2016 IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications

Masking Method for Local Information on Distributed Optimization with Constraints

Kazuma Wada
Graduate School of Engineering
Tottori University, Koyama-Minami, Japan
Email: M15T1029C@edu.tottori-u.ac.jp

Kazunori Sakurama
Graduate School of Engineering
Tottori University, Koyama-Minami, Japan
Email: sakurama@mech.tottori-u.ac.jp

***Abstract*—We propose a masking method to protect agents' privacy for distributed optimization. In the proposed method, Agents add some signals to the own original state to conceal private information. To obtain the correct solution of the optimization problem, they exchange the added signals and subtract the received signals from the own state. Finally, we apply it to a microgrid and show that the supply-demand balance is kept via real-time pricing while protecting privacy of agent.**

I. INTRODUCTION

Distributed optimization methods have been actively studied and applied to various fields including power network systems[1], wireless sensor networks[2] and robotics[3]. In these problems, agent $i \in \{1, 2, \ldots, n\}$ which has a state variable $x_i \in \mathbb{R}$ is defined and they try to achieve a common task with constraints. This problem is formulated by an optimization problem with an objective function $F(x) \in \mathbb{R}$ and a constraint function $G(x) \in \mathbb{R}$ where $x = [x_1, x_2, \ldots, x_n]^\top$. The Lagrange function is defined as $L(x, \lambda) = F(x) + \lambda^\top G(x)$ to solve it, where $\lambda \in \mathbb{R}$ denotes the Lagrange multiplier.

In standard distributed optimization techniques[4], it is assumed that supervisors gathering all agents' states to update λ exist. On the other hand, a distributed algorithm without supervisors is proposed[5]. In [5], each agent exchanges the estimate of λ over a communication network. Then, agents can obtain the correct value of λ by themselves.

However, this approach has an information leakage problem, since agents exchange their states x_i with each other, where x_i includes private information, e.g. the power amount in smart grids[6]. The distributed optimization considering a privacy protection is proposed[7]. The approach is based on differencial privacy[8], and to protect agents' privacy, signals based on the differential privacy are added to information. However, the problem is that the correct optimization solution is not obtained because the added signals work as noises.

In this paper, we provide a masking method to protect agents' privacy in [5]. In this method, local information is added some random signals. Then, the added signals are exchanged in a proper way to obtain the correct solution. We prove that it is obtainable with the proposed method. Moreover, we evaluate the privacy protection performance by the correlation coefficient between the masked and original value. We also discuss a trade-off between the privacy protection and an optimization time-cost. The time-cost tends to be higher as the privacy protection performance is higher. Then, we give a property of the additional signal to achieve both of the privacy protection and the time-cost.

Finally, we apply the proposed method to real-time pricing[9] in a microgrid. A microgrid is a small power grid consisting of distributed generators, energy storage and power consumption facilities[10]. The components are expected to be controlled distributedly to disperse communication loads and realize scalability[11]. In this case, agents' states x_i represents a power amount, which is the private data of the components, and the Lagrange multiplier λ represents the electricity price. The security issue exists in sharing information to update the electricity price. We show that the supply-demand balance is controlled without the security issue by the proposed method.

II. PROBLEM SETTING

A. Distributed Optimization

Assume that agent $i \in \mathcal{V} = \{1, 2 \ldots, n\}$ has a state variable $x_i \in \mathbb{R}$. Agents have a common task with constraints. The task is formulated by an optimization problem with an objective function $F(x) \in \mathbb{R}$ and a constraint function $G(x) \in \mathbb{R}$

$$\begin{cases} \text{minimize} & F(x) \\ \text{subject to} & G(x) = 0 \end{cases} \tag{1}$$

where $x = [x_1, x_2, \ldots, x_n]^\top$.

The Lagrange method[12] is used as a solution of (1). The Lagrange function is written as $L(x, \lambda) = F(x) + \lambda^\top G(x)$ where $\lambda \in \mathbb{R}$ is the Lagrange multiplier. The algorithm is shown as Algorithm 1.

Algorithm 1 The centralized Lagrange algorithm

Require: The initial vectors $x_i^{[0]} \in \mathbb{R}$, $\lambda^{[0]} \in \mathbb{R}$ and constants α, β. The step $s = 0$ and the terminal step $S \in \mathbb{N}$.

[1.1] Set $x_i[0] = x_i^{[s]}$ and execute the recursive computation

$$x_i[k+1] = x_i[k] - \alpha \frac{\partial L}{\partial x_i}(x[k], \lambda^{[s]})$$

for k. Then, update $x_i^{[s]}$ to $x_i^{[s+1]} = \lim_{k\to\infty} x_i[k]$.

[1.2] Update λ according to the following update rule.

$$\lambda^{[s+1]} = \lambda^{[s]} + \beta G(x^{[s]}) \tag{2}$$

[1.3] If $s < S$, $s = s + 1$ and return to [1.1]. If $s = S$, stop the step.

978-1-5090-4403-0/16 $31.00 © 2016 IEEE
DOI 10.1109/CPSNA.2016.20

Here, let $x_i^{[s]}, \lambda^{[s]}$ be the update value in step s, and $x_i[k]$ denotes the update value to decide $x_i^{[s+1]}$. Algorithm 1 is a centralized optimization because updates λ based on $G(x)$ including all agents' local information in (2).

On the other hand, a distributed update rule of the Lagrange multiplier is proposed in [5]. It is realized by exchanging information over a communication network N. Fig. 1 shows an example of N, where the edges represent communiction links. Assume that $G(x)$ is the sum of the agent-wise functions $\bar{G}_i(x_i^{[s]}) \in \mathbb{R}$ as $G(x) = \sum_{i=1}^{n} \bar{G}_i(x_i)$. Here, $\bar{G}_i(x_i)$ includes private information. The algorithm is shown as Algorithm 2.

Algorithm 2 The distributed Lagrange algorithm

Require: The initial vectors $x_i^{[0]} \in \mathbb{R}$, $\hat{\lambda}^{[0]} \in \mathbb{R}$ and constants α, β, ϵ. The step $s = 0$ and the terminal step $S \in \mathbb{N}$.

[2.1] Set $x_i[0] = x_i^{[s]}$ and execute the recursive computation

$$x_i[k+1] = x_i[k] - \alpha \frac{\partial L}{\partial x_i}(x[k], \hat{\lambda}_i^{[s]})$$

for k. Then, update $x_i^{[s]}$ to $x_i^{[s+1]} = \lim_{k\to\infty} x_i[k]$.

[2.2] Update $\hat{\lambda}_i$ based on the following equations.

$$\theta_i[0] = \hat{\lambda}_i^{[s]} + \beta \bar{G}_i(x_i^{[s]}) \tag{3}$$

$$\theta_i[k+1] = \theta_i[k] - \epsilon \sum_{j\in\mathcal{N}_i} (\theta_i[k] - \theta_j[k]) \tag{4}$$

Then, update $\hat{\lambda}_i^{[s]}$ to $\hat{\lambda}_i^{[s+1]} = \lim_{k\to\infty} \theta_i[k]$.

[2.3] Execute the same procedure as [1.3]

Here, let $\mathcal{N}_i$ be the adjacent set of agent i on N, $\theta_i[k]$ be a state variable to calculate $\hat{\lambda}_i^{[s]}$. $\theta_i[0]$ is calculated by the corresponding agent in (3). Then, (4) updates $\theta_i[k]$ by the consensus control. As a result, all $\hat{\lambda}_i^{[s+1]}$ agree to λ in (2)[5].

B. Privacy Leakage Problem

Algorithm 2 has a privacy leakage problem, since the state variable $\theta_i[k]$ must be exchanged between agents in (4). $\theta_i[0]$ is calculated from local information $\bar{G}_i(x_i^{[s]})$ at (3). Then, $\bar{G}_i(x_i^{[s]})$ includes agent's private state x_i. For example, x_i is agent's power amount in a power grid. Hence, private information x_i leak out by exchanging $\theta_i[k]$ at (4).

In this paper, we provide a masking method which makes a *masked value* $\hat{G}_i(x_i^{[s]})$ to protect an *original value* $\bar{G}_i(x_i^{[s]})$ against the adjacent agents. Features of this method is that the correct solution is obtained. Moreover, we evaluate $\hat{G}_i(x_i^{[s]})$ from the viewpoint of the privacy protection. When $\hat{G}_i(x_i^{[s]})$ is not consistent with $\bar{G}_i(x_i^{[s]})$, the privacy is protected. We employ the correlation coefficient to evaluate it.

Here, the mean value and variance of signals in an evaluate interval $[d, d+D] \subset [0, S]$ are expressed as $\mathrm{E}[\cdot]$ and $\mathrm{Var}[\cdot]$, where d is an initial step and D is a number of sample steps. Then, $\mathrm{E}\big[\hat{G}_i(x_i)\big]$ is expressed by $\mathrm{E}\big[\hat{G}_i(x_i)\big] = \frac{1}{D}\sum_{s=d}^{d+D} \hat{G}_i(x_i^{[s]})$. $\mathrm{E}\big[\hat{G}_i(x_i)\big]$ represents the mean value of the masked value $\hat{G}_i(x_i)$. $\mathrm{Var}\big[\hat{G}_i(x_i)\big]$ represents the variance the masked value $\hat{G}_i(x_i)$. The covariance of the masked value and original value is given as $\mathrm{Cov}\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]$.

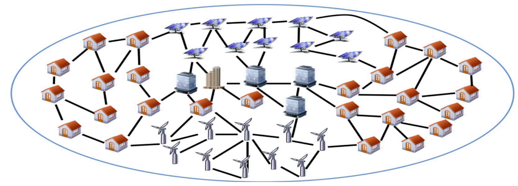

Fig. 1. Communication Network

Consequently, the correlation coefficient between $\hat{G}_i(x_i)$ and $\bar{G}_i(x_i)$ can be written as

$$\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big] = \frac{\mathrm{Cov}\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]}{\sqrt{\mathrm{Var}\big[\hat{G}_i(x_i)\big]\mathrm{Var}\big[\bar{G}_i(x_i)\big]}}, \tag{5}$$

where $\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big] \in [-1, 1]$. If the absolute value of it is close to zero, $\hat{G}_i(x_i)$ and $\bar{G}_i(x_i)$ are uncorrelated. Thus, (5) needs to be suppressed for privacy protection as

$$\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big] \le \delta_a \tag{6}$$

where δ_a is a threshold of the correlation coefficient. In general, a correlation coefficient is considered to be sufficiently small if it is less than 0.2[13].

Next, the optimization time-cost is mainly due to the consensus convergence of the estimated Lagrange multipliers $\hat{\lambda}_i^{[s]}$ at [2.2]. The convergence depends on a communication network structure and the variance of $\theta_i[0]$. Assume that $\hat{\lambda}_i^{[s]}$ almost match with all agents, the variance of $\hat{G}_i(x_i^{[s]})$ decide the convergence. The variance of $\hat{G}_i(x_i^{[s]})$ is $\hat{V}(x^{[s]}) = \frac{1}{n}\sum_{i=1}^{n}\big(\hat{G}_i(x_i^{[s]}) - \frac{1}{n}\sum_{i=1}^{n}\hat{G}(x_i^{[s]})\big)^2$. $\bar{V}(x^{[s]})$ is written for the original values similarly. To decrease the optimization time-cost, $\hat{V}(x^{[s]})$ for $\bar{V}(x^{[s]})$ is expected to be suppressed within δ_b, namely,

$$\frac{\Big(\mathrm{E}\big[\hat{V}(x)\big] - \mathrm{E}\big[\bar{V}(x)\big]\Big)}{\mathrm{E}\big[\bar{V}(x)\big]} \le \delta_b. \tag{7}$$

Consider the following problem in this paper.

Problem 1. *Assume that $\delta_a, \delta_b > 0$ are given. Then, generate a masked value $\hat{G}_i(x_i)$ which satisfies the following.*

[C.1] *Optimization problem* (1) *is solved correctly when $\hat{G}_i(x_i)$ is used instead of $\bar{G}_i(x_i)$ in* [2.2].

[C.2] *Agent's privacy can be protected in the meaning of* (6).

[C.3] *$\hat{V}(x^{[s]})$ is limitted in the meaning of* (7).

III. MAIN RESULT

First, a masking method is proposed in section III-A. Then, we discuss [C.1], [C.2] and [C.3] and derive the existence conditions for $\hat{G}_i(x_i)$ in subsection III-E.

A. Proposal of Masking Method

We propose a procedure to generate $\hat{G}_i(x_i)$. First, agent i adds an additional signals $\gamma_{ij} \in \mathbb{R}$ generated accroding to the adjacent agent $j \in \mathcal{N}_i$ to the original value $\bar{G}_i(x_i)$. Secondly, agent i sends γ_{ij} to the adjacent agents j. Thirdly, agent i receives γ_{ji} from j on the network N. Finally, agent i subtracts γ_{ji} from $\bar{G}_i(x_i)$. A masked value $\hat{G}_i(x_i)$ can be obtained as

$$\hat{G}_i(x_i^{[s]}) = \bar{G}_i(x_i^{[s]}) + \sum_{j\in\mathcal{N}_i} \gamma_{ij}^{[s]} - \sum_{j\in\mathcal{N}_i} \gamma_{ji}^{[s]}. \tag{8}$$

Algorithm 3 is defined by replacing $\bar{G}_i(x_i^{[s]})$ with $\hat{G}_i(x_i^{[s]})$ in (3) of Algorithm 2.

B. Obtainability of Correct Optimization Solution

We can obtain the correct solution of (1) with Algorithm 3.

Theorem 1. *Assume that the communication network* N *is described by an undirected graph. Then, the solution obtained by Algorithm* 3 *will be the same as Algorithm* 1.

Proof. The optimization problem (1) is solved correctly by Algorithm 2 in a distributed manner under the assumption satisfying $G(x) = \sum_{i=1}^n \bar{G}_i(x_i)$. This is because $G(x)$ is obtained as a result of averaging $\bar{G}_i(x_i)$ by (4). Then, the solution by Algorithm 2 is the same as the solution by Algorithm 1[5]. Thus, we describe that Algorithm 3 can obtain the same result as Algorithm 2. Concretely, we describe that the following equation holds for an arbitrary signal γ_{ij}.

$$\sum_{i=1}^n \hat{G}_i(x_i) = \sum_{i=1}^n \bar{G}_i(x_i) \tag{9}$$

From (8), (9) can be written as

$$\sum_{i=1}^n \hat{G}_i(x_i) = \sum_{i=1}^n \bar{G}_i(x_i) + \sum_{i=1}^n \sum_{j\in\mathcal{N}_i} \gamma_{ij} - \sum_{i=1}^n \sum_{j\in\mathcal{N}_i} \gamma_{ji}. \tag{10}$$

From the relation $j \in \mathcal{N}_i \Leftrightarrow i \in \mathcal{N}_j$ in the undirected graph, $\sum_{i=1}^n \sum_{j\in\mathcal{N}_i} \gamma_{ij} = \sum_{i=1}^n \sum_{j\in\mathcal{N}_i} \gamma_{ji}$ holds. Consequently, (9) is obtained from (10). □

Hence, $\hat{G}_i(x_i)$ in (8) satisfies the condition [C.1].

C. Feature of Signals for Privacy Protection

We discuss the feature of additional signals to satisfy [C.2].

Theorem 2. *Assume that signals γ_{ij} satisfy for all $i \in \mathcal{V}, j \in \mathcal{N}_i$ the following.* (i) $\mathrm{E}[\gamma_{ij}] = 0$. (ii) $\mathrm{E}\big[\gamma_{ij}\bar{G}_i(x_i)\big] = \mathrm{E}\big[\gamma_{ij}\big]\mathrm{E}\big[\bar{G}_i(x_i)\big]$. (iii) $\mathrm{Var}\big[\gamma_{ij}+\gamma_{ji}\big] = \mathrm{Var}\big[\gamma_{ij}\big] + \mathrm{Var}\big[\gamma_{ji}\big]$. *When the adjacent set $\mathcal{N}_i$ is non-empty for all $i \in \mathcal{N}_i$, the condition* (6) *is satisfied if the following holds for all $i \in \mathcal{V}$.*

$$\min_{j\in\mathcal{N}_i} \mathrm{Var}[\gamma_{ij}] \geq \frac{(1-\delta_a^2)\mathrm{Var}\Big[\bar{G}_i(x_i)\Big]}{2\delta_a^2|\mathcal{N}_i|} \tag{11}$$

Proof. From (8), the mean of the masked value is written as

$$\mathrm{E}\big[\hat{G}_i(x_i)\big] = \mathrm{E}\Big[\bar{G}_i(x_i)\Big] \tag{12}$$

where, Assumption (i) is used.

Substitute (8) and (12) in $\mathrm{Var}\big[\hat{G}_i(x_i)\big]$,

$$\mathrm{Var}\big[\hat{G}_i(x_i)\big] = \mathrm{Var}\big[\bar{G}_i(x_i)\big] + \mathrm{Var}\Big[\sum_{j\in\mathcal{N}_i}(\gamma_{ij}-\gamma_{ji})\Big] \tag{13}$$

is obtained. Moreover, if all $\mathrm{Var}\big[\gamma_{ij}\big]$ take a minimum value in (13), the following holds from Assumption (iii).

$$\mathrm{Var}\Big[\sum_{j\in\mathcal{N}_i}(\gamma_{ij}-\gamma_{ji})\Big] \geq 2\big|\mathcal{N}_i\big| \min_{j\in\mathcal{N}_i} \mathrm{Var}[\gamma_{ij}] \tag{14}$$

$|\mathcal{N}_i|$ represents the number of xadjacent agent. From (8) and (12), $\mathrm{Cov}\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]$ can be written as

$$\begin{aligned}\mathrm{Cov}\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big] &= \mathrm{E}\Big[\Big(\bar{G}_i(x_i) - \mathrm{E}[\bar{G}_i(x_i)]\Big)^2\Big] \\ &= \mathrm{Var}\big[\bar{G}_i(x_i)\big]\end{aligned} \tag{15}$$

Therefore, from (11), (13), (14) and (15), (5) is written as

$$\begin{aligned}&\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big] \\ &\leq \sqrt{\frac{\mathrm{Var}\big[\bar{G}_i(x_i)\big]}{\mathrm{Var}\big[\bar{G}_i(x_i)\big] + 2\big|\mathcal{N}_i\big|\min_{j\in\mathcal{N}_i}\mathrm{Var}[\gamma_{ij}]}} \\ &\leq \sqrt{\frac{\delta_a^2\mathrm{Var}\big[\bar{G}_i(x_i)\big]}{\delta_a^2\mathrm{Var}\big[\bar{G}_i(x_i)\big] + (1-\delta_a^2)\mathrm{Var}\big[\bar{G}_i(x_i)\big]}}.\end{aligned} \tag{16}$$

Hence, (6) is obtained from (16). □

$\hat{G}_i(x_i^{[s]})$ generated by $\mathrm{Var}[\gamma_{ij}]$ based on (11) satisfies [C.2].

D. Feature of Signals for Optimization Time-cost

We discuss the feature of additional signals to satisfy [C.3].

Theorem 3. *Assume Assumptions* (i), (ii) *and* (iii) *of γ_{ij} in Theorem 2,* (7) *is satisfied if the following holds for all $i \in \mathcal{V}$.*

$$\max_{j\in\mathcal{N}_i} \mathrm{Var}[\gamma_{ij}] \leq \frac{n\delta_b\mathrm{E}\big[\bar{V}(x)\big]}{2\sum_{i=1}^n\big|\mathcal{N}_i\big|} \tag{17}$$

Proof. From (8), (14) and (17), $\mathrm{E}\big[\hat{V}(x)\big]$ is reduced to

$$\begin{aligned}\mathrm{E}\big[\hat{V}(x)\big] &\leq \mathrm{E}\Big[\bar{V}(x)\Big] + \frac{2}{n}\Big(\sum_{i=1}^n\big|\mathcal{N}_i\big|\Big)\Big(\max_{j\in\mathcal{N}_i}\mathrm{Var}[\gamma_{ij}]\Big) \\ &\leq \mathrm{E}\Big[\bar{V}(x)\Big] + \delta_b\mathrm{E}\Big[\bar{V}(x)\Big]\end{aligned} \tag{18}$$

Hence, (7) is satisfied from (18). □

$\hat{G}_i(x_i^{[s]})$ generated by (8) satisfies the condition [C.3] by using $\mathrm{Var}[\gamma_{ij}]$ based on (17).

E. Existence Condition of Masked Value

This subsection discusses an exsistence condition of the masked value $\hat{G}_i(x_i^{[s]})$ satisfying [C.2] and [C.3].

Theorem 4. *Assume that*

$$\delta_b \geq \max_{i\in\mathcal{V}} \frac{(1-\delta_a^2)\mathrm{Var}\big[\bar{G}_i(x_i)\big]\sum_{i=1}^n\big|\mathcal{N}_i\big|}{n\delta_a^2\big|\mathcal{N}_i\big|\mathrm{E}\big[\bar{V}(x)\big]} \tag{19}$$

is satisfied. Then, $\hat{G}_i(x_i^{[s]})$ satisfying (6) *and* (7) *exists.*

Proof. From (19), the right-hand side of (17) is reduced to

$$\frac{n\delta_b\mathrm{E}\big[\bar{V}(x)\big]}{2\sum_{i=1}^n\big|\mathcal{N}_i\big|} \geq \frac{(1-\delta_a^2)\mathrm{Var}\big[\bar{G}_i(x_i)\big]}{2\delta_a^2\big|\mathcal{N}_i\big|}$$

Then, the existence condition of $\mathrm{Var}\big[\gamma_{ij}\big]$ is obtained. From Theorems 2 and 3, $\hat{G}_i(x_i)$ satisfying [C.2], [C.3] exists. □

From Theorems 1-4, the masked value $\hat{G}_i(x_i)$ satisfying [C.1], [C.2] and [C.3] exists if (19) holds.

IV. SIMULATION

Consider the microgrid model with the communication network shown in Fig. 1. The supply-demand balance is controlled by the real-time pricing. Agent $i \in \mathcal{V} = \{1, 2, \ldots, 50\}$ exists in the grid, and has power amount $x_i \in \mathbb{R}$. The supplier and consumer set are defined as $\mathcal{V}_s = \{1, 2, \ldots, 20\}$ and $\mathcal{V}_c = \{21, 22, \ldots, 50\}$. A time variation of x_i means agent i's life pattern which is private information. Thus, leaking out x_i to other agents is insecure. We prevent it by the proposed masking method.

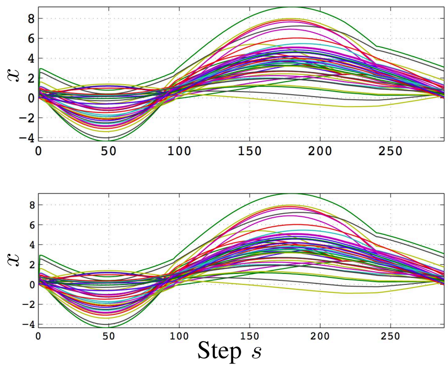

Fig. 2. Power amount of agent in regions with/without the masking method

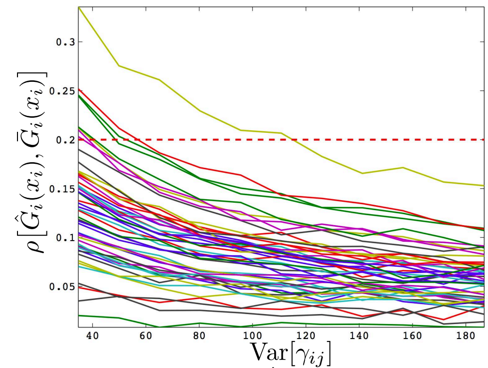

Fig. 3. Correlation coefficient $\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]$ each of $\mathrm{Var}[\gamma_{ij}]$

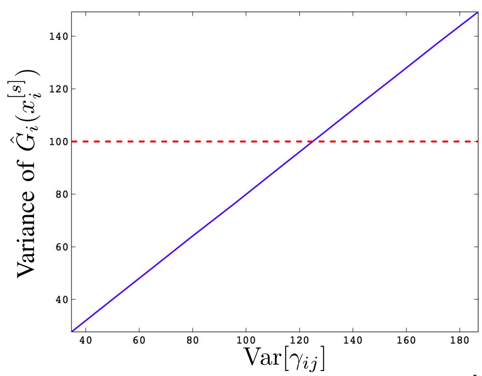

Fig. 4. The variance of the masked value each of $\mathrm{Var}[\gamma_{ij}]$

The objective function is given by $F(x) = \sum_{i\in\mathcal{V}} U_i(x_i)$. $U_i(x_i) = a_i(x_i - d_i)^2$ is the cost function of agent i, where $a_i, d_i > 0$ represent agent i's reaction rate for the lagrangian multiplier and desired consumption amount. Then, the constraint function is given by $G(x) = \sum_{i\in\mathcal{V}_s} x_i - \sum_{i\in\mathcal{V}_c} x_i$ which represents the supply-demand imbalance. To balance the power amount, $G(x) = 0$ must be satisfied. The terminal step $S = 288$, the threshold of (6) and (7) are given as $\delta_a = 0.2$, $\delta_b = 100$.

Now, we solve the optimization problem (1) by Algorithms 2 and 3. Algorithms 2 and 3 are the distributed optimization algorithms without and with the proposed method, respectively. Then, $\mathrm{Var}\big[\gamma_{ij}\big] = 120$ were chosen from $103.92 \leq \mathrm{Var}\big[\gamma_{ij}\big] \leq 124.59$ which are obtained from (11) and (17). To solve (1), the estimated Lagrange multiplier $\hat{\lambda}_i^{[s]}$ is introduced, and it regarded as the electricity price.

Fig. 2 depicts the power amount of each agent. The upper figure is the result of Algorithm 2, and the lower one is the result of Algorithm 3. They are completely the same. It shows that the correct solution of (1) is obtained by Algorithm 3.

Fig. 3 shows correlation coefficient $\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]$ for $\mathrm{Var}[\gamma_{ij}]$. The broken red line is the upper limit δ_a. $\rho\big[\hat{G}_i(x_i), \bar{G}_i(x_i)\big]$ is smaller than δ_a if $\mathrm{Var}[\gamma_{ij}]$ is chosen larger than 103.9209 as (11). Thus, we can confirm that agent's privacy is protected in the meaning of (6). Fig. 4 depicts the left-hand side of (7) for $\mathrm{Var}[\gamma_{ij}]$. The red broken line is the upper limit δ_b. Although, the left-hand side of (7) rise with increasing $\mathrm{Var}[\gamma_{ij}]$, it is suppressed within the limit δ_b when $\mathrm{Var}[\gamma_{ij}]$ is chosen smaller than 124.5856. Therefore, $\mathrm{Var}[\gamma_{ij}] = 120$ is used in the simulation.

V. CONCLUSIONS

We proposed a masking method to protect agents' privacy for the distributed optimization in [5]. It enables us to obtain the correct solution of the optimization problem. Moreover, we evaluated privacy protection performance, and showed that it can control by the variance of additional signals. Finally, we applied the proposed method to real-time pricing for the supply-demand balance in a microgrid and confirmed that the proposed method can control the supply-demand balance without leaking out private information by simulation.

REFERENCES

[1] Samadi, Pedram, et al., "Optimal real-time pricing algorithm based on utility maximization for smart grid," in Smart Grid Communications, IEEE, pp. 415-420, 2010.
[2] Rabbat, Michael, and Robert Nowak, "Distributed optimization in sensor networks," in Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 20-27, 2004.
[3] Feddema, John T., et al., "An optimization approach to distributed controls of multiple robot vehicles," IEEE/RSJ International Conference on Intelligent Robots and Systems, 2003.
[4] Boyd, Stephen, et al., "Distributed optimization and statistical learning via the alternating direction method of multipliers," Foundations and Trends in Machine Learning 3.1, pp. 1-122, 2011.
[5] Sakurama, Kazunori, and Masashi Miura, "Complete distributed optimization with constraints on networked multi-agent systems and its application to real-time pricing," Control Conference, IEEE, 2015.
[6] Gan, Lingwen, et al., "Optimal distributed protocol for electric vehicle charging," IEEE Transactions on Power Systems 28.2, pp. 940-951, 2013.
[7] Hale, M. T., and M. Egerstedty, "Differentially private cloud-based multi-agent optimization with constraints," American Control Conference, IEEE, pp. 1235-1240, 2015.
[8] Dwork, Cynthia. "Differential privacy: A survey of results," in International Conference on Theory and Applications of Models of Computation, pp. 1-19, 2008.
[9] Gans, Will, et al., "Smart meter devices and the effect of feedback on residential electricity consumption: Evidence from a natural experiment in Northern Ireland," Energy Economics, 36, pp. 729-743, 2013.
[10] Marnay, Chris, et al., "Shape of the microgrid," Lawrence Berkeley National Laboratory, 2000.
[11] Su, Wencong, and Jianhui Wang, "Energy management systems in microgrid operations," The Electricity Journal 25.8, pp. 45-60, 2012.
[12] D. G. Luenberger and Yinyu Ye, "Linear and nonlinear programming," 4th ed. Springer International Publishing Switzerland, 2016.
[13] Hinkle DE, et al., "Applied Statistics for the Behavioral Sciences." 5th ed., Houghton Mifflin, 2003.