# Detection of False Data Injection Attacks in Ambient Temperature-Dependent Battery Stacks

Victoria Obrien
*Electrical Engineering Department*
*Texas Tech University*
Lubbock, TX, USA
victoria.obrien@ttu.edu

Vittal Rao
*Electrical Engineering Department*
*Texas Tech University*
Lubbock, TX, USA
vittal.rao@ttu.edu

Rodrigo D. Trevizan
*Energy Storage Technology & Systems*
*Sandia National Laboratories*
Albuquerque, NM, USA
rdtrevi@sandia.gov

*Abstract*— **The state of charge (SoC) estimated by Battery Management Systems (BMSs) could be vulnerable to False Data Injection Attacks (FDIAs), which aim to disturb state estimation. Inaccurate SoC estimation, due to attacks or suboptimal estimators, could lead to thermal runaway, accelerated degradation of batteries, and other undesirable events. In this paper, an ambient temperature-dependent model is adopted to represent the physics of a stack of three series-connected battery cells, and an Unscented Kalman Filter (UKF) is utilized to estimate the SoC for each cell. A Cumulative Sum (CUSUM) algorithm is used to detect FDIAs targeting the voltage sensors in the battery stack. The UKF was more accurate in state and measurement estimation than the Extended Kalman Filter (EKF) for Maximum Absolute Error (MAE) and Root Mean Squared Error (RMSE). The CUSUM algorithm described in this paper was able to detect attacks as low as $\pm 1\ mV$ when one or more voltage sensor was attacked under various ambient temperatures and attack injection times.**

***Keywords— ambient temperature, anomaly detection, cumulative sum, false data injection attacks, smart grid.***

## I. Introduction

Cyberattacks on power grids and other cyber-physical systems (CPS) around the world have caused blackouts and other undesirable consequences. Notable examples of cyberattacks were the 2015 cyberattack on Ukraine's power grid and the 2010 discovery of the Stuxnet worm that was found in Iranian Industrial plants [1]. The discovery of these attacks and their consequences demonstrated the importance of implementing defenses to cyber threats targeting the smart grid.

Energy storage systems (ESSs) are connected to the smart grid to help keep up with energy demands and to integrate renewable generation sources. Battery ESS (BESS) have recently become popular due to their increased efficiency and reduced cost [2]. Lithium-ion (Li-ion) batteries are the most used BESS technology [3] because of their relatively low-cost, high-energy density, high power density, and long lifespan [3], [4].

Battery cells require a battery management system (BMS) to monitor sensor readings (typically current, voltage, and temperature), to balance cells, to ensure that batteries operate within their safety limits, and to estimate battery states like the state of charge (SoC) [5]. SoC is the ratio of available charge in a battery relative to the total capacity of the battery and it cannot be measured directly. Accurate SoC estimation is crucial for safe operation of the battery, including its charge and discharge cycles [6]. Errors in SoC estimation in grid-scale BESS could result in thermal runaway events (overheating, fires, or explosions), the degradation and reduced lifetime of batteries, increased costs to replace damaged equipment, or decreased reliability of systems (including blackouts) [5] - [8].

Variations of the Kalman Filter (KF), like the Extended KF (EKF) and the Unscented KF (UKF), can be used as estimators in nonlinear systems like battery cells. The EKF works well for systems that can be represented by a linear approximation but performs sub-optimally in systems with extreme nonlinearities [9]. The UKF works well under any nonlinearity and uses a collection of Sigma Points (SPs) to represent the probability distribution of the nonlinear function. Theoretically, the UKF can provide more accurate state estimation than the EKF [5]. EKFs have been used to estimate battery states in electric vehicle batteries [4], and in temperature-dependent Li-ion battery applications [10]. UKFs have been studied for nonlinear estimation in [9] and have also been used in power battery applications [6] and in personal navigation [11]. In this paper a UKF is implemented to estimate the states of a stack of three batteries whose internal parameters are dependent on the ambient temperature. Some simplified equivalent circuit models (ECMs) used to represent battery dynamics do not include the effects of cell or ambient temperature [4]. Papers such as [12] and [10] assert that battery parameters are ambient temperature-dependent (ATD).

False Data Injection Attacks (FDIAs) are cyberattacks that alter measurements in a CPS before they are used in state estimation, to cause inaccurate estimation [13]. FDIAs are typically designed by attackers who have knowledge of the system configuration, parameters, or state matrices [13]. In literature, FDIAs have been detected using statistical methods like the chi-squared test [14] and variations of the CUSUM algorithm [15], [16], or with data driven methods [17]. Previously published work [18] applied the CUSUM to FDIA detection in battery stacks but used an EKF for SoC estimation considering constant temperature battery stack models.

Victoria Obrien is also with the Energy Storage Technology & Systems Dept., Sandia National Laboratories, Albuquerque, NM, USA (email vaobrie@sandia.gov).

This work was supported by the U.S. Department of Energy, Office Electricity, Energy Storage program. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy National Nuclear Security Administration under contract DE-NA-0003525. 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.

SAND.

In this paper, we extend [18] to increase the accuracy of SoC estimation and FDIA detection. The contribution of this paper is to use the CUSUM algorithm to detect FDIA in the voltage sensors of the ATD model proposed in [10] under various ambient temperatures. Additionally, a UKF replaces the EKF used in [10] to estimate more accurately the SoC of each battery cell.

The remainder of this paper is organized as follows. Section II describes the ATD ECM for a stack of series-connected batteries and presents the UKF algorithm and the FDIA model. Section III describes the CUSUM algorithm taken from [18]-[21]. Section IV demonstrates the effectiveness of the CUSUM algorithm by testing the UKF and CUSUM algorithm at a variety of ambient temperatures, the results of which are presented in Section V. Section VI concludes this paper.

## II. SoC Estimation for ATD Battery Stacks

### A. ATD ECM

The ATD ECM for the j^th cell in a series connected stack of N batteries was adopted from [10] (Fig. 1.). Like the study in [18], three series-connected battery cells were studied.

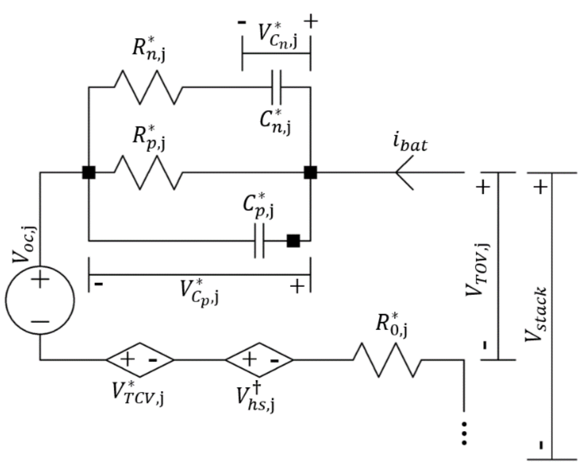

Fig. 1. ATD ECM for the j^th cell in a series-connected stack of N batteries [10]. * indicates the element is ATD and † indicates the element is SoC-dependent.

Continuous general governing equations (1) – (9) for the j^th cell in the battery stack can be derived from Fig. 1 [10].

$$\dot{V}_{\boldsymbol{C_n},j} = \frac{V_{C_n,j}}{R_{n,j}(T)C_{n,j}(T)} + \frac{V_{C_p,j}}{R_{n,j}(T)C_{n,j}(T)} \tag{1}$$

$$\dot{V}_{C_p,j} = -\frac{V_{C_n,j}}{R_{n,j}(T)C_{p,j}(T)} + \frac{i_{bat}}{C_{p,j}(T)} - \frac{V_{C_p,j}\left(R_{n,j}(T)+R_{p,j}(T)\right)}{C_{p,j}(T)R_{n,j}(T)R_{p,j}(T)} \tag{2}$$

$$V_{\mathrm{hs,j}} = p_{10}\varsigma_j + p_{00} \tag{3}$$

$$V_{oc,j} = p_{30}\varsigma_j^3 + p_{21}\varsigma_j^2(T) + p_{20}\varsigma_j^2 + \ p_{11}\varsigma_j(T) + p_{10}\varsigma_j + p_{01}(T) + p_{00} \tag{4}$$

$$V_{TCV,j} = p_{02}(T)^2 + p_{01}(T) + p_{00} \tag{5}$$

$$V_{TOV,j} = V_{oc,j} + V_{C_p,j} + R_{0,j}(T)i_{bat} + V_{hs,j} + V_{TCV,j} \tag{6}$$

$$V_{stack} = V_{TOV,1} + \cdots + V_{TOV,N} \tag{7}$$

$$i_{bat} = i_c + i_d \tag{8}$$

$$\dot{\varsigma}_j = \frac{1}{C_{cap,j}}\left(\eta_{c,j}i_c + i_d\right) - \eta_{s,j}\varsigma_j \tag{9}$$

where T is the ambient temperature, $i_{bat}$ is the current through the battery stack, $V_{stack}$ is the battery stack's voltage, $i_c \geq 0$ and $i_d \leq 0$ are the charge and discharge current, respectively. The remainder of the parameters varied from cell to cell and the subscript $_{,j}$ indicates a parameter is for the j^th battery cell. Where $R_{0,j}$ is the battery ohmic resistance, $\varsigma_j$ is the SoC, $V_{oc,j}$ is the open circuit voltage, $V_{TOV,j}$ is the voltage drop across the cell, $V_{TCV,j}$ is the temperature compensation voltage, $V_{hs,j}$ is the static hysteresis voltage, as described in [10].

Coefficients for each cell are listed in TABLE I, where the coefficients for Cell 1 were taken from [10]. The remaining coefficients for Cell 2 and Cell 3 were determined by adding a small random value to the coefficients from [10] and fitting a curve to the data.

TABLE I. Battery Model Voltage Coefficients [10].

| | $p_{30}$ | $p_{21}$ $(10^{-3})$ | $p_{20}$ | $p_{11}$ $(10^{-3})$ | $p_{10}$ $(10^{-2})$ | $p_{02}$ $(10^{-6})$ | $p_{01}$ $(10^{-3})$ | $p_{00}$ |
|---|---|---|---|---|---|---|---|---|
| $V_{\mathrm{oc,1}}$ | 1.36 | -5 | -1.917 | 7 | 8.79 | - | −2 | 3.149 |
| $V_{\mathrm{hs,1}}$ | - | - | - | - | −7.55 | - | - | 0.0755 |
| $V_{\mathrm{TCV,1}}$ | - | - | - | - | - | −9.2 | 1.2 | -0.097 |
| $V_{\mathrm{oc,2}}$ | 1.37 | -5 | -1.921 | 7.1 | 8.867 | - | -2 | 3.149 |
| $V_{\mathrm{hs,2}}$ | - | - | - | - | -7.27 | - | - | 0.07353 |
| $V_{\mathrm{TCV,2}}$ | - | - | - | - | - | -9.98 | 1.242 | -0.0964 |
| $V_{\mathrm{oc,3}}$ | 1.37 | -5 | -1.923 | 7.06 | 9.02 | - | -2 | 3.149 |
| $V_{\mathrm{hs,3}}$ | - | - | - | - | -7.869 | - | - | 0.077 |
| $V_{\mathrm{TCV,3}}$ | - | - | - | - | - | -10.75 | 1.188 | -0.0953 |

General polynomial equations to find the ATD internal battery parameters (10) were adopted from [10]. The list of ATD internal battery coefficients is presented in TABLE II.

$$P_{n,j} \ = p_{03}T^3 + p_{02}T^2 + p_{01}T + p_{00} \tag{10}$$

where $p_{kl}$ is a coefficient in the SoC and T dependent equations, $k$ corresponds to the order of the SoC and $l$ corresponds to the order of T. The polynomial $P_{n,j}$ could represent $R_{n,j}, R_{p,j}, C_{p,j}, C_{n,j}$, or $C_{cap,j}$, which are resistor and capacitor values for the series and parallel RC pairs (Fig. 1.) and $C_{cap,j}$ is the capacity of the battery.

### B. Unscented Kalman Filter

The UKF is used to estimate system states for an ATD battery stack model, due to the nonlinearity in the output equation of the model. The state transition function (11) and output function (12) are influenced by process and measurement noise, respectively.

$$x_{k+1} = f(x_k, u_k, w_k) \tag{11}$$

$$y_k = g(x_k, u_k, e_k) \tag{12}$$

where $x_k$ is a vector of state variables: the SoC $(\varsigma_j) \in [0,1]$, and the voltage drops across the parallel $(V_{p,j})$ and series $(V_{n,j})$ RC pairs , $u_k$ is a vector of system inputs: $i_c$ and $i_d$, $y_k$ is the system outputs: the cell voltages ($V_{TOV,j}$) and $V_{stack}$. The noise ($w_k \sim \mathcal{N}(0,Q)$ and $e_k \sim \mathcal{N}(0,R)$) are assumed to be additive Gaussian noise.

The UKF uses a collection of SPs to represent the probability density of the nonlinear measurement equation. The state equation is linear in this case, so states are predicted using the same technique as the traditional KF. The UKF follows four main steps: initialization (performed once), prediction of states, calculation of SP and weights, and correction/update, the latter three are performed recursively to estimate states over time [11].

Step 1: Initialization (13) – (14).

$$\hat{x}_{0|0} = \mathbb{E}[x_0] \tag{13}$$

$$P_{0|0} = P_0 \tag{14}$$

where $P_0$ is the initial covariance and $x_0$ is the initial state.

Step 2: Prediction of States (15) – (16).

This step is done with the same method as the traditional KF since the nonlinearity only affects the output equation.

$$\hat{x}_{k+1|k} = A\hat{x}_{k|k} + Bu_k \tag{15}$$

$$P_{k+1|k} = AP_{k|k}A^T + Q_k \tag{16}$$

Step 3: Generate the SPs and associated weights (17) – (23).

There are (2n+1) SPs used to represent the probability density of the nonlinear function, n is the number of states. The SPs (17) – (19) are centered around the mean of the function.

$$\mathcal{X}_{0_{k+1|k}} = \hat{x}_{k+1|k} \tag{17}$$

$$\mathcal{X}_{i_{k+1|k}} = \hat{x}_{k+1|k} + \left(\sqrt{(n+\lambda)P_{k+1|k}}\right)_i \tag{18}$$

$$\mathcal{X}_{i+n_{k+1|k}} = \hat{x}_{k+1|k} - \left(\sqrt{(n+\lambda)P_{k+1|k}}\right)_i \tag{19}$$

where $\hat{x}$ is the estimated state vector, $P$ is the covariance matrix, $\mathcal{X}$ is the SP matrix with dimensions $n \times (2n+1)$, $\lambda$ is a scaling parameter, and $i = 1, \dots, 2n$. The portion under the radical is a positive-definite matrix that is calculated using Cholesky decomposition for the lower triangle, as done in [11]. The weights for each sigma point are also calculated (20) – (23).

$$W^0_{m_{k+1|k}} = \frac{\lambda}{n+\lambda} \tag{20}$$

$$W_c^0{}_{k+1|k} = W^0_{m_{k+1|k}} + (1 - a^2 + b) \tag{21}$$

$$W^i_{m_{k+1|k}} = W_c^i{}_{k+1|k} = \frac{1}{2(n+\lambda)} \tag{22}$$

$$\lambda = a^2(n+\kappa) - n \tag{23}$$

where $W_m$ is used to predict the measurement vector in the correction step and $\sum W_m = 1$, $W_c$ is used to calculate the covariance matrix in the correction step, $b$ is a parameter related to the distribution of the probability density function of the state vector ($b = 2$ for Gaussians), $\lambda$ is a parameter that determines the spread of the SPs around the mean, the parameter $k \in [0, \infty)$ is usually set to zero, and the parameter $a \in (0,1]$ [11].

Step 4: Correction (24) – (30).

The correction step of the algorithm is used to update the estimated states, measurements, and covariance matrices before they are used in the next iteration of the recursive process.

$$\hat{y}_{k+1|k} = \sum_{i=0}^{2n} W_m^i \cdot h(\mathcal{X}_{i_{k+1|k}}) \tag{24}$$

$$\begin{aligned} P_{xy_{k+1|k}} = \sum_{i=0}^{2n} W_c^i \left(\mathcal{X}_{i_{k+1|k}} - \hat{x}_{k+1|k}\right) \cdot \\ \left\{h\left(\mathcal{X}_{i_{k+1|k}}\right) - \hat{y}_{k+1|k}\right\}^T \end{aligned} \tag{25}$$

$$\begin{aligned} P_{yy_{k+1|k}} = \sum_{i=0}^{2n} W_c^i \left(h\left(\mathcal{X}_{i_{k+1|k}}\right) - \hat{y}_{k+1|k}\right) \cdot \\ \left\{h\left(\mathcal{X}_{i_{k+1|k}}\right) - \hat{y}_{k+1|k}\right\}^T \end{aligned} \tag{26}$$

$$S_{k+1} = P_{yy_{k+1|k}} + R_{k+1} \tag{27}$$

$$K_{k+1} = P_{xy_{k+1|k}} \cdot S_{k+1}^{-1} \tag{28}$$

$$\hat{x}_{k+1|k+1} = \hat{x}_{k+1|k} + K_{k+1} \cdot (y_{k+1} - \hat{y}_{k+1|k}) \tag{29}$$

$$P_{k+1|k+1} = P_{k+1|k} - K_{k+1}S_{k+1}K_{k+1}^T \tag{30}$$

where $\hat{y}$ is the estimated measurement vector, $P_{xy}$ and $P_{yy}$ are covariance matrices, $S$ is the innovation covariance matrix, and $K$ is the Kalman gain matrix. The UKF parameters, taken from [11], are shown in TABLE II.

TABLE II. UNSCENTED KALMAN FILTER PARAMETERS [11].

| **Parameter** | ***n*** | ***a*** | ***b*** | ***κ*** | ***λ*** |
|---|---|---|---|---|---|
| **Value** | 9 | 0.1 | 2 | 0 | -8.91 |

### C. *False Data Injection Attack Model*

The FDIA attack model from [18] was repeated to introduce bias attacks to the measurements of ATD battery stacks.

$$y_a = y + \Delta y_a \tag{31}$$

where $\Delta y_a$ is an attack vector, y is the measurement vector, and $y_a$ is the manipulated measurement vector [18].

## III. DETECTION OF FDIA IN STACKS USING CUSUM

### A. *CUSUM Algorithm*

Variations of the CUSUM algorithm have been utilized for change detection [19], and it has been applied to detect FDIA in batteries without ambient temperature being taken into consideration [18][20]. The methodology and equations for the CUSUM algorithm used in this paper can be found in [18]-[20], and the general process of the CUSUM algorithm can be summarized in the form of a flowchart (Fig. 2.). Methods to calculate the CUSUM parameters ($k, h, d, \alpha, \beta, \delta, n_{samp}$, and $n_{samp}$) are described in [20] and [21].

The general process of the CUSUM algorithm is to calculate an upper (UCL) and lower (LCL) control limit, and then use a recursive high (SH) and low (SL) sum to determine if the system is in or out of control. An attack is present in the system if either the SH or SL exceeds the UCL or LCL, respectively [19]. It is not necessary for both sums to diverge to indicate an attack is present. As done in [18] and [20], the a priori measurement residual was used as the input data to the CUSUM algorithm.

$$z[k|k-1] = y[k] - \hat{y}[k|k-1] \quad (32)$$

where z is the a priori measurement residual, y is the actual measurement (which may or may not be attacked), and $\hat{y}$ is the estimated measurement which is generated by the UKF.

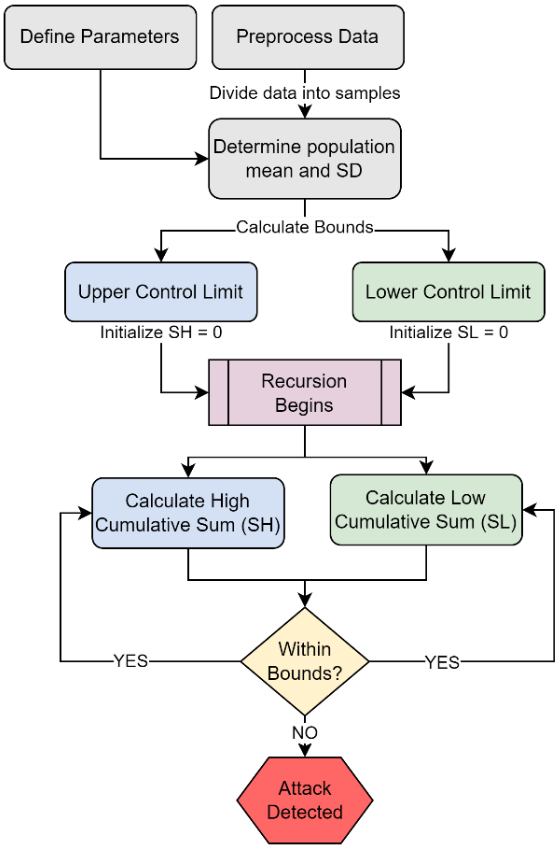

Fig. 2. CUSUM algorithm flowchart for attack detection

## IV. Case Study

In this section the estimation accuracy of the UKF is compared to the EKF for a stack of three ATD cells. For each test, the UKF and EKF were given the same ambient temperatures and internal battery parameters, the only difference between the tests being the estimator's equations. Two metrics were used to assess the accuracy of the estimators: root mean squared error (RMSE) and maximum absolute error (MAE) of the state variable ($\hat{x}_{k|k}$) and system output ($\hat{y}_k$) estimates.

The detection capability of CUSUM algorithm at various fixed-ambient temperatures was evaluated by using the a priori residuals at random ambient temperatures. FDIAs targeted individual cell voltage sensors and the stack voltage sensor. Due to the difficulty and expense associated with launching FDIAs, we assumed an attacker would target the minimum number of sensors that result in inaccurate state estimation (in most cases one sensor was sufficient). Therefore, we assume single-sensor attacks are more likely, but for completeness, attacks launched on multiple sensors were also tested. FDIAs were injected at random attack times (ranging from 2000 s to 7000 s) and random fixed-ambient temperatures (ranging from -30°C to 50°C) were used to generate ATD battery parameters.

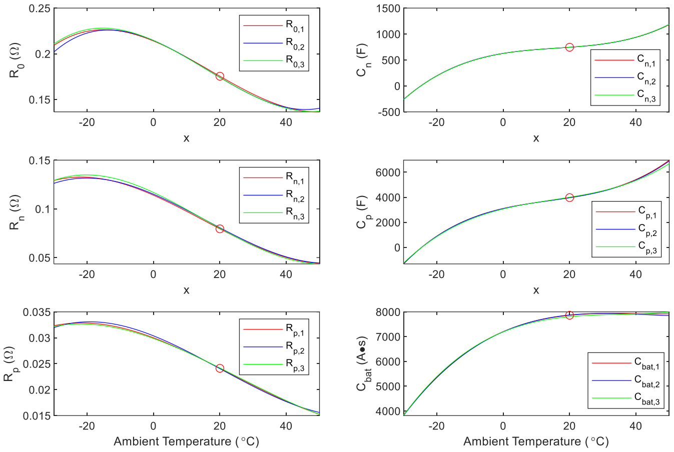

Fig. 3. Battery parameter vatiation with ambient temperature [10].

The batteries studied are $LiFePO_4$ chemistry. The parameters for Cell 1 were taken from [10]. The battery parameters for Cell 2 and Cell 3 were generated by adding noise to the parameters from Cell 1 based on the variation between cells' parameters in [4] and fitting a curve to the noisy data (Fig. 3.). The coefficients for each cell can be seen in TABLE IV [10].

TABLE III. ATD Battery Parameter Coefficients [10].

| | $p_{03}$ | $p_{02}$ | $p_{01}$ | $p_{00}$ |
|---|---|---|---|---|
| $\mathbf{R_{0,1}}$ | $6.8 \cdot 10^{-7}$ | $-3.5 \cdot 10^{-5}$ | $-1.5 \cdot 10^{-3}$ | 0.214 |
| $\mathbf{R_{p,1}}$ | $5.4 \cdot 10^{-8}$ | $-3.8 \cdot 10^{-6}$ | $-2.4 \cdot 10^{-4}$ | 0.03 |
| $\mathbf{C_{p,1}}$ | 0.04 | – 1.677 | 61.1 | 3100 |
| $\mathbf{R_{n,1}}$ | $4.4 \cdot 10^{-7}$ | $-2 \cdot 10^{-5}$ | $-1.5 \cdot 10^{-3}$ | 0.114 |
| $\mathbf{C_{n,1}}$ | $8 \cdot 10^{-3}$ | – 0.39 | 10.6 | 625 |
| $\mathbf{C_{cap,1}}$ | 0.012 | – 1.4652 | 57.6 | 7200 |
| $\mathbf{R_{0,2}}$ | $8.373 \cdot 10^{-7}$ | $-4.057 \cdot 10^{-5}$ | $1.548 \cdot 10^{-3}$ | 0.2146 |
| $\mathbf{R_{p,2}}$ | $7.461 \cdot 10^{-8}$ | $-4.53 \cdot 10^{-6}$ | $-2.56 \cdot 10^{-4}$ | 0.03 |
| $\mathbf{C_{p,2}}$ | 0.0397 | – 1.682 | 60.9 | 3099 |
| $\mathbf{R_{n,2}}$ | $4.654 \cdot 10^{-7}$ | $-2.232 \cdot 10^{-5}$ | $-1.459 \cdot 10^{-3}$ | 0.1151 |
| $\mathbf{C_{n,2}}$ | $8.17 \cdot 10^{-3}$ | – 0.39 | 10.5 | 628 |
| $\mathbf{C_{cap,2}}$ | 0.0112 | – 1.47 | 58.68 | 7198 |
| $\mathbf{R_{0,3}}$ | $7.356 \cdot 10^{-7}$ | $-3.565 \cdot 10^{-5}$ | $-1.604 \cdot 10^{-3}$ | 0.2146 |
| $\mathbf{R_{p,3}}$ | $4.779 \cdot 10^{-8}$ | $-3.639 \cdot 10^{-6}$ | $2.301 \cdot 10^{-4}$ | 0.02986 |
| $\mathbf{C_{p,3}}$ | 0.03483 | – 1.59 | 64.83 | 3066 |
| $\mathbf{R_{n,3}}$ | $5.116 \cdot 10^{-7}$ | $-2.346 \cdot 10^{-5}$ | $-1.574 \cdot 10^{-3}$ | 0.1169 |
| $\mathbf{C_{n,3}}$ | $8.04 \cdot 10^{-3}$ | – 0.39 | 10.6 | 626 |
| $\mathbf{C_{cap,3}}$ | 0.01435 | – 1.489 | 54.69 | 7192 |

## V. Results

The UKF outperformed the EKF in terms of RMSE and MAE at all ambient temperatures studied. The error study was conducted for each state variable and each measurement, by using the residual value between the actual and estimated state or measurement. The UKF was found to estimate each individual state and measurement more accurately than the EKF. TABLE V presents the results of the error studies for each estimator, with subscripts E and U referring to the results of the EKF and UKF, respectively. To make the table readable, the value in each column is the sum of the individual errors for the estimated states and measurements. So, the $RMSE_E$ at 10°C is the sum of the RMSE of each state and measurement for the EKF at 10°C.

The CUSUM algorithm was able to detect FDIA magnitudes as low as ±1 mV on voltage sensors, for random injection times and random ambient temperatures. Fig. 4 is an example of the CUSUM chart, which clearly diverges in the presence of an FDIA. Ambient temperatures tested, between -10°C and 50°C (and associated battery parameters), did not appear to have an impact on the accuracy of the CUSUM algorithm. Although the likelihood of a multi-sensor attack is lower than a single-sensor attack, the CUSUM algorithm functioned when multiple sensors were attacked but did not accurately indicate the sensor(s) attacked. The CUSUM did not trigger a false alarm at any of the ambient temperatures tested when there was no injected attack.

TABLE IV. EKF AND UKF ERROR RESULTS.

| T (℃) | $RMSE_E$ | $RMSE_U$ | $MAE_E$ | $MAE_U$ |
|---|---|---|---|---|
| -10 | 0.0936 | 0.0485 | 0.0675 | 0.0295 |
| 0 | 0.0964 | 0.0545 | 0.0713 | 0.0360 |
| 10 | 0.0931 | 0.0545 | 0.0686 | 0.0364 |
| 20 | 0.0892 | 0.0539 | 0.0651 | 0.0358 |
| 30 | 0.0859 | 0.0536 | 0.0620 | 0.0354 |
| 40 | 0.0836 | 0.0540 | 0.0609 | 0.0355 |
| 50 | 0.0835 | 0.0562 | 0.0623 | 0.0377 |

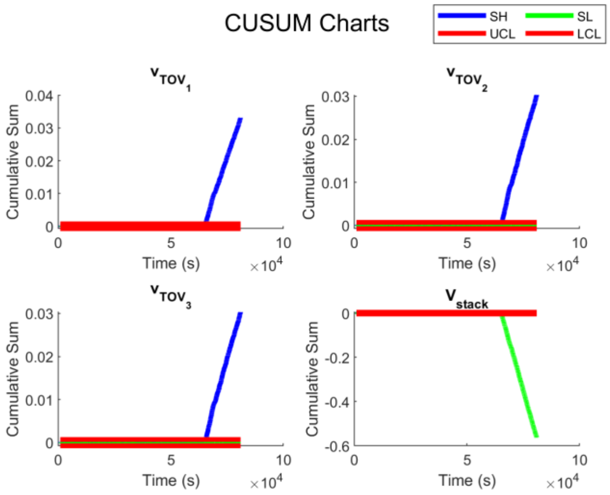

Fig. 4. CUSUM charts for a 1 mV attack in $v_{TOV_1}$ sensor at 6529 s and 39°C.

## VI. SUMMARY AND CONCLUSIONS

This paper extends the work in [18] to include an ATD battery model [10] and improves state and measurement estimation by using the UKF. The UKF estimator was found to be more accurate than the EKF when evaluated using RMSE and MAE. The CUSUM algorithm was able to detect FDIAs with magnitudes of at least $\pm 1\ mV$, in all voltage sensors (including multiple voltage sensors at a time) under varying ambient temperatures and random attack injection times.

## ACKNOWLEDGMENT

The authors would like to thank Dr. Imre Gyuk, Director of the Energy Storage Program, for his continued support. We also acknowledge the support of the U.S Department of Education's program on Graduate Assistance in Areas of National Need (GAANN) grant to Texas Tech University. The authors would like to thank Dr. Hyungjin Choi for his technical advice.

## REFERENCES

[1] D. Kushner, "The real story of stuxnet," in *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013, doi: 10.1109/MSPEC.2013.6471059.

[2] M. T. Lawder et al., "Battery Energy Storage System (BESS) and Battery Management System (BMS) for Grid-Scale Applications," in *Proc. of the IEEE*, vol. 102, no. 6, pp. 1014-1030, Jun. 2014.

[3] S. Kumbhar, T. Faika, D. Makwana, T. Kim and Y. Lee, "Cybersecurity for Battery Management Systems in Cyber-Physical Environments," *2018 IEEE Transportation Electrification Conf. and Expo (ITEC)*, 2018, pp. 934-938, doi: 10.1109/ITEC.2018.8450159.

[4] Z. Liu and H. He, "Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended kalman filter," *Applied Energy*, vol. 185, pp. 2033–2044, 2017.

[5] 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," *IEEE Trans. Power Electronics*, vol. 34, no. 10, pp. 9709–9718, 2019.

[6] 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.

[7] 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.

[8] N. Kharlamova, S. Hashemi and C. Træholt, "Data-driven approaches for cyber defense of battery energy storage systems," *Energy and AI*, 2021, pp. 188-192, doi: 10.1016/j.egyai.2021.100095.

[9] E. A. Wan and R. Van Der Merwe, "The unscented Kalman filter for nonlinear estimation," in *Proc. of the IEEE 2000 Adaptive Systems for Signal Processing, Comm., and Control Symp. (Cat. No.00EX373)*, 2000, pp. 153-158, doi: 10.1109/ASSPCC.2000.882463.

[10] H. Pang, L. Guo, L. Wu, and X. Jin, "An enhanced temperature-dependent model and state-of-charge estimation for a Li-Ion battery using extended Kalman filter," *Int. J. of Energy Research*, pp. 7254-7266, March 2020.

[11] P. Pasek and P. Kaniewski, "Unscented Kalman filter application in personal navigation", in *Proc. Radioelectronic Syst. Conf.*, Jachranka, Poland, 2019, 114421C.

[12] 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. of Hardware and Syst. Security*, vol. 1, no. 2, pp. 188–199, Jun 2017.

[13] 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 Comput. and Comm. Security*, New York, NY, 2009, pp. 21–32.

[14] Y. Mo and B. Sinopoli, "On the performance degradation of cyberphysical systems under stealthy integrity attacks," *IEEE Trans. Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[15] 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," in *Proc. 2020 IEEE 4th Conf. Energy Internet and Energy Syst. Integration (EI2)*, 2020, pp. 3400-3403.

[16] M. Severo and J. Gama, "Change Detection with Kalman Filter and CUSUM", in *Proc. Int. Conf. Discovery Science*, Barcelona, Spain, 2006, pp. 243-254.

[17] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R.G. Dutta, Y. Jin, and C. Konstantinou, "A 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.

[18] V. Obrien, 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.

[19] W. C. Navidi, *Statistics for Engineers and Scientists*, New York, NY: McGraw-Hill Education, 2015

[20] V. Obrien, R. D. Trevizan and V. Rao, "Detecting False Data Injection Attacks to Battery State Estimation Using Cumulative Sum Algorithm," in *Proc. 53rd North Amer. Power Symp.*, Nov. 2021 pp 1-6.

[21] *e-Handbook of Statistical Methods*, Nat. Institute of Standards and Technology and SEMATECH, Jun. 2012.