SAND2022-5062C

Sandia National Laboratories

Exceptional service in the national interest

Detection of False Data Injection Attacks in Power System State Estimation Using Sensor Encoding

Rodrigo D. Trevizan* and Matthew J. Reno

Sandia National Laboratories, Albuqueque, NM

2022 IEEE Kansas Power and Energy Conference

April 25 – 26 2022

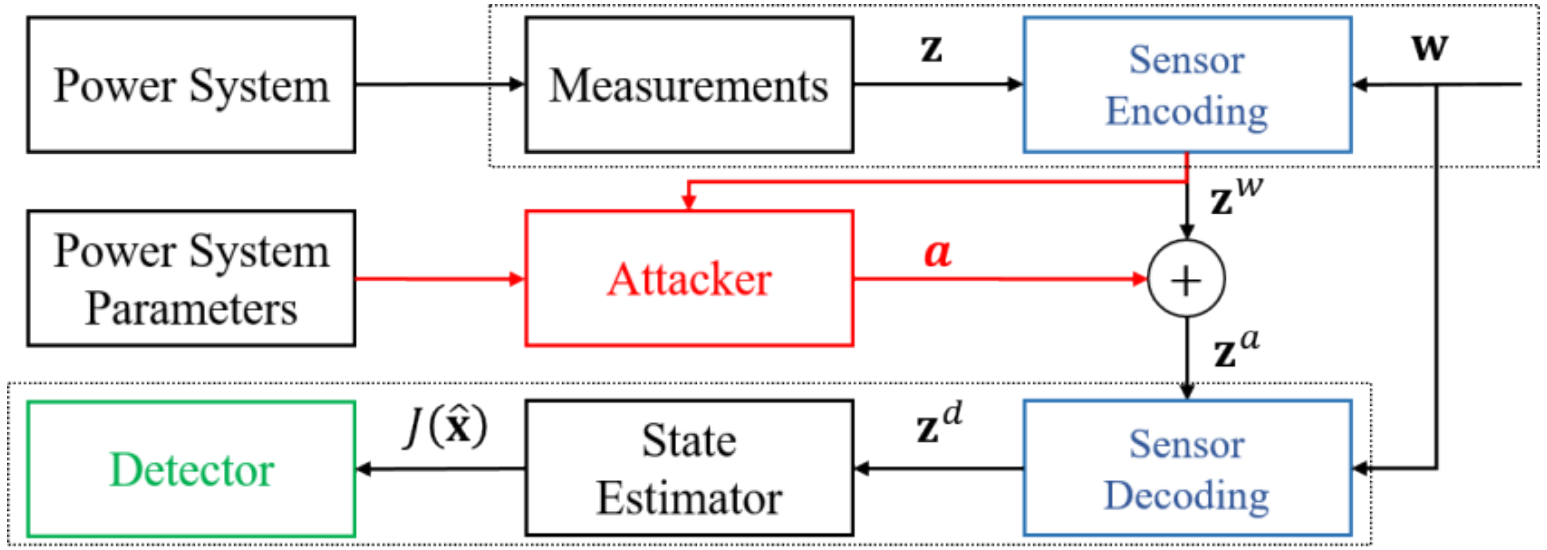
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline

1. Introduction
2. Power System State Estimation (PSSE)
3. Stealthy False Data Attacks on PSSE
4. Sensor Encoding
    1. Naïve Sensor Encoding
    2. Undetectable Sensor Encoding
5. Case Study
6. Results
7. Conclusion
8. Acknowledgment

Introduction

- Smart grids
  - Increased flexibility, cybersecurity risks
- Vulnerable power systems applications†
  - Power system state estimators (PSSEs), automatic generation control, voltage control, energy markets
- Data deception attacks
  - False data injection (FDI)
  - Integrity of measurements
  - Meter or communication level
- This paper:
  - Encoding method



†K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in 2017 IEEE Region 10 Symp. (TENSYMP), July 2017, pp. 1–6.

Power System State Estimation

- Model:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e}$$

  - Measurements: $\mathbf{z}$;
  - States: $\mathbf{x}$;
  - Measurement function: $\mathbf{h}(\mathbf{x})$;
  - Error: $\mathbf{e} \sim \mathcal{N}(\mathbf{0}, \mathbf{R})$;
  - Residuals: $\mathbf{r} = \mathbf{z} - \mathbf{h}(\mathbf{x})$
- Problem: find $\mathbf{x}$ that best fits measurements given a goodness of fit score
  - Weighted least-squares:

$$\min_{\mathbf{x}} J(\mathbf{x}) = \frac{1}{2}[\mathbf{z} - \mathbf{h}(\mathbf{x})]^{\mathrm{T}} \mathbf{R}^{-1}[\mathbf{z} - \mathbf{h}(\mathbf{x})]$$

- Solution using Newton-Raphson iterative algorithm:

$$\hat{\mathbf{x}}_{k+1} = \hat{\mathbf{x}}_k + \left(\mathbf{H}_k^{\mathrm{T}} \mathbf{R}^{-1} \mathbf{H}_k\right)^{-1} \mathbf{H}_k^{\mathrm{T}} \mathbf{R}^{-1}[\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}}_k)]$$

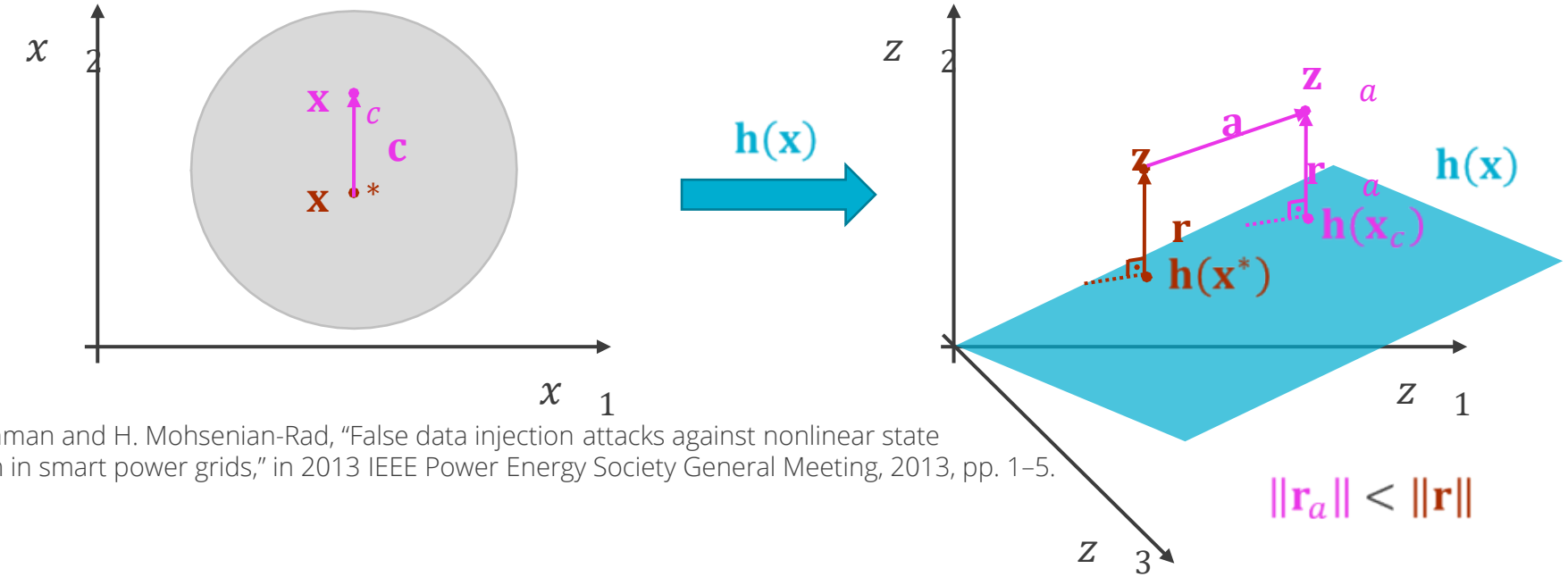
  - $\mathbf{H}_k = \frac{\partial \mathbf{h}(\hat{\mathbf{x}}_k)}{\partial \mathbf{x}}$
- Bad data detection using residual-based approaches like $J(\mathbf{x})$ (a.k.a. chi-squared test χ^2)
  - Detect an attack when $J(\mathbf{x}) > \chi^2_{\nu,\alpha}$

Stealthy False Data Attacks on PSSE

- Goal: circumvent traditional bad data detection approaches
- Sensors are manipulated so that low residual values $\mathbf{r}_a$ are obtained by an estimator
  - False data vector induces a solution of PSSE that is feasible
  - Similar to changing (or corrupting) the observed point of operation

$$\mathbf{x}_c = \mathbf{x}^* + \mathbf{c}$$

$$\mathbf{a} = -\mathbf{H}_c\left(\mathbf{H}_c^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H}_c\right)^{-1}\mathbf{H}_c^{\mathrm{T}}\mathbf{R}^{-1}[\mathbf{z} - \mathbf{h}(\mathbf{x}_c)] + \mathbf{h}(\mathbf{x}_c) - \mathbf{h}(\mathbf{x}^*)^{\ddagger}$$



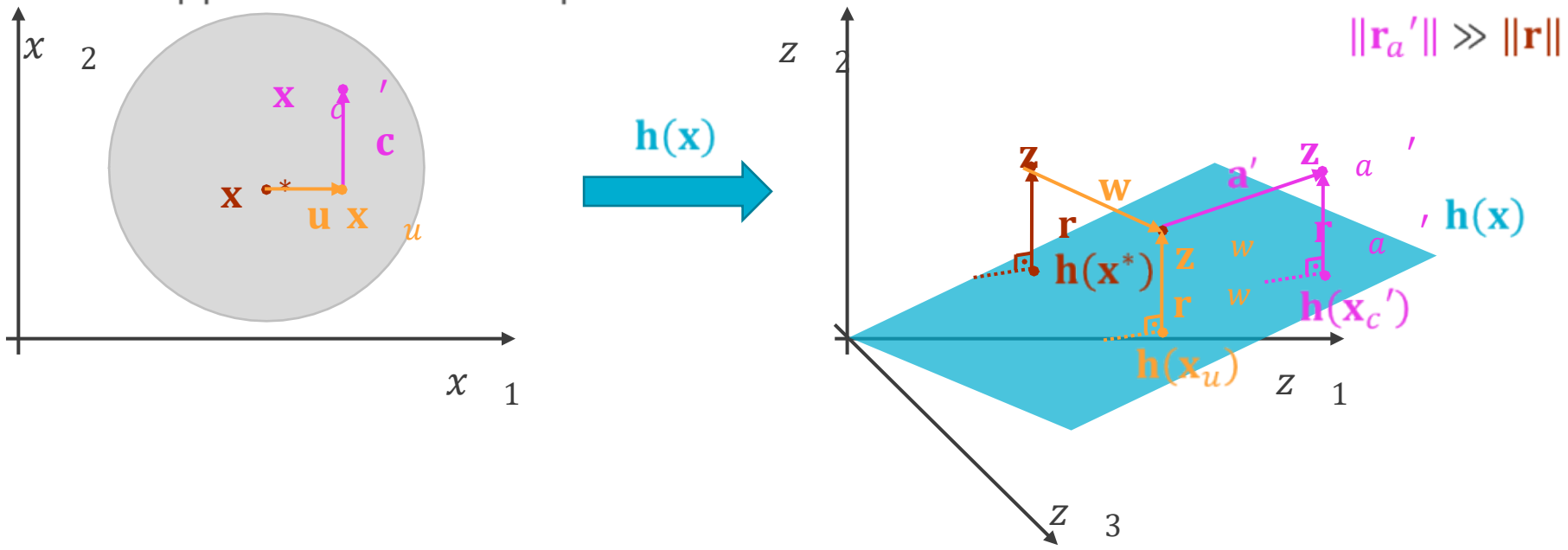
‡ M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in 2013 IEEE Power Energy Society General Meeting, 2013, pp. 1–5.

Sensor Encoding

- Change numerical values of measurements to deceive the attacker and detect the FDI

$$\mathbf{z}^w = \mathbf{f}(\mathbf{z}, \mathbf{w})$$
$$\mathbf{z}^d = \mathbf{g}(\mathbf{z}^w, \mathbf{w})$$

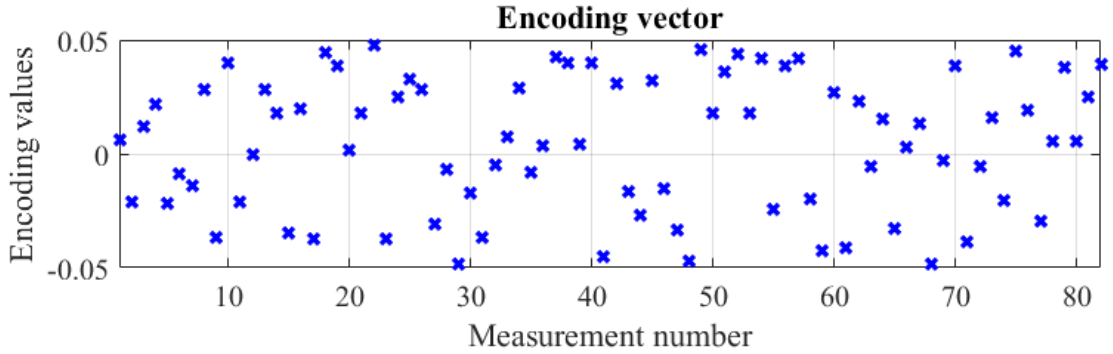
  - Encoding function $\mathbf{f}$;
  - Decoding function $\mathbf{g}$;
  - Secret encoding vector $\mathbf{w}$;
  - Encoded measurement vector $\mathbf{z}^w$;
  - If no attack happens we should expect decoded measurement vector $\mathbf{z}^d = \mathbf{z}$



Naïve Sensor Encoding

- Select a random encoding vector
  - Not too large so it is obvious an encoding vector is being used
  - Not too small so that it will not lead to an FDI detection
  - Defender's $J(\mathbf{x})$ has to produce a large value
  - Drawback: if an attacker uses $J(\mathbf{x})$ detector it will detect the encoding vector

$$\mathbf{z}^w = \mathbf{z} + \mathbf{w}$$
$$\mathbf{z}^d = \mathbf{z}^w - \mathbf{w}$$
$$\mathrm{w}_i \sim \mathcal{U}(-0.05, 0.05)$$



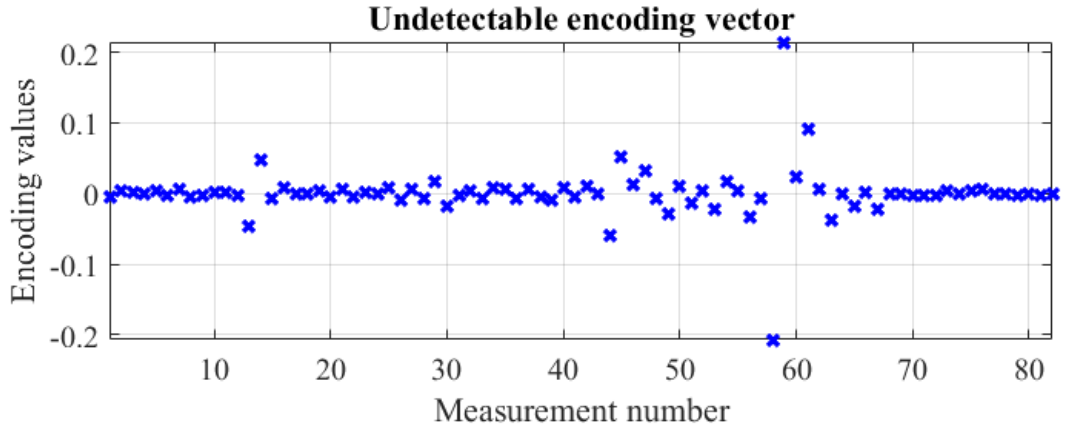
Undetectable Sensor Encoding

- Select an encoding vector that can bypass an attacker's $J(\mathbf{x})$ test
  - Design it using the same approach as a stealthy cyber attack

$$\mathbf{x}_u = \mathbf{x}^* + \mathbf{u}$$
$$\mathbf{z}^w = \mathbf{z} + \mathbf{w}^u$$
$$\mathbf{z}^d = \mathbf{z}^w - \mathbf{w}^u$$

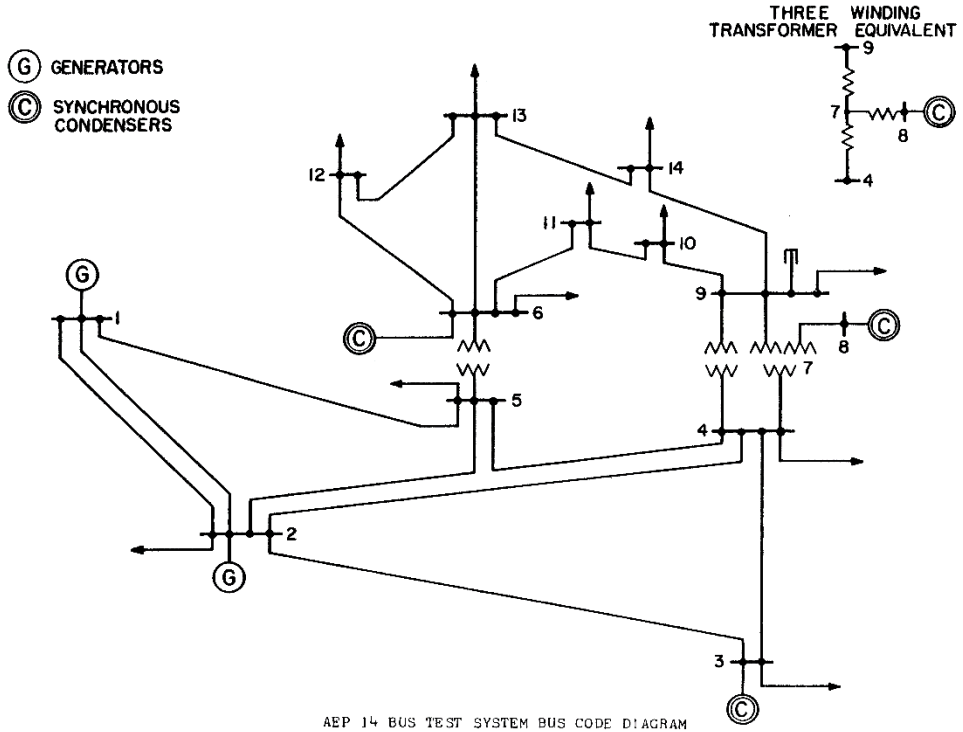
Deviation in state should be large enough so defender's $J(\mathbf{x})$ detects FDI

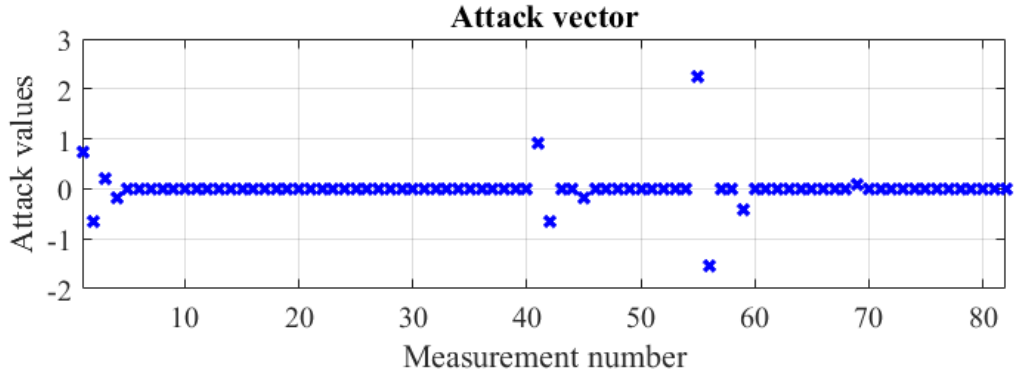
$$u_i \sim \mathcal{U}(-0.1, 0.1)$$

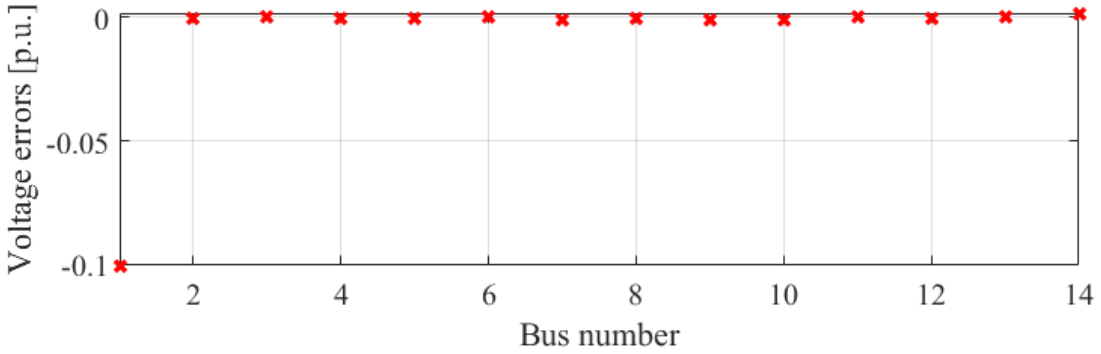


Case Study

- MATPOWER + Matlab
- IEEE 14-bus test system
- 82 measurements, 27 states (GRL-3.03)
- Measurements corrupted by noise
  - 0.01 p.u. for power, 0.001 p.u. for voltage
- Chi-squared test with 99% confidence level
  - $\chi^2_{55,99\%}$=82.29
- Goal of the attacker:
  - Inject a bias of 0.1 p.u. to voltage at bus 1

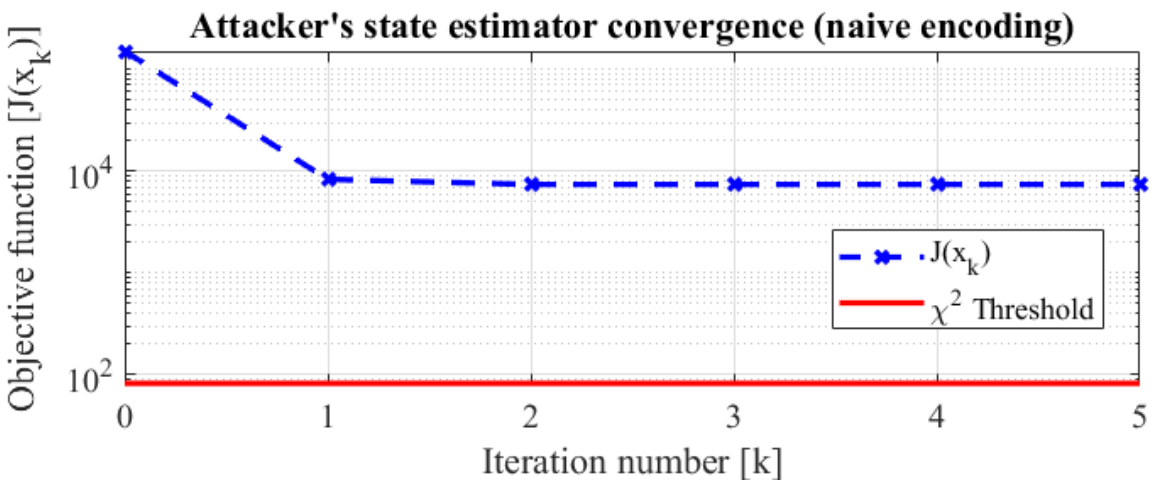


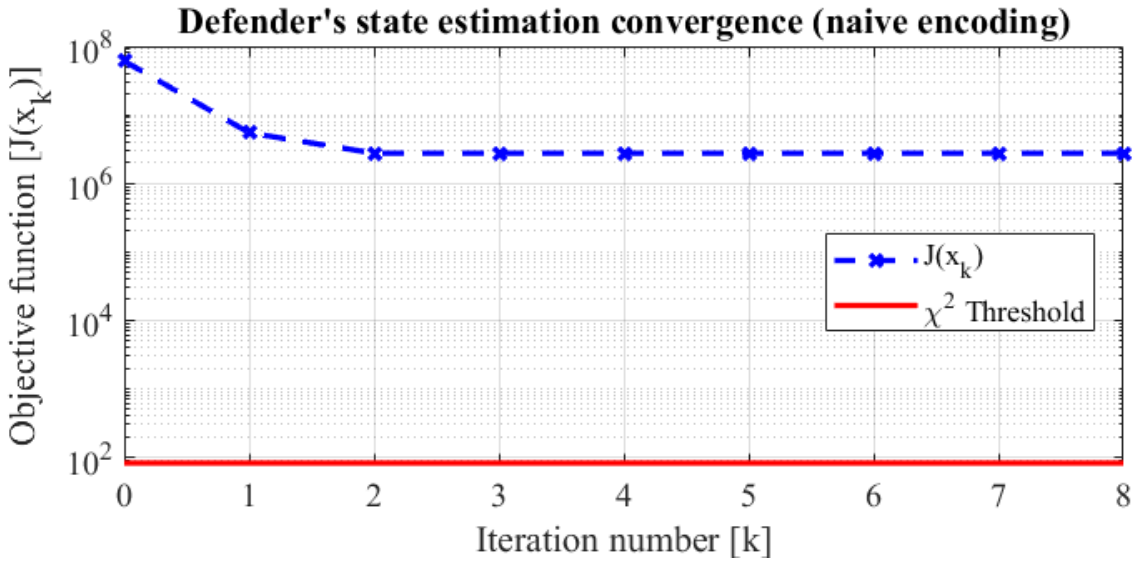




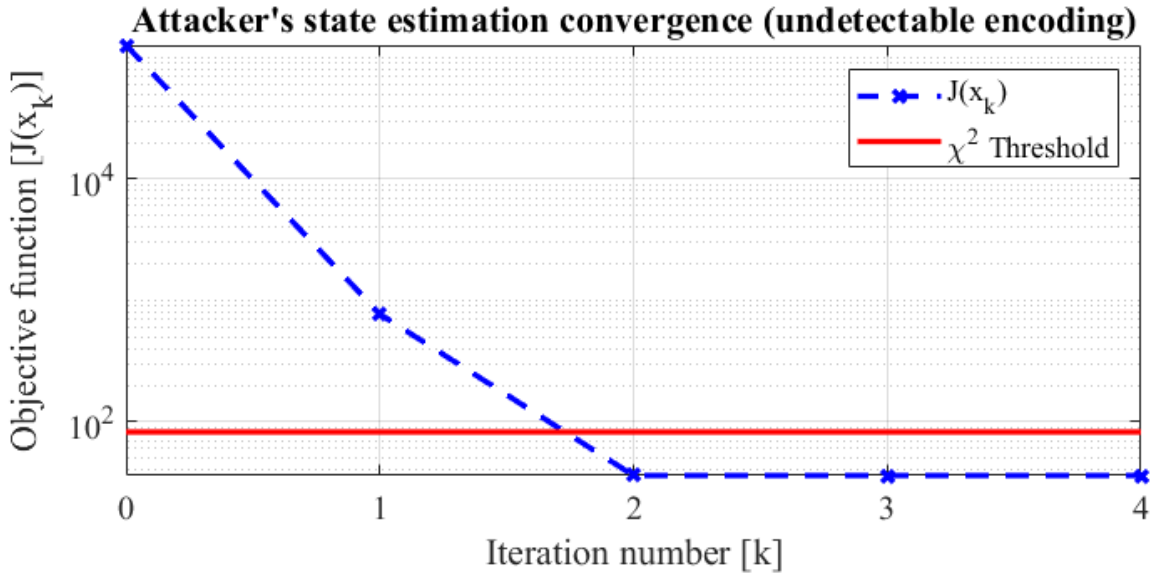
Results

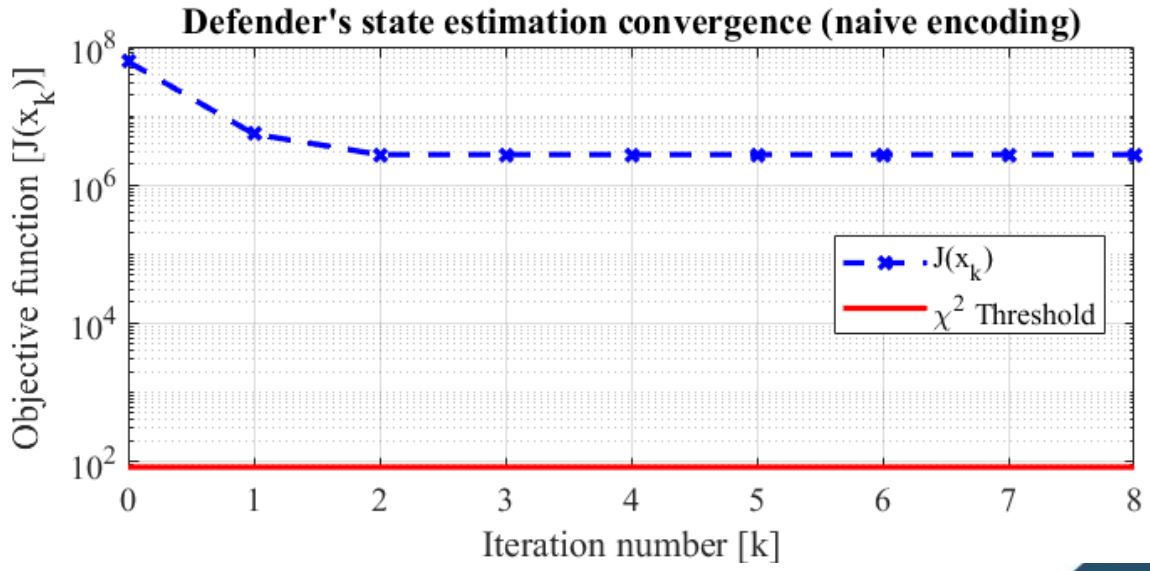
Naïve Sensor Encoding





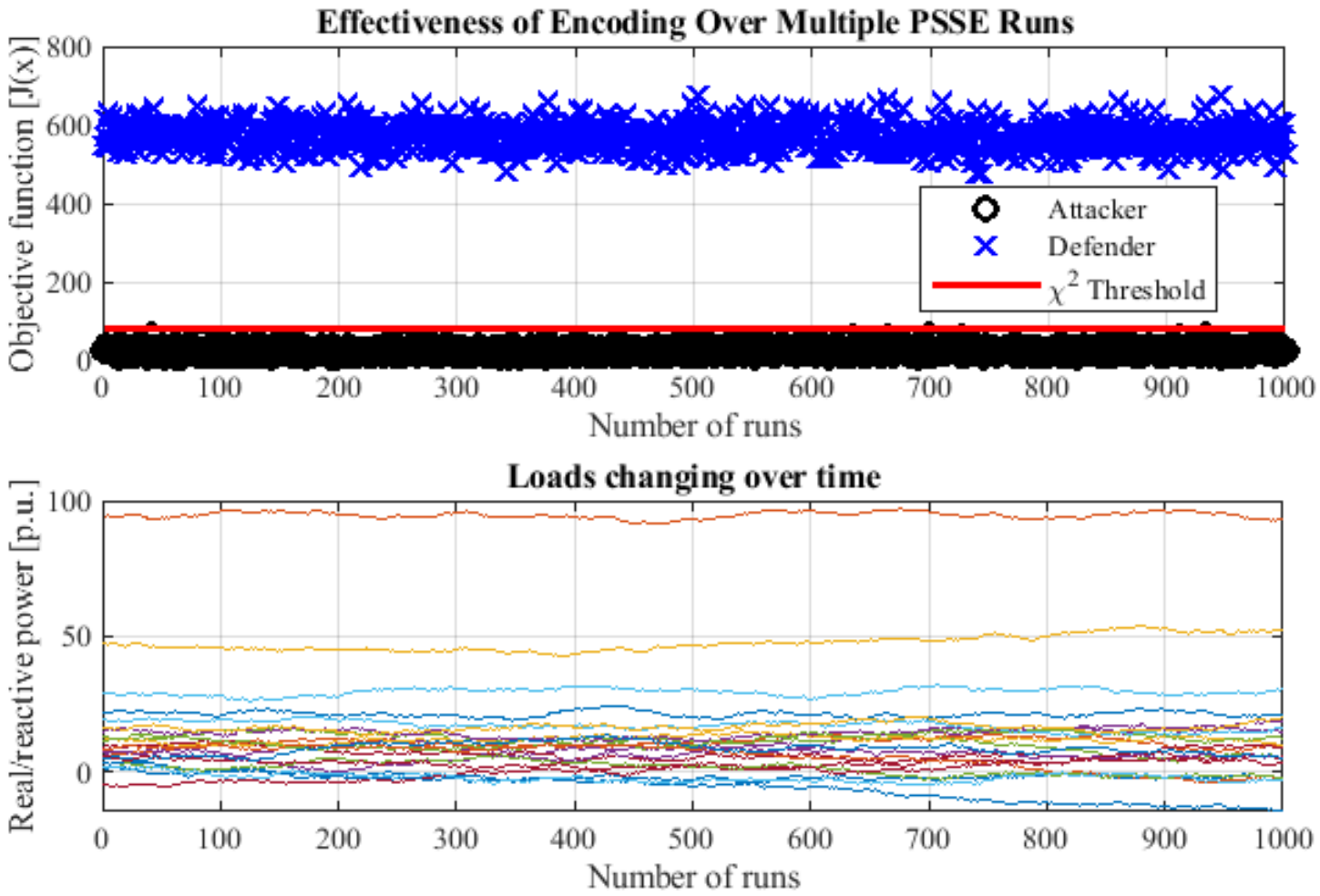
Undetectable Sensor Encoding





Results

Undetectable Sensor Encoding Sensitivity to load



Conclusion

- Two simple methods for defense against FDI attacks on PSSE using sensor encoding
- The encoding vectors induced detection of stealthy FDI cyberattacks on PSSE
- Naïve encoding can be detected by the attacker
  - Does not need any assumption on current system state
- Undetectable encoding cannot be detected by the attacker
  - Requires knowledge of system state at some point in time
- Low-cost method could be applied to PSSEs with minimal intervention
- Following a defense in-depth strategy, could be paired with other cybersecurity controls
  - E.g. communications encryption
- Future work
  - Considerations to practical implementation
  - Enable its application in dynamic PSSE
  - Analysis for design of vectors
  - Constraints on number of encoded measurements

Acknowledgment

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under Solar Energy Technologies Office (SETO) Agreement Number 34226.

Thank you!

Questions?