Addressing Model Uncertainty and Cyber Attacks Against Measurements for Dynamic State Estimation

Junjian Qi¹, Ahmad Taha², Jianhui Wang³

¹University of Central Florida
²The University of Texas at San Antonio
³Southern Methodist University
Importance of State Estimation

- Robust, real-time feedback control requires real-time dynamic state estimation

- Greg Zweigle from SEL yesterday at the Challenges of Cascading Failure panel
Dynamic State Estimation

- General nonlinear dynamical model:

  \[
  \begin{align*}
  \dot{x} &= f(x, u) \\
  y &= h(x, u)
  \end{align*}
  \]

- Information needed
  - Power system dynamic model, subject to model uncertainty
  - PMU measurements, subject to bad data/cyber attacks
Model Uncertainties

- Dynamics under unknown inputs
  \[ \dot{x}(t) = f(x, u) + B_w w(t) \]
  - A combination of unmeasurable or unmeasured disturbances, unknown control action, or unmodeled system dynamics

- Unavailable inputs
  - Unmeasurable or unmeasured known inputs

- Parameter inaccuracy in \( f(x, u) \)
Cyber Attacks Against Measurements

\[ y(t) = h(x, u) + v(t) \]

- **Data integrity attacks**
  - Corrupting the content of measurement, such as man-in-the-middle attacks that intercept, modify signals

- **Denial of Service attack**
  - Introducing a denial in communication of measurement such as by flooding the network

- **Replay attack**
  - Special case of data integrity attacks where the attacker replays a previous snapshot of a valid packet sequence
Observer for Linearized System

\[
\begin{align*}
\dot{\delta}_i &= \omega_i - \omega_0 \\
\dot{\omega}_i &= \frac{\omega_0}{2H_i} \left( T_{m_i} - T_{e_i} - \frac{K_{D_i}}{\omega_0} (\omega_i - \omega_0) \right) \\
\dot{e}_q &= \frac{1}{T_{d0,i}} \left( E_{fd_i} - e'_{q_i} - (x_{d_i} - x'_{d_i}) i_{d_i} \right) \\
\dot{e}_d &= \frac{1}{T'_{q0,i}} \left( -e'_{d_i} + (x_{q_i} - x'_{q_i}) i_{q_i} \right) \\
\dot{V}_{R_i} &= \frac{1}{T_{A_i}} (-V_{R_i} + K_{A_i} V_{A_i}) \\
\dot{E}_{fd_i} &= \frac{1}{T_{E_i}} \left( V_{R_i} - K_{E_i} E_{fd_i} - S_{E_i} \right) \\
\dot{R}_{fi} &= \frac{1}{T_{F_i}} \left( -R_{fi} + E_{fd_i} \right) \\
\dot{t}g_{1_i} &= \frac{1}{T_{s_i}} (D_i - t g_{1_i}) \\
\dot{t}g_{2_i} &= \frac{1}{T_{c_i}} \left( \left( 1 - \frac{T_{3_i}}{T_{c_i}} \right) t g_{1_i} - t g_{2_i} \right) \\
\dot{t}g_{3_i} &= \frac{1}{T_{5_i}} \left( \left( \frac{T_{3_i}}{T_{c_i}} t g_{1_i} + t g_{2_i} \right) \left( 1 - \frac{T_{4_i}}{T_{5_i}} \right) - t g_{3_i} \right)
\end{align*}
\]

\[
\begin{align*}
\dot{x}(t) &= f(x) \\
y_q(t) &= h(x)
\end{align*}
\]

Linearize

\[
\begin{align*}
\dot{x}(t) &= A x(t) \\
y_q(t) &= C_q x(t)
\end{align*}
\]
Observer for Linearized System, cont’d

\[
\begin{align*}
\dot{x}(t) &= A x(t) \\
 y_q(t) &= C_q x(t)
\end{align*}
\]

\[
\begin{align*}
\dot{x}(t) &= A x(t) + B_w \omega(t) \\
y_q(t) &= C_q x(t) + v_q(t)
\end{align*}
\]

Unknown inputs
Attack vector
Sliding Mode Observer Design

\[
\begin{align*}
\dot{x}(t) &= A\dot{x}(t) + L_q(y_q(t) - \hat{y}_q(t)) - B_w E(\hat{y}_q, y_q, \eta) \\
\hat{y}_q(t) &= C_q \hat{x}(t)
\end{align*}
\]

where \( E(\cdot) = \begin{cases} 
\eta \frac{F_q(\hat{y}_q - y_q)}{\|F_q(\hat{y}_q - y_q)\|_2 + \nu} & \text{if } F_q(\hat{y}_q - y_q) \neq 0 \\
0 & \text{if } F_q(\hat{y}_q - y_q) = 0
\end{cases} \)

- Design variables: matrices \( F_q, L_q \)
- Good design yields asymptotic convergence of est. error

\[ \lim_{t \to \infty} e(t) = \lim_{t \to \infty} (\hat{x}(t) - x(t)) = 0 \]
Observer Design: Finding $F_q$ & $L_q$

- Solve for $P$, $F_q$, $Y$

$$A^TP + PA - C_q^TY^T - YC_q = -Q$$

$$P = P^T$$

$$F_qC_q = B_w^TP$$

- Then recover the observer gain: $L_q = P^{-1}Y$

- The linear matrix inequality is scalable
Estimate Unknown Inputs

- Discrete version of the power system dynamics:
  \[ x(k + 1) = \tilde{A}x(k) + \tilde{B}_u u(k) + \tilde{B}_w w(k) \]

- Substituting \( x(k) \) by \( \hat{x}(k) \)
  \[ \hat{x}(k + 1) = \tilde{A}\hat{x}(k) + \tilde{B}_u u(k) + \tilde{B}_w \hat{w}(k) \]

- Estimated unknown inputs
  \[ \hat{w}(k) = (\tilde{B}_w)^\dagger \left( \hat{x}(k + 1) - \tilde{A}\hat{x}(k) - \tilde{B}_u u(k) \right) \]
Results on 16-Machine System

- 10-th order model for generator
- Six unknown inputs
- Randomly chosen
  \[ B_w \in \mathbb{R}^{160 \times 6} \]
- 12 PMUs are installed at the terminal bus of generator 1, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, and 16

\[
\begin{align*}
w_1(t) &= k_1 \left( \cos(\psi_1 t) + e^{-2t} + \max \left(0, 1 - \frac{|t-5|}{3}\right) \right) \\
w_2(t) &= k_1 \sin(\psi_1 t) \\
w_3(t) &= k_1 \cos(\psi_1 t) \\
w_4(t) &= k_2 \text{square}(\psi_2 t) \\
w_5(t) &= k_2 \text{sawtooth}(\psi_2 t) \\
w_6(t) &= k_2 \left( \sin(\psi_2 t) + e^{-5t} \right)
\end{align*}
\]
Nonlinear Observer/Estimator

\[
\begin{aligned}
    \dot{x} &= Ax + Bu + \phi(x) \\
    y &= h(x)
\end{aligned}
\]

- **Assumptions**
  - *One-sided Lipschitz condition*
    \[
    \langle \phi(x_1) - \phi(x_2), x_1 - x_2 \rangle \leq \rho \|x_1 - x_2\|^2
    \]
  - *Quadratically inner-bounded*
    \[
    (\phi(x_1) - \phi(x_2))^\top (\phi(x_1) - \phi(x_2)) \leq \mu \|x_1 - x_2\|^2 \\
    + \varphi \langle \phi(x_1) - \phi(x_2), x_1 - x_2 \rangle
    \]

Select parameters $\rho$, $\mu$, $\varphi$ to satisfy the conditions
Nonlinear Observer, cont’d

- Observer dynamics

\[ \dot{x} = A\dot{x} + Bu + \phi(\hat{x}) + L(y - C\hat{x}) \quad (*) \]

  - Measurement function is linearized
  - Key is to design the gain matrix \( L \)

*Theorem [Zhang2012]:* The observer is asymptotically stable if there exist scalars \( \epsilon_1, \epsilon_2, \sigma > 0 \) such that the following Riccati inequality has a symmetric positive definite solution \( P \)

\[ A^T P + PA + (\epsilon_1 \rho + \epsilon_2 \delta) I + \frac{1}{\epsilon_2} \left( P + \frac{\phi \epsilon_2 - \epsilon_1}{2} I \right)^2 - \sigma C^T C < 0 \]
Nonlinear Observer Design

**Algorithm** Observer Design Algorithm

*compute* constants $\rho, \mu,$ and $\varphi$ via an offline search algorithm

*solve* this LMI for $\epsilon_1, \epsilon_2, \sigma > 0$ and $P = P^T \succ 0$:

$$
\begin{bmatrix}
A^T P + PA + (\epsilon_1 \rho + \epsilon_2 \mu)I_n & -\sigma C^T C \\
-\sigma C^T C & P + \frac{\varphi \epsilon_2 - \epsilon_1}{2} I_n
\end{bmatrix} < 0.
$$

*obtain* the observer design gain matrix $L$:

$$
L = \frac{\sigma}{2} P^{-1} C^T.
$$

*simulate* the observer design given in (*)

$$
\dot{x} = A\hat{x} + Bu + \phi(\hat{x}) + L(y - C\hat{x})
$$

\[
\downarrow
\]

$$
\dot{x} = A\hat{x} + Bu + \phi(\hat{x}) + L(y - h(\hat{x}))
$$
Results on 16-Machine System

- Unknown inputs
  
  \[ w(t) = \begin{bmatrix} 
  0.5 \cos(\omega_u t) \\
  0.5 \sin(\omega_u t) \\
  0.5 \cos(\omega_u t) \\
  0.5 \sin(\omega_u t) \\
  -e^{-5t} \\
  0.2 e^{-t} \cos(\omega_u t) \\
  0.2 \cos(\omega_u t) \\
  0.1 \sin(\omega_u t) 
  \end{bmatrix} \]

- Cyber attacks
  - Data integrity:
    Four measurements are scaled by 0.6 and the other four are scaled by 1/0.6
  - Denial of service:
    Loss of measurements
  - Replay attacks:
    Previous measurements

- Unavailable inputs: steady-state values
- We compare with literature’s status quo
Results on 16-Machine System: Comparison with EKF, UKF, SR-UKF

\[ \| \frac{\mathbf{x}(t) - \hat{\mathbf{x}}(t)}{\mathbf{x}(t)} \|_2 \]

Estimation of one compromised measurement
Observer Results: Detection of Attacks

Data integrity attack: four measurements are scaled by 0.6 and the other four are scaled by 1/0.6
Results on 16-Machine System, cont’d

Denial of Service attack: first eight measurements are kept unchanged for $t \in [3 \text{ s}, 6 \text{ s}]$

Replay attack: for first eight measurements
\[ y_i(t) = y_i(t - 3) \] for $t \in [3 \text{ s}, 6 \text{ s}]$
References

Junjian.Qi@ucf.edu || ahmad.taha@utsa.edu || jianhui@mail.smu.edu


