A Secret-Sharing Based Privacy-Preserving Distributed Energy Resource Control Framework

Xiang Huo and Mingxi Liu
Department of Electrical and Computer Engineering
University of Utah
Salt Lake City, UT, USA
{xiang.huo, mingxi.liu}@utah.edu

2022 IEEE 31st International Symposium on Industrial Electronics (ISIE) | 978-1-6654-8240-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIE51582.2022.9831578

***Abstract*—The rapidly growing penetration of renewable energy resources brings unprecedented challenges to electricity distribution networks. A large population of grid-connected devices can lead to severe control scalability issues and potential user information leakage. However, few research focuses on the privacy preservation of distributed energy resource (DER) control in a fully scalable manner. In this regard, this study aims at designing a novel decentralized privacy-preserving DER control framework that can 1) achieve control scalability over a large population of heterogeneous DERs; 2) eliminate the peer-to-peer communications and secure the privacy of all participating DERs against various types of adversaries; and 3) enjoy higher computation efficiency and accuracy compared to state-of-the-art privacy-preserving methods. The DER control is demonstrated through a coupled optimization problem which optimizes the power flow within a distribution network that is integrated with solar generation and battery storage systems, and solved by using the projected gradient method. The novel privacy-preserving algorithm is designed based on cloud computing and secret sharing. Preliminary results show the promising capabilities of the proposed approach in DER control applications.**

***Index Terms*—Decentralized optimization, distributed energy resources, energy storage system, privacy, secret sharing, solar photovoltaic**

I. Introduction

A. Related Works

Large-scale deployment of distributed energy resources (DERs) has proven efficacy in reducing carbon footprint and providing grid-edge ancillary services. In the meantime, scalable control strategies including distributed and decentralized techniques are drawing more attention in large-scale DER control problems. For example, the distributed method in [1] can control large-scale grid-connected photovoltaic (PV) systems. However, it suffers from massive peer-to-peer communications that generically exist in distributed control strategies. As an improvement, Navidi *et. al* [2] developed a two-layer decentralized DER coordination architecture that can scale the solution to large networks, and no direct communication is required between local controllers. Similarly, a decentralized stochastic control strategy was designed in [3] for radial distribution systems considering the integration of controllable PV inverters and energy storage systems (ESSs). However, existing decentralized approaches fail to consider the privacy which is a major block to the implementation of DER control.

In addressing privacy concerns, differential privacy (DP) has received substantial attention owing to its rigorously mathematical formulation [4]. DP-based methods add persistent randomized perturbations to the datasets, constraints, or objective functions for privacy preservation. In [5], a multi-agent cloud-based framework was designed to keep each agent's state differentially private for constrained optimization problems. Han *et. al* in [6] developed a distributed optimization algorithm based on DP to preserve the privacy of the participating agents. However, DP-based methods inevitablely suffer from accuracy loss due to the added perturbations.

To improve the accuracy, another privacy preservation measure is encryption. Encryption-based strategies encrypt the original data into cyphertexts, and only those holding private keys can decrypt the cyphertexts. Lu *et. al* [7] proposed an efficient and privacy-preserving aggregation scheme for smart grid communications, in which the data is encrypted by Paillier cryptosystem. In [8], a privacy-preserving and fault-tolerant aggregation scheme was designed based on homomorphic cryptosystem, aiming at secure aggregation of metering data. However, the encryption-based methods prevalently demand massive computation which would limit their applicability. Other hardware integrated privacy-preserving methods, e.g., garbled circuit based strategy [9], [10], are deficient in flexibility and uneconomic due to the hardware cost.

Secret sharing (SS) [11] is a lightweight cryptographic method that can securely distribute a secret among a group of m participants. Each participant will be allocated with a share of the secret, and only when more than k, where $k \leq m$, participants collaborate can the secret be reconstructed from their shares. Adopting SS, Nabil *et. al* [12] designed a SS-based detection scheme to identify malicious consumers who steal electricity, in which system operators only collect masked meter readings from the consumers to avoid privacy violation. In [13], a SS-based algorithm was developed for the private consensus problems. Compared with encryption-based strategies, SS-based methods can achieve privacy preservation while avoiding the heavy computational load. In this paper, we will design a novel SS-based privacy-preserving algorithm that merits both high efficiency and accuracy.

This work has been supported in part by NSF Award: ECCS-2145408.

B. Statement of Contributions

Mandated and frequent communications in unprotected channels can cause unexpected privacy breaches, and yet privacy preservation is an generally ignored aspect in decentralized algorithms. Motivated by addressing both the scalability and the privacy in DER controls, we will orginally integrate SS into decentralized optimizations for privacy preservation. This novel scheme will be a perfect candidate for large-scale DER control with privacy protection as it facilitates decentralized optimization with scalablity as well as achieves privacy preservation, high computing efficiency, and accuracy. The applicability of the proposed method will be demonstrated through a hybrid PV and ESS setup in a distribution network.

The contributions of this paper is three-fold: 1) We design a novel decentralized privacy-preserving algorithm which can be used as a benchmark for secure and scalable DER control; 2) The proposed method eliminates the peer-to-peer communications and secures the privacy of the participating DERs against adversaries; 3) Compared to state-of-the-art approaches, our method achieves lower computational overhead and identically accurate solutions as the non-privacy-concerned algorithms.

II. Main Results & Methodologies

A. System Model

1) Branch Flow Model: Consider an n-bus radial distribution network where $\mathbb{N} = \{0, 1, \ldots, n\}$ denotes the set of buses. Let l_{ij} denote the line segment connecting buses i and j, $\mathbb{L}$ denote the set of lines, $\mathbb{C}_j$ denote the set of bus j's children, V_j denote the voltage magnitude at bus j, $\mathcal{P}_{ij}$ and $\mathcal{Q}_{ij}$ denote the active and reactive power flow from bus i to bus j respectively, and r_{ij} and x_{ij} be the resistance and reactance of line (i, j), respectively. For bus j, P_j and Q_j denote its active and reactive power consumptions, respectively, and p_j and q_j denote its active and reactive power injections, respectively. The power flow of the radial distribution network can be defined by the DistFlow branch equations [14] as

$$\mathcal{P}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{P}_{ju} = P_j - p_j + r_{ij}\mathcal{I}_{ij}^2 \tag{1a}$$

$$\mathcal{Q}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{Q}_{ju} = Q_j - q_j + x_{ij}\mathcal{I}_{ij}^2 \tag{1b}$$

$$V_i^2 - V_j^2 = 2(r_{ij}\mathcal{P}_{ij} + x_{ij}\mathcal{Q}_{ij}) - (r_{ij}^2 + x_{ij}^2)\mathcal{I}_{ij}^2 \tag{1c}$$

where $\mathcal{I}_{ij}^2 = (\mathcal{P}_{ij}^2 + \mathcal{Q}_{ij}^2)/V_i^2$. To simplify the network model, a DistFlow model can be linearized to the LinDistFlow model by ignoring the higher order terms [15]. This linearization only introduces a neglectable relative error which is normally of the order of 1% [16]. This paper adopts the LinDistFlow model to simplify the description and better illustrate the algorithm design. The LinDistFlow model can be represented as

$$\mathcal{P}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{P}_{ju} = P_j - p_j \tag{2a}$$

$$\mathcal{Q}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{Q}_{ju} = Q_j - q_j \tag{2b}$$

$$V_i^2 - V_j^2 = 2(r_{ij}\mathcal{P}_{ij} + x_{ij}\mathcal{Q}_{ij}). \tag{2c}$$

In this paper, one objective is to minimize the total power loss of the distribution network, which is approximated by

$$f_1(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n) = \sum_{l_{ij} \in \mathbb{L}} r_{ij} \left(\frac{\|\boldsymbol{\mathcal{P}}_{ij}\|_2^2 + \|\boldsymbol{\mathcal{Q}}_{ij}\|_2^2}{V_0^2} \right) \tag{3}$$

where V_0 denotes the nominal voltage magnitude, $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$, $\boldsymbol{\mathcal{P}}_{ij}$, $\boldsymbol{\mathcal{Q}}_{ij} \in \mathbb{R}^T$ where T denotes time intervals. Note that we assume the reactive power flows $\boldsymbol{\mathcal{Q}}_{ij}$ are constants and only consider the active power loss. Though reactive power loss is not included here for simplicity, it can be added without affecting the algorithm design. The active power flows are constrained by

$$\mathbf{0} \leq \boldsymbol{\mathcal{P}}_{ij} \leq \hat{\boldsymbol{\mathcal{P}}}_{ij} \tag{4}$$

where $\hat{\boldsymbol{\mathcal{P}}}_{ij}$ denotes the maximum active power flow limit.

2) Solar Photovoltaic: During T time intervals of a day, the active power injections from the ith PV should satisfy

$$\mathbf{0} \leq \boldsymbol{p}_i^v \leq \hat{\boldsymbol{p}}_i^v \tag{5}$$

where $\boldsymbol{p}_i^v \in \mathbb{R}^T$, and $\hat{\boldsymbol{p}}_i^v$ denotes the maximum available active power from the ith PV inverter. $\hat{\boldsymbol{p}}_i^v$ is assumed to be known by forecast. Herein, the curtailment cost is defined by

$$f_2(\boldsymbol{p}_i^v) = \|\hat{\boldsymbol{p}}_i^v - \boldsymbol{p}_i^v\|_2^2. \tag{6}$$

3) Energy Storage System: The discharging/charging rates of the ith ESS is constrained by

$$-\hat{\boldsymbol{p}}_i^{el} \leq \boldsymbol{p}_i^e \leq \hat{\boldsymbol{p}}_i^{eu} \tag{7}$$

where $\boldsymbol{p}_i^e \in \mathbb{R}^T$ denotes the discharging/charging rates of the ith ESS, and $\hat{\boldsymbol{p}}_i^{el}$ and $\hat{\boldsymbol{p}}_i^{eu}$ denote the maximum discharging and charging rates, respectively.

Aggregate the charging/discharging rates across T time intervals, the capacity of the ith ESS is constrained by

$$\hat{\boldsymbol{p}}_i^{cl} \leq \boldsymbol{A}\boldsymbol{p}_i^e \Delta T \leq \hat{\boldsymbol{p}}^{cu} \tag{8}$$

where $\hat{\boldsymbol{p}}_i^{cl}$ and $\hat{\boldsymbol{p}}_i^{cu}$ denote the lower and upper capacity bounds of the ith ESS, respectively, ΔT denotes the time interval, and $\boldsymbol{A}$ is a lower triangular matrix with only ones and zeros. Furthermore, the ith ESS's degradation cost can be calculated in terms of the smoothness of charging and discharging by

$$f_3(\boldsymbol{p}_i^e) = \|\boldsymbol{p}_i^e\|_2^2. \tag{9}$$

Therefore, the total active power injections $\boldsymbol{p}_i \in \mathbb{R}^T$ at bus i during T time intervals should satisfy

$$\boldsymbol{p}_i = \boldsymbol{p}_i^e - \boldsymbol{p}_i^v. \tag{10}$$

B. Decentralized Optimization

The optimization problem is then formulated by minimizing the total cost of the distribution network

$$\begin{aligned} \min \quad & \delta_1 f_1(\boldsymbol{p}^e, \boldsymbol{p}^v) + \sum_{i=1}^{n} (\delta_2 f_2(\boldsymbol{p}_i^v) + \delta_3 f_3(\boldsymbol{p}_i^e)) \\ \text{s.t.} \quad & \text{(2a)}, (4), (5), (7), (8), (10) \end{aligned} \tag{P1}$$

where δ_α denotes the weight associated with $f_\alpha(\cdot)$, $\boldsymbol{p}^e = [\boldsymbol{p}_1^{e\mathsf{T}}, \ldots, \boldsymbol{p}_n^{e\mathsf{T}}]^\mathsf{T}$, and $\boldsymbol{p}^v = [\boldsymbol{p}_1^{v\mathsf{T}}, \ldots, \boldsymbol{p}_n^{v\mathsf{T}}]^\mathsf{T}$.

This paper achieves scalability in solving (**P1**) via projected gradient method (PGM), where n agents (DERs) in the distribution network cooperatively solve (**P1**). In this setting, each agent updates its decision variable using PGM by

$$\boldsymbol{x}_i^{\ell+1} = \mathbb{P}_{X_i}[\boldsymbol{x}_i^{\ell} - \gamma^{\ell}\Phi_i(\boldsymbol{x}^{\ell})] \tag{11}$$

where $\boldsymbol{x}_i^{\ell}$ denotes the decision variable of the ith agent at the ℓth iteration, $\boldsymbol{x}^{\ell} = [\boldsymbol{x}_1^{\ell\,\mathsf{T}}, \ldots, \boldsymbol{x}_n^{\ell\,\mathsf{T}}]^{\mathsf{T}}$, γ^{ℓ} is the step size, $\Phi_i(\cdot)$ denotes the first-order gradient of the Lagrangian *w.r.t.* $\boldsymbol{x}_i^{\ell}$, and $\mathbb{P}_{X_i}[\cdot]$ denotes the projection operation on set X_i.

In PGM iterations, agent i needs to calculate $\Phi_i(\boldsymbol{x}^{\ell})$ in (11) where $\boldsymbol{x}_i$'s from all other agents need to be collected, e.g., the decision variables $\boldsymbol{p}^e$ and $\boldsymbol{p}^v$ in (**P1**). This unavoidable information exchange can lead to privacy breaches, especially attacks from other malicious agents. To address the privacy concerns, we develop a novel SS-based algorithm that can achieve secure information exchange in executing (11). The proposed two-layer privacy-preserving computing structure is shown in Fig. 1, in which the servers in the cloud computing layer only aggregate and distribute the secure data received from the agents in the distribution network layer.

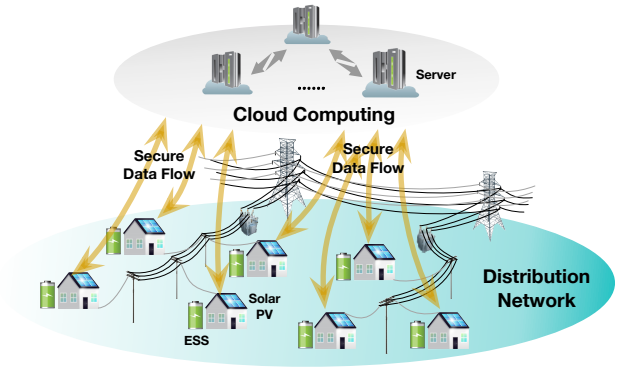


Fig. 1. Two-layer privacy-preserving computing structure for DER control in a distribution network

C. Proposed Privacy-Preserving Algorithm

In this section, we present a novel privacy-preserving algorithm based on SS. Before introducing the algorithm, we first briefly introduce the Shamir's SS scheme [11]. Suppose a manager seeks to distribute a secret s to m agents, and mandates at least k agents to reconstruct the secret. To this end, the Shamir's SS utilizes the idea of Lagrange polynomial interpolation for secret distribution and recovery. Specifically, the manager firstly constructs a random polynomial of

$$y(z) = s + c_1 z + \cdots + c_{k-1} z^{k-1} \tag{12}$$

where s denotes an integer secret, $c_1, \ldots, c_{k-1}$ denote random coefficients that are uniformly distributed in the field $\mathbb{E} \triangleq [0, e)$, and e denotes a prime number. Secondly, the manager calculates the outputs of (12) with non-zero integer inputs, e.g., setting $\tau = 1, \ldots, n$ to retrieve $(\tau, y(\tau))$ where $y_\tau = y(\tau) \bmod e$ and mod denotes the modular operation. Then, the share y_τ is distributed to agent τ. Lastly, at least k agents are required to reconstruct the polynomial based on Lagrange interpolation and hence recover the secret s by

$$s = \sum_{\tau=1}^{k} y_\tau \prod_{\substack{\upsilon=0 \\ \upsilon\neq\tau}}^{k} \frac{\upsilon}{\upsilon - \tau} \tag{13}$$

We next propose the novel two-layer decentralized privacy-preserving algorithm based on SS. In the distribution network layer, all agents (DERs) update their decision variables in parallel, and only masked data are sent to the servers. In the cloud computing layer, the servers aggregate and calculate $\Phi_i(\cdot)$ using the received data, then distribute $\Phi_i(\cdot)$ to the ith agent. Specifically, the proposed algorithm consists of three steps: 1) Each agent (DER) generates a random polynomial $y_i(z)$ using (12) and sends the outputs of the polynomial to the cloud servers; 2) The cloud servers then interact with each other for information aggregation to calculate $\Phi_i(\cdot)$'s; and 3) The cloud servers send $\Phi_i(\cdot)$ to the ith agent, then each agent performs the PGM updates using (11). Note that the agents only send the outputs of the polynomials to the servers so that the cloud servers are not aware of the true decision variables, as the cloud servers only need to calculate aggregated messages using those randomized outputs. The outline of the proposed method is shown in Algorithm 1, and the detailed version will be provided in the future work.

Algorithm 1 Decentralized SS-based privacy-preserving DER control strategy

1: DERs initialize decision variables, tolerance ϵ_0, iteration counter $\ell = 0$, and maximum iteration ℓ_{max}.
2: **while** $\epsilon_i^{\ell} > \epsilon_0$ and $\ell < \ell_{max}$ **do**
3: *Secret generation*: The ith DER generates a random polynomial $y_i(z)$ using (12) and sends the outputs of the polynomial to the cloud servers
4: *Secret reconstruction*: The cloud servers interact with each other and reconstruct the aggregated secrets to calculate $\Phi_i(\cdot)$'s, and send $\Phi_i(\cdot)$ to the ith agent
5: *Decentralized update*: The ith DER updates $\boldsymbol{p}_i^e$ and $\boldsymbol{p}_i^v$ by PGM using (11) and calculates the error ϵ_i^{ℓ}.
6: $\ell = \ell + 1$.
7: **end while**

To prove the privacy preservation of the proposed scheme, we will consider three types of adversaries, including *honest-but-curious-agent* who may observe the intermediate or input/output data to infer the private information of other agents; *external eavesdroppers* who launch attacks by wiretapping and intercepting exchanged messages between agents and the cloud server; and *cloud servers* who may be attacked to cause the leakage of agents' decision variables. Detailed privacy analyses will be provided in our future work.

III. Preliminary Results

Simulations of a DER control problem were conducted on the IEEE 13-bus test feeder where ESSs and solar PVs are considered. Without loss of generality, each bus is assumed

to be connected with a house that is equipped with an ESS and 5 solar panels, resulting in total 12 houses connected. The maximum capacity of each ESS is 15 kWh, and the maximum charging/discharging rates are ± 2 kW, respectively [17]. The forecasted solar PV generation is chosen from 01/01/2021 with $\Delta T = 5$ mins on a sunny day in California [18]. The decentralization does not alter the solution compared with the centralized method, herein we only present the centralized results of (**P1**).

In Fig. 2, all 12 houses are assumed to be located in the same area with identical forecasted solar generation and utility power supply, but each house is assigned with a unique baseline load profile [18], [19]. Fig. 3(a) and Fig. 3(b) show the active power injections or consumptions from the solar PVs and ESSs, respectively. As can be seen, at around 12:00, the solar PVs generate maximum amount of energy and the ESSs charge at the peak rates. Before 8:00 and after 16:00, energy stored in ESSs is extracted to compensate for the power loss in the distribution network.

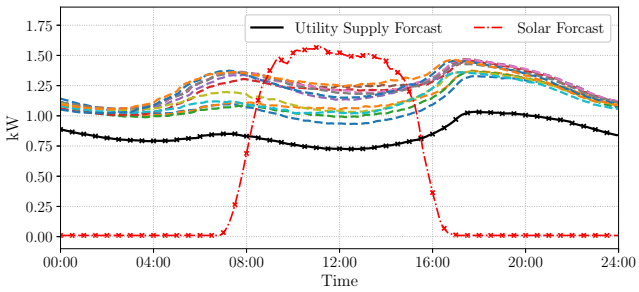
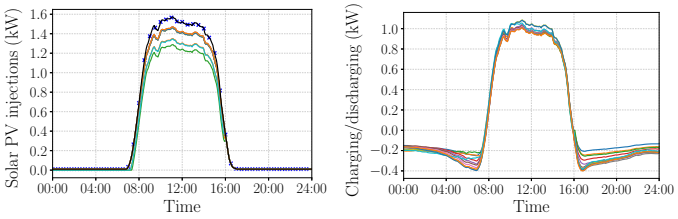


Fig. 2. Daily solar generation forecast, active power supply forecast, and baseline loads of 12 houses (dashed lines)



(a) Active power injections from solar PVs at 12 buses (blue marked line represents forecasted solar power limit)

(b) Charging and discharging rates of the 12 ESSs

Fig. 3. Active power injections and consumptions from the DERs

IV. Conclusion and Future Work

In this paper, a novel privacy-preserving algorithm was proposed for DER control in distribution networks. The proposed algorithm secures the privacy of DER owners including the DERs' generation and consumption and daily electricity usage. We firstly formulated the coupled optimization problem that aims at minimizing the line loss, PV curtailment cost, and ESS degradation cost. Then, we presented the outline of the privacy-preserving algorithm based on SS, and showed applicability of the proposed privacy preservation method.

The preliminary results prove the feasibility and potential of the proposed approach. To fulfill this research direction, future work includes 1) designing a real number to integer quantization strategy with arbitrary precision that can integrate SS into decentralized optimization seamlessly; 2) providing a more detailed algorithm design and comprehensive privacy analyses; and 3) conducting realistic large-scale experiments to show that the proposed method can be readily applied in real-world DER control applications.

References

[1] L. Zhang, K. Sun, Y. W. Li, X. Lu, and J. Zhao, "A distributed power control of series-connected module-integrated inverters for PV grid-tied applications," *IEEE Transactions on Power Electronics*, vol. 33, no. 9, pp. 7698–7707, 2017.

[2] T. Navidi, A. El Gamal, and R. Rajagopal, "A two-layer decentralized control architecture for DER coordination," in *Proceedings of the IEEE Conference on Decision and Control*, Miami, FL, USA, Dec. 17-29 2018, pp. 6019–6024.

[3] W. Lin and E. Bitar, "Decentralized stochastic control of distributed energy resources," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 888–900, 2017.

[4] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proceedings of the Theory of Cryptography Conference*, New York, NY, USA, Mar. 4-7 2006, pp. 265–284.

[5] M. Hale and M. Egerstedty, "Differentially private cloud-based multi-agent optimization with constraints," in *Proceedings of the American Control Conference*, Chicago, IL, USA, Jul. 1-3 2015, pp. 1235–1240.

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

[7] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[8] A. Mohammadali and M. S. Haghighi, "A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5212–5220, 2021.

[9] S. Wang, Q. Hu, Y. Sun, and J. Huang, "Privacy preservation in location-based services," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 134–140, 2018.

[10] R. Gilad-Bachrach, K. Laine, K. Lauter, P. Rindal, and M. Rosulek, "Secure data exchange: A marketplace in the cloud," in *Proceedings of the ACM SIGSAC Conference on Cloud Computing Security Workshop*, London, United Kingdom, Nov. 11 2019, pp. 117–128.

[11] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[12] M. Nabil, M. Ismail, M. M. Mahmoud, W. Alasmary, and E. Serpedin, "PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96 334–96 348, 2019.

[13] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing," in *Proceedings of the European Signal Processing Conference*, A Coruña, Spain, Sep. 2-6 2019, pp. 1–5.

[14] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Power Engineering Review*, vol. 9, no. 4, pp. 101–102, 1989.

[15] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Transactions on Power Delivery*, vol. 4, no. 1, pp. 735–743, 1989.

[16] M. Farivar, L. Chen, and S. Low, "Equilibrium and dynamics of local voltage control in distribution systems," in *Proceedings of the IEEE Conference on Decision and Control*, Florence, Italy, Dec. 10-13 2013, pp. 4329–4334.

[17] Residential Battery Storage. [Online]. Available: https://atb.nrel.gov/electricity/2021/residential_battery_storage

[18] U.S. Energy Information Administration. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=49276

[19] Electric Power Annual. [Online]. Available: https://www.eia.gov/electricity/annual/