

Online and Offline Identification of False Data Injection Attacks in Battery Sensors Using a Single Particle Model

Victoria A. O'Brien, *Member, IEEE*, Vittal S. Rao, *Life Senior Member, IEEE*, and Rodrigo D. Trevizan, *Member, IEEE*

Abstract The cells in battery energy storage systems are monitored, protected, and controlled by battery management systems whose sensors are susceptible to cyberattacks. False data injection attacks (FDIAs) targeting batteries' voltage sensors affect cell protection functions and the estimation of critical battery states like the state of charge (SoC). Inaccurate SoC estimation could result in battery overcharging and over discharging, which can have disastrous consequences on grid operations. This paper proposes a three-pronged online and offline method to detect, identify, and classify FDIAs corrupting the voltage sensors of a battery stack. To accurately model the dynamics of the series-connected cells a single particle model is used and to estimate the SoC, the unscented Kalman filter is employed. FDIA detection, identification, and classification was accomplished using a tuned cumulative sum (CUSUM) algorithm, which was compared with a baseline method, the chi-squared error detector. Online simulations and offline batch simulations were performed to determine the effectiveness of the proposed approach. Throughout the batch simulations, the CUSUM algorithm detected attacks, with no false positives, in 99.83% of cases, identified the corrupted sensor in 97% of cases, and determined if the attack was positively or negatively biased in 97% of cases.

Index Terms—anomaly detection, anomaly identification, chi-squared, concentration model, cumulative sum, false data injection attacks, single particle model, smart grid.

I. INTRODUCTION¹

AS energy demands increase, the integration of grid-scale battery energy storage systems (BESSs) is necessary for a number of grid functions [1], [2]. BESSs are equipped with battery management systems (BMSs) to collect sensor measurements, estimate states, ensure operation within safe limits, and balance cell voltages within stacks [3]- [7]. The safe operation of battery packs depends on accurate state of charge (SoC) estimation, otherwise batteries could overcharge or over discharge, which could lead to severe consequences like thermal runaway or rapidly degrading battery cells [3], [8] - [13]. Modern BMSs may utilize communication technologies, cloud-based systems, and the internet-of-things [14], making them susceptible to cyberattacks that

could damage cells or disrupt operation.

Common cyberattacks targeting cyber-physical systems (CPSs) include denial of service (DoS) attacks, replay attacks, and deception attacks [15]. DoS attacks and replay attacks are simpler to detect than deception attacks. Missing sensor data caused by DoS attacks would be trivial to detect by data-driven or residual-based methods. Replay attacks like those identified in the Stuxnet malware [16] are well suited for physical processes that operate in steady state. Most BESS applications, however, are based on the response to grid conditions, which are inherently variable, thus making stealthy replay attacks hard to implement.

On the other hand, data deception attacks like false data injection attacks (FDIAs) are harder to detect, as small changes in sensor readings could be missed by traditional

¹This work was supported by the U.S. Department of Energy, Office Electricity, Energy Storage program. This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan <https://www.energy.gov/downloads/doe-public-access-plan>. This paper

describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

V. A. O'Brien is with the Electric Grid Security & Communications group, Sandia National Laboratories, Albuquerque, NM, 87185 USA (e-mail: vaobrie@sandia.gov).

V. S. Rao is with the Department of Electrical & Computer Engineering, Texas Tech University, Lubbock, TX 79409 USA. (e-mail: vittal.rao@ttu.edu).

R. D. Trevizan is with the Energy Storage Technology & Systems group, Sandia National Laboratories, Albuquerque, NM, 87185 USA (e-mail: rdtrevi@sandia.gov).

bad data detection mechanisms.

Failing to detect FDIAs injected into sensors could result in incorrect BMS operation, including inaccurate SoC estimation and malfunction of safety functions [3], [12]. In [17], the authors assert that FDIAs are the most common class of threats targeting smart grids. Unlike many other cyberattacks which fall into a single category, FDIA integrity attacks can be launched as physical-based attacks, cyber-based attacks, communication-based attacks, and network-based attacks [17]; resulting in a wide attack surface to launch FDIAs. FDIAs may be stealthy or model agnostic. Launching stealthy FDIAs requires knowledge of the system's configuration, dynamics, and simultaneous sensor attacks, making stealthy FDIAs expensive [18], [19]. Local system knowledge for multiple parameters is used in [19] to inject FDIAs into BESSs in smart distribution networks and to evade typical detection mechanisms. Alternatively, small-magnitude, model agnostic FDIAs are more likely to be launched and can be hard to detect. Therefore, model agnostic FDIAs were studied in this paper.

Detecting FDIAs requires model-based statistical methods [20] - [22], or data-driven methods that solely use system measurements to flag anomalies [23] - [25]. Machine learning (ML) methods [23] - [25] have been successful in detecting anomalies but rely heavily on training datasets [25]. In [23] the authors used a convolutional neural network trained with 400 simulated datasets to detect abnormalities in battery systems. Simulated data could be subject to biases and there is limited data for grid tied BESSs, so ML methods may have limitations in their accuracy. Model-based detection methods postprocess test statistics to detect attacks in the system; some methods for postprocessing test statistics are recursive summations and the chi-squared test (χ^2). In [26] the authors used a recursive sum to detect FDIAs in CPSs. As discussed in [20], the χ^2 test failed to detect stealthy integrity attacks in CPSs. The χ^2 test was applied in [27] to detect outliers in battery measurements during state estimation but flagged multiple false positives. While the χ^2 test is a popular choice for bad data detection, its main drawback is its false positive rate which is correlated with its confidence level. On the other hand, many recursive summation methods, like the cumulative sum (CUSUM) algorithm, can be tuned to a false positive rate of 0%.

When utilizing model-based detectors, accurate CPS modeling is essential for calculating small residuals and minimizing false positives. Model errors can introduce biases in the estimates [28], consequently, using low-fidelity models and methods to detect changes in the mean of random variables can cause false positives. Battery modeling is typically done using equivalent circuit models (ECMs) [30] - [33] or concentration models [30], [34] - [36]. Concentration models are more complex, requiring more parameters and equations than ECMs, but concentration models can outperform ECMs across long time horizons [30]. Common concentration models include the single particle model (SPM), the pseudo two-dimensional model, and the polynomial porous electrode model [35]. In this paper, a SPM is considered, as it is the

simplest concentration model in terms of the required number of equations and parameters, and despite their advantages, SPMs have not been used for FDIA detection [27], [29], [31], [32], [37].

In the method proposed in this paper, the battery model is used to estimate states, measurements, and test statistics which are postprocessed for FDIA detection. The state variables of the SPM include the average concentration of the anode and cathode, and the SoC. The SPM is nonlinear; hence, a nonlinear estimator is needed. Common nonlinear state estimation methods applied to battery systems are the extended Kalman filter (EKF) [3], [33] and the unscented Kalman filter (UKF) [37], [38]. EKFs require the calculation of a Jacobian matrix, which can be challenging in systems with nonlinear algebraic equations. Additionally, EKFs introduce errors in the state estimates by assuming the expected value of a nonlinear function is equivalent to the nonlinear function applied to a point estimate of the system estimates, and by neglecting the nonlinear terms of the Taylor series expansion of state transition and output functions [38]. Whereas UKFs represent systems with a collection of sigma points (SPs) that capture nonlinearities more accurately than linear approximations, making them more accurate for state estimation [37], [39]. Variations of EKFs and UKFs have been applied to battery systems to estimate the SoC, model parameters, and state variables [8], [32], [36], [39] - [41]. In this paper a UKF was selected as the estimator.

Estimation algorithms can be repurposed to detect anomalies in sensor data, including those caused by cyberattacks and faults [33]. Model-based detection approaches typically compare sensor readings, such as cell and stack voltages, to the predicted values by state estimation algorithms based on battery models. Large differences between the sensor reading and the prediction indicates abnormal system behavior. Battery SoC estimation is negatively impacted by measurement errors and analysis of the residuals is important for safety and security [43]. Attack-resilient state estimators and feedback control methods have also been proposed to secure CPS [44]. Offline, variable-magnitude FDIA detection was achieved via model-based detectors; however, identifying the compromised sensors was not possible [31], [32], [37]. In [32], Liu and He used a residual-based method to identify if faults were in the current or voltage sensors, but not much work has been done for FDIA identification. Identifying compromised battery sensors is important for the isolation and mitigation of cyberattacks and can improve system resilience.

We propose a FDIA detection, identification, and classification method by combining the SPM, UKF, and CUSUM algorithm. A non-segmented SPM battery model, modified from [34], was used to represent a stack of N series-connected batteries. A UKF provided estimations of the system states and produced residuals of the system outputs. A tuned CUSUM algorithm processed the residuals obtained by the UKF to detect, identify, and classify FDIAs in the voltage sensors. The results from the CUSUM algorithm were then compared to the χ^2 test, which was used as a baseline. The detection methods were performed offline and online using

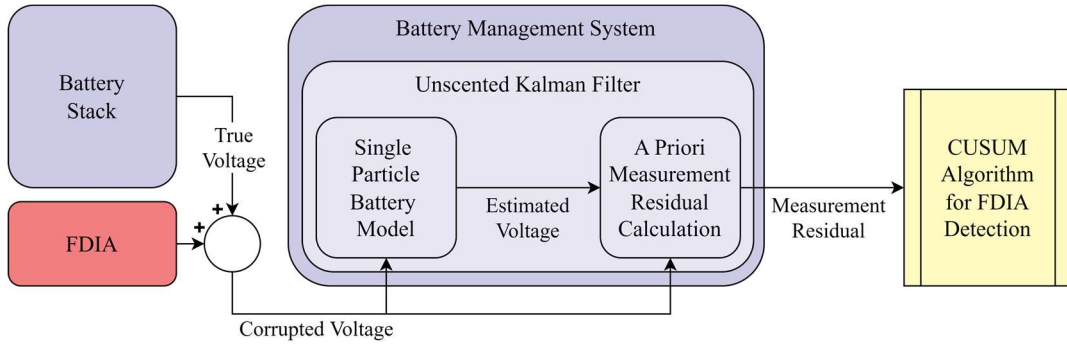


Fig. 1. Framework for FDIA detection in battery stacks.

MATLAB/Simulink. A description of the FDIA detection algorithm is given in Algorithm 1 and a block diagram of the process is given in Fig. 1.

Algorithm 1: Model-Based Approach for FDIA Detection

Input: Measurement a priori residual data

Output: FDIA detection, identification, and classification flags

1. Use SPM to represent battery stack dynamics.
 2. Use UKF to estimate states, measurements, and to calculate a priori measurement residual.
 3. Run a priori residual data through CUSUM algorithm for FDIA detection, identification, and classification.
 4. Continuously monitor battery stack for FDIAs; detection, identification, and classification flags are triggered upon FDIA injection.
-

The contributions of the proposed method are:

- 1) The application of the three-pronged method (utilizing a SPM, UKF, and tuned CUSUM algorithm) for **detection** of FDIAs in the voltage sensors of battery stacks.
- 2) **Identification** of the corrupted voltage sensors in the series-connected battery stack by employing the CUSUM algorithm.
- 3) FDIA bias **classification** using the CUSUM algorithm.
- 4) The implementation of the proposed approach in online and offline simulations.

The remainder of the paper is organized as follows. Section II gives the equations of the concentration-based model. The UKF estimator, which is used to estimate the states and measurements of each cell, is presented in Section III. The FDIA setup and the FDIA detection mechanisms are presented in Section IV. Section V includes case studies that were used to determine the effectiveness of the proposed method for detecting, identifying, and classifying FDIAs. Section VI. presents the results of the case studies and conclusions and future work are included in Section VII.

II. SINGLE PARTICLE BATTERY MODEL

Concentration models are used to describe the behavior of Li-ion battery cells [30], [34] - [36]; the SPM is derived from principles of the electrochemical reactions that occur during battery charge and discharge. In SPMs, each electrode is represented as a single spherical particle [30], in this case without any particle segmentation, whose area represents the “active area of the solid phase in the porous electrode” while neglecting the effects of the solution phase [35]. When simplifying the model from a spherical coordinate system to a parabolic profile to eliminate the spatial variable, the solid

phase concentration is represented by a second-order polynomial [35]. Since only one charge/discharge cycle is considered, battery degradation is negligible in this application. Therefore, the solid electrolyte interphase growth side reaction is disregarded to simplify the model. Table I gives the set of differential equations that were simplified from a set of differential and algebraic equations [34] used to model the cells and the parameter nomenclature was adopted from [35], [36].

TABLE I
SPM GOVERNING EQUATIONS FOR ELECTRODE J OF CELL H

Continuous System Model	
$\dot{x} = A_p x + B_p u$	
$y = V(x, u)$	
Governing Equations	
$\frac{dc_{j,h}^{avg}}{dt} = -\frac{3J_{j,h}}{r_{j,h}F}$	
$c_{j,h}^s = c_{j,h}^{avg} - \frac{J_{j,h}r_{j,h}}{5D_{j,h}F}$	
$J_{j,h} = 2i_{0,j,h} \sinh\left(\frac{0.5F}{RT}\eta_{j,h}\right)$	
$i_{0,j,h} = Fk_{j,h}(c_{j,h,max}^s - c_{j,h}^s)^{0.5}(c_{j,h}^s)^{0.5}(c_e)^{0.5}$	
$J_{n,h} = -\frac{I_{app}}{S_{n,h}}$	
$J_{p,h} = \frac{I_{app}}{S_{p,h}}$	
$S_{j,h} = \mathcal{A}_{j,h}A_{j,h}l_{j,h}$	
$\mathcal{A}_{j,h} = \frac{a_{j,h}}{r_{j,h}}$	
$\eta_{j,h} = \phi_{j,h} - U_{j,h}(\theta_{j,h})$	
$\theta_{j,h} = \frac{c_{j,h}^s}{c_{j,h,max}^s}$	
$v_{bat,h} = \phi_{p,h} - \phi_{n,h}$	
$V_{stack} = v_{bat,1} + \dots + v_{bat,N}$	
$\phi_{n,h} = \frac{RT}{0.5F} \sinh^{-1}\left(\frac{-I_{app}}{2S_{n,h}i_{0,n,h}}\right) + U_{n,h}(\theta_{n,h})$	
$\phi_{p,h} = \frac{RT}{0.5F} \sinh^{-1}\left(\frac{I_{app}}{2S_{p,h}i_{0,p,h}}\right) + U_{p,h}(\theta_{p,h})$	
$\varsigma_{j,h} = \frac{\theta_{j,h} - \theta_{j,0\%}}{\theta_{j,100\%} - \theta_{j,0\%}}$	

III. UNSCENTED KALMAN FILTER FOR STATE ESTIMATION

The UKF performs prediction and correction recursively. To handle nonlinearities in the functions, the UKF samples a minimum collection of SPs to represent the probability density of the function. Then the Unscented Transform (UT) is applied to the SPs, and the transformed SPs are used in the correction step of the UKF. Utilizing SPs and the UT allows

for an accurate estimator, since the SPs represent the full probability density of the function. The UKF is a well-established state estimation method, and the standard UKF equations are given in Table 2. For more information regarding the UKF's derivation and equations, [37] - [39] are suggested.

TABLE II
STANDARD UKF EQUATIONS

System Model
$x[k+1] = f(x[k], u[k], w[k])$ $y[k] = g(x[k], u[k], e[k])$ $w[k] \sim \mathcal{N}(0, Q), e[k] \sim \mathcal{N}(0, R)$
Initialization and Weights Calculation
$\hat{x}[0 0] = \mathbb{E}[x[0]]$ $P[0 0] = P[0]$ $W_m^o[k+1 k] = \frac{\lambda}{n+\lambda}$ $W_c^o[k+1 k] = W_m^o[k+1 k] + (1-a^2+b)$ $W_m^i[k+1 k] = W_c^i[k+1 k] = \frac{1}{2(n+\lambda)}$ $\lambda = a^2(n+\kappa) - n$
State Prediction
$\hat{x}[k+1 k] = A\hat{x}[k k] + Bu[k]$ $P[k+1 k] = AP[k k]A^T + Q[k]$
Sigma Points
$\mathcal{X}_0[k+1 k] = \hat{x}[k+1 k]$ $\mathcal{X}_i[k+1 k] = \hat{x}[k+1 k] + \left(\sqrt{(n+\lambda)P[k+1 k]}\right)_i$ $\mathcal{X}_{i+n}[k+1 k] = \hat{x}[k+1 k] - \left(\sqrt{(n+\lambda)P[k+1 k]}\right)_i$
Correction
$\hat{y}[k+1 k] = \sum_{i=0}^{2n} W_m^i \cdot g(\mathcal{X}_i[k+1 k], u[k])$ $P_{xy}[k+1 k] = \sum_{i=0}^{2n} W_c^i (\mathcal{X}_i[k+1 k] - \hat{x}[k+1 k]) \cdot \{g(\mathcal{X}_i[k+1 k], u[k]) - \hat{y}[k+1 k]\}^T$ $P_{yy}[k+1 k] = \sum_{i=0}^{2n} W_c^i (g(\mathcal{X}_i[k+1 k], u[k]) - \hat{y}[k+1 k]) \cdot \{g(\mathcal{X}_i[k+1 k], u[k]) - \hat{y}[k+1 k]\}^T$ $S[k+1] = P_{yy}[k+1 k] + R[k+1]$ $K[k+1] = P_{xy}[k+1 k] \cdot S^{-1}[k+1]$ $\hat{x}[k+1 k+1] = \hat{x}[k+1 k] + K[k+1] \cdot (y[k+1] - \hat{y}[k+1 k])$ $P[k+1 k+1] = P[k+1 k] - K[k+1]S[k+1]K^T[k+1]$
Residual
$z[k k-1] = y[k] - \hat{y}[k k-1]$

The UKF has parameters that can be tuned to suit the system and the authors have considered the standard parameters described in [39] in this paper. The number of states (n) is dependent on the number of batteries in the stack, as each battery has two states (the anode and cathode average concentration for each cell).

IV. DETECTION OF FDIA IN BATTERY STACKS

This section discusses the FDIA formulation and the FDIA detection mechanisms. The χ^2 error detector and a normalized innovation-based error identifier were used as a benchmark for comparison against the CUSUM algorithm. The CUSUM algorithm is a versatile detector that was applied for FDIA detection in multiple ECMs [31], [32], [37].

A. False Data Injection Attack Model

FDIAs are bias attacks, which are constant values added to the voltage sensor data that persists over the charge/discharge cycle. It is possible for the attack to be injected at any

time in the charge/discharge cycle.

$$y_a = y + \Delta y_a \quad (1)$$

where Δy_a is a small-magnitude positive or negative attack vector added to the measurement vector (y), yielding the manipulated measurement vector (y_a).

B. Chi-Squared Error Detector

Data integrity can be verified by comparing the estimated and measured system outputs. Because it is assumed that the measurements and state transition process are corrupted by additive zero-mean Gaussian noise with known covariance, the innovation and residuals of the estimation also follow a Gaussian distribution with zero-mean and known covariance. Since the square of the normalized Gaussian random variable follows a χ^2 distribution, the χ^2 test assesses the goodness of fit of estimated data [45], [46].

In this statistical test, the null hypothesis states that the residual data follows a χ^2 distribution with ν degrees of freedom, while the alternative hypothesis suggests the opposite. Measurements corrupted by non-zero disturbances, such as FDIA, are likely to introduce a bias in the residuals, which violates the assumption of zero-mean residual data, thus causing the null hypothesis to be rejected. To perform the χ^2 test, it is necessary to obtain the χ^2 score, $g[k]$, based on the squares of the normalized residuals:

$$g[k] = z[k|k-1]^T S[k]^{-1} z[k|k-1], \quad (2)$$

Since the additive noise is assumed to be Gaussian, $g[k]$ follows a χ^2 distribution with ν degrees of freedom. An arbitrarily defined threshold C_{χ^2} is used for the statistical test based on the χ^2 distribution and confidence level c_l . c_l defines the tradeoff between error detection sensitivity and tolerance for false positives. The expected rate of false positives is $1 - c_l$.

C. Normalized Innovation-Based Error Identification

After the χ^2 test detects an error, the innovations are analyzed to identify a candidate source of error. Inspired by the Largest Normalized Residual Test used in power system state estimation [46], a normalized innovation error identification approach can be applied. The hypothesis is that the largest normalized innovations should be associated with non-Gaussian errors and are good candidates for error sources. The vector of normalized innovations ($z_n[k]$) is defined as

$$z_n[k] = S_d[k]^{-1/2} z[k|k-1], \quad (3)$$

where $S_d[k]$ is a diagonal matrix containing the main diagonal elements of $S[k]$, used to obtain the standard deviations of the innovations vector.

Two rules are devised to identify the corrupted sensors. First, all sensors whose absolute value of normalized innovations exceed a threshold $|z_n[k]| > C_{z_n}$ are flagged as corrupt. If no sensor is flagged in this step, the sensor with the largest absolute normalized innovation is flagged.

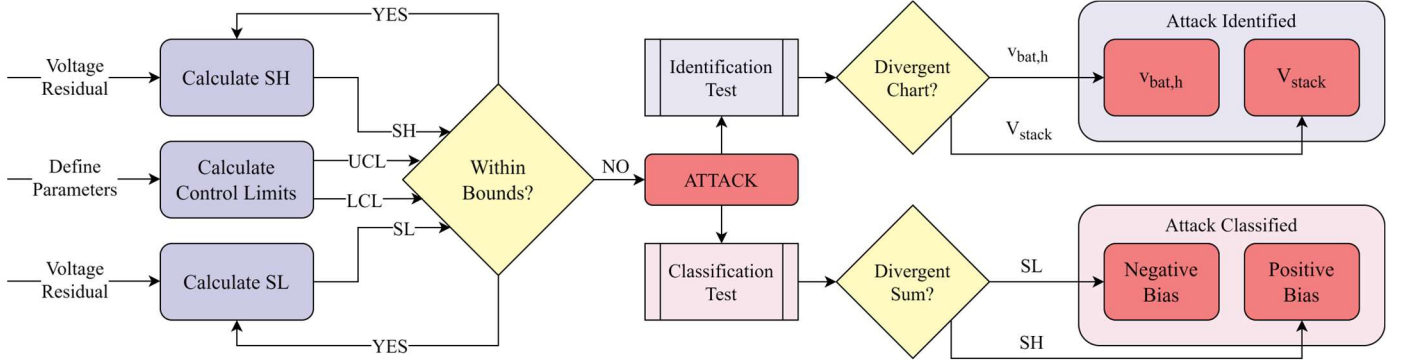


Fig. 2. The proposed CUSUM algorithm could be applied to detect, identify, and classify additive FDIA targeting the battery voltage sensors.

D. CUSUM Algorithm

The additive FDIA model is expected to change the average value of the measurement residuals, which the CUSUM algorithm is well-suited to detect. In broad terms, the CUSUM method recursively performs a regularized sum of the measurement residuals to determine if the sample mean of the residuals stays close to zero (normal case) or if it drifts from the expected mean, indicating an FDIA. Thresholds are implemented by defining an upper (UCL) and a lower (LCL) control limit as

$$UCL = h\sigma_{\bar{z}}, \quad (4)$$

$$LCL = -h\sigma_{\bar{z}}, \quad (5)$$

where h is a tunable parameter controlling the boundaries' width and $\sigma_{\bar{z}}$ is the estimated population standard deviation:

$$\sigma_{\bar{z}} = \frac{A_3\bar{s}}{3} \quad (6)$$

where \bar{s} is the mean of the sample standard deviations for the first m samples, and A_3 is a correction term taken from the Table of Control Chart Constants [48].

To detect both increasing and decreasing residual means, the CUSUM algorithm is implemented with two recursive cumulative sums: a high sum (SH) and a low sum (SL). $SH_k \in [0, \infty)$ and $SL_k \in (-\infty, 0]$ are initialized to zero and are then updated for each sample $k \geq 1$.

$$SH_k = \max(0, \bar{z}_k - \mu - \gamma\sigma_{\bar{z}} + SH_{k-1}) \quad (7)$$

$$SL_k = \min(0, \bar{z}_k - \mu + \gamma\sigma_{\bar{z}} + SL_{k-1}) \quad (8)$$

where \bar{z}_k is the mean of the residual (z) for sample k , μ is the population mean which is expected to be zero for residual data, and γ limits the correction term. The inputs to the CUSUM algorithm are moving averages of $z[k | k-1]$ with a window size of n_{samp} . An FDIA is detected when the values of SH or SL exceed the UCL or LCL, respectively.

The parameters of the CUSUM algorithm are typically tuned experimentally. References [30], [31], [48] present the CUSUM tuning in more detail. The value of h was tuned experimentally to eliminate false positives. A flowchart describing how the CUSUM algorithm can be used for FDIA detection, identification, and classification is given in Fig. 2.

V. CASE STUDIES

This section presents the case studies used to test the CUSUM algorithm's ability to detect, identify, and classify FDIA targeting the voltage sensors of batteries. Additionally, tests using a baseline method (the χ^2 test) are shown. Identification refers to the detectors' ability to identify the corrupted sensor and classification refers to the detector classifying the FDIA as positively or negatively biased. Online and offline studies are performed using MATLAB/Simulink.

A. Simulation Setup

A simulated stack of three series-connected battery cells was modeled using an SPM. The cells were Nickel Manganese Cobalt (NMC) chemistry and the parameters for Cell 1, listed in Table 3, were taken from [35], [50]. The equations for U_n and U_p were taken from [50]. The UKF was implemented considering a sampling period of 0.1 s. The capacity of each battery cell was experimentally estimated as 32 Ah. The stack has four voltage sensors ($v_{bat,1}$, $v_{bat,2}$, $v_{bat,3}$, and V_{stack}) that are vulnerable to FDIA.

TABLE III
BATTERY PARAMETERS [35]

Symbol	Negative Electrode	Positive Electrode	Unit
r	2×10^{-6}	2×10^{-6}	m
ε	0.490	0.590	-
l	88×10^{-6}	80×10^{-6}	m
\mathcal{A}	7.35×10^5	8.85×10^5	m^{-1}
A	603.06×10^{-6}	531.3×10^{-6}	m^2
S	64.68	70.8	m^2
D	3.9×10^{-14}	1×10^{-14}	$\text{m}^2 \text{s}^{-1}$
k	4.854×10^{-6}	2.252×10^{-6}	$(\text{Am}^{-5} \text{mol})^{1.5}$
c_{max}^s	30555	51555	mol m^{-3}
c_0^{avg}	$0.015c_{max}^s$	$0.98c_{max}^s$	mol m^{-3}
c_e	1×10^3	1×10^3	mol m^{-3}

To model the heterogeneity of the cell parameters, the parameters for Cells 2 and 3 were generated by adding a small random percent [-0.01, 0.01] to Cell 1's parameters.

$$P_{2...N} = P_1 + vP_1 \quad (9)$$

where P represents the parameters of each cell, that could be r , ε , l , a , S , D , or k , and v is a small random percentage used to create a small variation in the cells' parameters. The maximum concentration, average electrolyte, and initial average concentrations are equal for all cells.

Assuming that the SPM model is accurate, the process noise covariance matrix (Q) was set to relatively low values. The measurement noise covariance matrix (R) was a diagonal matrix whose nonzero elements were set to 0.1% of the expected maximum voltage of each cell (4.2 V).

The SPM and UKF were simulated using Simulink for a single charge/discharge cycle which was simulated to take 8000 s (including rest times). The UKF generated a priori residuals for each sensor and χ^2 test statistics. During the offline analysis, the χ^2 test and CUSUM algorithm were run on a single charge/discharge cycle of data using MATLAB. During the online analysis, the χ^2 test and CUSUM algorithm were run in Simulink in parallel with the UKF estimator. UKF, CUSUM algorithm, and χ^2 test parameters are given in Table 4, Table 5, and Table 6, respectively.

TABLE IV
UKF PARAMETERS [39]

Parameter	n	a	b	κ	λ
Value	6	0.1	2	0	-5.94

TABLE V
CUSUM PARAMETERS [32]

Parameter	h	γ	m	n_{samp}	α	β	δ
Value	11.8089	0.5	86	12	0.0027	0.01	1

TABLE VI
CHI-SQUARED DETECTOR AND NORMALIZED INNOVATION-BASED ERROR IDENTIFICATION PARAMETERS [32]

Parameter	ν	c_l	C_{χ^2}	C_{z_n}
Value	4	99.999%	28.4733	3

The input to the system, the applied stack current, was 30 A during charge and -30 A during discharge. A current of 0 A was applied during rest periods. Figure 3 gives a) the input current, b) the estimated voltage drop for Cell 1, c) the estimated concentration of the cathode and d) the estimated concentration of the anode. The cell voltage varied from roughly 2.9 to 4.1 V, and due to the series-connected configuration of the cells, the stack voltage remained within 8.7 to 12.3 V.

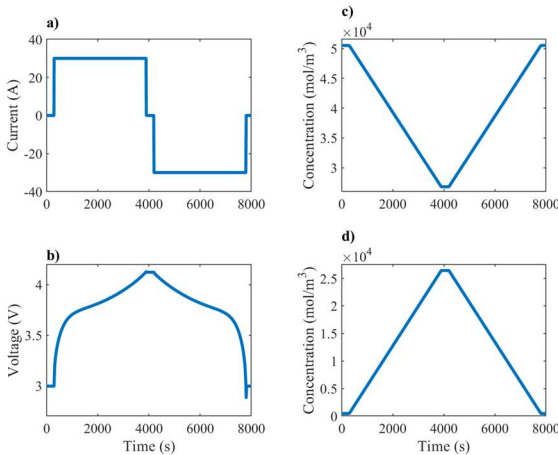


Fig. 3. a) input current b) estimated voltage drop across Cell 1 c) estimated concentration of the cathode d) estimated concentration of the anode.

B. Protocol for FDIA Vectors

To assess the effectiveness of the algorithms in detecting, identifying, and classifying FDIAs, simulations where FDIAs were injected into the voltage sensors of the battery stack were run. To represent different attack scenarios, the following parameters were varied: the attack injection time, number of sensors targeted, targeted sensor(s), and the value of the positive or negative bias attack. The attack time for each sensor was chosen randomly following a uniform distribution between 2000 s and 7000 s, and the FDIA formulation was consistent with the cell voltage sensor attacks in [50]. The maximum possible attack magnitude was selected as ± 20 mV, since in [30] attacks larger than ± 20 mV were detected with the χ^2 test. Larger magnitude FDIA values were also tested (with values up to ± 2 V), and the detection results were the same as small magnitude FDIA, therefore small magnitude FDIA was focused on in the case studies since it is more likely to be missed by detection mechanisms. Every combination of sensor attacks was tested, including single-sensor attacks and multi-sensor attacks by cycling through the targeted sensor(s) each simulation. A summary of the main test protocol parameters is given in Table 7.

TABLE VII
FDIA VECTOR CHARACTERISTICS

Parameter	Value
Attack magnitude range*	-20 mV to 20 mV
Attack magnitude resolution	153 μ V
Attack time range	2000 s to 7000 s
Number of test runs	3000
Vulnerable sensors	$v_{bat,h}, v_{stack}$
Number of attacks on each sensor	1600

*Excluding 0 V.

VI. RESULTS

A. Offline Analysis

This section presents the results of the offline batch simulations for FDIA detection, identification, and classification using the CUSUM algorithm, χ^2 test, and normalized innovation error identifier.

1) CUSUM

The CUSUM algorithm minimized the false alarm rate while maximizing accurate detection, identification, and classification of FDIAs. An FDIA is flagged when either the SL or SH crosses the LCL or UCL, respectively. The h parameter is tuned to obtain a false alarm rate of zero when no FDIA is injected (Fig. 4.). The CUSUM parameters are validated using 900 charging cycles with no FDIAs.

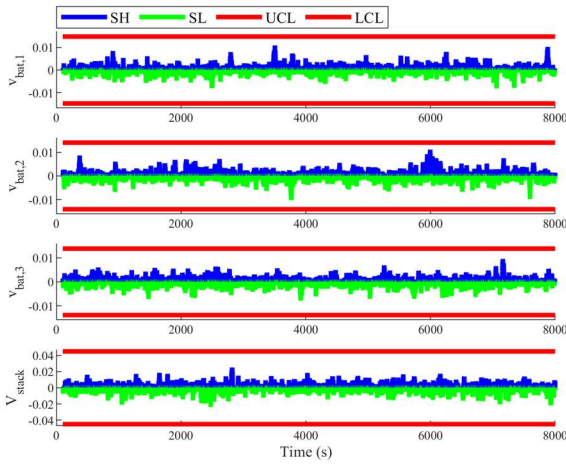


Fig. 4. CUSUM chart when no FDIA was injected.

The CUSUM algorithm was able to detect FDIA in 99.83% of the 3000 offline attack simulations. The correct identification rate was 97% and the correct classification rate was 97%. The results for the offline batch simulations are given in Table VIII.

TABLE VIII
OFFLINE CUSUM BATCH SIMULATION RESULTS

Test	Total Tests	Correct	Incorrect	Accuracy
No Attack	900	900	0	100%
Detection	3000	2995	5	99.83%
Identification	3000	2910	90	97%
Classification	3000	2910	90	97%

The CUSUM charts for each voltage sensor are given for a single sensor attack and multi sensor attacks. The divergent CUSUM chart corresponded to the attacked sensor and the divergent SL or SH corresponded to a negatively or positively biased FDIA, respectively. For a single sensor attack, a 20 mV attack was injected into the $v_{bat,1}$ sensor at 5400 s (Fig. 5); shortly after the attack was injected the $v_{bat,1}$ sensor's SH crossed the UCL.

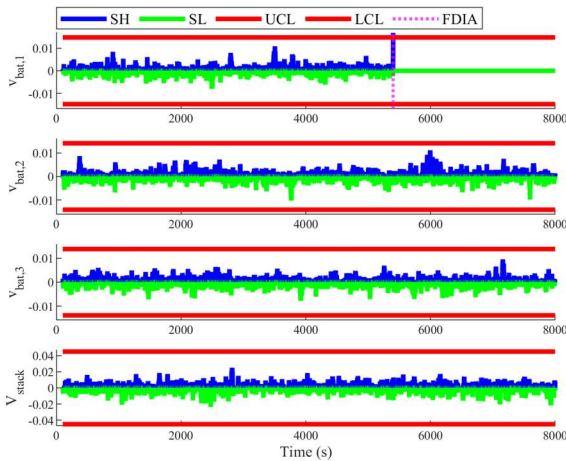


Fig. 5. CUSUM chart following a single sensor FDIA.

In the cascaded multi sensor attack case (Fig. 6) a 20 mV attack was injected into the $v_{bat,1}$ and $v_{bat,3}$ sensors at 5350 s and 5450 s, respectively, and a -20 mV attack was injected into the $v_{bat,2}$ and V_{stack} sensors at 5400 s and 5500 s, respectively. The divergent SHs flagged positively biased

FDIAs, and similarly, the divergent SLs flagged negatively biased FDIAs. The sums remained within the UCL and LCL until FDIA was injected into that sensor, allowing for the detection and identification of attacks.

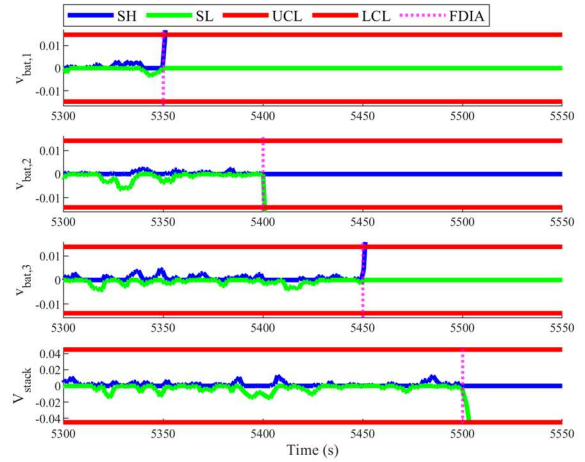


Fig. 6. CUSUM chart following a cascaded multi sensor FDIA.

Next, a simultaneous multi sensor FDIA scenario is given; a 20 mV FDIA was injected into each voltage sensor at 2500s. Each CUSUM chart successfully detected, identified, and classified the simultaneous FDIAs, as the corresponding SH crossed the UCL in each chart (Fig. 7).

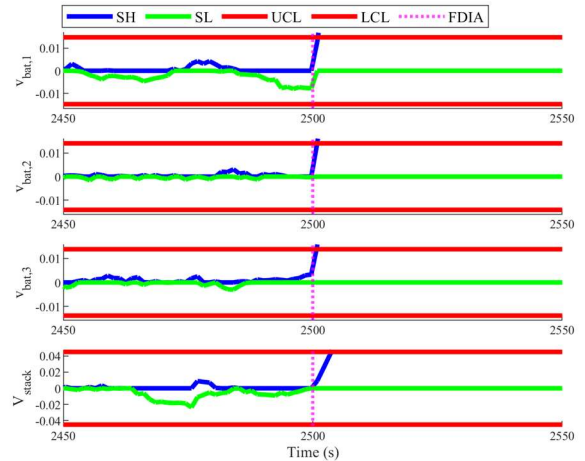


Fig. 7. CUSUM chart following a simultaneous multi sensor FDIA.

2) χ^2 Test

The χ^2 test has a false positive rate that is correlated to the confidence level of the test, and based on its selected parameters some false positives are expected. A FDIA is flagged by the χ^2 test when the χ^2 test statistic exceeds the selected detection threshold. 900 simulations were performed where no attack was injected, and the χ^2 test flagged attacks in all simulations resulting in a false positive rate of 100%. A chi-squared chart following an attack-free simulation is given in Fig. 8; the χ^2 test statistic surpasses the threshold multiple times causing false alarms.

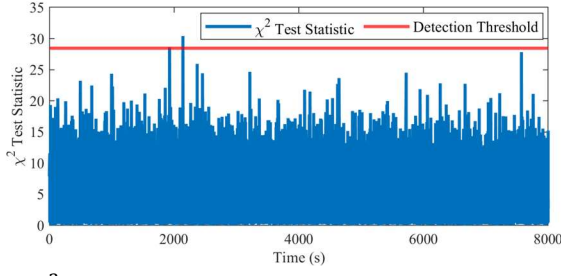


Fig. 8. χ^2 chart when no FDIA was injected.

The attack simulations with the CUSUM algorithm were repeated with the χ^2 test as the detector, and the normalized innovation error identifier as the identification and classification method. The baseline methods accurately detected FDIA in 100% of simulations, identified FDIA in 6.17% of simulations and classified FDIA in 2.53% of simulations. Due to its high false positive rate, the χ^2 test requires an additional method to determine if flagged data is FDIA or inaccuracies with the detector. The batch simulation results for the baseline methods are given in Table 9.

TABLE IX
OFFLINE BASELINE METHOD BATCH SIMULATION RESULTS

Test	Total Tests	Correct	Incorrect	Accuracy
No Attack	900	0	900	0%
Detection	3000	3000	0	100%
Identification	3000	185	2815	6.17%
Classification	3000	76	2924	2.53%

The χ^2 charts for a single sensor attack and multi sensor attack are given in Fig. 9 and Fig. 10. The single sensor and cascaded multi sensor attack scenarios are identical to those evaluated by the CUSUM algorithm, and the simultaneous multi sensor attack is excluded from this study. In the single sensor attack (Fig. 9), the χ^2 test statistic went well above the detection threshold following the 20 mV attack on the $v_{bat,1}$ sensor; although, there were multiple false positives prior to the injected attack at 5400 s.

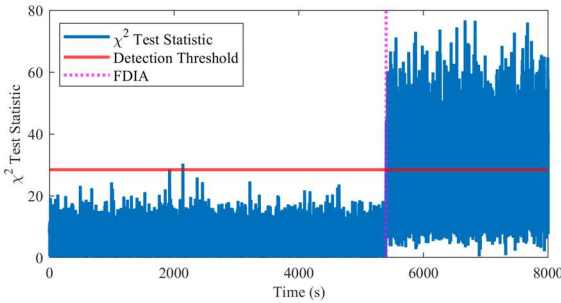


Fig. 9. χ^2 chart following a single sensor FDIA.

In the cascaded multi sensor attack (Fig. 10) a 20 mV attack was injected into $v_{bat,1}$ at 5350 s, a -20 mV attack was injected into $v_{bat,2}$ at 5400 s, a 20 mV attack was injected into $v_{bat,3}$ at 5450 s, and a -20 mV attack was injected into V_{stack} at 5500 s; the χ^2 test statistic gradually increased as each FDIA was injected into the voltage sensors and surpassed the detection threshold to indicate an attack, but there were multiple false positives before the first FDIA was injected.

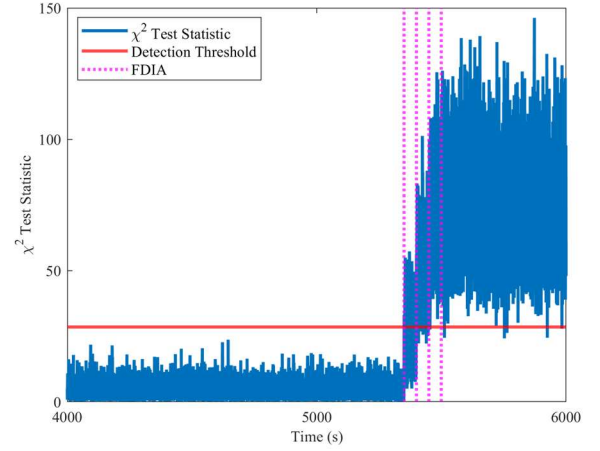


Fig. 10. χ^2 chart following a cascaded multi sensor FDIA.

B. Online Analysis

An online analysis was performed where the χ^2 test and CUSUM algorithm were run in parallel with state estimation to detect, identify, and classify FDIAs as they occurred.

1) CUSUM

An online CUSUM algorithm was run every 1.2 s in Simulink to detect, identify, and classify FDIAs injected into the voltage sensors of the simulated battery stack. The parameters of the CUSUM algorithm were the same as the offline implementation. A CUSUM flag was used on each sensor to detect FDIAs and identify the targeted sensor. A flag of zero indicated no attack was injected, a flag of one indicated a positive attack was injected, and a flag of negative one indicated a negative attack was injected. The online CUSUM algorithm had a false positive rate of 0%.

Two attack scenarios are given, a single sensor attack (Fig. 11) and a cascaded multi sensor attack (Fig. 12). In the single sensor attack, a -10 mV FDIA was injected into the $v_{bat,1}$ sensor at 5500 s and 2 s after the attack was injected, the negative $v_{bat,1}$ flag was triggered, accurately detecting the negatively biased FDIA in the $v_{bat,1}$ sensor.

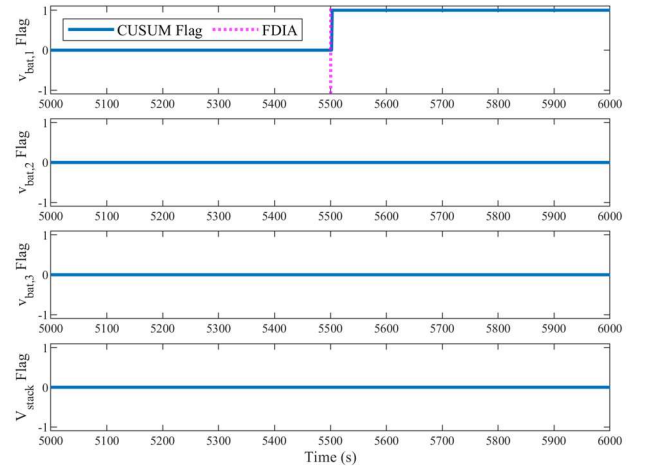


Fig. 11. Online CUSUM flag following a single sensor FDIA.

All sensors were attacked in the cascaded multi sensor attack (Fig. 12). First, a 20 mV FDIA was injected into the $v_{bat,1}$ sensor at 5350 s and was detected by the positive $v_{bat,1}$

flag 0.8 s later. Next, a -20 mV attack was injected into the $v_{bat,2}$ sensor at 5400 s, which was detected by the negative $v_{bat,2}$ flag 1.2 s after its injection. Then, the $v_{bat,3}$ sensor was corrupted by a 20 mV FDIA at 5450 s and 1.6 s after its injection, the positive $v_{bat,3}$ flag detected the attack. Finally, at 5500 s, the V_{stack} sensor was injected with a -20 mV FDIA, which was detected within 2 s by the negative V_{stack} flag.

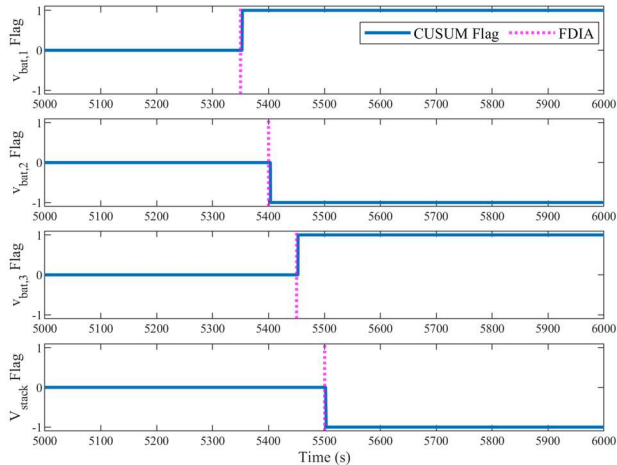


Fig. 12. Online CUSUM flag following a cascaded multi sensor FDIA.

2) χ^2 Test

The χ^2 test was implemented online using Simulink, where the χ^2 test statistic was compared to its detection threshold each 0.1 s. When the χ^2 test statistic surpassed its detection threshold, the χ^2 attack flag was set to one, otherwise it was set to zero. The online χ^2 test detection results are given in Fig. 13 when no attack was injected, and in Fig. 14 when a -10 mV attack was injected to the $v_{bat,2}$ sensor at 5500 s. When no FDIA was injected the χ^2 test has a false positive rate of zero (Fig. 13).

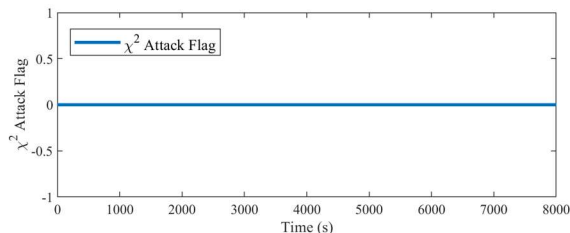


Fig. 13. Online χ^2 flag when no FDIA was injected.

Prior to the injected FDIA, the χ^2 test flag remained at zero, and after the attack was injected at 5500 s the χ^2 test statistic was sporadically above the detection threshold, accurately detecting the injected FDIA (Fig. 14).

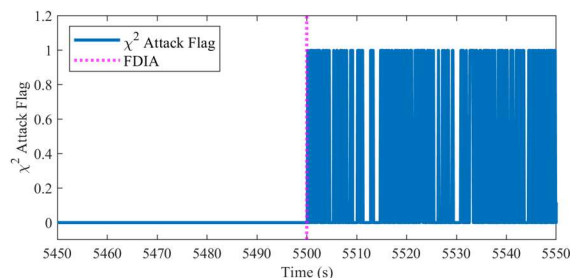


Fig. 14. Online χ^2 flag following a single sensor FDIA.

C. Discussion of Results

When comparing the CUSUM algorithm with the other residual-based approaches for offline attack detection, identification, and classification, the CUSUM method was far superior. While the χ^2 and normalized innovation approaches rely on single time step estimates to determine if a given set of measurements is anomalous or not, the CUSUM algorithm's response to biases in measurements considers time-series data. This fundamental difference means that the χ^2 detector might be able to respond more quickly to sensor attacks, but it is much more prone to false positives. Repeatedly flagging false alarms would make it challenging to respond to true FDIAs in the system, therefore the CUSUM algorithm would be better suited for grid-scale applications since its false alarm rate was tuned to 0%.

In addition, the CUSUM algorithm performed similarly to the χ^2 test in terms of FDIA detection, with detection rates of 99.83% and 100%, respectively. On the other hand, the CUSUM algorithm was far superior to the normalized innovation-based error identifier during identification and classification testing. The CUSUM algorithm was able to identify the attacked sensor in 97% of the cases, whereas the normalized innovation-based error identifier could only identify the corrupted sensor in 6.17% of trials. In addition, the CUSUM algorithm was capable of accurately classifying the FDIA vector as positive or negative in 97% of simulations, while the normalized innovation-based error identifier could only classify attacks correctly in 2.53% of the simulations. Due to its far superior performance in terms of false positive rate, attack identification, and attack classification, and similar performance in terms of FDIA detection, it can be concluded that the CUSUM algorithm is more suitable for attack detection in this application compared to the χ^2 test and normalized innovation-based error identifier.

VII. CONCLUSION

The detection and identification of FDIAs targeting the voltage sensors of BESSs is a critical research problem to ensure the safe operation of the power grid. In this paper, a three-part method is proposed that uses a battery model (the SPM) to model a series-connected stack of three batteries, a nonlinear estimator (the UKF) to perform estimation, and a tuned CUSUM algorithm for FDIA detection, identification, and classification. The CUSUM algorithm postprocesses the residuals from battery voltages estimated by the UKF to determine a shift in their means, which indicates an FDIA. To demonstrate the merit of the proposed method, results of the CUSUM algorithm were compared to a χ^2 test. Online and offline simulations were performed for single and multi sensor attacks with random attack injection times and magnitudes, to evaluate the effectiveness of both detection algorithms.

Four metrics were used to compare the CUSUM algorithm and the χ^2 test: false positive rate, detection, identification, and classification. During the false positive rate tests, FDIAs were not injected to the system and the detection algorithms

were run to determine if either algorithm would register a false alarm. During offline tests, the CUSUM algorithm was found to have a false alarm rate of 0%, while the χ^2 test had multiple false alarms in each simulation – resulting in a false positive rate of 100%. During the detection tests, the CUSUM algorithm was able to detect FDIA in 99.83% of the simulations; only missing attacks smaller than $\pm 500 \mu\text{V}$. On the other hand, the χ^2 test detected FDIA in 100% of the simulations, but there was no way to differentiate the false alarms from true attacks, making the χ^2 test an unreliable detector compared to the CUSUM algorithm. The identification tests were done by evaluating if the corrupted sensors were correctly identified by the algorithms. The CUSUM algorithm identified the compromised sensors in 97% of the testcases whereas the normalized innovation-based error identifier only identified the appropriate sensors in 6.17% of trials. Lastly, during the classification tests, the CUSUM algorithm was able to classify positively biased attacks when the SH diverged and negatively biased attacks when the SL diverged, and did so accurately in 97% of the simulations, and the normalized innovation-based error identifier could only classify attacks correctly in 2.53% of cases. So, the CUSUM algorithm was found to greatly outperform the χ^2 test and normalized innovation-based error identifier in terms of false positive rate, identification, and classification, and performed similarly to the χ^2 test in terms of detection.

In future research it would be valuable to design remedial actions to respond to and mitigate the damage from injected FDIAs during single sensor and multi sensor attacks. In this paper, the corrupted sensors are accurately identified when using the CUSUM algorithm during online and offline simulations, which is an important first step in implementing attack isolation protocols. Another important research direction is to study the effect of FDIAs on a true battery system which would require an experimental setup.

ACKNOWLEDGMENT

The authors thank Dr. Imre Gyuk, Director of the Energy Storage Program, for his continued support. The authors thank Dr. Ujjwol Tamrakar for his technical advice.

REFERENCES

- [1] Z. Hameed, S. Hashemi, and C. Træholt, "Site Selection Criteria for Battery Energy Storage in Power Systems," *2020 IEEE Canadian Conf. on Electr. & Comp. Eng. (CCECE)*, London, ON, Canada, 2020.
- [2] R. H. Byrne, T. A. Nguyen, D. A. Copp, B. R. Chalamala, and I. Gyuk, "Energy management and optimization methods for grid energy storage systems," *IEEE Access*, vol. 6, pp. 13 231–13 260, 2018.
- [3] R. Xiong, Q. Yu, W. Shen, C. Lin and F. Sun, "A sensor fault diagnosis method for a lithium-ion battery pack in electric vehicles," in *IEEE Trans. Power Electronics*, vol. 34, no. 10, pp. 9709-9718, Oct. 2019, doi: 10.1109/TPEL.2019.2893622.
- [4] F. Han, K. See, Y. Feng, X. Yu and X. Yi, "Online SoC estimation for Li-ion batteries: A survey explore the distributed secure cloud management to battery packs," *2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2017, pp. 1838-1843, doi: 10.1109/ICIEA.2017.8283137.
- [5] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia and M. A. Al Faruque, "A security perspective on battery systems of the Internet of Things", *J. Hardw. Syst. Secur.*, vol. 1, no. 2, pp. 188-199, Jun. 2017.
- [6] M. T. Lawder, B. Suthar, P.W. C. Northrop, S. De, C. M. Hoff, O. Leitermann, M. L. Crow, S. Santhanagopalan, and V. R. Subramanian, "Battery energy storage system (BESS) and battery management system (BMS) for grid-scale applications," *Proceedings of the IEEE*, vol. 102, no. 6, pp. 1014–1030, June 2014.
- [7] M. Lelie, T. Braun, M. Knips, H. Nordmann, F. Ringbeck, H. Zappen, and D. Sauer, "Battery management system hardware concepts: An overview," *Applied Sciences*, vol. 8, no. 4, p. 534, Mar 2018
- [8] M. Zeng, P. Zhang, Y. Yang, C. Xie, and Y. Shi, "SOC and SOH joint estimation of the power batteries based on fuzzy unscented Kalman filtering algorithm," *Energies*, vol. 12, no. 16, 2019.
- [9] N. Kharlamova, S. Hashemi, and C. Træholt, "The cyber security of battery energy storage systems and adoption of data-driven methods," in *2020 IEEE Third Int. Conf. on Artificial Intelligence and Knowledge Eng. (AIKE)*, 2020, pp. 188–192.
- [10] N. Kharlamova, S. Hashemi and C. Træholt, "Data-driven approaches for cyber defense of battery energy storage systems," *Energy and AI*, vol. 5, pp. 188-192, 2021. doi: 10.1016/j.egyai.2021.100095.
- [11] "Operational risk management in the U.S. energy storage industry: Lithium-ion fire and thermal event safety," Energy Storage Association, Tech. Rep., Sep 2019.
- [12] R.D. Trevizan, J. Obert, V. De Angelis, T.A. Nguyen, V.S. Rao and B.R. Chalamala, "Cyberphysical Security of Grid Battery Energy Storage Systems," *IEEE Access*, vol. 10, pp. 59675-59722, 2022
- [13] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *2018 IEEE Transportation Electrification Conf. and Expo (ITEC)*, June 2018, pp. 934–938.
- [14] A. Adhikaree, T. Kim, J. Vagdoda, A. Ochoa, P. J. Hernandez, and Y. Lee, "Cloud-based battery condition monitoring platform for large-scale lithium-ion battery energy storage systems using internet-of-things (IoT)," *2017 IEEE Energy Conversion Congress and Exposition (ECCE)*, Cincinnati, OH, USA, 2017.
- [15] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018. 51.
- [16] J. Fruhlinger. "Stuxnet explained: The first known cyberweapon." Csoonline.com. <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html> (accessed: Sept. 24, 2023)
- [17] H. Rahimpour, J. Tusek, A. Abuadba, A. Seneviratne, T. Phung, A. Musleh, B. Liu, "Cybersecurity Challenges of Power Transformers," 2023, arXiv:2302.13161
- [18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of the 16th ACM Conf. on Computer and Comm. Security, ser. CCS '09*. New York, NY, USA: ACM, 2009, pp. 21–32.
- [19] E. -N. S. Youssef and F. Labeau, "False Data Injection Attacks Against State Estimation in Smart Grids: Challenges and Opportunities," *2018 IEEE Canadian Conf. on Electrical & Comp. Eng. (CCECE)*, Quebec, QC, Canada, 2018, pp. 1-5, doi: 10.1109/CCECE.2018.8447683.
- [20] Y. Mo and B. Sinopoli, "On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks," in *IEEE Trans. Automatic Control*, vol. 61, no. 9, pp. 2618-2624, Sept. 2016.
- [21] K. Fang, Y. Huang, Q. Huang, S. Yang, Z. Li and H. Cheng, "An Event Detection Approach Based on Improved CUSUM Algorithm and Kalman Filter," *2020 IEEE 4th Conf. Energy Internet and Energy System Integration (EI2)*, 2020, pp. 3400-3403.
- [22] M. Severo and J. Gama, "Change Detection with Kalman Filter and CUSUM", *Proc. Int. Conf. Discovery Science*, pp. 243-254, 2006.
- [23] H. Lee, G. Bere, K. Kim, J. J. Ochoa, J. -h. Park and T. Kim, "Deep Learning-Based False Sensor Data Detection for Battery Energy Storage Systems," *2020 IEEE CyberPELS (CyberPELS)*, Miami, FL, USA, 2020, pp. 1-6, doi: 10.1109/CyberPELS49534.2020.9311542.
- [24] H. -J. Lee, K. -T. Kim, J. -H. Park, G. Bere, J. J. Ochoa and T. Kim, "Convolutional Neural Network-Based False Battery Data Detection and Classification for Battery Energy Storage Systems," in *IEEE Trans. Energy Conversion*, vol. 36, no. 4, pp. 3108-3117, Dec. 2021, doi: 10.1109/TEC.2021.3061493.
- [25] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, et al., "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581-595, Oct. 2020.
- [26] D. Ye and T. -Y. Zhang, "Summation Detector for False Data-Injection Attack in Cyber-Physical Systems," in *IEEE Trans. Cybernetics*,

- vol. 50, no. 6, pp. 2338-2345, June 2020, doi: 10.1109/TCYB.2019.2915124.
- [27] H. Chen, E. Tian, L. Wang and S. Liu, "A Joint Online Strategy of Measurement Outliers Diagnosis and State of Charge Estimation for Lithium-Ion Batteries," in *IEEE Trans. Industrial Informatics*, vol. 19, no. 5, pp. 6387-6397, May 2023, doi: 10.1109/TII.2022.3202949.
- [28] P. D. Hanlon and P. S. Maybeck, "Characterization of Kalman filter residuals in the presence of mismodeling," in *IEEE Trans. Aerospace and Electronic Syst.*, vol. 36, no. 1, pp. 114-131, Jan. 2000.
- [29] P. Zhuang and H. Liang, "False Data Injection Attacks Against State-of-Charge Estimation of Battery Energy Storage Systems in Smart Distribution Networks," *IEEE Trans. Smart Grid*, vol. 12, pp. 2566-2577, 2021.
- [30] D. M. Rosewater, D. A. Copp, T. A. Nguyen, R. H. Byrne and S. Santoso, "Battery Energy Storage Models for Optimal Control," in *IEEE Access*, vol. 7, pp. 178357-178391, 2019, doi: 10.1109/ACCESS.2019.2957698
- [31] V. O'Brien, R. D. Trevizan and V. Rao, "Detecting False Data Injection Attacks to Battery State Estimation Using Cumulative Sum Algorithm," *53rd North Am. Power Symp. (NAPS)*, Nov. 2021 pp 1-6.
- [32] V. O'Brien, V. Rao and R.D. Trevizan, "Detection of False Data Injection Attacks in Battery Stacks Using Physics-Based Modeling and Cumulative Sum Algorithm," in *Proc. 2022 IEEE Power and Energy Conf. at Illinois (PECI)*, 2022, doi: 10.1109/PECI54197.2022.9744036.
- [33] Z. Liu and H. He, "Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended Kalman filter", *Appl. Energy*, vol. 185, pp. 2033-2044, 2017.
- [34] Y. Cao, S. B. Lee, V. R. Subramanian, V. M. Zavala, "Multiscale model predictive control of battery systems for frequency regulation markets using physics-based models," *J. of Process Control*, vol. 90, pp. 46-55, June 2020. <https://doi.org/10.1016/j.jprocont.2020.04.001>.
- [35] Santhanagopalan, S., Guo, Q., Ramadass, P., & White, R. E. "Review of Models for Predicting the Cycling Performance of Lithium Ion Batteries." *J. of Power Sources*, vol. 156, no. 2, pp. 620 – 628. 2006. <http://dx.doi.org/10.1016/j.jpowsour.2005.05.070>.
- [36] D. Di Domenico, A. G. Stefanopoulou, and G. Fiengo, "Lithium-Ion Battery State of Charge and Critical Surface Charge Estimation Using an Electrochemical Model-Based Extended Kalman Filter." *J. of Dyn. Syst. Meas. and Control-Trans. of The ASME*, vol. 132, pp. 061302-1-061302-11, Nov. 2010.
- [37] V. O'Brien, V. Rao and R. D. Trevizan, "Detection of False Data Injection Attacks in Ambient Temperature-Dependent Battery Stacks," in *2022 IEEE Elect. Energy Storage Appl. and Technol. Conf. (EESAT)*, Austin, TX, USA, 2022, pp. 1-6, doi: 10.1109/EESAT55007.2022.9998042.
- [38] G. L. Plett, "Sigma-point Kalman filtering for battery management systems of LiPb-based HEV battery packs: Part 1: Introduction and state estimation," *J. of Power Sources*, vol. 161, no. 2, pp. 1356 – 1368, 2006.
- [39] P. Pasek and P. Kaniewski, "Unscented Kalman filter application in personal navigation", in *Proc. Radioelectronic Syst. Conf.*, Jachranka, Poland, 2019, 114421C.
- [40] L. Ma, Y. Xu, H. Zhang, F. Yang, X. Wang, and C. Li, "Co-estimation of state of charge and state of health for lithium-ion batteries based on fractional-order model with multi-innovations unscented Kalman filter method," *J. of Energy Storage*, vol. 52, 2022.
- [41] N. Wassiliadis, J. Adermann, A. Frericks, M. Pak, C. Reiter, B. Lohmann, and M. Lienkamp, "Revisiting the dual extended Kalman filter for battery state-of-charge and state-of-health estimation: A use-case life cycle analysis," *J. of Energy Storage*, vol. 19, pp. 73 – 87, 2018.
- [42] L. Ling and Y. Wei, "State-of-Charge and State-of-Health Estimation for Lithium-Ion Batteries Based on Dual Fractional-Order Extended Kalman Filter and Online Parameter Identification," *IEEE Access*, vol. 9, pp. 47588-47602, 2021.
- [43] S. Zhao, S. R. Duncan, and D. A. Howey, "Observability Analysis and State Estimation of Lithium-Ion Batteries in the Presence of Sensor Biases," *IEEE Trans. Control Syst. Tech.*, vol. 25, pp. 326-333, 2017.
- [44] H. Fawzi, P. Tabuada and S. Diggavi, "Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks," in *IEEE Trans. Automatic Control*, vol. 59, no. 6, pp. 1454-1467, June 2014, doi: 10.1109/TAC.2014.2303233.
- [45] R. Mehra and J. Peschon, "An innovation approach to fault detection and diagnosis in dynamic systems", *Automatica*, vol. 7, no. 5, pp. 637-640, Sep. 1971.
- [46] B. Brumback and M. Srinath, "A Chi-square test for fault-detection in Kalman filters," in *IEEE Trans. on Autom. Control*, vol. 32, no. 6, pp. 552-554, June 1987, doi: 10.1109/TAC.1987.1104658.
- [47] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*; Springer: New York, NY, USA, 1999.
- [48] W. C. Navidi, *Statistics for Engineers and Scientists*, New York, NY, USA: McGraw-Hill Education, 2015
- [49] "e-Handbook of Statistical Methods," National Institute of Standards and Technology and SEMATECH, Jun 2012. [Online]. Available: <http://www.itl.nist.gov/div898/handbook/>
- [50] P. Ramadass, B. Haran, P.M. Gomadam, R.E. White, B.N. Popov, "Development of First Principles Capacity Fade Model for Li-Ion Cells," *J. Electrochem. Soc.*, vol. 151, no. 2, pp. A196–A203, 2004
- [51] V. O'Brien, V. S. Rao and R. D. Trevizan, "Detection of False Data Injection Attacks in Battery Stacks Using Input Noise-Aware Nonlinear State Estimation and Cumulative Sum Algorithms," in *IEEE Trans. on Industry Appl.*, doi: 10.1109/TIA.2023.3308548.



Victoria A. O'Brien received the B.S. degree, M.S. degree, and Ph.D. degree in electrical engineering from Texas Tech University, Lubbock, TX, USA in 2020, 2021, and 2023, respectively. She currently works as an R&D S&E electrical engineer in the Electric Grid Security & Communications group at Sandia National Laboratories, Albuquerque NM, USA. From 2021 to 2023 she worked at Sandia National Laboratories as a Year-Round R&D Graduate Intern for the Energy Storage Technology & Systems Department in Albuquerque, NM, USA. From 2020 to 2023, she worked as a Research Assistant at Texas Tech University, Lubbock, TX, USA. Her research interests include the cybersecurity of battery energy storage systems, control systems, and the smart grid. Dr. O'Brien was a recipient of the Graduate Assistance in Areas of National Need (GAANN) Fellowship (Texas Tech University) in 2020, and the Power and Energy Conference at Illinois (PECI) "Best Paper" Award in 2022.



Vittal Rao received the M. Tech and Ph.D. degrees in electrical engineering from the Indian Institute of Technology Delhi. He is currently an emeritus professor of electrical and computer engineering with Texas Tech University. He was a Rutledge-Emerson Distinguished Professor of electrical and computer engineering and the Director of Intelligent Systems Center with the University of Missouri-Rolla (UMR). He has also served as the Program Director with the National Science Foundation. His research interests include cyber security of smart grid and industrial control systems, and distributed energy management systems. He was a recipient of the IEEE Centennial Medal, the Faculty Excellence Awards at UMR, and the NSF Director Award for Program Management Excellence.



Rodrigo D. Trevizan is research engineer at Sandia National Laboratories. He received the *Diplôme d'Ingénieur* in Power Systems Engineering from the Grenoble Institute of Technology (ENSE3) in 2011, the B.S. and M.Sc. degree in Electrical Engineering from the Federal University of Rio Grande do Sul, Brazil, in 2012 and 2014, respectively, and the Ph.D in Electrical Engineering from the University of Florida in 2018. He has authored research papers on the subjects of cyberphysical security of battery energy storage systems, techno-economic analysis of energy storage systems, control of energy storage systems and demand response for power grid stabilization, power system state estimation, and detection of nontechnical losses in power distribution. His current research interests are cyberphysical security, state estimation, control, and valuation of energy storage systems. An IEEE member since 2013, he serves as an Associate Editor for IEEE Transactions on Sustainable Energy.