Adversarial Attacks on Battery Energy Storage Systems Using Physics-Based Models in PyBaMM

Alaa Selim*, Harrison Faure*, Huadong Mo†, Hemanshu Pota*, Daoyi Dong‡

***Abstract*—This study explores the vulnerabilities of Battery Energy Storage Systems (BESS) to adversarial attacks using the Python-based Battery Mathematical Modeling framework and the Doyle-Fuller-Newman (DFN) model. Our work focuses on simulating targeted attacks on critical battery signals—current, voltage, and temperature—across both single and multiple time windows. By introducing noise with varying amplitudes and spike probabilities, we analyze how these disturbances affect the terminal voltage, revealing specific weaknesses in BESS operation. What sets this work apart is its emphasis on simulating coordinated attacks that occur at different time intervals, helping us to understand both short-term and extended disruptions in BESS performance. The study also provides insight into the design of effective defenses that can respond to these attacks in real time. Our findings aim to contribute to a better understanding of how to protect BESS in modern energy systems, ensuring their reliability and stability under potential cyber threats.**

I. Introduction

Modern energy infrastructure relies heavily on Battery Energy Storage Systems (BESS) for renewable energy integration, stabilising grids, and powering vehicles, securing them from cyber-attacks becomes increasingly important. However, studying their vulnerabilities is challenging due to the lack of available models and datasets that reflect battery behavior under adversarial conditions. Most datasets focus on conventional applications, contain clean unlabelled data or are proprietary. This gap limits understanding of how BESS respond to malicious attacks and hinders the development of effective security measures for BESS.

Batteries rely on key metrics such as State of Charge (SoC) and State of Health (SoH) to convey internal dynamics. However, these metrics are not adequately represented in the available datasets [1]–[3]. The traditional methods and models referring to conventional models for modelling battery behaviour mainly Equivalent Circuit Models (ECM's) struggle to accurately simulate the non-linear behavior that batteries exhibit under adversarial attack [4]. To address this, Python Battery Mathematical Modeling (PyBaMM), library, and model are used which are indeed a physics-based modeling platform aimed specifically for modelling lithium-ion batteries. The Doyle-Fuller-Newman (DFN) model [5] is also employed, which is a lithium-ion battery model that captures the intricate processes occurring in lithium-ion batteries, including lithium-ion diffusion, electrolyte dynamics, and electrode potentials. Using this model allows for the exploration of how adversarial attacks disrupt these interactions.

The battery management system (BMS) uses the voltage as a parameter that provides critical information about the battery power output and charge level. Without applying current Open Circuit Voltage (OCV) is used to diagnose potential issues as a key metric and is directly related to SoC. Adversarial attacks that attempt voltage manipulation, such as voltage spoofing, can result in inaccurate SoC readings leading to incorrect charge and discharge commands [6]. This could potentially overcharge the battery and cause thermal failure or degradation of battery health, affecting battery life and posing a safety risk [7]. The charge and discharge process of the battery is directly affected by current, as it controls the rate of electrochemical reactions within the battery. Conducting adversarial attacks against the current readings can impact both SoC and State of Health (SoH) estimations resulting in possible overcharging or undercharging. Both of these effects can accelerate battery degradation and lead to potential safety concerns within BMS [8]. These incorrect values can also cause premature degradation and excessive heating, which can lead to early battery failure [9]. Temperature affects the reaction kinetics, stability, and battery capacity of the BMS and is a crucial parameter to ensure safe and efficient operations. Performing attacks on the target temperature sensors can cause incorrect readings, leading to poor temperature control and affecting the electrochemical performance of the battery [6]. This may create safety risks from non-uniform heating, degradation of battery components, and thermal runaway which can all lead to potential battery failure or overheating [8]. The internal resistance of the battery is partially determined by the solid electrolyte interphase (SEI) resistance, which is a critical factor in determining the long-term stability. Tampering with the SEI resistance may reduce battery efficiency and, therefore, adversarial attacks targeting this parameter may cause the BMS to misinterpret battery health [7]. Having incorrect SEI readings can lead to improper battery usage, unsafe operations, and premature failure due to incorrect charging/discharging cycles [8].

The reaction rates at the electrode-electrolyte interface are governed, but the Butler-Volmer equations are sensitive to current and temperature fluctuations. If current density can be manipulated this can lead to undercharging or overcharging due to incorrect predictions for energy delivery, and if so this may degrade the batteries electrodes. Accelerated degradation will result in loss of battery capacity and reduced operational efficiency [10].

Electrolyte Concentration controlling ion transport between electrodes is an essential component of BMS and the concentration of lithium ions within the electrolyte is a critical component of this. Attacking this parameter through sensor spoofing or perturbing the charge/discharge cycle can lead to a non-uniform charge distribution [11]. This non-uniform distribution can cause lithium plating or capacity loss, which leads to large reductions in battery lifespan and operational efficiency [8].

The DFN model provides a detailed and precise representation of battery behavior, but also highlights vulnerabilities that can be exploited by cyber-attacks such as current or voltage manipulation [4]. Since physics-based models are based on assumptions about operating conditions, they are sensitive to small changes in the current, temperature, and internal resistance parameters. Adversarial attacks exploit these sensitivities by introducing strategically designed but minor perturbations that can result in large deviations in behavior [12]. For example, manipulating the current input can lead to incorrect SoC estimates, accelerating battery degradation and causing voltage collapse [13].

Adversarial attacks can target multiple BESS and their parameters, increasing the impact of individual attacks, which makes them a major concern. By simultaneously exploiting vulnerabilities such as current perturbations, voltage spoofing, and temperature manipulation [14], [15], attackers create a compounding effect that destabilizes the system. This can lead to incorrect SoC and

*School of Engineering and Technology, University of New South Wales, Canberra, Australia. e-mails: a.selim@unsw.edu.au, h.pota@unsw.edu.au

†School of Systems and Computing, University of New South Wales, Canberra, Australia. e-mail: huadong.mo@unsw.edu.au

‡CIICADA Lab, School of Engineering, Australian National University, ACT, Australia. e-mail: daoyi.dong@anu.edu.au

SoH predictions, disrupting energy management and accelerating battery degradation, resulting in system-wide failures [16]. Coordinated attacks of this nature are challenging to detect and mitigate, posing a sophisticated threat to battery energy storage systems.

Adversarial attacks can exploit the interdependence between multiple battery parameters in combined attacks. For example, manipulating temperature and current together can cause overheating, degrading internal resistance, and accelerating wear. On top of this, voltage spoofing further destabilizes the system by triggering incorrect charging or discharging commands. Traditional physics-based models such as ECM struggle to account for these interactions, as they are traditionally designed to model under stable conditions, leaving them vulnerable to complex coordinated attacks that leverage these interdependencies [15], [17].

The motivation for this research arises from the increasing reliance on BESS in critical infrastructure such as renewable energy grids, electric vehicle networks, and smart grid operations, along with a lack of research on their vulnerabilities to adversarial attacks. Current research focuses on improving control under normal operational conditions, focusing on battery management. However, there is a significant gap in understanding how adversarial attacks can exploit these systems. The rise of machine learning (ML)-based models for SoC and SoH prediction adds new attack surfaces, as these models are vulnerable to adversarial examples and poisoning attacks [18]. Furthermore, the interaction between ML vulnerabilities and physics-based vulnerabilities in a combined attack is underexplored. Therefore, this research aims to address that gap and reveal how such attacks compromise the integrity of BESS..

BESS that incorporate ML models are vulnerable to adversarial attacks that inject malicious data,corrupting the decision-making process, and leading to incorrect predictions. [19]–[21]. Even small input perturbations can lead to significant prediction errors, as noted in prior studies. However, limited research addresses how these attacks interact with physics-based models such as PyBaMM [22], [23]. Understanding this interaction is crucial for developing defenses that account for vulnerabilities in both ML-based and physics-based frameworks.

This paper addresses the literature gap by simulating adversarial attacks on the DFN model to explore how cyber attacks such as current perturbations, voltage spoofing, and temperature manipulation affect key battery metrics such as SoC and SoH. The goal is to develop a framework to defend BESS against these attacks, mitigating the risks of system-wide failures, unexpected battery degradation, and increased operational costs [20]. In summary, this work aims to enable more robust defenses for critical BESS operations.

The paper is organised as follows: Section II introduces the system model that uses PyBaMM to implement the DFN model. Section III details attack formation and the simulation of adversarial attacks on the Battery Management System (BMS). Section IV outlines the methodology, explaining how the attacks were conducted, and the solution-oriented approach. Section V presents numerical results, graphs, sensitivity analysis, and discusses the implications for BESS security. Section VI provides the conclusion, followed by future research directions in Section VII.

II. System Modeling

The DFN model is a mathematical model for simulating the electrochemical behavior of lithium-ion batteries. It accounts for complex interactions, such as lithium-ion diffusion, electrolyte dynamics, and electrode potentials. The model is crucial for accurately predicting battery parameters such as SoC and SoH, which will be assessed under adversarial attack conditions.

The model is governed by a set of partial differential equations (PDEs) that describe the transport and reaction processes within the solid and electrolyte phases of the battery. These equations are derived from the theory of porous electrodes and concentrated solutions and include variables such as potential distribution, lithium concentration, and current density. The governing equations for the DFN model are as follows:

- **Solid-phase lithium-ion concentration** c_s:
$$\frac{\partial c_s}{\partial t} = D_s \frac{1}{r^2} \frac{\partial}{\partial r} \left(r^2 \frac{\partial c_s}{\partial r} \right) \tag{1}$$
This equation governs the diffusion of lithium ions within the solid particles of the electrode. An adversarial attack that manipulates the current could alter the lithium concentration profile, leading to inaccurate SoC predictions by inducing non-uniform diffusion.
- **Electrolyte-phase lithium-ion concentration** c_e:
$$\epsilon_e \frac{\partial c_e}{\partial t} = \frac{\partial}{\partial x} \left(D_e \epsilon_e^p \frac{\partial c_e}{\partial x} \right) + \frac{3(1-t^+)}{R_s} j_n \tag{2}$$
This equation describes lithium-ion transport in the electrolyte phase. Perturbations in temperature or current could disrupt electrolyte transport, leading to erroneous SoH and SoC predictions by altering ion distribution.
- **Solid-phase potential** ϕ_s:
$$\frac{\partial}{\partial x} \left(\sigma \epsilon_s \frac{\partial \phi_s}{\partial x} \right) = \frac{3\epsilon_s F}{R_s} j_n \tag{3}$$
The solid-phase potential is related to current flow through the electrode. An adversarial current attack could distort this potential, leading to unstable control and misjudgments of the battery's electrochemical state.
- **Electrolyte-phase potential** ϕ_e:
$$\frac{\partial}{\partial x} \left(\kappa \epsilon_e \frac{\partial \phi_e}{\partial x} + \kappa \epsilon_e \nu \frac{2RT}{F} \frac{\partial \ln c_e}{\partial x} \right) = -\frac{3\epsilon_s F}{R_s} j_n \tag{4}$$
This equation governs the electrolyte potential. A temperature perturbation can alter the electrolyte potential, impacting the overall voltage response of the battery. An attack targeting this phase could induce significant voltage deviations.
- **Butler-Volmer kinetics** j_n:
$$j_n = \frac{i_0}{F} \left(\exp\left(\frac{\alpha_a F \eta}{RT} \right) - \exp\left(-\frac{\alpha_c F \eta}{RT} \right) \right) \tag{5}$$
The Butler-Volmer equation describes the current density at the electrode-electrolyte interface. Attacks that manipulate current or temperature can significantly affect the reaction kinetics, leading to misjudgments in battery performance.
- **Exchange current density** i_0:
$$i_0 = k_0 c_e^{\alpha_a} (c_{s,\max} - c_s)^{\alpha_a} c_s^{\alpha_c} \tag{6}$$
The exchange current density depends on both the solid and electrolyte-phase concentrations. A current perturbation could lead to decreased exchange current density, resulting in incorrect SoH assessments.
- **Electrode overpotential** η:
$$\eta = \phi_s - \phi_e - U \tag{7}$$
The overpotential drives the electrochemical reaction. Perturbing the current or SEI resistance during an attack directly affects the overpotential, causing incorrect predictions of the battery's health or charge state.
- **Battery terminal voltage** $V(t)$:
$$V(t) = \phi_s(L,t) - \phi_s(0,t) - R_f \frac{i_{\text{app}}(t)}{A_{\text{surf}}} \tag{8}$$
The terminal voltage is a critical output that measures battery health and performance. An adversarial attack manipulating the current, temperature, or SEI resistance could induce deviations in terminal voltage, leading to unsafe or suboptimal battery operation.

Adversarial perturbations, such as current manipulation, temperature variations, and SEI resistance alterations, introduce nonlinear behaviors that disrupt of SoC and SoH estimates. These perturbations affect the internal states of the battery as governed by the aforementioned equations, providing potential opportunities for an attacker to disrupt battery performance, induce unsafe conditions, or degrade battery management systems. It is essential to validate the DFN model against experimental data to ensure accuracy under both normal and adversarial conditions. Proper calibration of

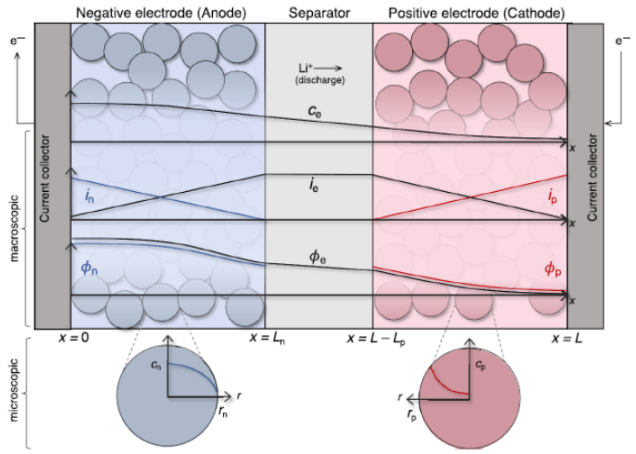

Fig. 1: DFN cell geometry detailing the macroscopic and microscopic coordinate systems and domains for the variables. Represented is a discharge scenario with current density (i_e and i_p), lithium-ion concentration (c_e), and potential distribution (ϕ_n and ϕ_p) for both phases [23].

model parameters, such as reaction rates and transport properties, ensures that the model can predict battery behavior even when subjected to adversarial perturbations. This validation also helps identify vulnerabilities, as models that perform well under normal conditions may fail when subjected to adversarial attacks.

The DFN model offers a robust platform for simulating lithium-ion battery behavior, particularly in scenarios where adversarial attacks are introduced. Understanding how each equation responds to external perturbations allows for the identification of system vulnerabilities and the development of more resilient monitoring and control strategies.

III. Adversarial Attack Formulation

This study formulates adversarial attacks on BBESS by introducing perturbations to three key parameters: applied current, ambient temperature, and SEI (Solid Electrolyte Interphase) resistance. The adversarial attacks target all these parameters simultaneously and can be applied over either a **single-window** or **multiple-window** function of time. The defined attack windows are represented by intervals $t_{s_i} \leq t \leq t_{e_i}$, where t_{s_i} and t_{e_i} denote the start and end times of attack window i, respectively. The perturbations within each attack window consist of two components: a gradual variation that smoothly alters the parameter over time, and sudden spikes that represent abrupt changes. This combined approach allows for a comprehensive simulation of both sustained and transient disturbances in BESS behavior.

For each attack signal, the adversarial perturbation is defined as a combination of gradual changes and spikes. Specifically, the perturbed signal $X_{\text{adv}}(t)$ (where X stands for current, temperature, or SEI resistance) is given by:

$$X_{\text{adv}}(t) = X_{\text{base}} + \sum_{i=1}^{N} \left[\Delta X_i(t) + S_{X,i}(t)\right], \tag{9}$$

where X_{base} is the nominal value of the signal, and N is the total number of attack windows. The term $\Delta X_i(t)$ represents the gradual perturbation in window i, while $S_{X,i}(t)$ denotes the spikes that occur within window i. This formulation ensures that the perturbations are active only within the specified windows, allowing for a flexible representation of both single-window and multi-window attack scenarios.

The gradual perturbation, $\Delta X_i(t)$, within each attack window i is modeled to increase smoothly from the baseline value. It is defined as:

$$\Delta X_i(t) = \gamma_i(t)\left(X_{\text{max},\,i} - X_{\text{base}}\right), \tag{10}$$

where $X_{\text{max},\,i}$ is the maximum allowed increase for the signal $X(t)$ within window i. The transition function $\gamma_i(t)$ governs the activation of the perturbation within each window and is expressed as:

$$\gamma_i(t) = \frac{1}{2}\left[1 + \tanh\left(\frac{t - t_{s_i}}{\tau}\right)\right] \cdot \frac{1}{2}\left[1 + \tanh\left(\frac{t_{e_i} - t}{\tau}\right)\right], \tag{11}$$

where τ is a time constant controlling the smoothness of the perturbation's onset and offset. This function ensures that the gradual increase in the parameter begins smoothly at the start of the attack window, peaks at the maximum defined value, and returns to baseline as the window ends. The formulation applies uniformly across all target signals—current, temperature, and SEI resistance—within each attack window, maintaining a consistent attack strategy for each parameter.

The spike component, $S_{X,i}(t)$, introduces sudden, high-amplitude deviations in each attack signal during window i. It is formulated as:

$$S_{X,i}(t) = \gamma_i(t) \cdot \mathbf{1}_{\{p_i(t) < P_{\text{spike}}\}} \cdot \min\left(\sigma_{X,i},\, \sigma_{X,\text{max}}\right), \tag{12}$$

where $\mathbf{1}_{\{p_i(t) < P_{\text{spike}}\}}$ is an indicator function that triggers spikes with a probability P_{spike} during window i. The term $\sigma_{X,i}$ represents the spike amplitude for signal $X(t)$ in window i, and is bounded by $\sigma_{X,\text{max}}$ to ensure that the spikes remain within realistic limits. The inclusion of this spike component models rapid, transient disturbances that occur alongside the gradual perturbations, making the attack representation more realistic and capturing both sustained and transient vulnerabilities in BESS operation.

The overall objective of the adversarial attack is to maximize the deviation in terminal voltage, $\Delta V(t)$, defined as:

$$\Delta V(t) = \left|V_{\text{adv}}(t) - V_{\text{nom}}(t)\right|, \tag{13}$$

where $V_{\text{adv}}(t)$ is the terminal voltage under adversarial conditions and $V_{\text{nom}}(t)$ is the nominal terminal voltage. The attack parameters, $\boldsymbol{\theta} = (X_{\text{max},\,i}, \sigma_{X,i})$, are optimized to maximize $\Delta V(t)$ across all attack windows i, ensuring that the perturbations produce the greatest possible deviation while remaining within feasible bounds.

The optimization is subject to realistic constraints on the perturbation parameters. The gradual perturbation amplitude is bounded by $0 \leq \Delta X_i(t) \leq \Delta X_{\text{max}}$, ensuring that the increase does not exceed the specified maximum for each signal. Similarly, the spike amplitude is constrained by $0 \leq \sigma_{X,i} \leq \sigma_{X,\text{max}}$, maintaining the spikes within practical limits. The optimization is carried out using the L-BFGS-B algorithm [24], a bound-constrained optimization method that allows for efficient exploration of the parameter space while adhering to the specified limits. This rigorous formulation applies uniformly to all attack signals—current, temperature, and SEI resistance—across both single-window and multiple-window scenarios, providing a comprehensive and realistic assessment of BESS vulnerabilities under adversarial conditions.

IV. Numerical Results

A. Case Studies

This study simulates adversarial attacks on a lithium-ion battery model using the CasadiSolver [25] from PyBaMM. The solver is configured to ensure stability, with a maximum of 50,000 steps, a relative tolerance of 1×10^{-6}, an absolute tolerance of 1×10^{-8}, and a maximum time step of 0.01 seconds. The attacks introduce Gaussian noise to the current, temperature, and SEI thickness parameters. The analysis evaluates the battery's terminal voltage under varying noise levels, focusing on two distinct scenarios: a single attack window and multiple attack windows.

1) *Case 1: Combined Attack - Single Window*

In this case, a combined adversarial attack is implemented within a single time window from 150 to 151 seconds. The noise levels tested are 0.01, 0.1, 0.5, and 1 (in appropriate units), with a spike probability of 0.01 and a spike factor of 100, generating occasional high spikes during the attack period. The base values for adversarial functions include a constant discharge current of 3 A, a nominal temperature of 298.15 K (25°C), and an initial SEI thickness based on the model's default parameters. The impact is analyzed by comparing terminal voltage responses under varying noise amplitudes.

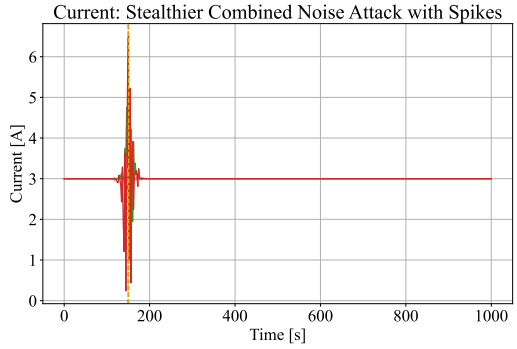

Fig. 2: Single Window — Current Noise attack

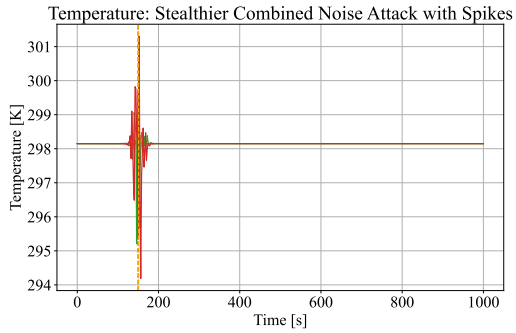

Fig. 3: Single Window — Temperature Noise attack

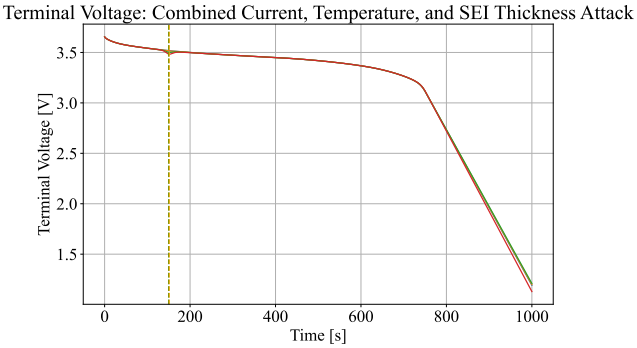

Fig. 4: Single-Window — Terminal Voltage

The figures illustrate the impact of a single-window adversarial attack on key battery signals: current, temperature, and terminal voltage. In Fig. 2, the attack causes sharp current spikes between 150 and 151 seconds, creating significant deviations from the baseline, which could disrupt normal BESS operation. Fig. 3 shows a similar response for temperature, where brief, sudden spikes during the same window deviate from the nominal 298.15 K, highlighting how such disturbances can mislead control systems that depend on stable temperature data. Fig. 4 reflects the combined impact of these attacks on the terminal voltage, showing slight perturbations during the attack window while maintaining the overall discharge pattern. The results emphasize that even brief, localized attacks can induce notable deviations across critical battery metrics, underscoring the importance of rapid detection and mitigation to ensure BESS reliability and grid stability under potential cyber threats.

2) *Case 2: Combined Attack - Multiple Windows*

This scenario involves extending the combined adversarial attack across five distinct time windows: 100-110, 200-210, 300-310, 400-410, and 500-510 seconds. The noise levels are set to 0.5 and 0.001, maintaining a spike probability of 0.01 but reducing the spike factor to 2, limiting spikes within the noise amplitude range. As in Case 1, the focus is on the battery's terminal voltage, assessing the effects of multiple attacks over different periods.

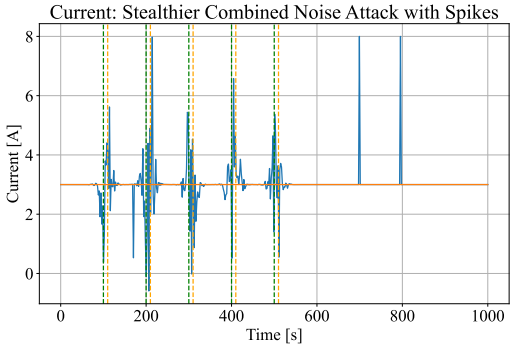

Fig. 5: Multi-Window — Temperature Noise attack

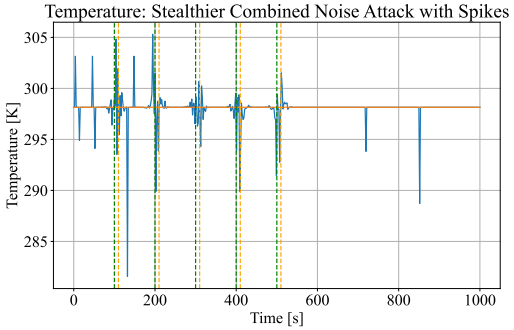

Fig. 6: Multi-Window — Temperature Noise attack

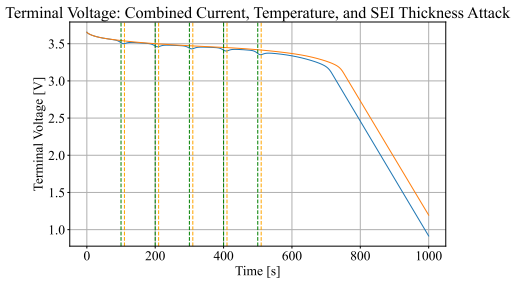

Fig. 7: Multi-Window — Terminal Voltage

The figures illustrate how multi-window adversarial attacks affect key battery parameters—current, temperature, and terminal voltage—across several time intervals. In Fig. 5, the current signal exhibits clear, sharp spikes within each of the five attack windows (100-110, 200-210, 300-310, 400-410, and 500-510 seconds). These spikes are pronounced, reaching amplitudes of up to 8 A from a baseline of 3 A. The signal fluctuates rapidly within each window, displaying both positive and negative deviations that indicate potential instability in BESS operation. Outside these attack windows, the current returns to its baseline, emphasizing how the attack is localized but intense, capable of briefly disrupting normal battery control mechanisms that manage discharge.

Fig. 6 demonstrates a similar multi-window attack on the temperature signal, with each attack window showing sudden fluctuations that range between approximately 295 K and 305 K. The base temperature remains close to 298.15 K. The disturbances during each window are both upward and downward, indicating abrupt changes that could confuse thermal management systems, especially those relying on accurate and consistent temperature readings. The spikes are relatively less sharp than those in the current signal but exhibit more erratic behavior, suggesting that

temperature dynamics may be slower to respond but still significantly affected by rapid noise injections.

In Fig. 7, the terminal voltage reflects the combined impact of current, temperature, and SEI thickness disturbances across the same multi-window attack intervals. Unlike the clear spikes in current and temperature, the voltage perturbations appear as slight dips within each attack window, with amplitudes relatively small compared to the overall voltage profile. The voltage trend continues its gradual decline after the attacks, following the normal discharge trajectory. This suggests that while the individual attacks on current and temperature cause sharp deviations, their combined effect on terminal voltage is more gradual, indicating some inherent filtering capacity of the system. However, the persistent small dips during each window still pose a risk to BESS operation, potentially leading to cumulative inaccuracies in voltage estimation and management over time.

Overall, these results show that multi-window attacks create more frequent and varied disturbances compared to a single-window attack, with clear and repeated deviations in current and temperature and minor cumulative effects on terminal voltage. This highlights the importance of robust detection mechanisms that can respond to frequent, intermittent attacks and ensure the reliable operation of BESS under ongoing adversarial conditions.

B. Sensitivity Analysis

The sensitivity analysis of the terminal voltage under varying noise levels and initial SoC provides critical insights into the battery's performance under adversarial conditions. As shown in Fig. 8, the terminal voltage response is observed over the entire simulation period (0-1000 seconds), illustrating the effects of different noise amplitudes ranging from 0.01 0.01 to 2 2. The vertical dashed lines mark the attack windows where noise is applied. As the noise amplitude increases, a more pronounced deviation in the terminal voltage is evident, with higher noise amplitudes, like 2 2, causing sharper drops compared to lower levels, such as 0.01 0.01. This behavior reveals the significant sensitivity of the system to larger noise injections across the full simulation duration.

To provide a more detailed view, Fig. 9 focuses on the critical collapse region of the terminal voltage, zooming in on the latter part of the simulation (600-1000 seconds). Here, the differences in voltage behavior across varying noise amplitudes are clearer, showing that higher noise levels accelerate the voltage collapse as the battery approaches lower voltage states. This zoomed-in analysis highlights the increased sensitivity of the battery when it is nearing discharge, emphasizing the need for effective control measures during this critical phase.

Further examining the impact of initial SoC levels, Fig. 10 shows how different starting SoC values (0.2, 0.5, and 0.8) influence terminal voltage behavior over time. The results indicate that a lower initial SoC (e.g., 0.2) leads to a faster voltage drop, while a higher initial SoC (e.g., 0.8) offers greater resilience against voltage degradation. This demonstrates that maintaining a sufficient initial charge level is essential for enhancing battery performance and stability, particularly under noise and adversarial conditions. Together, Figs. 8, 9, and 10 underscore the importance of both noise management and maintaining adequate initial charge levels to sustain battery reliability and prevent premature voltage collapse.

The sensitivity analysis of terminal voltage is further extended to assess the impact of changes in SEI (Solid Electrolyte Interphase) resistance and electrolyte concentration. As illustrated in Fig. 11, the terminal voltage response is examined under varying SEI resistance levels, specifically 0.001 m, 0.002 m, and 0.005 m. The results indicate that as SEI resistance increases, there is a noticeable decrease in terminal voltage, suggesting that higher SEI resistance contributes to a more rapid voltage drop. This behavior underscores the significance of managing SEI resistance

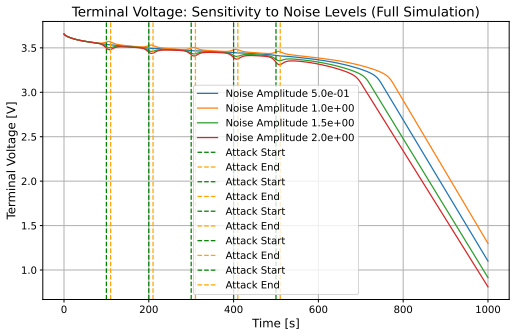

Fig. 8: Sensitivity To Noise [No Zoom]

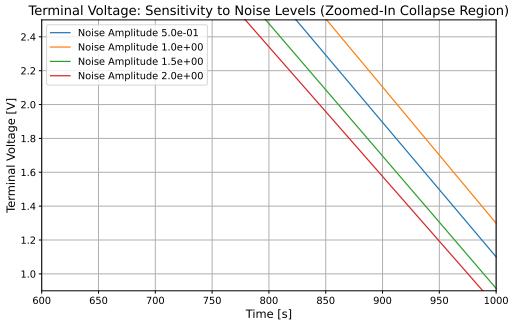

Fig. 9: Sensitivity To Noise [Zoom]

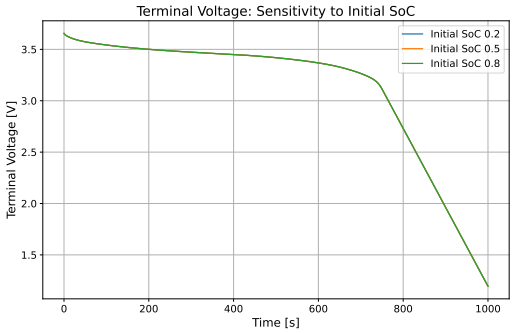

Fig. 10: Sensitivity To Initial SoC

to maintain stable battery performance, as higher resistance accelerates energy losses and degrades overall battery efficiency. In Fig. 12, the analysis focuses on the sensitivity of terminal voltage to different initial electrolyte concentrations, ranging from 1.0×10^3 to 2.0×10^3 mol/m^3. The figure demonstrates that higher electrolyte concentrations contribute to improved voltage stability, as evidenced by the slower voltage decline over the simulation period. Conversely, lower concentrations are associated with faster voltage drops, indicating a diminished ionic conductivity that adversely affects battery performance. This highlights the importance of maintaining optimal electrolyte concentrations for better charge transport and sustained battery operation.

The sensitivity analysis of terminal voltage under varying perturbation amplitudes is presented in both Fig. 13 and Fig. 14. In Fig. 13, the terminal voltage is shown over the full simulation period (0-1000 seconds) for perturbation amplitudes ranging from 0.001 to 0.500. The figure demonstrates that while higher perturbation amplitudes cause a more rapid decline in voltage, the overall impact is relatively small until the later stages of the simulation, where differences in voltage behavior become more evident. To provide a clearer perspective on the collapse region, Fig. 14 offers a zoomed-in view of the voltage behavior from 700 to 1000 seconds. Here, the impact of increasing perturbation amplitudes becomes more pronounced, with higher amplitudes leading to faster voltage collapse as the battery approaches lower voltage states. This detailed view emphasizes that larger perturbations significantly affect battery stability during the critical end-of-discharge phase.

Overall, the analysis indicates that terminal voltage is particularly sensitive to perturbation amplitudes during the later stages of discharge, highlighting the need for effective control measures to mitigate voltage collapse under increased disturbance levels.

The sensitivity analysis of terminal voltage to different sets of extreme attack windows, shown in Figs. 15 and 16, reveals how variations in attack timing and intensity affect battery performance. Over the full simulation period (Fig. 15), the voltage trend remains similar across all four sets, but differences emerge in the rate of decline, with earlier or more frequent attack windows causing slightly faster drops. In the zoomed-in collapse region (Fig. 16), the impact becomes more pronounced, as attack sets closer to the end of discharge lead to accelerated voltage collapse. This analysis highlights that strategic timing and placement of attack windows play a critical role in amplifying voltage deviations, emphasizing the need for timely countermeasures to maintain battery stability under extreme adversarial conditions.

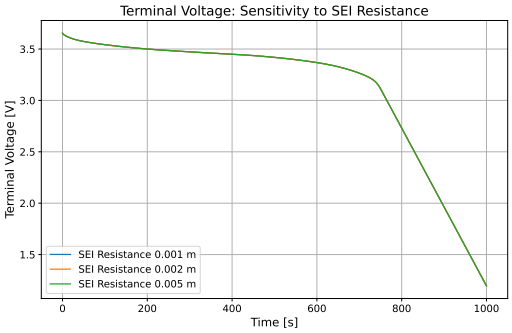

Fig. 11: Sensitivity To SEI Resistance

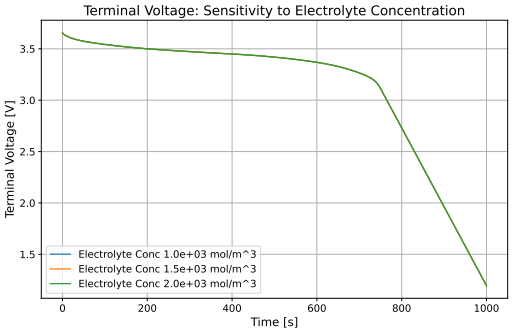

Fig. 12: Sensitivity To Electrolyte Concentration

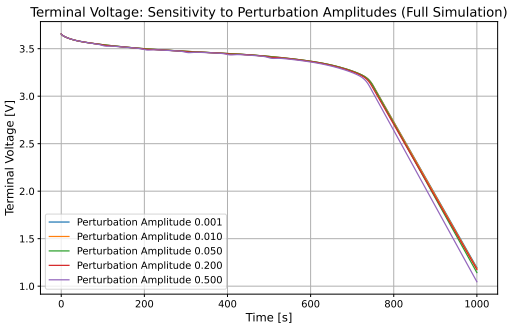

Fig. 13: Sensitivity To Perturbation Amplitude [No Zoom]

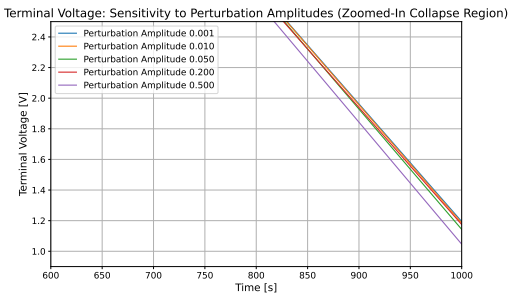

Fig. 14: Sensitivity To Perturbation Amplitude [Zoom]

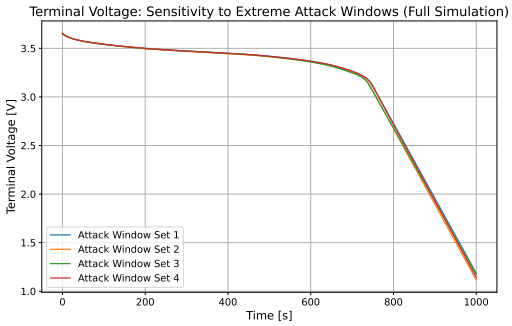

Fig. 15: Sensitivity To Extreme Attack Windows [No Zoom]

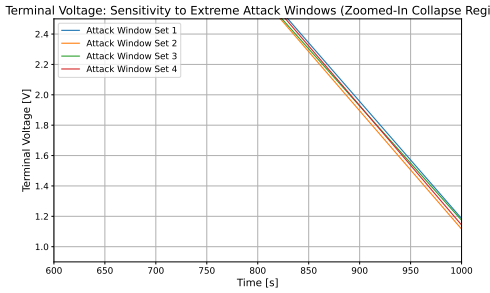

Fig. 16: Sensitivity To Extreme Attack Windows [Zoom]

V. Conclusion

The study proposed a method to simulate adversarial attacks on BESS using the DFN model and the PyBaMM framework. by utilising both single and multiple window attack windows the research identified specific vulnerabilities in BESS operation by targeting critical battery parameters including current, voltage, and temperature. The analysis found that noise levels and perturbation amplitudes have a substantial impact on the terminal voltage, showing deviations of up to 0.10 V and 0.3 V observed at 900 s. Variations in electrolyte concentration had minimal effect, causing a voltage deviation of approximately 0.05 V. Changes in initial state of charge and SEI resistance were found to have negligible impacts on the terminal voltage profile. Analysis of the effects of adversarial attacks on the terminal voltage determined that the coordinated multi-window attacks introduce varied and frequent disturbances and lead to a collapse in terminal voltage. The findings of the research demonstrate the necessity for developing resilient BMS that can be capable of real-time detection and mitigation of such adversarial threats and outlined the filtering capacity of the system which is built in and mitigates some of the immediate effects.

VI. Future Work

Future work will focus on enhancing the security and resilience of BESS against adversarial attacks by prioritizing the development of real-time detection methods integrated into BMS for rapid response. Expanding the study to include alternative chemistries like solid-state and flow batteries will broaden understanding of vulnerabilities and inform universal defense strategies. Efforts will also aim to fortify battery models against complex, coordinated attacks through robust estimation techniques and advanced control strategies, ensuring accurate predictions even under adversarial conditions. Exploring the interaction between machine learning and physics-based models in BMS, with a focus on adversarial-resistant algorithms such as robust optimization, adversarial training, and ensemble methods, will be key to improving resilience. Implementing defense mechanisms like anomaly detection, intrusion detection, and data fusion techniques, as well as examining the long-term impact of attacks on battery degradation and lifespan, will be essential. Lastly, experimental validation of the simulation results using real-world systems under controlled conditions will

confirm practical applicability and contribute to a comprehensive framework for evaluating BESS security.

REFERENCES

[1] X. Hu, F. Feng, K. Liu, L. Zhang, J. Xie, and B. Liu, "State estimation for advanced battery management: Key challenges and future trends," *Renewable and Sustainable Energy Reviews*, vol. 114, p. 109334, 2019.

[2] M. H. Lipu, M. A. Hannan, A. Hussain, M. Hoque, P. J. Ker, M. H. M. Saad, and A. Ayob, "A review of state of health and remaining useful life estimation methods for lithium-ion battery in electric vehicles: Challenges and recommendations," *Journal of cleaner production*, vol. 205, pp. 115–133, 2018.

[3] S. Vignesh, H. S. Che, J. Selvaraj, K. S. Tey, J. W. Lee, H. Shareef, and R. Errouissi, "State of Health (SoH) Estimation Methods for Second Life Lithium-ion Battery—Review and Challenges," *Applied Energy*, vol. 369, p. 123542, 2024.

[4] P. Zhuang and H. Liang, "False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2566–2577, 2020.

[5] M. Doyle, T. F. Fuller, and J. Newman, "Modeling of galvanostatic charge and discharge of the lithium/polymer/insertion cell," *Journal of the Electrochemical society*, vol. 140, no. 6, p. 1526, 1993.

[6] R. D. T. V. Obrien, "Cyber security of battery energy storage systems," *IEEE Access*, 2021.

[7] D. D. A. Selim, H. Mo, "Advanced battery management systems," *Journal of Power Sources*, vol. 478, 2023.

[8] J. T. T. Anas, "Fault-tolerant and adversarial high-availability lithium batteries health monitoring framework," *IEEE Access*, 2023.

[9] S. Z. D. Xiong, "Exploring adversarial threat models in cyber physical battery systems," *ACM Transactions on Cyber-Physical Systems*, 2023.

[10] M. D. Z. Khalik, "Exploiting vulnerabilities of load forecasting through adversarial attacks," *Journal of Power Sources*, 2024.

[11] E. U. M. Franceschelli, "Resilient and privacy-preserving multi-agent optimization and control of a network of battery energy storage systems under attack," *IEEE Transactions on Automation Science and Engineering*, 2023.

[12] M. Kaheni, E. Usai, and M. Franceschelli, "Resilient and privacy-preserving multi-agent optimization and control of a network of battery energy storage systems under attack," *IEEE Transactions on Automation Science and Engineering*, 2023.

[13] V. Obrien, R. D. Trevizan, and V. S. Rao, "Detecting false data injection attacks to battery state estimation using cumulative sum algorithm," in *2021 North American Power Symposium (NAPS)*. IEEE, 2021, pp. 01–06.

[14] M. M. Alhajri, D. B. Nour, K. R. Alshabib, and R. Rob, "Protecting energy storage systems–automated generation control-against coordinated and dynamic malicious data injection cyber attacks," in *2024 6th Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 2024, pp. 494–499.

[15] R. D. Trevizan, J. Obert, V. De Angelis, T. A. Nguyen, V. S. Rao, and B. R. Chalamala, "Cyberphysical security of grid battery energy storage systems," *IEEE Access*, vol. 10, pp. 59 675–59 722, 2022.

[16] F. Naseri, Z. Kazemi, P. G. Larsen, M. M. Arefi, and E. Schaltz, "Cyber-physical cloud battery management systems: review of security aspects," *Batteries*, vol. 9, no. 7, p. 382, 2023.

[17] e. a. Obrador Rey, C., "Battery management systems and their vulnerabilities in critical infrastructure," *Electronics*, vol. 13, pp. 860–870, 2024.

[18] H. Yuan, S. Li, T. Zhu, S. O'Kane, C. Garcia, G. Offer, and M. Marinescu, "A electrochemical-electro-thermal coupled computational framework to simulate the performance of li-ion batteries at cell-level: Analysis on the thermal effects," *arXiv preprint arXiv:2303.09838*, 2023.

[19] . J. M. Rahim, P., "Intelligent microgrid control using adversarial machine learning approaches," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2321–2330, 2020.

[20] A. Sayghe, J. Zhao, and C. Konstantinou, "Evasion attacks with adversarial deep learning against power system state estimation," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[21] L. Y. . Y. H. Zhang, X., "Online data poisoning attacks," in *NeurIPS*, 2020, pp. 1–12.

[22] V. Sulzer, S. G. Marquis, R. Timms, M. Robinson, and S. J. Chapman, "Python battery mathematical modelling (pybamm)," *Journal of Open Research Software*, vol. 9, no. 1, 2021.

[23] Z. Khalik, M. Donkers, and H. J. Bergveld, "Model simplifications and their impact on computational complexity for an electrochemistry-based battery modeling toolbox," *Journal of Power Sources*, vol. 488, p. 229427, 2021.

[24] C. Zhu, R. H. Byrd, P. Lu, and J. Nocedal, "Algorithm 778: L-bfgs-b: Fortran subroutines for large-scale bound-constrained optimization," *ACM Transactions on mathematical software (TOMS)*, vol. 23, no. 4, pp. 550–560, 1997.

[25] J. A. Andersson, J. Gillis, G. Horn, J. B. Rawlings, and M. Diehl, "Casadi: a software framework for nonlinear optimization and optimal control," *Mathematical Programming Computation*, vol. 11, pp. 1–36, 2019.

[26] G. F. Lawler and V. Limic, *Random walk: a Modern Introduction*. Cambridge University Press, 2010, vol. 123.

[27] A. Selim, H. Mo, H. Pota, and D. Dong, "Optimal scheduling of battery energy storage systems using a reinforcement learning-based approach," *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 11 741–11 747, 2023.

[28] B. Zou, J. Peng, R. Yin, Z. Luo, J. Song, T. Ma, S. Li, and H. Yang, "Energy Management of the Grid-Connected Residential Photovoltaic-battery System using Model Predictive Control Coupled with Dynamic Programming," *Energy and Buildings*, vol. 279, p. 112712, 2023.

[29] F. Zhang, A. Fu, L. Ding, and Q. Wu, "MPC based Control Strategy for Battery Energy Storage Station in a Grid with High Photovoltaic Power Penetration," *International Journal of electrical Power & energy systems*, vol. 115, p. 105448, 2020.

[30] A. Raghavan, P. Maan, and A. K. Shenoy, "Optimization of Day-ahead Energy Storage System Scheduling in Microgrid using Genetic Algorithm and Particle Swarm Optimization," *IEEE Access*, vol. 8, pp. 173 068–173 078, 2020.

[31] L. Ling, S. Yang, and S. Tong, "State of Health Estimation of Lithium-Ion Batteries Under Random Walk Operation Based on Probability Density Functions," *Available at SSRN 4706895*, 2022.

[32] S. Jiang and Z. Song, "A Review on the State of Health Estimation Methods of Lead-acid Batteries," *Journal of Power Sources*, vol. 517, p. 230710, 2022.

[33] J. Lee and J. Won, "Enhanced Coulomb Counting Method for SoC and SoH Estimation based on Coulombic Efficiency," *IEEE Access*, vol. 11, pp. 15 449–15 459, 2023.

[34] L. Chen, Z. Lü, W. Lin, J. Li, and H. Pan, "A New State-of-Health Estimation Method for Lithium-ion Batteries through the Intrinsic Relationship Between Ohmic Internal Resistance and Capacity," *Measurement*, vol. 116, pp. 586–595, 2018.

[35] M. Cacciato, G. Nobile, G. Scarcella, and G. Scelba, "Real-time Model-based Estimation of SOC and SOH for Energy Storage Systems," *IEEE Trans. Power Electronics*, vol. 32, no. 1, pp. 794–803, 2016.

[36] T. Oji, Y. Zhou, S. Ci, F. Kang, X. Chen, and X. Liu, "Data-driven Methods for Battery SoH Estimation: Survey and a Critical Analysis," *IEEE Access*, vol. 9, pp. 126 903–126 916, 2021.

[37] B. Oksendal, *Stochastic Differential Equations: an Introduction with Applications*. Springer Science & Business Media, 2013.

[38] NASA, "Randomized battery usage 1 (random walk)," https://data.nasa.gov/Raw-Data/Randomized-Battery-Usage-1-Random-Walk, 2024, accessed: 2024-06-10.

[39] E. Schulz, M. Speekenbrink, and A. Krause, "A Tutorial on Gaussian Process Regression: Modelling, Exploring, and Exploiting functions," *Journal of Mathematical Psychology*, vol. 85, pp. 1–16, 2018.

[40] A. Selim, "Optimal scheduled control operation of battery energy storage system using model-free reinforcement learning," in *2022 IEEE Sustainable Power and Energy Conference (iSPEC)*. IEEE, 2022, pp. 1–5.

[41] A. Selim, H. Mo, and H. Pota, "Optimal scheduling of grid supply and batteries operation in residential building: Rules and learning approaches," in *2022 IEEE 5th Student Conference on Electric Machines and Systems (SCEMS)*. IEEE, 2022, pp. 1–6.

[42] N. Q. Doan, S. M. Shahid, S.-J. Choi, and S. Kwon, "Deep reinforcement learning-based battery management algorithm for retired electric vehicle batteries with a heterogeneous state of health in besss," *Energies*, vol. 17, no. 1, p. 79, 2023.

[43] M. Varewyck and J.-P. Martens, "A Practical Approach to Model Selection for Support Vector Machines with a Gaussian Kernel," *IEEE Trans. Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 41, no. 2, pp. 330–340, 2010.

[44] J. O. Ogutu, T. Schulz-Streeck, and H.-P. Piepho, "Genomic Selection using Regularized Linear Regression Models: Ridge Regression, Lasso, Elastic net and Their extensions," in *BMC proceedings*, vol. 6. Springer, 2012, pp. 1–6.

[45] Z. Ren, D. Dong, H. Li, and C. Chen, "Self-paced Prioritized Curriculum Learning with Coverage Penalty in Deep Reinforcement

Learning," *IEEE Trans. Neural Networks and Learning Systems*, vol. 29, no. 6, pp. 2216–2226, 2018.

[46] Q. Wei, H. Ma, C. Chen, and D. Dong, "Deep Reinforcement Learning with Quantum-inspired Experience Replay," *IEEE Trans. Cybern.*, vol. 52, no. 9, pp. 9326–9338, 2021.

[47] G. Ciaburro, *MATLAB for machine learning*. Packt Publishing Ltd, 2017.

[48] M. N. Amiri, A. Håkansson, O. S. Burheim, and J. J. Lamb, "Lithium-ion battery digitalization: Combining physics-based models and machine learning," *Renewable and Sustainable Energy Reviews*, vol. 200, p. 114577, 2024.

[49] S. Gunn, D. Jang, O. Paradise, L. Spangher, and C. J. Spanos, "Adversarial poisoning attacks on reinforcement learning-driven energy pricing," in *Proceedings of the 9th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, 2022, pp. 262–265.

[50] M. Massaoudi, K. R. Davis, H. Abu-Rub, A. Ghrayeb, and T. Huang, "Accurate joint detection of false data injection attacks on islanded pv output power and state of health estimation of lithium-ion batteries," in *2024 4th International Conference on Smart Grid and Renewable Energy (SGRE)*. IEEE, 2024, pp. 1–6.

[51] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.

[52] P. Venugopal, S. S. Shankar, C. P. Jebakumar, R. Agarwal, H. H. Alhelou, S. S. Reka, and M. E. H. Golshan, "Analysis of optimal machine learning approach for battery life estimation of li-ion cell," *Ieee Access*, vol. 9, pp. 159 616–159 626, 2021.

[53] P. Arunachalam and Others, "Full homogenised model and its application to lithium-ion batteries," *Journal of Electrochemical Energy Conversion*, vol. 30, no. 4, pp. 45–56, 2021.

[54] V. Brosa, S. Kumar, and H. Fahl, "Multiscale modelling for lithium-ion batteries: Thermal and electrochemical coupling," *Journal of Power Sources*, vol. 17, no. 3, pp. 231–248, 2021.

[55] P. Arunachalam and S. Gupta, "Enhanced parameter identification capabilities in homogenised lithium-ion battery models," *Journal of Computational Physics*, vol. 367, pp. 41–55, 2018.

[56] K. Smith, C. Rahn, and C. Wang, "Model-based electrochemical estimation of lithium-ion batteries," *Journal of Power Sources*, vol. 180, pp. 173–184, 2008.

[57] N. Reddy and R. Sitaram, "Parameter estimation for dfn models of lithium-ion batteries," *Energy Storage Journal*, vol. 12, pp. 77–88, 2019.

[58] K. Smith and C. Rahn, "Model-based estimation and control of lithium-ion battery systems," *IEEE Transactions on Control Systems Technology*, vol. 15, pp. 545–557, 2007.

[59] M. G. Reniers, J. and D. Howey, "Multiscale modelling of lithium-ion batteries: A review," *Journal of Energy Storage*, vol. 30, pp. 101–113, 2020.

[60] B. Liu, X. Hu, X. Lin, and Y. Li, "Advanced modelling techniques for lithium-ion batteries," *Journal of Power Sources*, vol. 22, pp. 102–118, 2021.

[61] T. Nguyen, M. Senol, and J. Kowal, "Review of lithium-ion battery modelling," *Energy Storage Journal*, vol. 14, pp. 89–103, 2018.

[62] A. Bizeray, S. Kim, Y. Lee, and M. Choi, "Battery management system: Electrochemical modelling and control," *Journal of Energy Storage*, vol. 22, pp. 147–164, 2016.

[63] B. Wu, M. Ouyang, and S. Liu, "Multi-physics modelling of lithium-ion batteries: Challenges and opportunities," *Journal of Energy Storage*, vol. 35, pp. 204–218, 2022.

[64] S. Patnaik and A. Mishra, "Adversarial attacks on lithium-ion battery management systems," *Journal of Cybersecurity and Energy Storage*, vol. 27, pp. 65–78, 2021.

[65] H. Li, F. Zhang, and G. Xu, "Battery modelling for advanced management systems in electric vehicles," *Journal of Power Sources*, vol. 30, pp. 140–155, 2021.

[66] M. Prasad and R. Kumar, "Cybersecurity of battery management systems in electric vehicles," *Journal of Cybersecurity and Power Systems*, vol. 21, pp. 113–130, 2019.

[67] X. Lin, Q. Wang, and X. Feng, "Aging mechanisms of lithium-ion batteries: Modelling and simulation," *Journal of Power Sources*, vol. 18, pp. 34–49, 2017.

[68] J. Reniers, G. Mulder, and D. Howey, "Modelling lithium-ion battery degradation: A comprehensive review," *Journal of Energy Storage*, vol. 34, pp. 122–140, 2021.

[69] Q. Zhang, Y. Liu, and D. Pan, "Advanced control techniques for lithium-ion battery management systems," *Journal of Power Sources*, vol. 22, pp. 112–135, 2018.

[70] L. Chang, H. Tang, and J. Gao, "Optimal control techniques for battery management systems," *Journal of Power Electronics*, vol. 28, pp. 99–119, 2017.

[71] H. Wang and J. Zhao, "Cyber-physical security in battery management systems," *Journal of Cybersecurity and Energy Storage*, vol. 19, pp. 43–65, 2021.

[72] K. A. Severson, P. M. Attia, N. Jin, N. Perkins *et al.*, "Data-driven prediction of battery cycle life before capacity degradation," *Nature Energy*, vol. 4, no. 5, pp. 383–391, 2019.

[73] J. Keil and A. Jossen, "Electrochemical modeling of linear and nonlinear aging of lithium-ion cells," *Journal of the Electrochemical Society*, vol. 164, no. 4, pp. A6066–A6070, 2017.

[74] A. S. H. Pota, "Cybersecurity of battery energy storage systems and adoption of data-driven methods," *IEEE Transactions on Smart Grid*, 2023.

[75] S. Lee, J. Kim, J. Lee, and B.-H. Cho, "State-of-charge and capacity estimation of lithium-ion battery using a new open-circuit voltage versus state-of-charge relationship," *Journal of Power Sources*, vol. 185, pp. 1367–1373, 2016.

[76] S. Sepasi, R. Ghorbani, and B. Y. Liaw, "Inline state of health estimation of lithium-ion batteries using state of charge calculation," *Journal of Power Sources*, vol. 299, pp. 246–254, 2015.

[77] A. P. e. a. Severson, K.A., "Data-driven prediction of battery cycle life before capacity degradation," *Nature Energy*, vol. 5, pp. 233–242, 2020.

[78] V. E. . J. S. Harippriya, S., "Analysis of optimal machine learning approach for battery life estimation of li-ion cell," *Journal of Physics: Conference Series*, vol. 2325, no. 1, p. 012004, 2022.

[79] e. a. Islam, M., "Battery management system to estimate battery aging using deep learning and machine learning algorithms," in *IEEE Transactions on Energy Systems*, 2022, pp. 301–310.

[80] . M. A. Ali, A., "Adversarial poisoning attacks on reinforcement learning-driven energy pricing," in *Neural Information Processing Systems (NeurIPS)*, 2020, pp. 1–10.

[81] . G. R. Singh, C., "Accurate joint detection of false data injection attacks on islanded pv output power and soh estimation," in *International Conference on Smart Grid Renewable Energy (SGRE24)*, 2024, pp. 1–6.

[82] . T. H. Wang, H., "Cybersecurity threats in battery management systems: A comprehensive review," *Journal of Energy Storage*, vol. 35, pp. 3010–3020, 2021.

[83] . G. L. Khan, M., "Adversarial machine learning for critical infrastructure systems: Case study on energy networks," in *ICML Security Conference*, 2024, pp. 17–25.

[84] . L. S. Soltani, R., "Challenges in adversarial machine learning for cyber-physical systems," *Cyber-Physical Systems Journal*, vol. 7, pp. 201–217, 2021.