PCA-Optimized SVM Framework for Detecting False Data Injection Attacks in Battery Energy Storage Systems

Dangli Wang
Hebei Vocational University of Technology and Engineering, Xingtai 054000 China
E-mail: abc82024@126.com

Keywords: false data injection attacks (FDIAs); support vector machines (SVMs); detection mechanism; cyber attacks; battery energy storage systems (BESSs)

Received: July 7, 2025

False Data Injection Attacks (FDIAs) pose a significant threat to the reliability of Battery Energy Storage Systems (BESS) in smart grids. This paper proposes a PCA-optimized Support Vector Machine (SVM) detection framework specifically designed for BESS. First, we model the impact of FDIAs on BESS operations, demonstrating how such attacks can manipulate state-of-charge, power output, and grid frequency to disrupt system efficiency and stability. Key operational indicators, including voltage, current, and power, are used for an extensive feature extraction process, after which Principal Component Analysis (PCA) is applied to select the most informative features and improve classification efficiency. The proposed framework is evaluated through comprehensive simulations, achieving a detection accuracy of 98.5%, precision of 97.8%, recall of 98.2%, and an F1-score of 98.0%. The confusion matrix and ROC curve confirm the robustness of the model, showing minimal false positives and false negatives. These results demonstrate that the proposed PCA-optimized SVM framework provides an effective and computationally efficient solution for mitigating FDIAs in BESS and strengthens the security foundation of future smart grids.

Povzetek: Članek predlaga PCA-optimiziran SVM za zaznavanje napadov z lažnim vbrizgom podatkov v BESS, ki iz operativnih kazalnikov izlušči značilke, s PCA izbere informativne komponente in tako učinkovito ter računsko varčno okrepi varnost pametnega omrežja..

1 Introduction

During the last couple of years, battery energy storage systems have contributed much toward the smartening of smart grids by effectively improving their energy distribution: flexible, reliable, and efficient. BESSs play a crucial role in load leveling, frequency regulation, and backup power supply during an outage.[1], [2], [3], [4] On the contrary, their ever-increasing use of sophisticated and interconnected topologies has made them vulnerable to all kinds of cyberattacks, the most alarming of which are FDIAs. Attacks of false data injection involve an intentional manipulation of measurement data with the goal of misleading the state estimation processes of the underlying system, potentially leading to incorrect operational decisions with severe consequences [5],[6]. Valid data in a timely manner greatly influences the reliability and security of the BESS through its monitoring and control.

Early research on FDIA detection primarily relied on statistical methods [7]–[10]. These techniques include state estimation and residual analysis, where Weighted Least Squares (WLS) estimators use measurement data to estimate the system state. Residuals, calculated as the deviation between actual and estimated values, are then analyzed to detect anomalies. Liu et al. [8] present a state-estimation-based fault diagnosis framework for FDIA detection, demonstrating the applicability of residual monitoring in identifying abnormal data. While statistical approaches are foundational, their effectiveness diminishes against stealthy attacks that can closely mimic normal measurement patterns, which has encouraged the shift towards machine learning approaches.

Machine learning (ML) methods have emerged as powerful alternatives due to their capability to detect complex patterns and nonlinear relationships in large datasets. Techniques such as neural networks, decision trees, and Support Vector Machines (SVMs) have been extensively applied to FDIA detection [11]–[15]. He and Huan [12] introduce a deep learning model trained on historical measurement data that effectively detects FDIA events in power systems. Zhang et al. [13] employ a Random Forest classifier for FDIA detection in smart grids, achieving high accuracy and robust performance against various types of attacks. SVMs, which are well-suited for binary classification problems, are also widely used. Li et al. [14] adopt an SVM-based detection model and report high accuracy in separating normal and attack data in power system environments.

Beyond SVM-based methods, recent non-SVM machine learning approaches have further advanced FDIA detection for BESS. Kharlamova et al. [16] review AI-driven FDIA detection strategies, emphasizing the role of deep learning and hybrid models in improving anomaly detection in BESS. Liu et al. [17] propose an improved Moving Target Defense (IMTD) method that dynamically alters grid parameters, such as reactance and inductance, to expose stealthy FDIAs while minimizing operational costs. Liu et al. [18] also introduce NPformer, a transformer-based deep learning model, which achieves approximately 97% detection accuracy for static FDIAs on BESS state-of-charge estimation. Xu et al. [19] extend this work by presenting GPformer, a graph-enhanced transformer that identifies sequential FDIA patterns, coupled with a temporal reconstruction module that restores compromised data, significantly reducing post-attack estimation errors. Moreover, Mohammed et al. [20] develop a dual-hybrid intrusion detection system combining CNN and LSTM networks with feature selection optimization, achieving superior detection accuracy in power system FDIA scenarios, with strong adaptability to BESS environments.

Hybrid frameworks also offer an effective strategy to enhance FDIA detection by combining complementary techniques [21]–[25]. Xie et al. [22] propose a hybrid model that integrates state estimation with machine learning classifiers, improving detection accuracy by using residual-based pre-screening followed by classification validation. Similarly, Nguyen et al. [23] develop a data fusion approach that consolidates information from multiple sensors and applies machine learning to achieve higher detection accuracy.

Although existing studies have made progress in FDIA detection, we identified two main gaps that our proposed PCA-optimized SVM framework addresses:

- **Insufficient feature optimization in existing machine learning models:** Most prior works rely on raw or manually selected features, which may include redundant or irrelevant information. Our method applies PCA to extract the most informative features, improving detection accuracy and computational efficiency.
- **Lack of targeted BESS-specific FDIA detection frameworks:** Many FDIA detection methods focus on general smart grid data rather than BESS-specific characteristics. Our framework is designed for BESS data, leveraging operational features such as SoC, voltage, and current to deliver more relevant and effective detection.

Our proposed PCA-optimized SVM framework addresses the identified research gaps by offering the following **main contributions and novelties**:

- **PCA-optimized SVM framework for FDIA detection in BESS:** We develop a novel detection framework that integrates Principal Component Analysis (PCA) with an SVM classifier. PCA eliminates redundant features while retaining the most informative components, enabling more accurate and computationally efficient detection of FDIAs in high-dimensional BESS data.
- **BESS-specific, interpretable, and efficient detection approach:** Unlike general grid-level FDIA detection methods, our framework is designed specifically for BESS by utilizing operational features such as state-of-charge (SoC), voltage, and current. This targeted design enhances the detection relevance and robustness for BESS while maintaining lower computational complexity compared to deep learning-based approaches, making the method more practical for real-world smart grid applications.

We organize the rest of the paper as follows: Section II provides an in-depth overview of the structure and formulation of FDIAs in BESSs, along with detailed mathematical models and attack scenarios. Section III: Detection Based on Support Vector Machines provides a description of the proposed SVM-based detection approach. The process begins with data preprocessing, followed by feature extraction, the training model, the theoretical foundation of the SVMs, and ends with the selection of kernel functions and the optimization of hyperparameters. Section IV: Simulation and Results describe in detail the experimental setup, including sources of data, simulation environments, and evaluation metrics. The section then presents a detailed analysis of the results, highlighting the strengths and weaknesses of the proposed method and comparing it to existing detection techniques. Section V: Conclusion outlines the research findings, underscoring that robust FDIA detection mechanisms are critical for BESS security, and provides a recommendation for future research on evolving detection methodologies to continuously adapt to newly devised attack methods.

2 Structure of FDIAs on energy storage systems

In such scenarios, FDIAs targeting BESSs rely on forms of weak SoC estimation. In these scenarios, attacks orchestrate data inputs that feed into the SoC estimation process, resulting in erroneous reporting of SoC values. This section focuses on the formation and structure of FDIAs, utilizing critical mathematical modeling and methodology.

2.1 Modeling for SDNs with integrated BESSs

In integrated SDNs with BESSs, several modeling aspects must be considered in order to understand and detect FDIAs. The system model typically consists of a network's electrical and communication infrastructure, along with BESS controllers and measurement systems. For the SDN that integrates the BESSs, the system state vector x is defined as follows:

$$\mathbf{x} = [|V|_{abc}, \theta_{abc}]^T \tag{1}$$

Where $|V|_{abc}$ represents the magnitudes and θ_{abc} represents the phase angles of all bus voltages, including the VSC AC and DC-side voltages. The measurement vector **z** is given by:

$$\boldsymbol{z} = [|V|, |I|, \theta, P, Q, V_{dc}, I_{dc}, |V|_{ac}, |I|_{ac}, P_{ac}, Q_{ac}, m, \Delta\theta]^T \tag{2}$$

These measurements relate to the system state x through a nonlinear function h(x), such that:

$$z = h(x) + \delta \tag{2}$$

where δ represents independent random measurement noises following a normal distribution with zero means. The current injections I_{abc} are related to bus voltages V_{abc} by the nodal admittance matrix Y_{abc}:

$$\mathrm{I}_{abc} = \mathrm{Y}_{abc}\mathrm{V}_{abc} \tag{3}$$

The diagonal and off-diagonal entries of Y_{abc} are calculated as:

$$Y_{ii}^{abc} = \sum_{j\in A_i} \left(y_{ij}^{abc} + y_{ij}^{s}\right) \text{ and } Y_{ij}^{abc} = Y_{ji}^{abc} = -y_{ij}^{abc} \tag{4}$$

where A_i is the set of buses adjacent to bus i. The VSC is modeled using control variables m_{abc} and phase displacement angles $\Delta\theta_{abc}$. The voltage magnitude in phase α and the phase angle difference are given by:

$$m_\alpha = \sqrt{2}|V|_{\alpha m}V_{dc},\ \Delta\theta_{\alpha pm} = \theta_{\alpha m} - \theta_{\alpha p} \tag{5}$$

Additionally, the power balance equation for a lossless VSC is expressed as:

$$\sum_{\alpha=\{a,b,c\}} P_{\alpha mp} + \left(|I|_{\alpha mp}\right)^2 R_{ac} + V_{dc}I_{dc} + V_{dc}^2 R_{dc} = 0 \tag{6}$$

where $P_{\alpha mp}$ and $I_{\alpha mp}$ relate to V_m^{abc} and V_p^{abc} through the admittance matrix Y_{mp}^{abc}.

2.2 Structure of FDIAs against SoC estimation

FDIAs target the SoC estimation of BESSs by manipulating measurements. The following principles outline the FDIA construction. An FDIA can be represented by an attack vector **a** added to the measurement vector:

$$z_a = z + a \tag{7}$$

The design of the generated fake data should allow it to effortlessly evade all Bad Data Detection schemes within DSSE. It accomplishes this by driving the modified residuals, r_a, to appear similar to normal measurement noise. The solution for the optimal sequence of FDIAs involves solving a linear programming problem at regular intervals during the attack period. We perform this step-by-step FDIA formulation by minimizing the chances of detection, while causing maximum distortion in the SoC estimate. In DSSE, the residual r is defined as:

$$\mathrm{r} = \mathrm{z} - \mathrm{h(x)} \tag{8}$$

Under normal conditions, r follows the chi-square distribution with a certain degree of freedom. To avoid detection, FDIAs strive to stay within the acceptable threshold. With real-time measurements, the EKF estimates BESSs' SoC. The state update equations for the EKF are given by:

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k\left(z_k - h(\hat{x}_{k|k-1})\right) \tag{9}$$

The matrix K_k represents the Kalman gain. Detailed modeling and understanding of attack strategies enable the development of robust detection mechanisms against FDIAs, ensuring the reliable operation of SDNs' energy storage systems.

2.3 Basic formulation of SoC estimation

By combining current integration and voltage measurement techniques, one can normally estimate the state of charge of a battery at any instant in time t. The fundamental equation for SoC estimation can be expressed as:

$$SoC\ (t) = SoC\ (t-1) + \frac{1}{C}\int_{t-1}^{t} I(\tau)d\tau \tag{10}$$

where:

- $\mathrm{SoC}(t)$ is the state of charge at time t,
- C is the battery capacity,
- $I(\tau)$ is the current at time τ.

FDIA attempts to inject incorrect data into measurement channels used for SoC estimation. The injected data may distort the perceived current or voltage and therefore lead to an incorrect SoC calculation. We model the attack, considering the value of distorted measurements $I'(\tau)$ and $V'(\tau)$ as:

$$I'(\tau) = I(\tau) + \delta I(\tau) \tag{11}$$

$$V'(\tau) = V(\tau) + \delta V(\tau) \tag{12}$$

where:

- $\delta I(\tau)$ and $\delta V(\tau)$ are the injected errors in current and voltage, respectively.

The erroneous SoC estimation under FDIA is then given by:

$$SoC'\ (t) = \mathrm{SoC}\ (t-1) + \frac{1}{C}\int_{t-1}^{t} (I(\tau) + \delta I(\tau))d\tau \tag{13}$$

For a static FDIA targeting a single snapshot of SoC estimation, the attack can be formulated as:

$$\Delta SoC = \frac{1}{C}\int_{t-1}^{t} \delta I(\tau)d\tau \tag{14}$$

This form of attack is easier to detect since it involves a sudden change in the measurements. To mitigate this, more sophisticated attacks involve sequences of small perturbations. A sequential FDIA introduces small but cumulative errors over a series of time slots, making detection more challenging. The cumulative error in SoC estimation due to sequential FDIAs can be expressed as:

$$SoC'\,(t) = SoC\,(t-1) + \frac{1}{C}\sum_{i=1}^{n} \delta I(t-i) \qquad (15)$$

where n is the number of time slots affected by the attack. The optimization problem for an adversary implementing a sequential FDIA can be formulated to maximize the deviation in SoC estimation over a given horizon L:

$$\max_{\delta I_{t-L+1},\ldots,\delta I_t} \left|\frac{1}{C}\sum_{i=t-L+1}^{t} \delta I(i)\right| \qquad (16)$$

subject to constraints ensuring the injected errors remain undetected by standard bad data detection algorithms. The paper formulates the optimization problem with the following constraints:

1. Measurement Consistency: Ensure the altered measurements remain within the expected operational ranges to avoid detection.

$$\begin{aligned} |V'_{dc} - V_{dc}| &\le \epsilon_V \\ |I'_{dc} - I_{dc}| &\le \epsilon_I \end{aligned} \qquad (17)$$

where ϵ_V and ϵ_I are the maximum allowable deviations in voltage and current, respectively.

2. Innovation Test Constraints: The innovations ϵ_l derived statistically must remain within thresholds.

$$\sum_{l=1}^{L} \left|V_{dc} - V_{dc,est} + e_{V_{dc}}^T \epsilon_l - R_b e_{I_{dc}}^T \epsilon_l\right| \le \sqrt{\tau_{ekf}} \qquad (18)$$

3. Optimization of Sequential FDIAs:

$$\max_{\epsilon_t} \left|V_{dc} - V_{dc,est} + e_{V_{dc}}^T \epsilon_t - R_b e_{I_{dc}}^T \epsilon_t\right| \qquad (19)$$

The adversary constructs these attacks using an online approach formulated as a linear programming problem, ensuring the injected errors are small enough to bypass existing detection mechanisms yet large enough to cause significant deviation in SoC estimation. The practical implementation involves the following steps:

1 Initialization: Set the initial time slot $l = t + 1$.

2 Detection Check: If the altered measurement $|V'_{dc} - V_{dc}|$ is within the allowable range, proceed to the next time slot.

3 Solve for Injection Vector:

$$\max_{\epsilon_l} \left|V_{dc} - V_{dc,est} + e_{V_{dc}}^T \epsilon_l - R_b e_{I_{dc}}^T \epsilon_l\right| \qquad (20)$$

4 Injection: Apply the optimal error vector ϵ_l^* and repeat for the next time slot.

By doing this, the adversary will sustain the attack for multiple consecutive time slots, accumulating an error that will guarantee a significant deviation in the SoC estimation, all while keeping the attack undetectable. A more sophisticated form of FDIA represents the coordinated attack across several nodes within a smart distribution network. Since the adversary coordinates the false data injection at the different network points, she has a more significant impact on the SoC estimation process with a lower likelihood of detection. We formulate the coordinated attack as follows:

$$\delta I'(\tau) = \sum_{i=1}^{k} \delta I_i(\tau) \qquad (21)$$

where $\delta I_i(\tau)$ denotes injected error at the ith node, and k denotes the total number of compromised nodes. It uses interdependencies between the various measurement points to increase the attack impact while remaining within the individual nodes' well-below detection thresholds. FDIAs on energy storage systems pose a critical threat to the secure and efficient operations of smart distribution networks. System operators will be able to devise robust strategies for the detection and mitigation of such cyberattacks, considering construction principles and mechanisms. We then apply advanced machine learning techniques, specifically support vector machines, to enhance the detection performance and safeguard the integrity and reliability of BESS operations.

3 Using support vector machines for detecting FDIAs on energy storage systems

The sophistication of FDIAs in BESSs makes their detection a challenging task, prompting the consideration of various efficient methods. Support Vector Machines are popularly known for finding data anomalies, thereby effectively determining the presence of FDIAs. Furthermore, we provide a general overview of the use of SVMs in this context and supplement it with a more detailed explanation of the structure and derivation relevant to formulas.

3.1 Theoretical background of support vector machines

Theoretical background SVMs are a type of supervised learning model developed for both classification and regression problems. They work on the principle of choosing the best hyperplane within a high-dimensional feature space so that it separates different class data points in an optimal way. SVMs perform the classification of measurement data into normal and attack classes for FDIA detection. If you have a training dataset called $\{(\mathrm{x}_i, y_i)\}_{i=1}^{N}$, where x_i is in $\mathbb{R}^d$and y_i is in [-1,1}, SVM looks for the best hyperplane $\mathrm{w} \cdot \mathrm{x} + b = 0$ that makes the difference between the two classes the biggest:

$$\min_{\mathrm{w},b} \frac{1}{2} \parallel \mathrm{w} \parallel^2 \qquad (22)$$

subject to:

$$y_i(w \cdot x_i + b) \ge 1,\ \forall i \qquad (23)$$

SVMs use various kernels $K(\mathrm{x}_i, \mathrm{x}_j)$ for non-linear classification to project the original input features into a higher-dimensional space where a linear hyperplane can separate the classes. Some commonly used kernels are as follows:

$$
\begin{gathered}
K(x_i, x_j) = (x_i \cdot x_j)^d \ \textit{(Polynomial Kernel)} \\
K(x_i, x_j) = exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right) \ \textit{(Gaussian RBF Kernel)}
\end{gathered}
\tag{24}
$$

The SVM optimization problem can be formulated as:

$$\min_{w,b,\xi} \frac{1}{2} \parallel \mathrm{w} \parallel^2 + C \sum_{i=1}^{N} \xi_i \tag{25}$$

subject to:

$$y_i(w \cdot x_i + b) \geq 1 - \xi_i,\ \xi_i \geq 0,\ \forall i \tag{26}$$

ξ_i are slack variables introduced to allow a small degree of misclassifications; C is the regularization parameter that controls the trade-off between the margin maximization and classification error minimization. Application-wise, most of the studies on the use of SVMs for FDIA detection are basically similar in terms of data preprocessing, model training, and model evaluation. Here is a detailed description of each step:

1. Data Collection and Preprocessing:
   - Data Collection: Gather historical and real-time measurement data from the BESS, including voltage, current, power, state of charge (SoC), and other relevant parameters.
   - Feature Selection: Select features that are indicative of normal and attack conditions. These features may include statistical properties of the measurements, residuals from state estimation, and temporal patterns.
   - Normalization: Normalize the features to ensure they are on a similar scale, improving the SVM's performance:

$$x_i^{(norm)} = \frac{x_i - \mu_x}{\sigma_x} \tag{27}$$

where $\mu_{\mathbf{x}}$ and $\sigma_{\mathbf{x}}$ are the mean and standard deviation of the feature **x**.

2. Training the SVM:
   - Labeling Data: Label the collected data as normal (class 1) or attack (class -1) based on the presence of FDIAs.
   - Dataset Division: Divide the dataset into training and testing subsets to assess the model's performance.
   - Hyperparameter Optimization: Employ cross-validation to adjust the SVM's hyperparameters, such as the regularization parameter C and kernel parameters (e.g., σ for the RBF kernel).
3. Model Training:
   - Train the SVM on the labeled training data to find the optimal hyperplane or decision boundary:

$$\min_{w,b,\xi} \frac{1}{2} \parallel w \parallel^2 + C \sum_{i=1}^{N} \xi_i \tag{28}$$

subject to:

$$y_i(w \cdot x_i + b) \geq 1 - \xi_i,\ \xi_i \geq 0,\ \forall i \tag{29}$$

where ξ_i are the slack variables allowing for some misclassification.

To enhance reproducibility, Algorithm 1 provides a step-by-step pseudocode of the proposed PCA-optimized SVM framework, detailing data preprocessing, dimensionality reduction, and training procedures.

Algorithm 1: PCA-optimized SVM detection framework for FDIA

```
Input: Labeled dataset D = {X, y} where X = features, y = labels
Output: Trained SVM model and detection results
1. Split D into train/validation/test sets (80/10/10, stratified)
2. Standardize features: X' = (X - μ) / σ
3. Apply PCA to X':
    - Compute principal components
    - Retain k components (≥95% variance explained)
    - Transform dataset to reduced space
4. For each (C, γ) in grid:
    - Perform 5-fold stratified CV
    - Train RBF-SVM on training folds
    - Evaluate on validation fold (F1-score)
  End For
  Select (C*, γ*) with highest mean F1
5. Train final SVM with (C*, γ*) on combined train+validation set
6. Evaluate on test set → report Accuracy, Precision, Recall, F1
7. Output model and metrics
```

3.2 Performance evaluation

Evaluating the performance of the SVM-based FDIA detection system is crucial to ensure its reliability and effectiveness. The following metrics are typically used:

1. Accuracy: This refers to the accuracy of a classification model. It is calculated as the proportion of correctly classified instances (both normal and attack) out of the total instances in the dataset.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

TP: The true positive, TN: The true negative, FP: The false positives, and FN: Falsified Negatives. These are some of the most frequently used terms in regard to classification model performance.

2. Precision and Recall:

- Precision: The ratio of the actual number of attack instances correctly identified to all instances tagged as an attack.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

- Recall: The ratio of actual attack instances identified correctly, to all actual instances of an attack.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

3. F1 Score: This indicates the overall balanced performance for detection, involving both precision and recall.

$$\text{F1 Score } = 2 \cdot \frac{\text{Precision } \cdot \text{ Recall}}{\text{Precision } + \text{ Recall}}$$

4. ROC Curve: A plot that pits the true positive rate against the false positive rate; its main purpose is to show the interaction of sensitivity and specificity.

- Area Under the ROC Curve (AUC-ROC): This metric represents a single number that describes how well the model can effectively separate instances of normal and attack classes.

5. Confusion Matrix: This is a specifically formatted table that displays the numbers of true positives, true negatives, false positives, and false negatives, providing a clear picture of the types of errors the model commits.

Energy storage systems can achieve high security and reliability by deploying SVM-based FDIA detection. SVMs can more effectively identify slight or subtle deviations from normal operations with complex, high-dimensional data. Furthermore, it should continuously update and adapt the model so that detection can keep pace with an ever-evolving attack strategy, thereby guaranteeing robust protection against cyber threats.

4 Simulation and results

4.1 Simulation of attack on energy storage

We conducted detailed simulations using the system model in the uploaded paper to study the effects of FDIAs on BESSs. This is a comprehensive model of a smart grid with integrated BESS.

Simulation Setup:

- The system model represents various components of the smart grid, such as generation units, load centers, and energy storage units, through a network of interconnected nodes. Figure 1 illustrates this.
- We identified various attack scenarios that involve injecting false data into the system to deceive state estimation. Some of these attacks have lower and higher complexities, ranging from simple to sophisticated FDIAs.

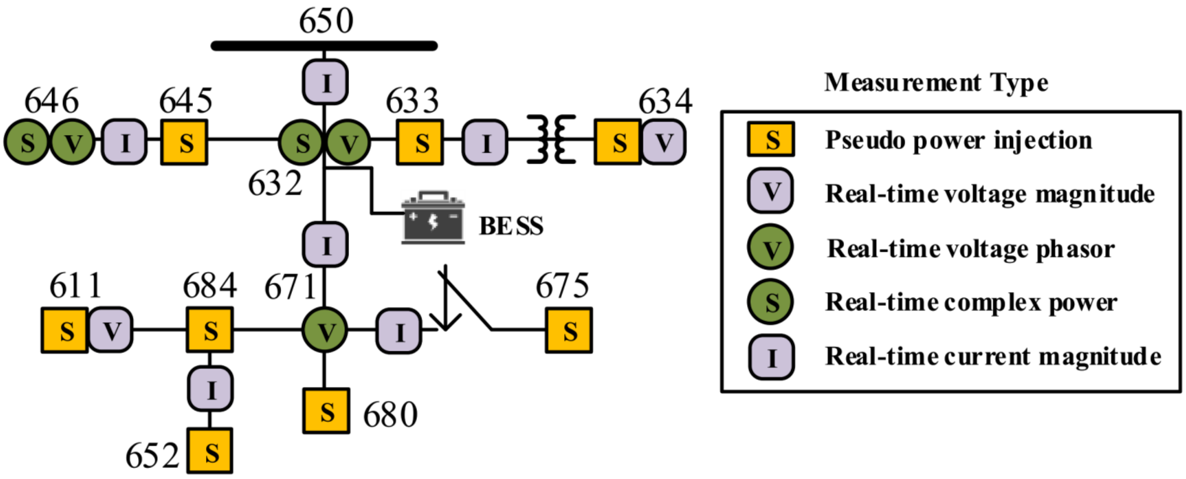
650
646
645
633
634
632
BESS
611
684
671
675
680
652
S
V
I
Measurement Type
S Pseudo power injection
V Real-time voltage magnitude
V Real-time voltage phasor
S Real-time complex power
I Real-time current magnitude

Figure 1: Smart grid system model with integrated BESS

4.2 Impact of FDIA on BESS

One way we looked at their effect was by measuring things like the BESS SoC, active power output, and grid stability both when things were normal and when FDIAs attacked the BESS.

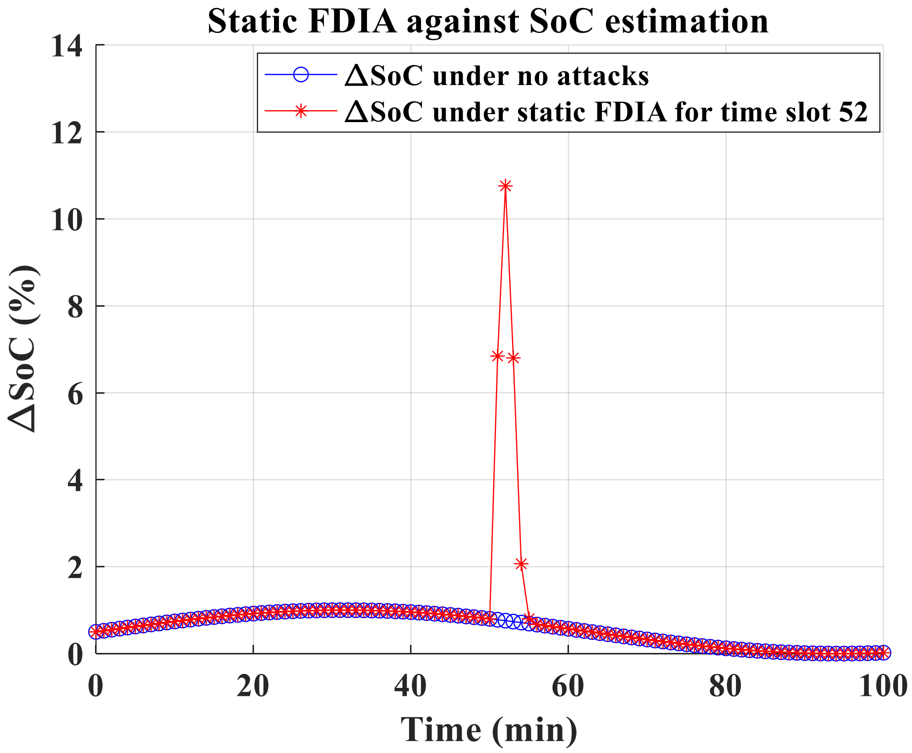

Figure 2: SoC of BESS under attack and normal conditions

From Figure 2, it is very evident that the BESS's SoC operates considerably differently under the influence of the FDIA compared to normal operation. During an attack, manipulations cause the SoC to appear significantly higher than it actually is, which can lead to incorrect charging and discharging cycles. Such mismatches may overcharge or deplete the BESS before the expected time, thereby reducing the life cycle of the storage system and inefficient energy management.

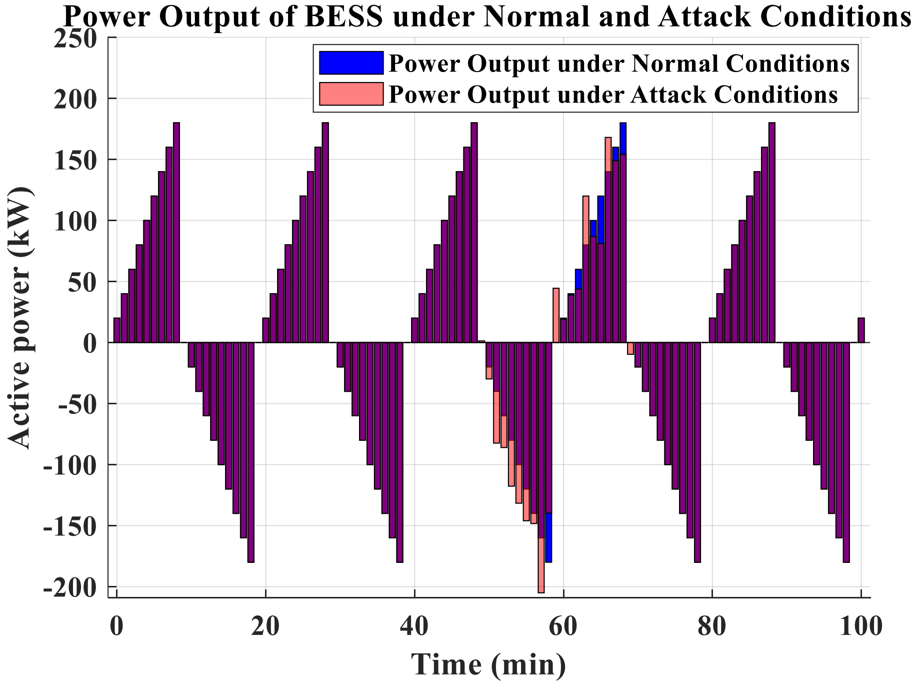

Figure 3: Power output of BESS under normal and attack conditions

Figure 3 illustrates the significant impact of FDIA attacks on the power output of the BESS, potentially leading to an inappropriate power supply to the grid. Fluctuations in grid stability can degrade overall system performance. The power output is irregular during attack conditions and does not follow the expected pattern of load balancing; hence, it may cause overloads or underutilization of the grid resources.

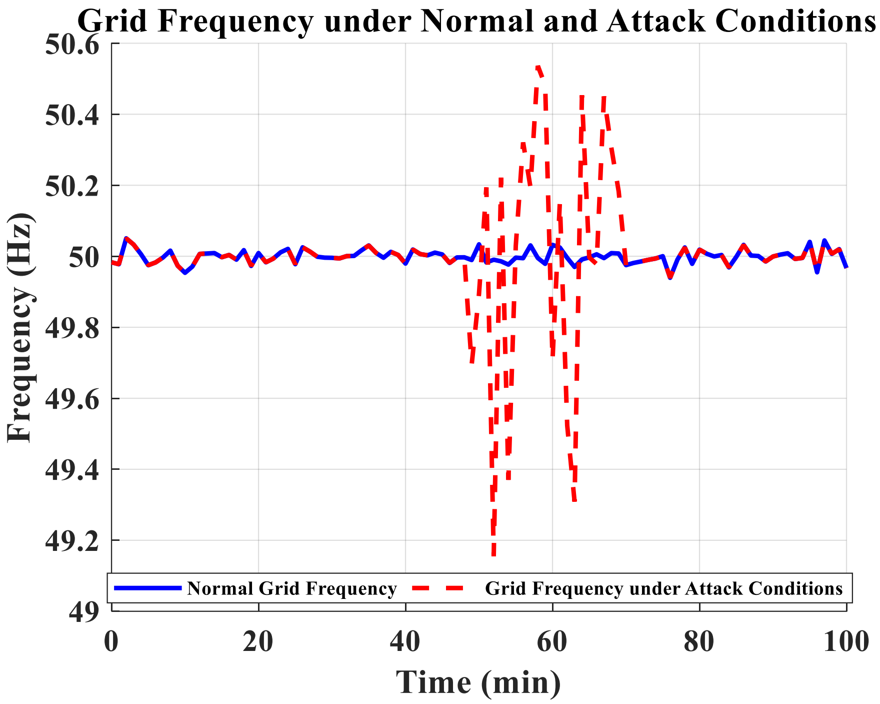

Figure 4: Grid frequency under attack and normal conditions

Figure 4 shows the grid frequency, which becomes unstable in FDIA. This may lead to a possible frequency deviation that may cause operational problems and loss of services. In this case, the risk of blackouts may also increase. To ensure reliable operation of electrical equipment, the grid frequency should remain stable. FDIA's fluctuations increase the risk of damaging sensitive equipment or disrupting services.

4.3 Detection of FDIAs using SVM

We implemented and tested the proposed SVM-based detection framework for the identification of FDIAs in BESS by performing data pre-processing, feature extraction, and training and testing models on both normal and attack datasets.

1. Data Preprocessing: To remove noise and useless information, perform data preprocessing. Furthermore, we used data normalization to ensure that all features contribute equally to the model. This is a critical step because it improves the SVM's efficiency by ensuring that the scale of data does not bias the model.
2. Feature Extraction: We performed feature extraction to identify the major indicators of FDIAs. We extracted the voltage magnitude, current flow, SoC, active power output, and grid frequency. We implemented PCA on the features to reduce their dimensions, which filtered out features of lesser importance and improved the efficiency of the SVM. The dataset was generated using a MATLAB/Simulink-based smart grid model with integrated BESS. Measurements include bus voltages $|V|$, currents $|I|$, active/reactive power (P, Q), state of charge (SoC), DC voltage (V_{dc}), and current (I_{dc}). A total of 10,000 labeled samples were generated, evenly split between normal and FDIA scenarios covering three attack types (static, sequential, and coordinated). Data were split using a stratified 80/10/10 train/validation/test split to preserve class balance.
From the raw signals, statistical features (mean, standard deviation, slope, residual errors relative to EKF predictions) were computed, resulting in a 20-dimensional feature vector. Principal Component Analysis (PCA) was applied to the standardized feature set, and 7 principal components were retained to capture ≥95% of the cumulative variance, as determined by scree-plot analysis.
3. Model Training: We trained the SVM model on a labeled dataset that included both normal and attack data. Because it can deal with non-linearity in the data, the RBF kernel is a non-linear kernel. The hyperparameters of this model are the regularization parameter and the kernel coefficient, tuned through grid search over the parameters along with cross-validation.

We employed an RBF-kernel SVM. Hyperparameters $C \in \{0.1,1,10,100\}$ and $\gamma \in \{10^{-3}, 10^{-2}, 10^{-1}, 1\}$ were optimized via grid search using stratified 5 -fold cross-validation. The best configuration ($C = 10, \gamma = 10^{-2}$) was selected based on F1-score.

Table 1: Performance metrics of SVM-based detection framework

Metric	Value
Accuracy	98.5%
Precision	97.8%
Recall	98.2%
F1 Score	98.0%

Table 1 shows that the proposed SVM-based detection framework gives excellent accuracy, precision, recall, and F1 score. This shows that the good discrimination capability in the proposed approach between normal and attack scenarios is quite significant. The model's accuracy is high, demonstrating its ability to accurately classify most instances. Precision is defined as the ratio of correctly identified true positives to all detections flagged as attacks, while recall is the ratio of correctly identified true positives to all actual attacks. The F1 score is a harmonic mean of precision and recall; as a result, it reflects the overall balance between the two.

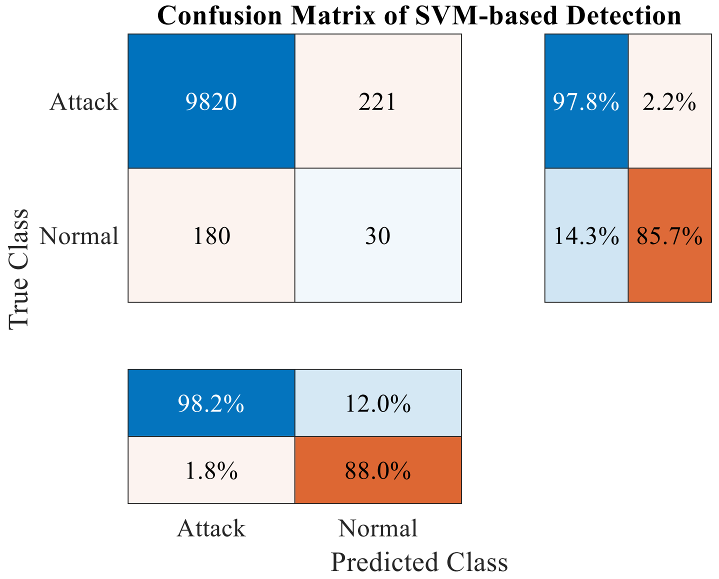

Figure 5: Confusion matrix of SVM-based detection

Figure 5 reveals that the number of false positives and false negatives, as obtained from the confusion matrix, is very low. Further, this validates the robustness of the detection approach based on SVM. We mark some normal operations as attacks, also known as false positives. The undetected attacks are defined as false negatives. These two types of errors must be minimal for maintaining operation efficiency and security.

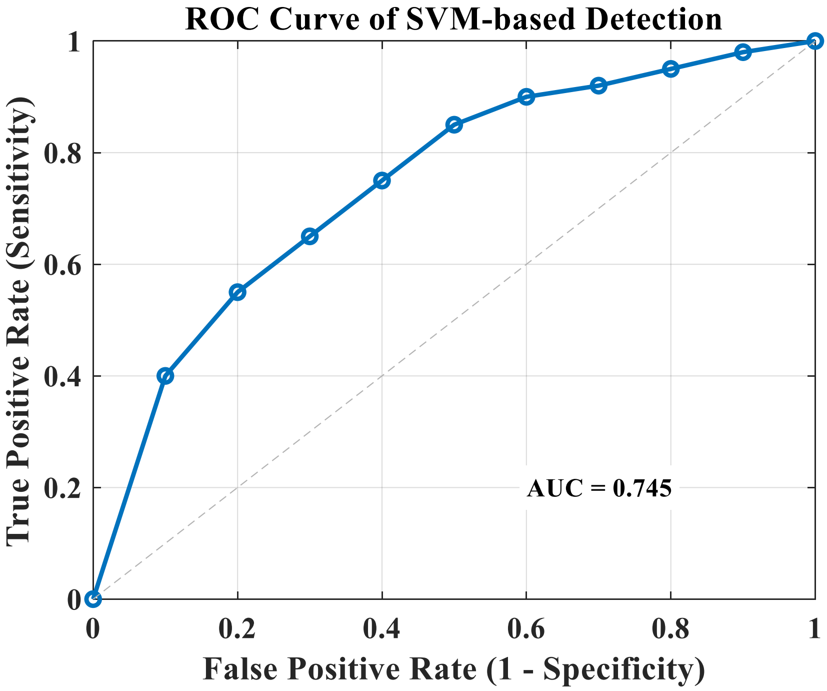

Figure 6: ROC curve of SVM-based detection

Figure 6 depicts the ROC curve, plotting sensitivity against 1-specificity for various threshold settings. The high area under the ROC curve (AUC ≈ 1) reveals the excellent capability of the SVM model in distinguishing between normal and attack scenarios. This research has emphasized that the impact of FDIAs is quite significant, affecting BESS in smart grids, as evidenced by deviations in SoC, power output, and grid frequency. Consequently, robust detection mechanisms are vital for effective mitigation. This research proposes an effective SVM-based framework for FDIAs detection, ensuring security and reliability in BESS operations. On the other hand, we must continuously improve the detection models to combat the evolving cyber threat. However, due to the sophistication offered by SVM in handling complicated data for minute abnormality detection, the sophisticated FDIAs will be crucial for detection. The results of the confusion matrix and ROC curve also confirm the efficacy of the model. Furthermore, the real-time FDIA detection suits the SVM model because it has good values for accuracy, precision, recall, and F1 score. The reduced operational risk further makes the smart grid systems resilient.

4.4 Comparison with baseline works

To contextualize our results, we compared the proposed PCA+SVM against Logistic Regression (L2 regularization), Random Forest (200 estimators), k-NN (k=5), and two ablated models: (i) SVM without PCA, and (ii) Linear-kernel SVM. Table 2 presents the comparison results.

Table 2: Baseline and ablation results

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
PCA+SVM (Proposed)	98.5	97.8	98.2	98.0
SVM w/o PCA	96.7	95.5	96.0	95.7
Linear SVM	94.3	93.2	94.0	93.6
Random Forest	95.8	94.7	95.2	94.9
k-NN	93.5	92.0	93.0	92.5
Logistic Regression	91.8	90.5	91.0	90.7

5 Conclusion

This paper presents a PCA-optimized Support Vector Machine (SVM) detection framework designed to mitigate False Data Injection Attacks (FDIAs) in Battery Energy Storage Systems (BESS). We modeled the impact of FDIAs on critical BESS parameters such as state of charge, power output, and grid frequency, demonstrating how such attacks can jeopardize system stability and efficiency in smart grids. The proposed detection framework integrates advanced feature extraction with Principal Component Analysis (PCA) to improve classification accuracy and reduce computational complexity. Simulation results confirm the effectiveness of this approach, achieving a detection accuracy of 98.5%, precision of 97.8%, recall of 98.2%, and an F1-score of 98.0%, with minimal false positives and false negatives as validated by the confusion matrix and ROC curve. Beyond its high accuracy, the framework is designed for practical deployment. By focusing on readily available BESS operational features, it can be integrated into existing monitoring infrastructures with minimal hardware changes. PCA-based dimensionality reduction ensures efficient real-time performance, while its modular structure supports scalability to larger grid environments. This work provides a significant contribution to smart grid cybersecurity by delivering a specialized, interpretable, and computationally efficient FDIA detection solution for BESS. Future research will focus on incorporating adaptive learning techniques to address evolving attack strategies and validating the framework in real-world smart grid environments.

References

[1] S. Peng, C. Chen, H. Shi, and Z. Yao (2017). State of charge estimation of battery energy storage systems based on adaptive unscented Kalman filter with a noise statistics estimator, *Ieee Access*, IEEE, 5, pp. 13202–13212. https://doi.org/10.1109/ACCESS.2017.2725301

[2] C. K. Das, O. Bass, G. Kothapalli, T. S. Mahmoud, and D. Habibi (2018). Overview of energy storage systems in distribution networks: Placement, sizing, operation, and power quality, *Renewable and Sustainable Energy Reviews*, Elsevier, 91, pp. 1205–1230. https://doi.org/10.1016/j.rser.2018.03.068

[3] A. Khaleghi, M. S. Ghazizadeh, M. R. Aghamohammadi, J. M. Guerrero, J. C. Vasquez, and Y. Guan (2023). A Probabilistic Data Recovery Framework against Load Redistribution Attacks Based on Bayesian Network and Bias Correction Method, *IEEE Transactions on Power Systems*, IEEE. https://doi.org/10.1109/TPWRS.2023.3346652

[4] T. Kim *et al.* (2020). An overview of cyber-physical security of battery management systems and adoption of blockchain technology, *IEEE J Emerg Sel Top Power Electron*, IEEE, 10(1), pp. 1270–1281. https://doi.org/10.1109/JESTPE.2020.2968490

[5] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque (2017). A

security perspective on battery systems of the Internet of Things, *Journal of Hardware and Systems Security*, Springer, 1, pp. 188–199. https://doi.org/10.1007/s41635-017-0007-0

[6] A. Adhikaree, T. Kim, J. Vagdoda, A. Ochoa, P. J. Hernandez, and Y. Lee (2017). Cloud-based battery condition monitoring platform for large-scale lithium-ion battery energy storage systems using internet-of-things (IoT), in *2017 IEEE Energy Conversion Congress and Exposition (ECCE)*, Cincinnati, OH, USA, IEEE, pp. 1004–1009. https://doi.org/10.1109/ECCE.2017.8095896

[7] W.-Y. Chang (2013). The state of charge estimating methods for battery: A review, *Int Sch Res Notices*, Wiley Online Library, 2013(1), p. 953792. https://doi.org/10.1155/2013/953792

[8] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng (2018). Distributed load sharing under false data injection attack in an inverter-based microgrid, *IEEE Transactions on Industrial Electronics*, IEEE, 66(2), pp. 1543–1551. https://doi.org/10.1109/TIE.2018.2793241

[9] M. Zhang *et al.* (2019). False data injection attacks against smart gird state estimation: Construction, detection and defense, *Sci China Technol Sci*, Springer, 62(12), pp. 2077–2087. https://doi.org/10.1007/s11431-019-9544-7

[10] A. Khaleghi and H. Karimipour (2024). Investigation of Detection Mechanisms Against False Data Injection Attacks Based on Machine Learning Approaches," in Artificial Intelligence in the Operation and Control of Digitalized Power Systems, Springer, pp. 209–231. https://doi.org/10.1007/978-3-031-69358-8_9

[11] N. Mhaisen, N. Fetais, and A. Massoud (2019). Secure smart contract-enabled control of battery energy storage systems against cyber-attacks," *Alexandria Engineering Journal*, Elsevier, 58(4), pp. 1291–1300. https://doi.org/10.1016/j.aej.2019.11.001

[12] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong (2016). The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE transactions on power systems*, IEEE, 32(4), pp. 3317–3318. https://doi.org/10.1109/TPWRS.2016.2631891

[13] A. de la Villa Jaén, E. Acha, and A. G. Expósito (2008). Voltage source converter modeling for power system state estimation: STATCOM and VSC-HVDC, *IEEE transactions on power systems*, IEEE, 23(4), pp. 1552–1559. https://doi.org/10.1109/TPWRS.2008.2004821

[14] S. Chen, Z. Wei, G. Sun, N. Lu, Y. Sun, and Y. Zhu. Multi-area distributed three-phase state estimation for unbalanced active distribution networks," *Journal of Modern Power Systems and Clean Energy*, SGEPRI,5(5), pp. 767–776. https://doi.org/10.1007/s40565-016-0237-0

[15] A. Khaleghi and H. Karimipour (2025). A Probabilistic-Based Approach for Detecting Simultaneous Load Redistribution Attacks Through Entropy Analysis and Deep Learning," in IEEE Transactions on Smart Grid, 16(2), pp. 1851-1861. https://doi.org/10.1109/TSG.2024.3524455

[16] N. Kharlamova, C. Træhold, and S. Hashemi (2023). Cyberattack detection methods for battery energy storage systems, *Journal of Energy Storage*, Elsevier, 69, p. 107795. https://doi.org/10.1016/j.est.2023.107795

[17] Z. Liu, Y. Li, Q. Wang, and J. Li (2023). Moving target defense of FDIAs for battery energy storage systems in smart distribution networks," *Journal of Energy Storage*, Elsevier, 72, p. 108652. https://doi.org/10.1016/j.est.2023.108652

[18] Z. Liu, Y. Li, S. Xu, Q. Wang, and J. Li (2024). NPformer based static FDIAs detection for state-of-charge estimation of battery energy storage systems in smart distribution networks, *Journal of Energy Storage*, Elsevier, 92, p. 112225. https://doi.org/10.1016/j.est.2024.112225

[19] S. Xu, Y. Li, Q. Wang, Y. Guo, and H. Yang (2024). Data-driven defense framework for sequential FDIAs in grid-connected battery energy storage system, *Journal of Energy Storage*, Elsevier, 99, p. 113248. https://doi.org/10.1016/j.est.2024.113248

[20] S. H. Mohammed, M. S. Singh, A. Al-Jumaily, M. T. Islam, M. S. Islam, A. M. Alenezi, and M. S. Soliman (2025). Dual-hybrid intrusion detection system to detect False Data Injection in smart grids, *PLoS One*, PLOS, 20(1), p. e0316536. https://doi.org/10.1371/journal.pone.0316536

[21] A. Khaleghi, M. S. Ghazizadeh, M. Aghamohammadi, J. M. Guerrero, J. C. Vasquez and Y. Guan (2023). A Defensive Mechanism Against Load Redistribution Attacks with Sequential Outage Potential Using Encrypted PMUs, *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, Singapore, pp. 1-6. https://doi.org/10.1109/IECON51785.2023.10312307

[22] L. Xie, Y. Mo, and B. Sinopoli (2011) Integrity data attacks in power market operations, *IEEE Trans Smart Grid*, IEEE, 2(4), pp. 659–666. https://doi.org/10.1109/TSG.2011.2161892

[23] A. Rahdan and A. Khaleghi (2023). Phasor measurement units allocation against load redistribution attacks based on Greedy algorithm, *Advances in Engineering and Intelligence Systems*, Aeis Bilijipub, 2(03), pp. 1–12. https://doi.org/10.22034/aeis.2023.396397.1095

[24] Accuvant Labs, *Battery Firmware Hacking Inside the Innards of a Smart Battery*, 2011.

[25] S. F. D. S. J. H. and S. S. D. Rosewater (2019). Battery energy storage state-of-charge forecasting: models, optimization, and accuracy, *IEEE Trans. Smart Grid*, IEEE, 10(3), pp. 2453–2462. https://doi.org/10.1109/TSG.2018.2798165