UNIVERSITY OF WYOMING

NASPI Work Group Meeting
March 23-24,2015
San Francisco, CA

GPS-Spoofed Synchrophasor Data Correction for State Estimation

Xiaoyuan Fan[1], Dongliang Duan[1], and Liang Du[2]
1. Department of Electrical and Computer Engineering
University of Wyoming, Laramie, WY, USA
2. Schlumberger, Sugar Land, TX, USA
Email: xfan3@uwyo.edu, dduan@uwyo.edu, ldu3@slb.com

Outline

- Introduction
- Challenges for Synchrophasor Data: GPS Spoofing Attack
- GPS-Spoofed Synchrophasor Data Correction
- Summary and Future Work

Phasor Representation for Power System

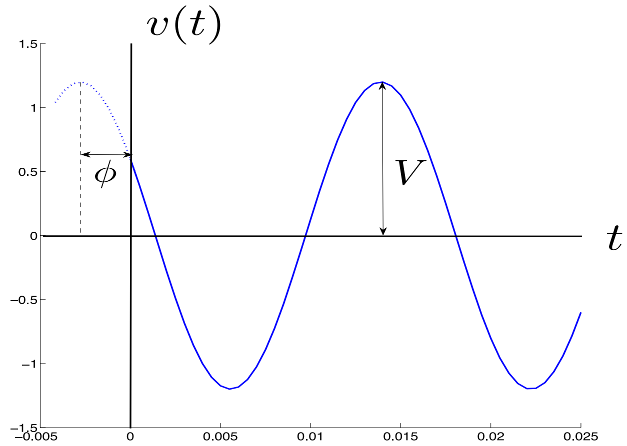
Power system signal:

$$v(t) = |V| \cos(2\pi f_0 t + \phi)$$

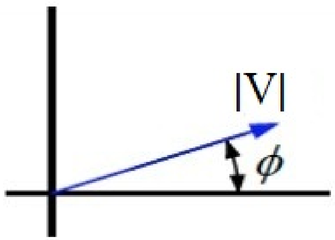
f_0 : fundamental frequency, 60 Hz in U. S.

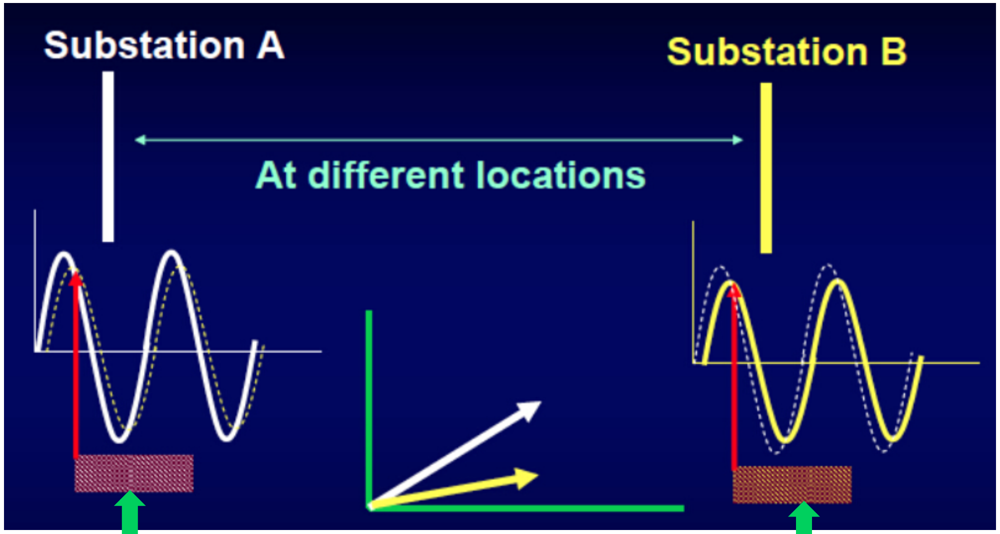
$|V|$: voltage amplitude

ϕ : voltage phase



Phasor: $\mathbf{V} = |V| e^{j\phi}$

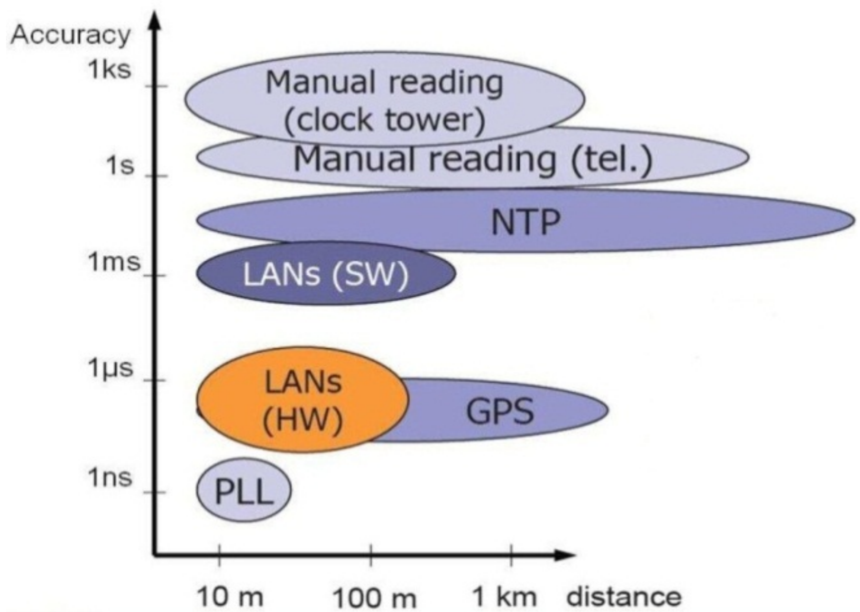


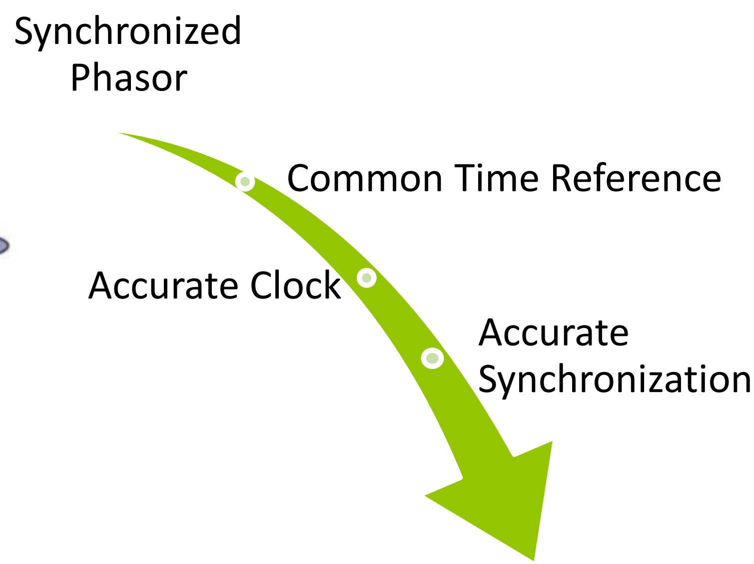


Synchrophasor: Need a common time reference

Time Synchronization for PMU

- PMU will be deployed in a huge geographical area.





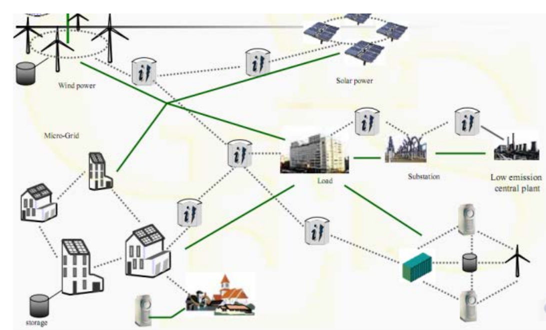
GPS is the best choice.

- GPS signal is received once per second;
- Time tagging accuracy better than 1µs ⟺ 0.02° in phase.

PMU versus SCADA

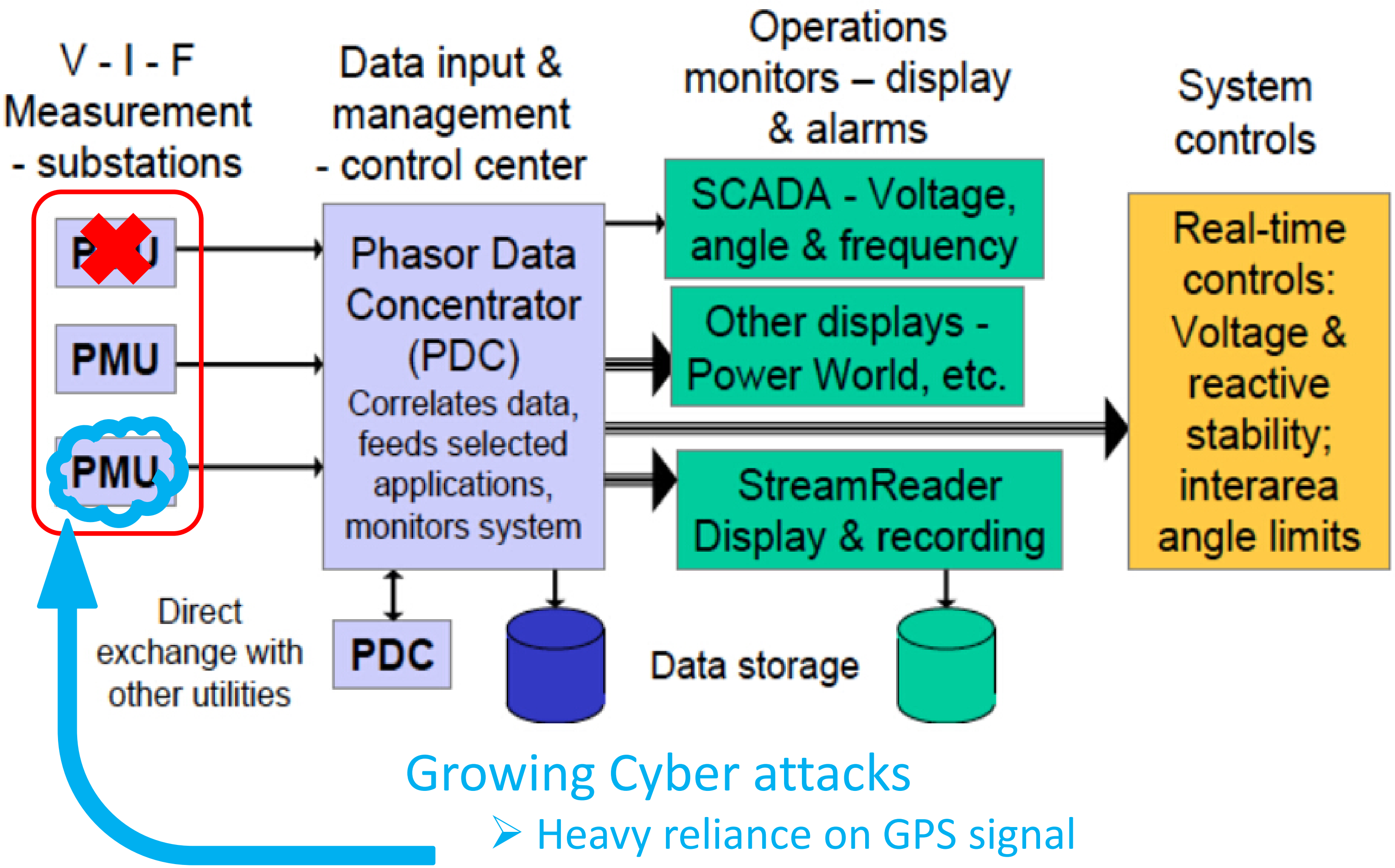
	SCADA	PMU
measurements	power, voltage, current *magnitude*	voltage & current *phasors*, frequency (derivative)
meas. model	non-linear	linear
reporting rate	one every 1-4 sec	30-60/sec
wide-area sync	poor (~1 sec)	precise (~1 μs)

"It's like going from an X-ray to an MRI of the grid," Terry Boston, PJM CEO



A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and their Applications*, Springer, 2008.

PMU Measurement Example



Growing Cyber attacks

- Heavy reliance on GPS signal
- Network connection

[Dr. Anurag K.S., WSU]

Challenges for PMU

- Only civilian GPS signal available
  - Publicly known, easy to predict
  - Subject to GPS Spoofing Attack (GSA)
- GSA on PMU
  - Field tests from Northrop Grumman Information Systems and University of Texas Radio Navigation Laboratory on Dec. 2012
  - Inexpensive hardware
  - Mobile attack in certain distance (~ hundreds of meters)
  - ✗ No warning for the spoofed data from PMU ⇒ Reliability and security of power system is endangered !!!
- Solution
  - ✓ Spoofed PMU data must be detected, corrected or removed.

Impact of GSA on Synchrophasor Data

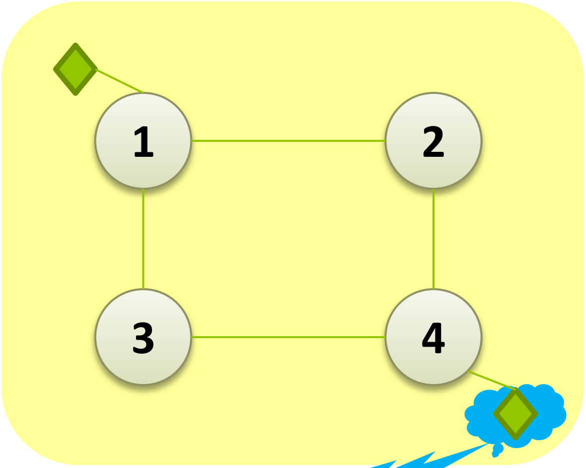
- Presence of GSA ⇨ synchronization is lost
  - Timestamps on these data are compromised
  - Mismatch b/w the measured phasor & the true phasor
  - Equivalent to a phase error on these synchrophasor measurements
- Mathematically,

$$V_{spf} = V_{true} \times e^{j\theta_{spf}}$$
$$I_{spf} = I_{true} \times e^{j\theta_{spf}}$$

where θ_{spf} is the spoofed phase shift from GSA.

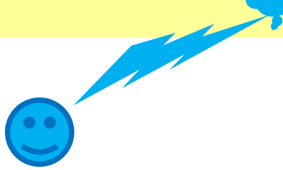
Impact of GSA on State Estimation (SE)

- Example: 4-bus benchmark system
- PMU installed on bus 1 and bus 4
- GSA information: (4, 0.1π)
- PMU data: $V_1, I_{12}, I_{13}, V_4, I_{42}, I_{43}$



GSA's Impact on State Estimation

Estimated State	SE Error, no GSA		SE Error, under GSA	
	Mag.(%)	Pha. (deg.)	Mag.(%)	Pha.(deg.)
S1	0.2909	0.2168	1.0180	-8.4112
S2	0.3141	0.2106	1.3210	-8.7127
S3	0.1297	0.4136	1.1834	-8.7018
S4	0.1491	0.4232	1.6222	-8.5204



Inaccurate state estimation

↓

Unreliable further application

Correction vs. Removal?

- GSA can be denoted by (location, spoofed phase shift)
- One PMU has multiple measurements
- Measurements from same GSA location are affected by the same θ_{spf}

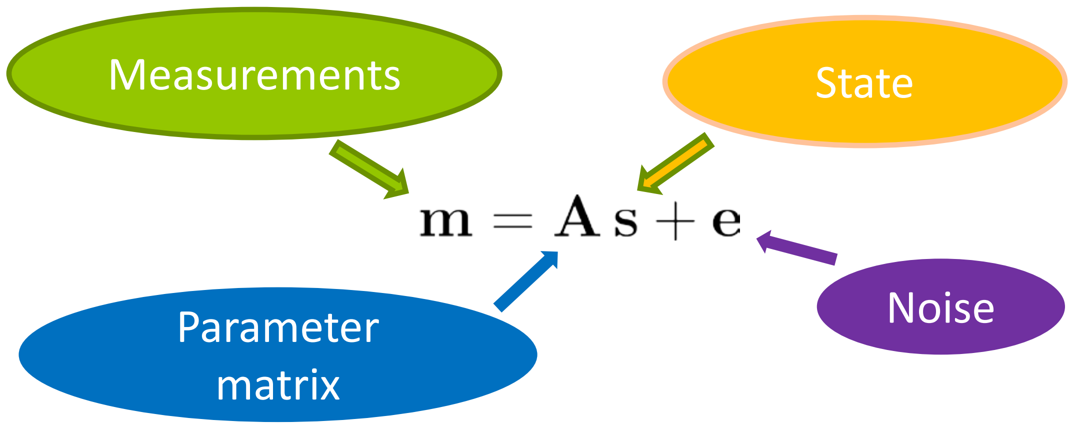
6 initial measurements	GSA location known		GSA location unknown	
	Correction	Removal	Correction	Removal
# of unknown states	4	4	4	4
# of GSA parameter	1	0	2	1
GSA Localization	6>4+1 OK	6>4 OK	6=4+2 OK	6>4+1 OK
# of remains for SE	6	6-3=3	6	6-3=3
Conclusion	better	Not applicable	OK	Not applicable

Conclusion: Correction is preferable for more accurate result.

PMU-based SE Model

- A linear model for static state estimation with synchrophasor data from *p* PMUs installed in power system

$$\begin{pmatrix} \boldsymbol{m}_1 \\ \boldsymbol{m}_2 \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix} = \begin{pmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \\ \vdots \\ \boldsymbol{A}_p \end{pmatrix} \boldsymbol{s} + \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \\ \vdots \\ \boldsymbol{e}_p \end{pmatrix}$$



where $\boldsymbol{A}_i$ can be obtained from grid structure and transmission line parameters.

PMU-based SE Model under GSA

- Assume GSA is on the *k*-th PMU with θ_{spf}

$$\boldsymbol{m}_{spf} = \boldsymbol{G} \cdot \boldsymbol{m} = \begin{pmatrix} \boldsymbol{I}_1 & \dots & 0 & \dots & 0 \\ 0 & \ddots & 0 & \dots & 0 \\ \vdots & \vdots & \boldsymbol{I}_k e^{j\theta_{spf}} & \vdots & \vdots \\ 0 & \dots & 0 & \ddots & 0 \\ 0 & \dots & 0 & \dots & \boldsymbol{I}_p \end{pmatrix} \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_k \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix} = \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_k e^{j\theta_{spf}} \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix}$$

Intuition for Correction

- Two unknowns for single GSA
  - Location k & Spoofed phase shift θ_{spf}
- (1) If location k is known, only need to find the best $\hat{\theta}_{spf}$

$$\hat{\theta}_{spf} = \arg\min_{\theta_{spf}} J(k, \theta_{spf})$$

- (2) If both are unknown
  - Enumerate all possible locations in bus index set
    - $i \neq k$, → adding GSA to another location → larger $J(k, \theta_{spf})$
    - $i = k$, → identifying the correct location → smaller $J(k, \theta_{spf})$
  - Find the best $\hat{k}$ and $\hat{\theta}_{spf}$

$$(\hat{k}, \hat{\theta}_{\hat{k},spf}) = \arg\min_{k,\theta_{spf}} J(k, \theta_{spf})$$

Cost Function J(k,θ_{spf})

- Best Linear Unbiased Estimator (BLUE)

$$\hat{\boldsymbol{s}}_{spf} = (\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{m}_{spf}$$

- Spoofed SE Correction

$$\hat{\boldsymbol{m}}_{true} = \hat{\boldsymbol{G}}^{\mathcal{H}}\boldsymbol{m}_{spf}$$

Residual Sensitivity Matrix

- Estimation residual with correction

$$\boldsymbol{r}_{est} = \hat{\boldsymbol{m}}_{true} - \boldsymbol{A}\hat{\boldsymbol{s}}_{true} = [\boldsymbol{I} - \boldsymbol{A}(\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}]\hat{\boldsymbol{G}}^{\mathcal{H}}\boldsymbol{m}_{spf}$$

- Cost function $J(k,\theta_{spf})$

$$J(k,\theta_{spf}) = \|\boldsymbol{r}_{est}(k,\theta_{spf})\|_2$$

GPS-spoofed Synchrophasor Data Correction

- Spoofing-Matched (SpM) Algorithm
  - Step 1: Estimate the GSA phase shift $\hat{\theta}_{spf}$

$$\hat{\theta}_{k,spf} = \arg \min_{\theta_{spf} \in [0, 2\pi]} \|\boldsymbol{r}_{est}(k, \theta_{spf})\|_2 \, \forall k \in \{0, 1, \ldots, p\}$$

  - Step 2: Identify the GSA location

$$\hat{k} = \arg \min_{k \in \{0,1,\ldots,p\}} \|\boldsymbol{r}_{est}(k, \hat{\theta}_{k,spf})\|_2$$

  - Step 3: Correct the spoofed data & recover true state

$$\hat{\boldsymbol{m}}_{true} = \hat{\boldsymbol{G}}^{\mathcal{H}}(\hat{k}, \hat{\theta}_{\hat{k},spf}) \cdot \boldsymbol{m}_{spf}$$

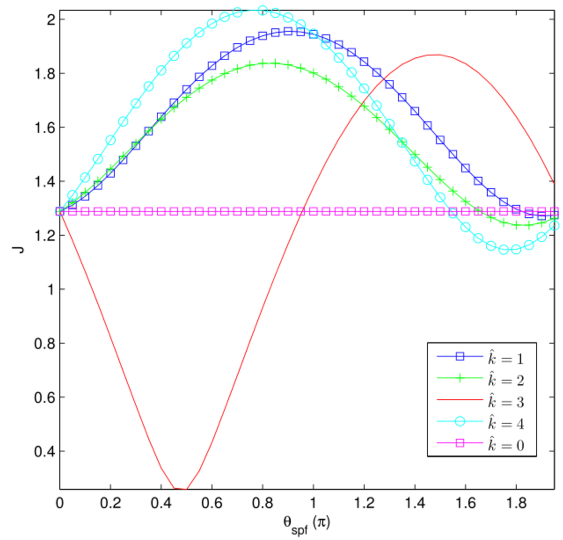
$$\hat{\boldsymbol{s}}_{true} = (\boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \boldsymbol{A})^{-1} \boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \hat{\boldsymbol{m}}_{true}$$

GPS-spoofed Synchrophasor Data Correction

- Performance preview for SpM algorithm with grid search
  - Linear with the total number of PMUs
  - Linear with the inverse of grid search precision
  - Constant residual sensitivity matrix

$$\boldsymbol{Y} = \boldsymbol{I} - \boldsymbol{A}(\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}$$

- Improved SpM algorithm
  - Better searching technique for Step 1
    - ✗ First order derivative test
    - ✗ Iterative methods
    - ✓ Golden Section search technique
      - ❖ Fast convergence
      - ❖ High accuracy



Simulation Setup

- IEEE 14-, 30-, 57-bus benchmark systems
- GSA information (k, θ_{spf}), $\theta_{spf} = rand(1,1) \times 2\pi$
- System SNR: 20 dB
- Golden Search Precision: $\epsilon = 10^{-5}$

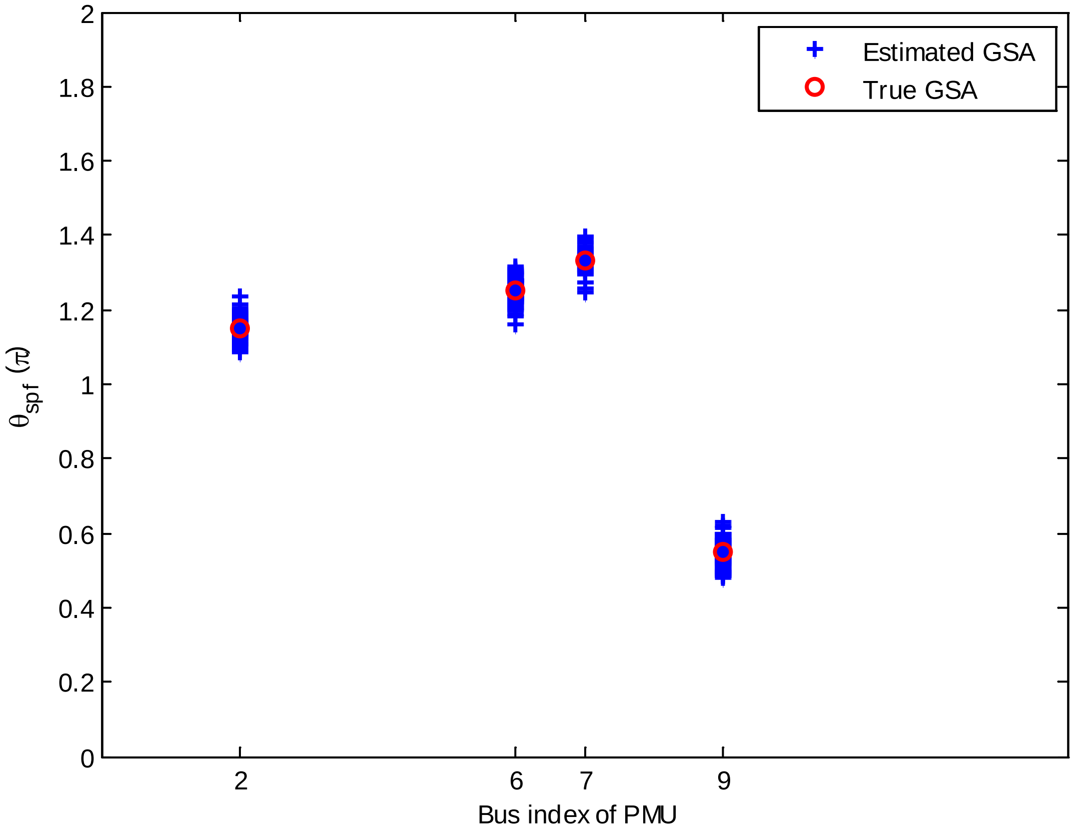
PMU PLACEMENT PROFILE UNDER DIFFERENT SCENARIOS

# of Buses	Index of Scenario	# of PMUs	Indices of Buses with PMUs	GSA location
14	1	4	2,6,7,9	7(3rd)
	2	6	2,4,6,7,9,13	7(4th)
30	3	10	1,7,9,10,12,18,24,25,27,28	25(8th)
	4	16	3,4,5,7,10,11,12,17, 19,22,24,25,26,28,29,30	25(12th)
57	5	17	1,4,6,13,20,22,25,27,29 32,36,39,41,45,47,51,54	41(13th)
	6	28	1,3,4,6,9,12,20,22,24,27,29, 30,32,34,36,38,39,41,43, 44,45,46,48,51,52,53,54,56	41(18th)

Performance Metrics

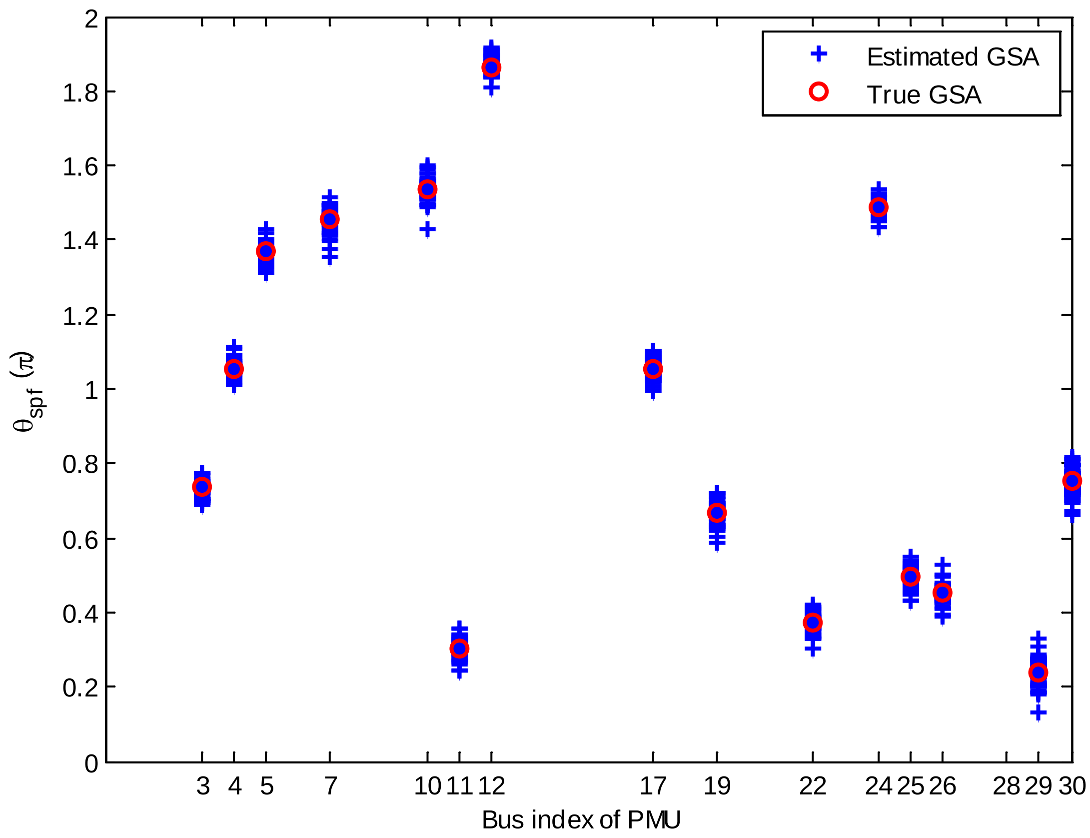
- Performance of GSA Detection
  - Correctness of location $\hat{k}$;
    - ➢ CDT: probability of correct detection
    - ➢ WDT: probability of wrong detection
  - Accuracy of $\hat{\theta}_{spf}$
    - ➢ Bias: $\hat{\theta}_{spf} - \theta_{true}$
    - ➢ RMSE: $||\hat{\theta}_{spf} - \theta_{true}||_2$
- Performance of State Estimation
  - Comparison b/w SpM, WLS, Genie
  - Magnitude $|V|$ and phase φ of system state
    - ➢ Estimation error
    - ➢ RMSE: root mean square error

Generalized Scenario 1: GSA(k, θ_{spf})



- Location $\hat{k}$: perfect GSA Phase shift $\hat{\theta}_{spf}$: good

Generalized Scenario 4: GSA(k, θ_{spf})



- Location $\hat{k}$: perfect GSA Phase shift $\hat{\theta}_{spf}$: good

Performance of GSA Detection

GSA DETECTION PERFORMANCE UNDER DIFFERENT SCENARIOS

Scenario	1	2	3	4	5	6
$p_{\mathrm{CDT}}(\%)$	100	100	100	100	100	100
$p_{\mathrm{WDT}}(\%)$	0	0	0	0	0	0
$Bias(\hat{\theta}_{spf})$	0.0226	0.0213	0.0255	0.0240	0.0310	0.0207
$RMSE(\hat{\theta}_{spf})$	0.0266	0.0262	0.0323	0.0309	0.0385	0.0254

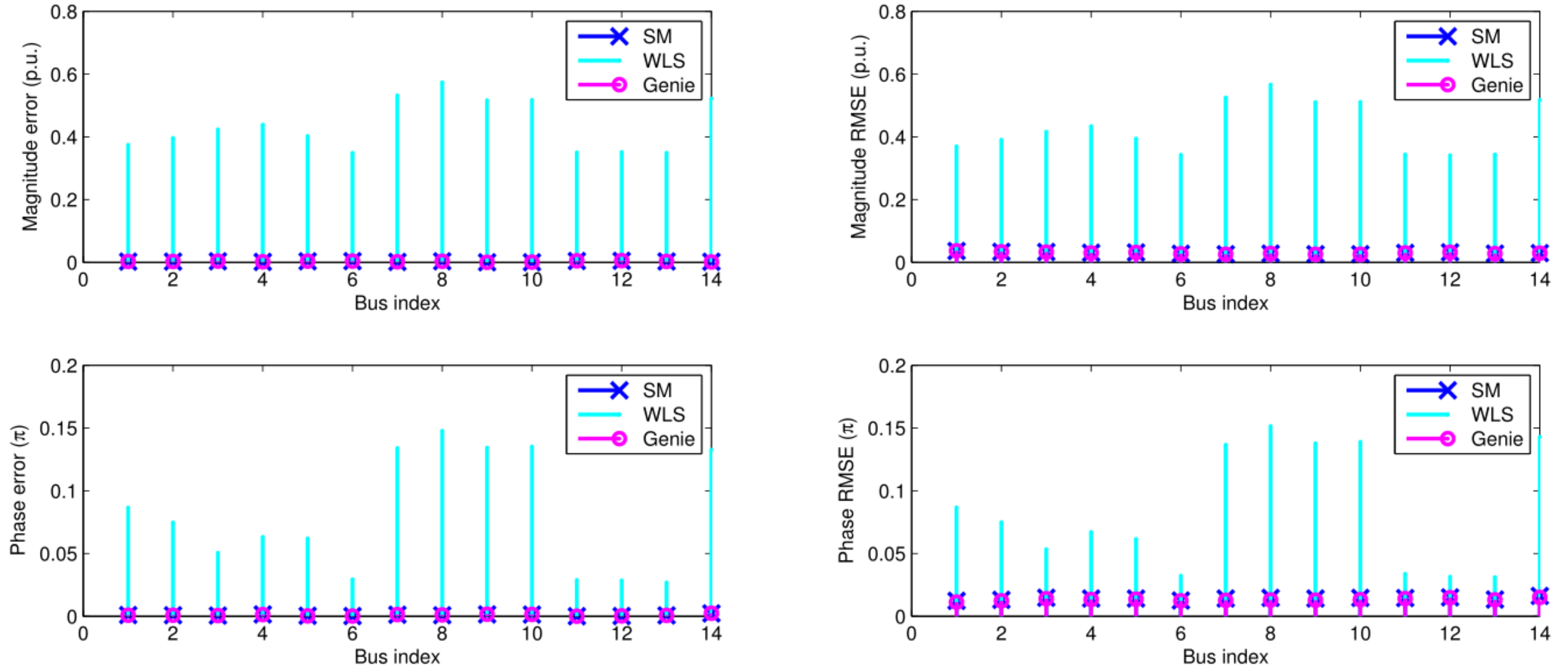
- The detection of location is almost perfect;
- The estimation for GSA phase shift is good considering the noise.

✓ SpM has good performance to detect single GSA.

Scenario 1: GSA(k, θ_{spf})

- State Estimation Error

RMSE



SpM ≈ Genie, much better than WLS.

Performance of State Estimation

RMSE OF STATE ESTIMATION UNDER DIFFERENT SCENARIOS

Scenario	SM		WLS		Genie		Improvement	
	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(%)	Pha.(%)
1	0.0307	0.0156	0.4355	0.0851	0.0309	0.0134	92.95	81.66
2	0.0250	0.0121	0.3250	0.0622	0.0249	0.0110	92.30	80.55
3	0.0324	0.0158	0.1758	0.0333	0.0324	0.0152	81.57	52.48
4	0.0188	0.0080	0.1082	0.0163	0.0188	0.0078	82.63	50.57
5	0.0430	0.0203	0.1400	0.0536	0.0430	0.0196	69.27	62.13
6	0.0186	0.0081	0.0642	0.0118	0.0186	0.0081	71.06	30.94

- Improvement by SpM compared with WLS is significant;
- SpM can achieve good performance close to Genie.
  - ✓ SM improves the state estimation under single GSA.

$$Impr. = \left(1 - \frac{RMSE_{SM}}{RMSE_{WLS}}\right) * 100$$

Summary & Future Work

- GSA is an imminent threat to current power grid
- Spoofed PMU data can be corrected instead of removal
- SpM algorithm provides good performance under single GSA
- Potential research areas:
  - Multiple GSA's impact and detection;
  - Anti-GSA strategies, including PMU placement, synchronization protocols.

Q & A

Thank you!