4*, 1861–1869.
22. Yang, L.; Chen, X.; Zhang, J.; Poor, H.V. Cost-Effective and Privacy-Preserving Energy Management for Smart Meters. *IEEE Trans. Smart Grid* **2015**, *6*, 486–495.
23. Acs, G.; Castelluccia, C. *I Have a DREAM! (Differentially Private Smart Metering)*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 118–132.
24. Marmol, F.G.; Sorge, C.; Ugus, O.; Perez, G.M. Do not snoop my habits: Preserving privacy in the smart grid. *IEEE Commun. Mag.* **2012**, *50*, 166–172.
25. Badra, M.; Zeadally, S. Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 321–329.
26. Gan, L.K.; Shek, J.; Mueller, M. Hybrid wind-photovoltaic-diesel-battery system sizing tool development using empirical approach, life-cycle cost and performance analysis: A case study in Scotland. *Energy Convers. Manag.* **2015**, *106*, 479–494.

27. Zhou, N.; Liu, N.; Zhang, J.; Lei, J. Multi-Objective Optimal Sizing for Battery Storage of PV-Based Microgrid with Demand Response. *Energies* **2016**, *9*, 591.
28. Ogunjuyigbe, A.S.O.; Ayodele, T.R.; Akinola, O.A. Optimal allocation and sizing of PV/Wind/Split-diesel/Battery hybrid energy system for minimizing life cycle cost, carbon emission and dump energy of remote residential building. *Appl. Energy* **2016**, *171*, 153–171.
29. Salazar, J.; Tadeo, F.; Prada, C.D. A microgrid library in a general simulation language. *IFAC Proc. Vol.* **2014**, *47*, 3599–3604.
30. Liu, N.; Tang, Q.; Zhang, J.; Fan, W.; Liu, J. A hybrid forecasting model with parameter optimization for short-term load forecasting of micro-grids. *Appl. Energy* **2014**, *129*, 336–345.
31. Shi, W.; Xie, X.; Chu, C.C.; Gadh, R. Distributed Optimal Energy Management in Microgrids. *IEEE Trans. Smart Grid* **2015**, *6*, 1137–1146.
32. Nguyen, T.A.; Crow, M. Stochastic Optimization of Renewable-Based Microgrid Operation Incorporating Battery Operating Cost. *IEEE Trans. Power Syst.* **2015**, *31*, 2289–2296.
33. Zhao, B.; Zhang, X.; Chen, J.; Wang, C.; Guo, L. Operation optimization of standalone microgrids considering lifetime characteristics of battery energy storage system. *IEEE Trans. Sustain. Energy* **2013**, *4*, 934–943.
34. Saad, W.; Han, Z.; Poor, H.V. Coalitional Game Theory for Cooperative Micro-Grid Distribution Networks. In Proceedings of the 2011 IEEE International Conference on Communications Workshops (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
35. Boyd, S.; Parikh, N.; Chu, E.; Peleato, B.; Eckstein, J. Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers. *Found. Trends Mach. Learn.* **2011**, *3*, 1–122.
36. Sulc, P.; Backhaus, S.; Chertkov, M. Optimal distributed control of reactive power via the alternating direction method of multipliers. *IEEE Trans. Energy Convers.* **2014**, *29*, 968–977.
37. Erseghe, T. Distributed optimal power flow using ADMM. *IEEE Trans. Power Syst.* **2014**, *29*, 2370–2380.
38. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Springer: Heidelberg, Germany, 1999; pp. 223–238.
39. Lu, R.; Liang, X.; Li, X.; Lin, X.; Shen, X.S. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1621–1631.
40. Jung, T.; Li, X.Y. Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 45–57.



© 2016 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).