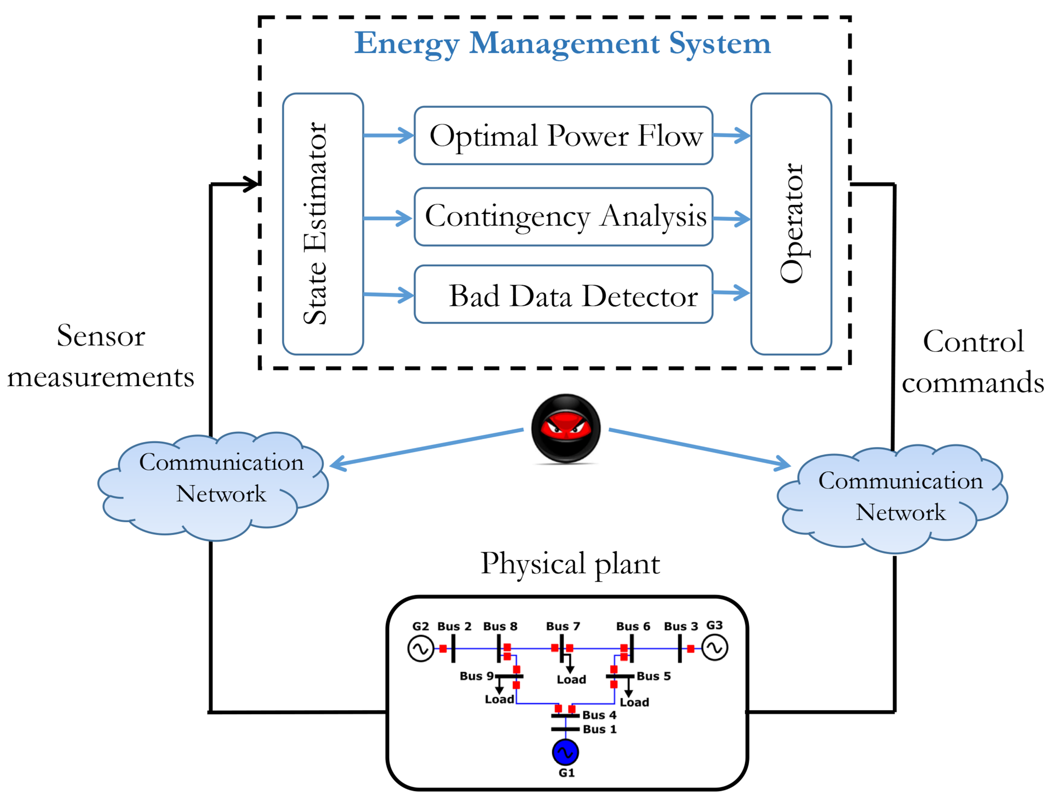
Trade-offs in Data-Driven False Data Injection Attacks Against the Power Grid

Subhash Lakshminarayana[1], Fuxi Wen[2], David K.Y. Yau[1,3],
[1]Advanced Digital Sciences Center, Illinois at Singapore, [2] Chalmers University of Technology, Sweden, [3]Singapore University of Technology and Design

1 Introduction

Focus of This Work

- Constructing undetectable false data injection (FDI) attacks against power grid state estimation [Liu'09]
  - FDI attacks that can bypass the grid's bad-data detector (BDD)
- Attacker can craft undetectable FDI attacks by monitoring the grid's measurement data only [Kim'15]
  - Referred as data-driven undetectable FDI attacks

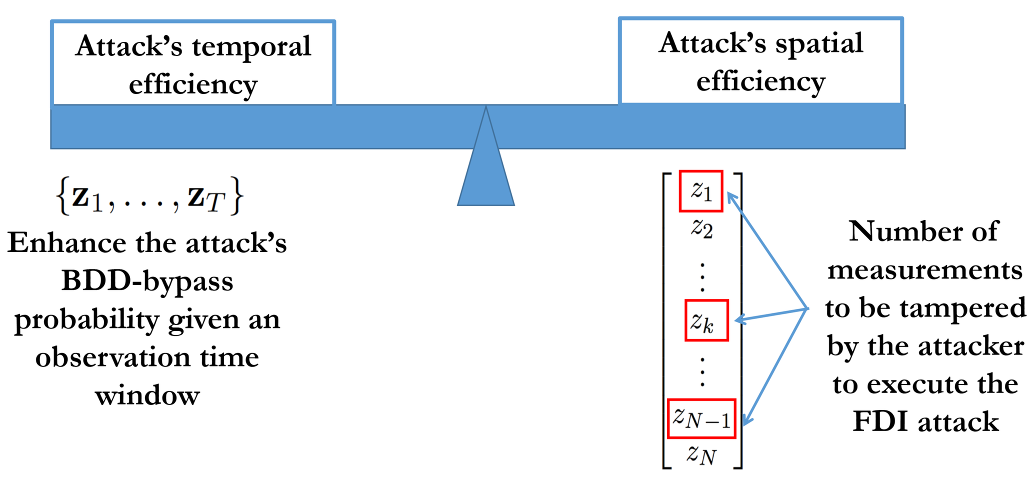


Drawbacks of Existing Work

- The attacker's learning was studied in the setting of a long measurement period (asymptotically infinite) only
- It is important to understand these attacks under a limited measurement time window, due to
  - Active topology control, renewable energy integration
  - Attacker's limited exploitation time window

Our Findings

1. Existing approaches do not perform well when the attacker has a limited number of data samples
   - We design an enhanced algorithm to construct the FDI attacks that can bypass the BDD with a high probability
2. The attacker faces an important trade-off in this regime:



2 System Model

Power Grid Measurement Model

$$\mathbf{z}[t] = \mathbf{H}\theta[t] + \mathbf{n}[t], \quad t = 1, 2, \cdots, T,$$

- $\mathbf{z}[t]$: Power grid measurements at time t (branch power flows, nodal power injections)
- $\boldsymbol{\theta}[t]$: System state (nodal voltage phase angles at time t)
- $\mathbf{H}$: Power grid measurement matrix
- $\mathbf{n}[t]$: Sensor measurement noise
- T : Period of observation
- $\boldsymbol{\Sigma}_z = \mathbb{E}[(\mathbf{z}[t] - \mathbb{E}[\mathbf{z}[t]])(\mathbf{z}[t] - \mathbb{E}[\mathbf{z}[t]])^T]$: Covariance matrix of $\mathbf{z}[t]$

State Estimation and Bad Data Detection

- System state estimate

$$\widehat{\boldsymbol{\theta}}[t] = \left(\mathbf{H}^T\mathbf{W}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}[t]$$

- Power grid bad data detector

$$r_t(\mathbf{z}_t) = ||\mathbf{z}_t - \mathbf{H}_t\widehat{\boldsymbol{\theta}}_t|| = \begin{cases} < \tau, & \text{No alarm,} \\ \geq \tau, & \text{Bad data alarm} \end{cases}$$

Undetectable FDI attack

- FDI attack of the form $\mathbf{a}_t = \mathbf{H}\mathbf{c}_t$ can bypass the power grid's BDD [Liu'09]
  - Attacker requires the knowledge of $\mathbf{H}$
- Alternately, attacker can construct undetectable FDI attack by accessing the grid's measurements

Algorithm for Data-Driven FDI Attack Construction ([Kim'15])

Main Idea: Estimate the basis vectors that span $Col(\mathbf{H})$ (column space of the measurement matrix)

1. Using measurements $\{\mathbf{z}[1], \dots, \mathbf{z}[T]\}$, compute the sample covariance matrix $\widehat{\boldsymbol{\Sigma}}_\mathbf{z}$ as

$$\widehat{\boldsymbol{\Sigma}}_\mathbf{z} = \frac{1}{T-1}\sum_{t=1}^{T}(\mathbf{z}[\mathbf{t}] - \widehat{\mu}_\mathbf{z})(\mathbf{z}[\mathbf{t}] - \widehat{\mu}_\mathbf{z})^T,$$

where $\widehat{\mu}_\mathbf{z} = \frac{1}{T-1}\sum_{t=1}^{T}\mathbf{z}[t]$: sample mean.

2. Perform singular value decomposition (SVD) of $\widehat{\boldsymbol{\Sigma}}_\mathbf{z}$ as

$$\widehat{\boldsymbol{\Sigma}}_\mathbf{z} = \widehat{\mathbf{U}}\widehat{\boldsymbol{\Lambda}}\widehat{\mathbf{V}}^T.$$

3. Let $\widehat{\mathbf{U}}_s$ be the first N columns of $\widehat{\mathbf{U}}$. Construct an undetectable FDI attack vector as $\mathbf{a}[t] = \widehat{\mathbf{U}}_s\mathbf{c}[t]$, where $\mathbf{c}[t] \in \mathbb{R}^N$.

- $\widehat{\boldsymbol{\Sigma}}_\mathbf{z}$ is a consistent estimate of Σ_z asymptotically ($T \to \infty$)
- Estimated singular vectors are well aligned with the basis vectors of $Col(\mathbf{H})$

Drawbacks for Finite Measurement Samples

- For finite T, the estimated basis vectors are inaccurate
- We illustrate this for the IEEE-4 bus system
  - $\delta(\mathbf{u}_i) = \mathbf{u}_i - \widehat{\mathbf{u}}_i$: Estimation accuracy
  - $\mathbf{u}_i$: Basis vector of $Col(\mathbf{H})$
  - $\widehat{\mathbf{u}}_i$: Estimate of the basis vector $\mathbf{u}_i$

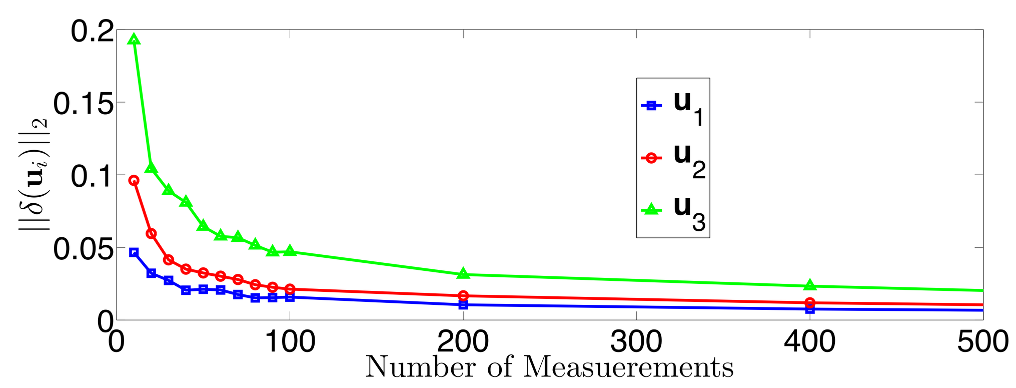


Figure 2: Accuracy of the estimated basis vectors as a function of the number of measurements for an IEEE 4-bus systems.

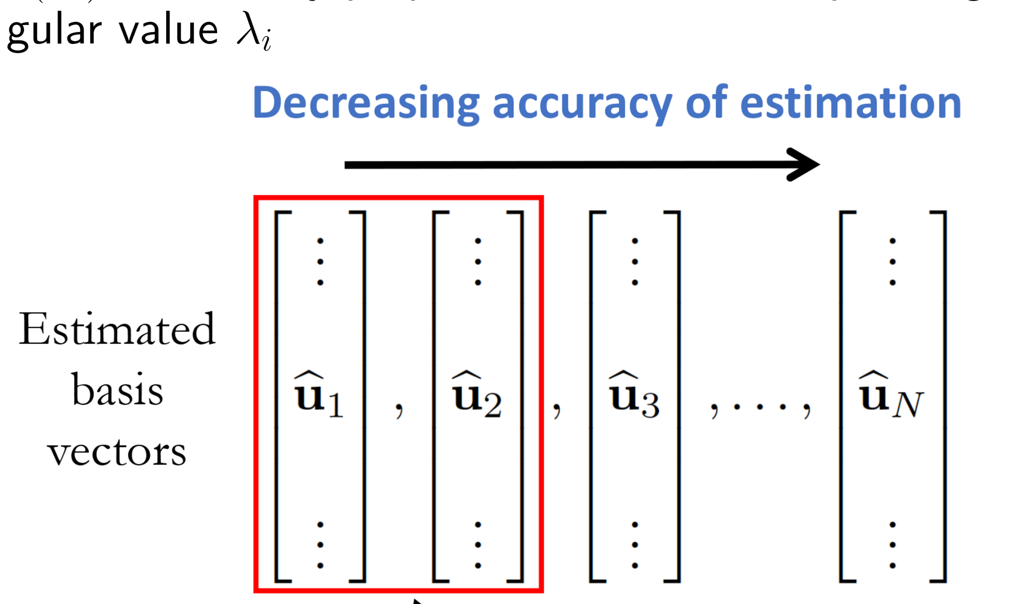
Proposition 1 *For a data-driven FDI attack constructed using the algorithm above with a limited number of measurement samples, $r_a[t] \neq r[t]$. Hence, it violates the condition for an undetectable attack.*

3 Enhanced Algorithm for Data-driven FDI Attacks

- Accuracy of estimation of the basis vectors for finite T

$$\delta(\mathbf{u}_i) \approx \lambda_i^{-1}\mathbf{U}_n\mathbf{U}_n^H\mathbf{N}\mathbf{v}_i, i = 1, \dots, N$$

  - λ_i, $i = 1, \dots, N$: Singular values of matrix Σ_z.
- $\delta(\mathbf{u}_i)$ is inversely proportional to its corresponding singular value λ_i



Restrict the attack vector to a lower-dimensional subspace spanned by the accurately estimated basis vectors

- These column vectors are well aligned with the basis vectors of the targeted subspace $Col(\mathbf{H})$.

Restricting K will increase the attack's BDD-bypass probability
$\implies$ Attack is more efficient temporally

4 Trade-offs in Data-Driven FDI Attacks

- A resource-constrained attacker's objective
  - Minimize the number of meters that must be compromised to execute the attack

$\implies$ Maximize the attack vector's sparsity

$$S_K^* = \min_{\mathbf{c}} ||\widehat{\mathbf{U}}_{s,[1:K]}\mathbf{c}||_0, \text{ s.t. } ||\mathbf{c}||_\infty \geq \tau,$$

- $\widehat{\mathbf{U}}_{s,[1:K]}$: The matrix with the first $K(\leq N)$ columns of $\widehat{\mathbf{U}}_s$
- S_K^* : Sparsest attack vector while restricting the attack to $Col(\widehat{\mathbf{U}}_{s,[1:K]})$

Restricting K will decrease the attack's sparsity
$\implies$ Attack is less efficient spatially

5 Results & Conclusions

- We consider the IEEE-14 bus system
- We use the MATPOWER simulator
- System states are derived from real-world load data trace in New York state (NYISO)

Attack's BDD-bypass probability

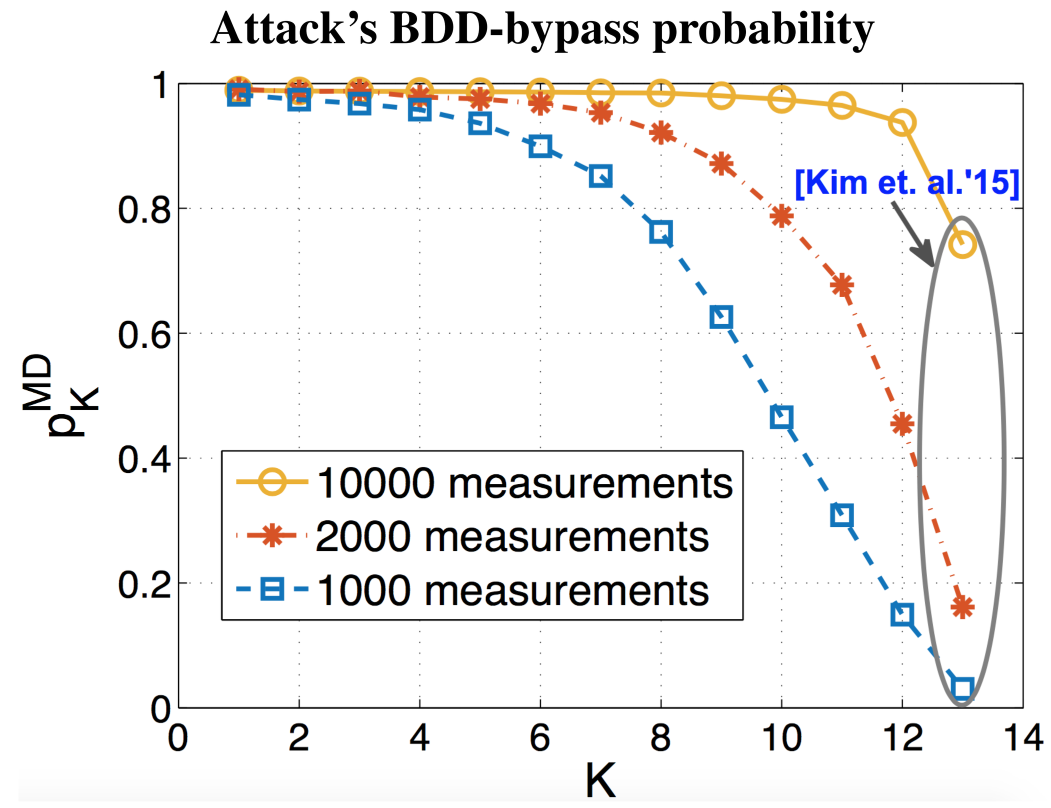


Figure 3: BDD-bypass probability versus the number of estimated basis vectors used in the construction of the FDI attack for IEEE 14-bus system.

Attack's BDD-bypass probability is significantly enhanced following the proposed approach

Attacker's Trade-off

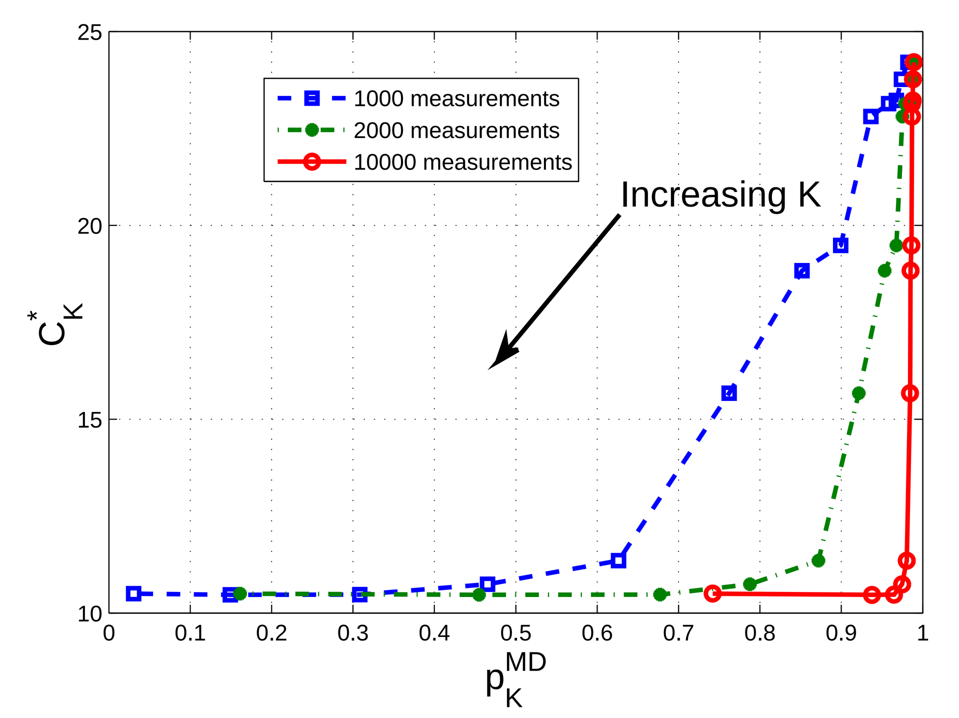


Figure 4: Trade-off between the number of compromised sensors required to construct sparse FDI attacks and the probability of bypassing the BDD.

The trade-off curve gives practical guidance to a resource-constrained attacker in designing stealthy FDI attacks

6 References

1. [Liu'09] - Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. ACM CCS, 2009, pp. 21–32.
2. [Kim'15] - J.Kim, L.Tong, and R.J.Thomas,"Subspace methods for data attack on state estimation: A data driven approach," IEEE Trans. on Signal Processing, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.