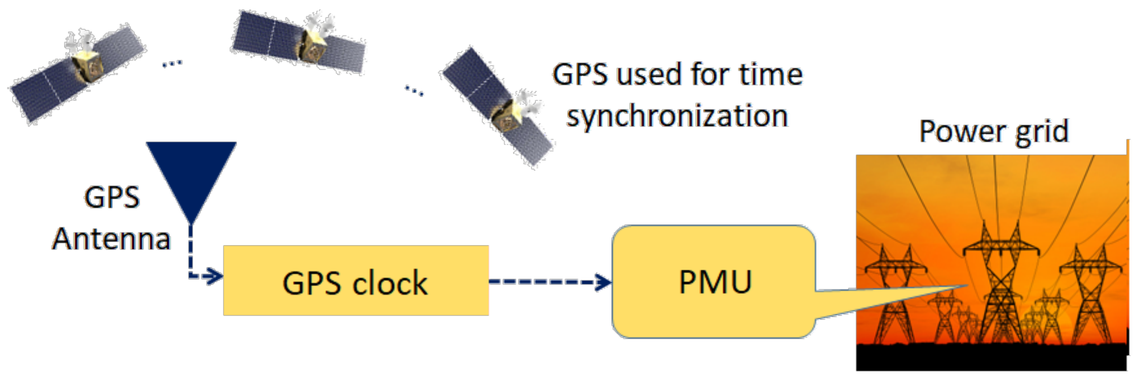
Robust and Secure GPS-based Timing for Power Systems

GPS Spoofing-Resilient Voltage Phasor Estimation for the Power Grid

Shubhendra Chauhan, Sriramya Bhamidipati and Grace Xingxin Gao

GRID VULNERABILITY TO GPS SPOOFING ATTACKS

- GPS provides accurate and precise time synchronization for PMUs to perform wide area monitoring and control
  - GPS time accuracy $\sim 100ns$ and frequency accuracy $\sim 10^{-12}\text{Hz}$

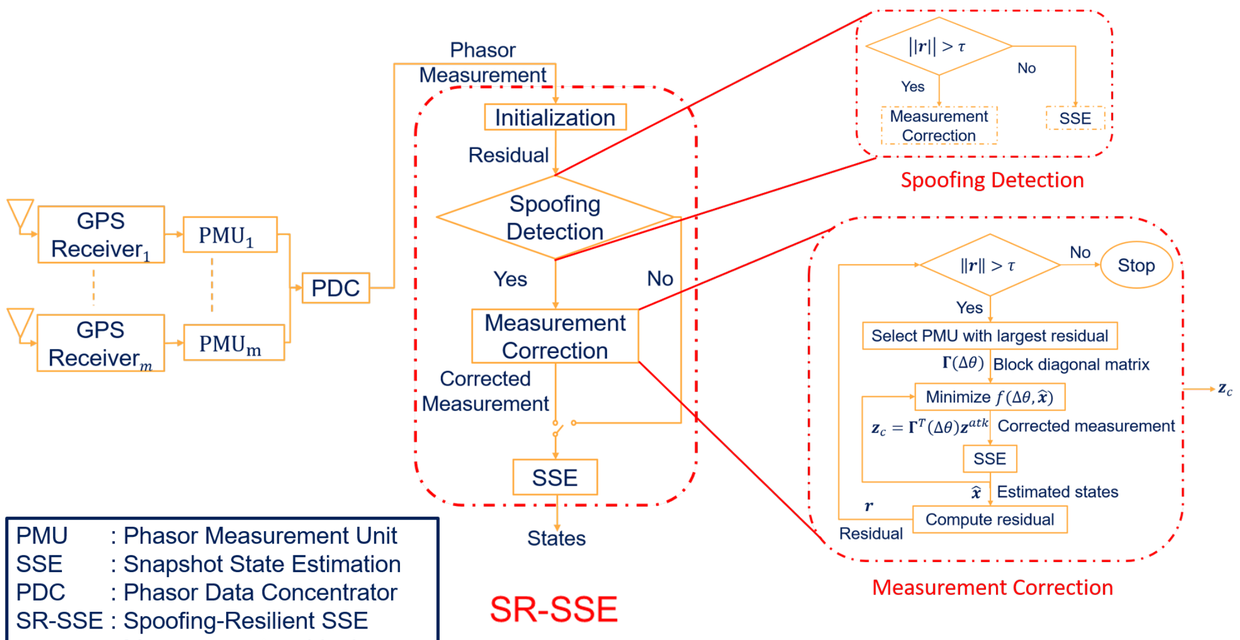


- Civil GPS signals are susceptible to malicious spoofing attacks
  - The received signal power is as low as $-130dBm$; the civil signal structure is unencrypted and known to the public
  - An attacker broadcasts counterfeit civil GPS signals and manipulate victim receivers' time
- Manipulated receivers' time shifts the phase angles for all the PMU measurements at the attacked bus
  - Degrades the performance of the state estimation algorithm
  - Reduces the efficacy of the fault location and voltage stability monitoring algorithms
- GPS spoofing attack detection and mitigation are critical to ensure safe operation of the power grid
- The following aspects related to detection and mitigation of GPS spoofing attacks will increase the resiliency of the power grid
  - Mitigation of multiple spoofing attacks on different buses of the power grid network
  - Necessary condition based on PMU measurement residuals for detecting GPS spoofing attacks
  - Simultaneous detection and mitigation of spoofing attacks using PMU measurements for state estimation algorithms

RESEARCH GOALS

- Provide a necessary condition for detecting GPS spoofing attacks using PMU measurement residuals
- Devise algorithm to mitigate the effect of multiple GPS spoofing attacks by correcting PMU measurements
- Develop a method for simultaneous detection and mitigation of GPS spoofing attacks, thereby advancing power grid resiliency

OUR ARCHITECTURE



PMU	: Phasor Measurement Unit
SSE	: Snapshot State Estimation
PDC	: Phasor Data Concentrator
SR-SSE	: Spoofing-Resilient SSE
$\boldsymbol{r}$	: Measurement residual
τ	: Threshold to detect spoofing

Key aspects:

- Our method jointly estimate voltage phasors and attack angles. This is achieved by two algorithms that simultaneously detect and mitigate GPS spoofing attacks
  - Spoofing Detection: Residual-based detection algorithm
  - Measurement Correction: An iterative-minimization algorithm to correct PMU measurements
- Derived mathematical necessary condition for detecting GPS spoofing attacks using PMU measurement residuals

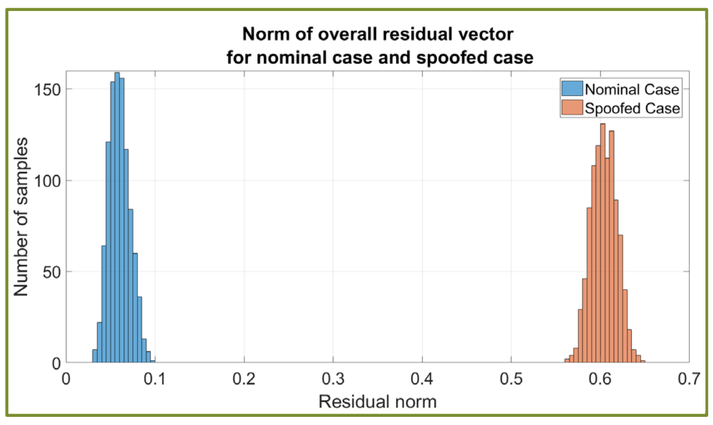
$$\left(\boldsymbol{I} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\right) \geq \boldsymbol{0}$$

Necessary Condition

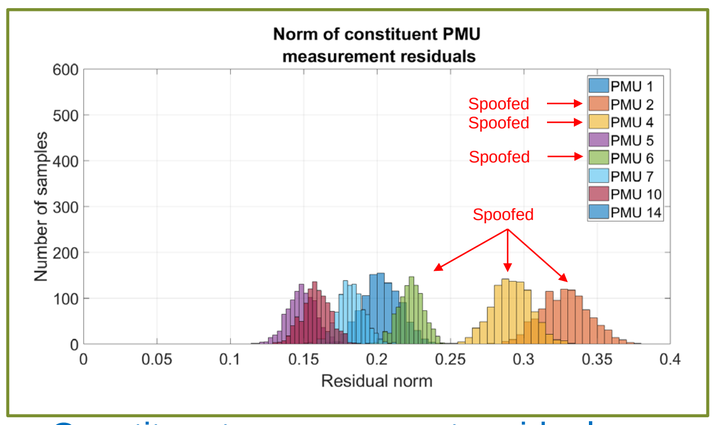
Identity Matrix — Admittance Matrix — Pseudoinverse

KEY IDEAS USED IN OUR METHOD

- Monte-Carlo simulation confirms our theoretical analysis and shows that distribution of measurement residual norm changes under a GPS spoofing attack as shown on the right plot
- The introduced bias in the measurement residual norm is used as a detection criteria to detect single or multiple attacks



Measurement residual norm under nominal and spoofed scenario

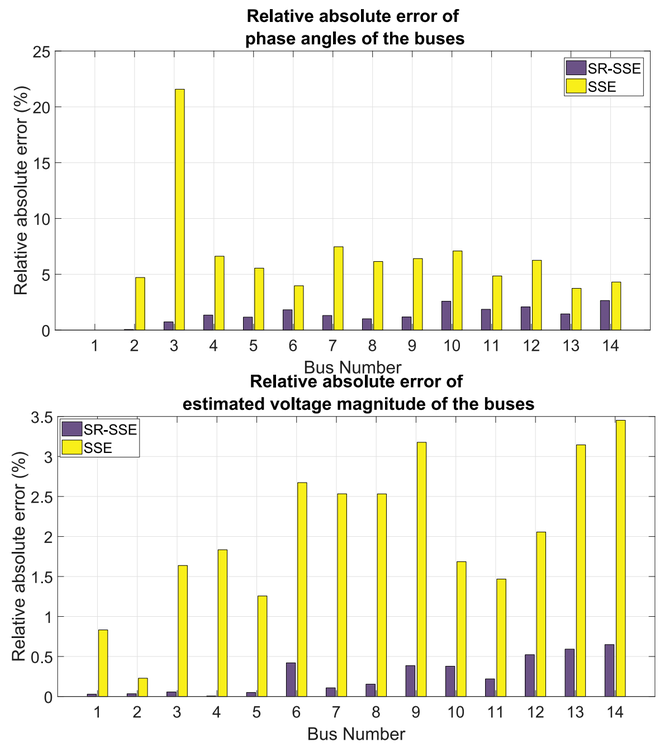


Constituent measurement residual norm under spoofed scenario

- A major contribution in measurement residual norm comes from the spoofed PMU measurements as shown on the left plot
- Above criteria is utilized in the Measurement Correction algorithm to distinguish spoofed PMUs from other

OUR RESEARCH RESULTS

- Simulated IEEE 14 test bus case in Matlab using Matpower. Single and multiple GPS spoofing attacks at various nodes were simulated
- Validated our algorithm for multiple GPS spoofing attacks. Our algorithm reduces the estimation error by an order of magnitude
  - Shown results in which PMU measurements at bus 2,4 and 6 were spoofed



	RMSE	
	Voltage (pu)	Phase (deg)
SSE	2.42×10^{-2}	1.06
SR-SSE	3.69×10^{-3}	2.38×10^{-1}

Voltage and Phase angle estimation errors for SR-SSE and SSE

IMPACT ON POWER GRID

Performance benefits:

- By implementing our method, the power grid monitoring systems will:
  - Provide spoofing resilient voltage phasor estimates
  - Reduce the system risks against external timing attacks
  - Ensure continued robust performance even in degraded scenarios
  - Elevate the maturity of wide area monitoring for future power grids

Business benefits:

- No added hardware and infrastructure costs
- Real time implementation capability
- Increased resilience against GPS spoofing attacks

POTENTIAL COLLABORATION OPPORTUNITIES

Cooperation, support and guidance from industry partners in the following areas would benefit this research activity:

- Inputs regarding the details of PMU setup including latencies, communication network and processing capabilities
- Specifications regarding the expected response time to counteract the timing attacks on the PMUs
- Platform for state estimation analysis via datasets or test bed setup to validate the impact of our algorithm

- Contact: **gracegao@Illinois.edu, chauhan7@Illinois.edu, sbhamid2@Illinois.edu**

- Activity webpage: **https://cred-c.org/researchactivity/robust-and-secure-gps-based-timing-power-systems**

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY