Secure Estimation and Attack Detection for Power Grids Under Adversarial Attacks

Mukai Zhang [1], Vijay Gupta [1], Rodrigo Trevizan [2], Babu Chalamala [3], Raymond H. Byrne [2]

[1]School of Electrical and Computer Engineering, Purdue University [2]Energy Storage Technology & Systems, Sandia National Laboratories [3]Nuclear Fuel Cycle and Grid Modernization, Sandia National Laboratories

Abstract

We consider a radial distribution grid in which the nodes are providing reactive power for voltage control. Some nodes may be adversarial and inject more or less power than prescribed. We propose an estimator to simultaneously estimate the state of the grid and reconstruct any power being inputted by the adversarial nodes.

Problem Formulation

1. Radial distribution network with n buses; bus 0 has fixed voltage. Voltage magnitudes $v(k)$ can be observed and reactive power injections $q(k)$ can be controlled.
2. Linearized power flow equations at 1 p.u. voltage result in the evolution:

$$\Sigma_l : \begin{aligned} q(k+1) &= u(k) \\ y(k) &= v(k), \end{aligned} \tag{1}$$

with $u(k)$ given by a droop controller

$$u(k) = \begin{cases} q_{\max} & v(k) < v_l \\ u^\star(k) - \overline{K}\,(v(k) - v^\star) & v_l \le v(k) \le v_h \\ q_{\min} & v(k) > v_h. \end{cases} \tag{2}$$

3. The voltage $v(k)$ and reactive power $q(k)$ satisfy $v(k) = Xq(k) + \tilde{v}(k)$, where X is a positive definite matrix that characterizes the reactance of the network and $\tilde{v}(k)$ depends on the real power injections and the network parameters and is not controllable.
4. One or more nodes are adversarial in that they do not follow the control algorithm and instead add an additive attack vector $d(k)$ at the input.
5. Thus, the overall system evolution is given by

$$\begin{aligned} q(k+1) &= u(k) + d(k) \\ y(k) &= Xq(k) + \tilde{v}(k), \end{aligned} \tag{3}$$

where $u(k)$ is the control action prescribed by a controller of the form (2).

6. Problem Considered: Simultaneously estimate the adversarial vector $d(k)$ and the state $q(k)$. Note that while the vectors $y(k)$ and $u(k)$ are known to the estimator, the input $\tilde{v}(k)$ that arises due to linearization of the non-linear model is unknown

Motivation

1. With the induction of Distributed Energy Resources (DERs), the distribution grid will become vulnerable to cyberattacks. However, many relevant standards such as by NERC still pertain to bulk power systems.
2. Power system state estimators (PSSEs) are particularly vulnerable to cyberattacks, thus jeopardising reliable situational awareness at the system operator and critical grid functions.
3. Relatively less work has considered controller-side false data injection attacks (FDIA) on PSSEs in which the attacker can inject false controller data, although it has been recognized that such attacks can be very harmful.
4. One difficulty is that the distribution grid is non-linear; yet, a linearized model is often used for PSSE. This introduces a residual error term. In sensor FDIA, this residual error and the false data can be subsumed into one 'error' term. In controller FDIA, the residual error corrupts the sensor measurement and the attacker corrupts the control vector, and the two can interact in intricate ways.

Our Contributions

1. If the attack vector is sparse and residual linearization error is small, we combine 1-norm approximator for output disturbance reconstruction and an unknown input observer (UIO) for state estimation.
2. If such sparsity assumptions cannot be made, we utilize a robust-UIO design for state estimation and attack reconstruction.

Rather than the assumption of known structure (mean, variance, and so on) on the attacker induced false data, we assume only that it is bounded in the ℓ_∞ norm.

Case 1: Sparse Attack and Small Linearization Error

First, we assume that the vector $\mathcal{E}^k$ defined as concatenation of $\tilde{v}^k_{k-\tau+1}$ and $d^{k-1}_{k-\tau+1}$ is sparse (perhaps after thresholding).

1. Collect τ-step observation of the output measurements

$$\begin{aligned} \hat{Y}^k &\triangleq y^k_{k-\tau+1} - \mathcal{B} r^{k-1}_{k-\tau+1} \\ &= \mathcal{O}^{\tau-1} q(k-\tau+1) + \Omega \mathcal{E}^k, \end{aligned} \tag{4}$$

where $\mathcal{O}^{\tau-1}$ is observability matrix and Ω is controllability matrix for the system.

2. First, we use this equation for recovery of the sparse attack and linearization error through the optimization

$$\min \|\mathcal{E}^k\|_0 \quad \text{subject to} \quad \hat{Y}^k = \mathcal{O}^{\tau-1} q(k-\tau+1) + \Omega \mathcal{E}^k.$$

We replace the problem with the 1-norm minimization

$$\min \|\mathcal{E}^k\|_1 \quad \text{subject to} \quad \hat{Y}^k = \mathcal{O}^{\tau-1} q(k-\tau+1) + \Omega \mathcal{E}^k.$$

3. To estimate the state of the plant, we use an unknown input observer (UIO) of the form

$$\begin{aligned} z(k+1) =& (I - MC_l)\,(A_l z(k) + A_l M\tilde{y}(k) + B_l r(k)) \\ &+ L(\tilde{y}(k) - C_l z(k) - C_l M\tilde{y}(k)) \qquad (5) \\ \hat{q}(k) =& z(k) + M\tilde{y}(k), \qquad (6) \end{aligned}$$

where $z(k) \in \mathbb{R}^n$ is the internal state of the UIO, $M \in \mathbb{R}^{n\times n}$ and $L \in \mathbb{R}^{n\times n}$ are design parameter matrices chosen such that (i) the matrix $((I - MC_l)A_l - LC_l)$ is Schur stable, and (ii) the matrix $(I - MC_l)B_l$ is identically a zero matrix. Let $e_q(k) = q(k) - \hat{q}(k)$ be the estimation error. Under the sparsity assumption of the error collection vector $\mathcal{E}^k$, the norm-estimator can have correct estimate of $\tilde{v}$ and further erase it. After calculation, the error dynamics becomes

$$e_q(k+1) = ((I - MC_l)A_l - LC_l)e_q(k) + (I - MC_l)B_l d(k).$$

Since $((I - MC_l)A_l - LC_l)$ is Schur stable and $(I - MC_l)B_l = O$, the dynamics are asymptotically stable.

Guarantees from this Estimator

1. If the error collection vector $\mathcal{E}^k$ is sufficiently sparse, then the attack vector is reconstructed almost everywhere.
2. The state estimation error approaches zero asymptotically regardless of the presence of attacks against control input.

Case 2: Non-Sparse Error

If the sparsity assumptions do not hold, we propose an estimator of the form

$$\begin{aligned} z(k+1) =& (I - MC_l)\,(A_l z(k) + A_l M y(k) + B_l r(k)) \\ &+ L(y(k) - C_l z(k) - C_l M y(k)) \qquad (7) \\ \hat{q}(k) =& z(k) + My(k), \qquad (8) \end{aligned}$$

where the input $y(k)$ is obtained from the system. Further, the gains M and L are chosen as

$$M = B_l(C_l B_l)^\dagger, \qquad L = P_{\mathcal{O}}^{-1} N,$$

where $P_{\mathcal{O}} = P_{\mathcal{O}}^\top \succ 0$, N, and $\kappa \in (0, 1)$ are obtained by solving the linear matrix inequality (LMI):

$$\begin{bmatrix} -P_{\mathcal{O}} & P_{\mathcal{O}}(I - MC_l)A_l - NC_l & -I \\ \star & -(1-\kappa)P_{\mathcal{O}} & O \\ \star & O & -\kappa I \end{bmatrix} \preceq 0. \tag{9}$$

Finally, the estimate of the attack vector is given by

$$\begin{aligned} \hat{d}(k-1) = (C_l B_l)^\dagger C_l \big[&\hat{q}(k) - A_l \hat{q}(k-1) \\ &- B_l u^\star - A_l y(k-1) + A_l y^\star\big]. \end{aligned} \tag{10}$$

Guarantees from this Estimator

1. Define the state estimation error $e_q(k) = q(k) - \hat{q}(k)$. The error dynamics e_q is globally uniformly ℓ_∞-stable with performance level $\gamma = \frac{1}{\sqrt{\lambda_{\min}(P_{\mathcal{O}})}}$. Thus, $\|e_q(k)\|_\infty \le \gamma \|\alpha(k)\|_\infty$, where $\alpha(k) = -L\tilde{v}(k) - M\tilde{v}(k+1)$.
2. The attack reconstruction error $e_d(k) = d(k) - \hat{d}(k)$ satisfies

$$\limsup_{k\to\infty} \|e_d(k-1)\|_\infty \le \gamma \|\Theta\|_\infty \|D_q\|_\infty \|\tilde{v}\|_\infty, \tag{11}$$

where $\Theta = (C_l B_l)^\dagger C_l \begin{bmatrix} I & -A_l \end{bmatrix}$ and $D_q = -\begin{bmatrix} L & M \end{bmatrix}$.

Case Study: IEEE 13-bus test feeder system

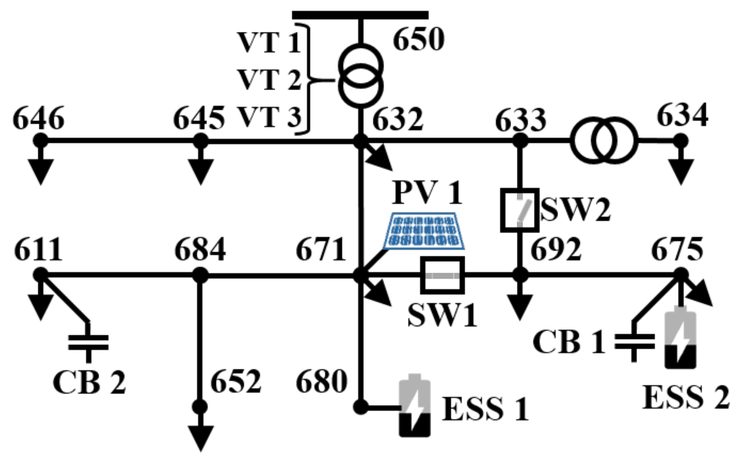

Figure 1. Modified test feeder with two 3-phase 600 kW energy storage systems (ESSs), two PV generators and switch SW2.

OpenDSS simulation with time step of 1s.

Attack Identification: Case 1

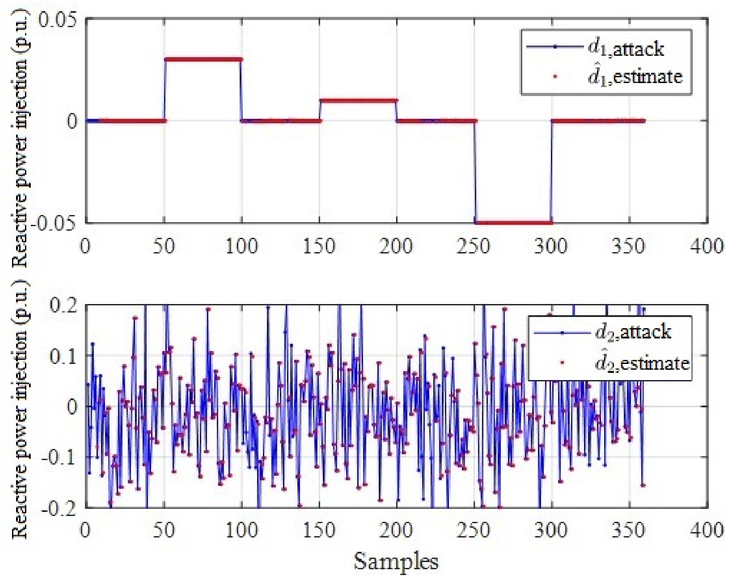

Figure 2. Attack sequence can be reconstructed by the observer.

Attack Identification: Case 2

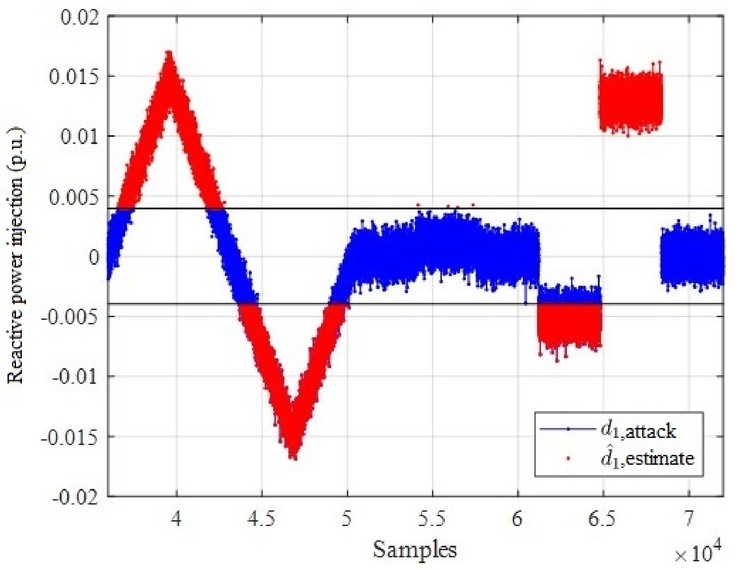

Figure 3. Attack vector can be detected, but not reconstructed.

Conclusions

1. We proposed two centralized observers for the case when distribution grids are under adversarial FDIA attacks on the controller side, while explicitly considering the fact that the distribution grid dynamics are non-linear. We utilize UIO theory from robust control and provide analytical guarantees.
2. Future work includes extending this approach to distributed observer design.

Acknowledgment

The authors would like to thank Dr. Imre Gyuk, Director of the Energy Storage Program, for his continued support.

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-NA0003525. SAND2023-10513 C.

rdtrevi@sandia.gov