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

Junjian Qi[1], Ahmad Taha[2], Jianhui Wang[3]

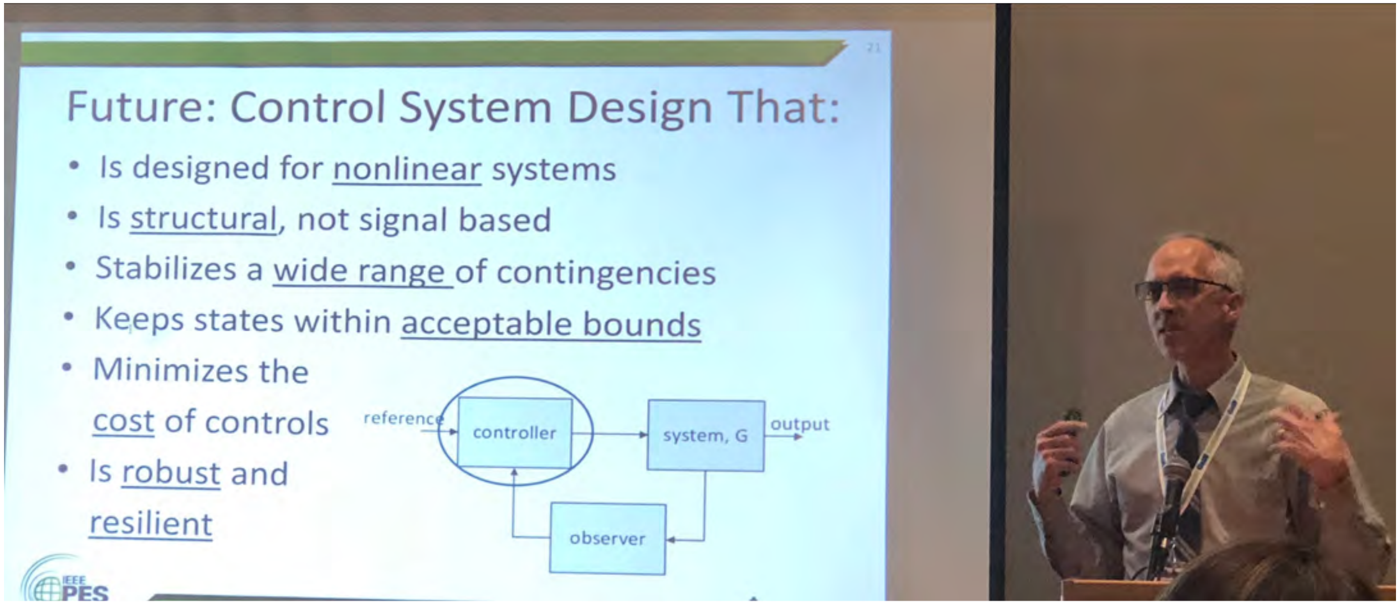
[1]University of Central Florida

[2]The University of Texas at San Antonio

[3]Southern 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:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{u}) \\ \mathbf{y} = \mathbf{h}(\mathbf{x}, \mathbf{u}) \end{cases}$$

- 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 un-modeled 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

$$
\begin{cases}
\dot{\delta}_i = \omega_i - \omega_0 \\
\dot{\omega}_i = \dfrac{\omega_0}{2H_i}\left(T_{\mathrm{m}_i} - T_{\mathrm{e}_i} - \dfrac{K_{\mathrm{D}_i}}{\omega_0}(\omega_i - \omega_0)\right) \\
\dot{e}'_{\mathrm{q}_i} = \dfrac{1}{T'_{\mathrm{d0}_i}}\left(E_{\mathrm{fd}_i} - e'_{\mathrm{q}_i} - (x_{\mathrm{d}_i} - x'_{\mathrm{d}_i})i_{\mathrm{d}_i}\right) \\
\dot{e}'_{\mathrm{d}_i} = \dfrac{1}{T'_{\mathrm{q0}_i}}\left(-e'_{\mathrm{d}_i} + (x_{\mathrm{q}_i} - x'_{\mathrm{q}_i})i_{\mathrm{q}_i}\right) \\
\dot{V}_{\mathrm{R}_i} = \dfrac{1}{T_{\mathrm{A}_i}}(-V_{\mathrm{R}_i} + K_{\mathrm{A}_i}V_{\mathrm{A}_i}) \\
\dot{E}_{\mathrm{fd}_i} = \dfrac{1}{T_{\mathrm{E}_i}}(V_{\mathrm{R}_i} - K_{\mathrm{E}_i}E_{\mathrm{fd}_i} - S_{\mathrm{E}_i}) \\
\dot{R}_{f_i} = \dfrac{1}{T_{F_i}}(-R_{f_i} + E_{fd_i}) \\
\dot{tg}_{1_i} = \dfrac{1}{T_{\mathrm{s}_i}}(D_i - tg_{1_i}) \\
\dot{tg}_{2_i} = \dfrac{1}{T_{\mathrm{c}_i}}\left(\left(1 - \dfrac{T_{3_i}}{T_{\mathrm{c}_i}}\right)tg_{1_i} - tg_{2_i}\right) \\
\dot{tg}_{3_i} = \dfrac{1}{T_{5_i}}\left(\left(\dfrac{T_{3_i}}{T_{\mathrm{c}_i}}tg_{1_i} + tg_{2_i}\right)\left(1 - \dfrac{T_{4_i}}{T_{5_i}}\right) - tg_{3_i}\right)
\end{cases}
$$

$$
\begin{cases}
\dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}) \\
\boldsymbol{y}_q(t) = \boldsymbol{h}(\boldsymbol{x})
\end{cases}
$$

Linearize

$$
\begin{cases}
\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\,\boldsymbol{x}(t) \\
\boldsymbol{y}_q(t) = \boldsymbol{C}_q\,\boldsymbol{x}(t)
\end{cases}
$$

Observer for Linearized System, cont'd

$$\begin{cases} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\,\boldsymbol{x}(t) \\ \boldsymbol{y}_q(t) &= \boldsymbol{C}_q\,\boldsymbol{x}(t) \end{cases}$$

$$\Downarrow$$

$$\begin{cases} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\boldsymbol{x}(t) + \boxed{\boldsymbol{B}_w \boldsymbol{w}(t)} \\ \boldsymbol{y}_q(t) &= \boldsymbol{C}_q \boldsymbol{x}(t) + \boxed{\boldsymbol{v}_q(t)} \end{cases}$$

Unknown inputs

Attack vector

Sliding Mode Observer Design

$$\begin{cases} \dot{\hat{\boldsymbol{x}}}(t) & = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{L}_q(\boldsymbol{y}_q(t) - \hat{\boldsymbol{y}}_q(t)) - \boldsymbol{B}_w \boldsymbol{E}(\hat{\boldsymbol{y}}_q, \boldsymbol{y}_q, \eta) \\ \hat{\boldsymbol{y}}_q(t) = \boldsymbol{C}_q \hat{\boldsymbol{x}}(t) \end{cases}$$

where $\boldsymbol{E}(\cdot) = \begin{cases} \eta \dfrac{\boldsymbol{F}_q(\hat{\boldsymbol{y}}_q - \boldsymbol{y}_q)}{\|\boldsymbol{F}_q(\hat{\boldsymbol{y}}_q - \boldsymbol{y}_q)\|_2 + \nu} & \text{if } \boldsymbol{F}_q(\hat{\boldsymbol{y}}_q - \boldsymbol{y}_q) \neq \boldsymbol{0} \\ \boldsymbol{0} & \text{if } \boldsymbol{F}_q(\hat{\boldsymbol{y}}_q - \boldsymbol{y}_q) = \boldsymbol{0} \end{cases}$

- Design variables: matrices $\boldsymbol{F_q}$, $\boldsymbol{L_q}$
- Good design yields asymptotic convergence of est. error

$$\lim_{t \to \infty} \boldsymbol{e}(t) = \lim_{t \to \infty} \big(\hat{\boldsymbol{x}}(t) - \boldsymbol{x}(t)\big) = \boldsymbol{0}$$

Observer Design: Finding F_q & L_q

- Solve for P, F_q, Y

$$
\begin{aligned}
A^\top P + PA - C_q^\top Y^\top - YC_q &= -Q \\
P &= P^\top \\
F_q C_q &= B_w^\top P
\end{aligned}
$$

- 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:

$$\boldsymbol{x}(k+1) = \tilde{\boldsymbol{A}}\boldsymbol{x}(k) + \tilde{\boldsymbol{B}}_u\boldsymbol{u}(k) + \tilde{\boldsymbol{B}}_w\boldsymbol{w}(k)$$

- Substituting $\boldsymbol{x}(k)$ by $\hat{\boldsymbol{x}}(k)$

$$\hat{\boldsymbol{x}}(k+1) = \tilde{\boldsymbol{A}}\hat{\boldsymbol{x}}(k) + \tilde{\boldsymbol{B}}_u\boldsymbol{u}(k) + \tilde{\boldsymbol{B}}_w\hat{\boldsymbol{w}}(k)$$

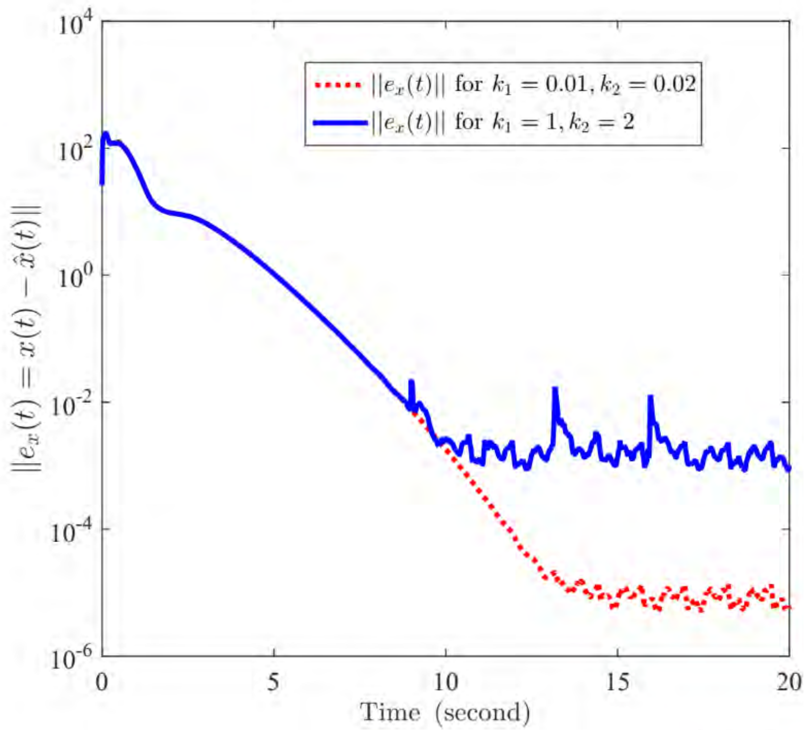
- Estimated unknown inputs

$$\hat{\boldsymbol{w}}(k) = \left(\tilde{\boldsymbol{B}}_w\right)^{\dagger}\left(\hat{\boldsymbol{x}}(k+1) - \tilde{\boldsymbol{A}}\hat{\boldsymbol{x}}(k) - \tilde{\boldsymbol{B}}_u\boldsymbol{u}(k)\right)$$

Results on 16-Machine System

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

$$\boldsymbol{w}(t) = \begin{bmatrix} w_1(t) & = & k_1\left(\cos(\psi_1 t) + e^{-2t} + \max\left(0, 1 - \frac{|t-5|}{3}\right)\right) \\ w_2(t) & = & k_1 \sin(\psi_1 t) \\ w_3(t) & = & k_1 \cos(\psi_1 t) \\ w_4(t) & = & k_2\,\mathrm{square}(\psi_2 t) \\ w_5(t) & = & k_2\,\mathrm{sawtooth}(\psi_2 t) \\ w_6(t) & = & k_2\left(\sin(\psi_2 t) + e^{-5t}\right) \end{bmatrix}$$



Nonlinear Observer/Estimator

$$\begin{cases} \dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} + \boldsymbol{\phi}(\boldsymbol{x}) \\ \boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) \end{cases}$$

- Assumptions
  - *One-sided Lipschitz condition*

$$\langle \boldsymbol{\phi}(\mathbf{x}_1) - \boldsymbol{\phi}(\mathbf{x}_2), \mathbf{x}_1 - \mathbf{x}_2 \rangle \leq \rho \left\| \mathbf{x}_1 - \mathbf{x}_2 \right\|^2$$

  - *Quadratically inner-bounded*

$$\left(\boldsymbol{\phi}(\mathbf{x}_1) - \boldsymbol{\phi}(\mathbf{x}_2) \right)^\top \left(\boldsymbol{\phi}(\mathbf{x}_1) - \boldsymbol{\phi}(\mathbf{x}_2) \right) \leq \mu \left\| \mathbf{x}_1 - \mathbf{x}_2 \right\|^2 + \varphi \langle \boldsymbol{\phi}(\mathbf{x}_1) - \boldsymbol{\phi}(\mathbf{x}_2), \mathbf{x}_1 - \mathbf{x}_2 \rangle$$

Select parameters ρ, μ, φ to satisfy the conditions

Nonlinear Observer, cont'd

- Observer dynamics

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}\mathbf{u} + \phi(\hat{\mathbf{x}}) + \mathbf{L}\big(\mathbf{y} - \mathbf{C}\hat{\mathbf{x}}\big) \quad (*)$$

  – Measurement function is linearized
  – **Key is to design the gain matrix** $\mathbf{L}$

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*

$$A^T P + PA + (\epsilon_1 \rho + \epsilon_2 \delta) I + \frac{1}{\epsilon_2}\Big(P + \frac{\varphi \epsilon_2 - \epsilon_1}{2} I\Big)^2 - \sigma C^T C < 0$$

Nonlinear Observer Design

Algorithm Observer Design Algorithm

compute constants ρ, μ, and φ via an offline search algorithm
solve this LMI for $\epsilon_1, \epsilon_2, \sigma > 0$ and $\mathbf{P} = \mathbf{P}^\top \succ \boldsymbol{O}$:

$$\left[\begin{array}{c|c} \mathbf{A}^\top\mathbf{P} + \mathbf{P}\mathbf{A} + (\epsilon_1\rho + \epsilon_2\mu)\mathbf{I}_n & \\ -\sigma\,\mathbf{C}^\top\mathbf{C} & \mathbf{P} + \dfrac{\varphi\,\epsilon_2 - \epsilon_1}{2}\mathbf{I}_n \\ \hline \left(\mathbf{P} + \dfrac{\varphi\,\epsilon_2 - \epsilon_1}{2}\mathbf{I}_n\right)^\top & -\epsilon_2\mathbf{I}_n \end{array}\right] < 0.$$

obtain the observer design gain matrix $\mathbf{L}$:

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

simulate the observer design given in (*).

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}\mathbf{u} + \phi(\hat{\mathbf{x}}) + \mathbf{L}\big(\mathbf{y} - \boxed{\mathbf{C}\hat{\mathbf{x}}}\big)$$

$$\Downarrow$$

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}\mathbf{u} + \phi(\hat{\mathbf{x}}) + \mathbf{L}\big(\mathbf{y} - \boxed{\mathbf{h}(\hat{\mathbf{x}})}\big)$$

Results on 16-Machine System

- Unknown inputs

$$\mathbf{w}(t) = \begin{bmatrix} 0.5\cos(\omega_u t) \\ 0.5\sin(\omega_u t) \\ 0.5\cos(\omega_u t) \\ 0.5\sin(\omega_u t) \\ -e^{-5t} \\ 0.2\,e^{-t}\cos(\omega_u t) \\ 0.2\cos(\omega_u t) \\ 0.1\sin(\omega_u t) \end{bmatrix}$$

- Unavailable inputs: steady-state values
- We compare with literature's status quo

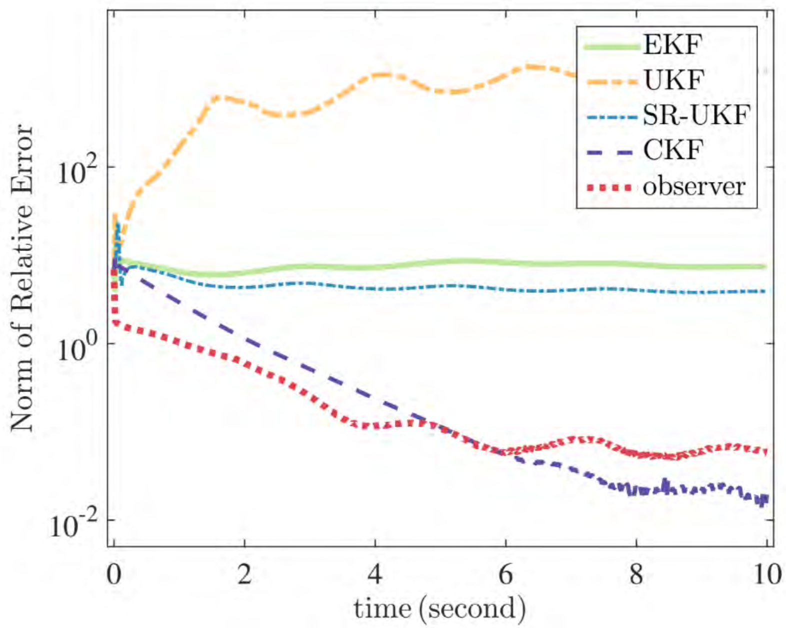
- Cyber attacks
  - *Data integrity*:

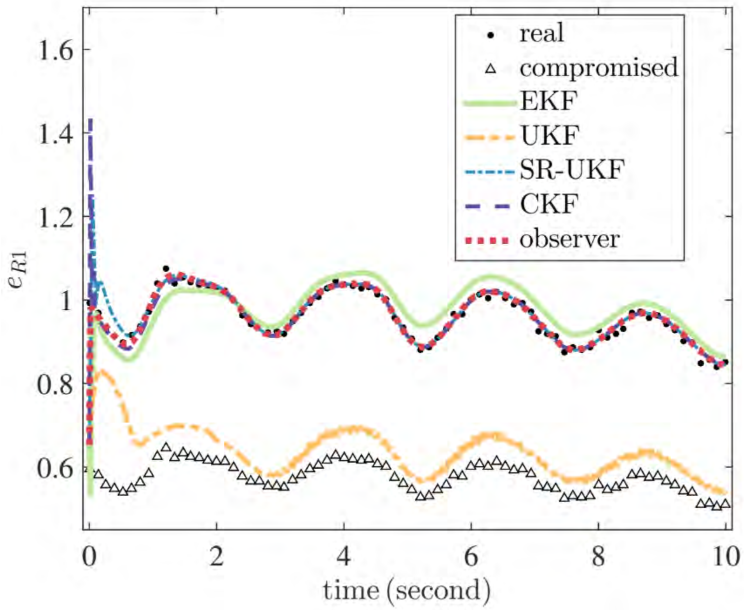
    Four measurements are scaled by 0.6 and the other four are scaled by 1/0.6
  - *Denial of service:*

    Loss of measurements
  - *Replay attacks:*

    Previous measurements

Results on 16-Machine System: Comparison with EKF, UKF, SR-UKF

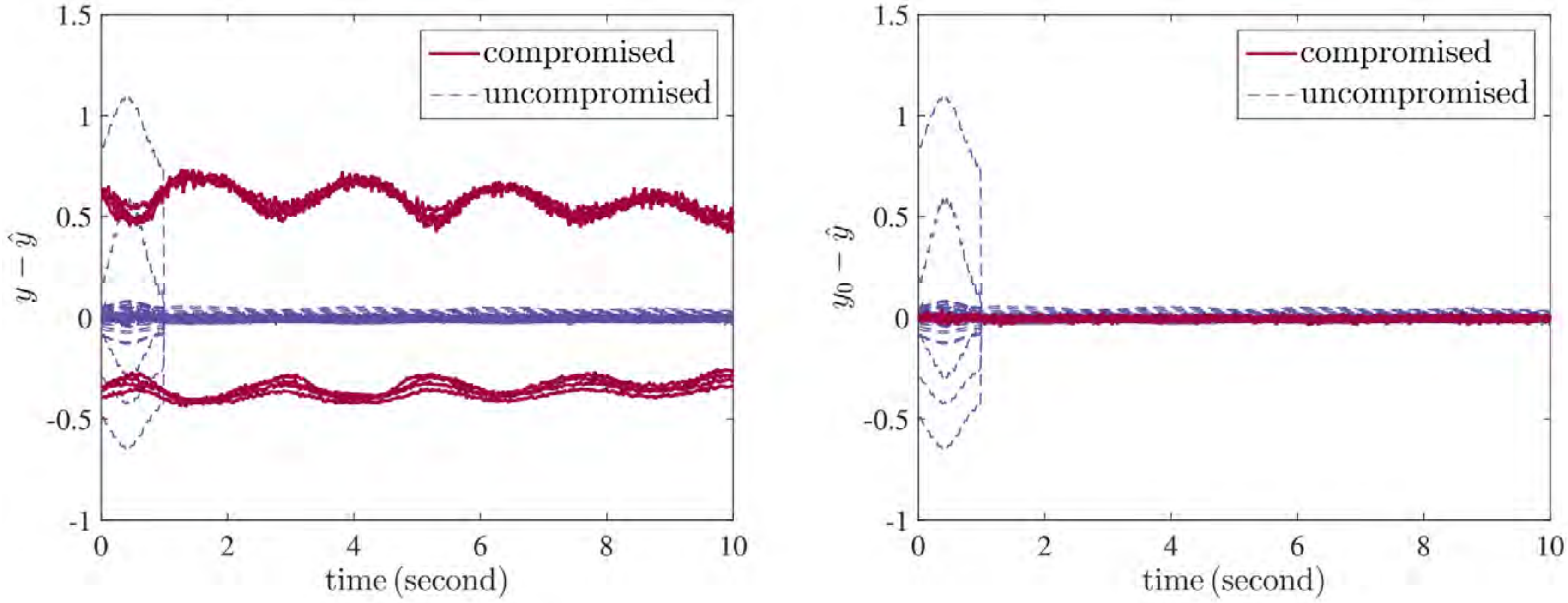




$$||(\mathbf{x}(t) - \hat{\mathbf{x}}(t))/\mathbf{x}(t)||_2$$

Estimation of one compromised measurement

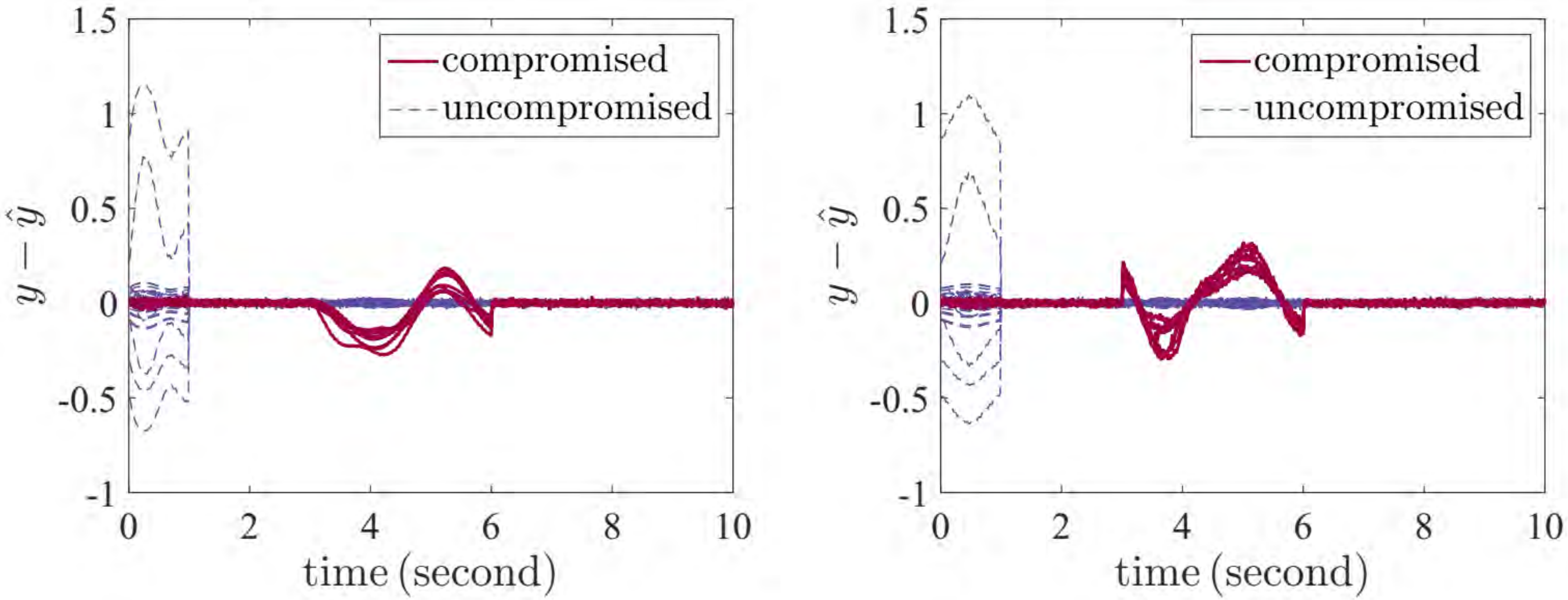
Observer Results: Detection of Attacks



(a) (b)

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



(a)

(b)

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

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

References

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

- J. Qi, A. F. Taha, and J. Wang, "Comparing Kalman Filters and Observers for Power System Dynamic State Estimation with Model Uncertainty and Malicious Cyber Attacks." [Online]: https://arxiv.org/pdf/1605.01030.pdf
- A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 886–899, Mar. 2018.
- J. Qi, K. Sun, J. Wang, and H. Liu, "Dynamic state estimation for multi-machine power system by unscented Kalman filter with enhanced numerical stability," *IEEE Trans. Smart Grid*, vol. 9, no. 2. pp. 1184–1196, Mar. 2018.
- W. Zhang, H. Su, H. Wang, and Z. Han, "Full-order and reduced-dorder observers for one-sided lipschitz nonlinear systems using Riccati equations," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4968–4977, Dec. 2012.

IEEE PES Power & Energy Society IEEE