2025 IEEE 19th International Conference on Control & Automation (ICCA)
June 30 - July 3, 2025. Tallinn, Estonia

Distributed Resilient Consensus and Demand Tracking in Battery Energy Storage Systems under Adversarial Attacks

Shiheng Zhang and Yiding Ji*

Abstract— **Battery Energy Storage Systems (BESS) are critical in balancing power supply and demand by dynamically adjusting charging and discharging power. However, their deployment in public networks renders them vulnerable to adversarial attacks, which can disrupt system coordination and potentially lead to failures. In order to resolve these challenges, this work develops a resilient consensus method that integrates the Mean Subsequence Reduced with demand tracking, structured within a leader-follower control framework. The proposed algorithm guarantees that all non-adversarial agents achieve resilient state-of-charge (SoC) consensus and equitable power distribution, even under malicious battery storage unit conditions. Additionally, we introduce an error tracking factor for leader agents to facilitate accurate demand tracking by the BESS. We establish convergence conditions, demonstrating that the system converges to a final value determined by the communication graph, initial values, and BESS parameters. The performance of our approach is validated by a simulation under adversarial conditions, confirming its robustness and reliability.**

Index Terms— **resilient consensus, distributed control, demand tracking, adversarial attacks, energy storage systems**

I. Introduction

Renewable energy, such as wind, solar, and hydropower, has seen remarkable growth in power generation recently. However, these sources often suffer from significant uncertainty and intermittency due to varying seasonal and climatic conditions, causing imbalances between power supply and demand. Incorporating demand-side resources into power system regulation has emerged as a viable strategy to tackle the issue, leveraging the vast diverse entities operating at low voltage levels [1]. Specifically, BESS, composed of multiple Battery Storage Units (BSUs), plays a critical role in maintaining power balance [2]. BSUs, equipped with bidirectional charging and discharging capabilities, enable dynamic power regulation by absorbing surplus energy during low-demand periods and supplying it when demand peaks. This allows BESS to actively contribute to addressing power regulation and tracking energy demand problems.

Despite the advantages of BESS, the geographic dispersion of BSUs and their ownership by various stakeholders pose challenges to centralized control, particularly in large-scale networks. In this context, distributed control within Multi-Agent Systems (MASs) offers a promising solution that achieves low communication overhead and high scalability [3]–[10]. BESS can be modeled as an MAS, with each BSU functioning as an independent agent. These agents communicate local information and make decisions based on localized computations, enabling the execution of complex tasks that individual BSUs cannot accomplish alone. This distributed approach is increasingly adopted in demand response scenarios [11]–[13], particularly for coordinating the State of Charge (SoC) among BSUs [14]–[16]. Effective SoC coordination is essential for achieving consensus in charging and discharging operations, thus preventing overheating from overcharging and extending battery lifespan. Moreover, synchronized disconnection from the power system enhances overall capacity utilization [17]. The main objectives of this coordination process are: (1) achieving SoC consensus; (2) proportionally distributing charging and discharging power.

While existing SoC control methods offer valuable solutions, they usually assume a fully reliable system and do not account for potential adversarial attacks [18]–[20]. Since BSUs are often deployed in public networks, they are vulnerable to failures and malicious interventions. In such scenarios, some BSUs may operate in an adversarial setting and disseminate deceptive information to neighboring units, compromising system integrity [21]. To mitigate the risks posed by adversarial threats, resilient consensus has gained considerable research interest [22]–[26]. Notably, authors of [27] introduced a resilient algorithm from the MSR method, which reduces the impact of malicious nodes by employing median estimates under robust network conditions. Work [28] extended this approach by integrating optimization techniques, providing explicit formulations for convex combinations of local optimal points, and establishing the existence of a transition matrix. However, the final state in these approaches is stochastic in nature, which complicates the issue of precise demand tracking.

In light of the concerns mentioned above, this paper proposes a leader-follower control framework aimed at accurate demand tracking for SoC consensus, and proportionally distributing charging power in the presence of malicious BSUs. Compared to conventional SoC coordination methods [14]–[16], we introduce an error tracking factor for leader BSUs, enabling accurate tracking of power demand. In contrast to existing resilient consensus methods [21], [27], [28], our strategy guarantees convergence within a leader-follower control framework. Furthermore, unlike existing methods

Shiheng Zhang and Yiding Ji (corresponding author) are both with Robotics and Autonomous Systems Thrust of Systems Hub, the Hong Kong University of Science and Technology (Guangzhou), Guangzhou, China. (Email addresses: florianzsh7@gmail.com, jiyiding@hkust-gz.edu.cn).

This work is supported by the National Natural Science Foundation of China grants 62303389 and 62373289; Guangdong Basic and Applied Basic Research Funding grants 2022A151511076 and 2024A1515012586; Guangdong Scientific Research Platform and Project Scheme grant 2024KTSCX039; Guangzhou Basic and Applied Basic Research Scheme grant 2023A04J1067; Guangzhou-HKUST(GZ) Joint Funding Program grants 2023A03J0678, 2023A03J0011, 2024A03J0618 and 2024A03J0680.

979-8-3315-9559-3/25/$31.00 ©2025 IEEE

that often rely on centralized control schemes, our approach is fully distributed and robust to adversarial conditions.

The technical contributions of our work are outlined as: (1) The development of a distributed leader-follower control framework for BESSs, which ensures exponential consensus convergence in the presence of malicious nodes. (2) A distributed compensation mechanism is designed to achieve accurate demand tracking without requiring global information exchange. (3) A rigorous theoretical analysis is provided to establish provable convergence and stability, using the properties of the network topology and initial conditions through a backward matrix product framework.

The remainder of our work is organized below. In section II, the notations, leader-follower control framework, communication network and problem settings are introduced. Section III details the control method that addresses the resilient consensus problem. Section IV confirms the the convergence of our method. Section V validates the proposed method through numerical simulations. Finally, Section VI concludes the paper and proposes future research directions.

II. Preliminary Knowledge and Problem Formulation

Let $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}_{>0}$ and $\mathbb{Z}_{\geq 0}$ represent the set of real numbers, integers, positive integers and non-negative integers, respectively. Additionaly, $|\cdot|$ and $\|\cdot\|$ denote the 1-norm and 2-norm, respectively, and $\langle \cdot, \cdot \rangle$ represents the inner product. The notation $|\mathcal{T}|$ indicates the cardinality of the set $\mathcal{T}$, while $\mathcal{T}_1 \cup \mathcal{T}_2$ and $\mathcal{T}_1 \backslash \mathcal{T}_2$ denote the union and difference of two sets, respectively. The (i, j)-th element of the matrix A is denoted by A_{ij}. Then $A \in \mathbb{R}^{n \times n}$ is termed row stochastic if $\forall i, j \in \{1, \ldots, n\}$, $A_{ij} \geq 0$ and $A\mathbf{1}_n = \mathbf{1}_n$. For a vector $E \in \mathbb{R}^{n \times 1}$, its i-th component is denoted by E_i. And E is called stochastic if $\forall i \in \{1, \ldots, n\}$, $E_i \geq 0$ and $E^T\mathbf{1} = \mathbf{1}$.

In a Battery Energy Storage System (BESS), Battery Storage Units, namely BSUs, are divided into three distinct categories: normal BSUs, leader BSUs, and malicious BSUs. Normal BSUs transmit and receive information through the communication network, meanwhile, adhere to the designated control law. Leader BSUs receive regulatory demand signals $P^* \in \mathbb{R}$ from the aggregator and are assumed to be immune to attacks. In contrast, malicious BSUs exhibit two problematic behaviors: (i) transmitting arbitrary information to neighboring units and (ii) arbitrarily updating their states regardless of the prescribed rules. The control framework for demand response of BESS comprises a physical and a communication layer, as depicted in Fig. 1.

The aggregator disseminates control information to the leader BSUs on receiving a demand signal from the power system in the communication layer. Subsequently, the BSUs exchange local state and iteratively adjust their charging/discharging power following the proposed distributed algorithm until balance is achieved. The physical layer establishes a connection between the BSUs and the power grid via a microgrid, which charges when the demand $P^* > 0$ and discharges when $P^* < 0$.

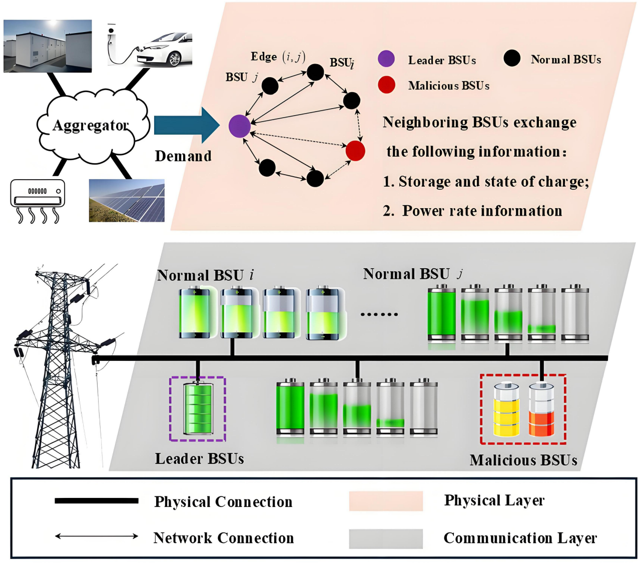


Fig. 1. Leader-Follower Control Scheme for Demand Tracking of BESS.

Remark 1. *Power systems are equipped with protective measures to isolate malicious BSUs by disconnecting affected loads at the physical layer upon detecting adversarial attacks. However, such measures cannot be implemented at the communication layer, thus it is still necessary to design algorithms to address these challenges within that layer.*

For a BESS with n BSUs, the communication network is modeled by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Set $\mathcal{V} = (1, 2, \ldots, n)$ corresponds to the BSUs, and set $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ represents the directed edges between BSUs. (j, i) is an incoming edge of i, which denotes that BSU j transmits information to BSU i with j defined as the in-neighbor of i. The in-neighbor set of node i is represented as $\mathcal{N}_i^- \triangleq \{j \in \mathcal{V} | (j, i) \in \mathcal{E}\}$, and the out-neighbor set is $\mathcal{N}_i^+ \triangleq \{j \in \mathcal{V} | (i, j) \in \mathcal{E}\}$. If there is a directed edge sequence $(i_0, i_1), \ldots, (i_{k-1}, i_k) \in \mathcal{E}$, then a directed path from i_0 to i_k exists. The sets of leader BSUs, normal BSUs, and malicious BSUs are denoted by $\mathcal{V}_{\mathcal{L}}$, $\mathcal{V}_{\mathcal{R}}$ and $\mathcal{V}_{\mathcal{A}}$, respectively. For convenience, define $|\mathcal{V}_{\mathcal{L}}| = \tau \in \mathbb{Z}_{>0}$ and assume that the malicious BSUs are bounded by $F \in \mathbb{Z}_{>0}$, i.e., $|\mathcal{V}_{\mathcal{A}}| = \lambda \in \mathbb{Z}_{\geq 0} \leq F$, and $n \geq 3F + 1$, see, e.g., [27], [28]. The dynamics of each BSU $i \in \mathcal{V}_{\mathcal{R}} \cup \mathcal{V}_{\mathcal{L}}$ are given by:

$$P_i\,(k+1) = P_i\,(k) \tag{1}$$

$$E_i(k+1) = E_i(k) + \frac{T}{3600} P_i(k) \tag{2}$$

where $T > 0$, $E_i(k) \in \mathbb{R}$ represents the energy storage state in kWh, and $P_i(k) \in \mathbb{R}$ denotes the charging/discharging power at step k that is constrained by

$$0 < E_i < \bar{E}_i, \underline{P_i} < P_i < \bar{P}_i. \tag{3}$$

where $\bar{E}_i$ is the maximum energy storage capacity, $\underline{P_i}$ and $\bar{P}_i$ are the maximum discharging and charging power, respectively. The State of Charge (SoC) is $\mathrm{SoC}_i(k) = E_i(k)/\bar{E}_i$, also we define $\tilde{E}_i(k) = \mathrm{SoC}_i(k)$ and $\tilde{P}_i(k) = P_i(k)/\bar{E}_i$.

Definition 1 (Source component)**.** *Given a directed graph $\mathcal{G}$, a set of nodes $\mathcal{C}$ is a source component if given any pair of nodes in $\mathcal{C}$, a directed path exists between them.*

Definition 2 (Reduced graph)**.** *A reduced graph $\mathcal{G}_{\mathcal{R}} = (\mathcal{V}_{\mathcal{R}}, \mathcal{E}_{\mathcal{R}})$ with respect to a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is obtained by removing all malicious nodes, all their edges and at most F additional incoming edges from each non-malicious node of $\mathcal{G}$. The adjacency matrix of $\mathcal{G}_{\mathcal{R}}$ is defined as: $\mathbf{R}_{ij} = 1$ if $i = j$ or edge $(i, j) \in \mathcal{E}_R$; otherwise $\mathbf{R}_{ij} = 0$. The set of reduced graphs w.r.t. $\mathcal{G}$ is denoted by $R(\mathcal{G})$.*

Assumption 1. *[28] Each reduced graph of $\mathcal{G}$ includes at least one nonempty source component.*

Problem 1 (Resilient Consensus with Demand Tracking)**.** *Given a BESS with n BSUs where λ BSUs are malicious, design a controller such that normal and leader BSUs track the power demand and achieve SoC consensus, specifically, (i) the total power of normal and leader BSUs converges to the aggregator's demand, that is, $\lim_{k\to\infty} \sum_{i\in\mathcal{V}_{\mathcal{R}}\cup\mathcal{V}_{\mathcal{L}}} P_i(k) = P^*$; (ii) for all normal and leader BSUs $i, j \in \mathcal{V}_{\mathcal{R}} \cup \mathcal{V}_{\mathcal{L}}$, SoC consensus is achieved, that is, $\lim_{k\to\infty}\tilde{E}_i(k) = \lim_{k\to\infty}\tilde{E}_j(k)$; (iii) for all normal and leader BSUs $i, j \in \mathcal{V}_{\mathcal{R}} \cup \mathcal{V}_{\mathcal{L}}$, charging and discharging power is asymptotically proportional to its respective maximum capacities, that is, $\lim_{k\to\infty}\tilde{P}_i(k) = \lim_{k\to\infty}\tilde{P}_j(k)$.*

III. Resilient Consensus Control with Demand Tracking

In this section, we introduce the State of Charge and Demand Tracking with MSR (SoCDT-MSR) algorithm to address Problem 1. The algorithm comprises three essential steps: (1) exchange of storage and power information with neighboring agents; (2) removing potentially malicious information from the network; (3) updating agent states based on the remaining information.

We are motivated by two primary advantages in utilizing the MSR method. First, it effectively mitigates the impact of malicious nodes in a distributed network without prior knowledge of their locations or quantities. Second, the MSR method exhibits low computational complexity and relies exclusively on local information, enabling efficient operation in a fully distributed environment. Its straightforward network topology further supports deployment in large-scale networks, where centralized approaches may be infeasible.

Then we propose Algorithm 1 where each BSU i in $\mathcal{V}_{\mathcal{R}} \cup \mathcal{V}_{\mathcal{L}}$ undergos three processes at each time step k:

1) *Interact Process:* BSU i transmits its storage information $\tilde{E}_i(k)$ and power information $\tilde{P}_i(k)$ to out-neighbors $\mathcal{N}_i^+$; receives $\tilde{E}_j(k)$ and $\tilde{P}_j(k)$ from in-neighbors $\mathcal{N}_i^-$.
2) *Remove Process:* BSU i sorts $\tilde{E}_j(k)$ and $\tilde{P}_j(k)$ respectively, then discards the F largest values and the F lowest values than $\tilde{P}_i(k)$, getting the subset $\mathcal{L}_i(k) \subset \mathcal{N}_i^-$ from the remaining BSUs. A similar procedure is applied to $\tilde{E}_i(k)$ to construct the subset $\mathcal{M}_i(k) \subset \mathcal{N}_i^-$.
3) *Update Process:* BSU i updates $\tilde{P}_i(k)$ and $\tilde{E}_j(k)$ based on the remaining values:

$$\tilde{P}_i(k+1) = a_{ii}(k)\tilde{P}_i(k) + \sum_{j\in\mathcal{L}_i(k)} a_{ij}(k)\tilde{P}_j(k), i \in \mathcal{V}_{\mathcal{R}} \tag{4a}$$

$$\begin{aligned}\tilde{P}_i(k+1) = {} & a_{ii}(k)\tilde{P}_i(k) \\ & + \sum_{j\in\mathcal{L}_i(k)} a_{ij}(k)\tilde{P}_j(k) - \phi(k), i \in \mathcal{V}_{\mathcal{L}}\end{aligned} \tag{4b}$$

$$\begin{aligned}\tilde{E}_i(k+1) = {} & w_{ii}(k)\tilde{E}_i(k) \\ & + \sum_{j\in\mathcal{M}_i(k)} w_{ij}(k)\hat{E}_j(k) + c_0\tilde{P}_i(k)\end{aligned} \tag{4c}$$

where $c_0 \in (0, 1)$ is the charging parameter and $\phi(k)$ is:

$$\phi(k) = \sum\nolimits_{i\in\mathcal{V}_{\mathcal{R}}\cup\mathcal{V}_{\mathcal{L}}} P_i(k) - P^*. \tag{5}$$

The weight coefficients $a_{ij}(k)$ and $w_{ij}(k)$ are calculated by:

$$a_{ij}(k) = \begin{cases} \frac{1}{(|\mathcal{L}_i(k)|+1)}, & \text{if} \quad i \neq j, \\ 1 - \sum\limits_{j\in\mathcal{L}_i(k)} \frac{1}{(|\mathcal{L}_i(k)|+1)}, & \text{if} \quad i = j, \\ 0, & \text{otherwise} \end{cases}$$

$$w_{ij}(k) = \begin{cases} \frac{1}{(|\mathcal{M}_i(k)|+1)}, & \text{if} \quad i \neq j, \\ 1 - \sum\limits_{j\in\mathcal{M}_i(k)} \frac{1}{(|\mathcal{M}_i(k)|+1)}, & \text{if} \quad i = j, \\ 0, & \text{otherwise} \end{cases}$$

The above two equations form the lazy Metropolis matrix, which is preferred in distributed algorithms for its compliance with the detailed balance condition, ensuring convergence to the correct equilibrium distribution. The agents are also driven to explore the state space by allowing equal probability transitions to any neighboring node. On the other hand, the error factor $\phi(k)$ adaptively tracks the global demand P^*, correcting local-global deviations and ensuring stable leader influence. Its boundedness and decreasing nature ensure asymptotic stability.

Remark 2. *For the implementation of the algorithm, network construction should be elaborated. Specifically, the parameter F determines the dimension of the network n, as outlined in* Assumption 1. *Subsequently, a weakly connected topology comprising $n - F$ nodes is established. An additional set of F nodes is then incorporated to enable bidirectional communication with all other nodes. Finally, the in-neighbor of each node is adjusted to at least $2F + 1$ [28], [29].*

IV. Convergence Analysis

We first review intermediate results concerning the transition matrix. Based on this foundation, we then provide the convergence analysis. We do not distinguish between $|\mathcal{V}_{\mathcal{R}} \cup \mathcal{V}_{\mathcal{L}}|$ and $n-\lambda$, and, index the leader and normal BSUs as $\{1, 2, \ldots, \tau, \tau + 1, \ldots, n - \lambda\}$. Inspired by [28], [29], we define two matrices $\mathbf{W}(k)$ and $\mathbf{A}(k)$, then reformulate equation (4) as the following form:

$$\tilde{P}(k+1) = \mathbf{A}(k)\tilde{P}(k) - \Phi(k) \tag{6a}$$

$$\tilde{E}(k+1) = \mathbf{W}(k)\tilde{E}(k) + c_0\tilde{P}(k) \tag{6b}$$

Here $\tilde{P}(k) = [\tilde{P}_1, \ldots, \tilde{P}_\tau(k), \tilde{P}_{\tau+1}(k), \ldots, \tilde{P}_{n-\lambda}(k)]^T$, $\tilde{E}(k) = [\tilde{E}_1, \ldots, \tilde{E}_\tau(k), \tilde{E}_{\tau+1}(k), \ldots, \tilde{E}_{n-\lambda}(k)]^T$,

Algorithm 1: SoCDT-MSR Algorithm

```
Input: $F$, $\bar{E}_i$, $\underline{P_i}$, $\bar{P}_i$, $c_0$.
Output: $P_i(k+1), E_i(k+1)$
Initialization: Set $\tilde{P}_i(0)$ and $\tilde{E}_i(0)$ to an arbitary value that satisfy the constraint (3);
for $k = 0, 1, \dots$ do
    Interact Process:
    Transmit $\tilde{E}_i(k)$, $\tilde{P}_i(k)$ to $j \in \mathcal{N}_i^+$;
    Receive $\tilde{E}_j(k)$, $\tilde{P}_j(k)$ from $j \in \mathcal{N}_i^-$;
    Remove Process:
    $\mathcal{L}_i(k) \leftarrow$ remove $F$ largest and smallest $\tilde{P}_j(k)$;
    $\mathcal{M}_i(k) \leftarrow$ remove $F$ largest and smallest $\tilde{E}_j(k)$;
    Update Process:
    Compute $a_{ij}(k)$ and $w_{ij}(k)$;
    Update $\tilde{P}_i(k+1) = \begin{cases} a_{ii}(k)\tilde{P}_i(k) + \sum_{j \in \mathcal{L}_i(k)} a_{ij}(k)\tilde{P}_j(k), i \in \mathcal{V}_\mathcal{R} \\ a_{ii}(k)\tilde{P}_i(k) + \sum_{j \in \mathcal{L}_i(k)} a_{ij}(k)\tilde{P}_j(k) - \phi(k), i \in \mathcal{V}_\mathcal{L}. \end{cases}$
    Update $\tilde{E}_i(k+1) =$
        $w_{ii}(k)\tilde{E}_i(k) + \sum_{j \in \mathcal{M}_i(k)} w_{ij}(k)\tilde{E}_j(k) + c_0\tilde{P}_i\,(k)$;
end
Result: $\tilde{P}_i(k+1), \tilde{E}_i(k+1)$
```

$\Phi(k) = [\underbrace{\phi(k), \phi(k), \phi(k)}_{\tau}, \underbrace{0, \cdots, 0}_{|\mathcal{V}_\mathcal{R}|}]^T$. The matrix $\mathbf{A}(k) = [\mathbf{A}_{ij}(k)]_{(n-\lambda)\times(n-\lambda)}$ satisfies: (1) $\mathbf{A}(k)$ is row stochastic; (2) $\mathbf{A}_{ij}(k)$ is not zero if $(j, i) \in \mathcal{E}$ or $j = i$; (3) if $\mathbf{A}_{ij}(k)$ is not zero, $\mathbf{A}_{ij}(k) \geq \xi$, where $\xi = \frac{1}{2\left(\max\left|\mathcal{N}_i^-\right|+1-2F\right)}$. The above properties also hold for $\mathbf{W}(k) = [\mathbf{W}_{ij}(k)]_{(n-\lambda)\times(n-\lambda)}$. There exist two reduced graphs $\mathcal{R}_a(k), \mathcal{R}_w(k) \in \mathcal{G}_\mathcal{R}$ with corresponding matrices $\mathbf{R_a}(k)$ and $\mathbf{R_w}(k)$ allowing that $\mathbf{A}(k) \geq \xi\mathbf{R_a}(k), \mathbf{W}(k) \geq \xi\mathbf{R_w}(k)$. The backward product is defined as $\Lambda(k, t) = \mathbf{A}(k)\cdots\mathbf{A}(t)$, $\Gamma(k, t) = \mathbf{W}(k)\cdots\mathbf{W}(t)$ for $t \leq k$, with $\Lambda(k, k+1) = \Gamma(k, k+1) = \mathbf{I}_{(n-\lambda)}$. Then we present the following lemma, whose proof is quite similar to those in [28], [29] and skipped here for simplicity. The convergence of Algorithm 1 is established in Theorem 1.

Lemma 1. *If Assumption 1 holds, MSR method guarantees that for all time t and* $k \geq t$*:* $\lim_{k\to\infty}\Lambda\left(k, t\right) = \psi(t)\mathbf{1}^\mathrm{T}$, $\lim_{k\to\infty}\Gamma\left(k, t\right) = \pi(t)\mathbf{1}^\mathrm{T}$, *where* $\psi(t), \pi(t) \in \mathbb{R}^{(n-\lambda)}$ *are stochastic time-varying vectors.*

Theorem 1. *If* Assumption 1 *holds, then the BESS achieves resilient SoC consensus, power distribution, and demand tracking through Algorithm 1, despite the presence of malicious BSUs. That is,* $\forall i, j \in \mathcal{V}_\mathcal{R} \cup \mathcal{V}_\mathcal{L}$, *conditions* $\lim_{k\to\infty}\sum_{i\in\mathcal{V}_\mathcal{R}\cup\mathcal{V}_\mathcal{L}} P_i(k) = P^*$, $\lim_{k\to\infty}\mathrm{SoC}_i\left(k\right) = \lim_{k\to\infty}\mathrm{SoC}_j\left(k\right)$ *and* $\lim_{k\to\infty}\tilde{P}_i(k) = \lim_{k\to\infty}\tilde{P}_j(k)$ *hold.*

Proof: From(6a), we get

$$\begin{aligned}\tilde{P}(k+1) =& \mathbf{A}(k)(\mathbf{A}(k-1)\tilde{P}(k-1) - \Phi(k-1)) - \Phi(k) \\ =& \mathbf{A}(k)\mathbf{A}(k-1)\cdots\mathbf{A}(0)\tilde{P}(0) \\ & - \sum_{t=0}^{k}\left(\mathbf{A}(k)\mathbf{A}(k-1)\cdots\mathbf{A}(t+1)\right)\Phi(t) \\ =& \Lambda(k, 0)\tilde{P}(0) - \sum_{t=1}^{k+1}\Lambda(k, t)\Phi(t-1) \end{aligned} \tag{7}$$

Take the derivative of $\phi(k) = \sum_{i\in\mathcal{V}_\mathcal{R}\cup\mathcal{V}_\mathcal{L}} P_i(k) - P^*$, then

$$\dot{\phi}(k+1) = \sum_{i=1}^{n-\lambda}\dot{P}_i(k+1) = \mathbf{1}^T\dot{\tilde{P}}(k+1)Z \tag{8}$$

where $Z = \mathrm{diag}(\frac{1}{\bar{E}_1}, \frac{1}{\bar{E}_2}, \dots, \frac{1}{\bar{E}_{n-\lambda}})$ is a diagonal matrix that normalizes the power values by the inverse of the maximum energy storage capacities $\bar{E}_i$. Then substitute (7) into (8),

$$\begin{aligned}\dot{\phi}(k+1) &= (\dot{\Lambda}(k, 0)\tilde{P}(0) - \sum_{t=1}^{k+1}\dot{\Lambda}(k, t)\Phi(t-1))Z \\ &= -\mathbf{1}^T(\sum_{t=1}^{k+1}\dot{\Lambda}(k, t)\mathbf{1}^T\phi(t-1))Z = -c\phi(k)\end{aligned}$$

where Z is a diagonal matrix whose entries are strictly less than 1, and $\Lambda(k, t)$ is row stochastic. Both matrices have eigenvalues confined to the interval $(0, 1)$, ensuring that $c > 0$ holds. Therefore, ϕ is exponentially stable and goes to zero as $k \to \infty$. According to *Lemma 1*, for any $k \geq t \geq 0$, the backward product $\Lambda(k, t)$ contracts at an exponential rate due to the assumption of joint strong connectivity over a finite time interval. Specifically, we have constants $C > 0$ and $0 < \eta < 1$ such that $\|\Lambda(k, 0)\| \leq C\eta^k$. Then, we obtain

$$\|\tilde{P}(k)\| = \|\Lambda(k, 0)\tilde{P}(0)\| \leq C\eta^k\|\tilde{P}(0)\|, \tag{9}$$

which indicates that the power ratio decays exponentially. Then we take $k \to \infty$ of (7) and apply *Lemma 1* to obtain

$$\begin{aligned}\lim_{k\to\infty}\tilde{P}(k+1) &= \mathbf{1}\psi^T(0)\tilde{P}(0) - \sum_{t=1}^{k+1}\mathbf{1}\psi^T(t)\Phi(t-1) \\ &= \left(\left\langle\psi^T(0), \tilde{P}(0)\right\rangle - \sum_{t=1}^{k+1}\left\langle\psi^T(t), \Phi(t-1)\right\rangle\right)\mathbf{1}.\end{aligned} \tag{10}$$

$\tilde{P}_i(k)$ converges to $\langle\psi^T(0), \tilde{P}(0)\rangle - \sum_{t=1}^{k+1}\langle\psi^T(t), \Phi(t-1)\rangle$ as $k \to \infty$. This value is determined by the maximum energy storage capacities $\bar{E}_i$, initial powers $P_i(0)$, and the communication graph $\mathcal{G}$. From (6b), we get

$$\begin{aligned}\tilde{E}(k+1) =& \mathbf{W}(k)\mathbf{W}(k-1)\cdots\mathbf{W}(0)\tilde{E}(0) \\ & + \sum_{t=0}^{k}(\mathbf{W}(k)\mathbf{W}(k-1)\cdots\mathbf{W}(t+1))c_0\tilde{P}(t) \\ =& \Gamma(k, 0)\tilde{E}(0) + c_0\sum_{t=1}^{k+1}\Gamma(k, t)\tilde{P}(t-1).\end{aligned} \tag{11}$$

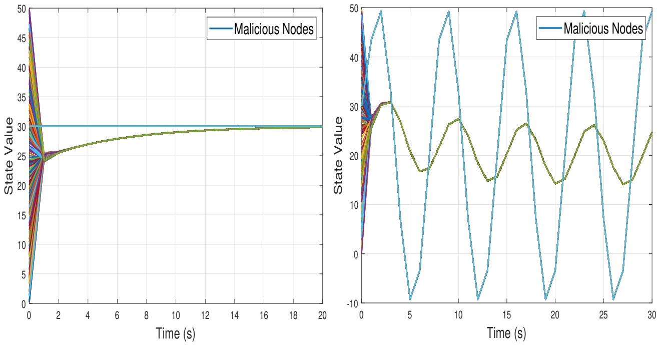
Taking the limit as $k \to \infty$ and applying *Lemma 1*, we obtain

$$\begin{aligned}\lim_{k\to\infty}\tilde{E}(k+1) &= \mathbf{1}\pi^\mathrm{T}(0)\tilde{E}(0) + c_0\sum_{t=1}^{k+1}\mathbf{1}\pi^\mathrm{T}(t)\tilde{P}(t-1) \\ &= \left(\left\langle\pi^\mathrm{T}(0), \tilde{E}(0)\right\rangle + c_0\sum_{t=1}^{k+1}\left\langle\pi^\mathrm{T}(t), \tilde{P}(t-1)\right\rangle\right)\mathbf{1}.\end{aligned} \tag{12}$$

Thus, $\tilde{E}_i(k)$ converges to a consensus value $\langle \pi^{\mathrm{T}}(0), \tilde{E}(0)\rangle + c_0 \sum_{t=1}^{k+1} \langle \pi^{\mathrm{T}}(t), \tilde{P}(t-1)\rangle$, determined by the maximum energy storage capacities $\bar{E}_i$, initial storage states $E_i(0)$, powers $P_i(k)$, charging parameter c_0 and the graph $\mathcal{G}$. ■

V. Simulation Results

In our empirical study, we first show that benchmark SoC methods fail to converge and stability is not guaranteed when malicious BSUs exist, as shown in Fig. 2. Note that final states converge to malicious nodes, which should be avoided.



(a) Constant Value (b) Time-varying value

Fig. 2. Convergence of benchmark SoC algorithm with malicious nodes.

We consider a small-scale BESS comprising 7 BSUs. In this configuration, node 1 serves as the leader BSU, while node 7 is the malicious BSU. Nodes 2 through 6 are normal BSUs that are not under attack. A reduced graph is also shown in Fig. 3, satisfying *Assumption 1* with $F = 1$. The maximum capacity $\bar{E}_i$, maximum discharge power $\underline{P_i}$, and maximum charge power $\bar{P}_i$ for each BSU are summarized in the table. The states of the malicious BSU are generated arbitrarily, with its charging/discharging power and energy storage state at time k set as $P_7(k) = 20\sin\left(\frac{\pi k}{20}\right)$ and $E_7(k) = 5\sin\left(\frac{\pi k}{50}\right) + 5$. The parameter c_0 is set to 3.3×10^{-4}.

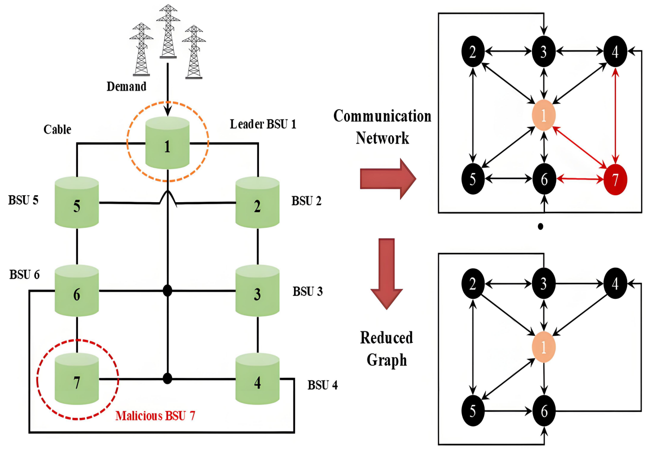


Fig. 3. Communication network of a small-scale BESS.

On receiving a regulation demand of $P^* = 30$kW, we run Algorithm 1 and obtain two values depicted in Fig. 4. The power ratio relative to maximum capacity, $\tilde{P}_i(k)$, achieves consensus in roughly 30 seconds and stabilizes at around 0.18. Due to varying maximum capacities, the real power is not uniform across all BSUs. The total real power of non-malicious BSUs, $\sum_{i\in\mathcal{V}_{\mathcal{L}}\cup\mathcal{V}_{\mathcal{R}}} P_i(k)$, is shown in Fig. 5.

IDs	$E_i(0)$	$P_i(0)$	$\bar{E}_i$	$\underline{P_i}$	$\bar{P}_i$
1	20kWh	0kW	50kWh	-50kW	100kW
2	25kWh	-5kW	50kWh	-50kW	100kW
3	10kWh	5kW	45kWh	-40kW	80kW
4	15kWh	1kW	45kWh	-40kW	80kW
5	5kWh	8kW	40kWh	-30kW	60kW
6	12kWh	4kW	40kWh	-30kW	60kW
7	/	/	/	/	/

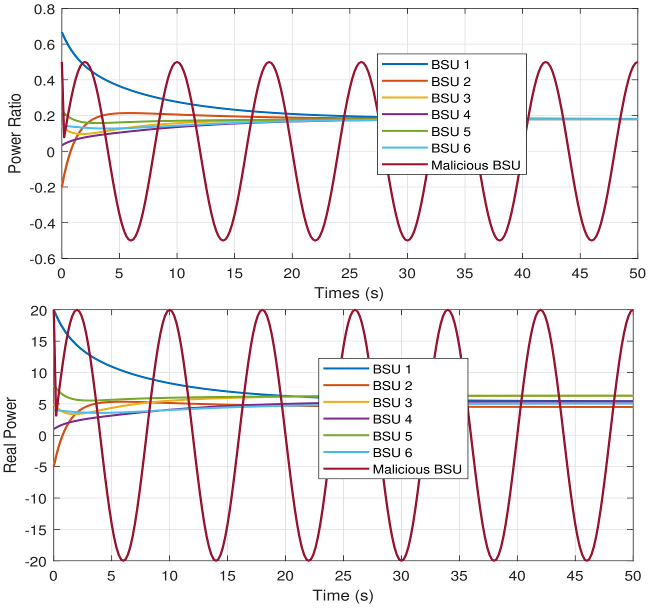


Fig. 4. Consensus of power ratio and convergence of real power.

Initially, the BESS struggles to track the demand due to incomplete filtering of malicious information. As the number of iterations increases, Algorithm 1 filters out malicious data, then the total power aligns with the demand at approximately 28 seconds and stabilizes at 30 kW. The SoC convergence and real energy storage is shown in Fig. 6. The SoC state $\tilde{E}_i(k)$ reaches consensus in approximately 35 seconds and stabilizes around 0.55. It continues to increase as the positive real power $P_i > 0$ indicates that the BSUs are in a charging state. The whole process are unaffected by malicious BSUs.

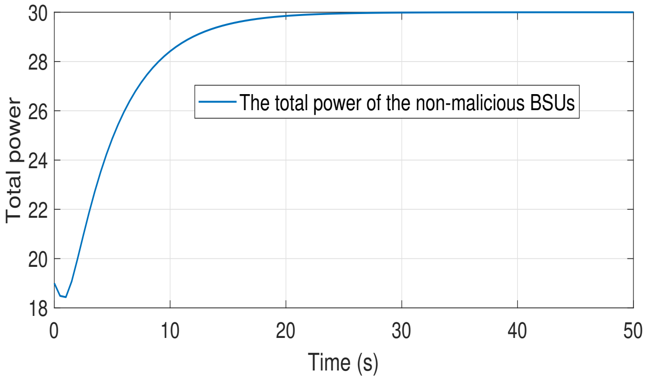


Fig. 5. Demand tracking performance of the BESS.

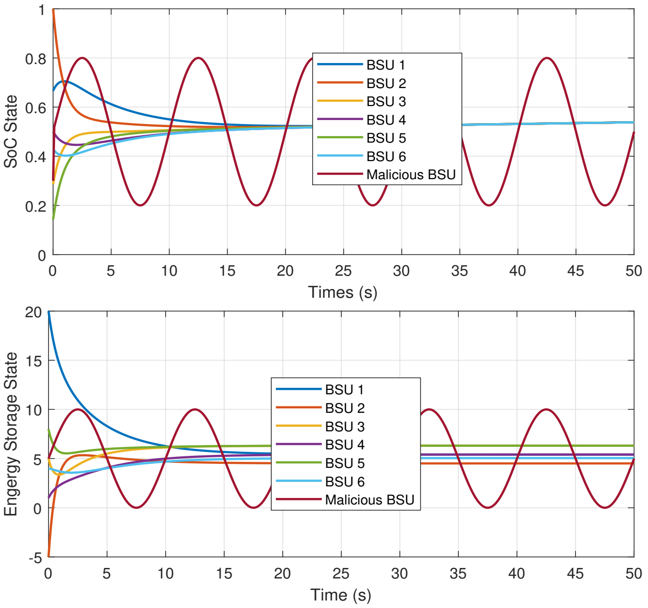


Fig. 6. SoC consensus and convergence of real energy storage.

VI. Conclusion

We proposed a distributed resilient consensus algorithm SoCDT-MSR for BESS operating with malicious BSUs. Our algorithm is established in a leader-follower control framework, which facilitates the BESS to achieve consensus on state of charge (SoC), track demand effectively, and distribute power utilizing the Mean Subsequence Reduced method. We have proved that our algorithm converges over finite time, which also ensures its correctness. The performance of our approach is then demonstrated through various numerical simulations. Future research will extend the framework to accommodate more complex demand-side resources in nonlinear control settings. As systems may encompass various heterogeneous demand-side resources, it is also critical to design a universal algorithm to manage them effectively.

References

[1] S. Panda, S. Mohanty, P. K. Rout, B. K. Sahu, S. M. Parida, I. S. Samanta, M. Bajaj, M. Piecha, V. Blazek, and L. Prokop, "A comprehensive review on demand side management and market design for renewable energy support and integration," *Energy Reports*, vol. 10, pp. 2228–2250, 2023.

[2] M. Behrangrad, "A review of demand side management business models in the electricity market," *Renewable and Sustainable Energy Reviews*, vol. 47, pp. 270–283, 2015.

[3] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[4] W. Zhu, Z.-P. Jiang, and G. Feng, "Event-based consensus of multi-agent systems with general linear models," *Automatica*, vol. 50, no. 2, pp. 552–558, 2014.

[5] Y. Lyu, J. Hu, B. M. Chen, C. Zhao, and Q. Pan, "Multivehicle flocking with collision avoidance via distributed model predictive control," *IEEE Trans. on Cybernetics*, vol. 51, no. 5, pp. 2651–2662, 2021.

[6] Y. Liu, J. Liu, Z. He, Z. Li, Q. Zhang, and Z. Ding, "A survey of multi-agent systems on distributed formation control," *Unmanned Systems*, vol. 12, no. 05, pp. 913–926, 2024.

[7] S. Zhang, Z.-W. Liu, G. Wen, and Y.-W. Wang, "Accelerated distributed optimization algorithm with malicious nodes," *IEEE Trans. on Network Science and Eng.*, vol. 11, no. 2, pp. 2238–2248, 2024.

[8] Z. Wang, X. Wang, and N. Pang, "Adaptive fixed-time control for full state-constrained nonlinear systems: Switched-self-triggered case," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 2, pp. 752–756, 2024.

[9] Y. Zhou, G. Wen, J. Zhou, and T. Yang, "Data-driven fault-tolerant bipartite consensus tracking for multi-agent systems with a non-autonomous leader," *IEEE/CAA Journal of Automatica Sinica*, vol. 12, no. 1, pp. 279–281, 2025.

[10] X. Chen, S. Hu, T. Yang, X. Xie, and J. Qiu, "Event-triggered bipartite consensus of multiagent systems with input saturation and dos attacks over weighted directed networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 7, pp. 4054 – 4065, 2024.

[11] C. Chen, J. Wang, and S. Kishore, "A distributed direct load control approach for large-scale residential demand response," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2219–2228, 2014.

[12] Y. Wang, Y. Huang, Y. Wang, M. Zeng, F. Li, Y. Wang, and Y. Zhang, "Energy management of smart micro-grid with response loads and distributed generation considering demand response," *Journal of Cleaner Production*, vol. 197, pp. 1069–1083, 2018.

[13] Y. Li, X. Long, Y. Li, Y. Ding, T. Yang, and Z. Zeng, "A demand–supply cooperative responding strategy in power system with high renewable energy penetration," *IEEE Transactions on Control Systems Technology*, vol. 32, no. 3, pp. 874–890, 2024.

[14] X. Lu, K. Sun, J. M. Guerrero, J. C. Vasquez, and L. Huang, "State-of-charge balance using adaptive droop control for distributed energy storage systems in dc microgrid applications," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 6, pp. 2804–2815, 2014.

[15] C. Li, E. A. A. Coelho, T. Dragicevic, J. M. Guerrero, and J. C. Vasquez, "Multiagent-based distributed state of charge balancing control for distributed energy storage units in AC microgrids," *IEEE Trans. on Industry Applications*, vol. 53, no. 3, pp. 2369–2381, 2017.

[16] T. Meng, Z. Lin, and Y. A. Shamash, "Distributed cooperative control of battery energy storage systems in DC microgrids," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 3, pp. 606–616, 2021.

[17] A. Khalid, A. Stevenson, and A. I. Sarwat, "Overview of technical specifications for grid-connected microgrid battery energy storage systems," *IEEE Access*, vol. 9, pp. 163554–163593, 2021.

[18] Z. Miao, L. Xu, V. R. Disfani, and L. Fan, "An SoC-based battery management system for microgrids," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 966–973, 2014.

[19] J. Khazaei and Z. Miao, "Consensus control for energy storage systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3009–3017, 2018.

[20] L. Xing, Y. Mishra, Y.-C. Tian, G. Ledwich, C. Zhou, W. Du, and F. Qian, "Distributed state-of-charge balance control with event-triggered signal transmissions for multiple energy storage systems in smart grid," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1601–1611, 2019.

[21] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[22] D. Saldaña, A. Prorok, S. Sundaram, M. F. M. Campos, and V. Kumar, "Resilient consensus for time-varying networks of dynamic agents," in *2017 American Control Conference (ACC)*, pp. 252–258, 2017.

[23] L. Yuan and H. Ishii, "Event-triggered approximate byzantine consensus with multi-hop communication," *IEEE Transactions on Signal Processing*, vol. 71, pp. 1742–1754, 2023.

[24] X. Gong, X. Li, Z. Shu, and Z. Feng, "Resilient output formation-tracking of heterogeneous multiagent systems against general byzantine attacks: A twin-layer approach," *IEEE Transactions on Cybernetics*, vol. 54, no. 4, pp. 2566–2578, 2024.

[25] D. M. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in asynchronous networks," *Automatica*, vol. 104, pp. 26–33, 2019.

[26] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, 2019.

[27] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[28] L. Su and N. H. Vaidya, "Byzantine-resilient multiagent optimization," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2227–2233, 2021.

[29] L. Tseng, G. Liang, and N. H. Vaidya, "Iterative approximate byzantine consensus in arbitrary directed graphs," *Distributed Computing*, vol. 37, no. 3, pp. 225–246, 2024.