Journal of *Marine Science and Engineering*

MDPI

Article

Detection and Defense Against False Data Injection Attacks for Secure Energy Management in Hybrid Electric Ships

Hao Sun [1], Na Li [2], Mo Guo [3], Jingwei Wei [4] and Tianqing Yuan [2,*]

[1] College of Electrical and Control Engineering, Jilin University of Chemical Technology, Jilin 132022, China; sunhao218@jlict.edu.cn
[2] Department of Electrical Engineering, Northeast Electric Power University, Jilin 132012, China; 2202300004@neepu.edu.cn
[3] State Grid Zhejiang Electric Power Co., Ltd. Construction Branch, Hangzhou 310000, China; noblefuture@163.com
[4] Unicompound Semiconductor Corporation, Putian 351117, China; weijingwei120@163.com
* Correspondence: 20192929@neepu.edu.cn

Abstract

Reliable battery state awareness is essential for energy management and power allocation in hybrid electric ships. However, battery management systems are increasingly exposed to False Data Injection Attacks (FDIAs) in intelligent connected environments, which can distort State of Charge (SOC) estimation and compromise the operational reliability of shipboard power systems. To address this challenge, this paper proposes a closed-loop "Modeling-Detection-Defense" framework for secure SOC estimation in marine cyber-physical energy systems. First, a stealthy FDIA model is developed based on battery dynamics and physical consistency constraints. Second, a hybrid detection method combining unsupervised and supervised learning is proposed to identify attacks. Finally, a long short-term memory network is employed to reconstruct compromised measurements and provide reliable SOC information for continuous energy management. Experimental results demonstrate that the proposed framework mitigates SOC estimation deviations caused by FDIAs. In addition, it effectively reduces power allocation errors and energy losses, thereby improving the cyber-resilience, operational reliability, and energy efficiency of hybrid ship power systems.

Keywords: hybrid electric ships; battery energy storage systems; energy management systems; battery management system; state of charge; false data injection attacks

Check for updates

Academic Editors: Rosemary Norman, Peilin Xie and Sen Tan

Received: 1 June 2026
Revised: 3 July 2026
Accepted: 3 July 2026
Published: 7 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Against the background of global energy transition and carbon emission reduction, vessels driven by clean energy have emerged as important solutions for achieving green shipping [1,2]. In this paper, these vessels are collectively referred to as New Energy Ships (NES), including electric ships and hybrid electric ships. In a typical marine power system, the Battery Energy Storage System (BESS) is integrated with diesel generators, propulsion loads, and the shipboard grid to form an AC/DC hybrid distribution architecture, enabling energy conversion and power output through the electric propulsion system. Due to their high energy density and superior dynamic response, lithium-ion batteries are extensively utilized in NES propulsion systems [3]. As the core of the NES powertrain, the Energy Management System (EMS) aims to coordinate energy distribution among power sources to optimize efficiency and ensure ship maneuvering performance [4,5]. The

optimal decision-making of the EMS relies heavily on the state information provided by the Battery Management System (BMS) [6,7]. Specifically, the BMS reports real-time data to the EMS, which generates optimal power allocation setpoints and issues them to the Power Management System (PMS) for execution. In this process, the State of Charge (SOC) serves as a critical input parameter, and its estimation reliability directly dictates the rationality of power distribution. Here, reliability is defined as a comprehensive performance metric encompassing accuracy, robustness, and anti-attack capability.

However, within the paradigm of intelligent connected ships, the BMS has evolved into a sophisticated cyber-physical system, increasingly vulnerable to False Data Injection Attacks (FDIA) [8–10]. Such attacks induce deviations in SOC estimation by tampering with raw sensory data, thereby misleading the EMS into executing erroneous power allocation decisions and degrading the coordinated operation of hybrid ship power systems, which ultimately results in reduced energy efficiency and increased operational risks [11]. Furthermore, marine power systems must adhere to stringent classification society rules and international maritime safety standards (such as DNV and IMO). These regulations mandate that critical control units possess the capability for resilient operation under cyberattacks or anomalous conditions [12,13]. Consequently, the detection and mitigation of FDIA targeting the BMS are not only vital for the reliability of energy management but also directly essential for the safety and regulatory compliance of vessel operations.

Currently, detection methodologies for FDIAs are primarily categorized into two paradigms: model-driven and data-driven approaches. Model-driven methods identify attacks by analyzing the deviation between measured data and the estimated values derived from physical models [14]. For instance, reference [15] utilizes an Adaptive Extended Kalman Filter (AEKF) to estimate the SOC in real-time and derive the theoretical voltage. By establishing a state consistency framework and performing statistical hypothesis testing on the residuals, effective identification of FDIAs is achieved. However, these methods exhibit a high dependency on precise model parameters and pre-defined thresholds, leading to suboptimal robustness under complex and highly dynamic sailing conditions.

Data-driven methods identify attacks by mining features from massive datasets without the need for complex physical modeling [16]. Among these, unsupervised learning adapts well to complex network environments by leveraging the inherent structural heterogeneity of data for attack identification, eliminating the requirement for labeled samples. In [17], an unsupervised Isolation Forest (IF) algorithm was proposed, which detects anomalies based on the susceptibility of attack points to being isolated within a tree structure. However, this approach lacks the guidance of prior knowledge, making it prone to false positives. In contrast, supervised learning achieves higher identification precision by training models to distinguish characteristic differences between normal and compromised data. For instance, reference [18] introduced a detection method that extracts power grid topology and spatial features using gated graph neural networks combined with attention mechanisms. Similarly, reference [19] utilized deep convolutional neural networks to capture spatio-temporal features, using detection indicators as network outputs to identify FDIAs. Nevertheless, such methods rely heavily on annotated datasets and exhibit limited generalization capabilities. With the rapid advancement of computing technology, integrating the high adaptability of unsupervised learning with the superior precision of supervised learning has emerged as a prominent research focus in the field of FDIA detection and defense.

While FDIAs have been extensively studied in power grids, research on FDIAs targeting new energy ships' BMS is still in its infancy. Therefore, this paper establishes a closed-loop "modeling-detection-defense" security framework centered on lithium-ion battery SOC estimation. First, by coupling the battery equivalent circuit model, a physically

consistent FDIA model is constructed, revealing the cumulative amplification effect of micro-disturbances in SOC estimation and their cascading hazards to the energy management loop. Second, a hybrid detection method is proposed by integrating the unsupervised Isolation Forest (IF) with the supervised Long Short-Term Memory (LSTM) network. This approach leverages the synergistic complementarity of these algorithms to enhance detection precision while mitigating reliance on labeled data. Finally, considering the temporal characteristics of BMS data, an LSTM-based prediction model is utilized to implement a reconstruction-based defense strategy for compromised data. Experimental results demonstrate that the proposed framework improves the data security of the BMS and enhances the cyber-resilience, power allocation reliability, and operational stability of hybrid ship power systems.

2. Shipboard Systems Background and FDIA Modeling

2.1. Shipboard Power System Architecture

Unlike terrestrial power grids or electric vehicle systems, modern all-electric ships and hybrid vessels typically employ highly integrated and safety-critical power system architectures. A typical shipboard power system comprises power generation units (such as diesel generators or fuel cells), energy storage systems (such as lithium-ion battery packs), propulsion systems, and various auxiliary loads, all interconnected via AC, DC, or hybrid AC/DC distribution networks. Among these, the DC distribution architecture has gained widespread adoption in next-generation vessels due to its superior energy conversion efficiency and flexibility in integrating renewable energy sources. Figure 1 illustrates the cyber-physical architecture of a shipboard BMS, highlighting the synergistic relationship between the shipboard power system, the BMS, and the energy management layer.

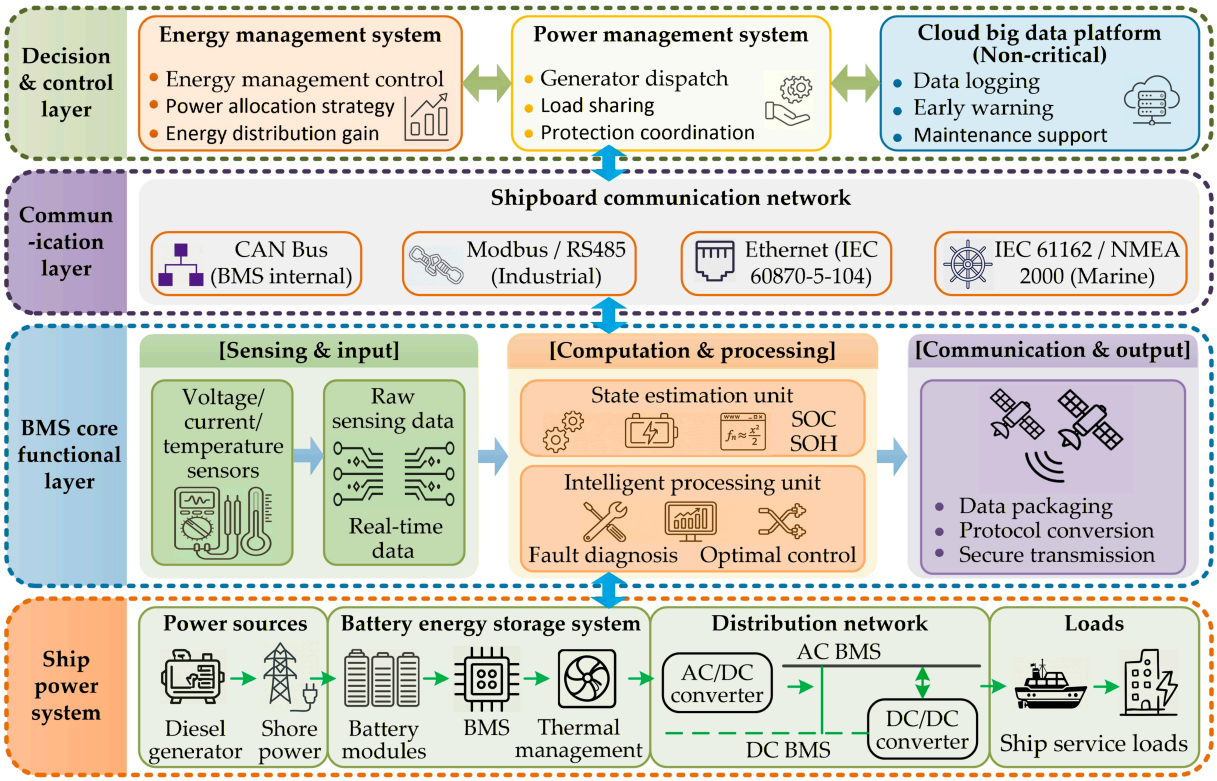


Figure 1. Cyber-physical architecture of the shipboard BMS [20,21].

As a vital subsystem within the shipboard power system, the BMS is formed by the coupling of the physical, sensing, computing, and communication layers. Its hardware

modules are responsible for the real-time acquisition of raw sensing data, while the software modules perform online battery state estimation, fault diagnosis, and optimal control [22]. When communication conditions permit, cloud-based big data analysis can be integrated to facilitate assisted operation, maintenance, and early warning; however, this component is generally treated as a non-critical optional feature during actual maritime navigation.

From a system control perspective, the BMS serves as the core information link connecting the physical battery layer with the EMS. The BMS provides critical state information, based upon which the EMS makes power allocation decisions for hybrid ship power systems, while the PMS translates these decisions into specific execution commands. In this closed-loop structure, the accuracy of SOC estimation dictates the rationality of energy management and power distribution. Consequently, if the SOC is perturbed by cyberattacks, it may lead to biased EMS decision-making. These biases are subsequently amplified by the PMS into power allocation errors, ultimately degrading the operational efficiency of onboard energy storage systems and ship power systems.

2.2. BMS Communication Fundamentals and Attack Surfaces

In shipboard systems, the BMS interacts with other subsystems through industrial communication protocols, such as Controller Area Network (CAN), Modbus, and Ethernet-based networks. Raw sensor data, including battery voltage, current, and temperature, are transmitted to the BMS via the onboard communication bus. Once state estimation is complete, the relevant information is uploaded to the EMS to support energy scheduling decisions. This forms a "sensing-estimation-control" closed-loop structure, constituting a typical maritime Cyber-Physical System (CPS).

As shipboard systems become increasingly intelligent and networked, they are exposed to heightened risks from internal threats, supply chain compromises, and remote access vulnerabilities, all of which facilitate FDIAs. These attacks primarily target two levels: the communication layer, where malicious data frames are injected to interfere with information transmission, and the sensing layer, where direct manipulation of voltage, current, or temperature measurements causes errors that propagate through state estimation algorithms, ultimately resulting in significant SOC deviations and compromised decision-making by the EMS.

Compared to communication layer attacks, sensing layer FDIAs exhibit greater stealth and destructiveness. Furthermore, unlike open power grid systems, shipboard power systems are characterized by a closed structure, clear control hierarchies, and stringent safety constraints. Therefore, this paper focuses the FDIA modeling on the BMS sensing layer to better align with practical maritime application scenarios, subsequently conducting research on its detection and defense mechanisms.

2.3. Battery Equivalent Circuit Model

As the core benchmark for measuring remaining battery energy and scheduling energy flow, the SOC is highly sensitive to subtle data manipulations, making it an ideal observation window for revealing FDIA mechanisms. To simulate FDIA against SOC estimation in the BMS, a classical second-order resistor-capacitor (RC) Equivalent Circuit Model (ECM) is adopted to characterize the battery dynamics. The ECM serves as the basis for deriving the state-space model required for Extended Kalman Filter (EKF)-based SOC estimation, a modeling procedure widely adopted in lithium-ion battery SOC estimation

studies [23–25]. The discretized state-space and observation equations of the ECM are formulated in Equations (1) and (2) as follows:

$$\begin{bmatrix} SOC_{k+1} \\ U_{1,k+1} \\ U_{2,k+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-T/\tau_1} & 0 \\ 0 & 0 & e^{-T/\tau_2} \end{bmatrix} \times \begin{bmatrix} SOC_k \\ U_{1,k} \\ U_{2,k} \end{bmatrix} + \begin{bmatrix} -\eta T/Q_c \\ R_1(1-e^{-T/\tau_1}) \\ R_2(1-e^{-T/\tau_2}) \end{bmatrix} \times I_k + \begin{bmatrix} w_{1,k} \\ w_{2,k} \\ w_{3,k} \end{bmatrix} \quad (1)$$

$$U_k = U_{\mathrm{OCV}}(SOC_k) - U_{1,k} - U_{2,k} - R_0 I_k + v_k \quad (2)$$

where U_{OCV} denotes the open-circuit voltage; U represents the terminal voltage; U_1 and U_2 are the polarization voltages across the RC networks, respectively; I is the discharge current; R_0 is the ohmic resistance; R_1 and C_1 correspond to the electrochemical polarization resistance and capacitance, respectively; R_2 and C_2 represent the concentration polarization resistance and capacitance. The state variable is defined as $\boldsymbol{x}_k = \begin{bmatrix} SOC_k & U_{1,k} & U_{2,k} \end{bmatrix}^{\mathrm{T}}$; the control input is $\mu_k = I_k$; and the observation variable is $y_k = U_k$; $\tau_1 = R_1C_1, \tau_2 = R_2C_2$. Furthermore, $\boldsymbol{w}_k = \begin{pmatrix} w_{1,k} & w_{2,k} & w_{3,k} \end{pmatrix}^{\mathrm{T}}$ denotes the system noise with covariance $\boldsymbol{Q}$, while $\boldsymbol{v}_k$ represents the observation noise with covariance $\boldsymbol{R}$. T is the sampling interval; η indicates the Coulombic efficiency; and Q_c refers to the rated capacity of the battery.

Given the nonlinear battery dynamics, the discrete equivalent circuit model described by Equations (1) and (2) is reformulated into the standard state-space representation for EKF-based SOC estimation, as shown in Equation (3) [26,27].

$$\begin{cases} \boldsymbol{x}_{k+1} = \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{B}_k \mu_k + \boldsymbol{w}_k \\ \boldsymbol{y}_k = \boldsymbol{C}_k \boldsymbol{x}_k + \boldsymbol{D}_k \mu_k + \boldsymbol{v}_k \end{cases} \quad (3)$$

Combining Equations (1)–(3), the following relationship can be obtained:

$$\boldsymbol{A}_k = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-T/\tau_1} & 0 \\ 0 & 0 & e^{-T/\tau_2} \end{bmatrix}; \ \boldsymbol{B}_k = \begin{bmatrix} -\eta T/Q_c \\ R_1(1-e^{-T/\tau_1}) \\ R_2(1-e^{-T/\tau_2}) \end{bmatrix};$$
$$\boldsymbol{C}_k = \begin{bmatrix} \frac{\partial U_{\mathrm{ocv}}}{\partial SOC}\Big|_{SOC=S\hat{O}C(k)} & -1 & -1 \end{bmatrix}; \ \boldsymbol{D}_k = -\boldsymbol{R}_0(k).$$

The EKF is employed to predict and update the various states of the battery. The relevant governing equations are defined in Equation (4):

$$\begin{cases} \hat{\boldsymbol{x}}_0 = E(\boldsymbol{x}_0) \\ \boldsymbol{P}_0 = E\left[(\boldsymbol{x}_0 - \hat{\boldsymbol{x}}_0)(\boldsymbol{x}_0 - \hat{\boldsymbol{x}}_0)^{\mathrm{T}}\right] \\ \hat{\boldsymbol{x}}_{k+1|k} = \boldsymbol{A}_k \hat{\boldsymbol{x}}_{k|k} + \boldsymbol{B}_k \mu_k \\ \boldsymbol{P}_{k+1|k} = \boldsymbol{A}_k \boldsymbol{P}_{k|k} \boldsymbol{A}_k^{\mathrm{T}} + \boldsymbol{Q}_{k+1} \\ \boldsymbol{K}_{k+1} = \boldsymbol{P}_{k+1|k} \boldsymbol{C}_{k+1}^{\mathrm{T}} \left(\boldsymbol{C}_{k+1} \boldsymbol{P}_{k+1\,|\,k} \boldsymbol{C}_{k+1}^{\mathrm{T}} + \boldsymbol{R}_{k+1}\right)^{-1} \\ \hat{y}_{k+1} = \boldsymbol{C}_{k+1} \hat{\boldsymbol{x}}_{k+1|k} + \boldsymbol{D}_k \mu_k \\ \hat{\boldsymbol{x}}_{k+1|k+1} = \hat{\boldsymbol{x}}_{k+1|k} + \boldsymbol{K}_{k+1}(y_{k+1} - \hat{y}_{k+1}) \\ \boldsymbol{P}_{k+1|k+1} = (\boldsymbol{I} - \boldsymbol{K}_{k+1} \boldsymbol{C}_{k+1}) \boldsymbol{P}_{k+1|k} \end{cases} \quad (4)$$

2.4. Mathematical Model of FDIA

Based on the EKF state estimation framework established in Section 2.3, the Jacobian matrix $\boldsymbol{H}$ derived from the measurement equation is employed to construct physically consistent stealthy FDIA. This study constructs a representative stealthy FDIA targeting voltage measurements, aiming to bypass BMS residual-based detection while continuously distorting SOC estimation under physical consistency constraints. Since voltage is one of

the most sensitive and vulnerable observation variables in battery management systems, this study focuses on this channel as a representative attack scenario. The main objective is to evaluate the detection and defense performance of the proposed method under this canonical stealth FDIA setting, rather than exhaustively modeling multiple attack types.

In general lithium-ion battery equivalent circuit models, the relationship between the measurement $\boldsymbol{z}$ and the state variable $\boldsymbol{x}$ can be expressed in Equation (5) [11]:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{5}$$

where $\boldsymbol{z}$ represents the data measured by battery sensors; $\boldsymbol{x}$ is the system state variable; $\boldsymbol{e}$ is the measurement error vector. The Jacobian matrix $\boldsymbol{H}$ is defined as the partial derivative of the measurement function with respect to the state variables, $\boldsymbol{H} = \frac{\partial h(x)}{\partial x}$. For the second-order RC equivalent circuit model, it can be expressed as: $\boldsymbol{H} = \left[\frac{\partial U_{\mathrm{ocv}}(SOC)}{\partial SOC}, \frac{\partial h}{\partial U_1}, \frac{\partial h}{\partial U_2}\right] = \left[\frac{\partial U_{\mathrm{ocv}}(SOC)}{\partial SOC}, -1, -1\right]$.

To effectively suppress the influence of cumulative measurement errors on state estimation, the weighted least squares estimate of the linearized state vector can be represented in Equations (6) and (7) as follows:

$$J(\boldsymbol{x}) = (z - \boldsymbol{H}x)^{\mathrm{T}}\boldsymbol{W}^{-1}(z - \boldsymbol{H}x) \tag{6}$$

$$\hat{\boldsymbol{x}} = \left(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}^{-1}\boldsymbol{z} \tag{7}$$

where $\boldsymbol{W}$ is a positive definite weighting matrix. Under the assumption of Gaussian noise, this matrix can be chosen as the measurement noise covariance matrix.

During a false data injection attack, an attack vector is typically added to the measurement vector to generate a corrupted measurement. Thus, the mathematical model of the FDIA can be defined in Equation (8):

$$\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} + \boldsymbol{a} \tag{8}$$

where $\mathbf{z}_a$ is the compromised measurement vector, and $\boldsymbol{a}$ is the injected attack vector.

In this scenario, the estimated state $\hat{\boldsymbol{x}}_a$ is expressed in Equation (9):

$$\hat{\boldsymbol{x}}_a = \left(\boldsymbol{H}^{T}\sum\nolimits_{e}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\mathrm{T}}\sum\nolimits_{e}^{-1}\boldsymbol{z}_a = \hat{\boldsymbol{x}} + \boldsymbol{c} \tag{9}$$

where $\boldsymbol{c}$ represents the deviation vector of the state variable caused by the attack, and $\sum_e$ is the covariance matrix of the measurement error vector $\boldsymbol{e}$, consistent with the $\boldsymbol{W}$.

BMS typically employs residual-based detection to identify bad data. If the residual exceeds a predefined threshold, it is classified as bad data; otherwise, it is regarded as a normal observation. The residual after the attack is expressed in Equation (10):

$$\|\boldsymbol{r}_a\| = \|\boldsymbol{z}_a - \boldsymbol{H}\hat{\boldsymbol{x}}_a\| = \|\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c})\| = \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} + (\boldsymbol{a} - \boldsymbol{H}\boldsymbol{c})\| \tag{10}$$

When the above equation satisfies $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, the measurement offset induced by the attack remains logically consistent with the physical modeling, resulting in a highly stealthy FDIA. This scenario is categorized as a "worst-case" attack. However, in practical shipboard systems, battery parameters vary dynamically due to factors such as temperature and aging, making it difficult for an adversary to acquire a precise system model. Consequently, this idealized attack model is primarily utilized to characterize the theoretical upper bound of system security and to provide a rigorous foundation for the subsequent design of robust detection and defense strategies.

3. FDIA Detection and Reconstruction-Based Defense Based on IF-LSTM

3.1. Isolation Forest Algorithm

Isolation Forest (IF) is an unsupervised anomaly detection algorithm capable of identifying outliers without the requirement for labeled data or extensive training. The algorithm partitions samples using Isolation Trees (iTrees). Due to their sparse distribution and low proportion in the overall dataset, anomaly points are more susceptible to rapid isolation, thereby residing closer to the root nodes of the trees. Consequently, FDIAs can be identified by the path length from the sample point to the root node: the shorter the path, the higher the anomaly score [28]. The structural diagram of the algorithm is illustrated in Figure 2.

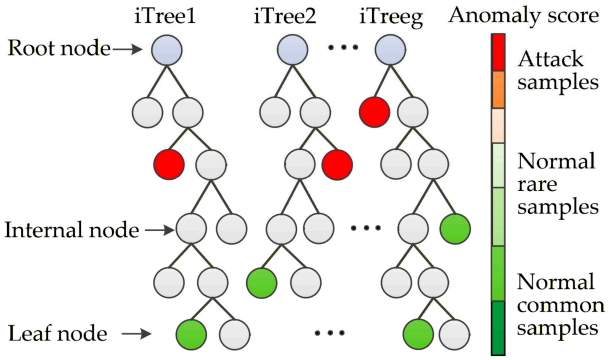


Figure 2. Structure of the isolation trees.

The anomaly score is calculated in Equation (11) as follows:

$$S(x,n) = 2^{\frac{-E[h(x)]}{c(n)}} \tag{11}$$

where $E[h(x)]$ represents the average path length of a sample point across all isolation trees; $c(n)$ is the average path length of an unsuccessful search in a binary search tree; and $h(x)$ denotes the path length of the tested sample in a single tree. As $S(x,n)$ approaches 1, the probability of the sample being an anomaly increases, whereas a value significantly lower than 0.5 generally indicates normal data. While this algorithm typically requires a predefined threshold to classify sample attributes, this study focuses on feature extraction; therefore, no decision threshold is set at this stage.

3.2. Long Short-Term Memory Neural Network

As an advanced variant of Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM) effectively overcomes the inherent challenges of gradient vanishing and explosion in long-sequence training by introducing a sophisticated gating mechanism consisting of a forget gate, an input gate, and an output gate. This architecture offers significant advantages in capturing the intricate temporal dependencies and long-range correlations of battery data [29,30]. The core of LSTM lies in the dynamic information flow within the cell state: the forget gate is responsible for discarding redundant historical information, the input gate filters and updates relevant features of the current time step, and the output gate extracts hidden feature outputs based on the updated state. This selective memory mechanism ensures that the network can preserve critical information across long time steps, effectively mitigating the loss of gradient signals while providing robust temporal modeling capabilities to accurately characterize the complex nonlinear evolution of battery sequence data under varying operational conditions, thereby enhancing the overall reliability of the state estimation process. The structure is illustrated in Figure 3.

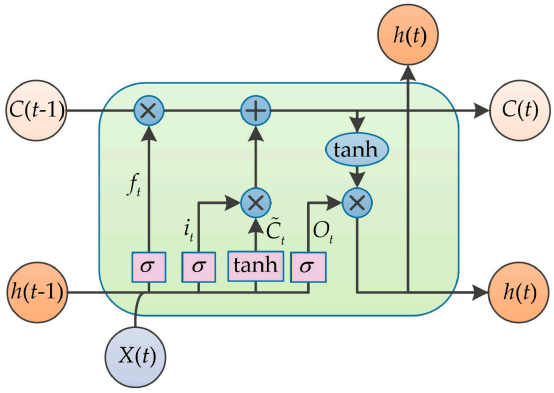


Figure 3. Schematic structure of the LSTM cell.

The LSTM architecture regulates information flow through gating mechanisms, which are defined by the recursive equations in (12).

$$\begin{cases} f_t = \sigma\left(\boldsymbol{W}_f \cdot [h_{t-1}, X_t] + \boldsymbol{b}_f\right) \\ \widetilde{C}_t = \tanh(\boldsymbol{W}_c \cdot [X_t, h_{t-1}] + \boldsymbol{b}_c) \\ i_t = \sigma(\boldsymbol{W}_i \cdot [X_t, h_{t-1}] + \boldsymbol{b}_i) \\ C_t = f_t \odot C_{t-1} + i_t \odot \widetilde{C}_t \\ o_t = \sigma(\boldsymbol{W}_0 \cdot [X_t, h_{t-1}] + \boldsymbol{b}_0) \\ h_t = o_t \odot \tanh(C_t) \end{cases} \tag{12}$$

where f_t represents the forget gate; $\boldsymbol{W}_f$, $\boldsymbol{W}_c$, $\boldsymbol{W}_i$ and $\boldsymbol{W}_0$ denote the weight matrices; $\boldsymbol{b}_f$, $\boldsymbol{b}_c$, $\boldsymbol{b}_i$ and $\boldsymbol{b}_0$ are the bias terms; X_t is the input data; h_t is the hidden state; σ represents the Sigmoid function; $\widetilde{C}_t$ is the candidate cell state; C_t is the current cell state; and i_t and o_t represent the input gate and output gate.

3.3. Coordination Scheme for Detection and Defense

The comprehensive procedure for the detection and defense of FDIAs is illustrated in Figure 4.

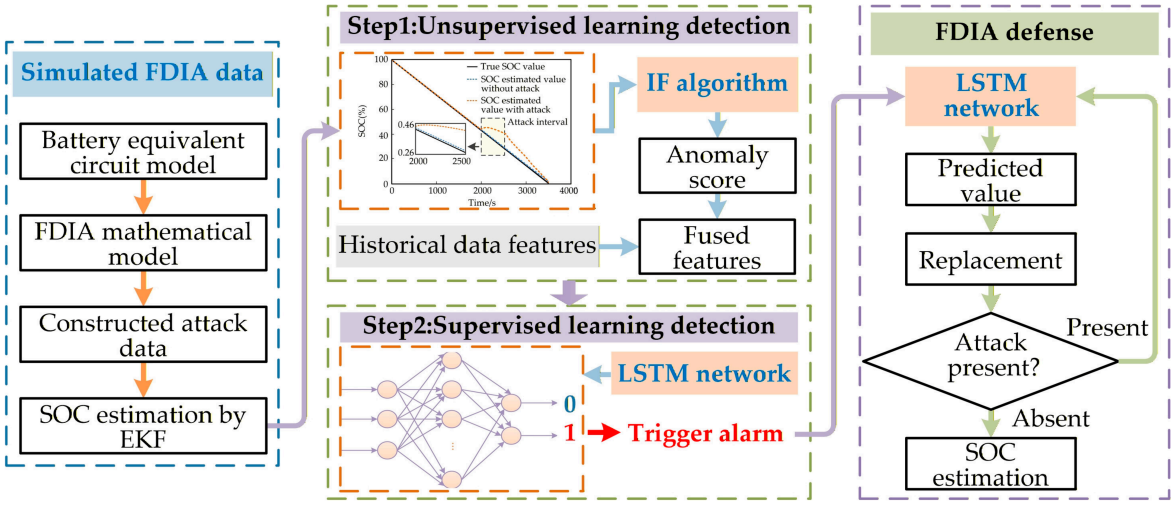


Figure 4. Flowchart of the FDIA detection and defense scheme.

When real-time measurement data are uploaded to the BMS, they first undergo detection via the IF-LSTM algorithm. The IF component mines the spatial distribution characteristics of the data to extract anomaly scores, while a sliding window mechanism is

employed to reconstruct high-dimensional matrices with local temporal envelopes. Subsequently, the gating mechanism of the LSTM is utilized to deeply capture the dynamic characteristics of the battery during charging and discharging processes, thereby achieving the precise identification of stealthy FDIAs.

The defense module relies on an offline-trained LSTM temporal model based on historical data from nominal operating conditions, ensuring it can accurately characterize the evolution patterns of lithium-ion battery states. Once an attack alert is triggered during the detection phase, the system invokes the optimal model to perform temporal extrapolation forecasting. High-confidence predicted values are then used to dynamically override the corrupted observation vectors. By estimating the SOC through the reconstructed measurement sequences, the BMS achieves state self-healing and steady-state operation following an FDIA, safeguarding the authenticity of the decision-making basis for the EMS.

4. Simulation Experiments and Results Analysis

This study focuses on mechanism-level validation of FDIA detection rather than exhaustive benchmarking across all operating conditions. It uses the publicly available Oxford lithium-ion battery dataset [31], derived from standardized single-cell tests. The dataset offers high precision, consistency, and controllable conditions, realistically capturing dynamic battery behavior and providing a reliable basis for FDIA analysis in SOC estimation. Since FDIAs primarily affect statistical distributions and temporal patterns rather than system scale or application scenario, this dataset is well suited for validating the proposed detection and defense algorithms. A summary of the dataset characteristics is provided in Table A1 in Appendix A. All simulations were conducted using MATLAB R2023b (MathWorks Inc., Natick, MA, USA).

To verify the effectiveness of the proposed method, this study utilizes the 10th discharge cycle data of Cell1 as the simulation benchmark. An attack intention is set for the voltage measurement term, and the state deviation vector $\boldsymbol{c}$ is configured with attacks of 100 mV and 200 mV. By employing the Jacobian matrix $\boldsymbol{H}$ from the EKF algorithm, attack vectors $\boldsymbol{a} = \boldsymbol{Hc}$ that satisfy topological constraints are constructed. These vectors are continuously injected during the 2000–2500 s interval, ensuring that the measurement residuals remain below traditional detection thresholds while achieving stealthy corruption of the SOC estimation through error accumulation.

The experimental performance is evaluated using a multi-dimensional set of metrics. For FDIA detection, Accuracy, Recall, Precision, and F1 score are adopted. For the predictive reconstruction phase, the performance is assessed via the Coefficient of Determination (R^2), Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and Maximum Error (MAX).

4.1. Experimental Analysis of SOC Estimation Based on EKF

To verify the feasibility of the proposed detection and defense algorithms, SOC estimation simulations under complex operating conditions were conducted for three scenarios: a no-attack baseline, and voltage attacks with intensities of 100 mV and 200 mV. The results are presented in Figures 5 and 6.

Figures 5 and 6 demonstrate that FDIAs severely compromise the state-awareness capabilities of the BMS. Under the 100 mV and 200 mV attacks, the SOC estimation trajectories deviate from the nominal states, with peak errors reaching 8.964% and 12.776%. The system robustness decreases as the attack magnitude increases. These results validate that subtle attacks satisfying physical consistency can be cumulatively amplified by state estimation algorithms, ultimately degrading energy management performance and misleading the EMS into erroneous power allocation decisions. Such deviations may affect the coordinated

operation of onboard energy storage systems and compromise the overall efficiency and reliability of hybrid ship power systems.

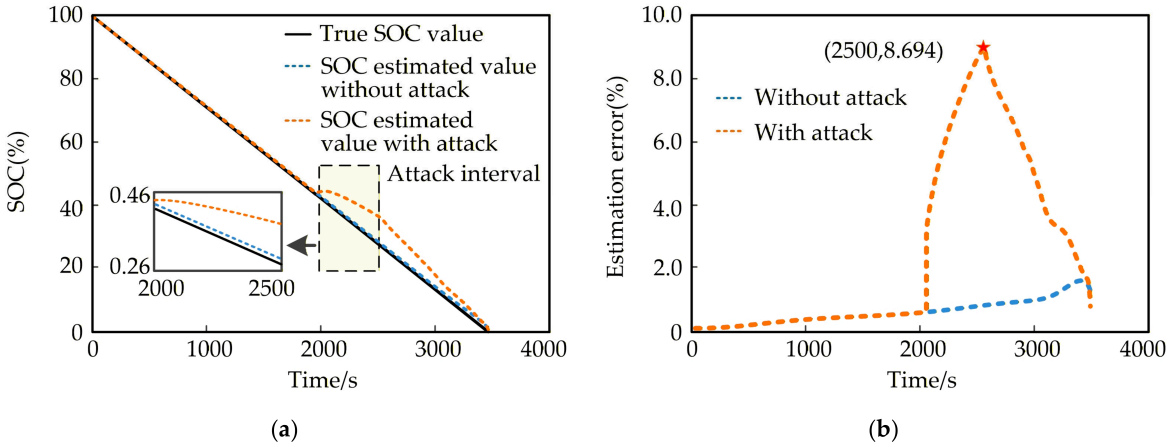


Figure 5. SOC estimation results under a 100 mV voltage attack: (**a**) SOC estimation values; (**b**) SOC estimation errors.

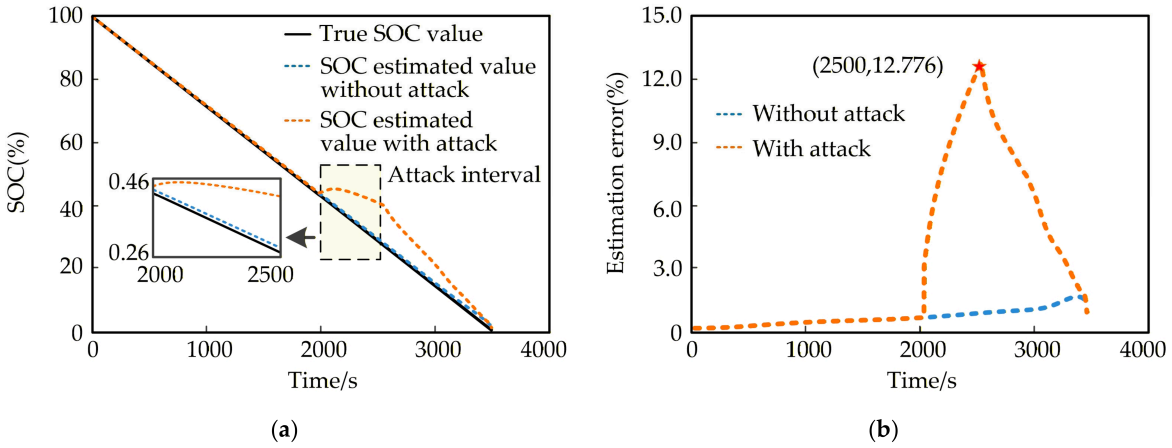


Figure 6. SOC estimation results under a 200 mV voltage attack: (**a**) SOC estimation values; (**b**) SOC estimation errors.

Furthermore, influenced by the recursive nature of the EKF, the estimation errors exhibit a temporal cumulative effect during the attack period, reaching their maximum values at the point of attack termination. Once the attack is withdrawn, the estimation error gradually converges thanks to the corrective action of the Kalman gain, allowing the system to achieve self-healing.

4.2. Experimental Analysis of FDIA Detection

4.2.1. Experimental Parameter Settings

This section evaluates the detection performance of the IF-LSTM algorithm on the FDIA dataset. In the feature engineering stage, the IF algorithm extracts anomaly scores from voltage, current, temperature, and SOC estimates. These scores are fused with the original features, and a sliding window (width = 10) is used to reconstruct samples. The processed data are then fed into the LSTM for binary classification. For IF, all 3421 samples are used for unsupervised scoring, while for IF-LSTM the dataset is split into training and testing sets (7:3), with results reported on the test set for classification. Although the total number of evaluated samples differs due to different learning paradigms, the results follow their standard evaluation protocols and remain comparable in terms of fairness.

Regarding parameter configuration, the IF performance is mainly influenced by the number of isolation trees n and the subsampling size m. In this study, the Area Under the ROC Curve (AUC) is adopted as the evaluation metric to optimize the parameter combinations via grid search. Table 1 presents the detection performance under various parameter combinations. The experimental results indicate that the AUC is closest to 1 when n = 200 and m = 32, representing the optimal anomaly discrimination capability.

Table 1. AUC values under different parameter combinations.

m	*n*				
	50	**100**	**150**	**200**	**250**
16	0.908	0.934	0.932	0.939	0.935
32	0.887	0.867	0.923	0.948	0.900
64	0.912	0.880	0.894	0.892	0.901
128	0.881	0.896	0.906	0.894	0.899
256	0.909	0.905	0.914	0.907	0.893

The experimental configuration employs an LSTM architecture with 5 layers and 20 hidden units per layer to enhance the model's capacity for representing complex dynamic patterns and increase sensitivity to subtle anomalous variations. To mitigate the risk of overfitting and ensure robust generalization, fundamental strategies were implemented during the training phase, including data normalization and the partitioning of datasets into training and testing subsets. A Sigmoid activation function is utilized for binary classification. The network weights are adjusted using the Adam optimizer, with an initial learning rate of 0.01 and a batch size of 128.

4.2.2. Experimental Results of the IF Algorithm

To verify the performance gain of the IF-LSTM compared to the standalone IF algorithm, a comprehensive benchmark test was first conducted on the IF component. The optimal decision thresholds were determined through a systematic dynamic optimization process, and the experimental results are illustrated in Figure 7. Under 100 mV and 200 mV attacks, the optimal thresholds were found to be 0.620 and 0.618, respectively. With this configuration, the algorithm's precision exceeded 0.8 and the recall surpassed 0.95, providing a robust and highly reliable baseline for subsequent comparative performance evaluations and improvements.

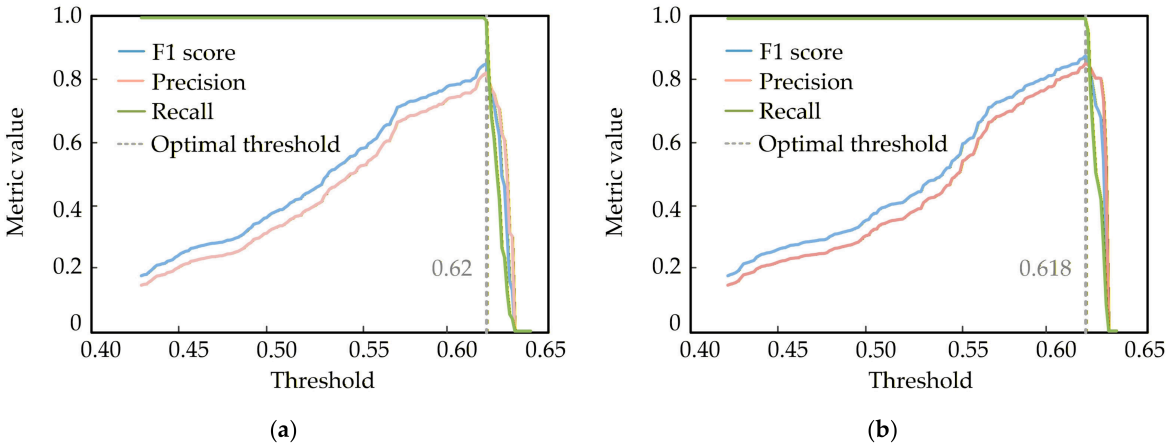


Figure 7. Threshold optimization curves: (**a**) 100 mV attack; (**b**) 200 mV attack.

Based on the selected optimal parameters and thresholds, simulation experiments were conducted. Figure 8 displays the confusion matrices of the IF classification results under

different attack intensities. The IF algorithm successfully identified 489 attack samples under the 100 mV attack, with a miss rate of only 2.40%, demonstrating a potent capacity for attack capture and robust detection capability. Although the detection performance improved further under the 200 mV attack condition, the algorithm exhibited a relatively high overall false alarm rate.

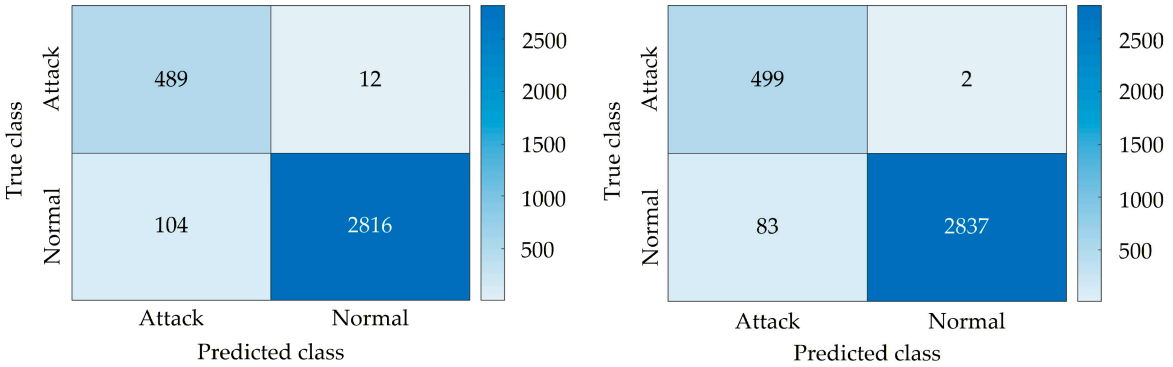


Figure 8. Confusion matrices of the IF algorithm: (**a**) 100 mV attack; (**b**) 200 mV attack.

Figure 9 illustrates the probability density distribution of the anomaly scores. Normal samples are concentrated within the [0.42, 0.60] range, while attack samples are highly clustered between [0.62, 0.64]. The precise segmentation provided by the threshold line further validates the high sensitivity and robustness of the proposed detection algorithm. The experimental results clearly demonstrate that the anomaly scores generated by the IF algorithm possess strong discriminative power, providing critical feature inputs for the subsequent LSTM model and significantly enhancing classification performance.

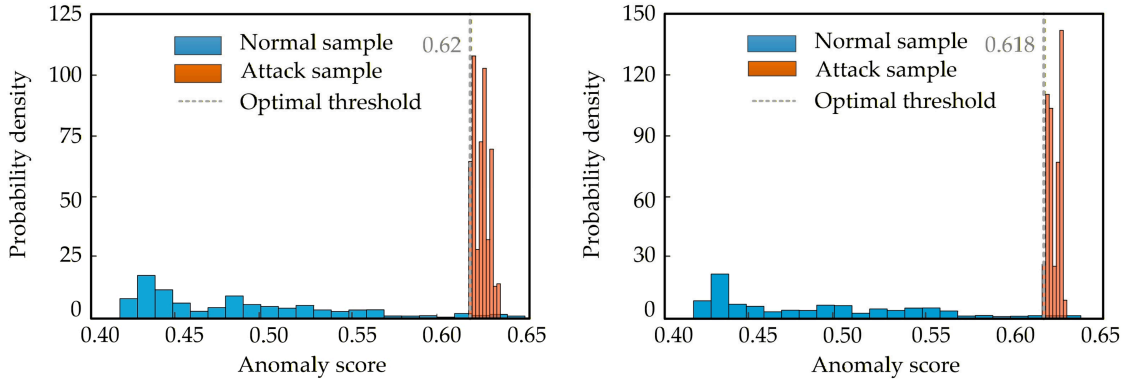
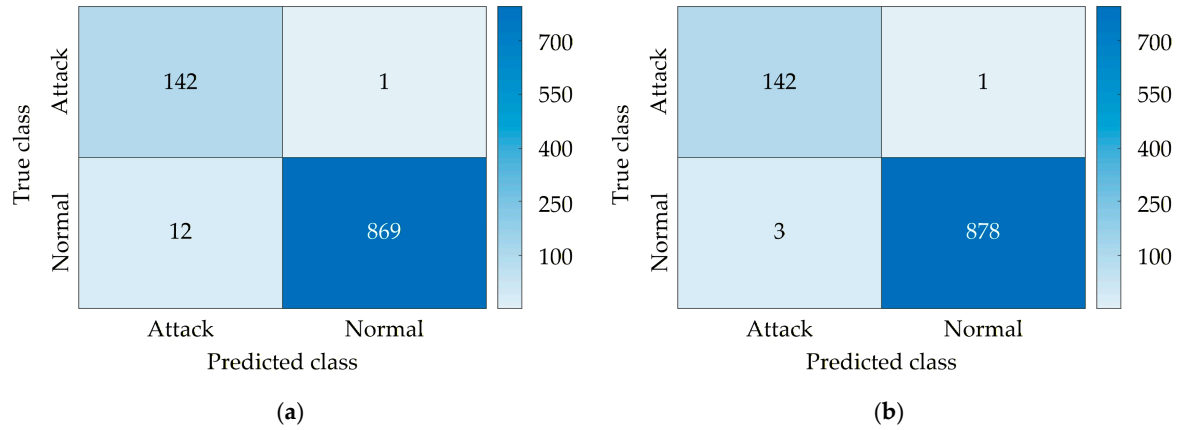


Figure 9. Anomaly score distribution of the IF algorithm: (**a**) 100 mV attack; (**b**) 200 mV attack.

4.2.3. Experimental Results of the IF-LSTM Algorithm

Analysis of the confusion matrices in Figure 10 shows that the proposed IF-LSTM model achieves effective classification performance under both attack intensities, with a low false positive rate and a consistently low miss rate. These results further demonstrate the model's strong capability in accurately identifying stealthy FDIA patterns while maintaining stable detection performance across different attack strengths and scenarios.



(**a**) (**b**)

Figure 10. Confusion matrices of the IF-LSTM algorithm: (**a**) 100 mV attack; (**b**) 200 mV attack.

To further quantify the performance gain and demonstrate the superiority of the proposed framework, Table 2 compares the statistical metrics of the IF-LSTM method with those of the IF and LSTM baselines, which represent unsupervised anomaly detection and supervised sequential learning paradigms, respectively. The comprehensive comparison provides a clear evaluation of the effectiveness, robustness, and generalization capability of the proposed approach under different detection settings and attack scenarios.

Table 2. Evaluation metrics of different detection algorithms.

Detection Algorithm	Attack Value	Accuracy	Precision	Recall	F1 Score	AUC-PR
IF algorithm	100 mV	0.966	0.825	0.976	0.853	0.902
	200 mV	0.975	0.857	0.996	0.881	0.927
LSTM algorithm	100 mV	0.975	0.911	0.920	0.916	0.921
	200 mV	0.980	0.925	0.938	0.932	0.936
IF-LSTM algorithm	100 mV	0.993	0.960	0.993	0.976	0.977
	200 mV	0.996	0.979	0.993	0.986	0.987

As indicated in the table, although the standalone IF algorithm achieves a high recall rate, its lack of temporal modeling and sensitivity to fluctuations lead to lower precision. The standalone LSTM is capable of extracting temporal features; however, it tends to favor the majority class when faced with imbalanced datasets, thereby limiting its recall. In contrast, the proposed IF-LSTM demonstrates significant advantages by leveraging the synergy between spatial anomaly isolation and temporal sequence learning, with all metrics comprehensively surpassing the benchmark models, effectively suppressing both false alarms and missed detections.

The area under the PR curve (AUC-PR) is used as a single scalar metric to further aggregate the precision-recall trade-off, and the calculated AUC-PR values are reported in Table 2 for quantitative comparison, highlighting the overall superiority and stability of the proposed IF-LSTM method.

Analysis of the evolution curves for various evaluation metrics in Figure 11 reveals that all indicators rise rapidly during the initial training phase and stabilize around the 20th epoch. FDIAs with higher intensity exhibit faster convergence rates and superior steady-state accuracy, while lower-intensity attacks show a slight lag but eventually achieve comparably high levels. This fully demonstrates that the proposed method can accurately identify attacks, which is instrumental in bolstering the cyber-resilience of shipboard energy management systems against potential operational disruptions under complex environments.

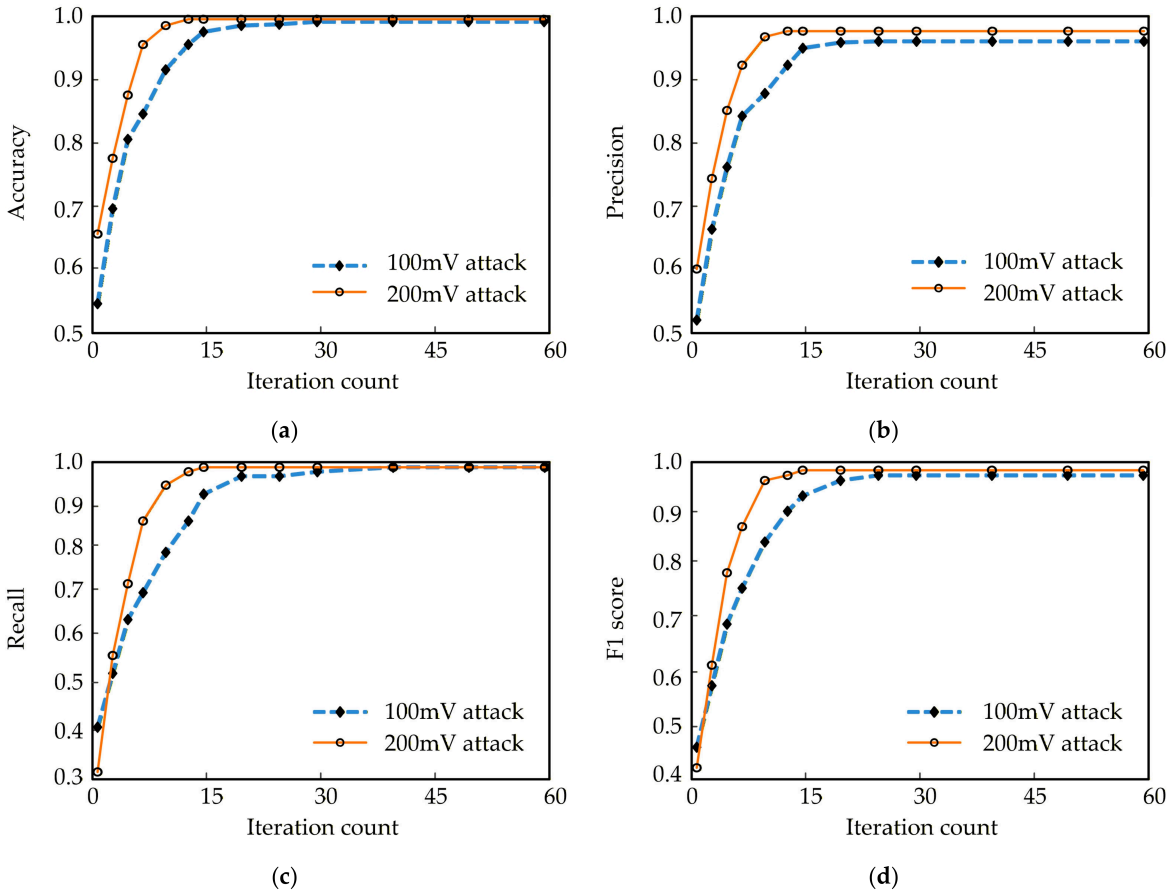


Figure 11. Evolution curves of evaluation metrics for the IF-LSTM: (**a**) Accuracy evolution curve; (**b**) Precision evolution curve; (**c**) Recall evolution curve; (**d**) F1 score evolution curve.

4.3. Experimental Analysis of FDIA Defense

4.3.1. Experimental Parameter Settings

After normalization of the raw sampling set, a sliding window with a width of 10 and a step size of 1 is employed to reconstruct the samples for capturing temporal features and local dynamic patterns effectively. The processed dataset is then partitioned into training and testing sets at a ratio of 7:3. The LSTM architecture is configured with 3 hidden layers, each containing 20 hidden units. The Adam optimizer is utilized for model training, with the initial learning rate and batch size set to 0.001 and 64, respectively, ensuring stable and efficient convergence.

4.3.2. Experimental Results of the Defense Algorithm

To further verify the comprehensive effectiveness of the proposed defense method, simulation experiments were specifically designed to evaluate the numerical discrepancy between predicted and ground-truth values. Figure 12 clearly illustrates the prediction results of the LSTM model on the testing set.

According to Figure 12a, the predicted curve fits the original ground-truth values with high fidelity, indicating that the model precisely captures the nonlinear evolution patterns of battery voltage and possesses reliable sequence reconstruction capabilities. The error curve in Figure 12b demonstrates that the majority of residual fluctuations are confined within 0.01 V. A slight increase in error, reaching a maximum of approximately 0.025 V, occurs only at the end of the sequence where the voltage drops sharply. However, relative to the nominal voltage of 4.2 V, such a deviation has a negligible impact on SOC estimation.

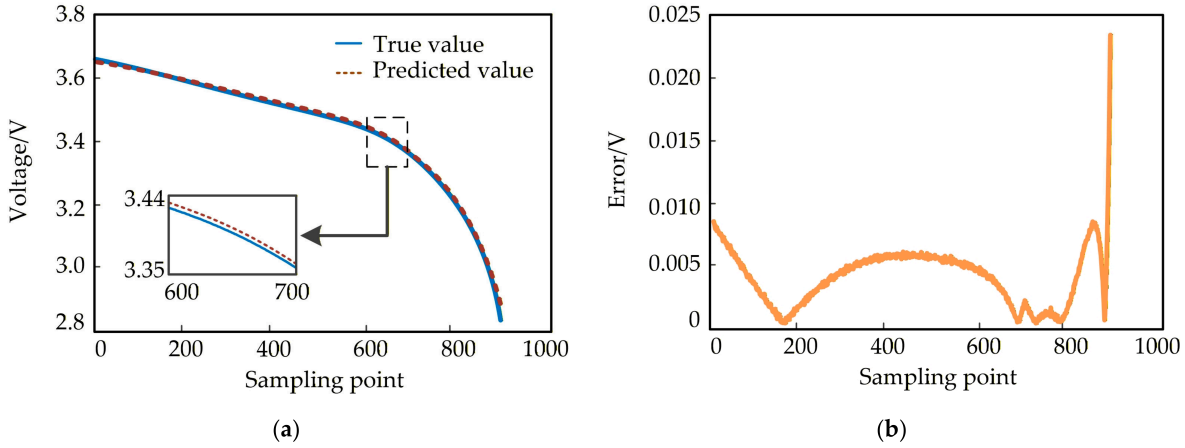


Figure 12. Prediction results based on the LSTM neural network: (**a**) Predicted voltage values vs. ground-truth values; (**b**) Voltage prediction errors.

To further validate the FDIA defense performance of the LSTM network, a comparison was conducted among SOC estimation results under three conditions: no-attack baseline, undefended attacks of varying intensities, and attacks with the proposed defense. The results are shown in Figure 13.

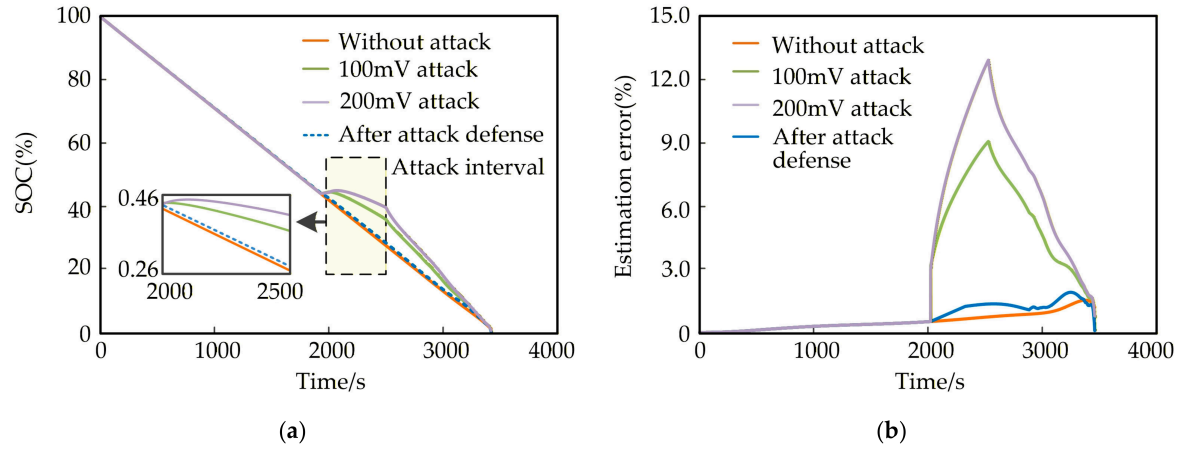


Figure 13. Comparison of SOC estimation results before and after defense under the Oxford dataset: (**a**) SOC estimation values; (**b**) SOC estimation errors.

As illustrated in Figure 13, without defensive measures, FDIAs cause the SOC estimates to deviate severely from the ground-truth values, with errors rising significantly as the attack intensity increases. Upon introducing the temporal reconstruction defense strategy based on LSTM, the SOC estimation error is effectively suppressed to within 2%, maintaining an accuracy level consistent with the no-attack condition. This clearly validates the effectiveness of the scheme in ensuring the data security of the BMS.

By implementing adaptive restoration of state information, this defense strategy prevents irrational operational policies, such as overcharging or overdischarging, that may be triggered by SOC estimation errors. Consequently, it mitigates operational risks and enhances the continuity and stability of the EMS and power allocation processes within complex network environments. It should be noted that this study does not directly model battery thermal runaway; instead, by improving state estimation reliability and reducing risks associated with erroneous decision-making, it indirectly enhances the operational safety and reliability of hybrid ship power systems.

4.4. Experimental Analysis of Power Deviation and Energy Efficiency

4.4.1. Simulation Methods and Strategies

To evaluate the impact of FDIA detection and defense on the operational performance of shipboard power systems, this study performs a quantitative analysis of the transmission mechanism from SOC estimation errors to power allocation and energy utilization efficiency. In hybrid electric ships, the EMS typically coordinates power allocation between the energy storage system and generators according to the battery SOC in order to achieve storage protection and optimized energy utilization efficiency. When the SOC estimation is affected by FDIA, erroneous state information may cause the EMS to misjudge the remaining capacity of the energy storage system, thereby leading to deviations in battery power allocation from normal operating conditions. This further results in additional energy consumption and degradation of overall energy utilization efficiency.

It should be clarified that, rather than constructing a complete shipboard power system model, a simplified energy management analysis framework [32] is adopted to highlight the direct influence of SOC errors on power scheduling. Specifically, drawing upon the fundamental principles of SOC-based power distribution in NES, the battery output power is assumed to be a functional mapping of the SOC to characterize how SOC fluctuations affect scheduling. The basic principle is that when the SOC is relatively high, the EMS tends to increase the output power of the energy storage system so that it can undertake a larger proportion of dynamic loads. In contrast, when the SOC is relatively low, the system actively reduces the battery output power in order to prevent over-discharge and ensure the operational safety of the energy storage system.

To minimize interference from complex system variables, the load is described using a normalized dynamic model, reflecting power demand variations under typical operating conditions [33]. On this basis, the power deviation is defined as the relative error of the battery output power under different operating conditions with respect to the battery output power under the true SOC condition. The energy loss is obtained by integrating the cumulative effect of the power deviation over the attack-affected interval, which is used to characterize the additional power regulation overhead caused by FDIA and its impact on the energy utilization efficiency of the system.

4.4.2. Experimental Results

As indicated by the combined data in Table 3 and Figure 14, the system exhibits minimal power deviation under no-attack conditions, with a maximum deviation of 10.68% and an average deviation of 1.68%. However, the introduction of malicious FDIAs leads to a significant escalation in power deviation across the network. Specifically, a 100 mV attack results in a maximum power deviation of 22.74%, which further climbs to 32.41% under a 200 mV attack, demonstrating a clear amplification trend relative to attack intensity. Upon implementing the proposed defense strategy, the power deviation is substantially reduced, effectively returning to stable baseline levels observed in the absence of attacks. This decisively underscores the effectiveness of the methodology at the systemic level.

Table 3. Metric values of power deviation and energy loss results.

Metric Value	Without Attack	100 mV Attack	200 mV Attack	After Attack Defense
Maximum power deviation	10.68%	22.74%	32.41%	10.48%
Average power deviation	1.68%	7.14%	9.27%	2.20%
Energy loss	−0.72%	−3.16%	−4.09%	−0.95%

Furthermore, an assessment of energy loss within the attack interval was conducted. As shown in Figure 15 and Table 3, a 100 mV attack causes approximately 3.2% energy

loss, which expands to roughly 4.1% under a 200 mV attack. In contrast, with the defense strategy in place, energy loss is suppressed to below 1%, approaching no-attack levels.

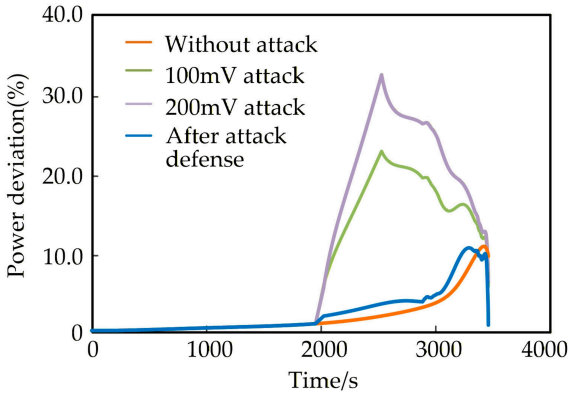


Figure 14. Power deviation comparison curves under the Oxford dataset.

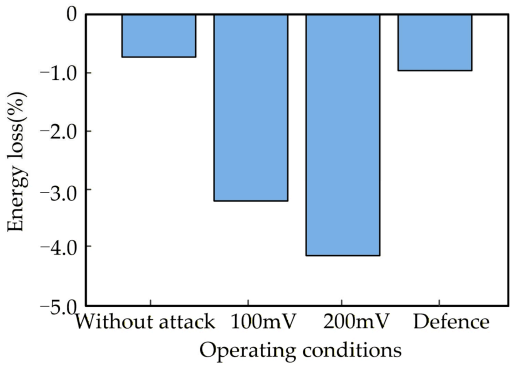


Figure 15. Comparison of energy loss under the Oxford dataset.

In summary, FDIAs induce power allocation biases by perturbing SOC estimation results, which subsequently degrade energy efficiency and increase operational costs. The proposed method not only restores the accuracy of SOC estimation but also effectively mitigates power deviations and energy losses, thereby enhancing the operational efficiency, reliability, and cyber-resilience of hybrid ship power systems.

4.5. Case Study of a Typical Hybrid Electric Ship Scenario

4.5.1. Simulation of Ship Dynamic Load Conditions

To further verify the engineering applicability of the proposed detection and defense method in practical ship operating scenarios, an energy management analysis case under the Dynamic Positioning (DP) condition of a typical hybrid electric ship is constructed in this study. Under DP operating conditions, the ship continuously adjusts the thruster output to resist ocean currents, waves, and external disturbances in order to maintain the target position and attitude stability. Therefore, the propulsion load generally exhibits continuous fluctuations and frequent dynamic variations. Under this operating mode, the energy storage system frequently participates in power regulation, and the SOC information directly affects EMS power allocation among onboard energy sources, thereby influencing the operational efficiency of the hybrid ship power system in real time.

To focus on the impact of cyberattacks on energy management performance, the ship load is represented using a normalized dynamic load model. Dynamic disturbances with different frequencies and amplitudes are constructed in different stages to simulate propulsion load variations under different sea conditions during DP operation [33], as shown in Figure 16. Specifically:

- The period from 0 s to 1000 s corresponds to a low dynamic steady-state operating condition;
- The period from 1000 s to 2000 s corresponds to a medium disturbance operating condition;
- The period from 2000 s to 3000 s introduces high-frequency dynamic disturbances to simulate the frequent regulation state of the propulsion system under complex sea conditions;
- After 3000 s, the system gradually returns to a relatively stable operating condition.

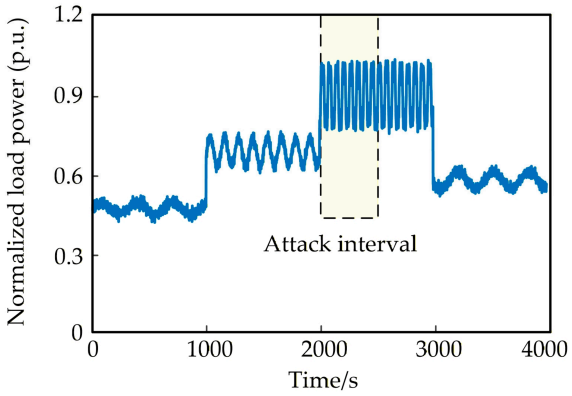


Figure 16. Load profile under the dynamic positioning operating condition.

4.5.2. Experimental Result Analysis

As shown in Figure 17, FDIA significantly increases the SOC estimation error, which exhibits a continuous accumulation trend during the attack period. Under the proposed detection and defense mechanism, the SOC estimation error is effectively suppressed, and the estimation result gradually approaches the level under normal operating conditions without attack. This demonstrates that the proposed method enhances the robustness of SOC estimation and improves the operational stability of the hybrid ship energy management system against FDIA.

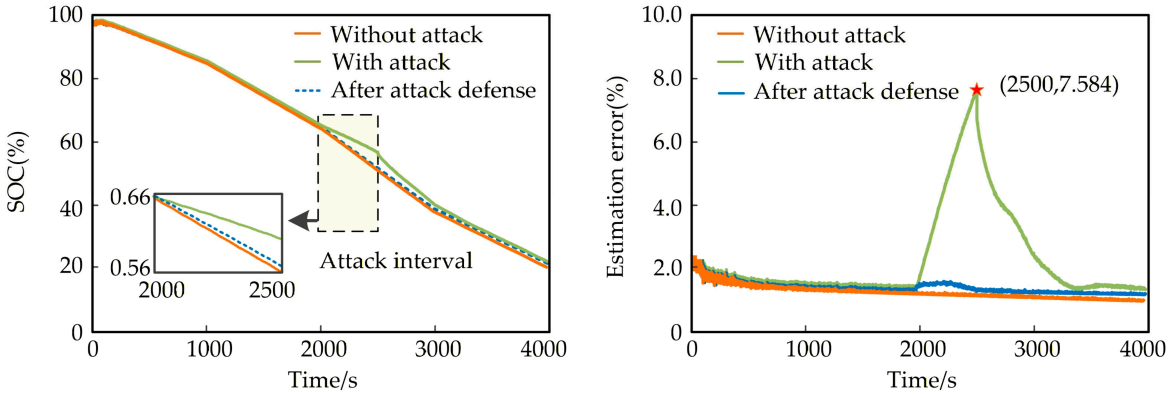


Figure 17. Comparison of SOC estimation results before and after defense under DP operating conditions: (**a**) SOC estimation values; (**b**) SOC estimation errors.

Figures 18 and 19 present the comparisons of power deviation and energy loss, respectively. Under attack conditions, erroneous SOC information distorts EMS power allocation decisions, causing the battery output power to deviate from its scheduled operating point and increasing system energy loss. In contrast, after the defense strategy is applied, the power deviation is significantly reduced, and the energy loss is restored to a level close to that under normal operating conditions.

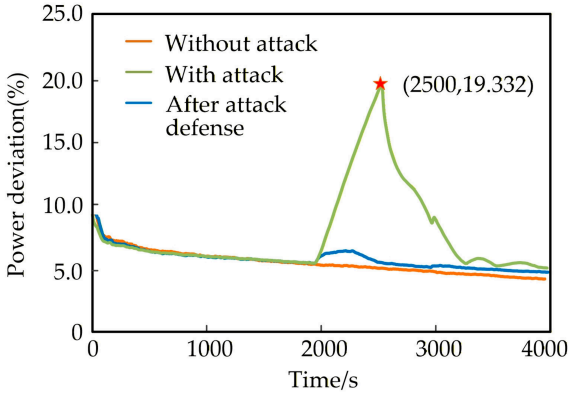


Figure 18. Power deviation comparison curves under DP operating conditions.

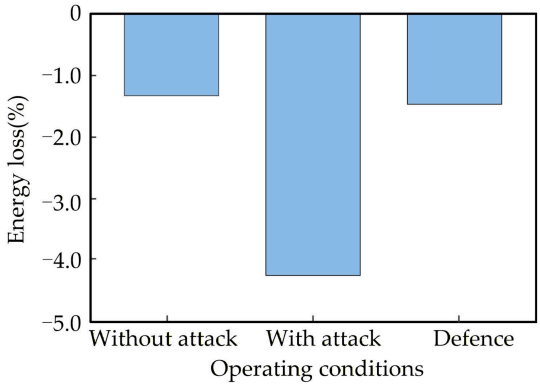


Figure 19. Comparison of energy loss under DP operating conditions.

The experimental results demonstrate that the proposed method effectively mitigates the impact of FDIA on EMS power allocation and enhances the operational stability, energy management reliability, and cyber-resilience of hybrid ship power systems under complex network environments.

It is noteworthy that, in practical deployment, the detection framework may inevitably encounter false positives, false negatives, or unnecessary reconstruction of normal measurements. Missed detections may lead to temporary deviations in SOC estimation, while false alarms may trigger unnecessary reconstruction of normal measurements. However, since the proposed LSTM-based reconstruction model learns the temporal evolution patterns under normal operating conditions, its predictions under nominal scenarios generally remain highly consistent with the true system states, thereby mitigating the impact of false alarms on SOC estimation accuracy.

5. Conclusions

This study addresses the critical issue of stealthy FDIA facing shipboard BMS in intelligent connected environments by constructing a "modeling-detection-defense" closed-loop security framework centered on battery SOC. Based on the battery equivalent circuit model, an FDIA mathematical model was established, revealing the recursive amplification effect of physically consistent, subtle measurement tampering through state estimation algorithms and its subsequent impact on shipboard energy management decisions. An IF-LSTM-based detection algorithm was proposed, and experimental results demonstrate that this model significantly outperforms standalone benchmark algorithms under varying attack intensities. Building upon this, an LSTM-based temporal model was introduced to perform prediction-based reconstruction of corrupted data, effectively reducing the post-attack SOC estimation error from approximately 10% to within 2%.

At the systemic level, the influence of SOC errors on EMS power allocation and energy efficiency was analyzed using a simplified energy management model. The results indicate that FDIAs induce significant power deviations and cause an energy loss of approximately 4%; however, with the integration of the proposed methodology, power deviations are markedly reduced, and energy loss is curtailed to within 1%, approaching no-attack baseline levels. In addition, the experimental results under the dynamic positioning operating condition of a typical hybrid electric ship demonstrate that the proposed method can effectively suppress the propagation of SOC estimation errors caused by FDIA, reduce power deviation and energy loss, and verify its engineering applicability in practical ship operating scenarios.

In conclusion, the proposed framework effectively identifies and defends against FDIAs. It not only ensures the data integrity of the BMS but also significantly mitigates power scheduling biases caused by SOC misestimation, thereby enhancing the cyber-resilience, operational reliability, and energy efficiency of hybrid ship power systems under cyber-attack environments. These findings provide useful insights for the secure operation of battery energy storage systems and energy management systems in next-generation hybrid electric ships. Future work will investigate cross-battery, cross-cycle, cross-operating-condition, and unseen attack generalization to further evaluate the generalization capability of the proposed method.

Author Contributions: Conceptualization and Project administration: H.S.; Data curation: M.G.; Investigation and Resources: T.Y.; Software and Writing—original draft: N.L.; Writing—review & editing: J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors would like to thank the anonymous reviewers for their insightful and valuable comments, which have significantly helped to improve the quality and clarity of this manuscript.

Conflicts of Interest: M.G. was employed by State Grid Zhejiang Electric Power Co., Ltd. J.W. was employed by Unicompound Semiconductor Corporation. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

Abbreviation	Full Name
NES	New Energy Ships
BMS	Battery Management System
BESS	Battery Energy Storage System
EMS	Energy Management System
PMS	Power Management System
FDIA	False Data Injection Attack
SOC	State of Charge
SOH	State of Health
ECM	Equivalent Circuit Model
RC Model	Resistance-Capacitance Model
IF	Isolation Forest
LSTM	Long Short-Term Memory
EKF	Extended Kalman Filter
RMSE	Root Mean Square Error

MAX	Maximum Error
MAE	Mean Absolute Error
AUC	Area Under the ROC Curve
Symbol	**Description**
R^2	Coefficient of Determination
U_{OCV}	Open-Circuit Voltage
U	Terminal Voltage
I	Discharge Current
R_0	Ohmic Resistance
T	Sampling Interval;
η	Coulombic Efficiency
Q_c	Rated Capacity of the Battery
$\boldsymbol{x}$	State Vector
$\boldsymbol{P}$	State Error Covariance Matrix
$\boldsymbol{Q}$	Process Noise Covariance Matrix
$\boldsymbol{K}$	Kalman Gain Matrix
$\boldsymbol{z}$	Data Measured
$\boldsymbol{H}$	Jacobian Matrix
$\boldsymbol{e}$	Measurement Error Vector.
$\boldsymbol{a}$	Attack Vector
$\boldsymbol{c}$	State Deviation Vector
$\sum_e$	Covariance Matrix of the Error Vector
r	Residual
f_t	Forget Gate
$\boldsymbol{W}$	Weight Matrices
$\boldsymbol{b}$	Bias Terms;
X_t	Input Data
h_t	Hidden State
σ	Sigmoid Function
C_t	Current Cell State
$\widetilde{C}_t$	Candidate Cell State
i_t	Input Gate
o_t	Output Gate

Appendix A

Table A1. Oxford battery dataset information.

Item	Value
Voltage range	2.7 V–4.2 V
Charge current	1.48 A
Discharge current	0.74 A
Temperature	40 °C
Nominal capacity	740 mAh

References

1. Zhao, Y.X.; Wen, S.L.; Zhao, Q.; Zhang, B. Deep reinforcement learning-based energy management strategy for green ships considering photovoltaic uncertainty. *J. Mar. Sci. Eng.* **2025**, *13*, 565. [CrossRef]
2. Pan, P.; Sun, Y.; Yuan, C. Research progress on ship power systems integrated with new energy sources: A review. *Renew. Sustain. Energy Rev.* **2021**, *144*, 111048. [CrossRef]
3. Lucà Trombetta, G.; Leonardi, S.G.; Aloisio, D. Lithium-ion batteries on board: A review on their integration for enabling the energy transition in shipping industry. *Energies* **2024**, *17*, 1019. [CrossRef]

4. Mishra, P.; Singh, G. Energy management systems in sustainable smart cities based on the internet of energy: A technical review. *Energies* **2023**, *16*, 6903. [CrossRef]
5. Munsi, M.S.; Chaoui, H. Energy management systems for electric vehicles: A comprehensive review of technologies and trends. *IEEE Access* **2024**, *12*, 60385–60403. [CrossRef]
6. Murlidharan, S.; Ravulakole, V.; Karnati, J. Battery management system: Threat modeling, vulnerability analysis, and cybersecurity strategy. *IEEE Access* **2025**, *13*, 37198–37220. [CrossRef]
7. Naseri, F.; Kazemi, Z.; Larsen, P.G. Cyber-physical cloud battery management systems: Review of security aspects. *Batteries* **2023**, *9*, 382. [CrossRef]
8. Xu, S.; Liu, Z.Y.; Li, Y.C. Research on intelligent detection methods for false data injection attacks on battery energy storage systems. *Proc. CSEE* **2023**, *43*, 6628–6639.
9. Qin, Y.; Luo, Z.; Che, Y. False data injection attacks against UAV battery state of health estimation with a capacity-informed latent diffusion model. *Green Energy Intell. Transp.* **2026**, 100404. [CrossRef]
10. Habib, A.K.M.A.; Hasan, M.K.; Alkhayyat, A. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. *Comput. Electr. Eng.* **2023**, *107*, 108638. [CrossRef]
11. Lu, P.; Fu, H.; Lu, W.J. Detection of false data injection attacks for VRB energy storage systems based on long- & short-term memory and generative adversarial networks. *Power Syst. Technol.* **2024**, *48*, 383–393.
12. DNV. *DNV-RP-0496: Cyber Security Resilience Management for Ships and Mobile Offshore Units*; DNV: Høvik, Norway, 2016.
13. IMO. *Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems*; IMO: London, UK, 2017.
14. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2020**, *11*, 2218–2234.
15. Liu, Z.T.; He, H.W. Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended kalman filter. *Appl. Energy* **2017**, *185*, 2033–2044. [CrossRef]
16. Francisco, J.; Montáns, F.C.; Chinesta, F. Data-driven modeling and learning in science and engineering. *Comptes Rendus Mécanique* **2019**, *347*, 845–855. [CrossRef]
17. Ahmed, S.; Lee, Y.D.; Seung-Ho, H. Unsupervised machine learning—Based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777.
18. Li, X.P.; Wang, Y.K.; Lu, Z.G. Graph-based detection for false data injection attacks in power grid. *Energy* **2023**, *263*, 125865.
19. Zhang, G.; Li, J.; Bamisile, O. A data driven threat-maximizing false data injection attack detection method with spatio-temporal correlation. In *Proceedings of the IEEE/IAS Industrial and Commercial Power System Asia*; Chengdu, China, 18–21 July 2021, IEEE: New York, NY, USA; pp. 318–325.
20. *IEC 60870-5-104*; Telecontrol Equipment and Systems—Part 5-104: Transmission Protocols—Network Access for IEC 60870-5-101 Using Standard Transport Profiles. International Electrotechnical Commission: Geneva, Switzerland, 2006.
21. *IEC 61162-1*; Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces—Part 1: Single Talker and Multiple Listeners. International Electrotechnical Commission: Geneva, Switzerland, 2016.
22. Naseem, H.; Hadi, A.; Kang, M.J. Enhancing energy storage efficiency: Advances in battery management systems in electric vehicles. *Energy Technol.* **2025**, *13*, 2500100. [CrossRef]
23. Ahmed, F.; Abulsaud, K.; Massoud, A.M. On equivalent circuit model-based state-of-charge estimation for lithium-ion batteries in electric vehicles. *IEEE Access* **2025**, *13*, 69950–69966.
24. Chen, Z.; Fu, Y.; Mi, C.C. State of charge estimation of lithium-ion batteries in electric drive vehicles using extended Kalman filtering. *IEEE Trans. Veh. Technol.* **2013**, *62*, 1020–1030.
25. Wang, C.; Li, R.; Cao, Y.; Li, M. A hybrid model for state of charge estimation of lithium-ion batteries utilizing improved adaptive extended Kalman filter and long short-term memory neural network. *J. Power Sources* **2024**, *620*, 235272.
26. He, Z.; Yang, Z.; Cui, X.; Li, E. A method of state-of-charge estimation for EV power lithium-ion battery using a novel adaptive extended Kalman filter. *IEEE Trans. Veh. Technol.* **2020**, *69*, 14618–14630.
27. Al-Gabalawy, M.; Hosny, N.S.; Dawson, J.A.; Omar, A.I.; Xiao, W. State of charge estimation of a Li-ion battery based on extended Kalman filtering and sensor bias. *Int. J. Energy Res.* **2020**, *45*, 6708–6726.
28. Al-Shehari, T.; Al-Razgan, M.; Alfakih, T. Insider threat detection model using anomaly-based isolation forest algorithm. *IEEE Access* **2023**, *11*, 118170–118185. [CrossRef]
29. Ren, X.Q.; Liu, S.L.; Yu, X.D. A method for state-of-charge estimation of lithium-ion batteries based on PSO-LSTM. *Energy* **2021**, *234*, 121236.
30. Kesici, M.; Pal, B.; Yang, G. Detection of false data injection attacks in distribution networks: A vertical federated learning approach. *IEEE Trans. Smart Grid* **2024**, *15*, 5952–5964. [CrossRef]
31. Howey, D.; Birkl, C. *Oxford Battery Degradation Dataset 1*; University of Oxford: Oxford, UK, 2017.

32. Andrus, M.; Bosworth, M.; Crider, J. *Notional System Models*; Electric Ship Research and Development Consortium: Arlington, VA, USA, 2013.
33. Bui, T.M.N.; Dinh, T.Q.; Marco, J. Development and real-time performance evaluation of energy management strategy for a dynamic positioning hybrid electric marine vessel. *Electronics* **2021**, *10*, 1280. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.