SAND2022-14854C

IEEE PES Power & Energy Society®
IEEE
EESAT
Austin, TX. November 7-9, 2022

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

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

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.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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-NA0003525.

Introduction

- Increased need for grid-scale energy storage systems
  - Battery Energy Storage Systems (BESSs)
  - Batteries are connected to meet voltage, current, and power requirements
- BESS employ a battery management system (BMS)
- State variable estimation and sensor measurements may be susceptible to cyber attacks

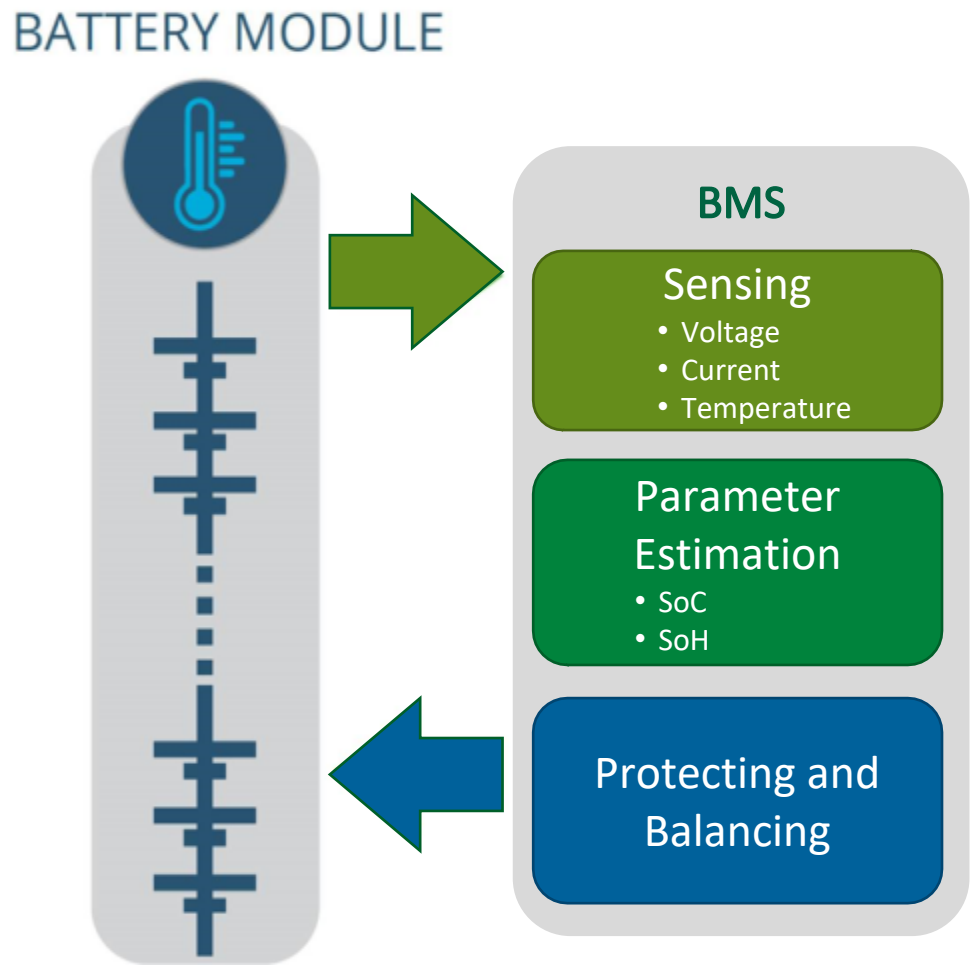


Figure 1. BMS functions

Problem Formulation

Goal: to increase battery cells' SoC estimation accuracy by incorporating ambient temperature dependent (ATD) models and by utilizing an Unscented Kalman Filter (UKF), then to detect FDIAs in voltage sensors under various attack scenarios

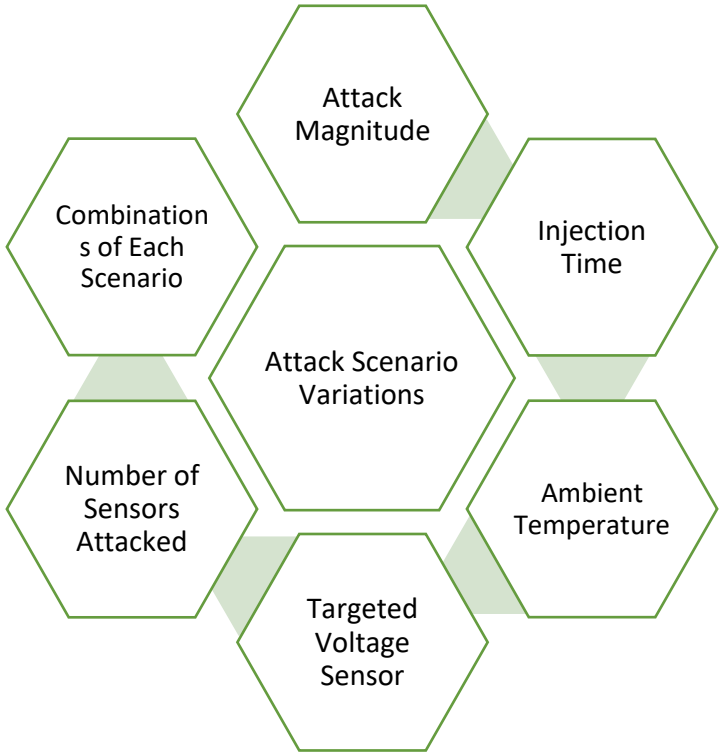


Figure 2. Tested Attack Scenario Variations

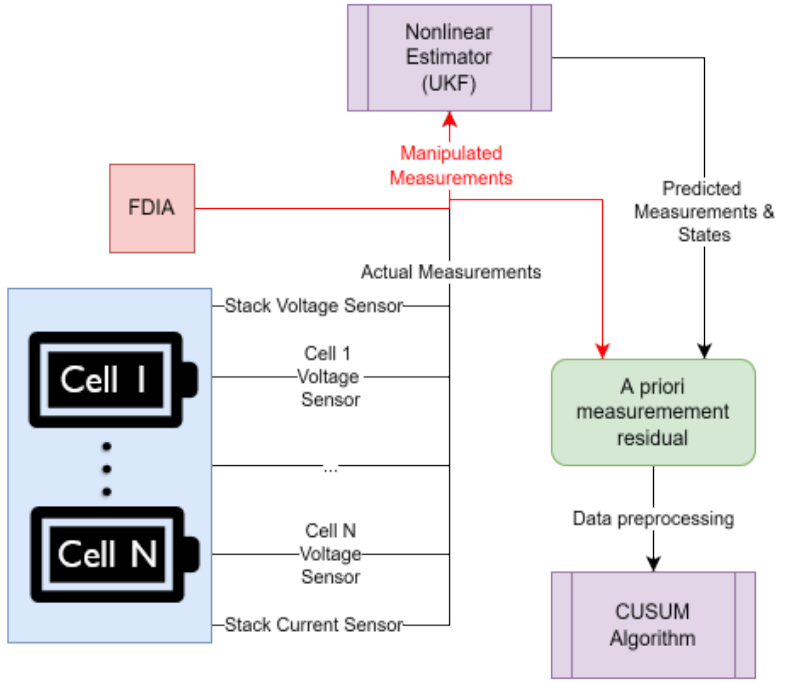


Figure 3. General process of SoC estimation and FDIA detection

False Data Injection Attacks (FDIAs)

- Possible Consequences:
  - Power outages
  - Damage to equipment / battery degradation
  - Thermal runaway events
  - Increased costs for utilities and consumers

- Bias attack:

$$y_a = y + \Delta y_a$$

- Δy_a is the attack vector
- y is the measurement vector
- y_a is the manipulated measurement vector

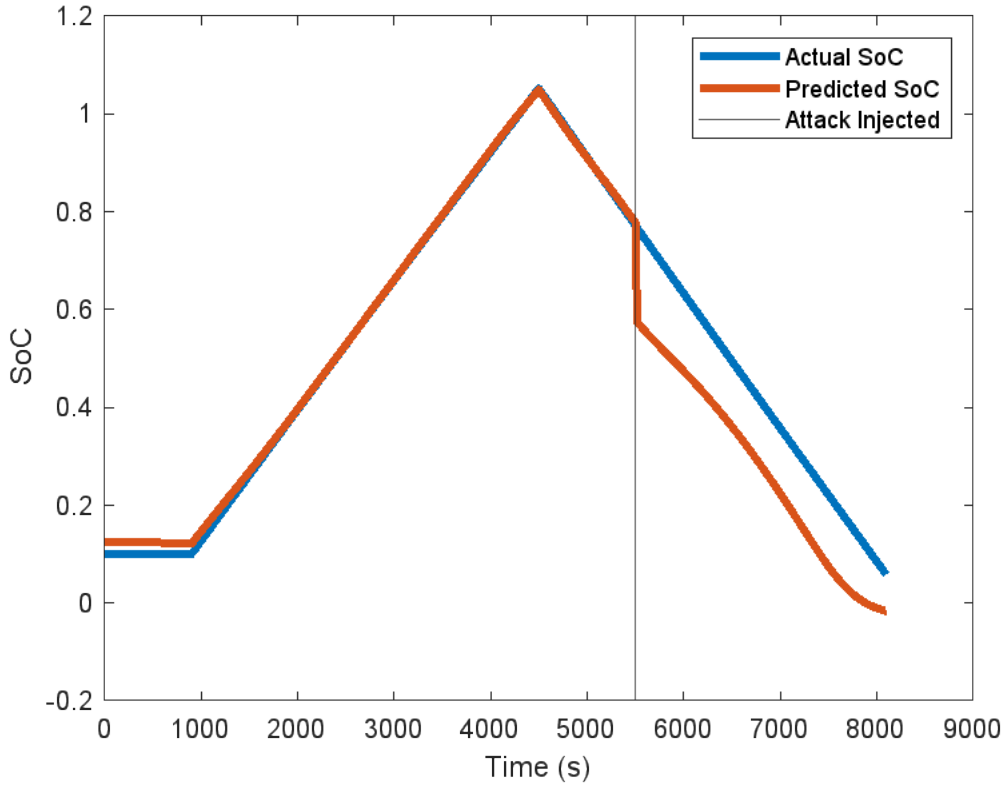


Figure 4. Cell 1 SoC when a 100 mV FDIA is Injected to the $v_{TOV,1}$ Measurement at 5500 s

Modeling Battery Dynamics

ATD Equivalent circuit model (ECM):

- Used to model dynamics of series-connected stacks of three batteries

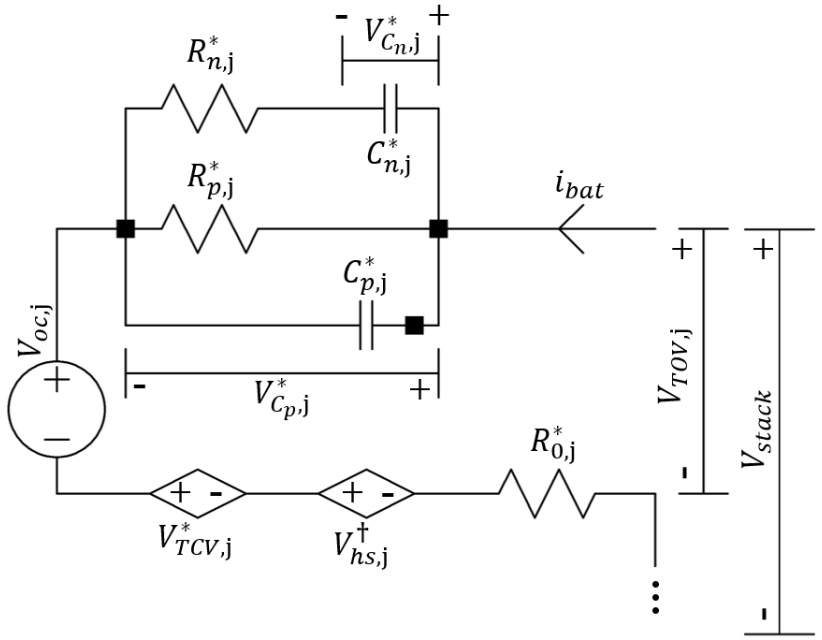


Figure 5. ECM for the j[th] Cell in a Stack of N Batteries

State of Charge (SoC):

- Available capacity relative to total capacity
- Described by charge reservoir model (CRM)

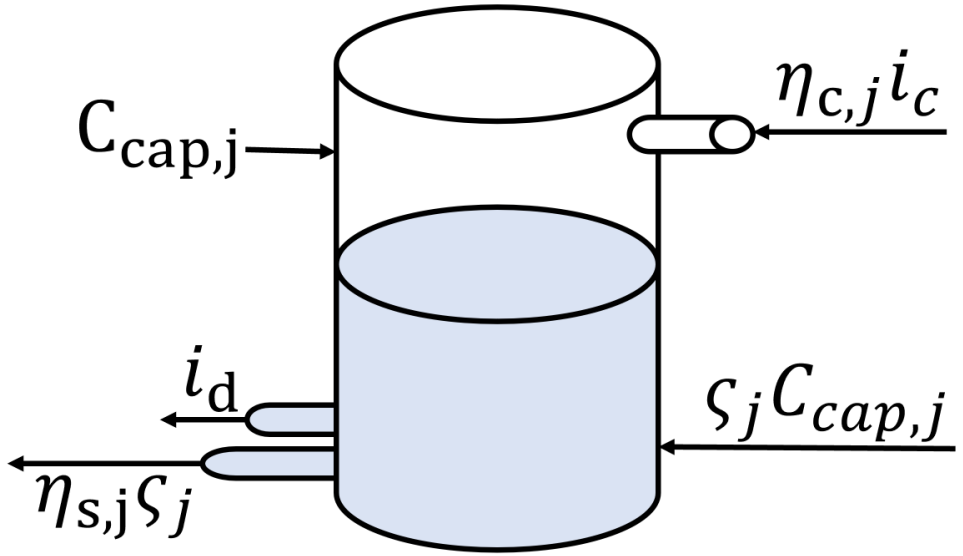


Figure 6. CRM for the j[th] Cell in a Stack of N Batteries

Ambient Temperature Dependence

- Internal battery parameters vary with ambient temperature
- The battery parameters for Cell 2 and Cell 3 were generated by adding a random value to the parameters from Cell 1 (based on the variation between cells' parameters in [4]) and fitting a curve to the data

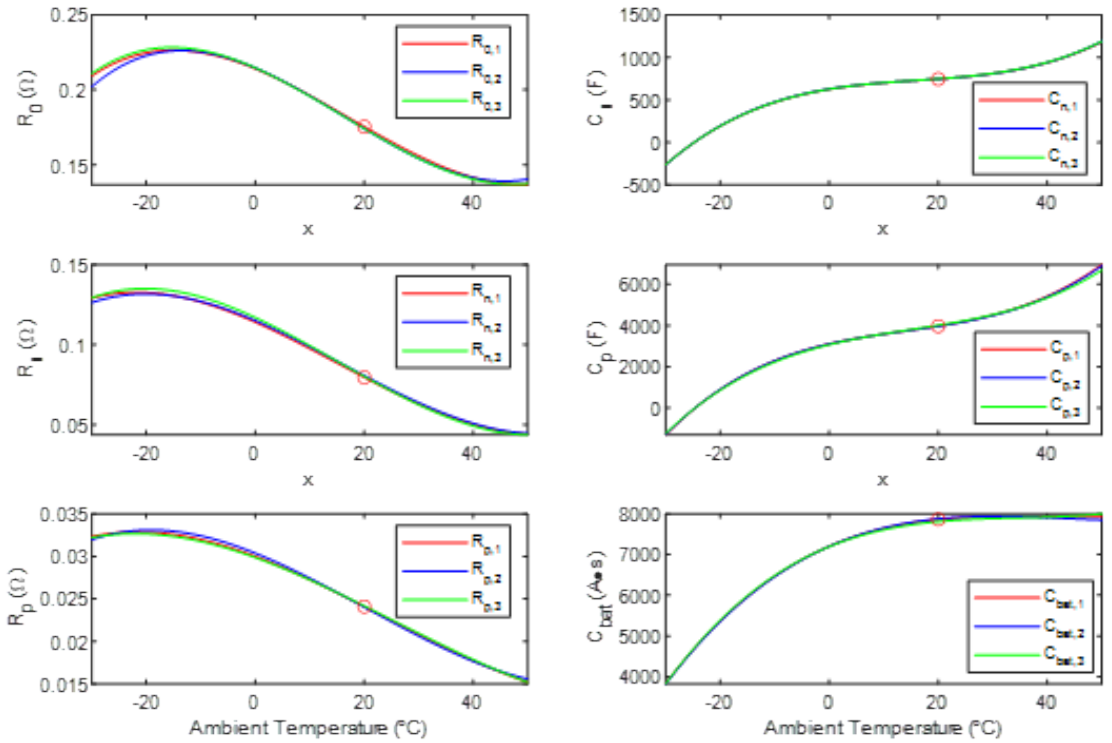


Figure 7. Internal battery parameter variation with ambient temperature [10]

Unscented Kalman Filter

- Typically more accurate for state estimation of nonlinear systems compared to the Extended Kalman Filter (EKF)
- Uses sigma points to represent the probability distribution of the nonlinear function

Figure 8. General steps of the UKF estimator

CUSUM Algorithm

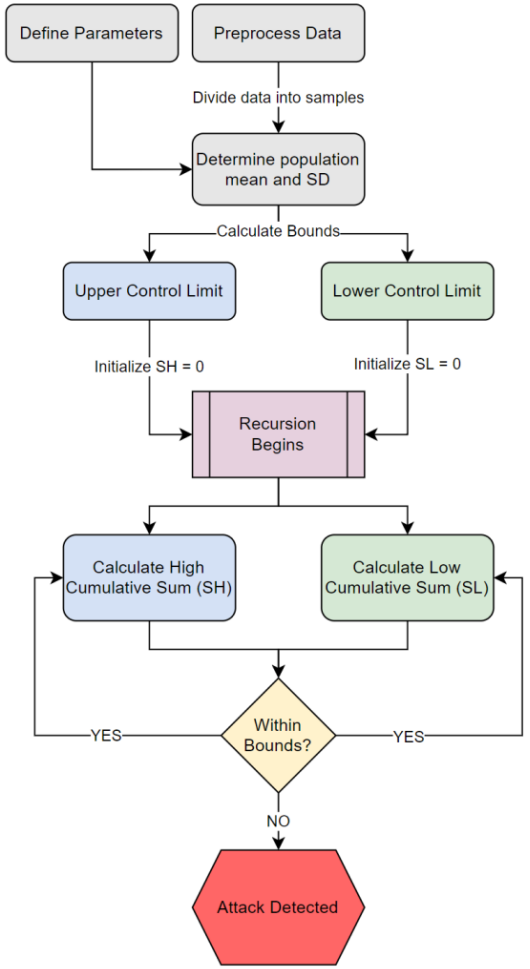


Figure 9. CUSUM Algorithm Flowchart

- Uses a priori residual with μ = 0:

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

- Population Standard Deviation:

$$\sigma_z = \frac{A_3 \bar{s}}{3}$$

- Upper / Lower Control Limit:

$$UCL = h\sigma_z \, , \, LCL = -h\sigma_z$$

- High and Low CUSUM:

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

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

- Determine presence of attack:

$SH_i > UCL$ or $SL_i < LCL$ → attack present

$SH_i \leq UCL$ and $SL_i \geq LCL$ → no attack

Case Studies & Results

Case Study 1: Estimation Accuracy

- Goal: Compare the estimation accuracy of the UKF vs. the EKF
  - In terms of state and measurement estimation
  - Metrics: Maximum Absolute Error (MAE) and Root Mean Squared Error (RMSE)

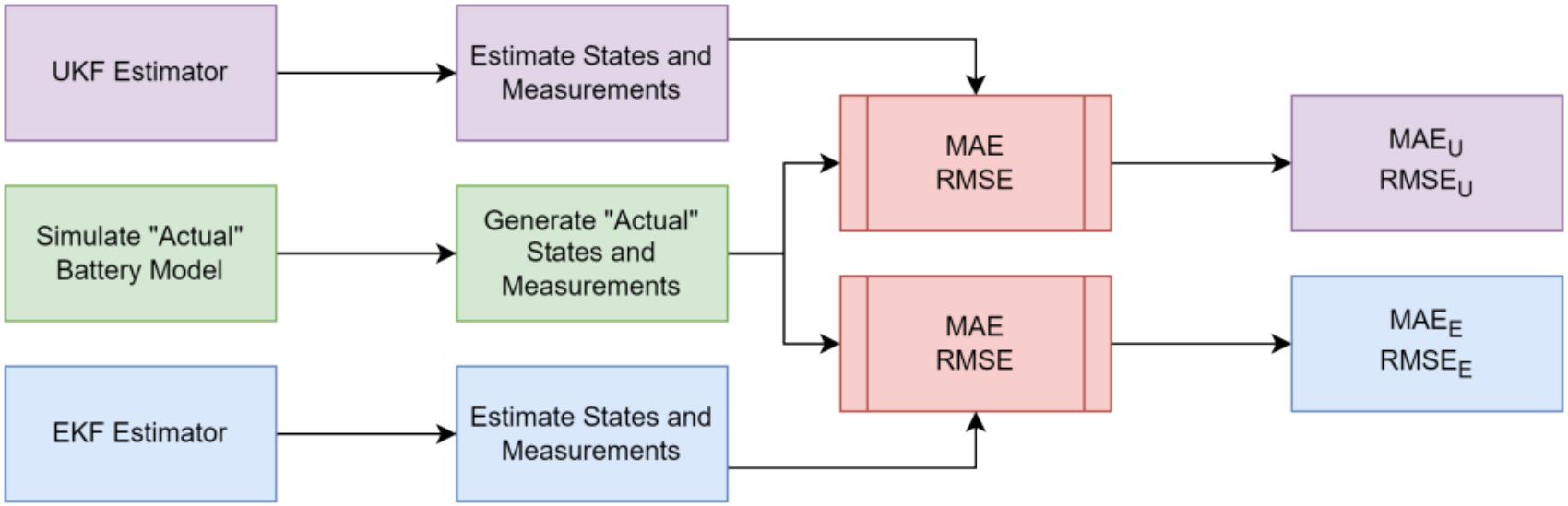


Figure 11. Estimation Accuracy Flowchart

Estimation Accuracy Results

- UKF vs. EKF error at various ambient temperatures
- Maximum Absolute Error (MAE):

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}|$$

- Root Mean Squared Error (RMSE):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y})^2}$$

- UKF was more accurate estimating states and measurements in all cases compared to EKF

T (°C)	MAE_E	MAE_U
-10	0.0675	0.0295
0	0.0713	0.0360
10	0.0686	0.0364
20	0.0651	0.0358
30	0.0620	0.0354
40	0.0609	0.0355
50	0.0623	0.0377

T (°C)	$RMSE_E$	$RMSE_U$
-10	0.0936	0.0485
0	0.0964	0.0545
10	0.0931	0.0545
20	0.0892	0.0539
30	0.0859	0.0536
40	0.0836	0.0540
50	0.0835	0.0562

Case Study 2: CUSUM Detection

- Goals:
  - Determine the magnitude of the minimum detectable attack
  - Determine if CUSUM could detect attacks under each attack scenario variation
  - Minimize false positives

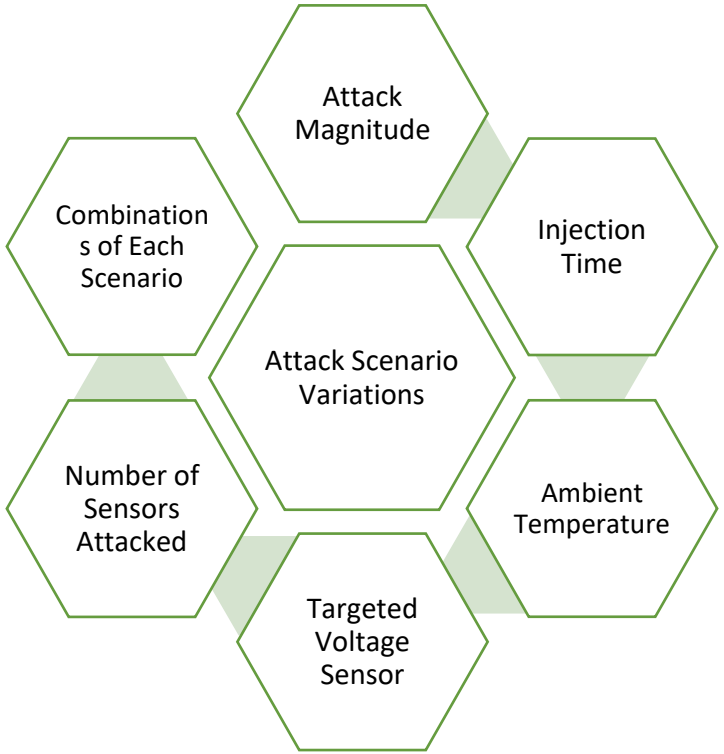


Figure 2. Tested Attack Scenario Variations

CUSUM Detection Results

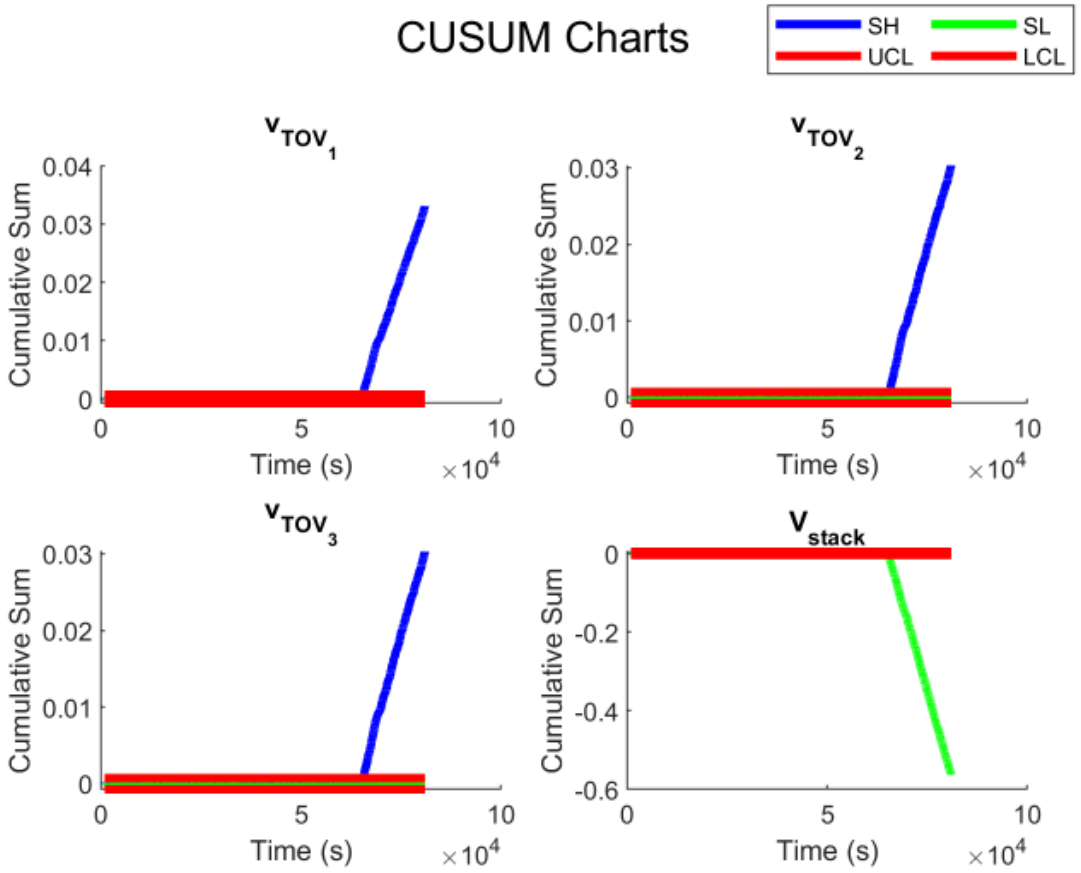


Figure 12. CUSUM Charts for a 1 mV Attack Injected to the v_{TOV_1} Sensor at a 6529 s and 39°C

- Attacks ±1 mV or greater were able to be detected
- Parameters that did not appear to have an impact on detectability:
  - Ambient temperature
  - Attack injection time
  - Targeted sensor
  - Number of sensors targeted
- No false positives

Conclusions

- The UKF was more accurate in estimating states and measurements in all cases compared to the EKF in terms of RMSE and MAE
- Attacks of ±1 $\mathcal{M}$ or greater in voltage sensor(s) were able to be detected by the CUSUM algorithm
- The varying attack scenarios did not appear to have an impact on the CUSUM's ability to detect FDIAs
- The CUSUM algorithm did not have any false positives when using the UKF or EKF

Acknowledgements

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 Hyungjin Choi and Atri Bera for their 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, doi: 10.1002/er.5435.

[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.

Questions?

Thank you!

ATD ECM Governing Equations

$$\dot{V}_{C_{n,j}} = \frac{V_{C_{n,j}}}{R_{n,j}(T)C_{n,j}(T)} + \frac{V_{C_{p,j}}}{R_{n,j}(T)C_{n,j}(T)}$$

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

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

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

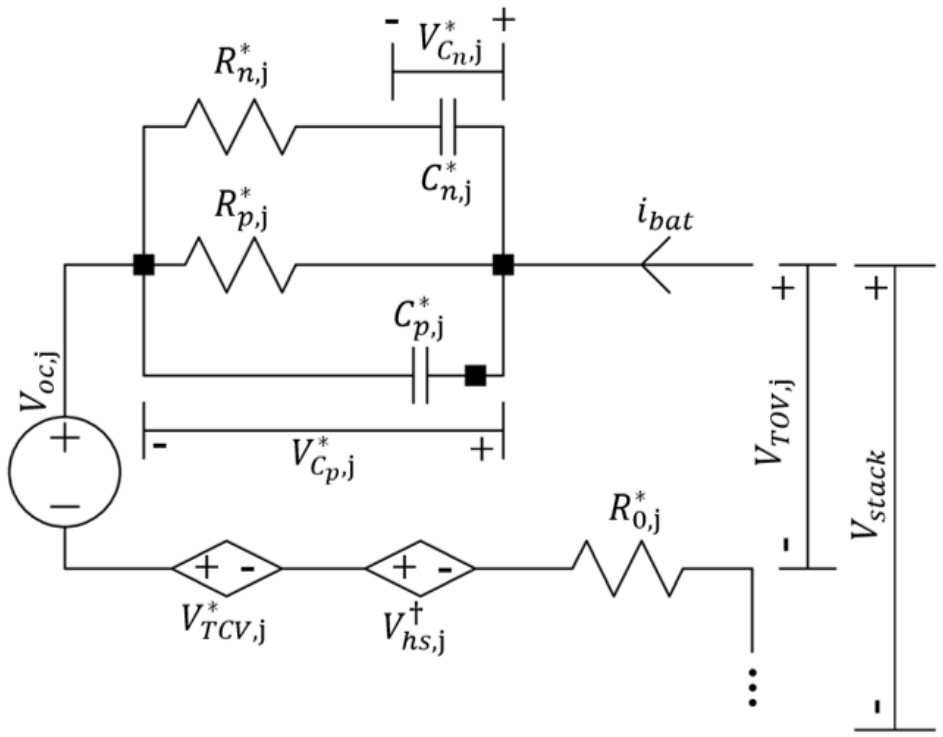
$$V_{TCV,j} = p_{02}(T)^2 + p_{01}(T) + p_{00}$$

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

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

$$i_{bat} = i_c + i_d$$

	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}
$V_{oc,1}$	1.36	-5	-1.917	7	8.79	-	−2	3.149
$V_{hs,1}$	-	-	-	-	−7.55	-	-	0.0755
$V_{TCV,1}$	-	-	-	-	-	−9.2	1.2	-0.097
$V_{oc,2}$	1.37	-5	-1.921	7.1	8.867	-	-2	3.149
$V_{hs,2}$	-	-	-	-	-7.27	-	-	0.07353
$V_{TCV,2}$	-	-	-	-	-	-9.98	1.242	-0.0964
$V_{oc,3}$	1.37	-5	-1.923	7.06	9.02	-	-2	3.149
$V_{hs,3}$	-	-	-	-	-7.869	-	-	0.077
$V_{TCV,3}$	-	-	-	-	-	-10.75	1.188	-0.0953



ATD Equations and Coefficients

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

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

UKF Equations

Step 1: Initialization

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

$$P_{0|0} = P_0$$

Step 2: Prediction of States

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

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

Step 3: Generate the SPs and associated weights

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

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

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

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

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

$$W^i_{m_{k+1|k}} = W^i_{c\ k+1|k} = \frac{1}{2(n+\lambda)}$$

$$\lambda = a^2(n+\kappa) - n$$

Step 4: Correction

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

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

$$P_{yy_{k+1|k}} = \sum_{i=0}^{2n} W^i_c \left(h\left(\mathcal{X}_{i_{k+1|k}}\right) - \hat{y}_{k+1|k}\right) \cdot \left\{h\left(\mathcal{X}_{i_{k+1|k}}\right) - \hat{y}_{k+1|k}\right\}^T$$

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

$$K_{k+1} = P_{xy_{k+1|k}} \cdot S^{-1}_{k+1}$$

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

$$P_{k+1|k+1} = P_{k+1|k} - K_{k+1}S_{k+1}K^T_{k+1}$$

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

EKF Equations

$$\hat{x}[k|k-1] = f\left(\hat{x}[k-1|k-1], u[k-1], \mathbb{E}\left[w[k-1]\right]\right)$$

$$P[k|k-1] = AP[k-1|k-1]A^T + Q$$

$$\hat{x}[k|k] = \hat{x}[k|k-1] + K[k](y[k] - \hat{y}[k|k-1]$$

$$\hat{y}[k|k-1] = g(\hat{x}[k|k-1], u[k], \mathbb{E}\left[e[k]\right])$$

$$\hat{y}[k|k] = g\left(\hat{x}[k|k], u[k], \mathbb{E}\left[e[k]\right]\right)$$

$$P[k|k] = P[k|k-1] - K[k]CP[k|k-1]$$

$$K[k] = P[k|k-1]C^T\left(CP[k|k-1]C^T + R\right)^{-1}$$

$$A[k] = \frac{\partial f(x[k],u[k],w[k])}{\partial x[k]}\Big|_{x[k]=\hat{x}[k|k]}$$

$$C[k|k] = \frac{\partial g(x[k], u[k], v[k])}{\partial x[k]}\Big|_{x[k]=\hat{x}[k|k]}$$

$$C[k|k-1] = \frac{\partial g(x[k],u[k],v[k])}{\partial x[k]}\Big|_{x[k]=\hat{x}[k|k-1]}$$

UKF vs. EKF Characteristics

UKF	EKF
• Works well in all nonlinearities • Uses sigma points to represent probability distribution of function • Theoretically more accurate than EKF • Examples of applications: power batteries, personal navigation	• Works well in systems represented by linear approximations • Requires calculation of Jacobian matrix • Examples of applications: electric vehicle batteries, temperature-dependent batteries