Simultaneous Localization of Multiple Jammers and Receivers Using Probability Hypothesis Density

Sriramya “Ramya” Bhamidipati, University of Illinois at Urbana-Champaign

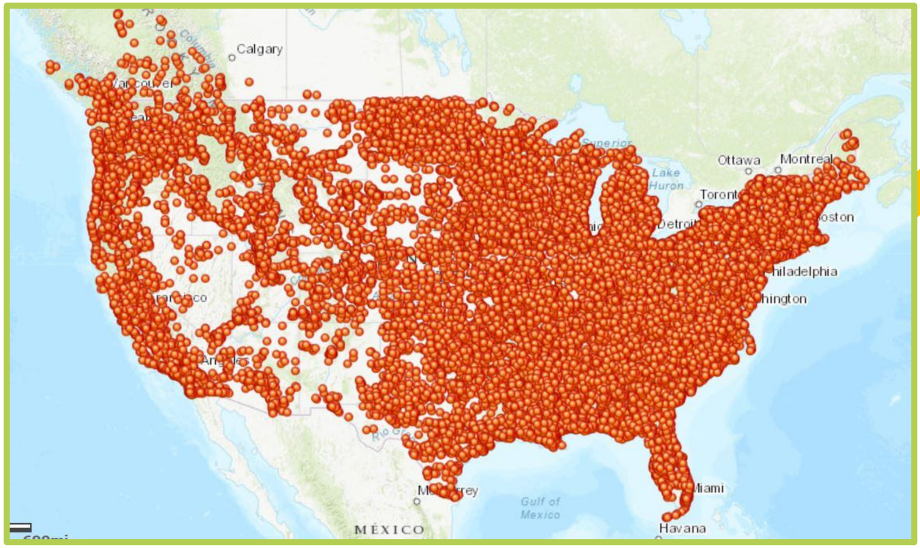
CREDC All Hands Meeting

April 6th, 2018

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Time Critical Applications

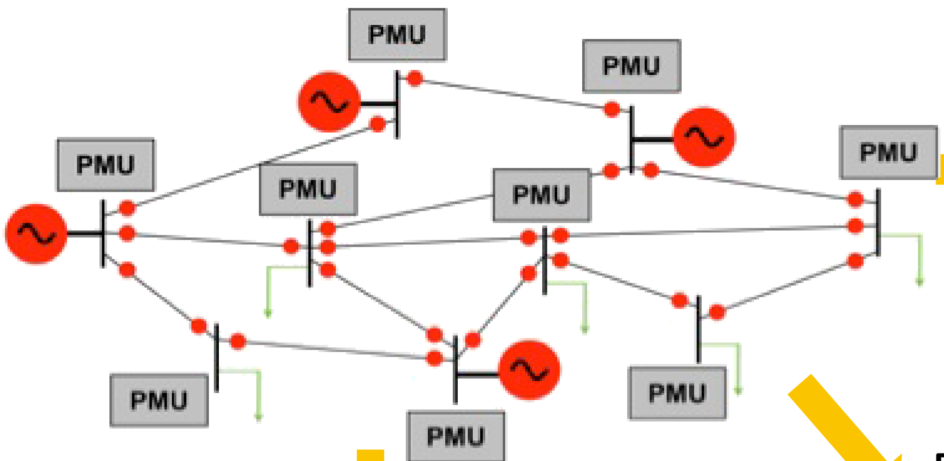
Transport | Banking, Finance | Communi-cations | Power Grid



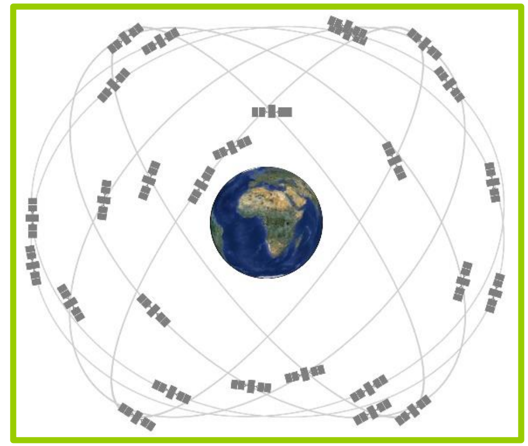
Densely distributed (>2000) Phasor Measurement Units (PMUs) across USA

Timing sources for Power Substations

Monitoring power substations via Phasor Measurement Units (PMUs)

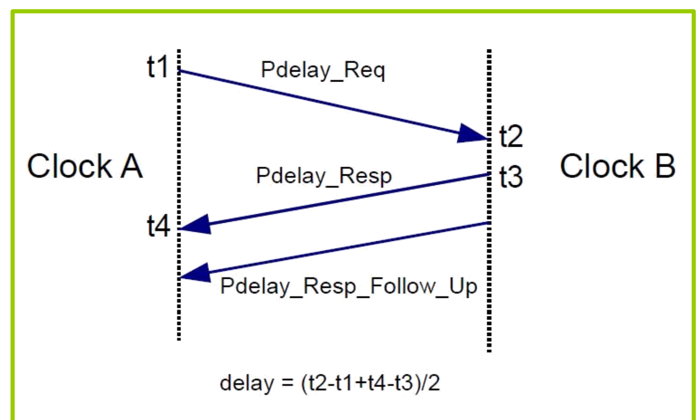


Global Positioning Systems

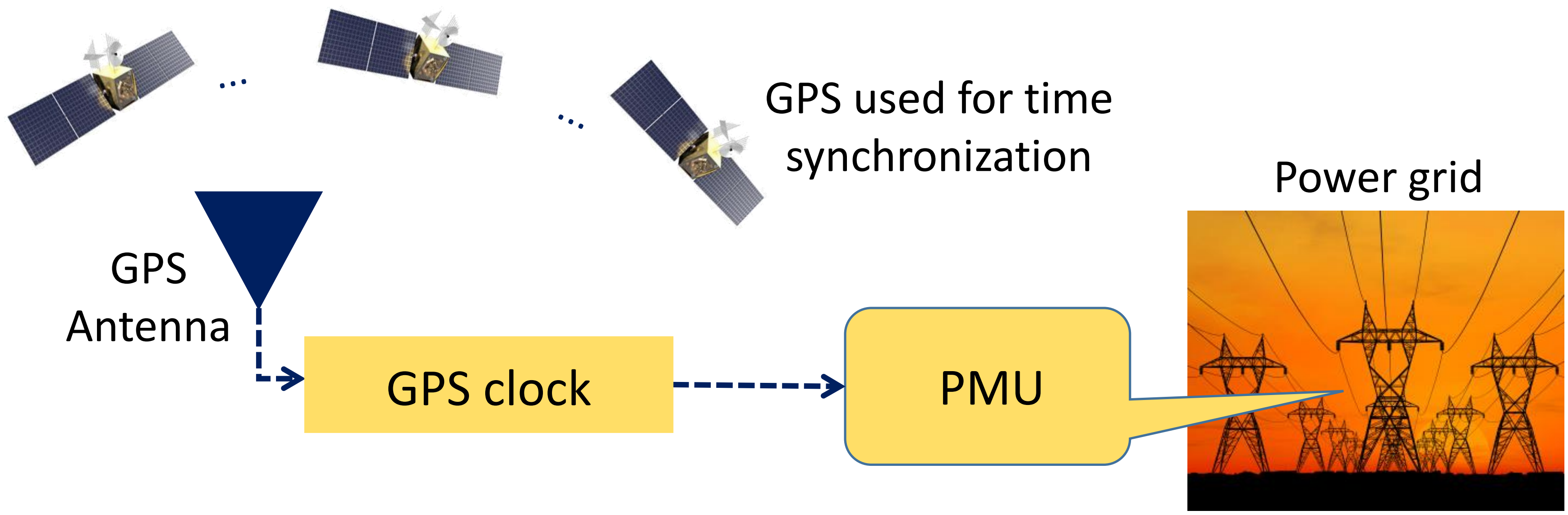


Clocks: TCXO, Atomic, XCXO

Precise Time Protocol (PTP)



GPS Timing for PMUs



Advantages
Global coverage
Freely available
μs-level accurate global time

Disadvantages
Low signal power
Unencrypted structure
Vulnerable to attacks

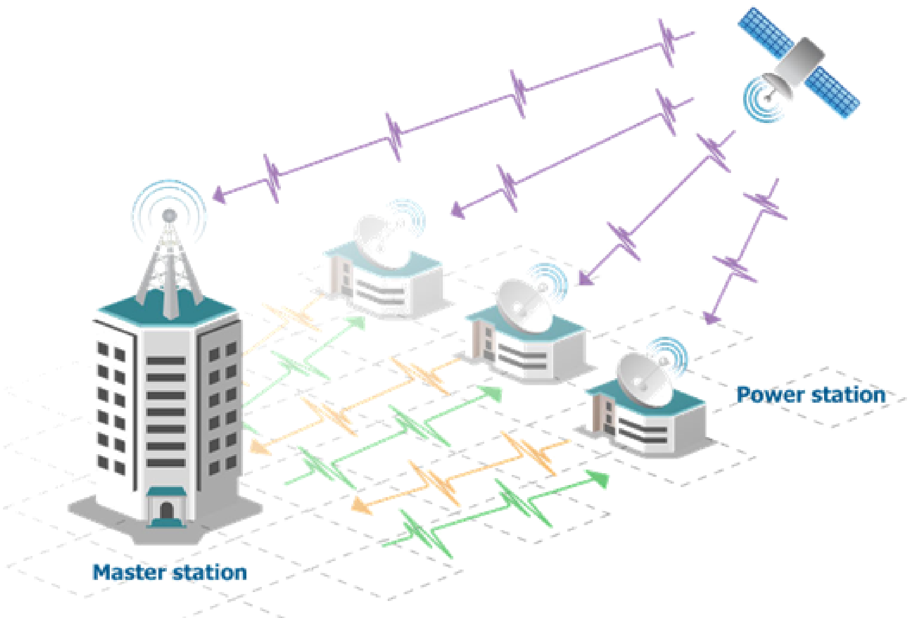
Outline

Background on GPS and Jamming Attacks

Simultaneous Localization of Multiple Jammers and Receivers

Experimental Verification and Validation

Summary

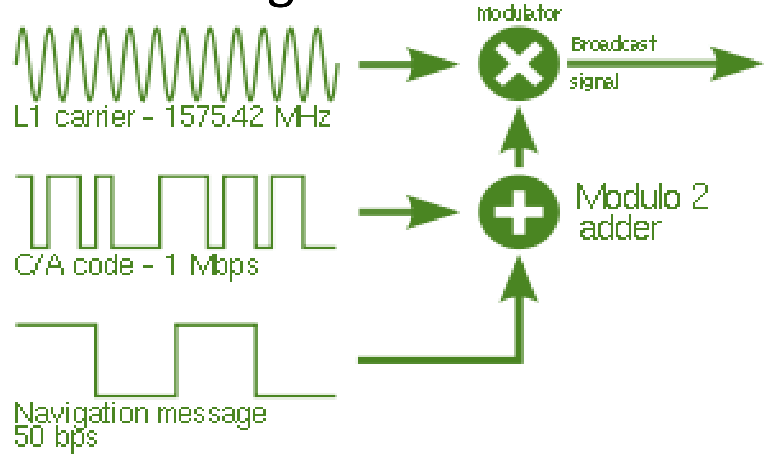


Traditional GPS Algorithm

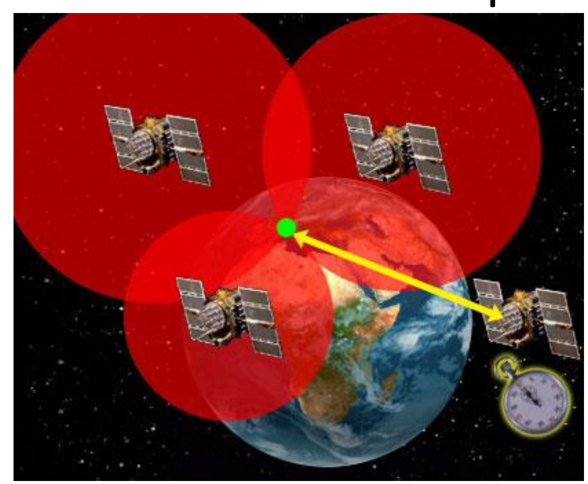
- Methodology
  - Trilateration with ≥ 4 satellites
  - Track carrier frequency and code phase
- Inputs
  - Center: $3D$ satellite position
  - Radius: Pseudoranges
- Unknowns to be estimated:
  - $3D$ position, Clock bias

By computing clock bias, we can estimate UTC time with satellite atomic clock level accuracy

GPS Signal Structure



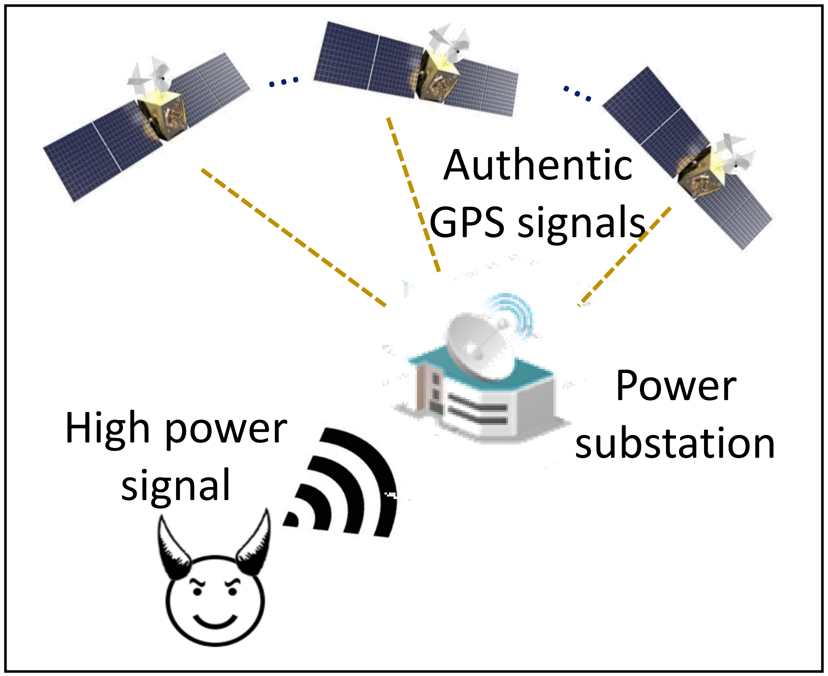
Trilateration technique



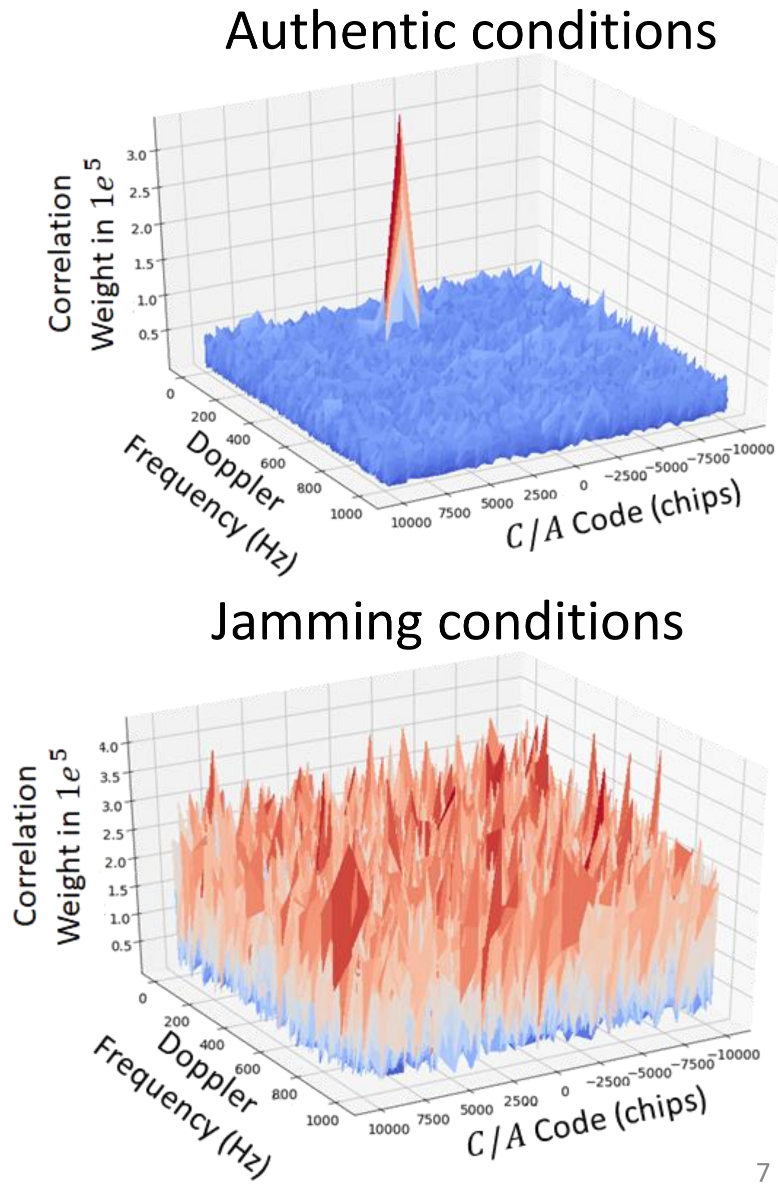
[Larson GPS Research Group]

What is GPS Jamming?

High powered signals transmitted in GPS frequency band



Jamming: Makes timing unavailable for PMUs



GPS Jamming Incidents

- Around 80 GPS jamming incidents between 2013 – 2016 [1]
- Few notable ones:
  - San Diego harbor, 2007 for 3 days [2]
  - Over 1000 planes, 250 ships in South Korea, 2012 for 16 days [3]
  - London Stock Exchange, 2012 everyday 10 mins [3]
  - Newark Liberty International Airport, 2013 2 months to track [1]
  - Cairo airport, 2016 [4]

Increasing number of GPS jamming incidents due to the ease of operation and low-cost availability

[1] Aviation today 01/31/2017

[2] GPS world 02/2014

[3] The economist "GPS jamming, Out of Sight" 07/2013

[4] Flight service bureau 05/24/2017

Multiple jammers

- Increasing risk due of low cost jammers ~$50-100
- Challenges due to multiple jammers:
  - Presence of unknown number of jammers
  - Unknown contribution of each jammer at receiver
  - Increase in complexity of localization
- Existing GPS anti-jamming techniques
  - Directional antenna, time difference of arrival and so on
  - Address single jammer scenario
  - Mostly don’t estimate receiver Position, Velocity and Time (PVT)

“Jaguar” mounted with directional antenna

[Perkins et.al, ION GNSS 2015]

Our Objectives

- Locate multiple jammers instead of one
- Improve the robustness of the Position, Velocity and Time (PVT) solution of the receivers experiencing jamming

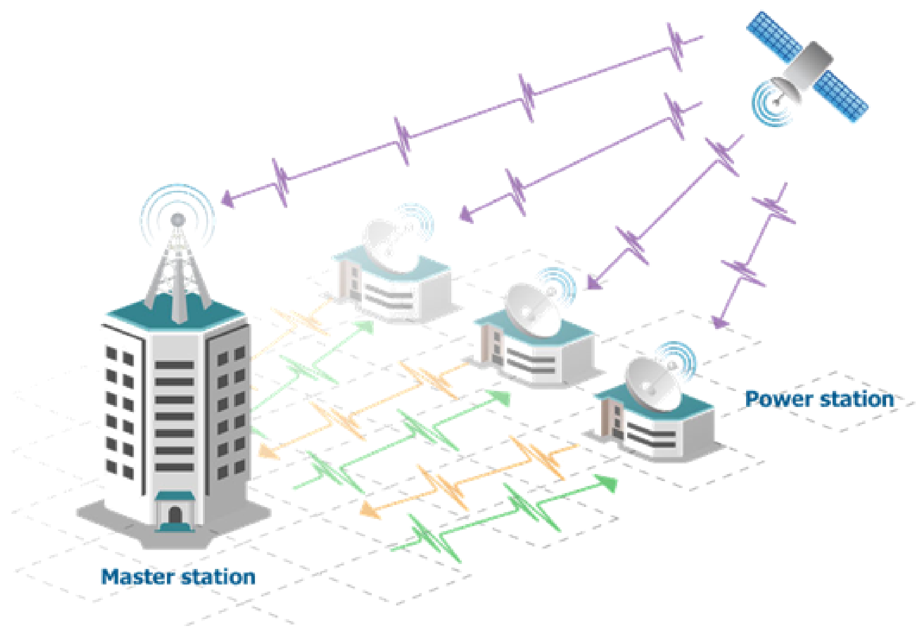
Outline

Background on GPS and Jamming Attacks

Simultaneous Localization of Multiple Jammers and Receivers

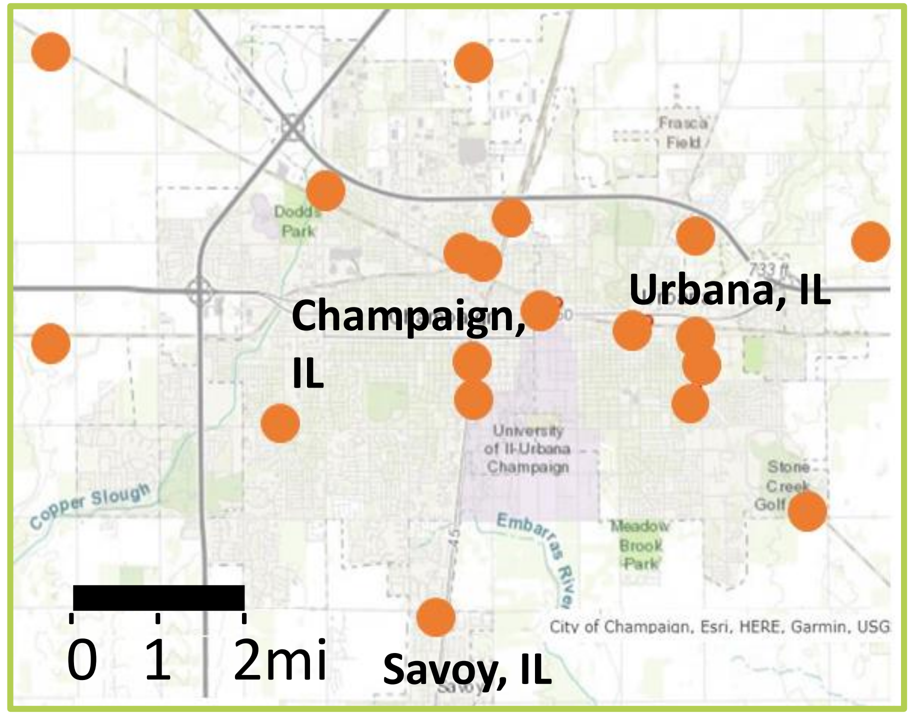
Experimental Verification and Validation

Summary



SLMR: Our Approach

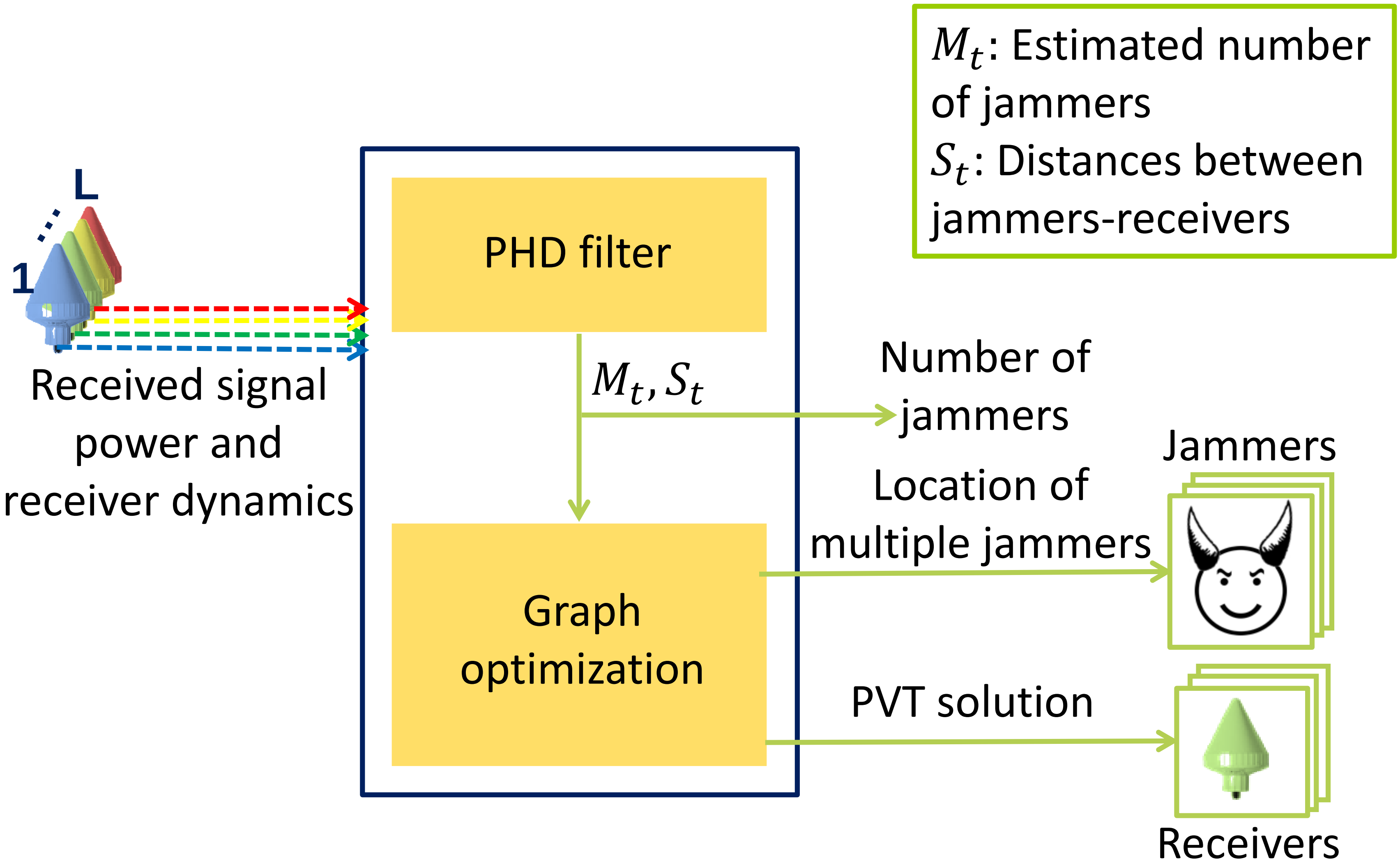
- Multiple receivers
  - Geographical diversity
  - Variation in the received GPS signal power
- Probability Hypothesis Density (PHD) Filter [5]
  - Estimation of unknown number of jammers
- Inspired from Simultaneous Localization and Mapping (SLAM) [5] for robotics
  - Robots: GPS receivers
  - Features: jammers
  - Graph optimization



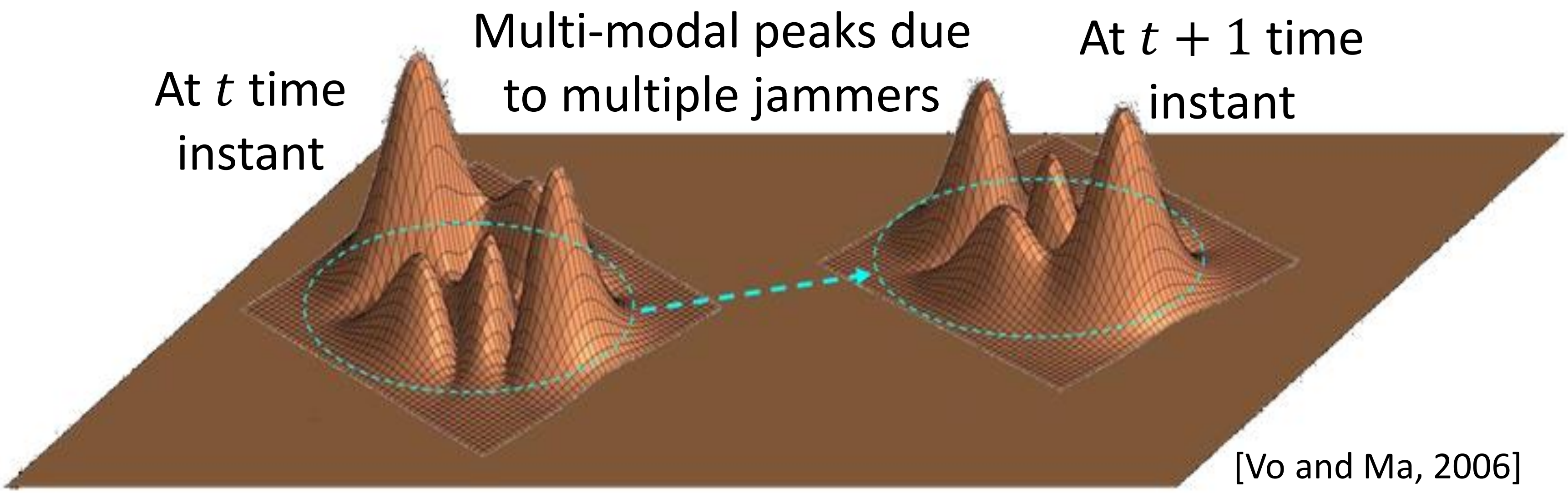
19 Illinois power substations in nearby 3 cities over 12x8miles

[5] Vo and Ma, IEEE Transactions on Signal Processing, 2006
[6] Cadena, et.al, IEEE Transactions on Robotics, 2016

SLMR: Our Architecture



Intuitive Explanation of PHD Filter



- Multiple jammers are observed via multi-modal Gaussian distributed peaks
- State and measurements modelled as Random Finite Sets
- Cardinality modeled as a random variable
- Non-linearity is due to received signal strength measurements

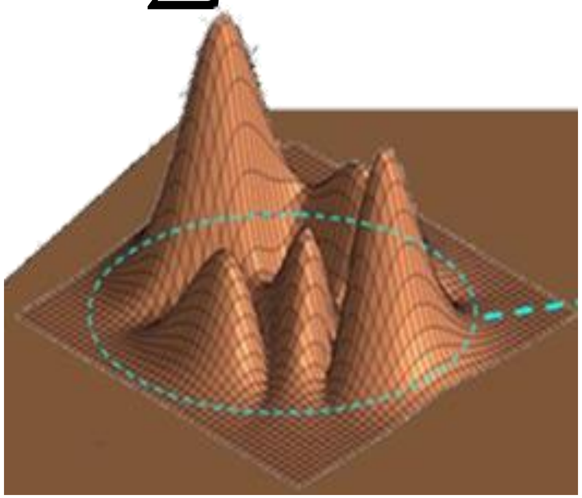
Non-Linear Gaussian Mixture PHD Filter

- Propagate posterior intensity modeled as Gaussian Mixture

$$v_t = \sum w_t \mathbb{N}(x: \mu_t, \Sigma_t)$$

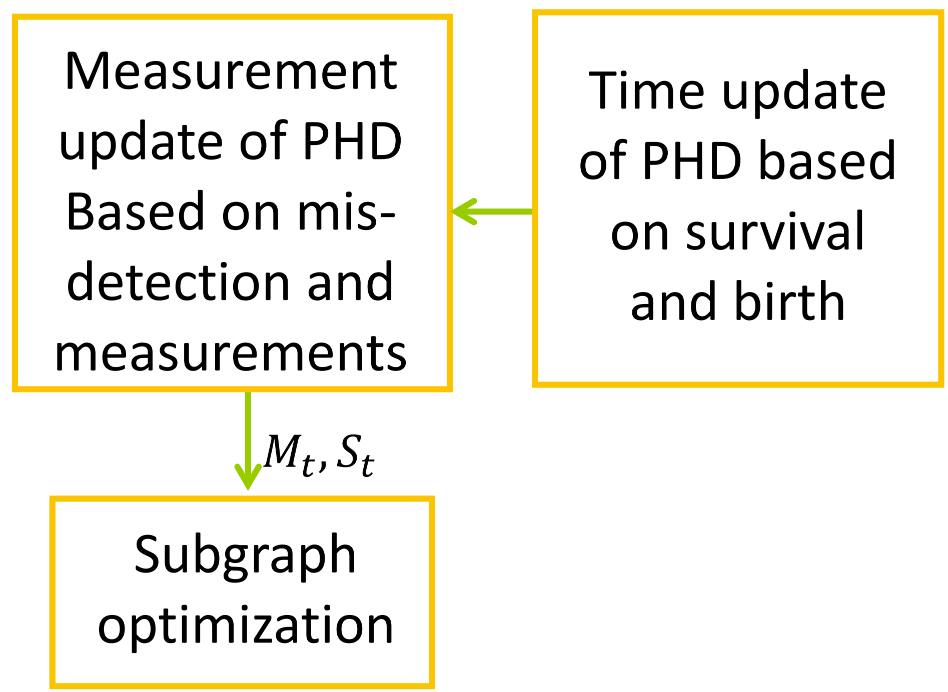
- Estimated number of jammers

$$M_t = \sum \mathbb{I}(w_t > \text{Threshold})$$



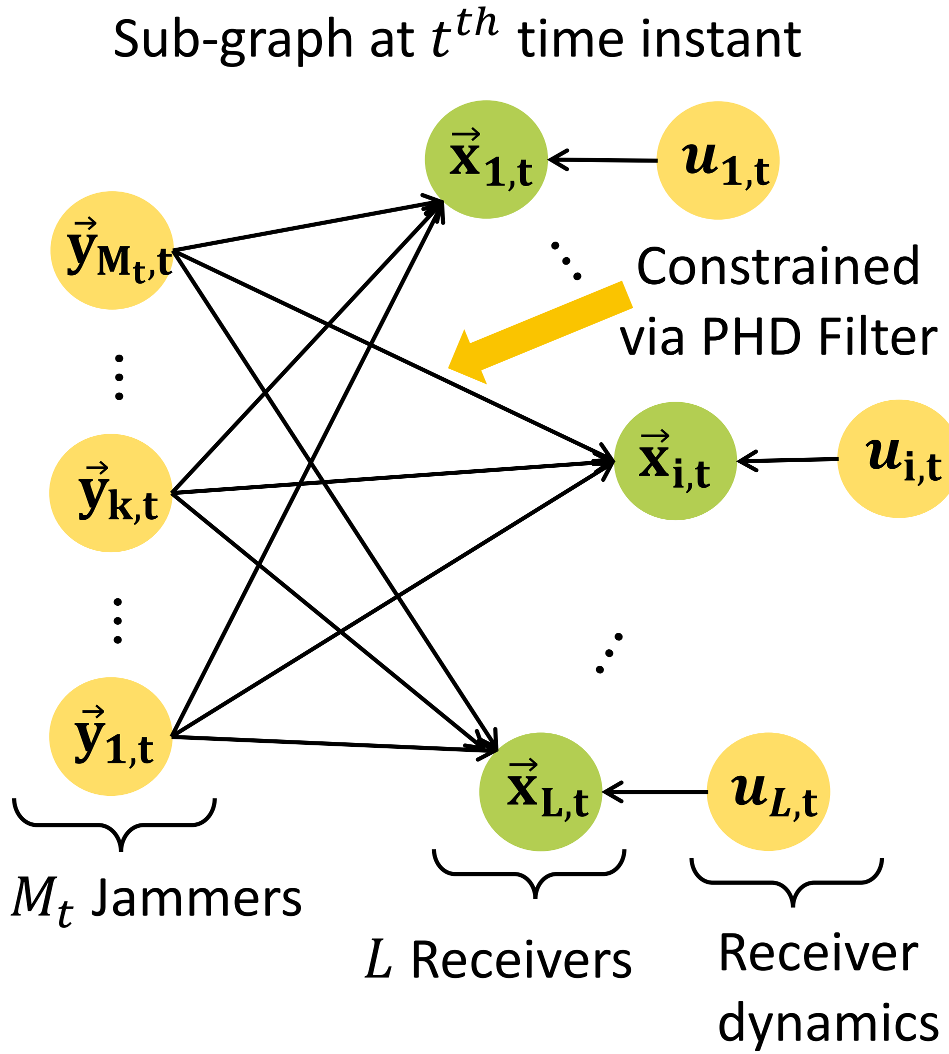
Multi-modal peaks modeled as Gaussian Mixture (GM)

μ_t: mean
Σ_t: covariance
w_t: weight
S_t: jammers-receivers distance



SLMR: Graph Framework

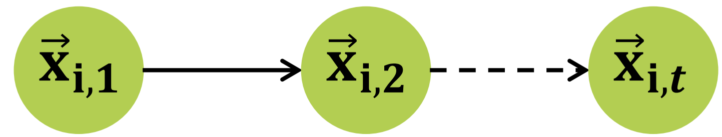
- Bipartite graph framework
  - M_t number of jammers $\vec{\boldsymbol{y}}$
  - L receivers $\vec{\mathbf{x}}$
  - Receiver dynamics $\boldsymbol{u}$ (Ex: static, uniform velocity or IMU)
- Sub-graph optimization at time each instant
- Periodically, full-graph optimization to account for drifts

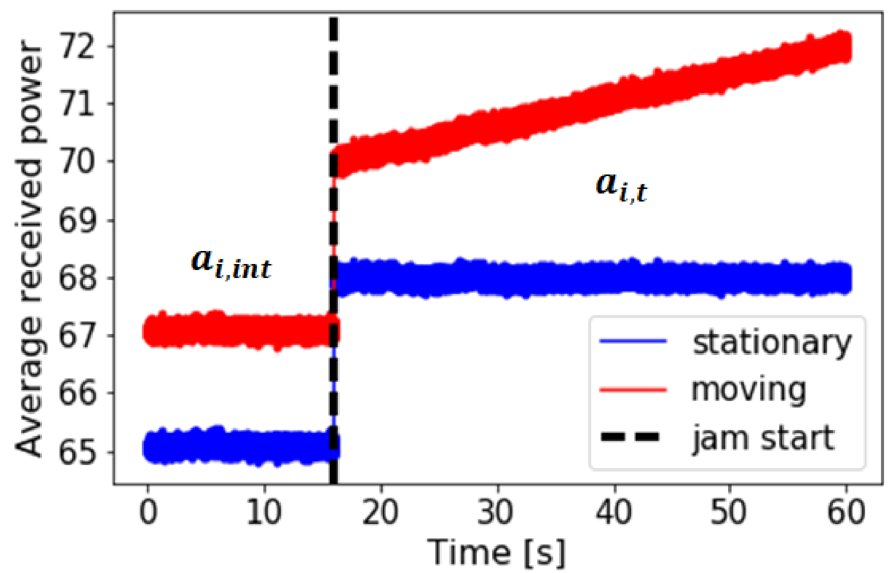


SLMR: Graph Optimization

- Levenberg-Marquardt minimizer [7]
  - Initial constraints of receivers
  - Constraints from PHD Filter
  - Constraints from receiver dynamics
- After jamming detected, SLMR initialized as follows:
  - Non-jammed received GPS signal power at each receiver
  - Single jammer with the initial location at the centroid of receivers
  - Graph based on the initial constraints of receivers and jammer

Graph framework across time





[7] Mor, Numerical Analysis, 1978

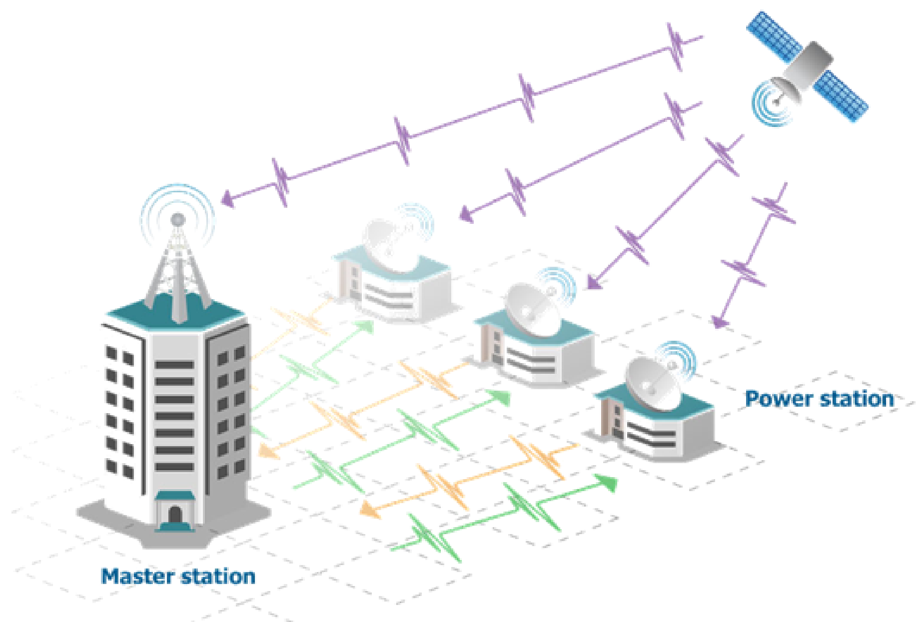
Outline

Background on GPS and Jamming Attacks

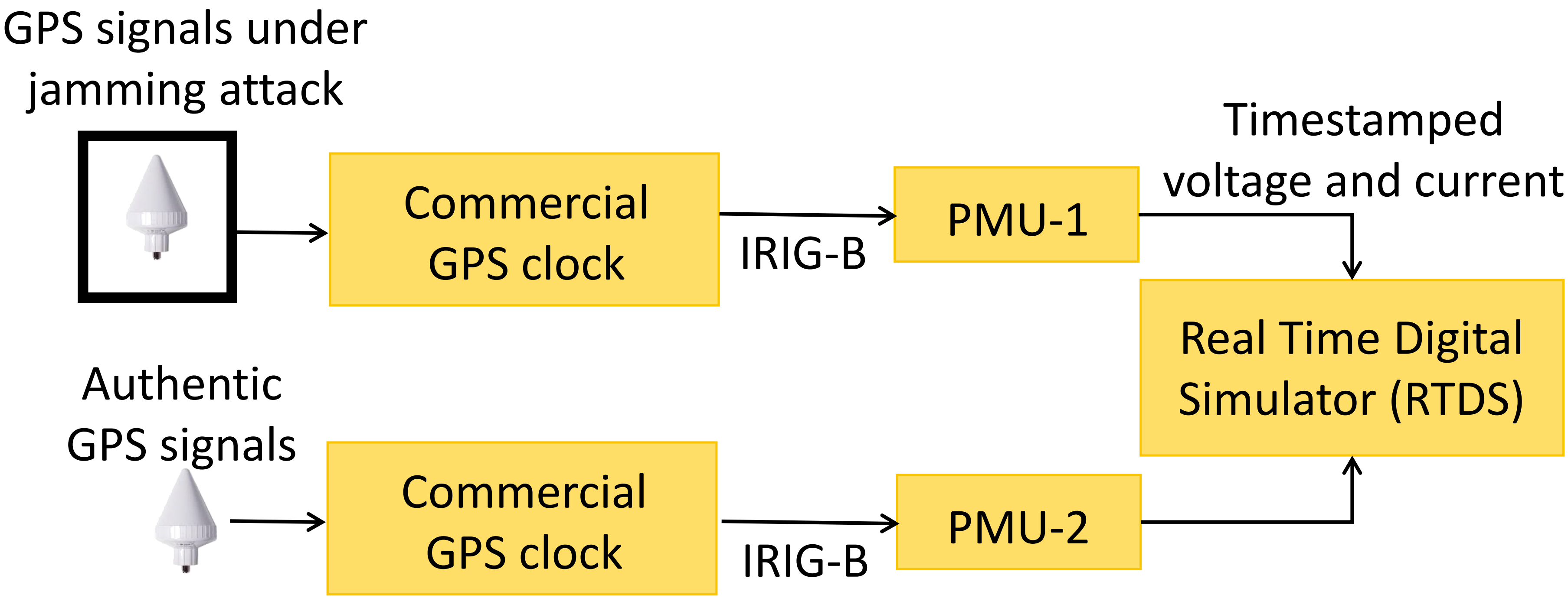
Simultaneous Localization of Multiple Jammers and Receivers

Experimental Verification and Validation

Summary

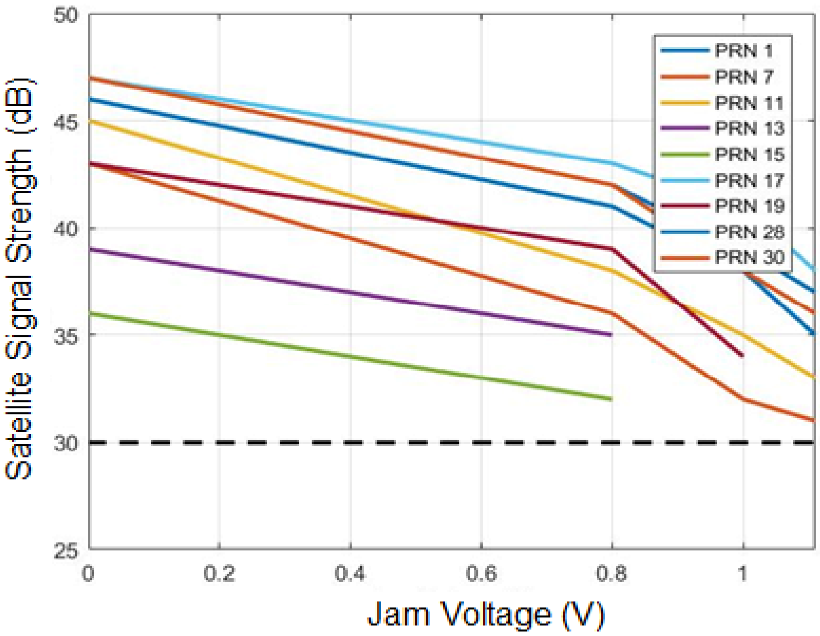


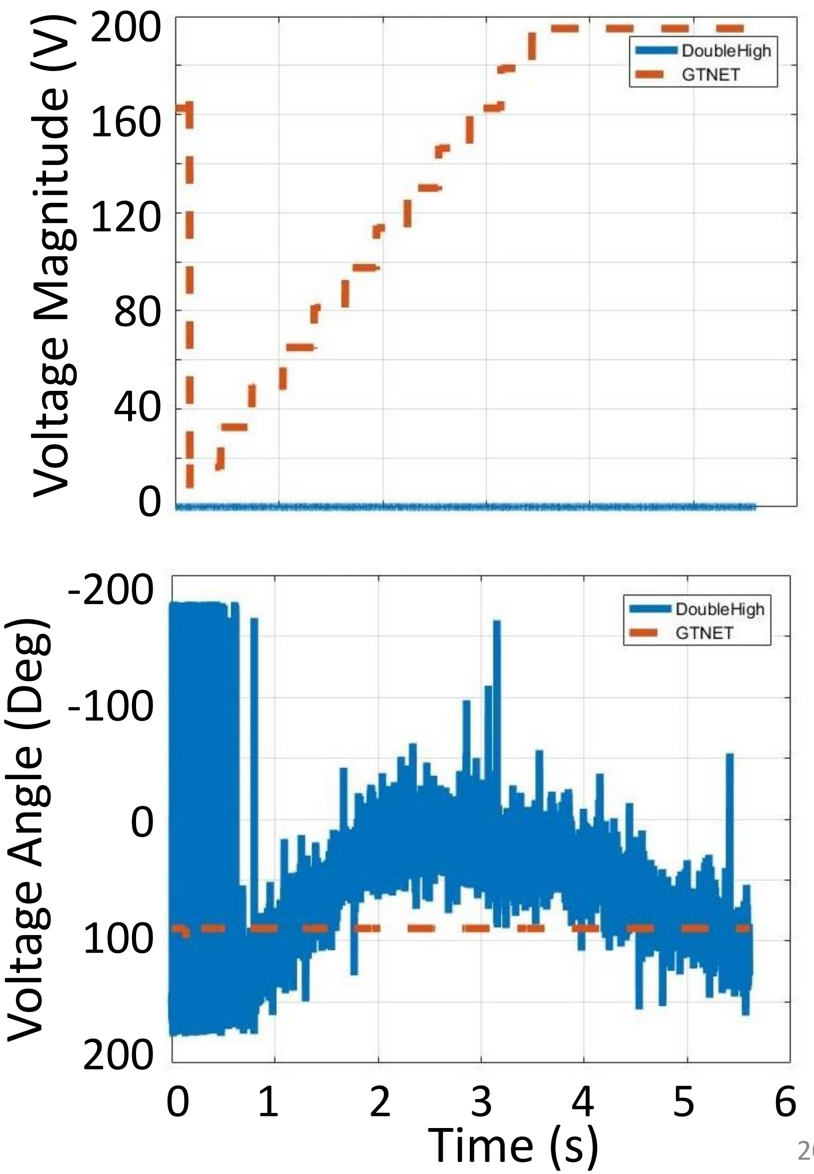
Timing Attack Setup



According to IEEE C37.118, max allowable phase angle error is $0.573°$ (~time error of $26.5\ \mu s$)

Effect of Jamming on Power Grid

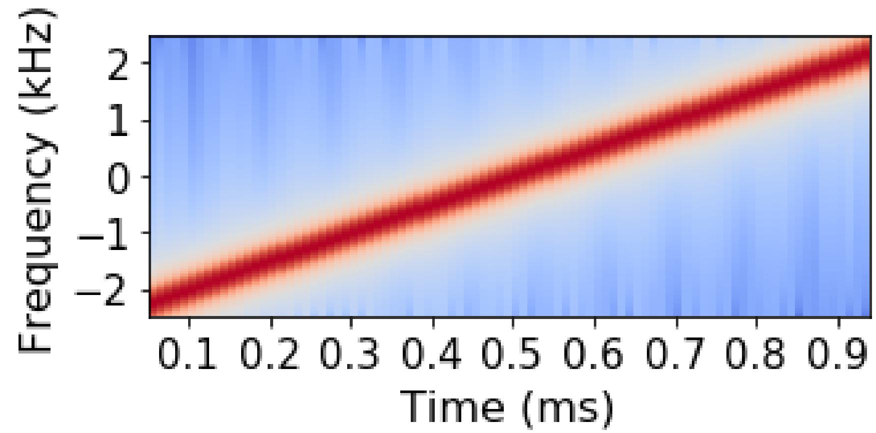


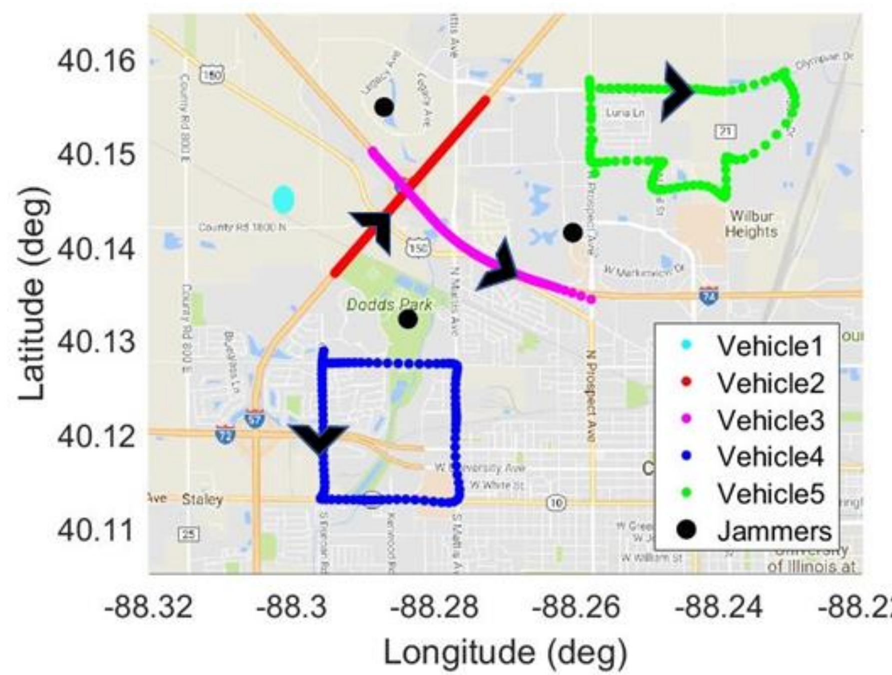


GPS jamming causes inoperability of PMUs to record phasor values

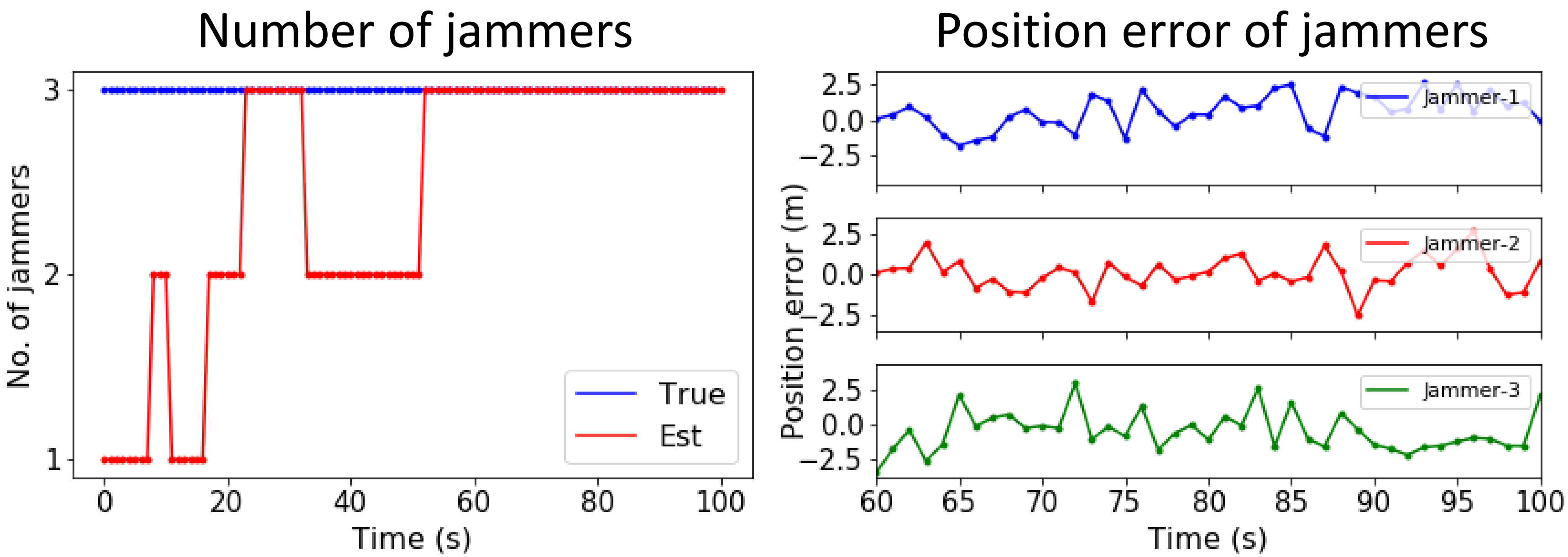
Experimental Setup

- Three stationary simulated jammers
  - Transmit power 50.3 W
  - Sweep continuous attack with frequency $-2.5\ kHz\ to\ 2.5\ kHz$
- Five moving GPS receivers
- GPS signals collected
  - Sampling rate $5MHz$
  - Received power computed using $\Delta T = 10ms$
- Post-processed using our python framework pyGNSS



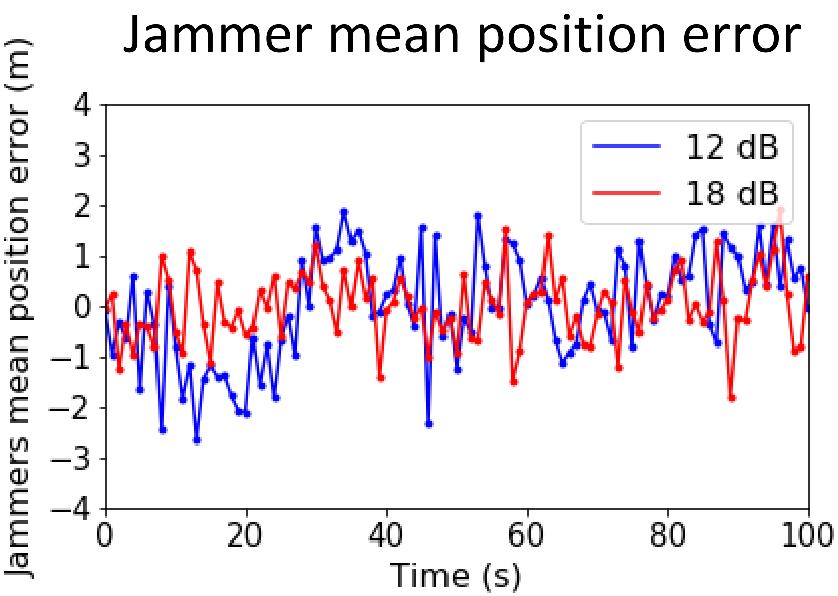


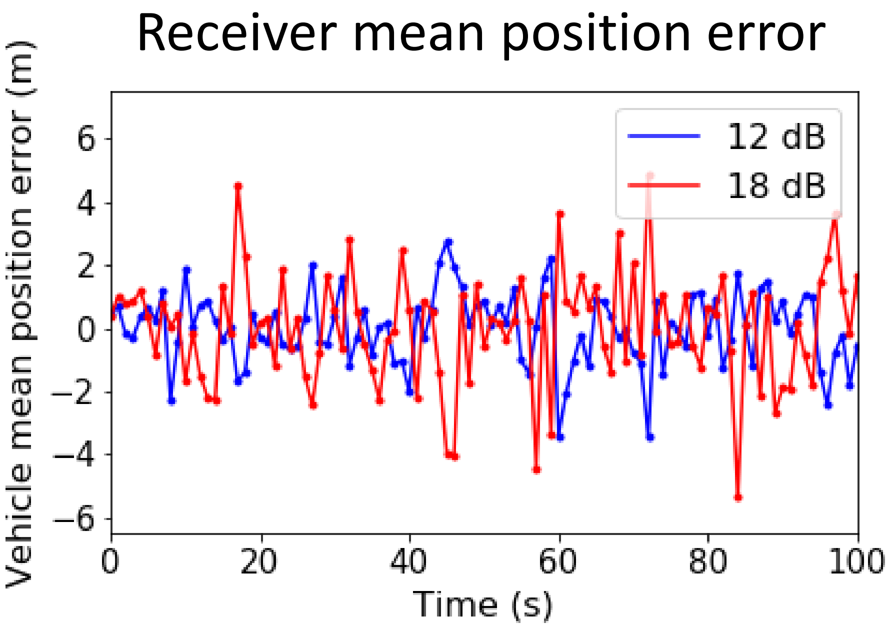
SLMR: Localization Accuracy of Jammers



Number of unknown jammers converges to 3 and positioning error of jammers estimated to within 5 m accuracy

SLMR: Different Levels of Jamming



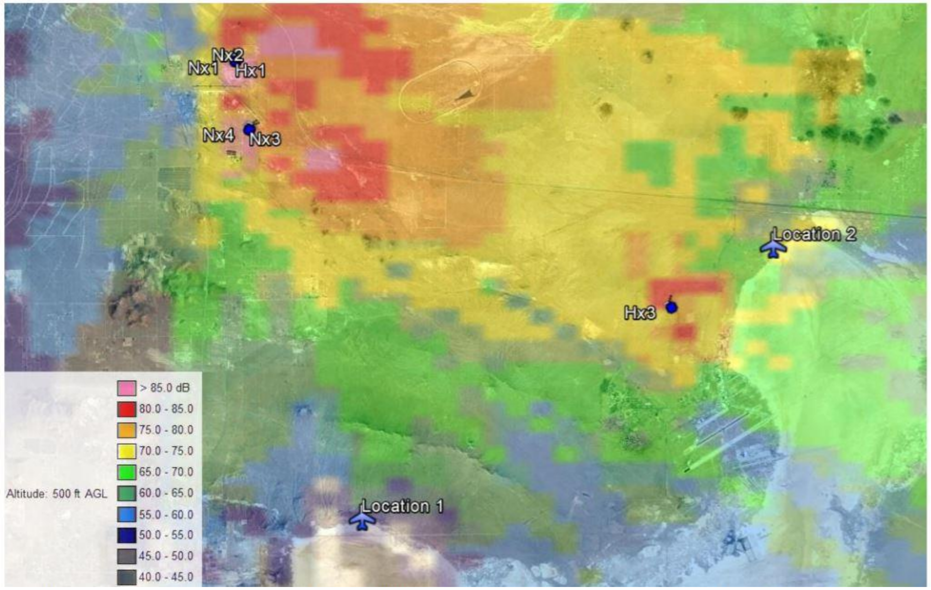


Under $12\ dB$ and $18\ dB$ added jamming,
mean position error of all jammers is within $4.8\ m$ and
mean position error of all receivers is within $5.6\ m$.

Summary

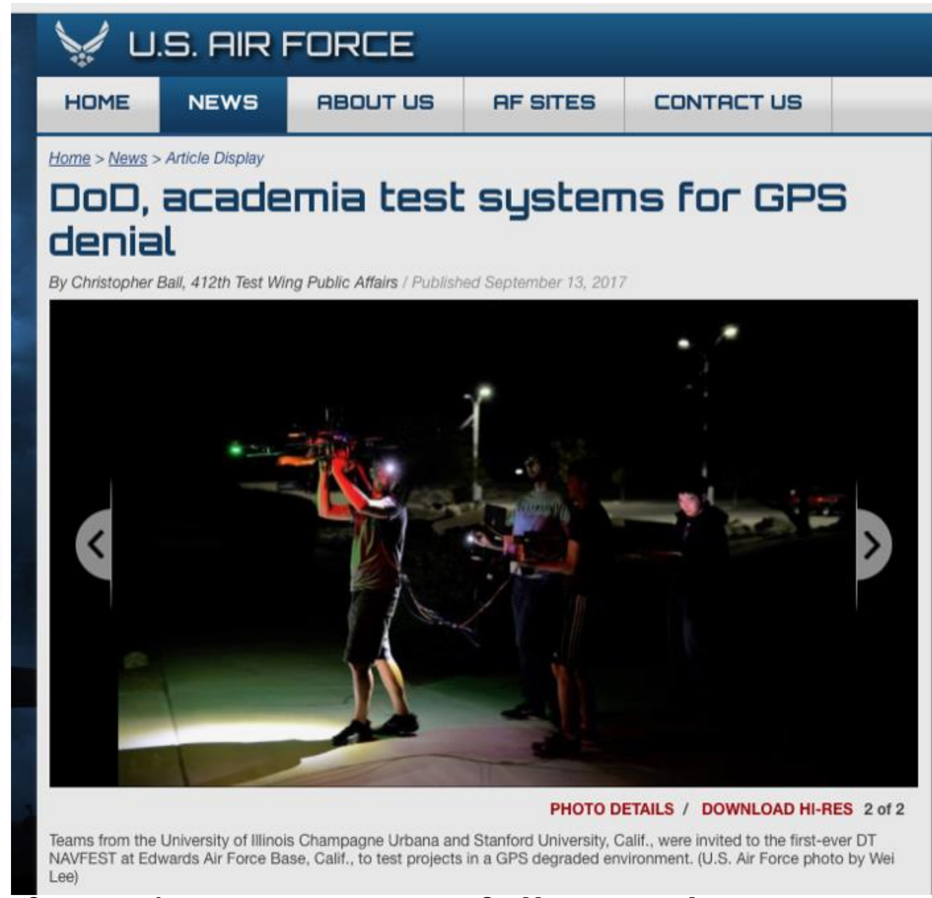
- Demonstrated the impact of GPS jamming attack on the stability of the power grid
- Proposed our Simultaneous Localization of Multiple Jammers and Receivers (SLMR) algorithm
- Demonstrated successful localization of jammers with $5\ m$ accuracy while simultaneously locating receivers with $6\ m$ accuracy under various levels of jamming attack

Future work | DT-NAVFEST Jamming Event



Heatmap of jammer to signal ratio

[Perkins et.al, ION GNSS 2017]



Teams from the **University of Illinois Champaign Urbana** and Stanford University, CA were invited to the first-ever DT NAVFEST at Edwards Air Force Base, CA, to test projects in a GPS degraded environment (U.S. Air Force photo by Wei Lee)

Our Published Work

- Position-Information Aided Vector Tracking *[Chou, Heng and Gao ION GNSS 2014]*
- Multi-Receiver Position-Information Aided Vector Tracking *[Chou, Ng and Gao ION ITM 2015]*
- Advanced Multi-Receiver Position-Information Aided Vector Tracking *[Chou, Ng and Gao ION GNSS+ 2015]*
- Direct Time Estimation *[Ng and Gao IEEE PLANS 2016]*
- Multi-Receiver Direct Time Estimation for PMUs *[Bhamidipati, Ng and Gao ION GNSS+2016]*
- Spoofer Localization based Multi-Receiver Direct Time Estimation *[Bhamidipati and Gao ION GNSS+2017]*
- Improved Jamming Resilience using Position-Information Aided Vector Tracking *[Bhamidipati and Gao ION GNSS 2017]*
- Simultaneous Localization of Multiple Jammers and Receivers using Probability Hypothesis Density *[Bhamidipati and Gao ION PLANS 2018]*

Acknowledgement

My sincere gratitude to my advisor, Prof. Grace Xingxin Gao, for her guidance and continuous support.

I would also like to thank Cyber Resilient Energy Delivery Consortium (CREDC) team members at University of Illinois: Alfonso Valdes, Prosper Panumpabi, Jeremy Jones, David Emmerich for setting up the power grid testbed and collecting the data.

Thank You

Contact info: sbhamid2@Illinois.edu

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security