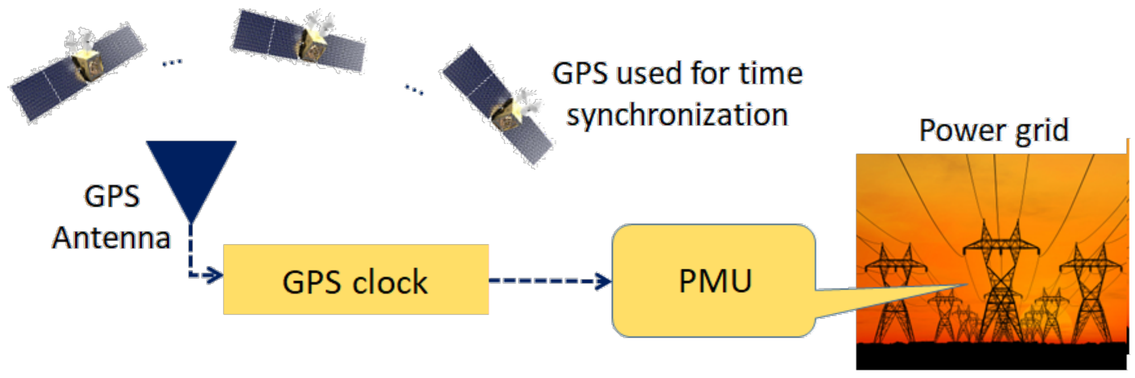
Robust and Secure GPS-based Timing for Power Systems

GPS Multi-Receiver Joint Direct Time Estimation and Spoofer Localization

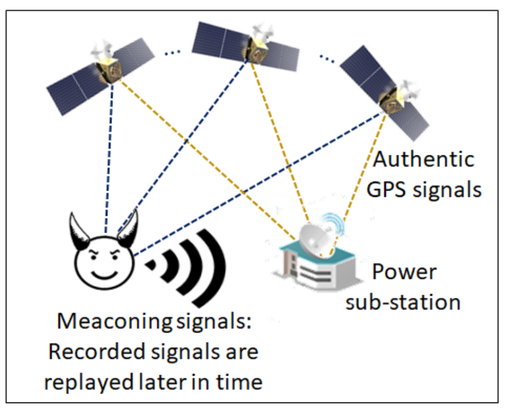
Sriramya Bhamidipati and Grace Xingxin Gao

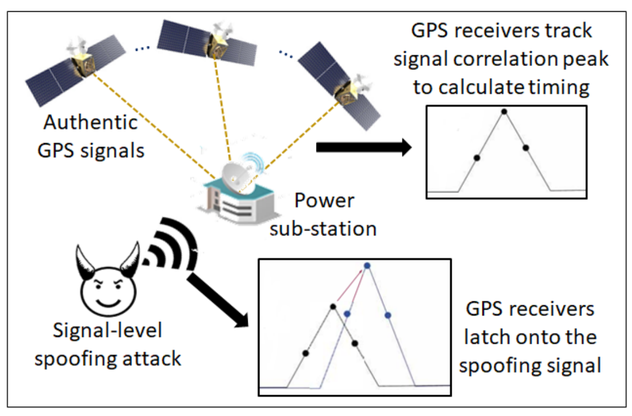
GRID VULNERABILITY TO SPOOFING ATTACKS

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



- According to IEEE-C37.118.1, to maintain grid stability, the maximum allowable phase angle error is $0.573°$ (~timing error of $26.5\ \mu s$)
- 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 and time drift solutions
- Incidents of GPS spoofing attacks reported in the recent past
  - In 2017, around 20 maritime vessels near the coast of Novorossiysk, Russia were effected by a mass spoofing attack
  - At the ION GNSS+ 2017, numerous devices reported incorrect time and position due to accidental spoofing caused by a leaky simulator





RESEARCH GOALS

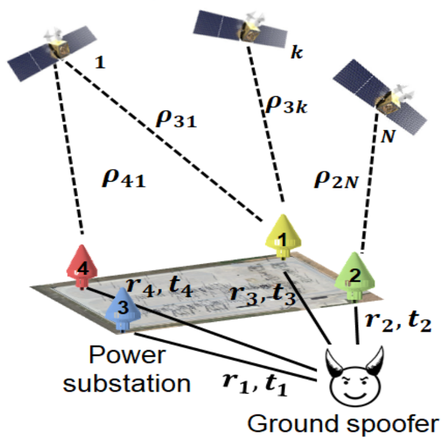
- **Address the GPS vulnerability by investigating spoofing attacks that adversely affect PMU accuracy**
- **Devise algorithms to counteract these attacks, thereby enabling the adoption of GPS/GNSS synchronized PMUs while advancing power grid resiliency**

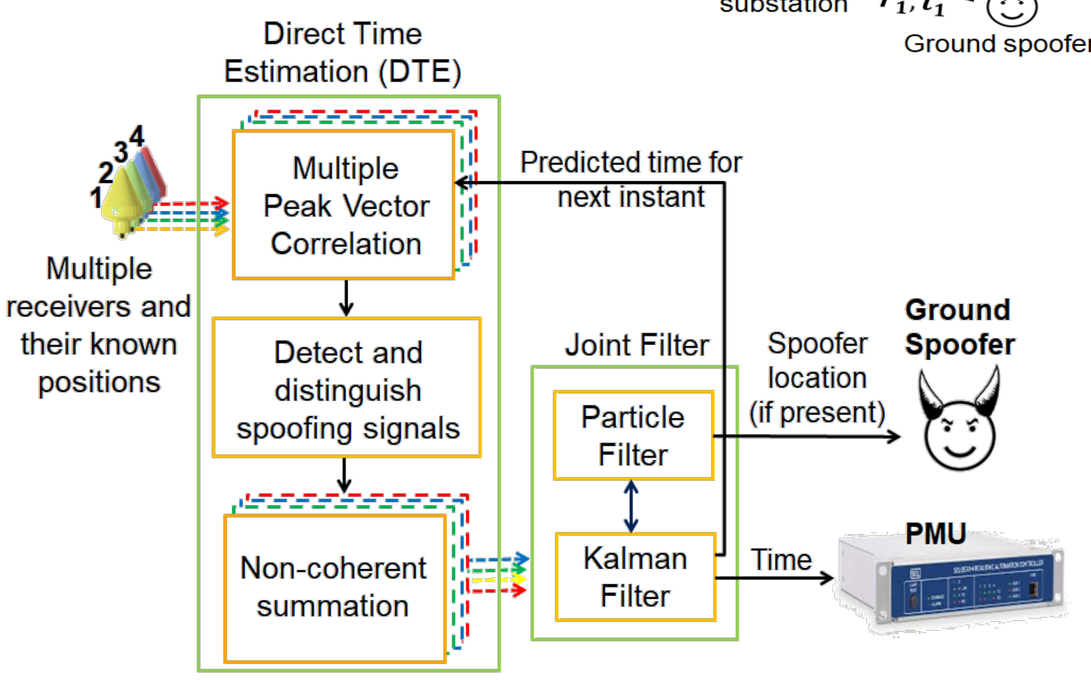
OUR ARCHITECTURE

Key aspects:

- Multiple **receivers**
  - Geographical diversity
  - Known receiver positions
- **Direct Time Estimation (DTE)**
  - Directly works in the timing domain
  - Detects spoofing attacks
- **Joint Particle and Kalman Filter**
  - Locates the ground spoofer

Geographically distributed receivers within power substation

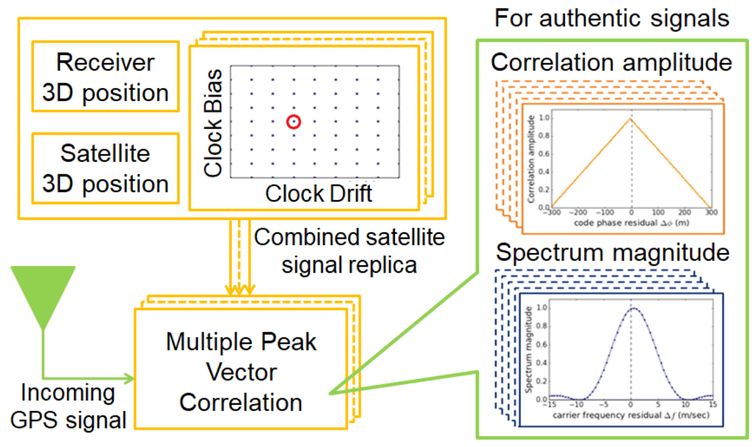




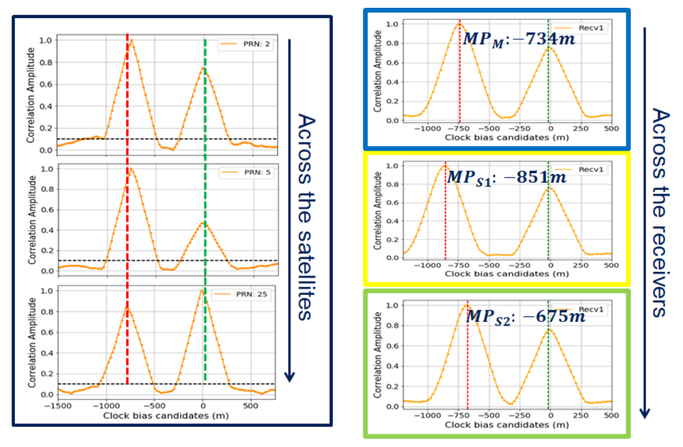
OUR ALGORITHM DETAILS

- Grid points in the 2-D search space represent the pre-generated clock bias and clock drift candidates
- At each receiver, the presence of multiple significant peaks during vector correlation indicate spoofing attack

Multiple peak vector correlation



Detection of spoofing signals

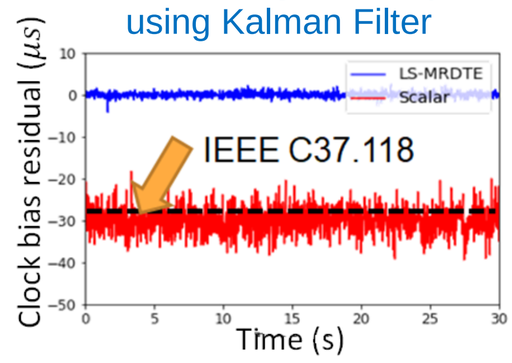


To detect and distinguish malicious peaks indicating spoofing, time delayed similarity is identified across the geographically distributed receivers

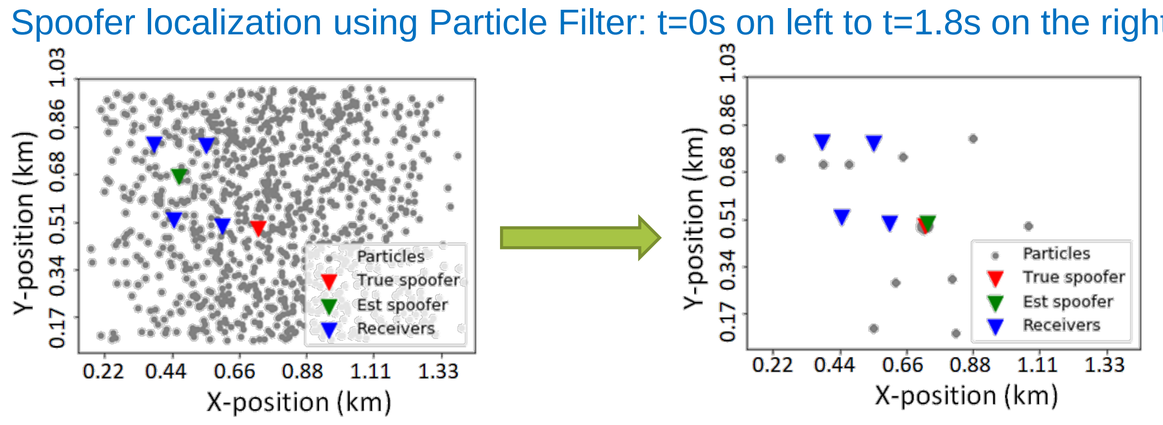
OUR RESEARCH RESULTS

- Simulated meaconing causing $30\mu s$ time delay is added to authentic data collected in open sky
- Geometry of multiple receivers comply with the Ameren Illinois Power Substation, Kansas, IL
- Our Joint Filter demonstrates spoofer localization to within $3m$ and accuracy of GPS time to within $1.5\mu s$

GPS timing accuracy using Kalman Filter



Spoofer localization using Particle Filter: t=0s on left to t=1.8s on the right



IMPACT ON POWER GRID

Performance benefits:

- By implementing our algorithm, the power system would:
  - Provide synchronized phasor measurements up to 100ns accuracy
  - 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:

- Minimal added hardware and infrastructure costs
- Increased timing resilience and precise time synchronization

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 power stability analysis via datasets or test bed setup to validate the impact of our algorithm

- Contact: **gracegao@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