Robust GPS-based Timing for Phasor Measurement Units

Grace Xingxin Gao

How to Make GPS Timing Robust?

Facts about GPS

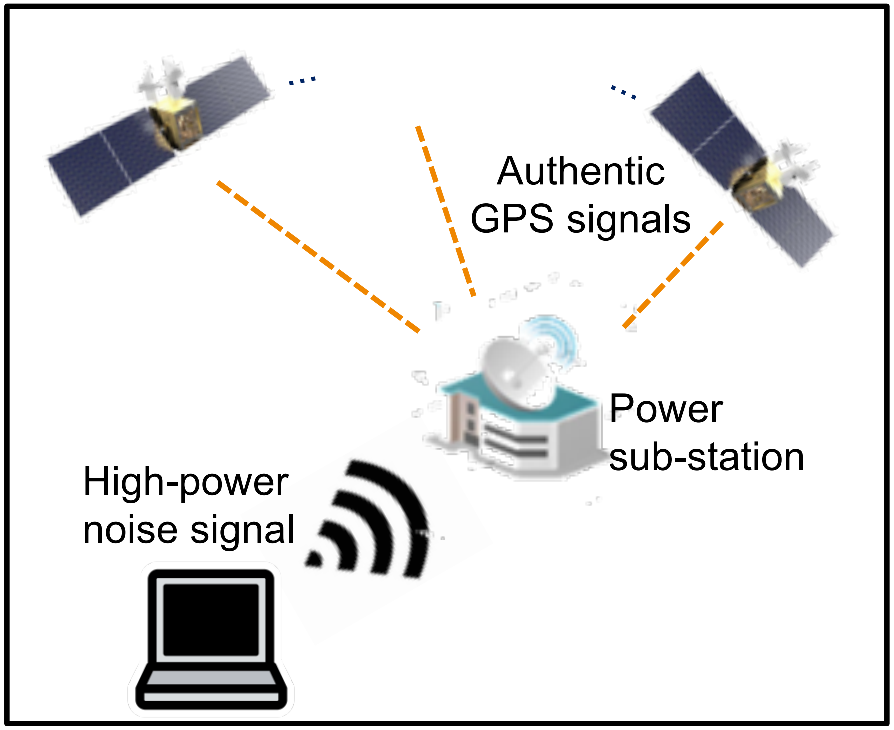
- GPS provides timing for many applications, such as PMUs
- GPS civil signals are unencrypted
- GPS civil signal structures are completely open
- GPS received signals are extremely weak
- GPS is a legacy system

GPS Time for PMUs

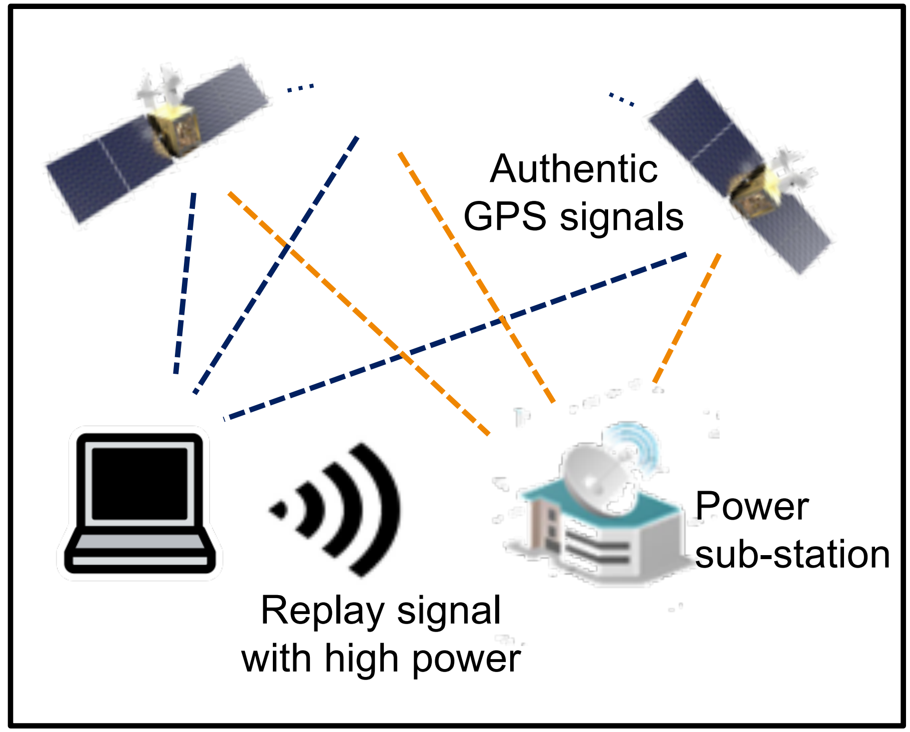
- Free, readily available GPS civilian signal
- <100ns time synchronization
- Wide area coverage

Risks	Goals
Noise, Jamming	Robustness against Interference
Multipath, Meaconing	
Data-level Spoofing	Spoofing detection
Receiver Errors	Accurate and Precise Time

Examples of GPS Timing Attacks

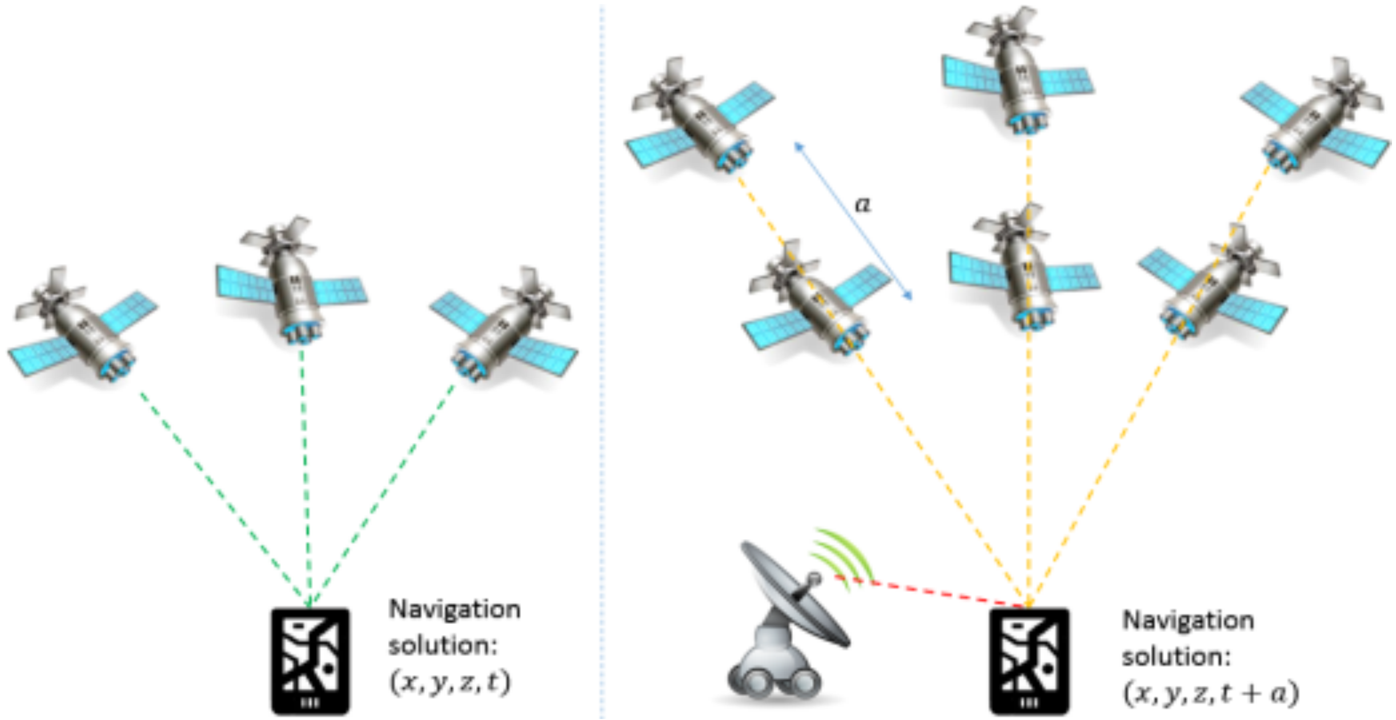


Jamming: Timing for PMU made unavailable



Meaconing: Mislead PMU with wrong time

Example Cont'd: Data-Level Spoofing



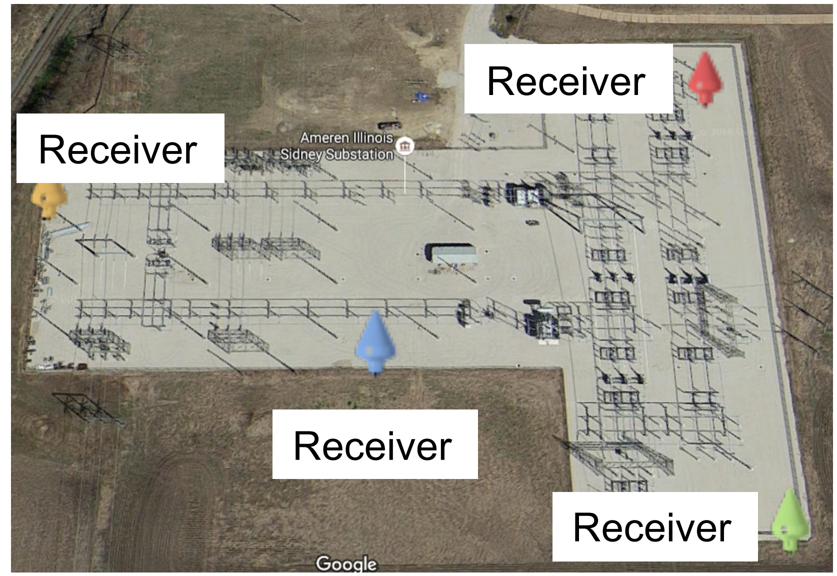
Attacked af_0 in Subframe 1 of Ephemerides → ephemerides

Outline

- Local-area robust GPS timing
  - Approach
  - Implementation
  - Results
- Wide-area robust GPS timing
  - Pairwise check
  - Decision aggregation
  - Results
- Summary

Local-Area Approach: Multi-Receiver Position Aiding

- Multiple receivers
  - Geographical diversity
- Position Aiding
  - Static receiver location
- Direct Time Estimation (DTE)
  - Directly works in time domain
  - No intermediate pseudoranges
- Vector Tracking
- Triggered by a common external clock



Power substation, Sidney, IL

Improved Redundancy

Tracking Scheme	Scalar	SRVT	SRPIAVT	MRDTE
Tracking Entities	N x 4 Channels	4 Receivers	4 Receivers	1 Network
Number of Unknowns	N x 4 x 4	4 x 8	4 x 2	1 x 2

N Channels
4 Receivers
4 Unknowns
$[\phi_{carr} \ \phi_{code} \ f_{carr} \ f_{code}]$

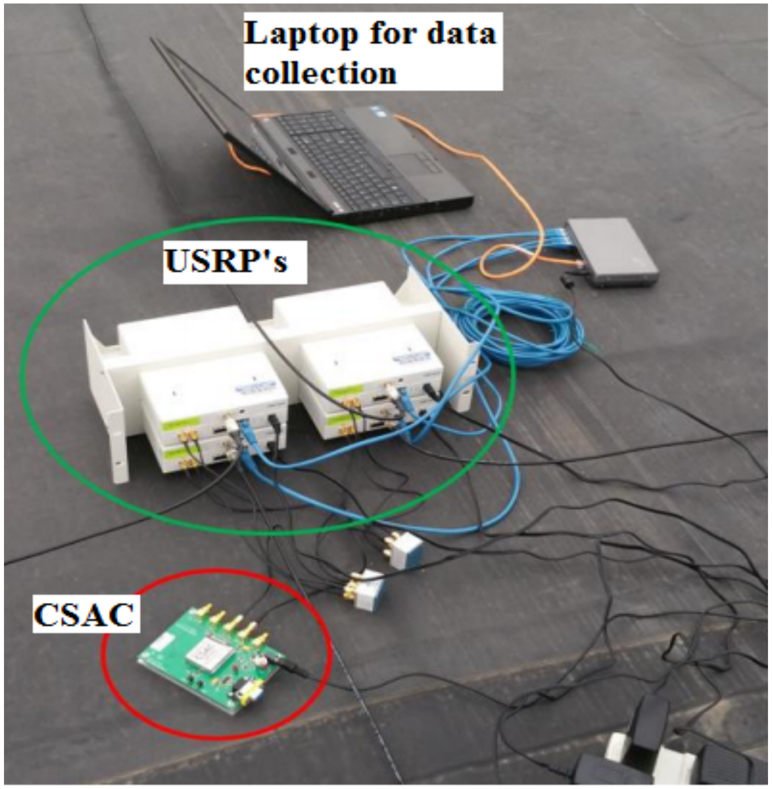
4 Receivers
8 Unknowns
$[x \ y \ z \ c\delta t \ \dot{x} \ \dot{y} \ \dot{z} \ c\dot{\delta t}]$

4 Receivers
2 Unknowns
$[c\delta t \ c\dot{\delta t}]$

1 Network
2 Unknowns
$[c\delta t \ c\dot{\delta t}]$

Search Space ↓| Redundancy ↑| Robustness ↑

Implementation



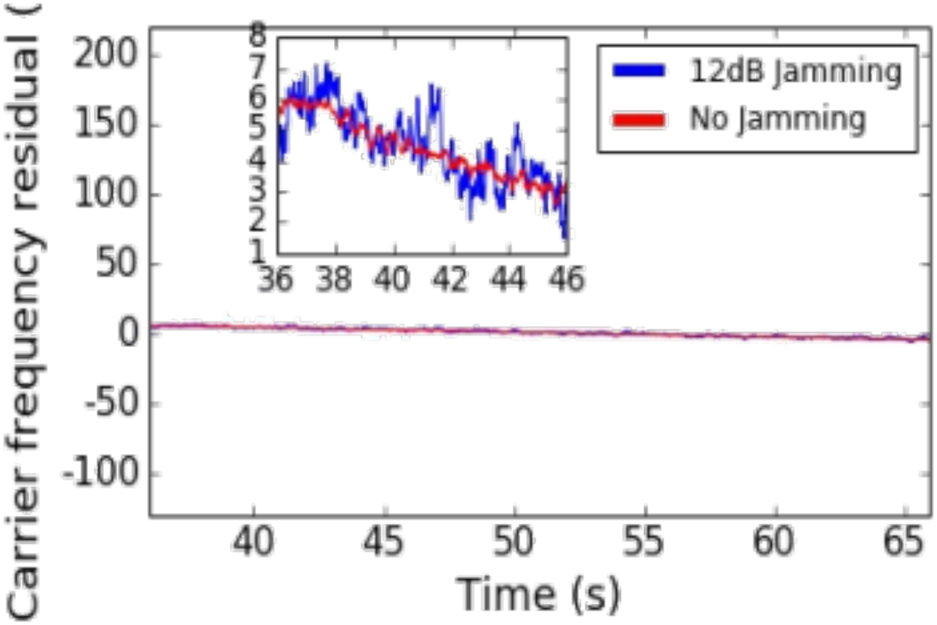
- 4 receivers on the rooftop of Talbot Lab, Urbana, Illinois

For processing the data: pyGNSS - object oriented python platform developed by our lab

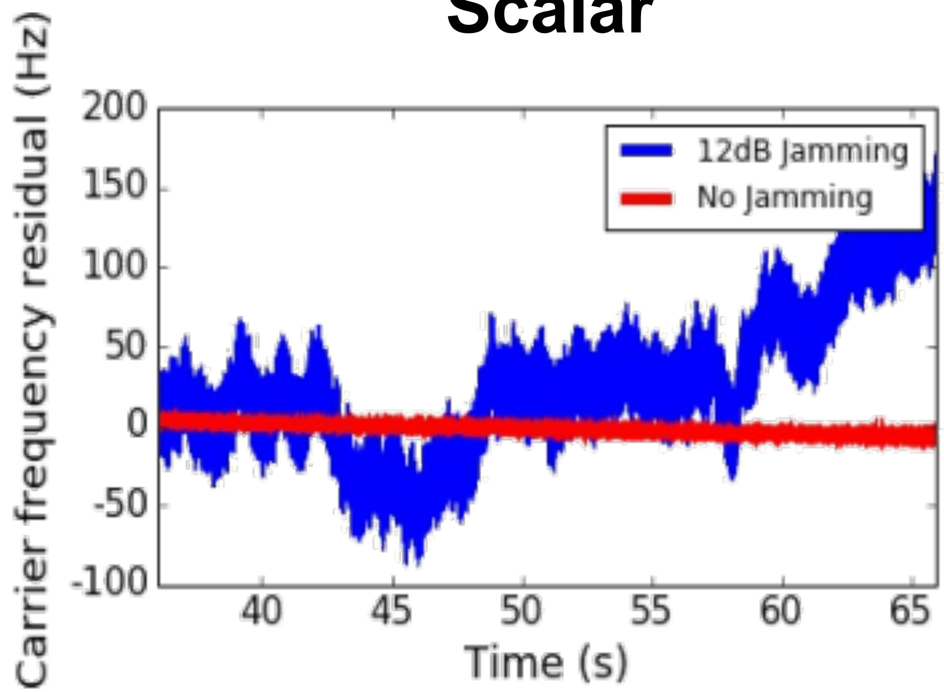
4 USRP's triggered by Chip Scale Atomic Clock (CSAC)

Jamming: Carrier frequency

MRDTE



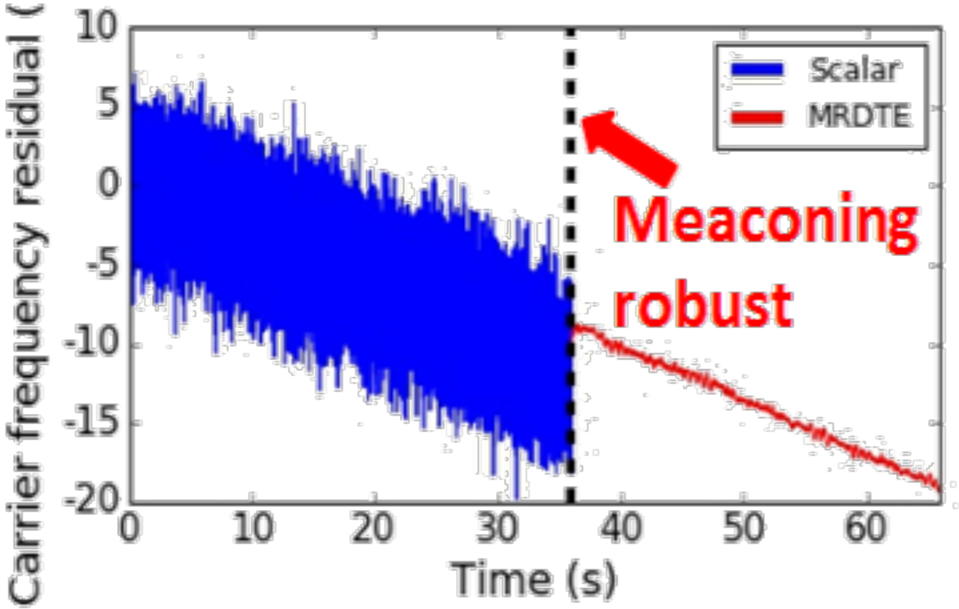
Scalar



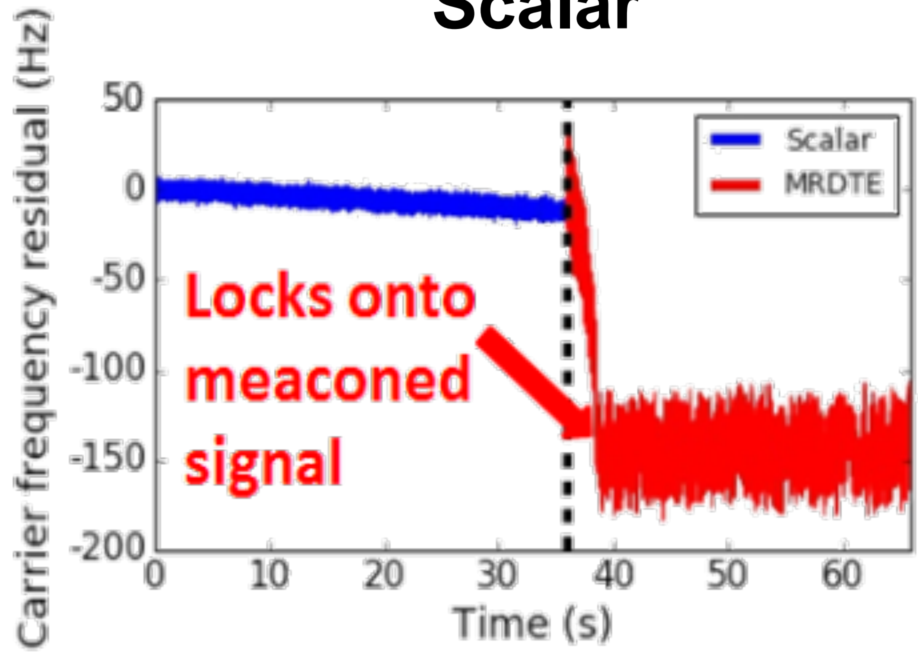
MRDTE (loses track at 17dB added jamming)
offers **5dB** more noise tolerance than
Scalar Tracking (loses track at 12dB added jamming)

Meaconing:

MRDTE



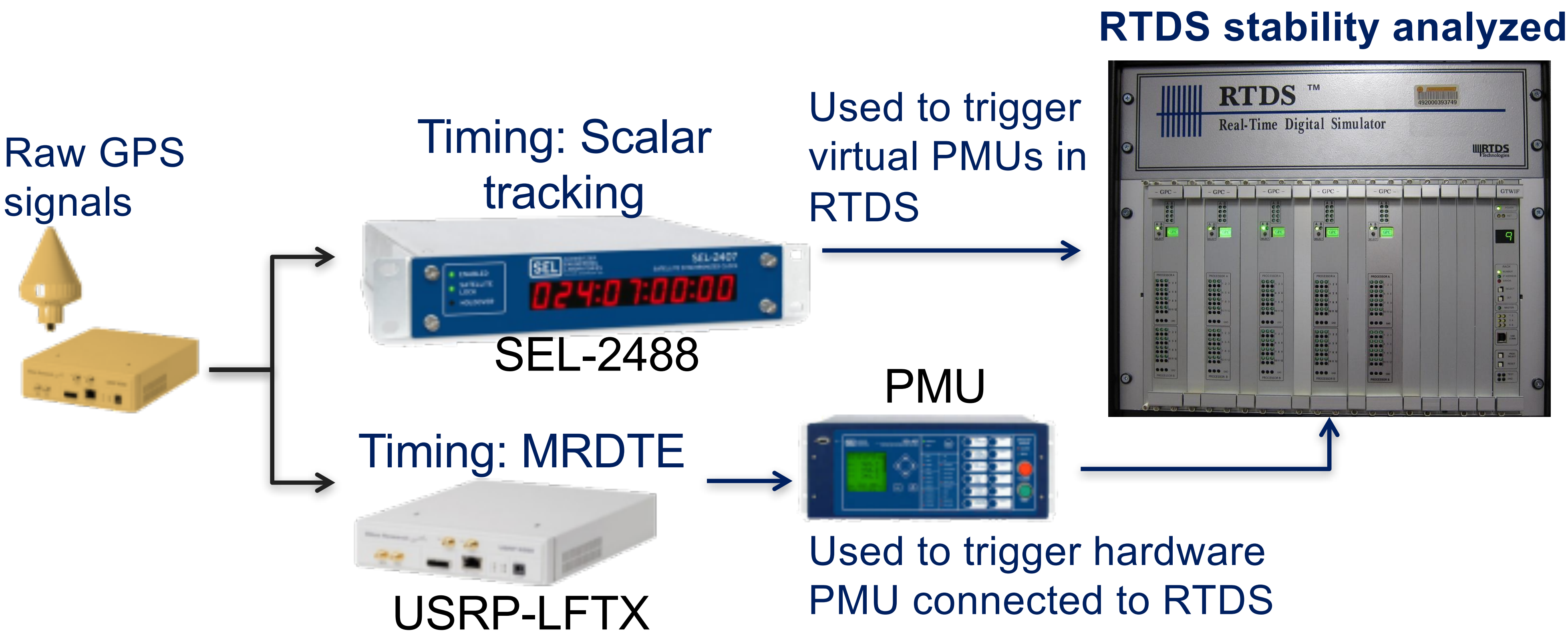
Scalar



Scalar tracking is operational until **2dB** of added meaconed signal while MRDTE is operational till **5dB**

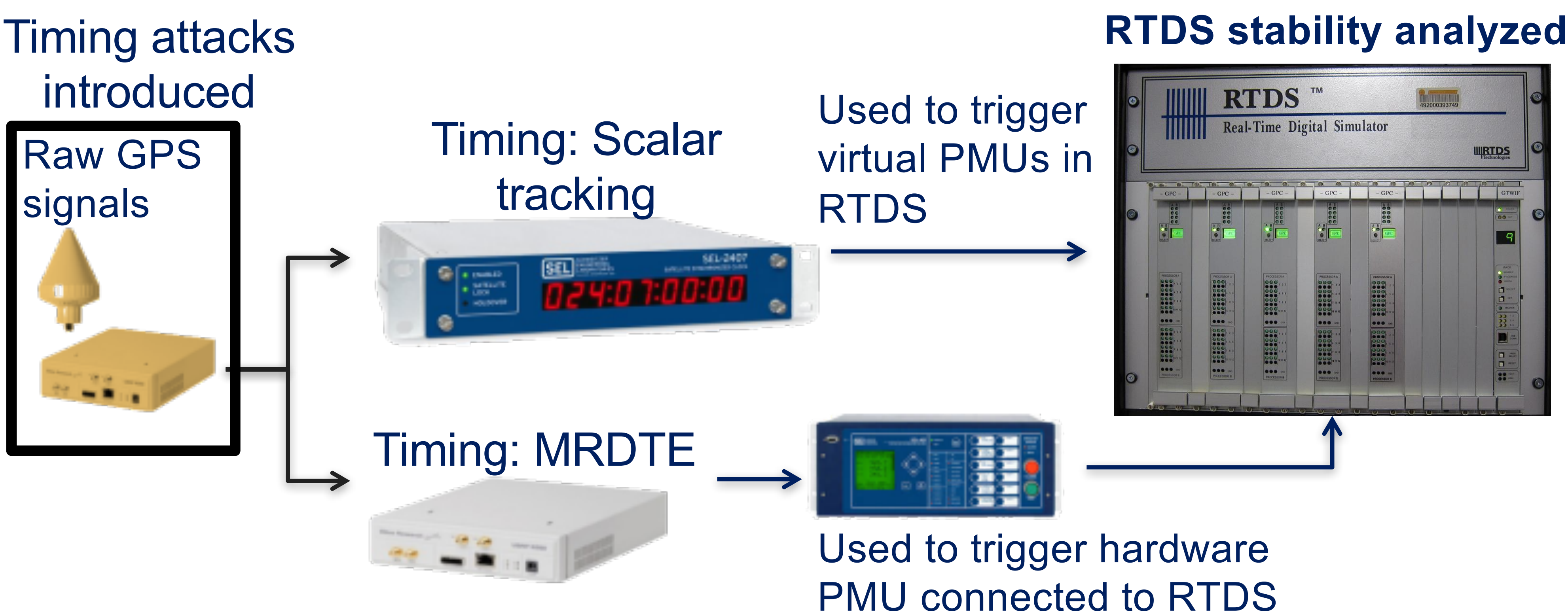
Ongoing Efforts: Impact on Power Systems

- Raw GPS signals are supplied to SEL-2488 (external clock) to trigger virtual PMU and the hardware PMU is triggered using our MRDTE algorithm.



Ongoing Efforts: Impact on Power Systems

- Timing attacks are simulated and added to the raw GPS signals being supplied to the SEL-2488 and USRP-LFTX.



Transforming GPS Time to IRIG-B

- Generated the IRIG-B000 timing pulse: Input to PMU
- Created a voltage shifter to convert the transmitted USRP-LFTX 0-1v IRIG-B signal to 0-5v IRIG-B000 signal

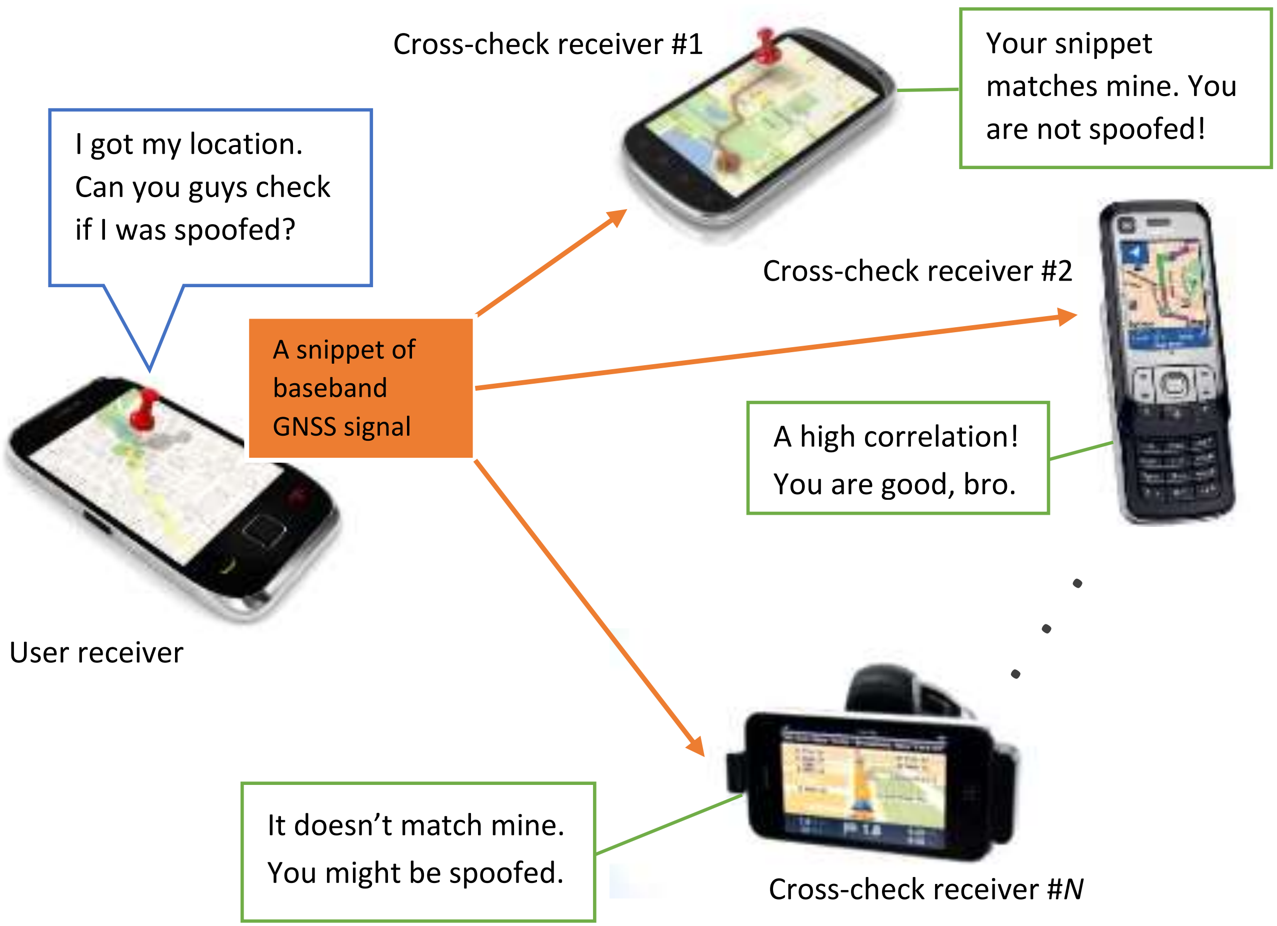
0-1v
IRIG-B000

0-5v
IRIG-B000

Outline

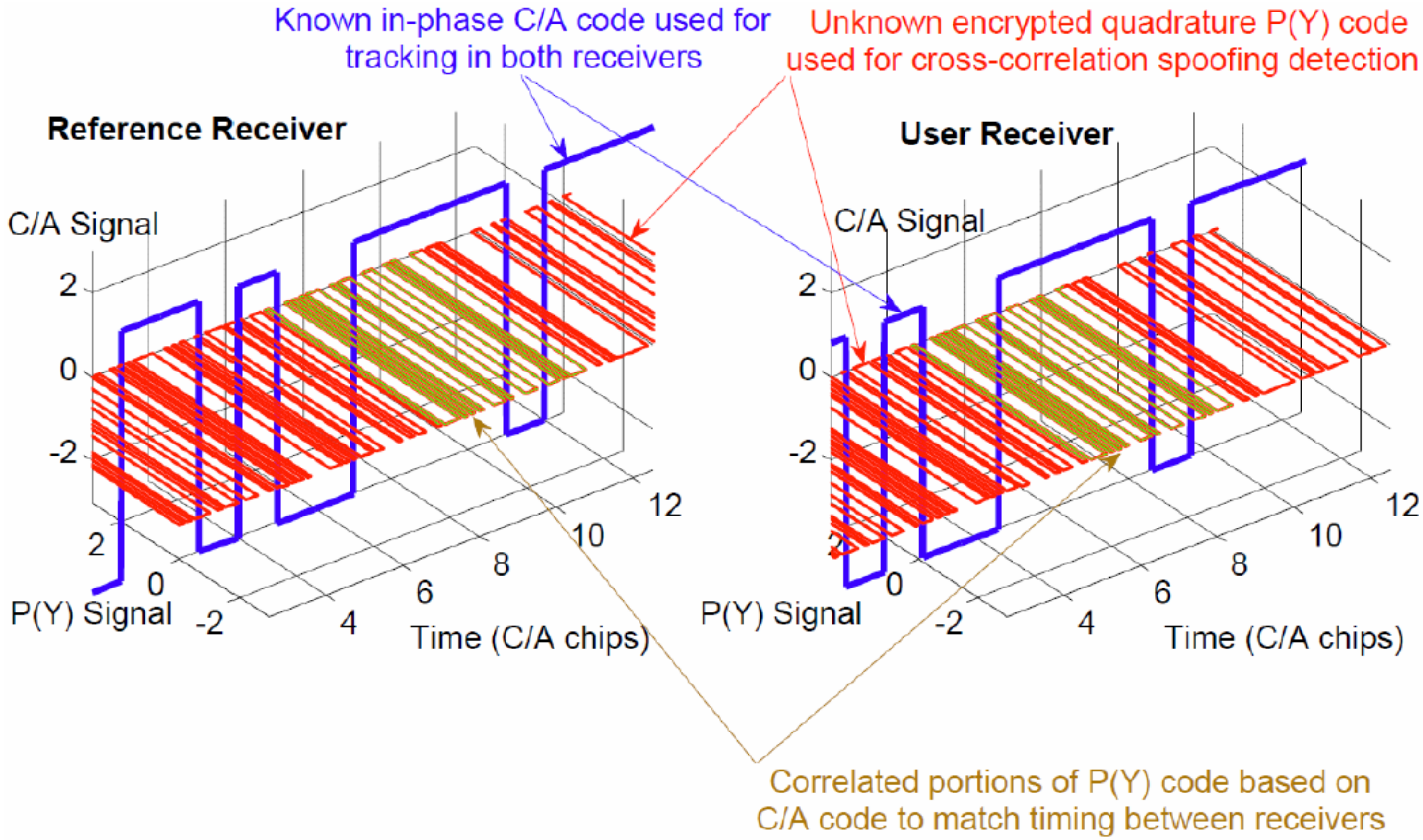
- Local-area robust GPS timing
  - Approach
  - Implementation
  - Results
- Wide-area robust GPS timing
  - Pairwise check
  - Decision aggregation
  - Results
- Summary

Cooperative Authentication: Architecture



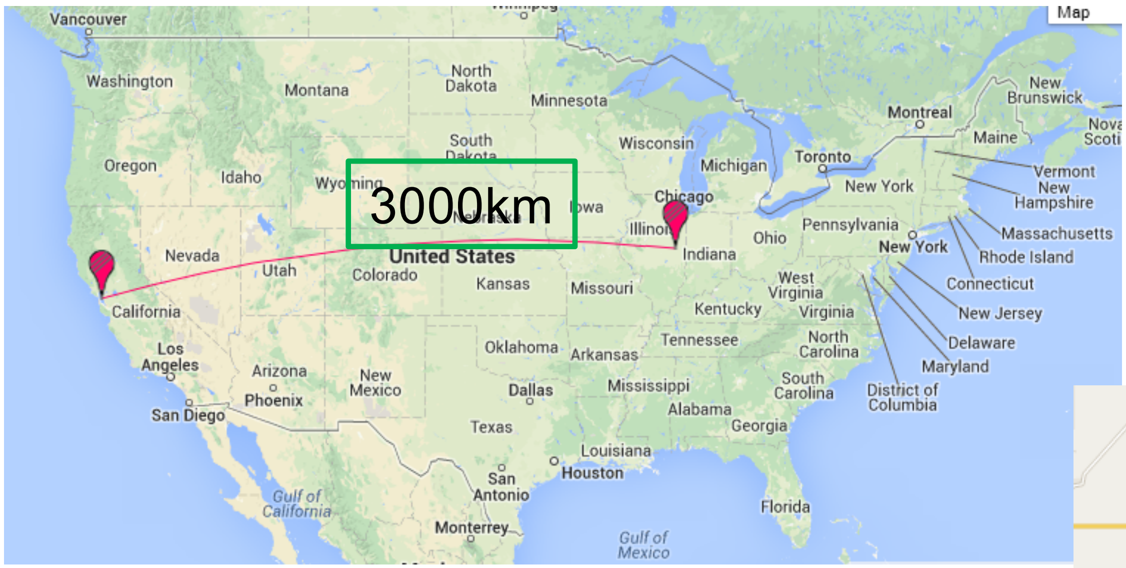
Merits: ***network*** and ***geographical*** redundancy

Pair-wise Checking: Cross-correlation of P(Y) Code

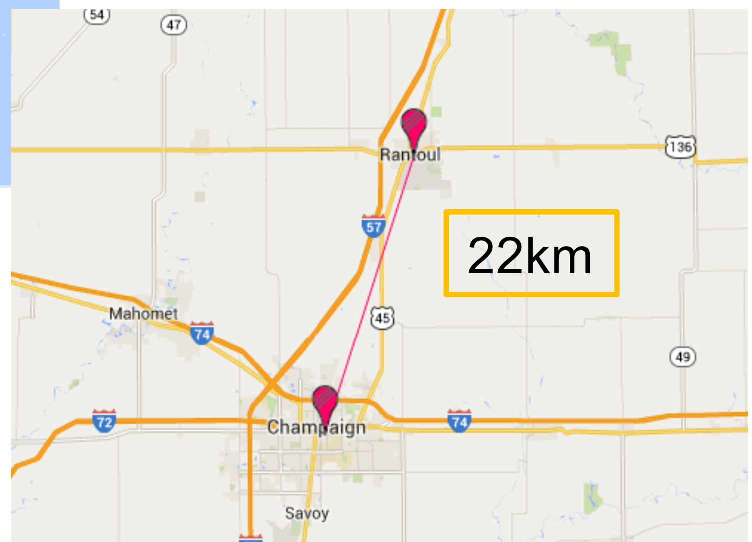


Lo *et al.*, 2009
Psiaki, Humphreys *et al.*, 2013

Experiments Scenarios

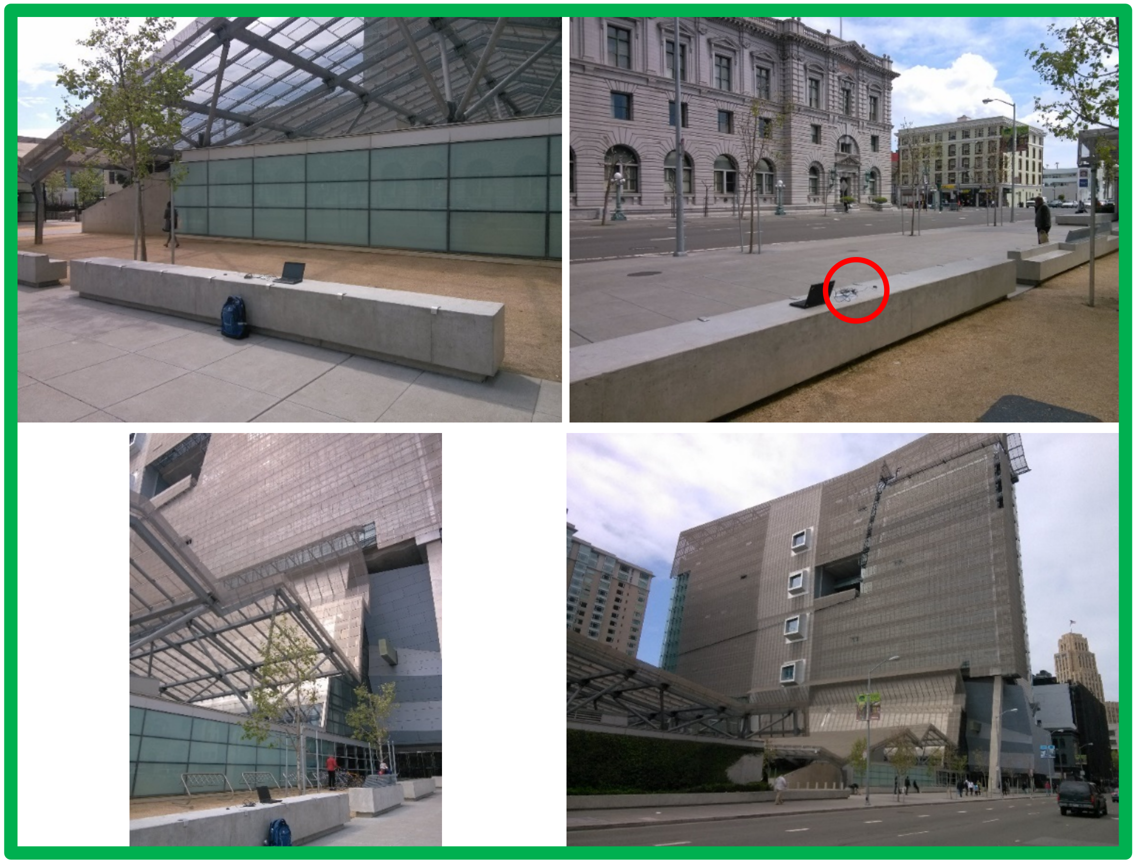


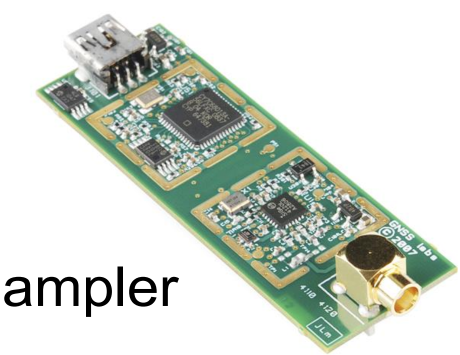
San Francisco CA and Champaign IL, static



Rantoul IL, moving at ~45 mph and Champaign IL, static

Experiments:
San Francisco & UIUC Everitt Lab

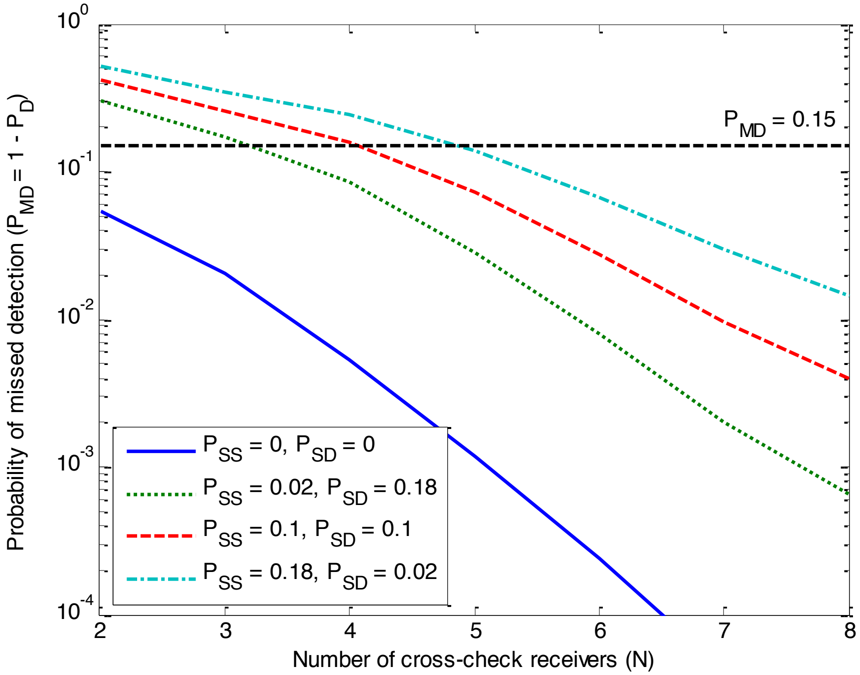




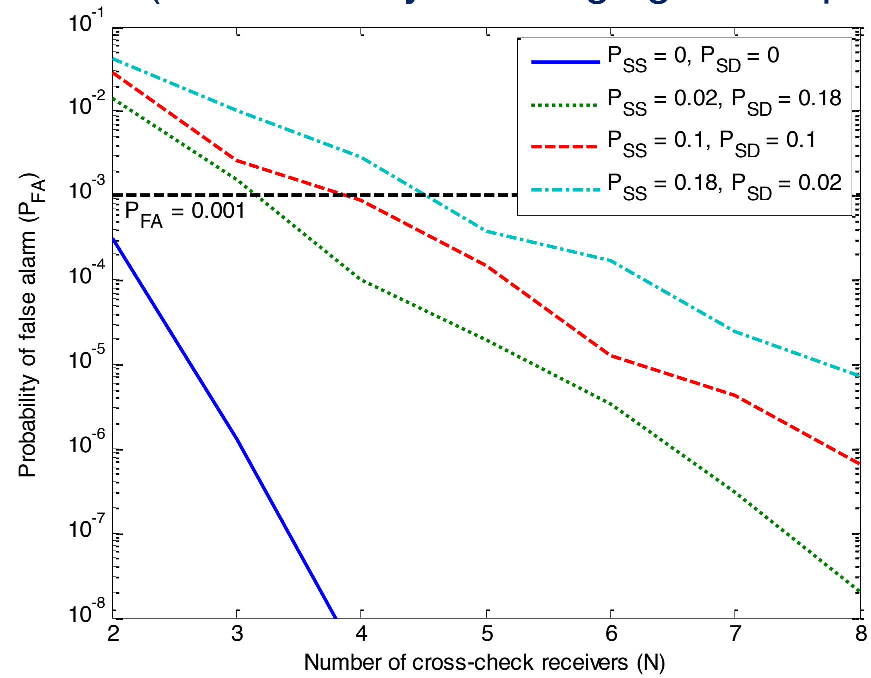
SiGe Sampler

Performance of Cooperative Authentication

Assume 20% of the cross-check receivers are spoofed (an extremely challenging assumption)



Probability of missed detection



Probability of false alarm

- Robustness grows ***exponentially*** with the number of cross-check receivers
- A small number of unreliable cross-check receivers are on par with a reliable cross-check receiver.

Summary

- Local-area robust GPS timing
  - Multi-Receiver Direct Time Estimation
  - Robust against jamming and meaconing attacks
- Wide-area GPS authentication
  - Cooperative authentication
  - Robustness increases exponentially with the number of cross-check receivers

List of Our Prior Work

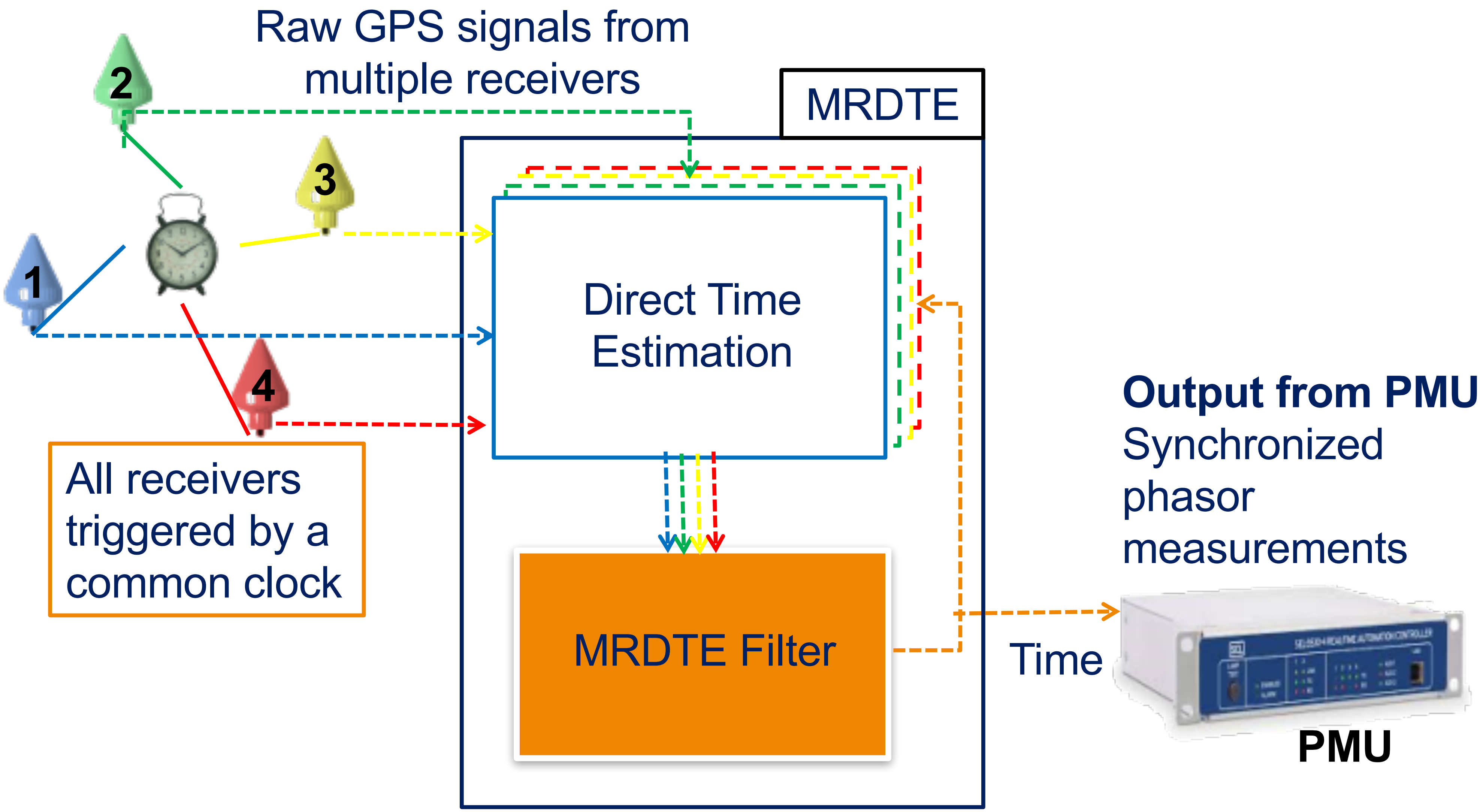
- Sriramya Bhamidipati, Yuting Ng and Grace Xingxin Gao, **Multi-Receiver GPS-based Direct Time Estimation for PMUs**, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2016), Portland OR, Sep 2016, ***Best Presentation of the Session Award***.
- Yuting Ng and Grace Xingxin Gao, **Robust GPS-Based Direct Time Estimation for PMUs**, in Proceedings of the IEEE/ION PLANS conference, Savanah GA, Apr 2016.
- Yuting Ng and Grace Xingxin Gao, **Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs**, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2015), Tampa FL, Sep 2015, ***Best Paper of the Session Award***.
- Liang Heng, Daniel B. Work, and Grace Xingxin Gao, **GNSS Signal Authentication from Cooperative Peers**, *IEEE Intelligent Transportation Systems.* vol. 16, no. 4, pp. 1794-1805, Aug. 2015.
- Daniel Chou, Yuting Ng, and Grace Xingxin Gao, **Robust GPS-Based Timing for PMUs Based on Multi-Receiver Position-Information-Aided Vector Tracking,** *ION International Technical Meeting 2015,* Dana Point, California, January 2015.
- Daniel Chou, Liang Heng, and Grace Xingxin Gao , “Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Vector Tracking Approach,” ION GNSS+ 2014, Tampa FL, Sep 2014, ***Best Presentation of the Session Award***.
- Liang Heng, Daniel Chou, and Grace Xingxin Gao , “Cooperative GPS Signal Authentication from Unreliable Peers,” ION GNSS+ 2014, Tampa FL, Sep 2014, ***Best Presentation of the Session Award***.
- Liang Heng, Jonathan Makela, Alejandro Dominguez-Garcia, Rakesh Bobba, William Sanders, and Grace Xingxin Gao, “Reliable GPS-based Timing for Power System Applications: A multi-Layered Multi-receiver Approach,” the 2014 IEEE Power and Energy Conference at Illinois (IEEE PECI 2014), Champaign, IL, Feb 2014.
- Liang Heng, Daniel B. Work, and Grace Xingxin Gao, “Reliability from Unreliable Peers: Cooperative GNSS Authentication,” Inside GNSS Magazine, September–October 2013.

Thank You

This material is based upon work supported by the Department of Energy under Award Number DE-OE000078

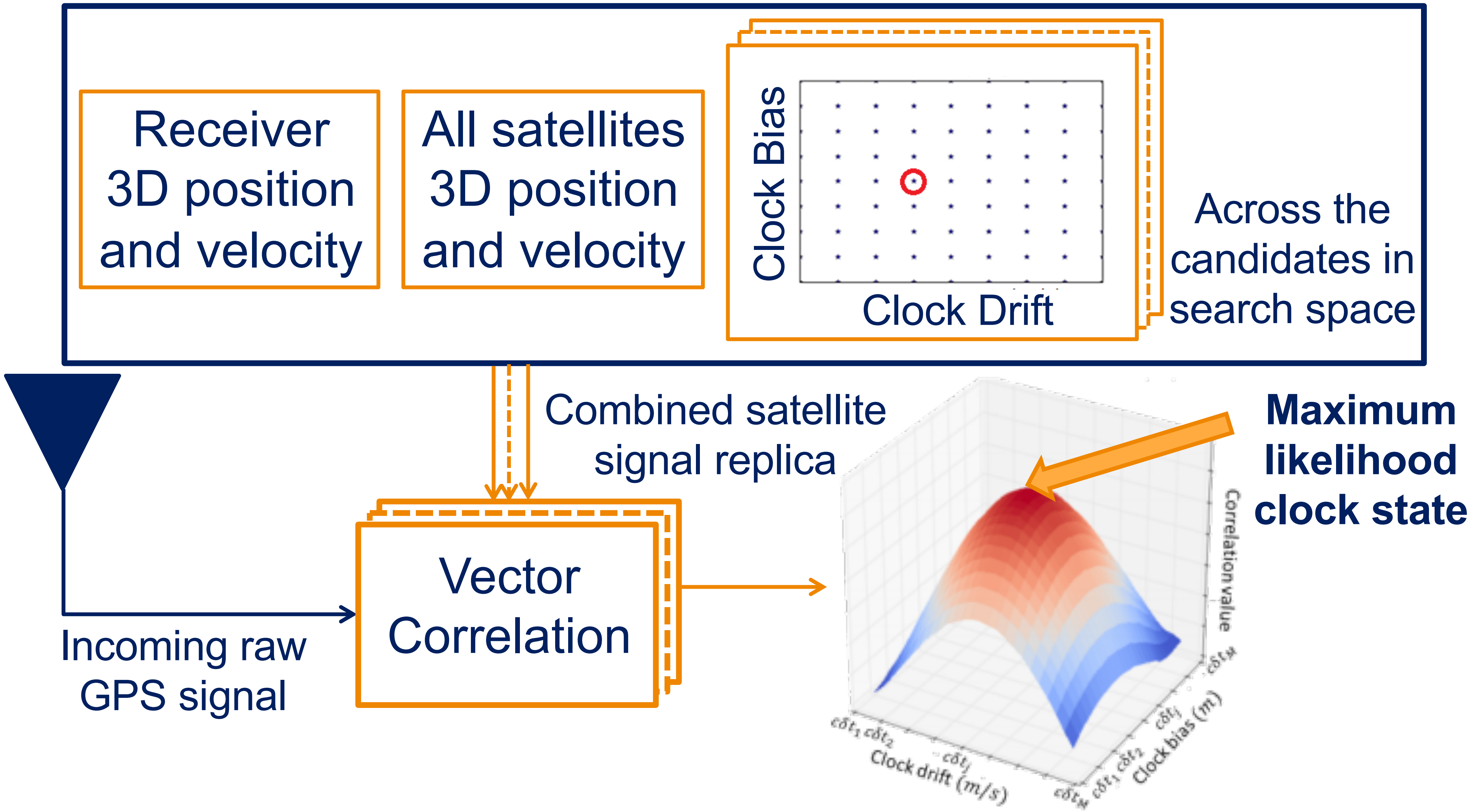
Backup slides

MRDTE: Architecture



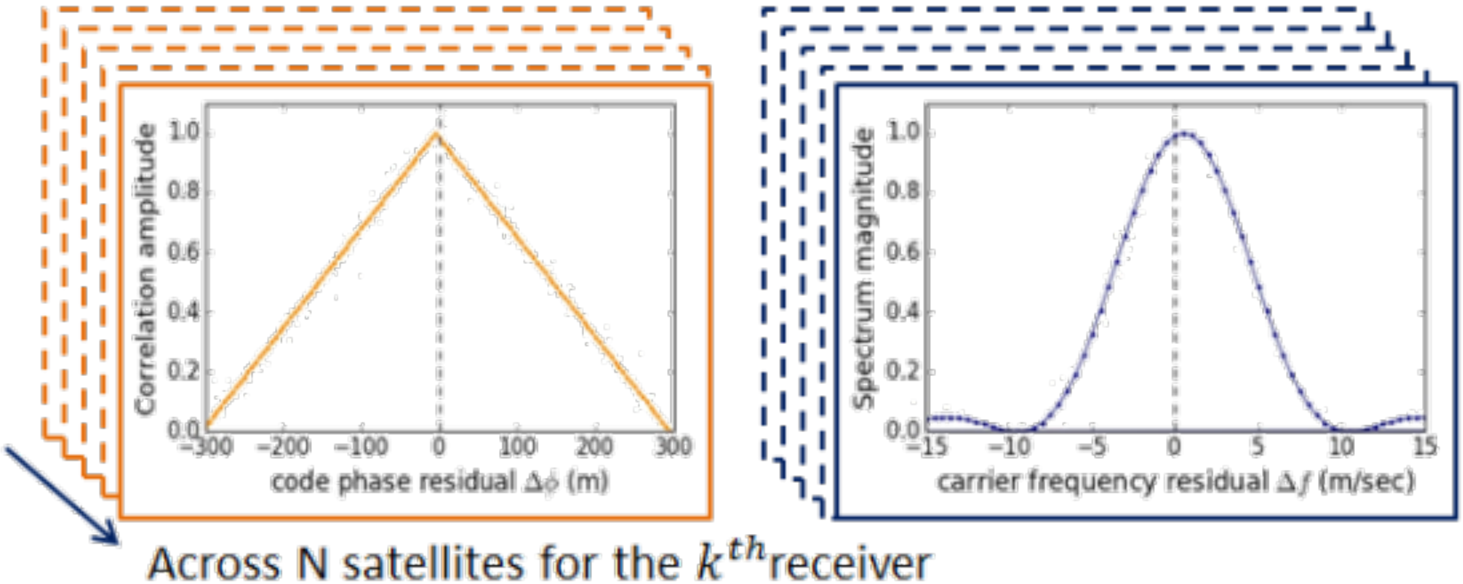
Output from PMU: Synchronized phasor measurements

Direct Time Estimation



Vector Correlation Continued

Direct correlation involves non-coherent summation



- Non-coherent summation across satellites
- Improved signal-to-noise ratio of the system

Pairwise Check

Received GPS signal from one satellite:

$$s(t) = \underbrace{C}_{\text{C/A Code}}(t-\tau)D_C(t-\tau)\sin(2\pi(f+f_D)(t-\tau)+\phi)$$
$$+\underbrace{P}_{\text{P(Y) Code}}(t-\tau)D_P(t-\underbrace{\tau}_{\text{Time Delay}})\cos(2\pi(f+\underbrace{f_D}_{\text{Doppler Frequency}})(t-\tau)+\underbrace{\phi}_{\text{Phase shift}})$$

We want to cross correlate the $P(t)D_P(t)$ signals from two different receivers.

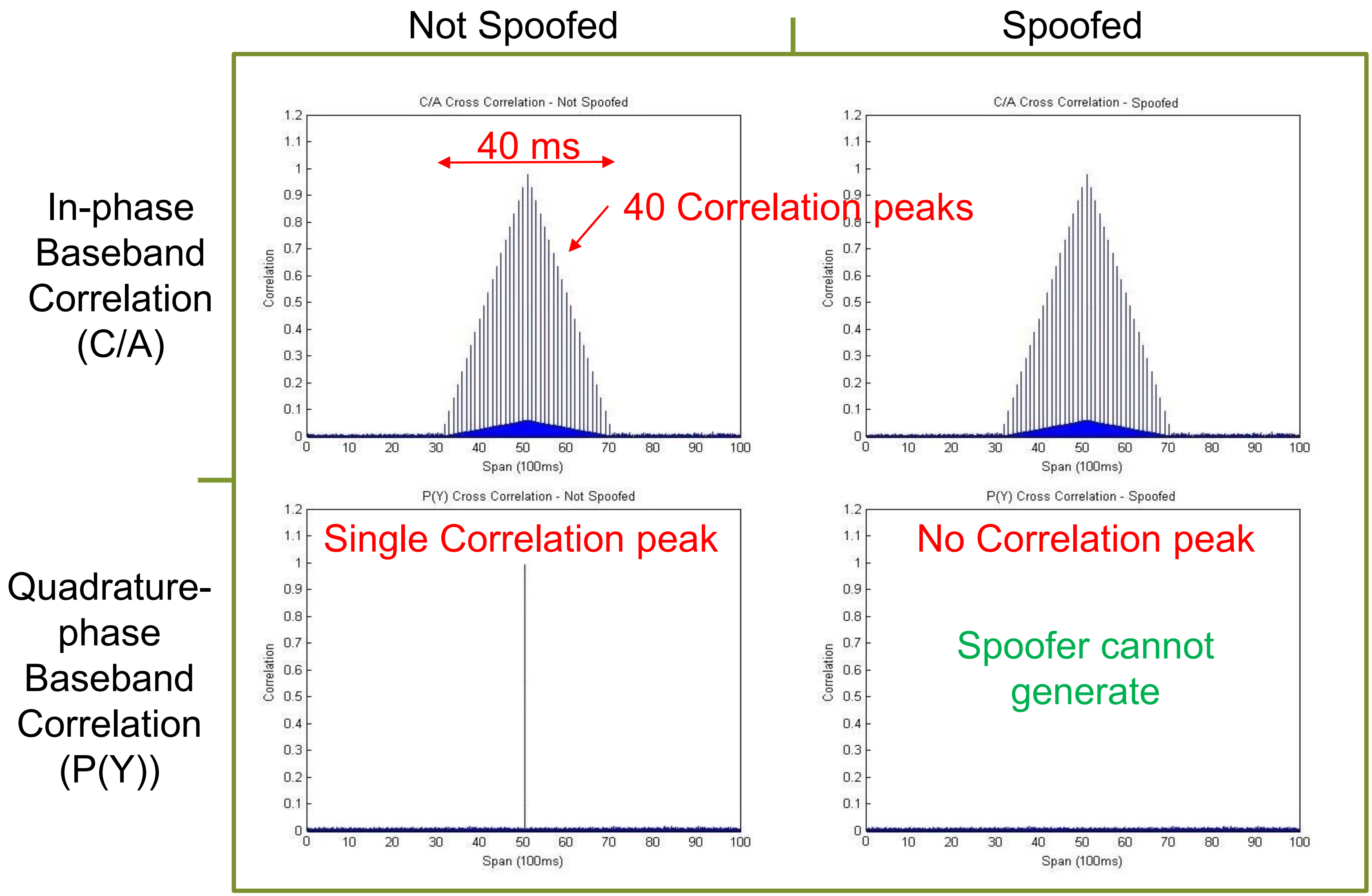
Estimate:

- Doppler frequency, f_D
- Phase shift, ϕ

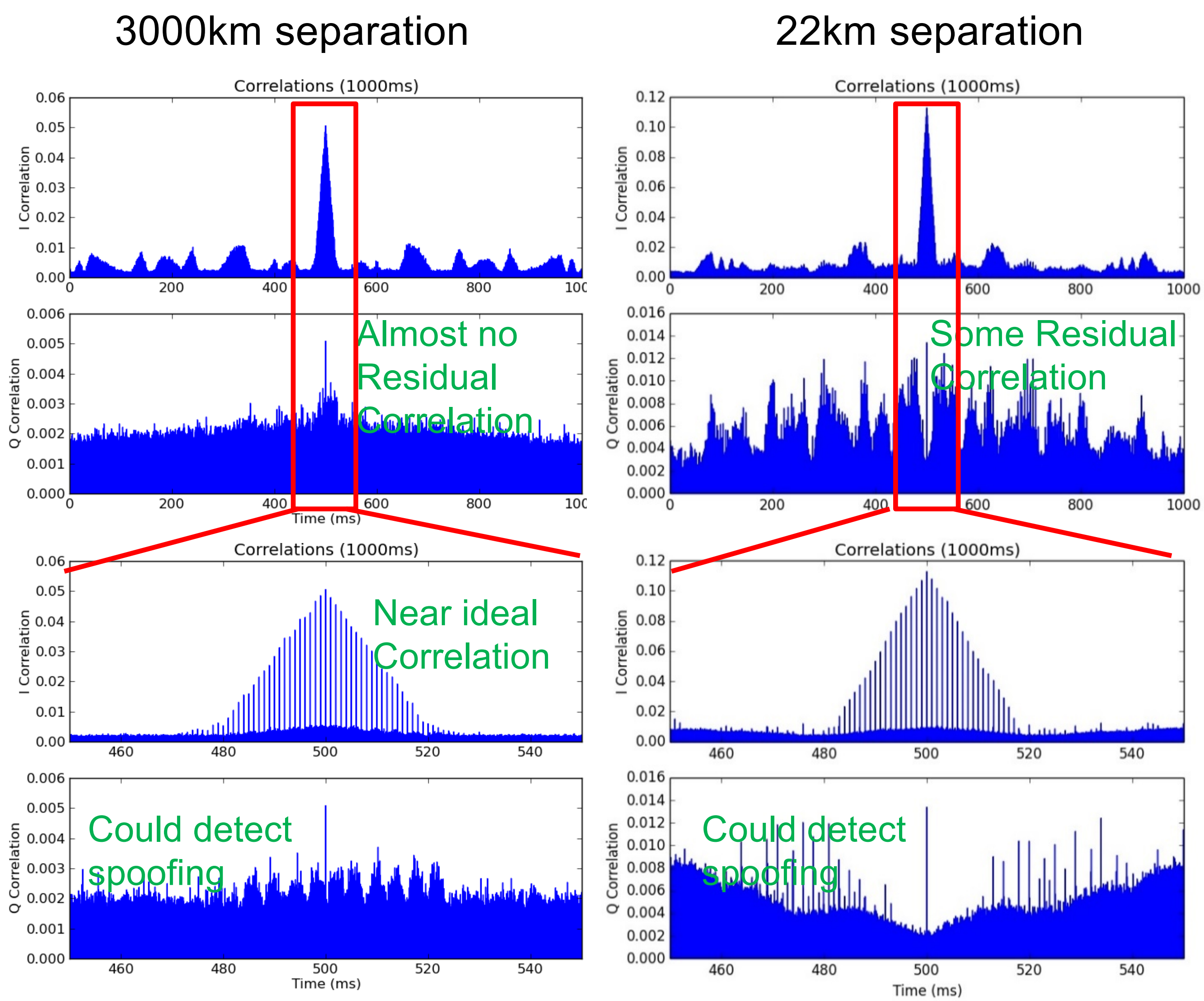
Wipe off Doppler and align phase:

$$P(t-\tau)D_P(t-\tau) = \mathrm{LPF}[\cos(2\pi(f+f_D)(t-\tau)+\phi)\cdot s(t)]$$

Pairwise Check – Ideal Results



Pairwise Results for Different Separations



Modeling Unreliable Cross-Check Receivers

Definition

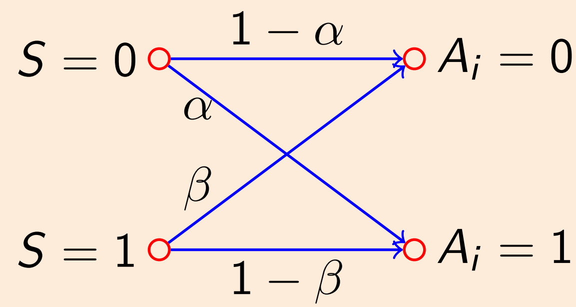
S Actual status of user receiver

A_i Authentication result using the ith cross-check receiver

$= 0$ authentic

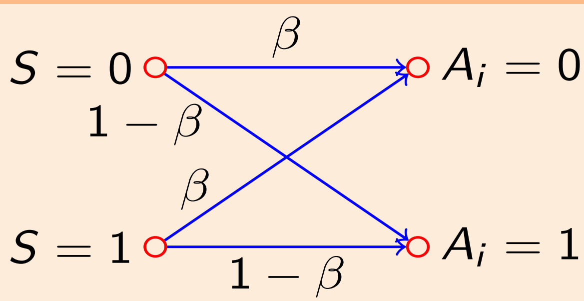
$= 1$ spoofed

Cross-check receiver is authentic



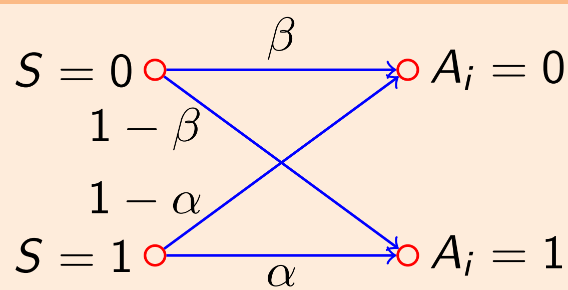
with a probability $1 - P_{SD} - P_{SS}$

Cross-check receiver is spoofed by a different spoofer



with a probability P_{SD}

Cross-check receiver is spoofed by the same spoofer



with a probability P_{SS}

Authentication Performance, Theoretical Results

$$P_{FA} = P_{MD} \leq \exp\left(-N\lambda^2\right).$$

$$\lambda = (1 - \alpha - \beta)(1 - P_{SD} - 2P_{SS}).$$

Pair-wise false alarm rate	Pair-wise missed detection rate	Probability of being spoofed by a different spoofer	Probability of being spoofed by the same spoofer

- Authentication performance improves ***exponentially*** with increasing number of cross-check receivers.
- P_{SS} causes twice as great performance deterioration as P_{SD} does.
  - Choose a cross-check receiver far from the user receiver.