Detection of False Data Injection Attacks Targeting State of Charge Estimation of Battery Energy Storage Systems

Victoria Obrien and Rodrigo Trevizan*

Dr. Vittal Rao

Texas Tech University – Electrical Engineering Department

*Sandia National Laboratories, Albuquerque, NM

PRESENTED AT

Introduction

- Modernizing the Electrical Grid and connecting hardware and software to the internet makes the Smart Grid vulnerable to a host of security threats
- State of Charge (SoC) must be estimated by the Battery Management System (BMS) as it cannot directly be measured
- Accurate SoC estimation is critical for the safe and effective operation of the Smart Grid
- SoC estimation is susceptible to False Data Injection Attacks (FDIA) which is when attackers use knowledge of the system's measurements and parameters to evade detection by bad data detectors
- Stealth attacks like FDIA require a separate detection mechanism, Chi Squared detectors have been used in papers [6]
- The proposed Cumulative Sum (CUSUM) algorithm is being studied to determine if it can detect FDIA more accurately than other methods such as the Chi Squared detector

Purpose

- To use Simulink to simulate Battery Models' SoC estimation and to simulate FDIA to the v_{bat} measurement
- To create a CUSUM Chart to detect a shift in the sample mean of the a priori residual, indicating an attack is present
- To determine if CUSUM is more accurate than other methods such as Chi Squared

Method

Cumulative Sum (CUSUM) Algorithm

- The CUSUM algorithm described in [1] was applied to the a priori measurement residual eq (1) to determine if a False Data Injection Attack was present:

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

- The a priori residual data was divided into 2880 samples, of size 25
- The population mean is expected to be 0, and the population standard deviation was estimated using the first 30 samples eq (2):

$$\sigma_{\bar{X}} = \frac{A_2 \bar{R}}{3} \quad (2)$$

- The high and low cumulative sums were calculated using eq (3) – (4):

$$SH_i = \max(0, \bar{X}_i - \mu - k\sigma_{\bar{X}} + SH_{i-1}) \quad (3)$$

$$SL_i = \min(0, \bar{X}_i - \mu - k\sigma_{\bar{X}} + SL_{i-1}) \quad (4)$$

- If the upper or lower cumulative sum goes out of bounds, there is an attack present

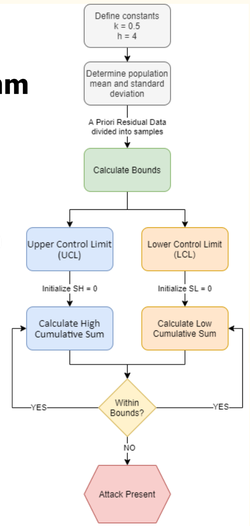

Figure 1: CUSUM Flowchart

Application

Model of Battery Energy Storage System

- A simplified Battery Energy Storage System (BESS) was modeled using a charge reservoir model and second order equivalent circuit with the governing equations eq (5) – (6), similar to the method used in [3]:

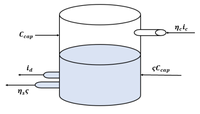

Figure 2: Charge Reservoir Model

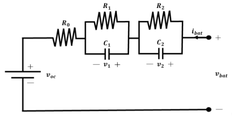

Figure 3: 2nd Order Equivalent Circuit

$$\begin{bmatrix} \dot{\zeta} \\ \dot{v}_1 \\ \dot{v}_2 \end{bmatrix} = \begin{bmatrix} -\eta_c & 0 & 0 \\ 0 & -\frac{1}{R_1 C_1} & 0 \\ 0 & 0 & -\frac{1}{R_2 C_2} \end{bmatrix} \begin{bmatrix} \zeta \\ v_1 \\ v_2 \end{bmatrix} + \begin{bmatrix} \frac{\eta_c}{C_{cap}} & \frac{1}{C_{cap}} \\ \frac{1}{C_1} & \frac{1}{C_1} \\ \frac{1}{C_2} & \frac{1}{C_2} \end{bmatrix} \begin{bmatrix} i_c \\ i_d \end{bmatrix} + w \quad (5)$$

$$\begin{bmatrix} v_{bat} \\ i_{bat} \end{bmatrix} = \begin{bmatrix} spline(c) & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \zeta \\ v_1 \\ v_2 \end{bmatrix} + \begin{bmatrix} R_0 & R_0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i_c \\ i_d \end{bmatrix} + v \quad (6)$$

Where w ~ $\mathcal{N}$ (0, Q) and v ~ $\mathcal{N}$ (0, R) representing white noise introduced in the estimation and measurements

Application

State of Charge Estimation

- The battery model was simulated in Simulink to estimate the State of Charge
- A third order nonlinear equation was used to find the coefficient for SoC in eq (6), as done in [5]
- Due to the Nonlinear nature of the SoC, an Extended Kalman Filter (EKF) was needed to estimate the State of Charge and calculate the a priori residual

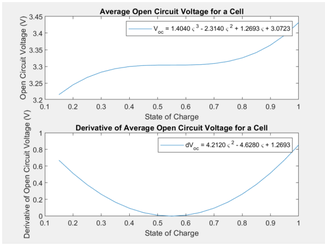

Figure 4: Average Open Circuit Voltage for a Cell and its derivative in order to determine SoC coefficient, as done in [5]

False Data Injection Attack

- To verify that the CUSUM is a viable FDIA detector, the CUSUM algorithm was applied to the a priori residual calculated in the simulation
- An attack was simulated by modifying the system's measurement: 20 mV was added to the v_{bat} measurement at timestep = 45000
- In this configuration, a 20 mV attack was the smallest detectable attack and was used to demonstrate the effectiveness of the CUSUM detector

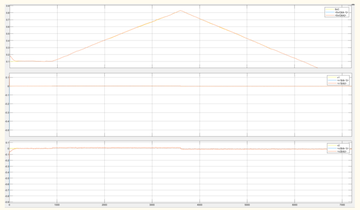

Figure 5: State Variable Estimates with No Attack Present

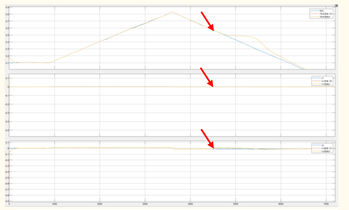

Figure 6: State Variable Estimates with a 20 mV attack Present

- When there is no attack the estimates of the SoC (top), V1 (middle), and V2 (bottom) follow the actual values
- When the attack occurs (indicated by red arrow) the estimates of SoC (top), V1 (middle), and V2 (bottom) differ from the actual values

Results

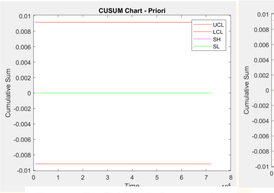

Figure 7: CUSUM Chart with No Attack Present

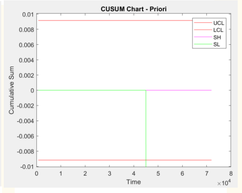

Figure 8: CUSUM Chart with 20 mV Attack Present

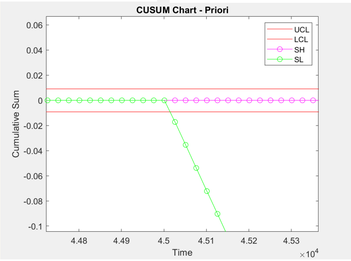

Figure 9: Magnified CUSUM Chart with 20 mV Attack Present, Samples of size 25

Conclusions

- The CUSUM algorithm discussed successfully detected FDIA injected in the v_{bat} measurement of the simulated system, by using the a priori residual
- In the future the CUSUM algorithm will be fine-tuned to determine which parameters optimize detection

References

[1] Navidi, W. (2015). In *Statistics for engineers and scientists* (pp. 793–795). essay, McGraw Hill.

[2] G. L. Plett, "Sigma-point Kalman filtering for battery management systems of LiPB-based HEV battery packs: Part 1: Introduction and state estimation,"in J. Power Sources, v. 161, no. 2, pp. 1356-1368, 2006

[3] D. Rosewater, S. Ferreira, D. Schoenwald, J. Hawkins and S. Santoso, "Battery Energy Storage State-ofCharge Forecasting: Models, Optimization, and Accuracy," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2453-2462, May 2019, doi: 10.1109/TSG.2018.2798165.

[4] Severo M., Gama J. (2006) Change Detection with Kalman Filter and CUSUM. In: Todorovski L., Lavrač N., Jantke K.P. (eds) Discovery Science. DS 2006. Lecture Notes in Computer Science, vol 4265. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11893318_25

[5] Liu, Z., & He, H. (2015). Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended Kalman filter. *Elsevier*, 2033-2044. www.elsevier.com/locate/apenergy

[6] Mo, Y., & Sinopoli, B. (2016). On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks. IEEE Transactions on Automatic Control, 61(9), 2618-2624. https://doi.org/10.1109/TAC.2015.2498708

Acknowledgement

This work was partially funded by the US DOE Energy Storage Program managed by Dr. Imre Gyuk of the DOE Office of Electricity Delivery and Energy Reliability.

We also acknowledge the support of the U.S Department of Education's program on Graduate Assistance in Areas of National Need (GAANN).