Letter

A Privacy-Preserving Distributed Subgradient Algorithm for the Economic Dispatch Problem in Smart Grid

Qian Xu, Chutian Yu, Xiang Yuan, Zao Fu, and Hongzhe Liu

Dear Editor,

This letter aims to establish a privacy-preserving distributed optimization algorithm by combining the consensus iteration by subgradients, which not only enables the privacy preservation of optimization but also guarantees the optimality of solutions with some bias bounds.

In the setting of distributed optimization, a network of nodes, having their own objective functions depending on the global agents' state, would like to distributedly optimize the sum of all objective functions through the local agent-to-agent information change. In comparison with the centralized methods, such as gradient search approach, iteration method and even the intelligent approaches, the distributed approaches are more robust with respect to the disturbances, and are more flexible and scalable. Besides, the centralized methods require a center to calculate the global system information at each iterating step, which may harm the robustness of the considered systems like grids and lead to the restriction of flexibility and scalability [1]–[3].

The recently rapid development on the research of multi-agent systems, specially the study of consensus problem, greatly induces several consensus-based distributed optimization algorithms. To just list a few, Nedic and Ozdaglar [4] developed a subgradent algorithm to optimize the total cost function over a network, where the objective function can be non-smooth. In their setting, the optimization admitting certain inaccuracies subject to iteration stepsizes and subgradient bounds can be realized through minimizing each agent's own cost functions. After that, this algorithm was improved into the broadcast-based algorithm named subgradient-push algorithm [5]. Moreover, by resorting to the leader-follower protocol, a leader was set to collect and maintain the error message with respect to the optimal solution, as a result, the eventual consensus vector is exactly the optimal solution of the considered optimization problem [6]. After that, based on the two-level structure, the leader in the above cited work can be removed [7].

In this letter, we shall consider a multi-agents-based distributed convex optimization problem, where the objective functions can be non-smooth. However, due to almost of the aforementioned methods are based on the multi-agent-consensus, their setup, no matter on the undirected or directed and time-varying or time invariant communication rules, requires each agent to communicate the state information with others. This may result in serious privacy disclosure problems. The one is that the direct message communications breach the privacy of certain individuals if their state values contain some sensitive information, and the other is that the accuracy information passes may be vulnerable to eavesdroppers that attempt to steal the information by tapping communication channels. For instance, as claimed in [8], the smart grids linked through such direct message communications may be tender for adversaries to attack the grid system effectively. Furthermore, in the case that agent privacy variables are disclosed, the adversaries may inject the optimal attacks which result in the increase of total generation cost, and damage the entire power systems.

Until now, there have been a certain amount of works focusing on the privacy-preserving distributed optimization algorithms. The first typical approach is the differential privacy defined in [9], [10]. As an unavoidable result of noises injection, the convergence accuracy of optimization algorithm would be compromised. Thus, there would be a tradeoff between optimality and privacy level. The observability design approaches were proposed in [11], [12] such that the privacy information is not available to nonneighboring agents but are unable to deal with eavesdroppers who can eavesdrop all information in the communication networks. However, these approaches can only address the undirected communication networks, and would be disabled if the communication topologies would be directed.

The contributions of this work can be summarized as follows: 1) We shall establish a subgradient algorithm based on the multi-agent consensus, wherein all agents only know the noises-injected state information of their in-neighbors. Thus, the most excellent improvement of these results in comparison to [4] is the ability to protect the privacy of individuals. 2) Compared with the distributed gradient-based algorithms in [5], the subgradient approach can deal with the convex non-smooth objective functions.

Problem formulation: Here, we shall be focusing on the following optimization problem with total demands constraints, named Economic Dispatch Problem:

$$\min_{g_i\in\Omega_i}\sum_{i=1}^{m} f_i(g_i),\ \ \Omega_i=[g_i^-,g_i^+],\quad \text{s.t.}\ \sum_{i=1}^{m} g_i=D \tag{1}$$

where m is the number of individual nodes (i.e., generators), D is the total demand of powers that need to be generated by this system, g_i is the power generated by agent i, and accordingly $f_i:\mathbb{R}^+\to\mathbb{R}^+$ simply denotes the local cost function of agent i to generate such amount of power. The interval Ω_i is the upper and lower bounds of powers yielded by individual i, wherein g_i^- and g_i^+ are respectively the lower and upper power bound of agent i. Finally, $\sum_{i=1}^m g_i=D$ is the constraint of total demands. Noting that f_i is increased with respect to the variable g_i as usual, the demand constraint in (1) is equivalent to $\sum_{i=1}^m g_i\geq D$ in the almost of cases. Moreover, functions f_i, $i=1,2,\ldots,m$, are always convex, and the inequality $\sum_{i=1}^m g_i^-\leq D\leq\sum_{i=1}^m g_i^+$ guarantees the existence of the optimal solution subject to the total demand assumption.

By defining $K_i(\lambda)=\min_{g_i\in\Omega_i} f_i(g_i)-\lambda(g_i-D_i)$ with arbitrarily decomposed D_i satisfying $\sum_{i=1}^n D_i=D$, we can equivalently solve the following dual problem of problem (1) by utilizing Lagrangian-multiplier-based conversion:

$$\max_{\lambda\in\mathbb{R}^+}\sum_{i=1}^{m} K_i(\lambda) \tag{2}$$

where $\lambda\in\mathbb{R}^+$ is the so-called Lagrangian multiplier subject to the demand constraint $\sum_{i=1}^n D_i=D$. One should note that the constants D_i here are just the virtual demands which can be arbitrarily assigned.

Remark 1: We finally claim how to obtain the optimal solution g_i^* to problem (1) from the optimal solution λ^* of problem (2).

Differentiating function $K_i(\lambda)$ subject to g_i, we have that $\frac{\partial K_i(\lambda)}{\partial g_i}=\nabla f_i(g_i^*)-\lambda^*=0$, that is, $g_i^*=\min\left\{\max\left\{(\nabla f_i)^{-1}(\lambda^*),g_i^-\right\},g_i^+\right\}$. Therefore, we also need the following assumptions:

Assumption 1: As for optimization problem (2), we assume its optimizing value is finite as K^*, and accordingly the optimizing solu-

Corresponding author: Hongzhe Liu.

Citation: Q. Xu, C. T. Yu, X. Yuan, Z. Fu, and H. Z. Liu, "A privacy-preserving distributed subgradient algorithm for the economic dispatch problem in smart grid," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 7, pp. 1625–1627, Jul. 2023.

Q. Xu, C. T. Yu, and X. Yuan are with the State Grid Zhejiang Economic Research Institute, Hangzhou 310008, China (e-mail: qianxuhangzhou@gmail.com; yuchutuanhangzhou@163.com; yuanxianghangzhou@163.com).

Z. Fu and H. Z. Liu are with Beijing Yinshan Technology CO., LTD., Beijing 100871, China (e-mail: 278437639@qq.com; 15150650205@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.106028

tion is denoted by set λ^* with $\lambda^* = \{\lambda \in \mathbb{R}^* | \sum_{i=1}^m K_i(\lambda) = K^*\}$.

Assumption 2: Cost functions f_i are locally differentiable around a small neighbor domain of at least one optimizing solution.

Given the node (i.e., agent) set $V = \{1,2,\ldots,m\}$, for each agent i, the state of agent i at time instant t_k is denoted by $\lambda^i(k)$, which is an estimate of agent i for solution λ . Then, at the next time instant t_{k+1}, the state of agent $\lambda^i(k+1)$ is updated in accordance with the states of its in-neighbor agents j, which is achieved through a directed link $(j,i) \in E_k$, where (V,E_k) is the communication topology during the time interval $[t_k,t_{k+1})$. Specifically, the updating state information $\lambda^i(t+1)$ combines its self state and in-neighbors' information as follows:

$$\lambda^i(k+1) = \sum_{j=1}^m w^i_j(k)\bar{\lambda}^j(k) - \alpha^i(k)\partial_{K_i}(k) \tag{3}$$

where $w^i(k) = (w^i_1(k), w^i_2(k),\ldots,w^i_m(k)) \in \mathbb{R}^m$ stands for the weight vector that agent i holds and assigned with its neighbors at time instant t_k, and each component $w^i_j(k)$ therein denotes the weight that agent i assigns to agent j, when the information is received in time interval (t_k,t_{k+1}). $\partial_{K_i}(k)$ is the subgradient of function K_i at $\lambda^i(k)$.

Specially, to protect the privacy of individuals, state $\bar{\lambda}^j(k)$ shared by agent j is processed by adding a noise $o_j(k) \in [-\bar{o}_j(k),+\bar{o}_j(k)]$ arbitrarily, i.e., $\bar{\lambda}^j(k) = \lambda^j(k)+o_j(k)$. Then, we shall prove that, given the following two assumptions, such distributed protocols can seek the optimal solution without disclosing privacy.

Assumption 3: Each agent i has at least one honest out-neighbors.

Assumption 4: The bounds for noises satisfy the following conditions: $\sum_{k=0}^\infty \bar{o}_i(k) < +\infty$, $0 < \bar{o}_i(k) \le \bar{o}_i(s)$, $\forall k > s > 0$.

Finally, we give some assumptions for assigned weights $w^i_j(k)$.

Assumption 5: The weight rule in (3) satisfies that 1) There is a positive number $\kappa \in (0,1)$ such that $w^i_i(k) \ge \kappa$, $w^i_j(k) \ge \kappa$ with $(j,i) \in E_k$, and $w^i_j(k) = 0$, otherwise. 2) The weight vector $w^i(k)$ is a stochastic vector for any k and i, i.e., $\|w^i(k)\|_1 = 1$. 3) The weight matrix $W(k) = (w^i_j(k))_{m\times m}$ is symmetric.

Assumption 6: Denote the edge set $E_\infty = \{(i,j) | \forall M \in \mathbb{R}^+, \exists \beta > M, \text{ s.t. } (i,j) \in E_\beta\}$. We assume that the directed graph (V,E_∞) is strongly connected.

Assumption 7: Consider the directed graph (V,E_∞). There exists a positive integer $N \ge 1$ such that any directed edge $(i,j) \in E_\infty$ satisfies that $(i,j) \in E_k \cup E_{k+1} \cup \cdots \cup E_{k+N-1}$ holds for all $k \ge 0$.

Main results: Given the following notation to record matrix product: $\mathbf{W}(k:s) = W(s)W(s+1)\cdots W(k-1)W(k)$ with $\mathbf{W}(k,k) = W(k)$, for all $s \in \mathbb{N}^+$ and $k \in \mathbb{N}^+$ with $k \ge s$, it leads to that the i-th column of matrix $\mathbf{W}(k,s)$ is denoted by $[\mathbf{W}(k:s)]^i = W(s)W(s+1)\cdots W(k-1)\times W(k)w^i(k)$, and the (i,j)-th entry of matrix $\mathbf{W}(k,s)$ is given by $[\mathbf{W}(k:s)]^i_j = [W(s)W(s+1)\cdots W(k-1)W(k)w^i(k)]_j$. In this setup, iteration (3) can be simplified as

$$\begin{aligned}\lambda^i(k+1) = &\sum_{j=1}^m [\mathbf{W}(k:s)]^i_j \lambda^j(s) + \sum_{r=s}^k \sum_{j=1}^m [W(k:r)]^i_j o_j(r)\\ &- \sum_{r=s+1}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j \alpha^j(r-1)\partial_{K_j}(r-1) - \alpha^i(k)\partial_{K_i}(k).\end{aligned} \tag{4}$$

From above iteration, we see that matrix $\mathbf{W}(k,r)$ occupies all three items of right hand side. We therefore specially pay attention on study the convergence of matrix $\mathbf{W}(k,r)$ as $k \to +\infty$, which has been established in [4].

Lemma 1: If Assumptions 5–7 hold,

1) Limitation $\bar{\mathbf{W}}(r)$ of matrix sequence $\mathbf{W}(k:r)$, as $k \to +\infty$, is doubly stochastic with the same entries, that is, $\lim_{k\to\infty} \mathbf{W}(k:r) = \bar{\mathbf{W}}(k) = (1/m)\mathbf{1}^T_m \mathbf{1}_m$, $\forall r \in \mathbb{N}^+$.

2) The convergence of every element $[\mathbf{W}(k,s)]^i_j$ subject to $1/m$ is geometric as $k \to +\infty$ and is uniform with respect to $i,j = 1,2,\ldots,m$. Moreover, it holds that $\left|[\mathbf{W}(k:s)]^j_i - \frac{1}{m}\right| \le 2\times\frac{1+\kappa^{-N_0}}{1-\kappa^{-N_0}} \times (1-\kappa^{N_0})^{\frac{k-s}{N_0}}$. for all $k \ge s$, κ is defined in Assumption 5, m is the number of agents, and $N_0 = (m-1)N$ with the given N in Assumption 7.

Now, we proceed to study the convergence of our subgradient algorithm. In order to simply the theoretic analysis, we consider the constant stepsize here, which is a constant to all agents at any time instant, that is, $\alpha^i(k) = \alpha$, for all $k \in \mathbb{N}^+$. Based on this setting, the iteration (4) can be

$$\begin{aligned}\lambda^i(k+1) = &\sum_{j=1}^m [\mathbf{W}(k:s)]^i_j \lambda^j(s) + \sum_{r=s}^k \sum_{j=1}^m [W(k:r)]^i_j o_j(r)\\ &- \alpha \sum_{r=s+1}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j \partial_{K_j}(r-1) - \alpha\partial_{K_i}(k).\end{aligned} \tag{5}$$

Subsequently, to consider a related "stopped" model, we assume that each agent would shutoff calculating his subgradient after a finite iterating step bound. Denoting this step threshold as $\bar{\iota}^*$, it can be mathematically formalized as follows:

$$\partial_{K_j}(k) = \begin{cases}\text{An arbitrary subgradient at } \lambda^j(k),\ k < \bar{\iota}^*\\ 0,\ k \ge \bar{\iota}^*.\end{cases} \tag{6}$$

In such setup, we utilize $\lambda^i(k)$ to represent the estimating state of $\lambda^i(k)$. Combining (6) and (5), the iterating scheme of agents would be turned to

$$\lambda^i(k+1) = \begin{cases}\displaystyle\sum_{j=1}^m [\mathbf{W}(k:s)]^i_j \lambda^j(s) + \sum_{r=s}^k \sum_{j=1}^m [W(k:r)]^i_j o_j(r)\\ \displaystyle\quad - \alpha \sum_{r=s+1}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j \partial_{K_j}(r-1) - \alpha\partial_{K_i}(k),\ k < \bar{\iota}^*\\ \displaystyle\sum_{j=1}^m [\mathbf{W}(k:s)]^i_j \lambda^j(s) + \sum_{r=s}^k \sum_{j=1}^m [W(k:r)]^i_j o_j(r)\\ \displaystyle\quad - \alpha \sum_{r=s+1}^{\bar{\iota}^*} \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j \partial_{K_j}(r-1),\ k \ge \bar{\iota}^*.\end{cases} \tag{7}$$

According to Lemma, as k goes infinity, we know that the limitation $\lim_{k\to+\infty} \lambda^i(k)$ exists and only depends on the setting "stopping" time $\bar{k}$. Therefore, we can correspondingly set the following notation to stand for this limitation: $\tau(\bar{k}) = \lim_{k\to+\infty} \lambda^i(k)$. By Lemma 1 and specially noting that matrix $\mathbf{W}(s)$ is doubly stochastic, it holds that

$$\tau(\bar{k}) = \frac{\sum_{j=1}^m \lambda^j(0) - \sum_{r=s}^{\bar{\iota}^*}\sum_{j=1}^m \alpha\partial_{K_j}(r-1)}{m} + \lim_{k\to\infty} \sum_{r=s}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j o_j(r). \tag{8}$$

Thereinto, observing that the first and the third terms are not affected by k limits, we shall focus on the second item about the accumulation limit $\lim_{k\to\infty} \sum_{r=s}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j o_j(r)$, whose positive-term series hold that

$$\begin{aligned}&\lim_{k\to\infty} \sum_{r=s}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j |o_j(r)|\\ &\quad \le 2\times \frac{1+\kappa^{-N_0}}{1-\kappa^{-N_0}} \times \sum_{j=1}^m \left(\lim_{k\to+\infty}\left(\sum_{r=s}^k (1-\kappa^{N_0})^{\frac{k-r}{N_0}} \times \bar{o}_j(r)\right)\right).\end{aligned}$$

Denote $a_r = (1-\kappa^{N_0})^{\frac{k-r}{N_0}} \times \bar{o}_j(r)$, we consider the rate of two adjacency items as $\left|\frac{a_{r+1}}{a_r}\right| = (1-\kappa^{N_0})^{-\frac{1}{N_0}} \times \frac{\bar{o}_j(r+1)}{\bar{o}_j(r)} < (1-\kappa^{N_0})^{-\frac{1}{N_0}} < 1$, thus, the series $\lim_{k\to\infty} \sum_{r=s}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j |o_j(r)|$ converges as $k \to \infty$. We define this limitation as $\lim_{k\to\infty} \sum_{r=s}^k \sum_{j=1}^m [\mathbf{W}(k:r)]^i_j o_j(r) = \phi_j$. Here, we suppose that $\phi_i = \phi_j$, for any $i,j \in \{1,2,\ldots,n\}$, to simplify the mathematical notations. Substituting it into (8) yields that

$$\tau(\bar{k}) = \frac{1}{m}\sum_{j=1}^{m}\lambda^j(0) + \phi - \alpha\sum_{r=s}^{\bar{k}}\left(\sum_{j=1}^{m}\frac{1}{m}\partial_{K_j}(r-1)\right) \tag{9}$$

and further implies

$$\tau(k+1) = \tau(k) - \frac{\alpha}{m}\sum_{j=1}^{m}\partial_{K_j}(k). \tag{10}$$

Theorem 1: For any $\lambda \in \mathbb{R}$, it holds that

$$\|\tau(k+1)-\lambda\|^2 \le \|\tau(k)-\lambda\|^2 + \frac{2\alpha}{m}\sum_{j=1}^{m}(\|\partial^T_{K_j}(k)\| + \|\partial^\tau_{K_j}(k)\|) \times \|\lambda^j(k)-\tau(k)\| - \frac{2\alpha}{m}[K(\tau(k)) - K(\lambda)] + \frac{\alpha^2}{m^2}\sum_{j=1}^{m}\|\partial_{K_j}(k)\|^2. \tag{11}$$

Theorem 2: Assume the initial point satisfies $\max_{1\le j\le m}|\lambda^j(0)| \le \alpha R$ and subgradient holds that $|\partial_{K_j}(k)| \le Q$. Then, we have

1) There is a uniform bound on $\|\tau(k)-\lambda^i(k)\|$, which is given as $\|\tau(k)-\lambda^i(k)\| \le 2\alpha Q R_1 + \phi$, $\forall\, i = 1,2,\ldots,m$, where $R_1 = 1 + \frac{(R+Q)}{Q} \times \frac{m(1+\kappa^{-N_0})}{1-\kappa^{-N_0}} \times \sum_{s=0}^{k-1}(1-\kappa^{-N_0})^{\frac{k-s-1}{N_0}}$.

2) Let $\hat{\tau}(k) = \frac{1}{k}\sum_{s=0}^{k-1}\tau(s)$ and $\hat{\lambda}^i(k) = \frac{1}{k}\sum_{s=0}^{k-1}\lambda^i(s)$. It holds that

$$K(\hat{\tau}(k)) \le K^* + \frac{m\|\tau(0)-\lambda^*\|^2}{2k\alpha} + \frac{4\alpha^2 Q R_1 + m\alpha^2 Q^2 + m^2\phi}{2\alpha}$$

and

$$K(\hat{\lambda}^i(k)) \le K^* + \frac{m\|\tau(0)-\lambda^*\|^2}{2k\alpha} + \frac{4\alpha^2 Q R_1 + 4\alpha^2(R_1+1)Q^2}{2\alpha} + mQ\phi + \frac{m^2\phi}{2\alpha}.$$

Finally, we analyze the privacy preserving of our algorithm.

Theorem 3: If eavesdroppers know the systems parameters, that is, the stepsize α and the iterating matrix $W(k)$, it cannot infer the privacy information of any agent, i.e., λ^i, $o_j(s)$, $\partial_{K_i}(k)$.

Computer simulations: As for the experiment setups, the number of individual agents is chosen as 3 for computation simplicity, the number of samples is selected to be 100, and the maximum of iteration steps is 200.

Furthermore, to simulate a real application in smart grid, the cost is further modified by the supermum of the quadratic function and a minimal constant cost, which is assigned by the following ground-truth non-differentiable cost function as $f(\mathbf{g}) = \max\{\mathbf{g}^T\mathbf{A}^T\mathbf{A}\mathbf{g} + \mathbf{b}^T\mathbf{g} + c,\ d\}$, where the coefficients are given as $c = 0.066$, $d = -0.167$,

$$\mathbf{A}^T\mathbf{A} = \begin{bmatrix} 96.640 & -3.342 & 0.349 \\ -3.342 & 76.557 & 8.927 \\ 0.349 & 8.927 & 82.401 \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 0.315 \\ 0.950 \\ -0.824 \end{bmatrix}$$

where d is the minimal generating cost. Furthermore, we can check its positive semi-definiteness according to its eigen-values as $eig(\mathbf{A}^T\mathbf{A}) = [69.769,\ 88.543,\ 97.287]$.

The convergence results with different step-sizes are shown in Fig. 1. It can be found that with over-large step sizes, the objective does not converge and even oscillate or overshoot (cases of step size $10^{-3}, 10^{-6}$); With over-small step sizes, the objective will converge to local optimum (cases of step size $10^{-12}, 10^{-15}$); Only with appropriate step size (case of step size 10^{-9}), the dual objective converges to the global optimum. Specifically, for the oscillating results, the hyper-parameters (step size here) need to satisfy certain conditions to hold for the uniform convergence. When the hyper-parameter attains a certain threshold, the objective started to convergence. In the experiments, we found the threshold for step size is 10^{-7}.

Acknowledgment: This work was supported by the Science and Technology Project from State Grid Zhejiang Electric Power CO. Ltd (5211JY20001Q).

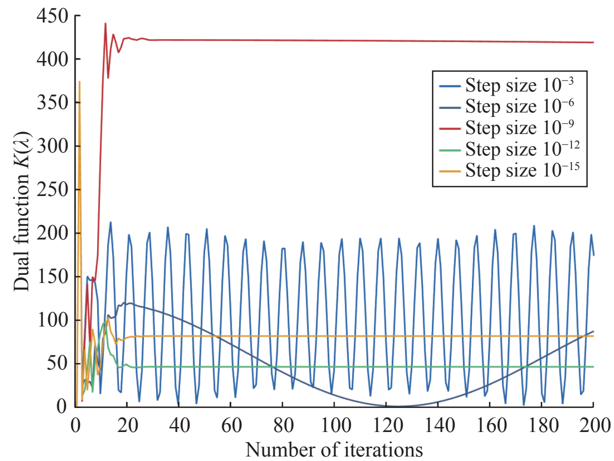

Fig. 1. The convergence results of the dual objective with different step sizes.

Supplementary material: The supplementary material of this letter can be found in links https://maifile.cn/est/d3296793221015/pdf.

References

[1] G. Binetti, A. Davoudi, F. L. Lewis, D. Naso, and B. Turchiano, "Distributed consensus-based economic dispatch with transmission losses," *IEEE Trans. Power Systems*, vol. 29, no. 4, pp. 1711–1720, 2014.

[2] S. Zhu, J. Lu, L. Lin, and Y. Liu, "Minimum-time and minimumtriggering observability of stochastic Boolean networks," *IEEE Trans. Automatic Control*, vol. 67, no. 3, pp. 1558–1565, 2022.

[3] L. Lin, J. Cao, S. Zhu, and P. Shi, "Synchronization analysis for stochastic networks through finite fields," *IEEE Trans. Automatic Control*, vol. 67, no. 2, pp. 1016–1022, 2022.

[4] A. Nedic and A. Ozdaglar, "Distributed subgradient methods for multiagent optimization," *IEEE Trans. Automatic Control*, vol. 54, no. 1, pp. 48–61, 2009.

[5] A. Nedić and A. Olshevsky, "Distributed optimization over time-varying directed graphs," *IEEE Trans. Automatic Control*, vol. 60, no. 3, pp. 601–615, 2014.

[6] Z. Zhang and M.-Y. Chow, "Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid," *IEEE Trans. Power Systems*, vol. 27, no. 4, pp. 1761–1768, 2012.

[7] Z. Zhang, X. Ying, and M.-Y. Chow, "Decentralizing the economic dispatch problem using a two-level incremental cost consensus algorithm in a smart grid environment," in *Proc. IEEE North American Power Symposium*, 2011, pp. 1–7.

[8] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 82–105, 2012.

[9] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," in *Proc. Inte. Conf. Distributed Computing and Networking*, 2015, pp. 1–10.

[10] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Trans. Automatic Control*, vol. 62, no. 1, pp. 50–64, 2016.

[11] S. Pequito, S. Kar, S. Sundaram, and A. P. Aguiar, "Design of communication networks for distributed computation with privacy guarantees," in *Proc. 53rd IEEE Conf. Decision and Control*, 2014, pp. 1370–1376.

[12] A. Alaeddini, K. Morgansen, and M. Mesbahi, "Adaptive communication networks with privacy guarantees," in *Proc. IEEE American Control Conf.*, 2017, pp. 4460–4465.