Journal of Energy Storage 86 (2024) 111180

Contents lists available at ScienceDirect

Journal of Energy Storage

journal homepage: www.elsevier.com/locate/est

Research papers

Distributed consensus controlled multi-battery-energy-storage-system under denial-of-service attacks

Don Gamage [a,*], Chathura Wanigasekara [b], Abhisek Ukil [a], Akshya Swain [a]

[a] The University of Auckland, Department of Electrical, Computer, and Software Engineering, Auckland, 1023, New Zealand
[b] German Aerospace Centre (DLR), Institute for the Protection of Maritime Infrastructures, Bremerhaven, 27572, Germany

ARTICLE INFO

Keywords:
Distributed control
Multi-agent systems
Multi-battery-energy-storage system
Denial of service attacks

ABSTRACT

The challenge of denial of service attacks (DoS) on distributed communication channels of multi battery energy storage systems (MBESSs) in a microgrid is discussed in this article. It is important to note that DoS attacks may prevent information from being shared between agents by stopping from transferring data, putting the devices in danger and jamming a communication network. Therefore, consensus-based control strategy with the state feedback of power and energy of battery storage mechanism is introduced to minimise the impact of DoS attacks by introducing the adaptive coefficient to the conventional consensus framework. This framework proposes a distributed resilient finite-time secondary control scheme so that DC bus voltage regulation, active power sharing, and energy level balancing of BESSs while maintaining the state of charge (SoC) of the individual BESS remain in the safe range. It is assumed that operational constraints can be satisfied at any control transient time. In addition, theoretical analysis is used to explicitly demonstrate the influence of DoS attack length time on the control algorithm's convergence time. Furthermore, the simulation study is carried out in Matlab/Simulink to validate proposed model with three different case studies, along with OPAL-RT based real-time validation.

1. Introduction

Due to the rising penetration of renewable energy sources (RES)s and electrical vehicles over the last decades, distributed multiple battery energy storage systems (BESSs) have played an important role in microgrid management and operation [1–3]. By effectively charging and discharging to balance intermittent power output and time-varying load demand, BESSs in microgrids may enhance power quality and network stability [4,5]. Many researchers have identified that due to the intermittent behaviour of the RESs, proper control algorithms will enhance the output power at its optimum value [6,7]. Although primary droop management may quickly stabilise the microgrid, it causes the steady-state frequency of BESSs to deviate from the nominal frequency [8,9]. As a result, secondary control is essential for returning the voltage of the microgrid and frequency to their nominal levels [10–12]. Researchers in [11] have proposed a PQ based controller to keep the voltage and frequency at grid exit point (GXP). When numerous heterogeneous BESSs engage in secondary frequency management in a microgrid, their energy levels or state of charge (SoC) levels of the energy storage must be correctly coordinated to ensure that the BESSs do not run out of energy or become overloaded. Thus, it is very critical to balance the BESS SoC levels to lengthen the life span of the BESSs while improving power quality of the grid by peak shaving/shifting [3], but it will also create oscillations in active power, which will affect frequency control. As a result, it is necessary to coordinate the SFC [13] and SoC balance [14] concerns concurrently.

Many recent works [3,15–17] have identified that consensus topology will have great impact on improving the system stability not only for frequency regulation but also to regulate the DC bus voltage of the microgrid. The leader follower consensus algorithm was proposed with novel approach by the researchers in [18]. Fast frequency and voltage regulations were discussed during the self delays and communication delays in [19]. However, the analysis of these consensus control based system performances during the cyber attacks is still a challenging task, and this paper mainly focuses at the system's stability during the DoS attacks. The general architecture of the MBESS with the cyber layer is shown in Fig. 1.

Cyber assaults, such as DoS attacks [20] and false data injection (FDI) attacks [10], targeting main SCADA systems in power systems have become more common, such as the 2020 Mumbai power outage and the 2016 Ukrainian power blackout [21]. DoS attackers disrupt the

* Corresponding author.
E-mail addresses: dgam963@aucklanduni.ac.nz (D. Gamage), chathura.wanigasekara@dlr.de (C. Wanigasekara), a.ukil@auckland.ac.nz (A. Ukil), a.swain@auckland.ac.nz (A. Swain).

https://doi.org/10.1016/j.est.2024.111180
Received 11 September 2023; Received in revised form 26 January 2024; Accepted 28 February 2024
Available online 6 March 2024

Nomenclature

$1/\tau_a \in (0,1)$	The level of DoS attack severity.
$\mathcal{F}_a$	The positive value denoting the frequency of DoS attacks
$\mathcal{N}a$	The number of count of DoS attacks
$\tilde{\Delta}_n$	The duration of a single attack
$\Xi_a\left(t_1,t_2\right)$	The intervals where jammed interactions occur within $\left[t_1,t_2\right]$
$\Xi_s\left(t_1,t_2\right)$	The intervals of normal interaction within $\left[t_1,t_2\right]$
c_{ij}	ith BESS and jth BESS adaptive law
C_i	ith BESS capacity
d_{b_i}	ith BESS duty cycle
K_i	ith BESS control gain
P_{B_i}	ith BESS's power input/output
SoC_i	ith BESS SoC
u_i	ith BESS Consensus Control input
V_{Bi}, I_{Bat_i}	ith BESS voltage and current
z, ψ_{ij}	Consensus error 'between ith BESS and jth BESS
a_{ij}	Adjacent parameters of ith and jth BESSs

communication channel, preventing network data from being correctly sent, destroying the data's authenticity. The problem will get worse if the generating is unable to receive effective control signals, thereby deteriorating the performance of the BESSs [22]. As a result, developing an appropriate control strategy for BESSs to cope with system's frequency and SoC balance issues that are vulnerable to DoS attacks on local communication networks between local and global controllers remains an intractable problem.

The increased frequency stability is thought to be the potential benefit of contemporary low-inertia energy systems with integrated BESSs [23]. Furthermore, authors in [24] have engaged with small signal and frequency stability analysis during the communication failures under DoS attacks. It is interesting to note that authors have used consensus approach to achieve their goals. They are able to make rapid adjustments to the frequency and distribute the load among traditional units of power generating The use of electric vehicles can greatly reduce the amount and cost of power factor-correction (PFC), as mentioned in [25].

Therefore, the main focus of this article is to propose the operational model for proportional automated generation control (AGC) involving many BESSs to cooperate in frequency and voltage regulation technique. This operating model is capable of evenly distributing the AGC burden across energy distribution. BESS and the grid operator converge to a pre-agreed value on storage sources [26]. The use of their BESSs' energy is examined in [27,28] with a focus on how each BESS manages its short-term energy resources and the dynamic application of a specific (or varying) percentage of its capacity to the calculation of AGC signals in order to enhance frequency grid operators' ability to regulate frequency. For an instance, the owner by regulation of the ith BESS undertakes to reserve 20% of the BESS capacity.

1.1. Main objective and rationale

While numerous studies have explored power management within microgrids, there has been comparatively less focus on researching the management of energy within multiple storage systems during DoS attacks. This study aims to examine whether a consensus control strategy can efficiently equalise power and energy in a microgrid containing multiple energy storage devices during the duration of the DoS attack by discharging the energy storage. It is noted that, the DC bus voltage remain constant throughout these times. During these convergences, the SoC of the batteries have been maintained at safe ranges. Consequently, this research introduces a distributed and coordinated consensus control method for managing multiple energy storage units, highlighting the numerous benefits it offers.

1.2. Main research contribution

The main contributions of this scope of research can be categorised as follow,

- A novel approach with multi energy storage system with consensus based controller to converge to an agreed value of SoC, power and energy in the event of power imbalance of the entire system.
- The system still approaches the consensus theory during the DoS attacks in communication channels. This will enhance the system stability during the time of DoS attacks. This will also keep the active power balance in the entire system to regulate the frequency of BESS.
- The DC bus voltage is regulated during the interruptions in communication channels.

The remainder of the paper is organised as follows. Section 2 explains the system modelling followed by the consensus approach in Section 3. The three case studies are carried out in Section 4 to validate the system performances, the followed by conclusion in Section 5.

2. Model of power systems with DoS attacks

In this section, the proposed MBESS model in [29] is analysed with DoS attacks. As shown in Fig. 2, the DoS attacks occur in the communication channels of the communication graph and this would affect the coordination between neighbour agents and, causing a congestion in the network traffic.

2.1. System model with energy storage

The dynamic model of multi agent system which has n number of battery agents can be illustrated as [3],

$$\underbrace{\begin{bmatrix}\dot{\mathcal{E}}_i(t)\\ \dot{\mathcal{P}}_i(t)\end{bmatrix}}_{\dot{x}_i} = \underbrace{\begin{bmatrix}0 & -1/3600\\ 0 & 0\end{bmatrix}}_{A_i}\underbrace{\begin{bmatrix}\mathcal{E}_i(t)\\ \mathcal{P}_i(t)\end{bmatrix}}_{x_i} + \underbrace{\begin{bmatrix}0\\ 1\end{bmatrix}}_{B_i} u_i(t), \tag{1}$$

where, referring to the ith energy storage system, the matrices A_i and B_i represent the system and input properties, respectively. Additionally, $\mathcal{E}_i$ and $\mathcal{P}_i$ correspond to the energy and power characteristics of the ith battery. It is important to note that a scaling factor of $\frac{1}{3600}$ is applied because the battery ratings are originally expressed in kilowatt-hours(Kwh) and kilowatts (Kw) for energy and power, respectively. Consequently, if a battery's initial energy matches its capacity, its energy in per unit (p.u) is equivalent to its SoC.

As seen in Fig. 2, the power balance of the entire system can be represented as,

$$\sum_{i=1}^{n} P_{B,i}(t) = R_l(t) - P_{PV}(t), \tag{2}$$

where $P_{B,i}$ and R_l are power of ith battery storage and DC load demand respectively.

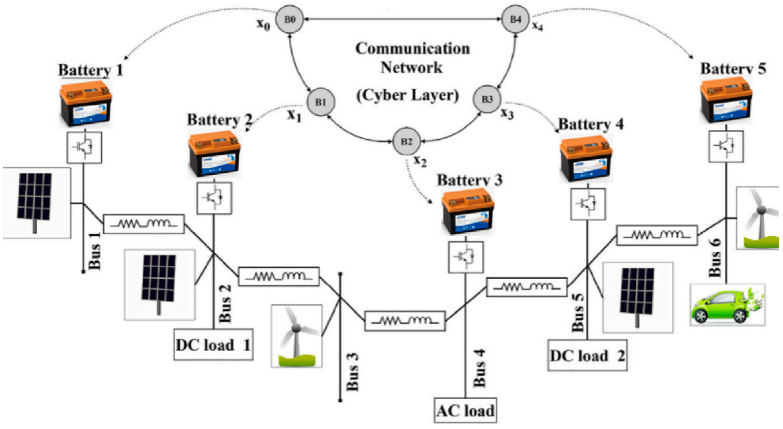


Fig. 1. MBESS with the cyber layer.

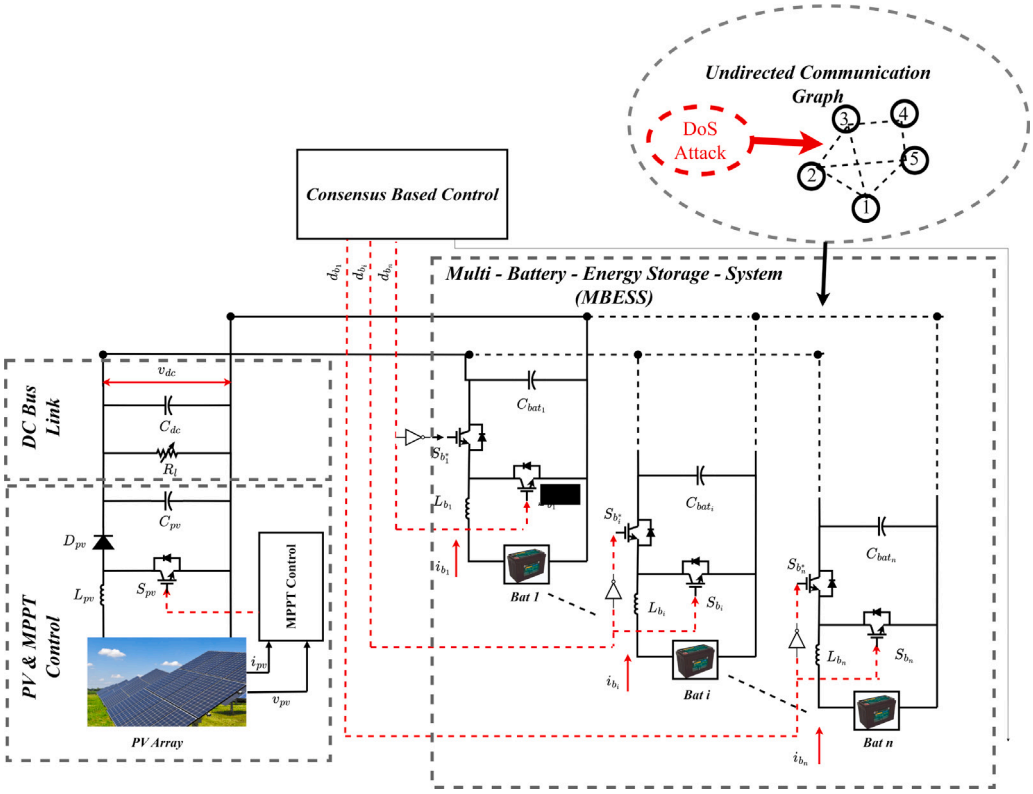


Fig. 2. Overall islanded power system with multiple battery energy storage and DoS attacks on the communication channels.

2.2. Estimation of the state-of-charge (SoC) of BESS

$SoC_i(t)$ represents the SoC of the ith BESS at time t, $SoC_i(0)$ represents the SoC of the ith BESS at time $t = 0$. Also, let C_i and I_{Bat_i} represent the capacity of the ith BESS and ith BESS charging/discharging current, respectively. $SoC_i(t)$ of the ith BESS can be found from conventional coulomb counting as mentioned in [9,30],

$$SoC_i(t) = SoC_i(0) - \frac{1}{C_i}\int I_{Bat_i}\,dt, i = 1, \ldots, n. \tag{3}$$

The result of finding the derivative of the both sides of the expression in (3) is given as $\dot{SoC}_i(t) = -I_{Bat_i}/C_i$. Let V_{Bi} represent the battery's output voltage. Hence, the output discharge/charge power P_{B_i} of the ith BESS can be calculated using the formula $P_{B_i} = V_{Bi} I_{Bat_i}$. As researchers elaborated in [9,30], output battery voltage V_{Bi} for $i = 1, \ldots, n$ remains unchanged throughout a wide range of SoC. Therefore, $\dot{SoC}_i(t)$ is formulated as:

$$\dot{SoC}_i(t) = -\frac{P_{B_i}}{C_i V_{Bi}}, \quad i = 1, \ldots, n. \tag{4}$$

The aim of the MAS controller is presented to achieve power equilibrium across the entire system by interacting with each individual agent, which, in this MAS framework, corresponds to the battery storage units. Simultaneously, the MAS controller ensures that the SoC levels of the battery units remain within a secure operational range. Importantly, this strategy maintains a consistence DC bus link voltage, irrespective of variations in the load demand.

Although a consensus based controller is proposed to generate battery reference $i_{b_{ref\,i}}$ current to each and individual battery storage, the conventional PI controller is used as local controller for each battery current loop. The standard block diagram can be seen in Fig. 3

The constant DC bus voltage is very important aspect for maintaining the stability of DC microgrids. In this research, we have made

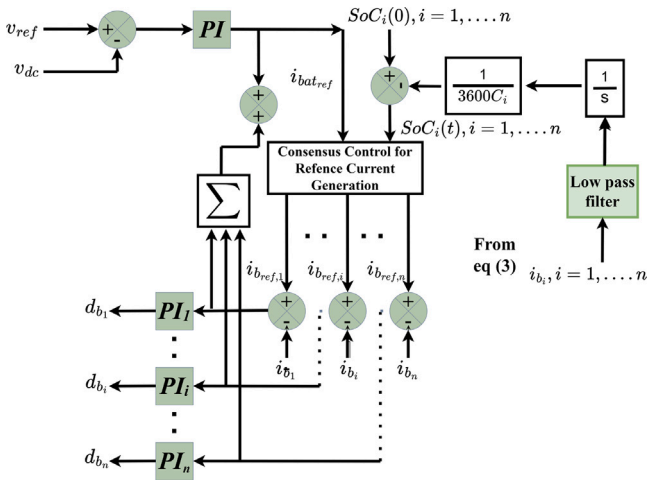


Fig. 3. Local control loop to generate $i_{b_{ref,i}}$.

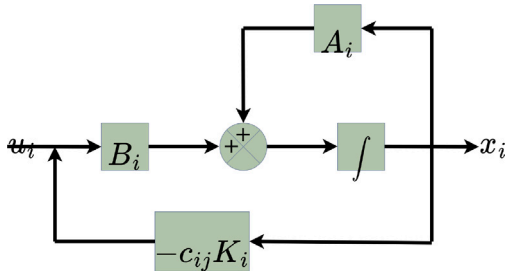


Fig. 4. State-feedback control model of the battery.

our DC bus to regulate at 48 V throughout the experiment. This phenomena can be achieved through the different battery reference current generated via consensus control in the battery control loop. This can be seen in Fig. 3. However, since we have assumed that our SoC of individual BESS is maintained in the safe operating region, we do not need to necessary consider the individual capacity or SoC of the battery. Furthermore, it is noted that, in a practical scenario, having a constant DC bus voltage will enhance better life span for appliances.

The state variable will be updated for the local controller of each of the batteries, as shown in Fig. 4.

2.3. Consensus algorithm

We Consider the MAS with n number of agents. Let the dynamics of the ith agent be described as:

$$\dot{x}_i = A_i x_i + B_i u. \tag{5}$$

In this investigation, we consider a scenario where $x = [x_1, x_2, \ldots x_n]^T$ denote the state variables, and the control input vector $u = [u_1, u_2, \ldots, u_n]^T$ signifies the inputs. Specifically, the state variables pertain to the energy ($\mathcal{E}(t)$) and power ($\mathcal{P}(t)$) of the batteries. The primary goal of the consensus algorithm is to facilitate the exchange of pertinent information among all the decentralised agents. It is essential to highlight that this research assumes the absence of a central controller and assumes perfect communication links with no delays.

The consensus controller, proposed here is given by [31]

$$\begin{aligned} u_i(t) &= c \cdot K \sum_{j=1}^{n} a_{ij}(\omega_j(t) - \omega_i(t)) \\ &= c \cdot K \sum_{j=1}^{n} a_{ij} \begin{bmatrix} \mathcal{E}_j(t) - \mathcal{E}_i(t) \\ \mathcal{P}_j(t) - \mathcal{P}_i(t) \end{bmatrix}, \end{aligned} \tag{6}$$

where the gain $K = R^{-1} B^T P$ and we assume $x_{ij}(t) = \omega_j(t) - \omega_i(t)$.

Similarly, an adaptive controller can be modelled as,

$$\begin{aligned} u_i(t) &= K \sum_{j=1}^{n} c_{ij}(t) \cdot a_{ij}(\omega_j(t) - \omega_i(t)), \\ &= K \sum_{j=1}^{n} c_{ij}(t) \cdot a_{ij} \begin{bmatrix} \mathcal{E}_j(t) - \mathcal{E}_i(t) \\ \mathcal{P}_j(t) - \mathcal{P}_i(t) \end{bmatrix}. \end{aligned} \tag{7}$$

Thus, the derivative of the c_{ij} can be found as,

$$\begin{aligned} \dot{c}_{ij}(t) &= K_{ij} c_{ij}(t) a_{ij} \begin{bmatrix} \mathcal{E}_j(t) - \mathcal{E}_i(t) \\ \mathcal{P}_j(t) - \mathcal{P}_i(t) \end{bmatrix}^{\mathrm{T}} (t) \\ &\Gamma \cdot \begin{bmatrix} \mathcal{E}_j(t) - \mathcal{E}_i(t) \\ \mathcal{P}_j(t) - \mathcal{P}_i(t) \end{bmatrix} - \frac{\mu_1 c_{ij}(t)}{2}, \end{aligned} \tag{8}$$

where $K \in \mathbb{R}^{m \times n}, \Gamma \in \mathbb{R}^{n \times n}$ are gain matrices while $\mu_1 > 0$ represents the attenuation rate as found in [10,32].

2.4. Theoretical approach with DoS attack

A DoS attack, occurs when the adversary obstructs the communication channel, causing disruption in data transmission. Subsequently, the attacker is presumed to engage intermittently, with varying periods, and must cease their actions to replenish energy for the next attack. Let us represent the sequence of DoS attacks as $\{\tilde{\imath}_n\}_{n \in \mathbb{N}}$, where each $\tilde{\imath}_n$ marks the moment when an attack begins. We will define the duration of a single attack as $\tilde{\Delta}_n$, where $\tilde{\Delta}_n$ is always greater than zero, and it is clear that $\tilde{\imath}n + 1 > \tilde{\imath}_n + \tilde{\Delta}_n$. Now, we introduce two sets of time intervals within a given period $[t_1, t_2]$ to differentiate between jammed and normal interactions. We denote these sets as follows:

$\Xi_a(t_1, t_2)$: This set represents the intervals where jammed interactions occur within $[t_1, t_2]$. It is obtained by the intersection of the union of all Dn (attack time intervals) and $[t_1, t_2]$.

$\Xi_s(t_1, t_2)$: In contrast, this set represents the intervals of normal interaction within $[t_1, t_2]$. It is derived by subtracting $\Xi_a(t_1, t_2)$ from $[t_1, t_2]$.

We use $|\Xi_a(t_1, t_2)|$ and $|\Xi_s(t_1, t_2)|$ to denote the respective lengths of $\Xi_a(t_1, t_2)$ and $\Xi_s(t_1, t_2)$.

In order to enhance the analysis of Denial of Service (DoS) attacks, the following standard assumptions can be applied:

Assumption 1 (*Attack Frequency [28]*)**.** When considering time intervals $t_2 > t_1 \geq 0$, we can represent the count of DoS attacks occurring between t_1 and t_2 as $\mathcal{N}a(t_1, t_2)$, and we can establish $\mathcal{F}a(t_1, t_2)$ as a positive value denoting the frequency of DoS attacks during this time frame, which execute,

$$\mathcal{F}_a(t_1, t_2) = \frac{\mathcal{N}_a(t_1, t_2)}{t_2 - t_1}. \tag{9}$$

Assumption 2 (*Attack Duration [28]*)**.** For any $t_2 > t_1 \geq 0$, there exists scalar $T_0 \geq 0$ such that the total DoS attack duration $|\Xi_a(t_1, t_2)|$ satisfies:

$$|\Xi_a(t_1, t_2)| \leq T_0 + \frac{t_2 - t_1}{\tau_a} \tag{10}$$

where $1/\tau_a \in (0, 1)$ signifies the level of DoS attack severity.

Therefore,as mentioned in Assumption 1, it is noted that when considering time intervals $t_2 > t_1 \geq 0$, we can represent the count of DoS attacks occurring between t_1 and t_2 as $\mathcal{N}a(t_1, t_2)$, and we can establish $\mathcal{F}a(t_1, t_2)$ as a positive value denoting the frequency of DoS attacks. Similarly, in Assumption 2, or any $t_2 > t_1 \geq 0$, there exists scalar $T_0 \geq 0$ such that the total DoS attack duration $|\Xi_a(t_1, t_2)|$. Thus, since, where κ^* and Δ^* are positive scalars that will satisfy the Eq. (8) and adaptive law c_{ij} will converge to finite value while satisfying the condition of $0 < \Delta^* \leq t^i_{k+1} - t^i_k$.

3. Control objective and stability analysis

3.1. Control objective

The objective of this paper is to create a fully decentralised control protocol, utilising a MAS as described in (5), even when confronted with DoS attacks, with the goal of attaining an average consensus.

It is presumed that the MAS described in (5) can successfully attain a consensus value even in the presence of DoS attacks, irrespective of the values of i, j, and t within the set of agents

$$\lim_{t\to\infty}\left\|\omega_i(t)-\frac{1}{N}\sum_{j=1}^{N}\omega_j(t)\right\|^2=0=z(t)=\psi_{ij}. \tag{11}$$

The main control goal of this paper is to achieve the consensus value in finite time even in the presence of the DoS attacks. Thus the (5) can be written as,

$$\begin{aligned}\dot{\omega}_i(t)&=A_i\omega_i(t)+B_iu(t)\\&=A_i\omega_i(t)+B_iK_{ij}\sum_{j=1}^{N}c_{ij}(t)a_{ij}\omega_{ij}(t).\end{aligned} \tag{12}$$

Thus, $\psi_{ij}=\omega_i(t)-\frac{1}{N}\sum_{j=1}^{N}\omega_j(t)$ due to $c_{ij}(t)=C_{ji}, a_{ij}=a_{ji}$. This will give the system consensus error as,

$$\dot{\psi}_i=A\psi(t)+BK\sum_{j=1}^{N}c_{ij}(t)\omega_{ij}(t). \tag{13}$$

3.2. Stability analysis

Theorem 3.1. *If the following conditions are met, then the consensus problem in the MAS over an undirected graph, subject to Assumption 1, can be effectively resolved in the presence of DoS attacks using the specified control protocol and adaptive law as mentioned in the (8). The MAS is governed by (5). The consensus control protocol is described by (6) with the choice of $K=-B^{\mathrm{T}}P$. The adaptive law is given by (7) with $\Gamma=-PBB^{\mathrm{T}}P$. The initial values are $c_0>0$ and $\pi_0>0$. Certain positive scalars μ_1, μ_2, σ, k_{ij}, and $\beta_1>0$, along with $\beta_2\in(0,1)$ and $\beta_3>0$, must satisfy the inequality $\beta_1-\left(2-\beta_2\right)\beta_3\geq\mu_1$. Under these conditions, the system defined by (16) is guaranteed to exhibit asymptotic stability, thereby successfully addressing the consensus problem in MAS (5) even when subjected to DoS attacks.*

1. *There exists $P>0$, which can be satisfied as:*

$$PA+A^TP-PBB^TP\leq-\sigma I_n \tag{14}$$

$$\begin{aligned}&PA+A^TP-\mu_2P\leq0\\&\sigma\lambda_{\min}\left(P^{-1}\right)-\lambda_{\max}\left(BB^TP\right)\geq\mu_1.\end{aligned} \tag{15}$$

2. *The following constraints are used to satisfy the DoS attack:*

$$\begin{aligned}\mathcal{F}_a\left(t_0,t\right)&=\frac{\mathcal{N}_a\left(t_0,t\right)}{t-t_0}\leq\frac{\kappa^*}{\left(\mu_1+\mu_2\right)\Delta^*},\\&\tau_a>\frac{\mu_1+\mu_2}{\mu_1-\kappa^*}.\end{aligned} \tag{16}$$

In this context, κ^* and Δ^* represent positive values, with κ^* falling within the range of 0, μ_1, and Δ^* satisfying the condition $0<\Delta^*\leqslant\inf t_{k+1}^i-t_k^i$, where t_0 denotes the initial time. Additionally,it is worth noting that the adaptive law c_{ij} ultimately converges to a finite value.

Proof. To begin, let us examine the scenario in the absence of DoS attacks and establish a Lyapunov-Krasovskii (L-K) functional for (16):

$$V=V_a+V_b, \tag{17}$$

where $V_a=\sum_{i=1}^{N}\psi_i^T(t)P\psi_i(t), V_b=\sum_{i,j=1}^{N}\frac{c_{ij}^2(t)}{2k_{ij}}$.

Define $\psi_{ij}(t)=\psi_i(t)-\psi_j(t)$ and $\omega_{ij}(t)=\omega_i(t)-\omega_j(t)$, then taking the derivation of V_a yields:

$$\begin{aligned}\dot{V}_a=&2\sum_{i=1}^{N}\psi_i^T(t)PA\psi_i(t)\\&+\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\psi_{ij}^T(t)PBK\hat{\omega}_{ij}(t).\end{aligned} \tag{18}$$

Since $\psi_{ij}(t)=\omega_{ij}(t)$ and $\mathcal{E}_i(t)=\hat{\omega}_i(t)-\omega_i(t)$, thus:

$$\begin{aligned}\dot{V}_a=&2\sum_{i=1}^{N}\psi_i^T(t)PA\psi_i(t)\\&-2\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\mathcal{E}_i^T(t)PBK\hat{\omega}_{ij}(t)\\&+2\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\left(\omega_i^T(t)+\mathcal{E}_i^T(t)\right)PBK\hat{\omega}_{ij}(t).\end{aligned} \tag{19}$$

Represent $e_{ij}(t)$ as the difference between $\mathcal{E}_i(t)$ and $\mathcal{E}_j(t)$. Note that:

$$\begin{aligned}&\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\left(\omega_i^T(t)+\mathcal{E}_i^T(t)\right)PBK\left(\omega_{ij}(t)+e_{ij}(t)\right)\\&=\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\omega_i^T(t)PBK\left(\omega_{ij}(t)+2e_{ij}(t)\right)\\&+\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\mathcal{E}_i^T(t)PBKe_{ij}(t)\end{aligned} \tag{20}$$

Assuming K is defined as $K=-B^{\mathrm{T}}P$, we can confirm this by referring to (6) (setting $\epsilon=1$), which states:

$$\begin{aligned}&-2\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\mathcal{E}_i^T(t)PBK\hat{\omega}_{ij}(t)\\&\leq\sum_{i,j=1}^{N}a_{ij}\mathcal{E}_i^T(t)PBB^TP\mathcal{E}_i(t)\\&+\sum_{i,j=1}^{N}c_{ij}^2(t)a_{ij}\hat{\omega}_{ij}^T(t)PBB^TP\hat{\omega}_{ij}(t)\end{aligned} \tag{21}$$

Substitute (20) into (21), we know:

$$\begin{aligned}\dot{V}_a\leq&2\sum_{i=1}^{N}\psi_i^T(t)PA\psi_i(t)\\&+\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\hat{\omega}_i^T(t)PBK\hat{\omega}_{ij}(t)\\&+\sum_{i,j=1}^{N}c_{ij}(t)a_{ij}\omega_i^T(t)PBK\left(\omega_{ij}(t)+2e_{ij}(t)\right)\\&+\sum_{i,j=1}^{N}a_{ij}\mathcal{E}_i^T(t)PBK\left(c_{ij}(t)e_{ij}(t)-\mathcal{E}_i(t)\right)\\&+\sum_{i,j=1}^{N}c_{ij}^2(t)a_{ij}\hat{\omega}_{ij}^T(t)PBB^TP\hat{\omega}_{ij}(t).\end{aligned} \tag{22}$$

If we set γ to 1 and Γ to $-PBB^TP$, and as we calculate the derivative of V_b, we obtain:

$$\begin{aligned}\dot{V}_b=&-\sum_{i,j=1}^{N}c_{ij}^2(t)a_{ij}\hat{\omega}_{ij}^T(t)PBB^TP\hat{\omega}_{ij}(t)\\&-\mu_1\frac{c_{ij}^2(t)}{2k_{ij}}.\end{aligned} \tag{23}$$

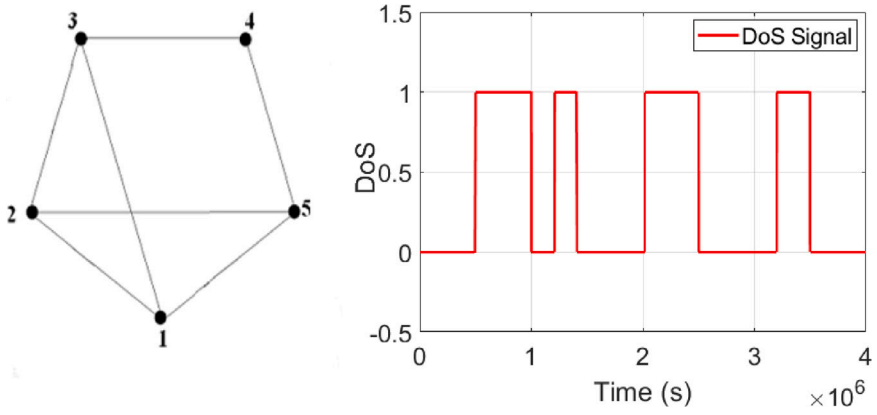
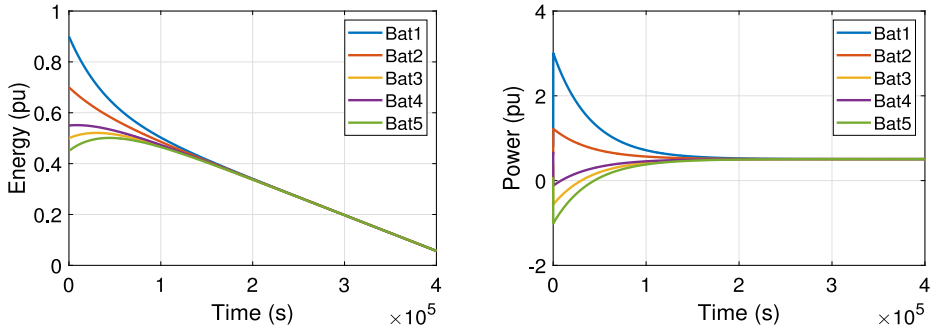


Fig. 5. Communication graph and DoS signal.



(a) (b)

Fig. 6. Case 1: Steady state characteristics with no DoS attacks (a) BESS energy discharge; (b) BESS power discharge.

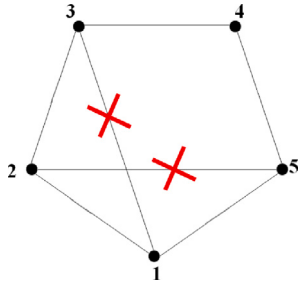


Fig. 7. Case 2: DoS attack on channel 1 – 3 and 2 – 5.

According to Eqs. (14), (16) and $\beta_1 - (2 - \beta_2)\beta_3 \geq \mu_1$, we obtain:

$$\begin{aligned}\dot{V} &\leq -\left[\sigma\lambda_{\min}\left(P^{-1}\right) - \lambda_{\max}\left(BB^T P\right)\right]\sum_{i=1}^{N}\psi_i^T(t)P\psi_i(t)\\ &\leq -\mu_1 V. \end{aligned} \tag{24}$$

Now, let us examine the scenario where DoS attacks are taken into account. Thus, the system's dynamics can be expressed as:

$$\dot{\psi}_i(t) = A\psi_i(t) \quad i = 1, \ldots, N.$$

Construct the same L-K function and compute the derivation of V:

$$\begin{aligned}\dot{V} &= \dot{V}_a + \dot{V}_b\\ &= \sum_{i=1}^{N}\psi_i^T(t)\left(PA + A^T P\right)\psi_i(t) - \mu_1\frac{c_{ij}^2(t)}{2k_{ij}}\\ &\leq \mu_2 V. \end{aligned} \tag{25}$$

Following the analytical process, we merge these two scenarios, one where the multi-agents are affected by DoS attacks and can be represented as,

$$\dot{V}(t) \leq \begin{cases} -\mu_1 V(t) t \in \Xi_s\left(t_0, t\right) \\ \mu_2 V(t) t \in \Xi_a\left(t_0, t\right). \end{cases}$$

Subsequently, using the Lyapunov stability theorem in conjunction with Eqs. (15) and (16), it can be inferred that as time approaches infinity, the function $V(t)$ tends to zero. Consequently, $\psi_i(t)$ converge to zero as well, indicating that the MAS defined by (1), even in the presence of DoS attacks, ultimately achieves average consensus. Furthermore, the adaptive law c_{ij} also converges to a finite value as time tends towards infinity. □

4. Results and discussion

To validate the proposed model shown in Fig. 2, the simulation studies were carried out in Matlab/Simulink environment. This simulation study illustrates 3 different case studies.

In Case 1, The system characteristics are in default conditions, which is standard steady-state mode without any DoS attacks.

In Case 2, the DoS attacks cause an impact on communication channels 2–5 and 1–3, which will result in delayed convergence. However, the stability of the system is still valid in these conditions.

In Case 3, the DoS attacks disrupted the communication between battery 3 – 4 and 4 – 5. This will result in agent 4 being isolated from the information exchanges with other battery agents.

Overall our simulation studies indicate, although the DoS attack signal affect the system's communication channels, the consensus among the agents will occur. This maintain the DC bus voltage V_{dc} at constant level (48 V) while regulate the stability of the systems according to the theoretical analysis explained in previous sections. Fig. 5 illustrates

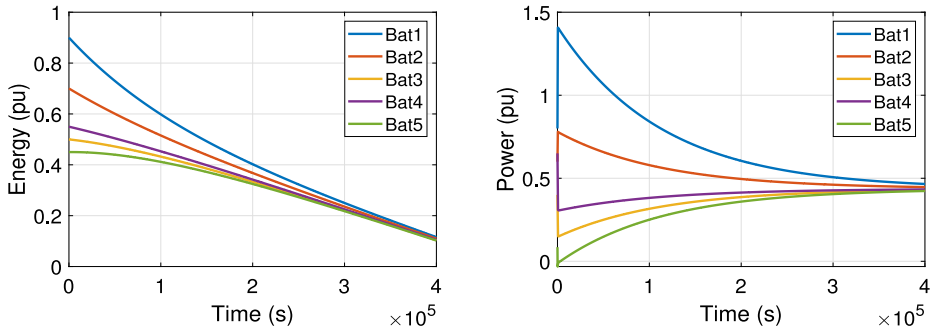


Fig. 8. Case 2: BESS characteristics under DoS attacks on communication links 2–5 and 1–3 (a) BESS energy discharge; (b) BESS power discharge.

Table 1
BESS parameters [29].

BESS i	SoC (%)	C_i (Wh)	V_{Bi} (V)
1	70	1	12
2	65	0.81	11.5
3	60	0.96	10.6
4	55	1.16	11
5	50	0.99	10.75

Table 2
Other parameters [29].

Parameter	*Value*
$V_{dc} = V_{ref}$	48 V
R_l	8–32 Ω
C_{bati}	500 μF
L_{sc}	4 mH
L_{b_i}	3 mH
L_{pv}	3 mH
$i_{b_{i,max}}$	6 A
$C_{dc} = C_{pv}$	1000 μF

that the undirected communication graph is affected by the DoS attack signal. As seen in Fig. 5, the 0 represent the no DoS attack while 1 represents the DoS attack.

Furthermore, the system parameters are displayed in the Tables 1 and 2.

4.1. Case 1: Steady state

In this case, the communication among all channels $BESS_{i,j}$ where i,j = 1,…,5 occurs as normal. This will lead to faster convergence of energy as shown in Fig. 6(a). After 1500 s all agents will consensus to finite value in terms of the energy.

Similarly, power dissipation through all the communication channels are merged to finite value after 1500 s as illustrated in Fig. 6(b).

4.2. Case 2

In this case, DoS attack occurs at Channel 1 – 3 and 2 – 5 as shown in Fig. 7. This will result a delayed coordination among all channels $BESS_{i,j}$, where i, j = 1,…,5. Fig. 8(a) shows that the communication delay results in delayed convergence of energy. Simulation results indicates that, the consensus occurs after 4000 s for all the channels.

Fig. 8(b) shows the power dissipation through all the channels $BESS_{i,j}$ where $i, j = 1, \ldots, 5$. It vividly shows that merging to finite value is delayed compared to steady - state due to the DoS attacks on the communication channels.

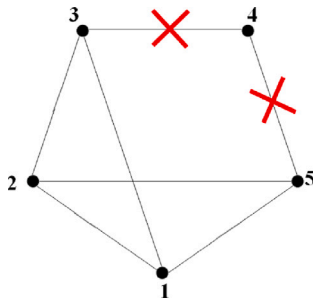


Fig. 9. Case 3: DoS attack on Channel 3 – 4 and 4 – 5e.

4.3. Case 3

In this case, DoS attack occurs at Channel 3 – 4 and 4 – 5 as shown in Fig. 9. This will result in a delayed coordination among all channels $BESS_{i,j}$ where i, j = 1,…,5. Fig. 10(a) shows the communication delay results delayed convergence of energy. Simulation results indicate that, the consensus occurs after 4000 s for all the channels and ith BESS, where $i = 4$ is being isolated from the communication graph.

Similarly, Fig. 10(b) shows the power dissipation through all the channels $BESS_{i,j}$ where i, j = 1,…,5. It shows that ith BESS, where $i = 4$ is not communicating with other channels and isolated from the communication graph. This will result in 4th BESS not merging to a finite value due to the DoS attacks on the communication channels.

The error of the consensus (Z) and its characteristics are shown in Fig. 11(a). As the error approaches the zero, the stability of the system is well maintained. Due to the constraints of the DoS attack, in order to satisfy the (16), $\mathcal{F}_a \leq 0.9$ and $\tau_a = 5$ s are used.

The adaptive law (C_{ij}) is graphically represented in Fig. 11(b). As can be seen, during the attack, when $t \to \infty$, $C_{ij} \to 0$.

Fig. 12(a) shows the DC bus voltage regulation during the DoS attacks. It clearly shows that regardless the DoS attack in the system, the proposed consensus model will maintain the DC bus voltage at a constant value (48 V).

As a result of the DoS attack in the communication channels, it is noted that there is power imbalance in the system. To accommodate this issue, the battery agents change their status to charging or discharging. In Fig. 12(b) depicts that ith battery discharge current at the interval of DoS signal to maintain energy/power equilibrium in the entire system.

4.4. Results validation using RT-LAB

In addition to the simulation studies, the results were validated in real-time using the OP5700 real-time simulator as shown in Fig. 13

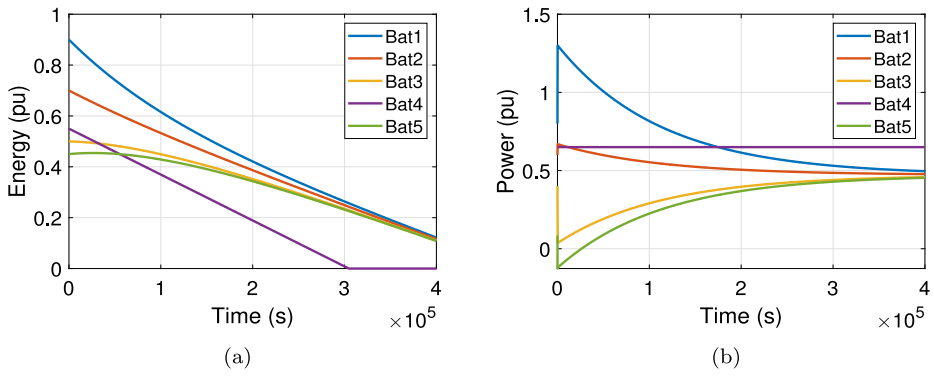


Fig. 10. Case 3: BESS characteristics under DoS attacks on communication links 3–4 and 4–5 (a) BESS energy discharge; (b) BESS power discharge.

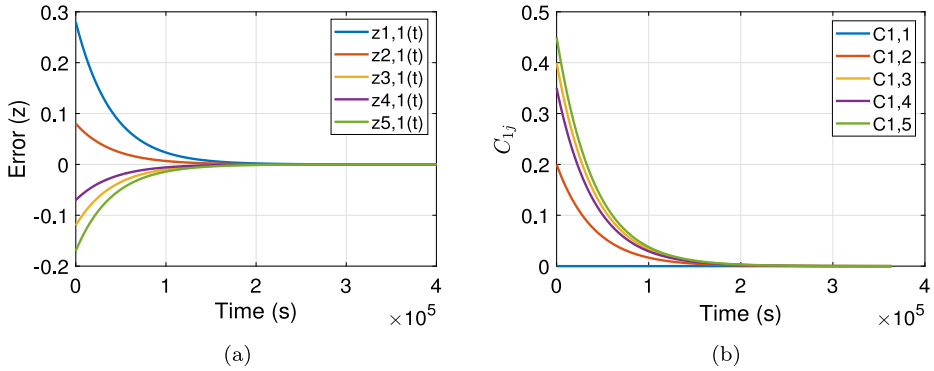


Fig. 11. Special characteristics under DoS attacks during Case 2 and 3 (a) consensus error Z; (b) adaptive parameter C_{ij}.

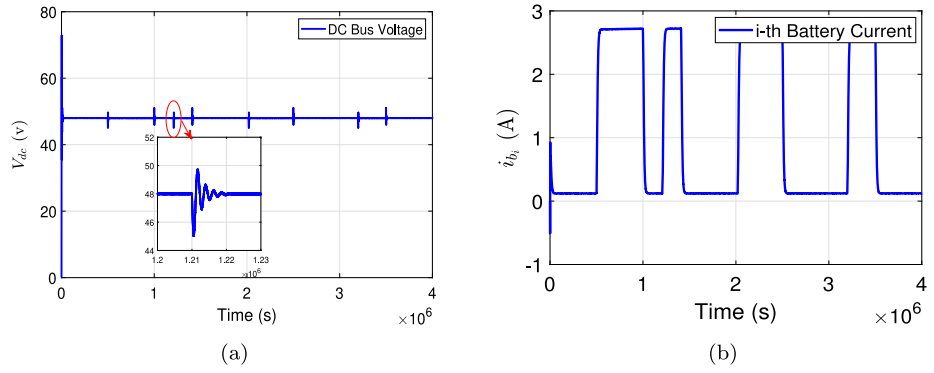


Fig. 12. DC bus characteristics under DoS attacks during Case 2 and 3 (a) DC bus voltage V_{dc}; (b) ith battery current i_{b_i}.

The proposed consensus algorithm regulates DC bus voltage at 48 V regardless during the DoS attacks in communication channels as shown in Fig. 14(a). Furthermore, the change of power of each battery energy storage are shown in per unit in Fig. 14(b) during the DoS attacks as stated in Case 2.

The SoC characteristics of each battery are shown in Figs. 15(a) and 15(b) for Case 2 and Case 3 respectively.

Further discussion of these real-time outcomes will be elaborated in next section.

4.5. Discussion

As seen in above section, simulation results indicate that proposed system will maintain its stability and regulated DC bus voltage at its DC link during the time of DoS attacks while maintaining its thresholds limits.

This is very crucial aspect when it comes to practical scenario. During the modelling of any DC bus, the voltage stability is a must. However, in the case of multi battery system, if there is a high percentage of DoS attacks and this will result in power imbalance in the entire system causing voltage sags. Hence, with the consensus topology, DC bus voltage can be regulate, at a constant value even in the presence of DoS attacks.

Case2 and Case3 indicate the controller's performances during the DoS attack. According to the results in Figs. 8(a) and 8(b) in case 2, the system still converge to a consensus value even though with the presence of the DoS attack while meeting the DoS attacks time in Eq. (16). In Figs. 10(a) and 10(b) of Case 3 shows that the system's performances during the complete failure of a communication link 3–4 and 4–5. As the battery 4 is isolated from the rest of the communication graph, it fails to meet the convergence analysis as the others. However, rest of the BESS still meets the system's primary requirements while achieving the consensus.

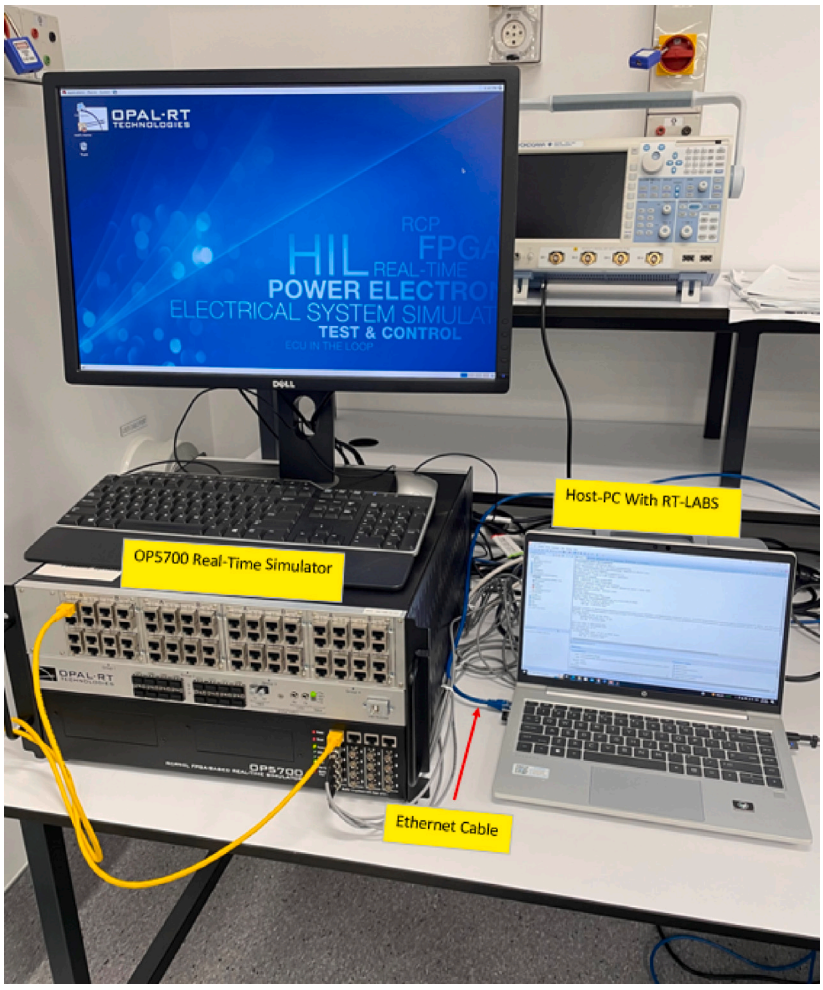


Fig. 13. Results validation using real-time simulator OP5700.

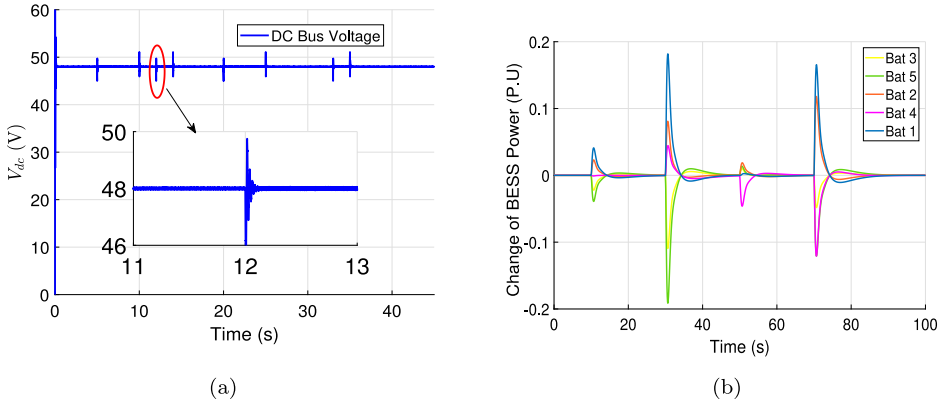


Fig. 14. DC bus characteristics under DoS attacks during Case 2 and 3. (a) DC bus characteristics in real-time Under DoS attacks during Case2 and 3 (V_{dc}). (b) change of power of BESS in real-time under DoS attacks ($P.U$).

Furthermore, it is noted that SoC of the each energy storage has achieved its consensus in finite time during the DoS attacks. As shown in Fig. 14(b), the SoC convergence is achieved during the DoS attacks in the communication channels mentioned in Case 2. Fig. 14(b) illustrates the SoC convergence as per DoS attacks in Case 3. We have noted that SoC of the BESS 4 has moved out of consensus due to the communication failure at channel 4 as shown in Fig. 9. However, rest of the multi energy storage has reached their consensus value as per the proposed method.

5. Conclusion

This paper addresses the issue of how DoS attacks in the communication channels of multi battery energy storage system can impact the dynamic behaviour. The proposed consensus based topology analyse that the effects of DoS attacks can be stabilised. The MATLAB simulation and OPAL-RT real-time simulator studies validate the proposed system with different case studies. The study identified that, the proposed system will be stable and converged to the consensus value in

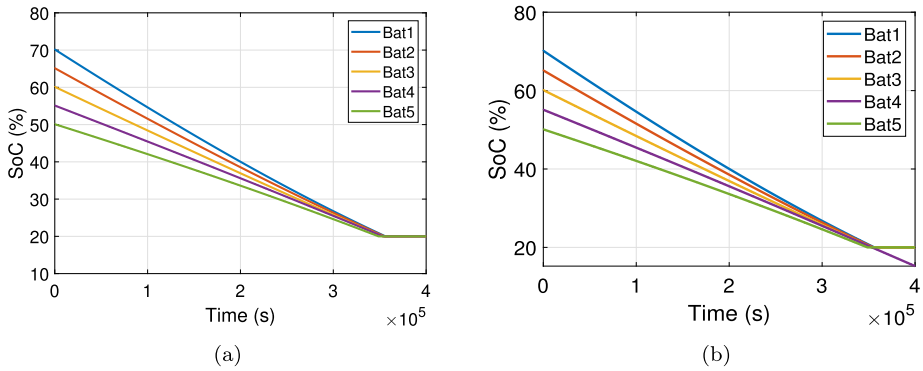


Fig. 15. SoC Characteristics Under DoS attacks during Case 2. (a) SoC Characteristics in real-time Under DoS attacks during Case 3 (V_{dc}). (b) SoC Characteristics of BESS in real-time Under DoS attacks ($P.U$).

finite time during the DoS attack. Furthermore, it is also noted that, the DC bus voltage remains constant throughout all the case studies. Therefore, the proposed model has more benefits in the modern power system, even with persistent cyber attacks.

CRediT authorship contribution statement

Don Gamage: Writing – review & editing, Writing – original draft, Validation, Software, Resources, Project administration, Methodology, Investigation, Formal analysis. **Chathura Wanigasekara:** Validation, Formal analysis. **Abhisek Ukil:** Supervision. **Akshya Swain:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] D.D. Sharma, S. Singh, J. Lin, Multi-agent based distributed control of distributed energy storages using load data, J. Energy Storage 5 (2016) 134–145.
[2] M. Zadehbagheri, V. Nazerian, M.J. Kiani, Charging and discharging of PHEVs in smart grids with ICA and TLBO algorithms with the approach of simultaneously reducing network peak load and distribution costs, J. Energy Storage 72 (2023) 108577.
[3] D. Gamage, X. Zhang, A. Ukil, C. Wanigasekara, A. Swain, Distributed coordinated consensus control for multi-energy storage of DC microgrid, in: 2021 IEEE Power Energy Society General Meeting, PESGM, 2021, pp. 1–5.
[4] H. Alsharif, M. Jalili, K.N. Hasan, An adaptive charge control strategy for participation of neighbourhood battery energy storage systems in frequency stability, J. Energy Storage 67 (2023) 107630.
[5] H. Pota, Control for microgrids with inverter connected renewable energy resources, in: IEEE PES General Meeting, Washington DC, 27-31 july 2014, no. July, 2014, pp. 1–2.
[6] K. El Mezdi, A. El Magri, A. Watil, I. El Myasse, L. Bahatti, R. Lajouad, H. Ouabi, Nonlinear control design and stability analysis of hybrid grid-connected photovoltaic-battery energy storage system with ANN-MPPT method, J. Energy Storage 72 (2023) 108747.
[7] M.E. Hassanzadeh, M. Nayeripour, S. Hasanvand, E. Waffenschmidt, Intelligent fuzzy control strategy for battery energy storage system considering frequency support, SoC management, and C-rate protection, J. Energy Storage 52 (2022) 104851.
[8] A.M. Taher, H.M. Hasanien, S.H.A. Aleem, M. Tostado-Véliz, M. Ćalasan, R.A. Turky, F. Jurado, Optimal model predictive control of energy storage devices for frequency stability of modern power systems, J. Energy Storage 57 (2023) 106310.
[9] U. Manandhar, A. Ukil, G. Beng, N. Tummuru, S. Kollimalla, B. Wang, K. Chaudhari, Energy management and control for grid connected hybrid energy storage system under different operating modes, IEEE Trans. Smart Grid 3053 (c) (2017) 1–11.
[10] S. Lakshminarayana, A. Kammoun, M. Debbah, H.V. Poor, Data-driven false data injection attacks against power grids: A random matrix approach, IEEE Trans. Smart Grid 12 (1) (2020) 635–646.
[11] D. Gamage, X. Zhang, A. Ukil, Fuzzy logic controller for efficient energy management of a PV system with HESS, in: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2018, pp. 3556–3561.
[12] X. Zhang, D. Gamage, A. Ukil, Energy management of a dual hybrid energy storage system of PV microgrids in grid-connected mode based on adaptive PQ control, in: 2019 IEEE Power & Energy Society General Meeting, PESGM, IEEE, 2019, pp. 1–5.
[13] D. Gamage, X. Zhang, A. Ukil, C. Wanigasekara, A. Swain, Design of ANFIS Controller for a DC Microgrid, in: 2020 3rd International Conference on Energy, Power and Environment: Towards Clean Energy Technologies, 2021, pp. 1–6.
[14] N. Chettibi, A. Mellit, G. Sulligoi, A.M. Pavan, Adaptive neural network-based control of a hybrid AC/DC microgrid, IEEE Trans. Smart Grid (2016).
[15] X. Li, G. Geng, Q. Jiang, Y. Zhao, T. Wu, F. Ma, Consensus-based multi-converter power allocation strategy in battery energy storage system, J. Energy Storage 60 (2023) 106623.
[16] X. Li, G. Geng, Q. Jiang, Y. Zhao, T. Wu, F. Ma, Consensus-based multi-converter power allocation strategy in battery energy storage system, J. Energy Storage 60 (2023) 106623.
[17] C. Wanigasekara, L. Zhang, A. Swain, S.K. Nguang, Delta-modulator-based quantised state feedback controller for T-S fuzzy networked systems, Int. J. Fuzzy Syst. 23 (3) (2021) 642–656.
[18] J. Khazaei, D.H. Nguyen, Multi-agent consensus design for heterogeneous energy storage devices with droop control in smart grids, IEEE Trans. Smart Grid 10 (2) (2017) 1395–1404.
[19] D.H. Nguyen, J. Khazaei, Multiagent time-delayed fast consensus design for distributed battery energy storage systems, IEEE Trans. Sustain. Energy 9 (3) (2017) 1397–1406.
[20] Y. Xu, M. Fang, Z.-G. Wu, Y.-J. Pan, M. Chadli, T. Huang, Input-based event-triggering consensus of multiagent systems under denial-of-service attacks, IEEE Trans. Syst. Man Cybern. Syst. 50 (4) (2018) 1455–1464.
[21] X. Li, K.W. Hedman, Enhancing power system cyber-security with systematic two-stage detection strategy, IEEE Trans. Power Syst. 35 (2) (2019) 1549–1561.
[22] L. Ding, Q.-L. Han, B. Ning, D. Yue, Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks, IEEE Trans. Ind. Inform. 16 (7) (2019) 4909–4919.
[23] C. Wanigasekara, A. Swain, D. Almakhles, L. Zhou, Design of Delta-Sigma Based PID Controller for Networked Wind Energy Conversion Systems, IEEE Trans. Ind. Appl. 58 (1) (2022).
[24] Q. Sun, B. Wang, X. Feng, S. Hu, Small-signal stability and robustness analysis for microgrids under time-constrained DoS attacks and a mitigation adaptive secondary control method, Sci. China Inf. Sci. 65 (6) (2022) 162202.
[25] P. Mercier, R. Cherkaoui, A. Oudalov, Optimizing a battery energy storage system for frequency control application in an isolated power system, IEEE Trans. Power Syst. 24 (3) (2009) 1469–1477.
[26] H. Liang, H. Hua, Y. Qin, M. Ye, S. Zhang, J. Cao, Stochastic optimal energy storage management for energy routers via compressive sensing, IEEE Trans. Ind. Inform. 18 (4) (2021) 2192–2202.
[27] B.D. Olaszi, J. Ladanyi, Comparison of different discharge strategies of grid-connected residential PV systems with energy storage in perspective of optimal battery energy storage system sizing, Renew. Sustain. Energy Rev. 75 (2017) 710–718.

[28] T.K. Chau, S.S. Yu, T. Fernando, H.H.-C. Iu, Demand-side regulation provision from industrial loads integrated with solar PV panels and energy storage system for ancillary services, IEEE Trans. Ind. Inform. 14 (11) (2017) 5038–5049.
[29] D. Gamage, X. Zhang, A. Ukil, C. Wanigasekara, A. Swain, Load frequency control with consensus based multi-energy storage system, in: 2022 7th IEEE Workshop on the Electronic Grid, EGRID, IEEE, 2022, pp. 1–5.
[30] L. Roin, K. Therani, Y. Manjili, M. Jamshidi, Microgrid energy management system using fuzzy logic control, in: 2014 World Automation Congress, WAC, 2014, pp. 462–467.
[31] A. Bidram, A. Davoudi, F.L. Lewis, J.M. Guerrero, Distributed cooperative secondary control of microgrids using feedback linearization, IEEE Trans. Power Syst. 28 (3) (2013) 3462–3470.
[32] Y. Gong, B. Zhang, M. Xiong, Fully distributed dynamic event-triggered consensus control for multi-agent systems under dos attacks, in: 2021 China Automation Congress, CAC, IEEE, 2021, pp. 2698–2703.