Detection of False Data Injection Attacks in Battery Stacks Using Physics-Based Modeling and Cumulative Sum Algorithm

Victoria Obrien*, Vittal Rao**, and Rodrigo Trevizan***

Abstract

As the power grid is modernized by adding electrical components that may be connected to the internet, the grid and its associated energy storage systems have become more vulnerable to cyberattacks. Battery Energy Storage Systems (BESSs) employ a Battery Management System (BMS) that is responsible for the safe and efficient operation of the system, including estimating variables to ensure the system remains within its operating limits. False Data Injection Attacks (FDIAs), a type of cyber attack, could be used to manipulate sensor readings, which could cause the BMS to inaccurately estimate variables critical to the system's operation, in this case the State of Charge (SoC). The impact of FDIAs could be degradation of the BESS or poor system performance. This poster presents a method for accurate SoC estimation for stacks of batteries and detection of FDIA injected in voltage sensors using physics-based models, an Extended Kalman Filter (EKF), and a Cumulative Sum (CUSUM) algorithm. Case studies were performed to verify the effectiveness of the proposed methods in various practical problems, including identifying the minimum detectable attacks and detecting an attack when a single sensor or multiple sensors are compromised by the attack. The CUSUM algorithm was found to detect small magnitude attacks with no false alarms. Detecting and responding to FDIAs is critical to the safety and reliability of the electrical grid, and the proposed method was able to detect attacks that evaded other commonly used detection mechanisms.

Introduction

- The electrical grid is being updated to help integrate renewable resources, and to improve reliability, availability, cost, and efficiency
- These updates require the addition of new systems to be connected to the grid:
  - Energy Storage Systems (ESSs): in this case Battery Energy Storage Systems (BESSs)
  - Electrical Components: sensors (voltage, current, temperature), communication devices, hardware components. These components may or may not be connected to the internet.
- Battery Energy Storage Systems Overview
  - Most commonly, stacks (multiple batteries connected together) of Lithium Ion (Li-ion) batteries are used in grid applications
  - A Battery Management System (BMS) is responsible for making sure the batteries perform within their operating and safety specifications, collecting data about the batteries (current, voltage, and temperature), performing state variable estimation, monitoring the health of the system and ensuring the system is safe
  - State variables cannot be measured and must be estimated by the BMS, inaccurate estimation could make the system unsafe
  - The state variable State of Charge (SoC) was investigated in this study. The SoC is a measure of how much charge is left on a battery relative to the total charge (ex: when your phone battery has 86% remaining, the SoC would be 0.86)
  - The SoC can be estimated using Equivalent Circuit Models (ECM) and Charge Reservoir Models (CRM) that approximate the physics of battery systems
- Cyber Threats Overview
  - With more devices being connected to the internet, the grid and its BESS have become more vulnerable to cyberattacks
  - Common cyberattacks include:
    - Denial of Service (DoS): prevents the system from doing its desired purpose by spamming the system with error messages
    - Replay Attacks: replacing new sensor measurements with old, repeated measurements so the system is performing with out-of-date information
    - False Data Injection Attacks (FDIAs): manipulates sensor readings that are needed for state variable estimation, this causes inaccurate estimation and incorrect orders from management systems
  - False Data Injection Attacks
    - Small-magnitude attacks that evade other commonly used detectors
    - The attacker typically has knowledge of the system design and targets sensors
    - Require additional detection mechanisms to be discovered
    - Could be randomly generated or targeted to a specific system
    - Usually expensive to implement, the attacker would target the minimum number of sensors required to damage the system

Purpose

- Detecting and responding to FDIA is critical to the safe operation of the electrical grid
- This poster presents an approach based on the Cumulative Sum (CUSUM) Algorithm that is capable of detecting FDIA injected into the voltage sensors of battery stacks
- Possible Consequences of FDIA on BESS and the electrical grid:
  - Power outages or failure of critical equipment (BESS, sensors, hardware devices)
  - Thermal runaway events (very hot batteries, fires, and in some cases explosions)
  - Increased costs to utility companies and consumers
  - Systems performing outside of specifications and decreased efficiency
  - Damage to equipment, including degradation of batteries

Method

FDIA Detection using CUSUM Algorithm

- Used to detect a shift in the mean of a stationary random process
- Fig. 1 is a flowchart that describes the processes to detect an FDIA using the CUSUM Algorithm
- Adds data over time and adds/subtracts a correction term to determine if the system goes out of bounds
  - The upper (UCL) and lower bounds (LCL) are symmetric about the horizontal axis:

$$UCL = h\sigma_{\bar{z}}$$
$$LCL = -h\sigma_{\bar{z}}$$

Where h is a correction term and $\sigma_{\bar{z}}$ is the population standard deviation.

  - High Sum (SH) and Low Sum (SL) are used to more accurately determine the presence of FDIA than using a single sum

$$SH_i = max(0, \bar{z}_i - \mu - k\sigma_{\bar{z}} + SH_{i-1})$$
$$SL_i = min(0, \bar{z}_i - \mu + k\sigma_{\bar{z}} + SL_{i-1})$$

Where $\bar{z}_i$ is the residual data, μ is the population mean, k is a correction term, $\sigma_{\bar{z}}$ is the population standard deviation, SH_{i-1} and SL_{i-1} are the previous high sum and low sum, respectively.

  - The data input into the CUSUM algorithm was the a priori residual data (the unadjusted difference between the estimated sensor values and actual sensor values):

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

Where z is the a priori residual, y is the actual measurements (sensor values), $\hat{y}$ is the sensor values estimated from the battery model, and k is the time step.

  - An out-of-bounds system indicates FDIA is present

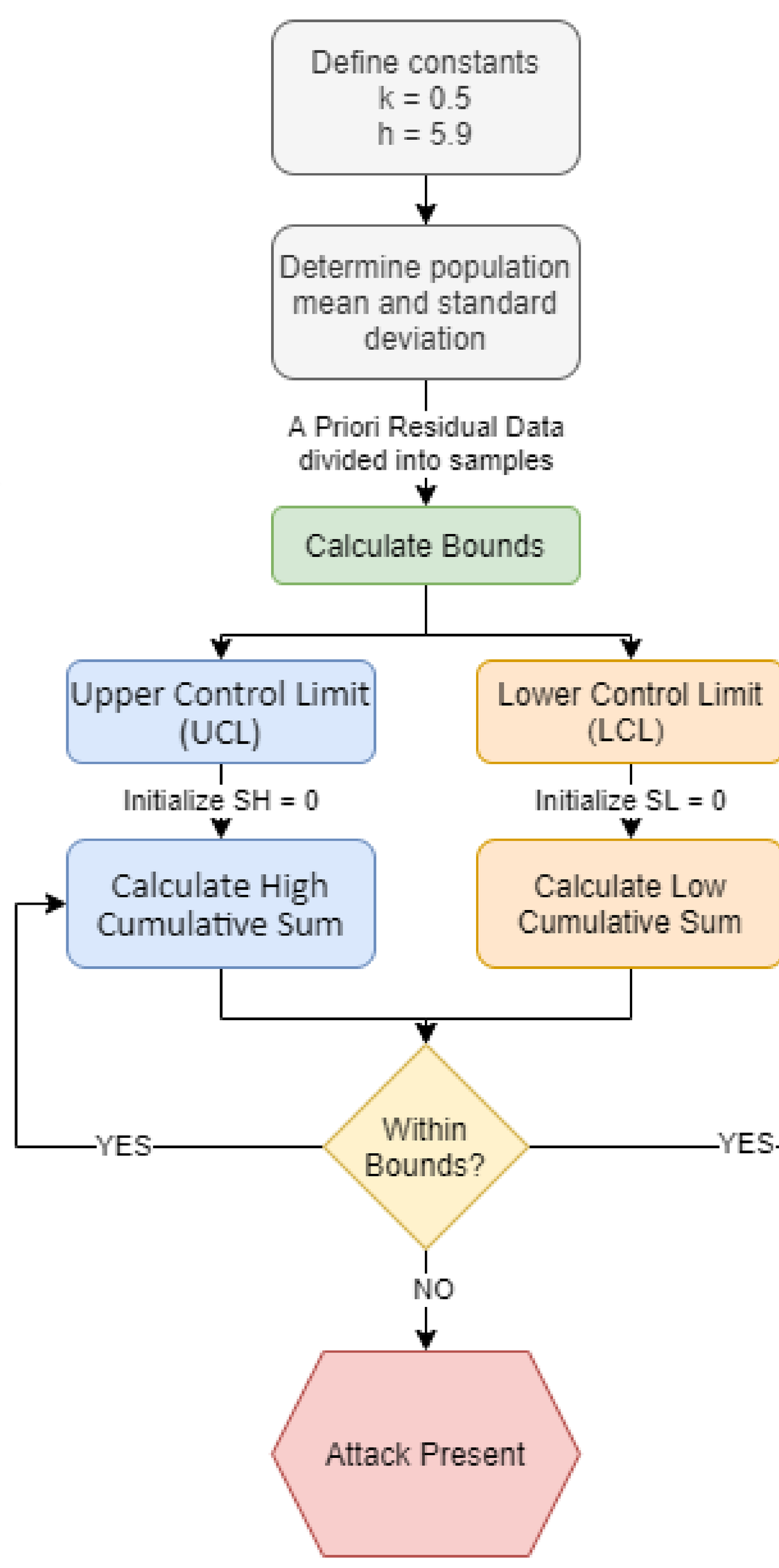

Fig. 1 : CUSUM Algorithm Flowchart

Application

Modeling of Battery Energy Storage System Stacks

- A simple battery stack can be represented using an Equivalent Circuit Model (ECM) (Fig. 2) and a Charge Reservoir Model (CRM) (Fig. 3)
- Equations were derived from Fig. 2 and Fig. 3 to approximate the physics of the batteries
  - The battery model (ECM and CRM) was used to estimate state variables for each battery cell in the stack
    - Voltage drops ($v_{1,1}, v_{2,1}, \ldots, v_{1,N}, v_{2,N}$) across the Resistor-Capacitor circuit (Fig. 2)
    - State of Charge: SoC ($\varsigma_1, \ldots, \varsigma_N$) (Fig. 3)
- Sensors were used to take measurements for each battery cell in the stack
  - Voltage drop across each battery cell ($v_{bat,1}, \ldots, v_{bat,N}$)
  - Total voltage drop across the battery stack (V_{stack})
- The a priori residual data, used in the CUSUM algorithm, was generated using this model

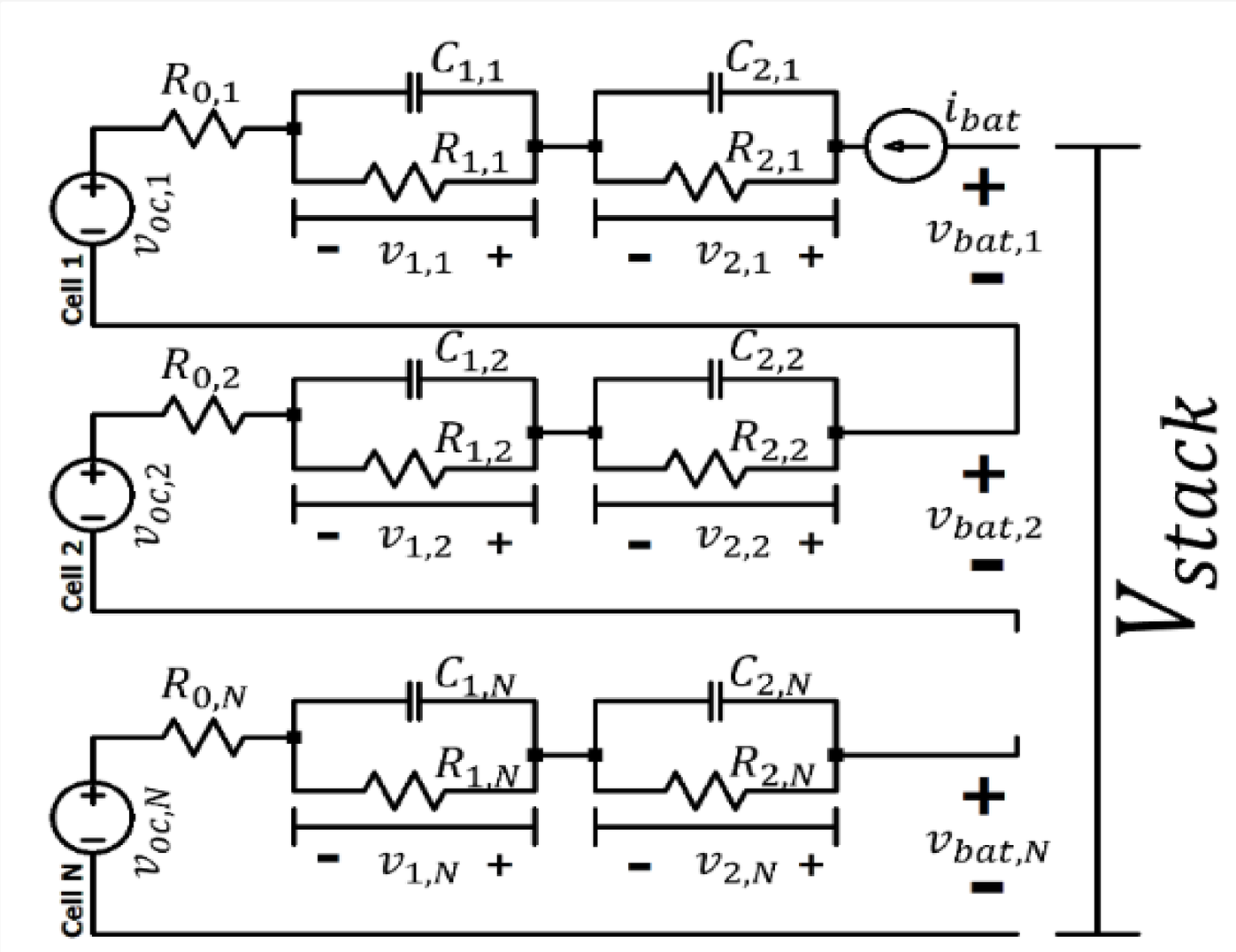

Fig. 2: Equivalent Circuit Model for Stack of N Batteries

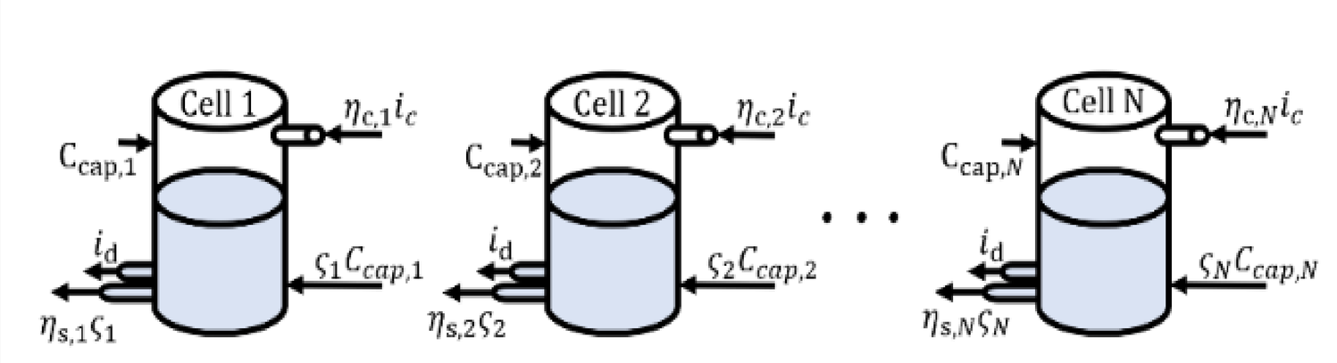

Fig. 3: Charge Reservoir Model for Stack of N Batteries

False Data Injection Attacks

- Injected into the voltage sensors of the battery model during simulation
  - Tested on single sensors and multiple sensors
  - Tested at random timesteps
- Larger magnitude attacks (Fig. 4) can be visually seen in state variable estimation, while smaller magnitude attacks require a detector to be noticed
  - During these experiments attacks of $\pm 500\ \mu V$ to $\pm 20\ mV$ were tested
- Attacks on voltage sensors may effect the a priori residual
- Used to verify the CUSUM algorithm is a viable attack detector

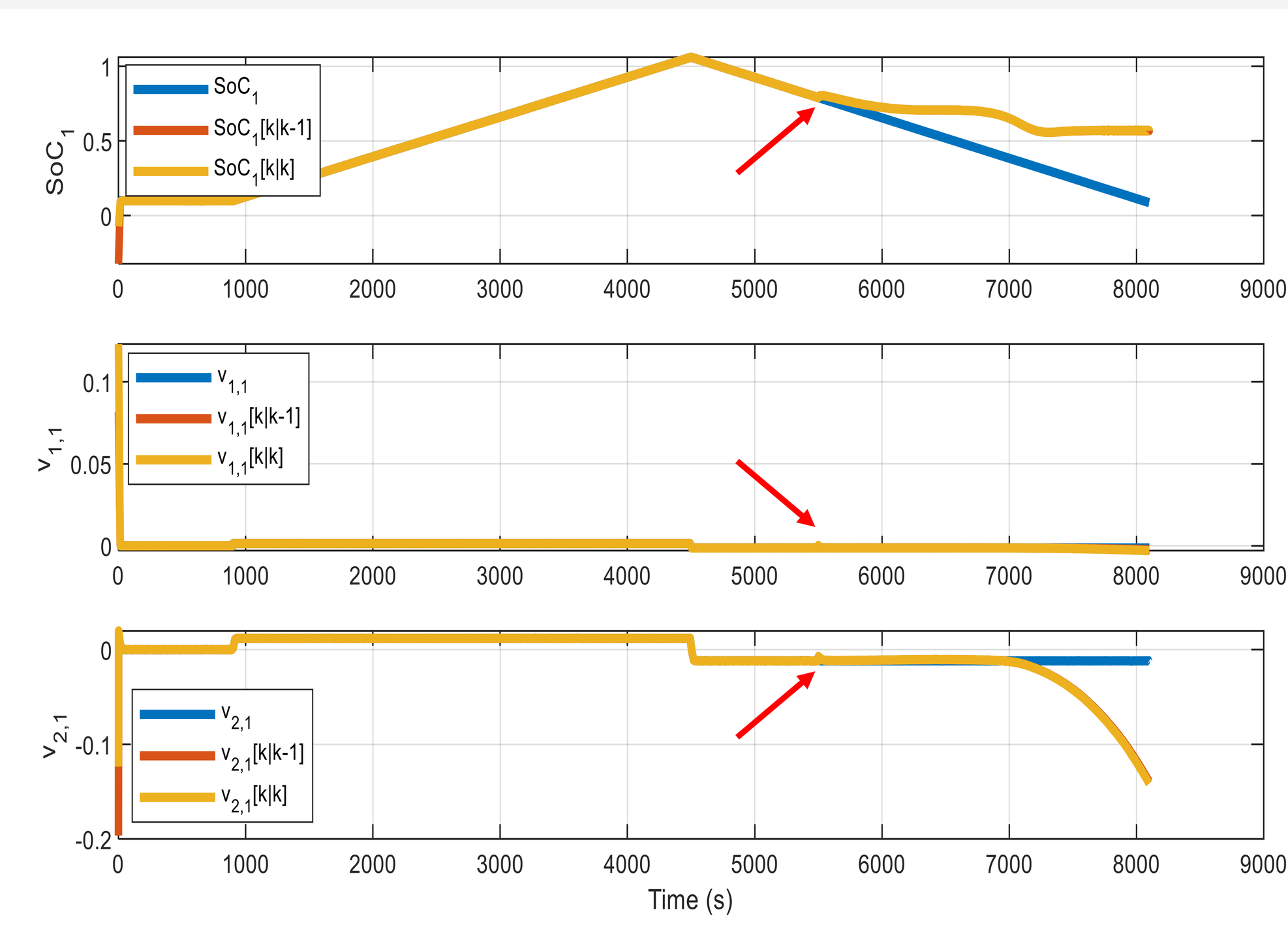

Fig. 4: Estimated State Variables for Cell 1, Following an Attack of 10 mV Injected in the $v_{bat,1}$ Sensor at t = 5500

Case Studies

Attack on a Single Sensor

- Most likely FDIA due to the cost and effort associated with launching a FDIA
- Was tested on a three-cell battery stack
  - Voltage sensors susceptible to attacks: $v_{bat,1}, v_{bat,2}, v_{bat,3}, V_{stack}$
  - Every sensor was tested with a variety of attack times and magnitudes
- Goal: to determine the minimum magnitude attack that was detectable by the CUSUM Algorithm

Observability Study

- Observability is a measure of whether a system is observable, unobservable systems are unable to perform state variable estimation
- A system may become unobservable when one or more sensors become disconnected / offline
- Was tested on a two-cell battery stack
  - Voltage sensors that could go offline: $v_{bat,1}, v_{bat,2}, V_{stack}$
  - The V_{stack} measurement added redundancy to the sensor measurements, as it was a combination of the other measurements ($v_{bat,1}$ and $v_{bat,2}$)
- Goal: to determine if state variables could still be accurately estimated in the event of sensor failure(s)

Time-To-Detection Analysis

- Time-To-Detection is a measure of how quickly an attack was detected by the CUSUM Algorithm
- Calculated for online and offline applications
  - Online applications: done in real-time, the amount of time it took the CUSUM Algorithm to detect an attack from the time it had been injected to a sensor
  - Offline applications: typically done over a longer timeframe (ex: once a day), once all the residual data was collected and stored, it was run through the CUSUM Algorithm all at once.
- Goal: to determine if CUSUM Algorithm is fast enough to work in real-world applications

Attack on Multiple Sensors

- Unlikely to occur if an attack on a single sensor will suffice, but included for completeness
- Was tested on a three-cell battery stack (with minimum detectable-magnitude attacks, where applicable)
  - Voltage sensors susceptible to attacks: $v_{bat,1}, v_{bat,2}, v_{bat,3}, V_{stack}$
  - Every combination of sensors was tested with a variety of attack times and magnitudes
  - Attack scenarios included:
    - Attacks of the same magnitude, injected at the same time
    - Attacks of different magnitudes, injected at the same time
    - Attacks of the same magnitudes, injected at different times
    - Attacks of different magnitudes, injected at different times
- Goal: to determine if the CUSUM Algorithm was able to detect attacks when multiple sensors were injected with FDIA

Results

- ❖ Successfully detected attacks (as low as $\pm 500\ \mu V$) injected in a single sensor with no false alarms

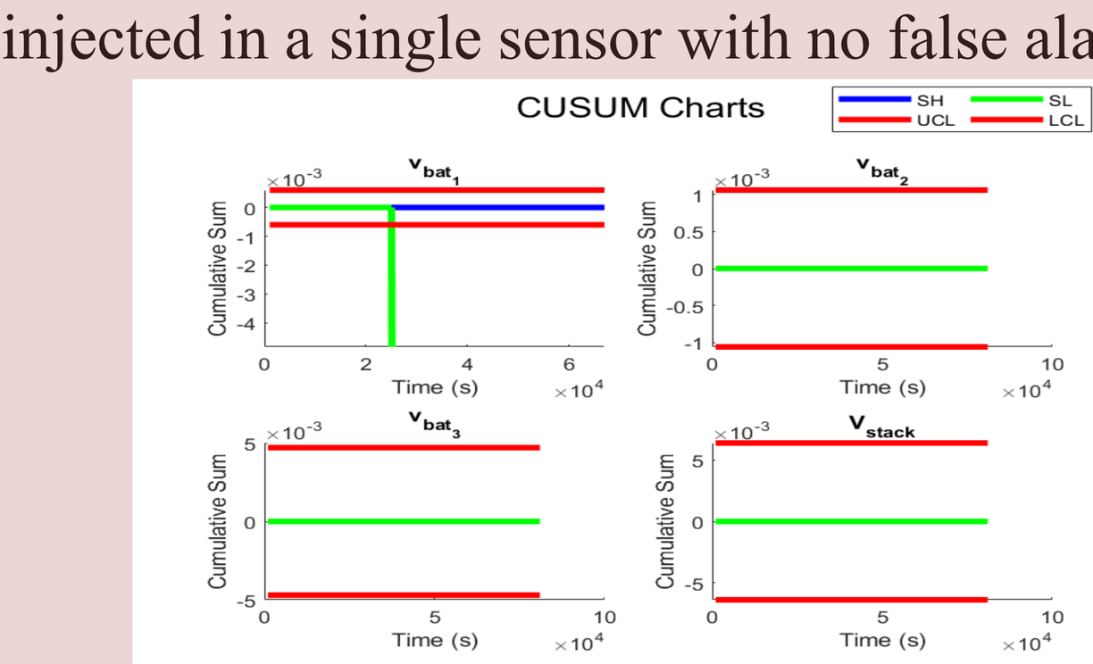

Fig. 5 : CUSUM Charts with a +1 mV Attack Injected to the $v_{bat,1}$ measurement at t = 5500

- ❖ For a stack of two batteries, the system remained observable in the event of a single sensor failure, therefore state variables were able to be accurately estimated
- ❖ The V_{stack} measurement added redundancy that created a more robust estimator
- ❖ In the event of a multi-sensor failure (where more than one sensor failed at a time), the system became unobservable and this method would no longer be effective to estimate states or detect FDIA using the a priori residual

- ❖ The CUSUM was found to be effective in online and offline grid applications
- ❖ In all offline experiments the attacks were detected in less than 0.1 s
- ❖ In all online experiments the attacks were detected in less than 10 s (sometimes less than 1 s)
- ❖ In general it took significantly longer to detect attacks in online applications than offline applications, this is because the CUSUM Algorithm had to wait for the system to generate residual data in real time

- ❖ The CUSUM Algorithm was able to detect attacks when multiple sensors were attacked

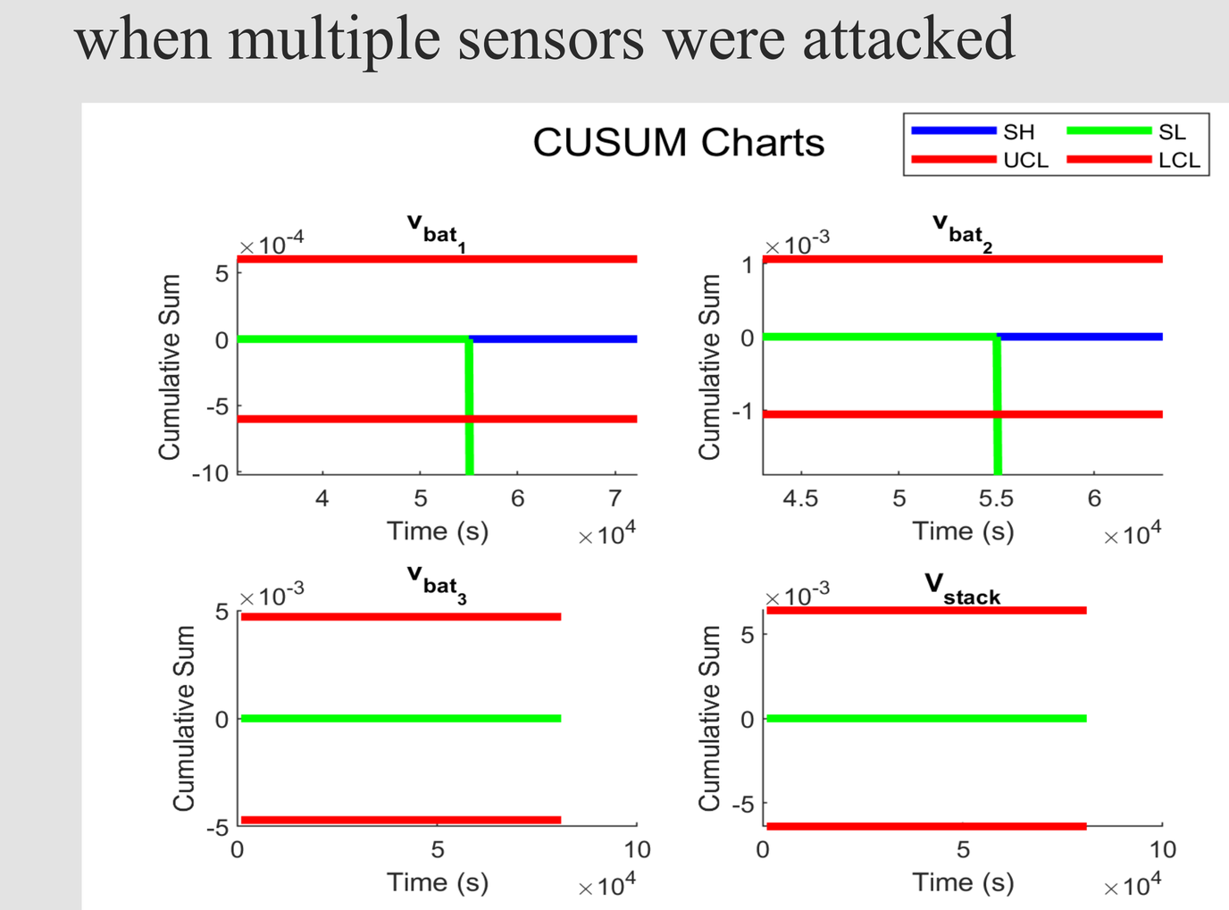

Fig. 6: CUSUM Charts with a +500 μV Attack Injected to the $v_{bat,1}$ and $v_{bat,2}$ measurement at t = 5500

Conclusions

- FDIAs pose a threat to the safe and efficient operation of the grid and its BESSs, and require additional detection mechanisms
- The CUSUM Algorithm presented was able to detect small-magnitude FDIA during single sensor and multi-sensor attacks with no false positives
- The redundancy added by the V_{stack} measurement allows the system to remain observable in the event of a single sensor failure
- The CUSUM Algorithm was unable to determine the sensor(s) being targeted or the magnitude of the attacks

References

[1] 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.

[2] 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 Transactions on Power Electronics*, vol. 34, no. 10, pp. 9709-9718, Oct. 2019, doi: 10.1109/TPEL.2019.2893622.

[3] Lopez, A.B., Vatanparvar, K., Deb Nath, A.P. *et al.* A Security Perspective on Battery Systems of the Internet of Things. *J Hardw Syst Secur* **1**, 188–199 (2017). https://doi.org/10.1007/s41635-017-0007-0

[4] 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.

[5] D. Rosewater, S. Ferreira, D. Schoenwald, J. Hawkins and S. Santoso, "Battery Energy Storage State-of-Charge Forecasting: Models, Optimization, and Accuracy," in *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2453-2462, May 2019.

[6] 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.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[8] 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.

[9] 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.

[10] 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.

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

[12] Sayghe, A., Hu, Y., Zografopoulos, I., Liu, X., Dutta, R.G., Jin, Y., & Konstantinou, C. (2020). A Survey of Machine Learning Methods for Detecting False Data Injection Attacks in Power Systems. *ArXiv, abs/2008.06926.*

[13] V. Obrien, R. D. Trevizan and V. Rao, "Detecting False Data Injection Attacks to Battery State Estimation Using Cumulative Sum Algorithm," *53rd North American Power Symposium (NAPS)*, Nov. 2021 pp 1-6

[14] "e-Handbook of Statistical Methods," National Institute of Standards and Technology and SEMATECH, Jun 2012. [Online]. Available: http://www.itl.nist.gov/div898/handbook/

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

[16] 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 Conference and Expo (ITEC), June 2018, pp. 934–938.

[17] 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.

[18] Bloomberg New Energy Finance, "Electric vehicle outlook," 2019. [Online]. Available: https://about.bnef.com/electric-vehicle-outlook/

[19] "Operational risk management in the U.S. energy storage industry: Lithium-ion fire and thermal event safety," Energy Storage Association, Tech. Rep., Sep 2019.

[20] 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.

[21] Miller, C. (2011, July 12). Battery Firmware Hacking: Inside the Innards of a Smart Battery. Accuvant Labs.

[22] 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.

[23] 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.

Acknowledgement

We 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. We would like to thank Dr. Ujjwol Tamrakar and Dr. Hyungjin Choi for their technical advice.

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's 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 .

*Victoria Obrien
Electrical Engineering Department at Texas Tech University / Energy Storage Technology & Systems at Sandia National Laboratories
Lubbock, TX / Albuquerque, NM, USA
victoria.obrien@ttu.edu, vaobrie@sandia.gov

**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