2026 IEEE 20th International Conference on Control and Automation (ICCA)
June 16-20, 2026. Almaty, Kazakhstan

Privacy-Preserving Distributed Estimation of Global Storage Capacity via Dynamic Differential Privacy

1st Yun Zhang
School of Electrical Engineering
University of Jinan
Jinan, China
cse_zhangyun@ujn.edu.cn

2nd Zhongrui Cui
School of Electrical Engineering
University of Jinan
Jinan, China
cse_cuizr@ujn.edu.cn

3rd Le Chang
College of Electric Power Engineering
Shanghai University of Electric Power
Shanghai, China
lchang@shiep.edu.cn

2026 IEEE 20th International Conference on Control and Automation (ICCA) | 979-8-3315-4853-7/26/$31.00 ©2026 IEEE | DOI: 10.1109/ICCA69928.2026.11618236

Abstract—Distributed Energy Storage Systems (DESSs) are critical for grid stability, yet their effective scheduling relies on accurate knowledge of the global total capacity. However, the capacity data of individual storage units is commercially sensitive. Traditional distributed consensus algorithms allow for decentralized estimation but often expose the initial states of nodes to neighbors, leading to privacy leakage. To address this challenge, this paper proposes a privacy-preserving distributed estimation strategy based on Dynamic Differential Privacy. We design a time-varying noise injection mechanism where Laplace noise is added to the consensus process. The noise scale is initialized at a high level to mask raw data and follows a decay function, reducing to zero at a pre-set time step T. Theoretical analysis proves that this method ensures the privacy of individual units during the transient phase and achieves exact convergence to the true global capacity at step T, effectively balancing the trade-off between privacy protection and estimation accuracy.

Index Terms—Distributed Energy Storage, Capacity Estimation, Dynamic Differential Privacy, Average Consensus, Smart Grid.

I. Introduction

With the increasing penetration of renewable energy, distributed energy storage systems (DESSs) have emerged as critical assets for grid regulation and peak shaving [1]. To effectively participate in power markets and ancillary services, the aggregator (e.g., a virtual power plant operator) requires precise knowledge of the global available capacity of the storage cluster [2], [3]. Conventionally, such information is collected via a centralized architecture. However, centralized approaches suffer from single-point failures and communication bottlenecks. More critically, they raise severe privacy concerns, as the capacity and State of Health (SoH) of a battery are commercially sensitive data that can reveal the operational strategy and degradation patterns of the asset owner [4].

To mitigate these risks, distributed average consensus algorithms have been widely adopted. In this framework, storage units communicate only with their immediate neighbors to iteratively compute the global average. Despite the decentralized nature, standard consensus protocols are vulnerable to inference attacks. An "honest-but-curious" adversary can infer a neighbor's initial state by observing the exchanged messages, thereby compromising privacy [5].

To address the privacy leakage in distributed consensus, several cryptographic and statistical approaches have been proposed in the literature. One line of research focuses on encryption-based methods, such as homomorphic encryption (HE) and secure multi-party computation (SMPC) [6]–[8]. While these methods provide strong security guarantees, they often incur heavy computational overhead and significant communication latency, rendering them unsuitable for resource-constrained battery controllers or real-time dispatch scenarios.

Another promising direction is Differential Privacy (DP), which obscures sensitive data by injecting random noise [9], [10]. Early works applied static noise to the initial states or communication links. Although computationally efficient, standard DP introduces a fundamental trade-off: a larger noise variance improves privacy but results in a permanent error floor in the estimation accuracy. To mitigate this error, recent studies have explored vanishing noise schemes. However, most existing decaying noise strategies rely on asymptotic convergence (i.e., requiring $t \to \infty$ to eliminate error), which is impractical for grid applications that require a definitive result within a fixed clearing time T [11], [12].

To overcome the limitations of permanent error in static DP and the slow convergence of asymptotic methods, this paper proposes a distributed estimation strategy leveraging Dynamic Differential Privacy with a finite-time horizon. We design a time-varying noise injection mechanism where the noise scale is initialized at a high magnitude to mask raw data and decays monotonically to zero at a pre-set step T.

The main contributions of this paper are summarized as follows: 1. We propose a dynamic noise scheduling framework that integrates seamlessly with average consensus, ensuring that the cumulative noise impact on the

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.

final result is negligible. 2. We provide a theoretical analysis of the privacy budget consumption, demonstrating that the initial high-variance noise effectively protects the initial capacity state. 3. We prove that the algorithm guarantees exact convergence to the true global capacity at the designated time T, satisfying the strict accuracy requirements of power system dispatch.

II. Problem Formulation and Preliminaries

A. Communication Network

Consider a distributed cluster of N Battery Energy Storage Systems (BESSs). The communication topology among the BESSs is modeled as an undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, 2, \ldots, N\}$ represents the set of storage units (nodes) and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the set of communication links (edges). A link $(i, j) \in \mathcal{E}$ exists if and only if node i and node j can exchange information with each other. The set of neighbors of node i is denoted by $\mathcal{N}_i = \{j \in \mathcal{V} \mid (i, j) \in \mathcal{E}\}$.

The adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$ is defined such that $a_{ij} > 0$ if $(j, i) \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. The graph is undirected, if for any $i, j \in \mathcal{V}$, $a_{ij} = a_{ji}$, i.e. $\mathcal{A}$ is symmetric. The Laplacian matrix $\mathcal{L} = [l_{ij}]$ is defined as $l_{ii} = \sum_{j=1}^{N} a_{ij}$ and $l_{ij} = -a_{ij}$ for $i \neq j$.

Assumption 1: The communication graph $\mathcal{G}$ is connected and undirected.

Based on the algebraic graph theory results in [13], [14], under Assumption 1, the Laplacian matrix $\mathcal{L}$ has a simple zero eigenvalue with the corresponding eigenvector $\mathbf{1}_N = [1, 1, \ldots, 1]^\top$, and all other eigenvalues are positive.

B. Distributed Capacity Estimation

Let c_i denote the true available capacity of the i-th BESS unit at the beginning of the estimation process. The primary objective of the aggregator is to obtain the global average capacity of the cluster, defined as:

$$\bar{c} = \frac{1}{N} \sum_{i=1}^{N} c_i \tag{1}$$

Once the average $\bar{c}$ is known, the total capacity can be trivially computed as $N\bar{c}$.

In a standard discrete-time average consensus protocol, each node i maintains a state $x_i(k)$, initialized as $x_i(0) = c_i$. The state update follows:

$$x_i(k+1) = x_i(k) - \epsilon \sum_{j \in \mathcal{N}_i} a_{ij}(x_i(k) - x_j(k)) \tag{2}$$

where $\epsilon > 0$ is a constant step size satisfying $0 < \epsilon < 1/\max_i l_{ii}$. In vector form, this is $x(k+1) = (I - \epsilon\mathcal{L})x(k)$. It is well-known that $\lim_{k\to\infty} x_i(k) = \bar{c}$.

While (2) ensures convergence, it completely exposes the initial state. An "honest-but-curious" adversary at node j can perfectly infer the private capacity c_i of its neighbor i simply by observing the first broadcast message $x_i(0)$.

To prevent such inference, nodes must inject random noise $\eta_i(k)$ into the exchange process. However, standard differential privacy mechanisms (e.g., adding i.i.i.d. Laplace noise) introduce a persistent error variance, preventing the system from converging to the exact average $\bar{c}$.

C. Problem Statement

The problem addressed in this paper is to develop a privacy-preserving distributed estimation strategy that resolves the conflict between privacy and accuracy. Specifically, we aim to achieve the following two goals simultaneously:

1) Privacy Preservation: The mechanism must satisfy ϵ-differential privacy, ensuring that an adversary cannot distinguish the true initial capacity c_i from a perturbed value with high probability.
2) Exact Finite-Time Convergence: The estimation error must vanish at a pre-specified time step T, i.e.,

$$\lim_{k \to T} \mathbb{E}[|x_i(k) - \bar{c}|] = 0, \quad \forall i \in \mathcal{V}. \tag{3}$$

D. Differential Privacy

In the context of distributed consensus, the private data corresponds to the vector of initial capacities $\mathbf{c} = [c_1, c_2, \ldots, c_N]^\top$. We strictly define the privacy guarantee as follows.

Definition 1 (Adjacency): Two state vectors $\mathbf{c}, \mathbf{c}' \in \mathbb{R}^N$ are said to be adjacent if they differ in at most one entry, i.e., there exists exactly one index i such that $c_i \neq c_i'$ and $c_j = c_j'$ for all $j \neq i$.

Definition 2 (ϵ-Differential Privacy): A randomized mechanism $\mathcal{M}$ is said to satisfy ϵ-differential privacy (ϵ-DP) if for any pair of adjacent state vectors $\mathbf{c}$ and $\mathbf{c}'$, and for any measurable subset of outputs $\mathcal{S} \subseteq \text{Range}(\mathcal{M})$, the following inequality holds:

$$\mathbb{P}[\mathcal{M}(\mathbf{c}) \in \mathcal{S}] \leq e^{\epsilon} \cdot \mathbb{P}[\mathcal{M}(\mathbf{c}') \in \mathcal{S}] \tag{4}$$

where probability $\mathbb{P}[\cdot]$ is taken over the randomness of the mechanism $\mathcal{M}$, and $\epsilon > 0$ is the privacy budget. A smaller ϵ indicates a stronger privacy protection.

Definition 3 (ℓ_1-Sensitivity): The ℓ_1-sensitivity of a function $f : \mathbb{R}^N \to \mathbb{R}$ is defined as:

$$\Delta f = \max_{\mathbf{c}, \mathbf{c}' \text{ adjacent}} \|f(\mathbf{c}) - f(\mathbf{c}')\|_1 \tag{5}$$

For the capacity estimation problem, the sensitivity is determined by the maximum possible variation of a single battery's capacity, denoted as $C_{\max}$.

III. Controller Design

To protect the initial capacity information from honest-but-curious neighbors, we propose a privacy-preserving consensus protocol based on output perturbation. The frame of the proposed mechanism is illustrated in Fig. 1.

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.

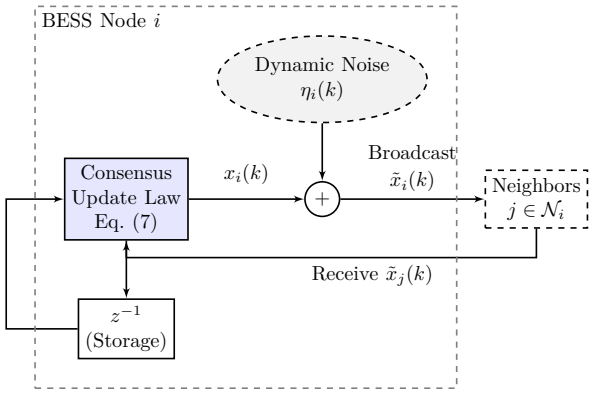

Fig. 1. Block diagram of the proposed privacy-preserving mechanism.

A. Privacy-Preserving Transmission Mechanism

In the proposed strategy, each BESS node i maintains a local state estimate $x_i(k)$. However, node i never transmits $x_i(k)$ directly. Instead, it generates a perturbed version $\tilde{x}_i(k)$ by injecting a time-varying noise $\eta_i(k)$ before transmission:

$$\tilde{x}_i(k) = x_i(k) + \epsilon_i(k) \tag{6}$$

where $\epsilon_i(k)$ is the artificial noise drawn from a Laplace distribution $Lap(0, b(k))$ to satisfy differential privacy.

B. Distributed Update Law

At time step k, node i receives the perturbed states $\{\tilde{x}_j(k) \mid j \in \mathcal{N}_i\}$ from its neighbors. Node i then updates its local estimate according to the following consensus protocol:

$$x_i(k+1) = x_i(k) - h \sum_{j \in \mathcal{N}_i} a_{ij} \left(x_i(k) - \tilde{x}_j(k) \right) \tag{7}$$

where $h > 0$ is control gain and a_{ij} is the element of the adjacency matrix $\mathcal{A}$.

Substituting (6) into (7), the system dynamics can be expanded as:

$$\begin{aligned} x_i(k+1) &= x_i(k) - h \sum_{j \in \mathcal{N}_i} a_{ij} \left(x_i(k) - (x_j(k) + \epsilon_j(k)) \right) \\ &= \underbrace{x_i(k) - \epsilon \sum_{j \in \mathcal{N}_i} a_{ij} (x_i(k) - x_j(k))}_{\text{Standard Consensus Term}} \qquad (8) \\ &+ \underbrace{h \sum_{j \in \mathcal{N}_i} a_{ij} \epsilon_j(k)}_{\text{Noise Injection Term}} \qquad (9) \end{aligned}$$

From (9), it is evident that the noise $\epsilon_j(k)$ introduced by neighbor j propagates to node i scaled by the coupling weight ϵa_{ij}.

Let $x(k) = [x_1(k), \ldots, x_N(k)]^\top$ and $\eta(k) = [\eta_1(k), \ldots, \eta_N(k)]^\top$ with $\eta_i(k) = \sum_{j \in \mathcal{N}_i} a_{ij} \epsilon_j(k)$. The collective dynamics of the BESS cluster can be written in compact matrix form as:

$$x(k+1) = (I - h\mathcal{L})x(k) + h\mathcal{A}\eta(k) \tag{10}$$

where $\mathcal{L}$ is the Laplacian matrix of the graph $\mathcal{G}$, and $\mathcal{A}$ is the adjacency matrix. This formulation explicitly separates the convergence dynamics (driven by $\mathcal{L}$) from the privacy perturbation (driven by $\mathcal{A}\eta$).

C. Convergence Analysis

We now analyze the convergence properties of the proposed algorithm. Let $\bar{c} = \frac{1}{N}\mathbf{1}^\top \mathbf{x}(0)$ be the true average capacity. We define the estimation error vector as $e(k) = x(k) - \bar{c}\mathbf{1}$.

Let $P = I - h\mathcal{L}$ be the Perron matrix. The system dynamics in (10) can be rewritten in terms of the error vector:

$$e(k+1) = Pe(k) + h\mathcal{A}\eta(k) \tag{11}$$

where η is the vector of privacy noises.

Theorem 1 (Convergence): Assume the communication graph $\mathcal{G}$ is connected, and the control gain h satisfies $0 < h < 2/\lambda_{\max}(\mathcal{L})$. If the noise scale parameter decays exponentially as $b(k) = \beta\rho^k$ with $0 < \rho < 1$, then the system achieves mean-square convergence to the true average, i.e.,

$$\lim_{k \to \infty} \mathbb{E}[\|\mathbf{e}(k)\|^2] = 0 \tag{12}$$

Proof: The trajectory of the error vector from $t = 0$ to k is given by:

$$e(k) = P^k e(0) + h \sum_{t=0}^{k-1} P^{k-1-t} \mathcal{A}\epsilon(t) \tag{13}$$

1) Convergence of the Expectation:
Taking the mathematical expectation on both sides of (13):

$$\mathbb{E}[e(k)] = P^k e(0) + h \sum_{t=0}^{k-1} P^{k-1-t} \mathcal{A}\mathbb{E}[\epsilon(t)] \tag{14}$$

Since the Laplace noise is zero-mean, $\mathbb{E}[\epsilon(t)] = 0$. The second term vanishes. For the first term, since the graph is connected and h is properly chosen, P is a doubly stochastic matrix with a simple eigenvalue at 1 and all other eigenvalues strictly within the unit circle. Since $e(0)$ is orthogonal to the vector of ones (i.e., the sum of errors is zero), we have $\lim_{k\to\infty} P^k e(0) = 0$. Thus, $\lim_{k\to\infty} \mathbb{E}[e(k)] = 0$.

2) Convergence of the Mean Square Error:
Using the independence of noise at different time steps, the mean square error is:

$$\begin{aligned} \mathbb{E}[\|e(k)\|^2] &= \|P^k e(0)\|^2 + \mathbb{E}\left[\left\| h \sum_{t=0}^{k-1} P^{k-1-t} \mathcal{A}\epsilon(t) \right\|^2 \right] \\ &= \|P^k e(0)\|^2 \\ &+ h^2 \sum_{t=0}^{k-1} \mathrm{Tr}\left(\mathcal{A}^\top (P^{k-1-t})^\top P^{k-1-t} \mathcal{A}\mathrm{Cov}(\epsilon(t)) \right) \end{aligned}$$

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.

The covariance matrix of the noise is $\mathrm{Cov}(\epsilon(t)) = \sigma^2(t)I$, where $\sigma^2(t) = 2\beta^2\rho^{2t}$. Let λ_s be the second largest eigenvalue modulus of P. The energy of the transition matrix is bounded by $\|P^t\|_2^2 \le c_0\lambda_s^{2t}$. The term $\mathrm{Tr}(\mathcal{A}^\top \dots \mathcal{A})$ is bounded by some constant M. Thus, the error variance is bounded by:

$$\mathrm{MSE}(k) \le \|P^k e(0)\|^2 + Mh^2\beta^2 \sum_{t=0}^{k-1} \lambda_s^{2(k-1-t)}\rho^{2t} \quad (15)$$

The first term decays to 0 exponentially as $k \to \infty$. The second term is the convolution of two decaying geometric sequences. Since both $\lambda_s < 1$ and $\rho < 1$, their convolution also decays to 0 as $k \to \infty$. Consequently, $\lim_{k\to\infty} \mathbb{E}[\|e(k)\|^2] = 0$. This completes the proof of convergence. ∎

D. Privacy Analysis

We now prove that the proposed algorithm satisfies ϵ-differential privacy over the finite horizon T.

Theorem 2 (Differential Privacy): Let c and c' be two adjacent initial capacity vectors differing by at most ΔC at a single node i. The proposed mechanism satisfies differential privacy, where the total privacy budget ϵ_{total} is given by:

$$\epsilon_{total} = \sum_{k=0}^{T-1} \frac{\Delta C [P^k]_{ii}}{b(k)} \quad (16)$$

where $[P^k]_{ii}$ is the diagonal element of the k-th power of the Perron matrix, and $b(k)$ is the noise scale parameter.

Proof: Consider the perspective of an honest-but-curious adversary observing the sequence of perturbed transmissions from node i, denoted by $O_i = \{\tilde{x}_i(0), \tilde{x}_i(1), \dots, \tilde{x}_i(T-1)\}$. Based on the output perturbation mechanism $\tilde{x}_i(k) = x_i(k) + \epsilon_i(k)$, the probability density function of the observation sequence conditional on the initial state c is:

$$\mathbb{P}(O_i|c) = \prod_{k=0}^{T-1} \frac{1}{2b(k)} \exp\left(-\frac{|\tilde{x}_i(k) - x_i(k)|}{b(k)}\right) \quad (17)$$

For two adjacent datasets c and c' differing only at node i with $|c_i - c_i'| \le \Delta C$, the local state $x_i(k)$ evolves as $x_i(k) = [P^k c]_i + \text{noise terms}$. The sensitivity of the unperturbed state $x_i(k)$ with respect to the initial variation is:

$$|x_i(k;c) - x_i(k;c')| = |[P^k(c-c')]_i| \le [P^k]_{ii}\Delta C \quad (18)$$

According to the sequential composition theorem of differential privacy, we examine the log-likelihood ratio:

$$\ln \frac{\mathbb{P}(O_i|c)}{\mathbb{P}(O_i|c')} = \sum_{k=0}^{T-1} \frac{|x_i(k;c') - \tilde{x}_i(k)| - |x_i(k;c) - \tilde{x}_i(k)|}{b(k)} \le \sum_{k=0}^{T-1} \frac{|x_i(k;c) - x_i(k;c')|}{b(k)} \quad (19)$$

Substituting the sensitivity bound:

$$\ln \frac{\mathbb{P}(O_i|c)}{\mathbb{P}(O_i|c')} \le \sum_{k=0}^{T-1} \frac{[P^k]_{ii}\Delta C}{b(k)} = \epsilon_{total} \quad (20)$$

Thus, the mechanism satisfies differential privacy. Since $b(k) = \beta\rho^k$, by appropriately choosing β and ρ, the total privacy leakage can be bounded within a desired range. ∎

IV. Numerical Simulation

In this section, we validate the effectiveness of the proposed privacy-preserving consensus algorithm through numerical simulations.

We consider a cluster of $N = 10$ distributed BESS units. The communication topology is modeled as a connected ring graph, where each node is connected to exactly two neighbors. The adjacency matrix $\mathcal{A}$ is set such that $a_{ij} = 1$ if nodes i and j are connected, and 0 otherwise. The control gain is set to $h = 0.15$.

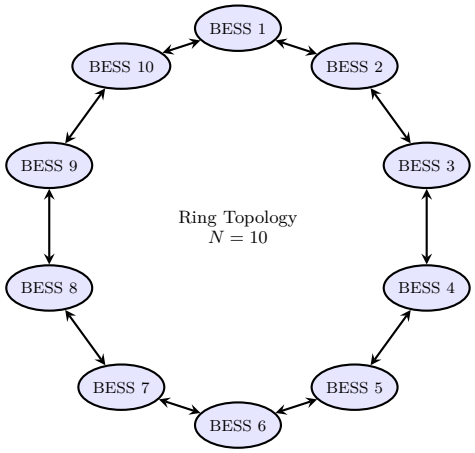

Fig. 2. Communication topology of the BESS cluster ($N = 10$, Ring Graph).

We consider a cluster of $N = 10$ distributed BESS units connected in a ring topology (see Fig. 2). The true initial capacities are randomly generated from $[10, 20]$ kWh. The control gain is $h = 0.15$, and the time horizon is $T = 100$. The privacy noise follows a Laplace distribution with a decaying scale parameter $b(k) = 2.0 \cdot 0.95^k$.

Fig. 3 depicts the temporal evolution of the estimated capacity states for all battery nodes. The ground truth global average $\bar{c}$ is indicated by the black dashed line.

During the initial phase ($k < 20$), the trajectories exhibit significant stochastic fluctuations driven by the high-magnitude noise injection. This high-variance behavior is intentional and crucial, as it effectively masks the true initial states from neighboring nodes. As the iteration proceeds, the noise scale decays, causing the oscillations to attenuate. Ultimately, at $k = T$, all nodal states synchronize and converge precisely to the true average value.

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.

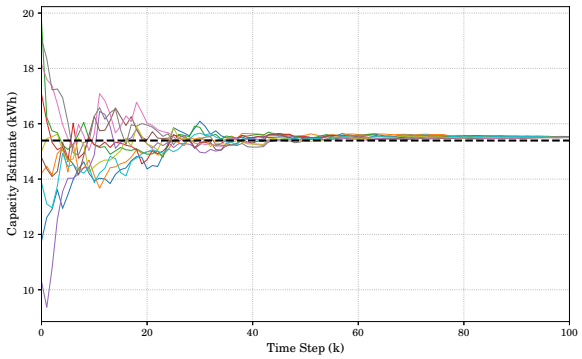

Fig. 3. State trajectories of 10 BESS units with dynamic privacy noise. The fluctuations in the initial phase mask the true values, while convergence is achieved at $k = 100$.

To demonstrate the superiority of the proposed dynamic mechanism, we compare its performance against the conventional static differential privacy approach ($b(k) = \text{constant}$). Fig. 4 presents the evolution of the mean square error (MSE) on a semi-logarithmic scale.

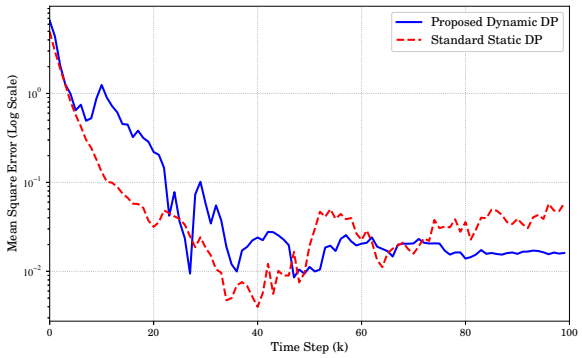

Fig. 4. Comparison of Mean Square Error (MSE) evolution between the proposed Dynamic DP and standard Static DP. The proposed method achieves exponential convergence.

The red curve (Static DP) saturates at a non-zero error floor, confirming that persistent noise prevents exact convergence. In sharp contrast, the blue curve (Proposed Dynamic DP) exhibits a linear decay trend, indicating that the MSE converges to zero exponentially. This verifies that our method eliminates the permanent accuracy loss inherent in traditional schemes.

We further investigate the sensitivity of the algorithm's convergence rate to the noise decay factor ρ. Fig. 5 compares the MSE trajectories under $\rho \in \{0.90, 0.95, 0.99\}$.

A smaller ρ (e.g., 0.90) accelerates the noise attenuation process, resulting in rapid convergence but reduced privacy protection intensity in the early iterations. Conversely, a larger ρ (e.g., 0.99) sustains high-level noise for a longer duration, providing stronger privacy preservation albeit requiring more iterations to achieve the same precision. This highlights the tunable trade-off between convergence speed and privacy security.

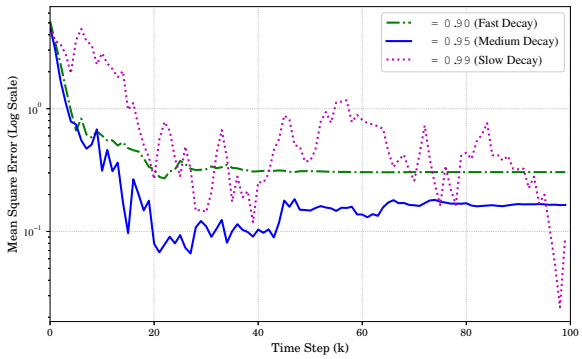

Fig. 5. Impact of different noise decay factors ρ on the convergence speed and privacy duration.

V. Conclusion

In this paper, we proposed a distributed consensus protocol with dynamic output perturbation to estimate the total capacity of BESS clusters. By injecting time-varying Laplace noise, the proposed method resolves the inherent conflict between privacy and accuracy found in traditional differential privacy schemes. Theoretical analysis and numerical simulations confirm that our algorithm ensures ϵ-differential privacy for initial states while achieving exact mean-square convergence to the true average. Future work will extend this framework to asynchronous networks and investigate resilience against active malicious attacks.

References

[1] T. Morstyn, B. Hredzak, and V. G. Agelidis, "Control strategies for microgrids with distributed energy storage systems: An overview," IEEE Transactions on Smart Grid, vol. 9, pp. 3652–3666, 2018.

[2] X. Zhang, G. Yan, M. Zhou, C. Tang, and R. Qu, "Energy management method for virtual power plant based on double-layer deep reinforcement learning game," 2024 6th International Conference on Energy, Power and Grid (ICEPG), pp. 650–655, 2024.

[3] W. jun Tang and H.-T. Yang, "Optimal operation and bidding strategy of a virtual power plant integrated with energy storage systems and elasticity demand response," IEEE Access, vol. 7, pp. 79 798–79 809, 2019.

[4] Q. Liu, J. Tian, K. Zhang, and Q. Yan, "Pricing strategy for a virtual power plant operator with electric vehicle users based on the stackelberg game," World Electric Vehicle Journal, 2023.

[5] J. Le, D. Zhang, X. Lei, L. Jiao, K. Zeng, and X. Liao, "Privacy-preserving federated learning with malicious clients and honest-but-curious servers," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4329–4344, 2023.

[6] M. Zhu, D. Du, X. Li, Q. Sun, M. Fei, and L. Wu, "Distributed security state estimation based on homomorphic encryption for privacy-preserving consensus in cloud environment," IEEE Internet of Things Journal, vol. 12, pp. 50 466–50 479, 2025.

[7] A. Krishnan and R. Arunachalam, "Blockchain-assisted secure iot transmission using homomorphic encryption and distributed consensus," 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), pp. 1295–1299, 2025.

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.

[8] M. Alsayegh and Y.-H. Xu, "A secure multi-party computation framework for decentralized row allocation in cooperative strawberry harvesting systems," 2025 IEEE 21st International Conference on Automation Science and Engineering (CASE), pp. 3399–3405, 2025.
[9] J. Zhou, L. Qu, Y. Sun, W. Yang, and Z. Q. Tian, "Differential privacy consensus in dynamic topologies: Performance analysis and optimization," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 73, pp. 548–561, 2026.
[10] Y. Wang and A. Nedić, "Robust constrained consensus and inequality-constrained distributed optimization with guaranteed differential privacy and accurate convergence," IEEE Transactions on Automatic Control, vol. 69, pp. 7463–7478, 2024.
[11] J. Yuan, W. Sun, Y. Sun, and S.-F. Su, "Mask privacy preservation prescribed-time consensus control for nonlinear multiagent systems," IEEE Transactions on Automation Science and Engineering, vol. 22, pp. 11 554–11 563, 2025.
[12] R. Cao, Y. Zhao, Y. Liu, and P. Huang, "Privacy-protected and prescribed-time dynamic average consensus over directed networks: An integral surplus-based approach," IEEE Transactions on Automatic Control, vol. 70, pp. 7968–7983, 2025.
[13] L. Chang, Q.-L. Han, X. Ge, C. Zhang, and X. Zhang, "On designing distributed prescribed finite-time observers for strict-feedback nonlinear systems," IEEE Transactions on Cybernetics, vol. 51, no. 9, pp. 4695–4706, 2021.
[14] J. Mei, W. Ren, and J. Chen, "Distributed consensus of second-order multi-agent systems with heterogeneous unknown inertias and control gains under a directed graph," IEEE Transactions on Automatic Control, vol. 61, pp. 2019–2034, 2016.

Authorized licensed use limited to: Shanghai Univ of Electric Power. Downloaded on November 05,2026 at 10:36:55 UTC from IEEE Xplore. Restrictions apply.