Robust GPS-Based Timing for Phasor Measurement Units

October 3, 2014

Grace Xingxin Gao

University of Illinois at Urbana-Champaign

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

How to Make GPS-based Timing Robust?

Facts about GPS

- GPS provides timing for many applications, such as PMUs
- GPS civil signals are unencrypted
  - Only GPS military signals are encrypted
  - Civil users (e.g. PMUs) do not have access to the military codes
- GPS civil signal structures are completely open
  - GPS civil signal definition is published in its Interface Control Documents (ICD)
- GPS received signals are extremely weak
  - GPS satellites are 20,200 km (12,550 miles) away
- GPS is operational
  - Satellites in orbits
  - Signals being broadcast
  - Billions of GPS receivers in use

Outline

- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation
- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results
- Conclusions

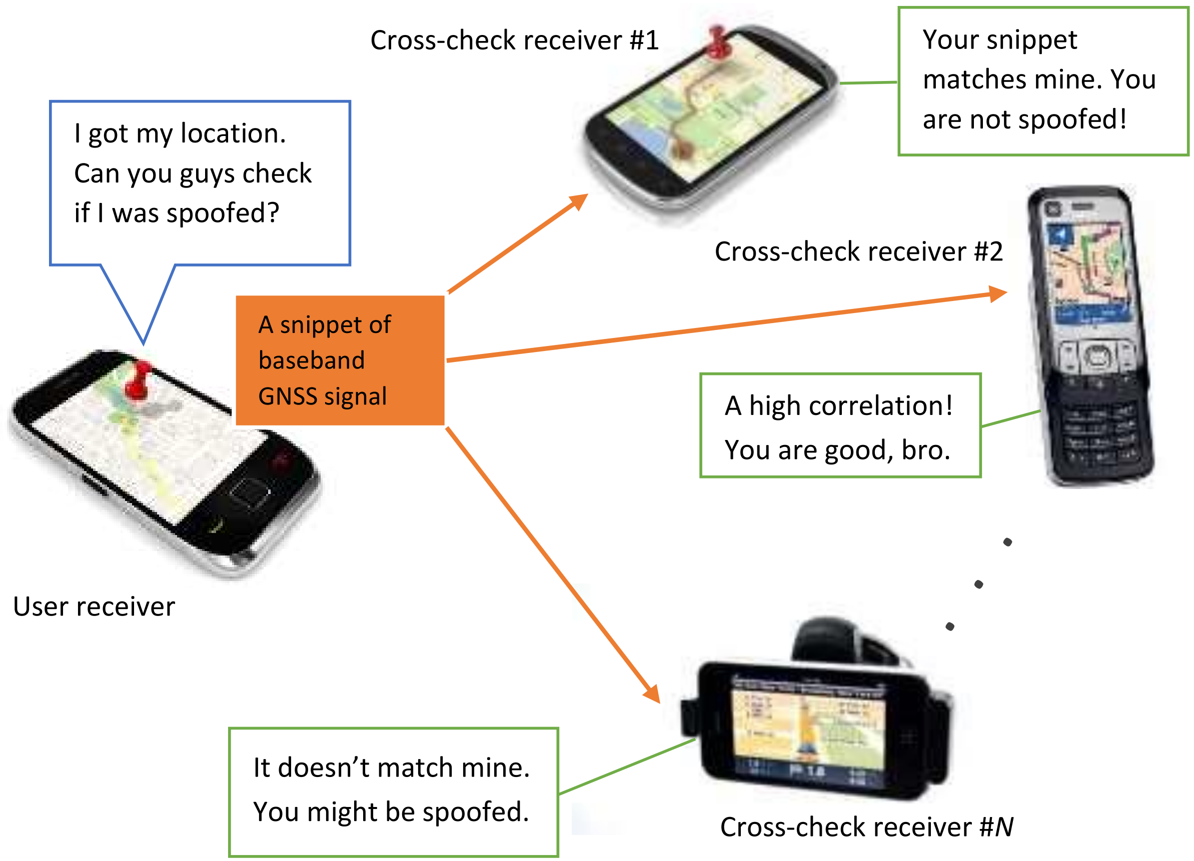
Outline

- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation

- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results

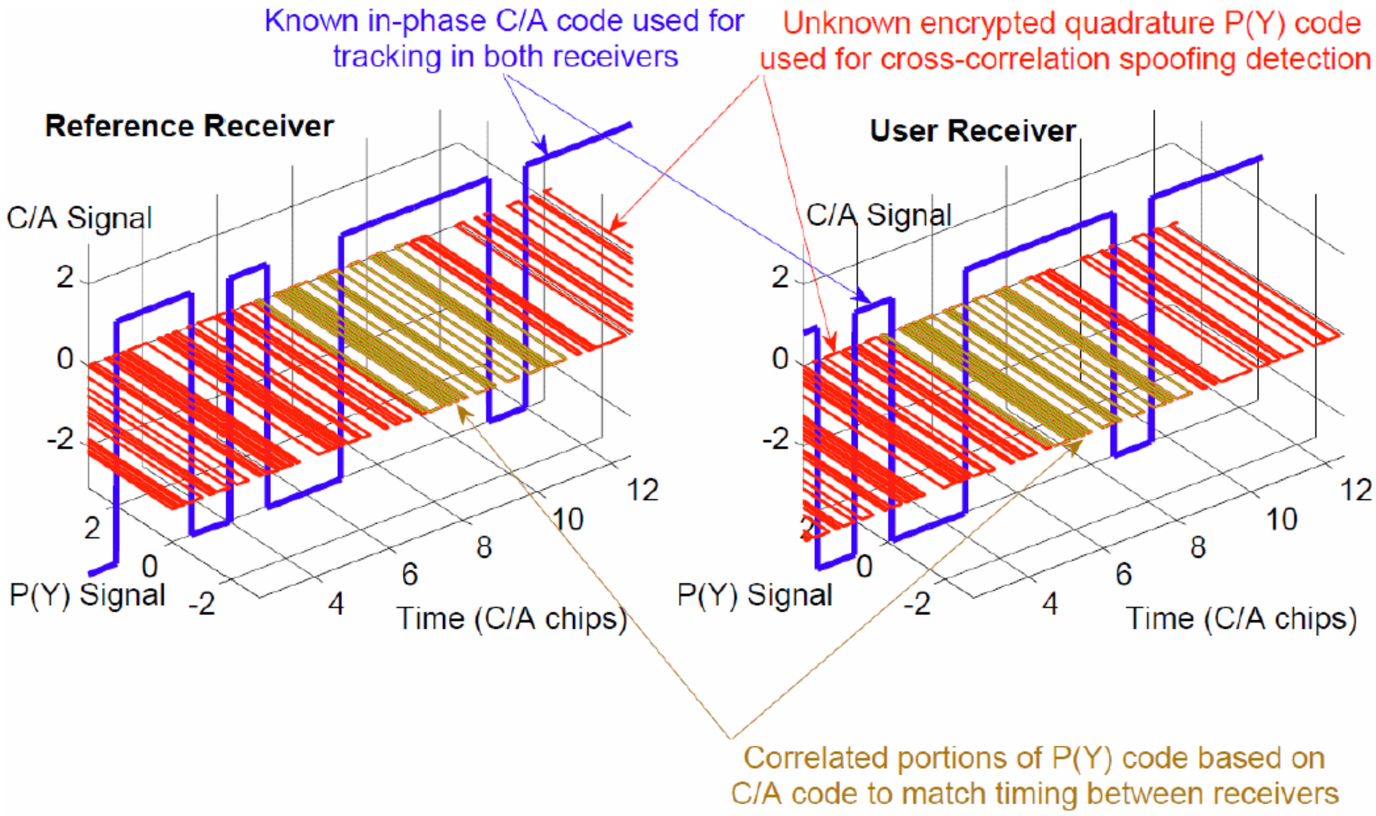
- Conclusions

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

Outline

- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation
- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results
- Conclusions

Pairwise Check

Received GPS signal from one satellite:

$$s(t) = C(t-\tau)D_C(t-\tau)\sin(2\pi(f+f_D)(t-\tau)+\phi)$$
$$+P(t-\tau)D_P(t-\tau)\cos(2\pi(f+f_D)(t-\tau)+\phi)$$

C/A Code | P(Y) Code | Time Delay | Doppler Frequency | 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:

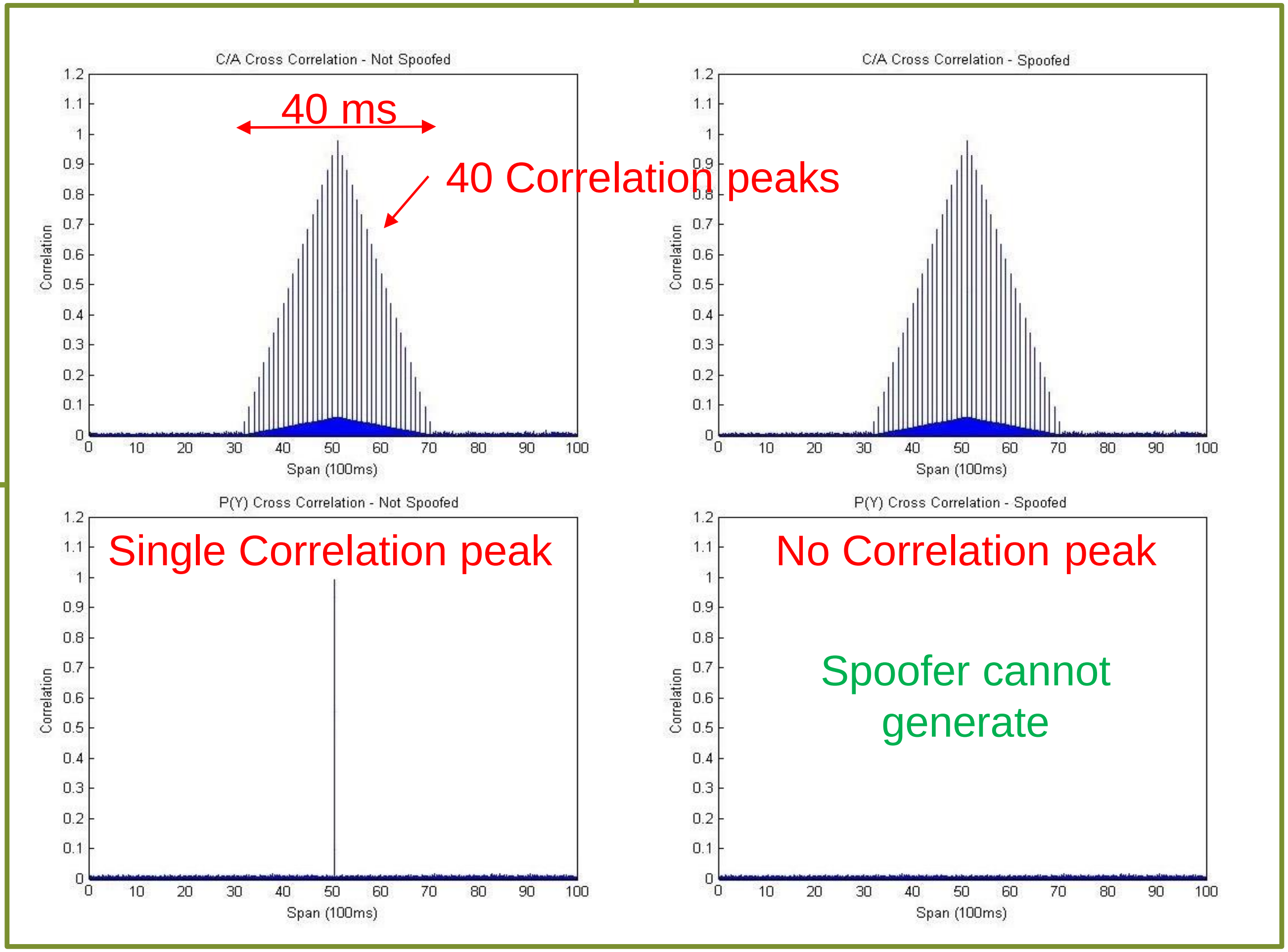
$$P(t-\tau)D_P(t-\tau) = \text{LPF}[\cos(2\pi(f+f_D)(t-\tau)+\phi)\cdot s(t)]$$

Pairwise Check – Ideal Results

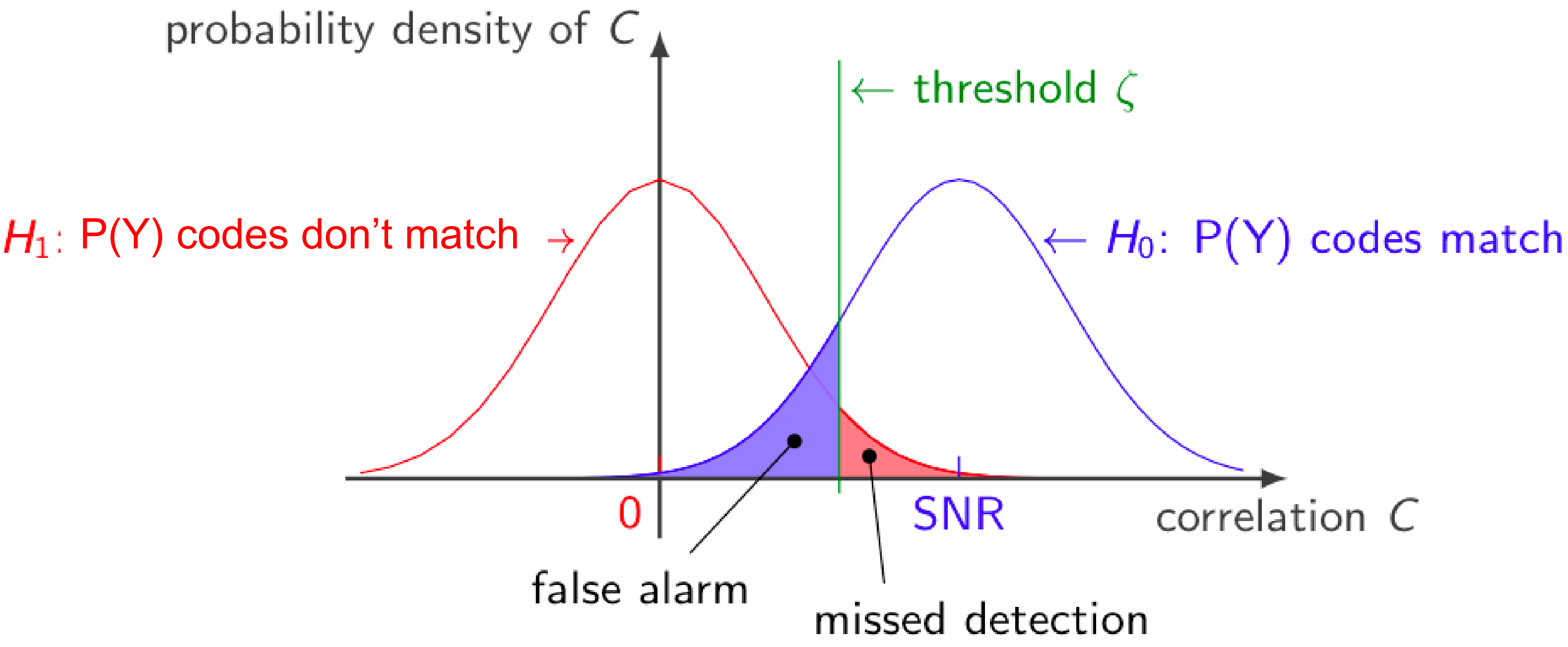
Not Spoofed | Spoofed

In-phase Baseband Correlation (C/A)

Quadrature-phase Baseband Correlation (P(Y))



Modeling Pairwise Check

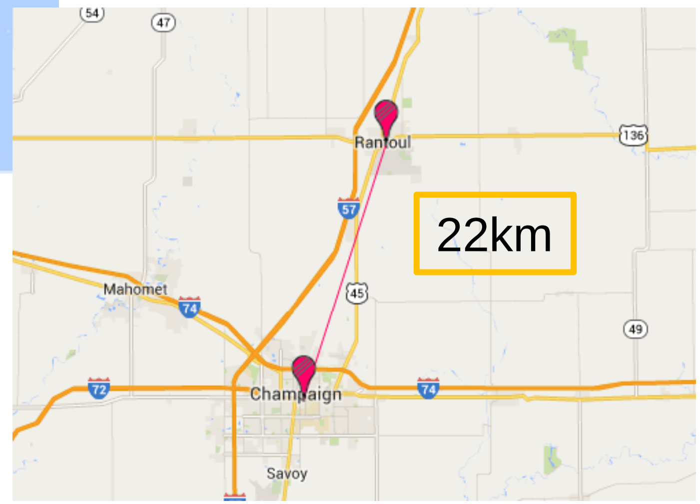


- Probability of false alarm α
- Probability of missed detection β

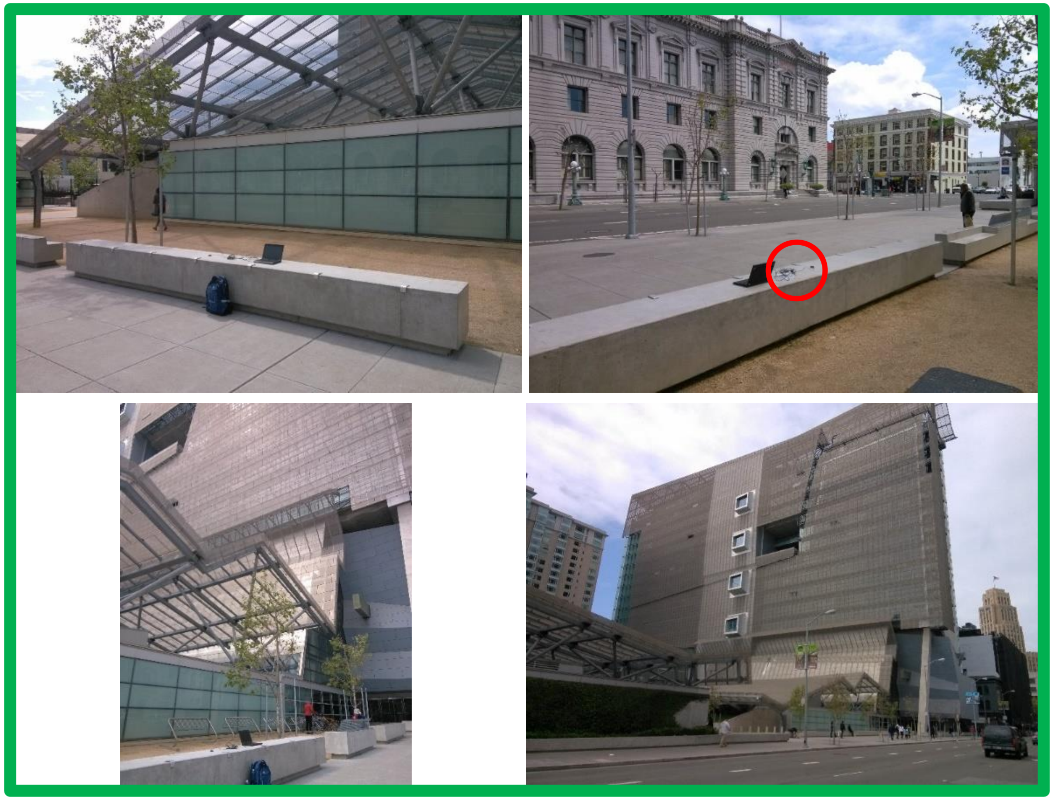
Experiments with Different Scenarios

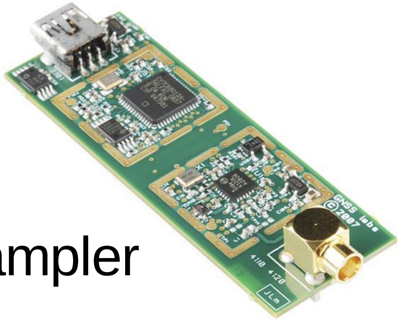
San Francisco CA and Champaign IL, static

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



Experiments: San Francisco & UIUC Everitt Lab

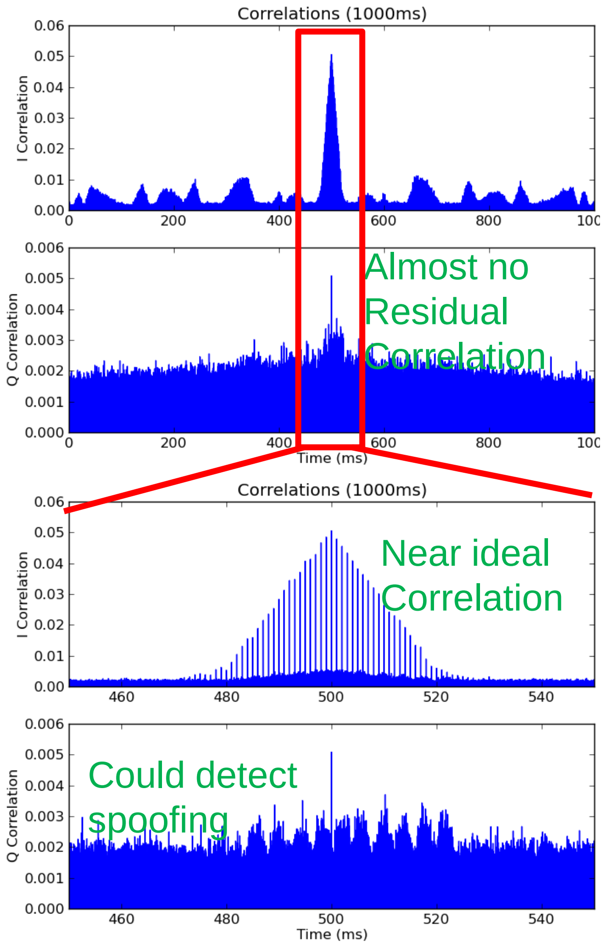




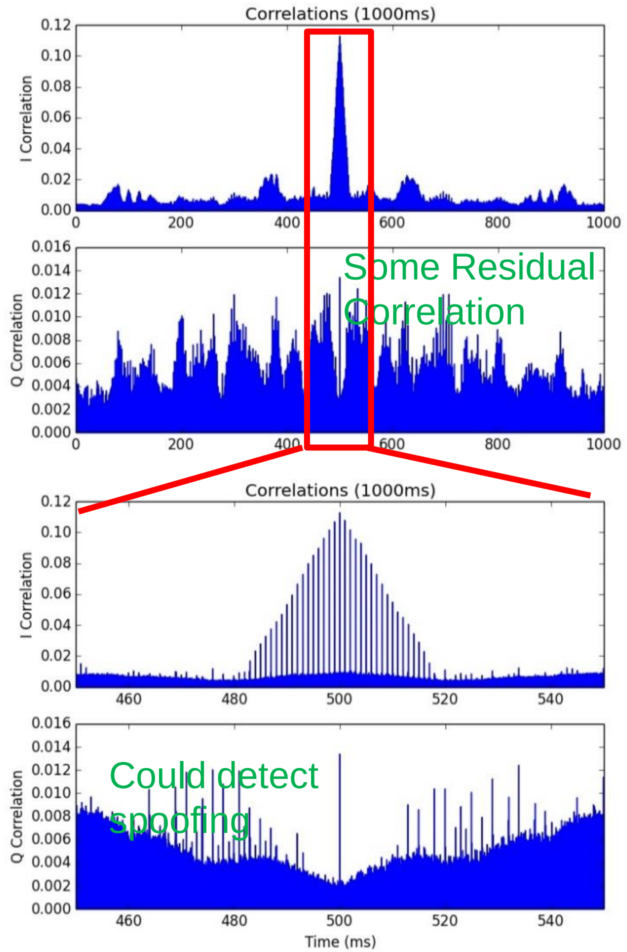
SiGe Sampler

Pairwise Results for Different Separations

3000km separation



22km separation



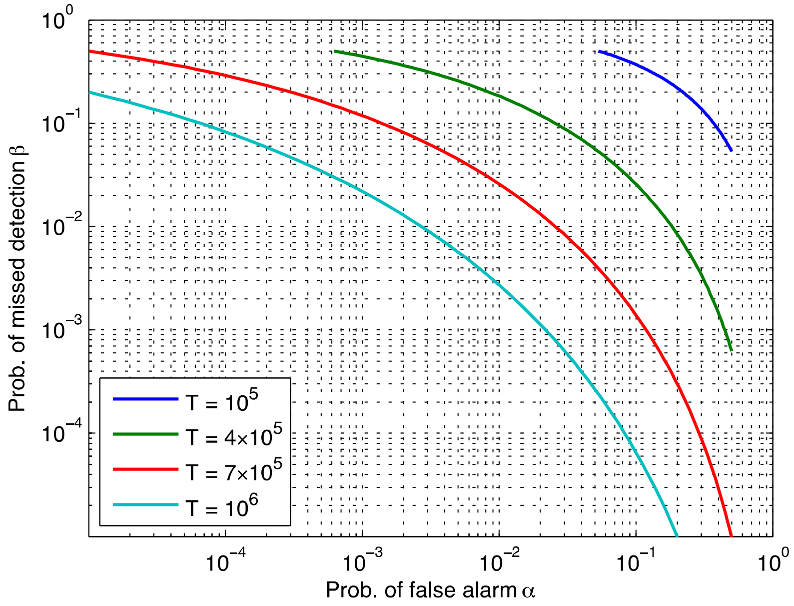
SNR Affects Pair-wise Check Performance

3000 km apart

one receiver in urban canyon

both receivers were static

$C/N_0 = 47$ dB-Hz

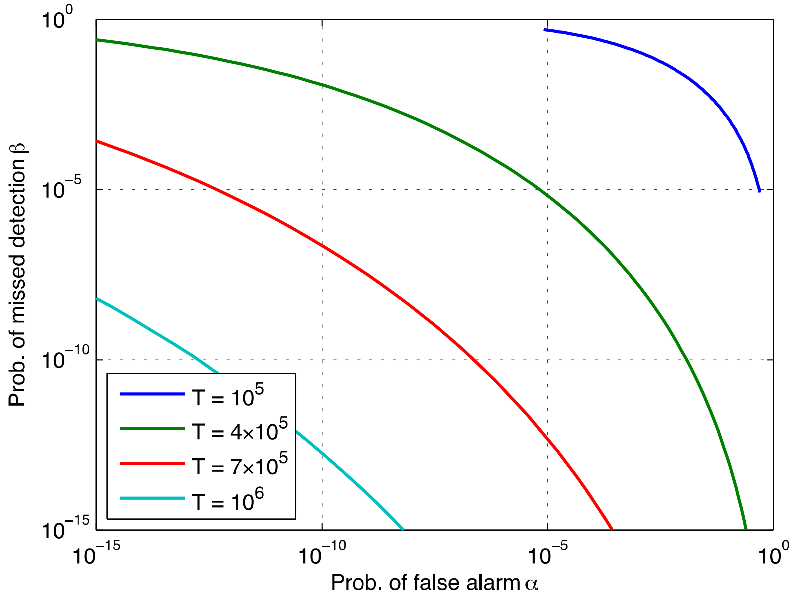


22 km apart

both receivers had an open sky

one receiver was moving at 45 mph

$C/N_0 = 51$ dB-Hz



Outline

- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation
- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results
- Conclusions

Modeling Unreliable Cross-Check Receivers

Definition

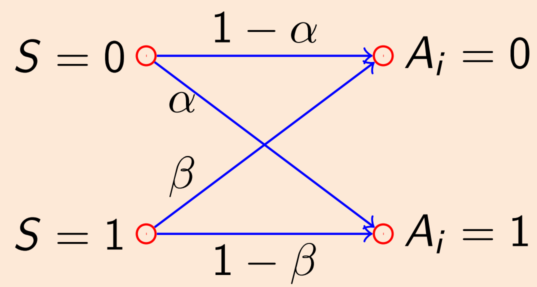
S Actual status of user receiver

A_i Authentication result using the ith cross-check receiver

$= 0$ authentic

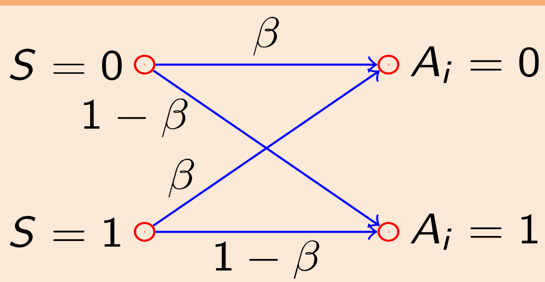
$= 1$ spoofed

Cross-check receiver is authentic



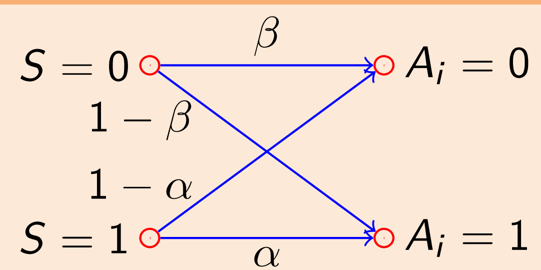
with a probability $1 - P_{SD} - P_{SS}$

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

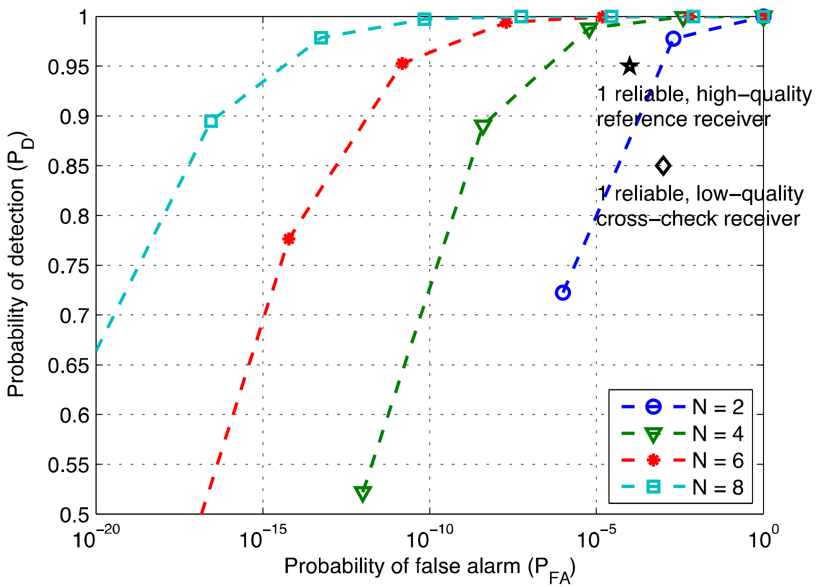
$$P_{FA} = P_{MD} \leq \exp\left(-N\lambda^2\right).$$

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

- Pair-wise false alarm rate (α)
- Pair-wise missed detection rate (β)
- Probability of being spoofed by a different spoofer (P_{SD})
- Probability of being spoofed by the same spoofer (P_{SS})

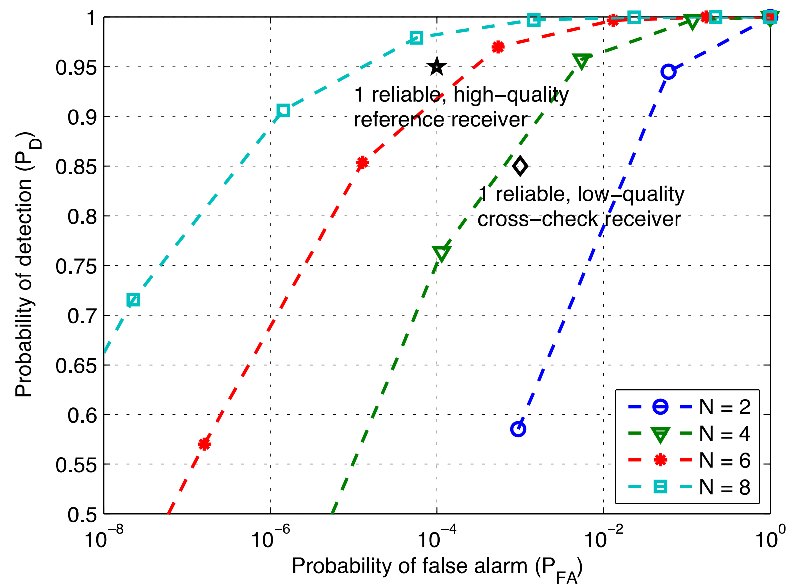
- Authentication performance improves ***exponentially*** with increasing number of cross-check receivers.
- P_{SS} causes twice as great performance deterioration as P_{SD} does.
  - Choose a cross-check receiver far from the user receiver.

Receiver Operating Characteristic (ROC) Curves



(a) Reliable cross-check receivers

$(P_{SS} = P_{SD} = 0)$



(b) Unreliable cross-check receivers

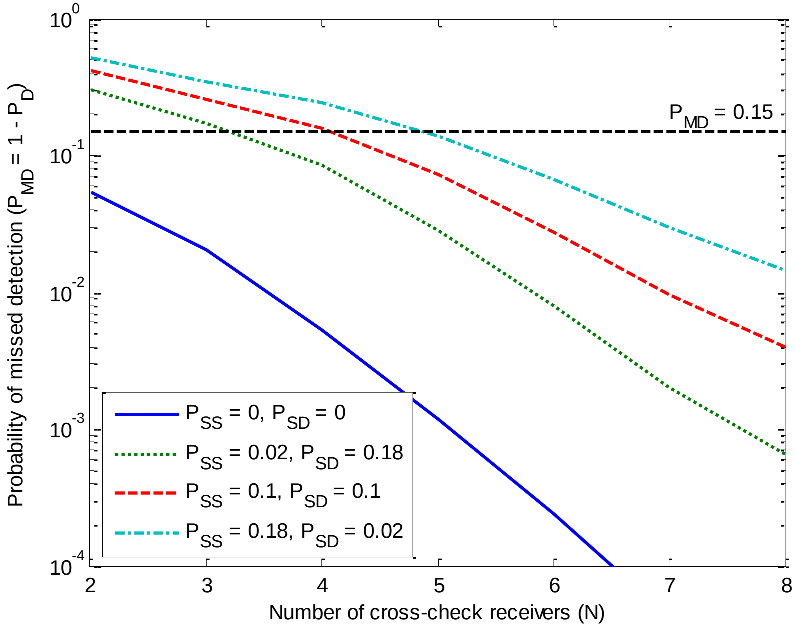
$(P_{SS} = P_{SD} = 0.1)$

Assumptions:

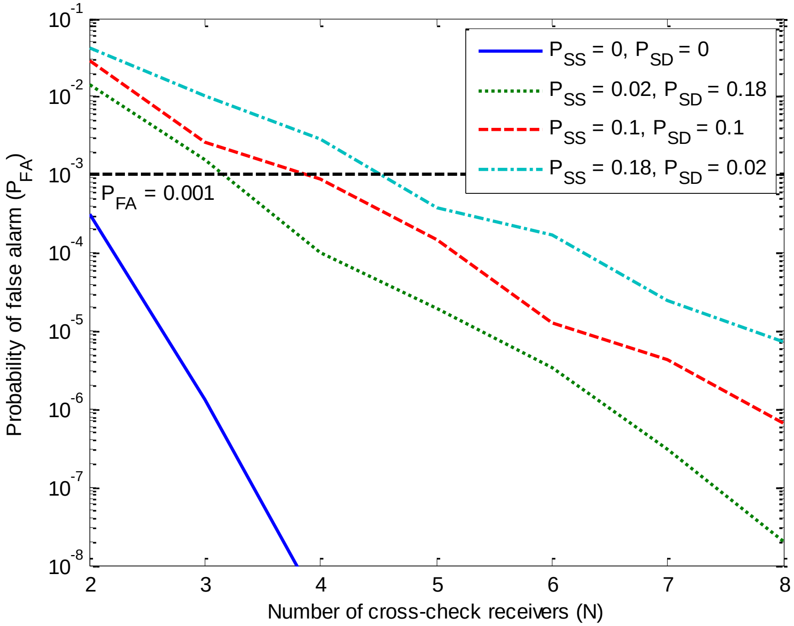
- High-quality reference receiver: $\alpha = 0.0001$ and $\beta = 0.05$.
- Low-quality cross-check receiver: $\alpha = 0.001$ and $\beta = 0.15$.

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.

Outline

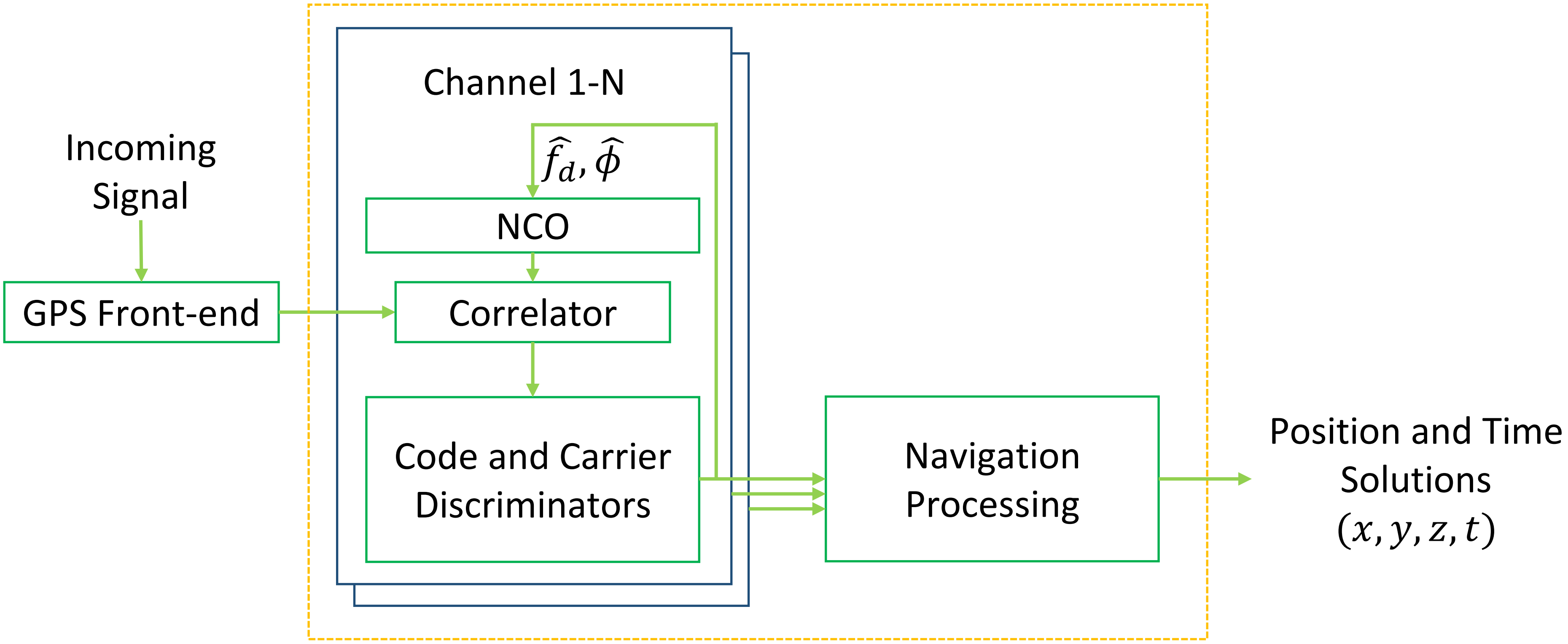
- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation
- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results
- Conclusions

Approach: Position-Information-Aided (P.I.A.) Vector Tracking

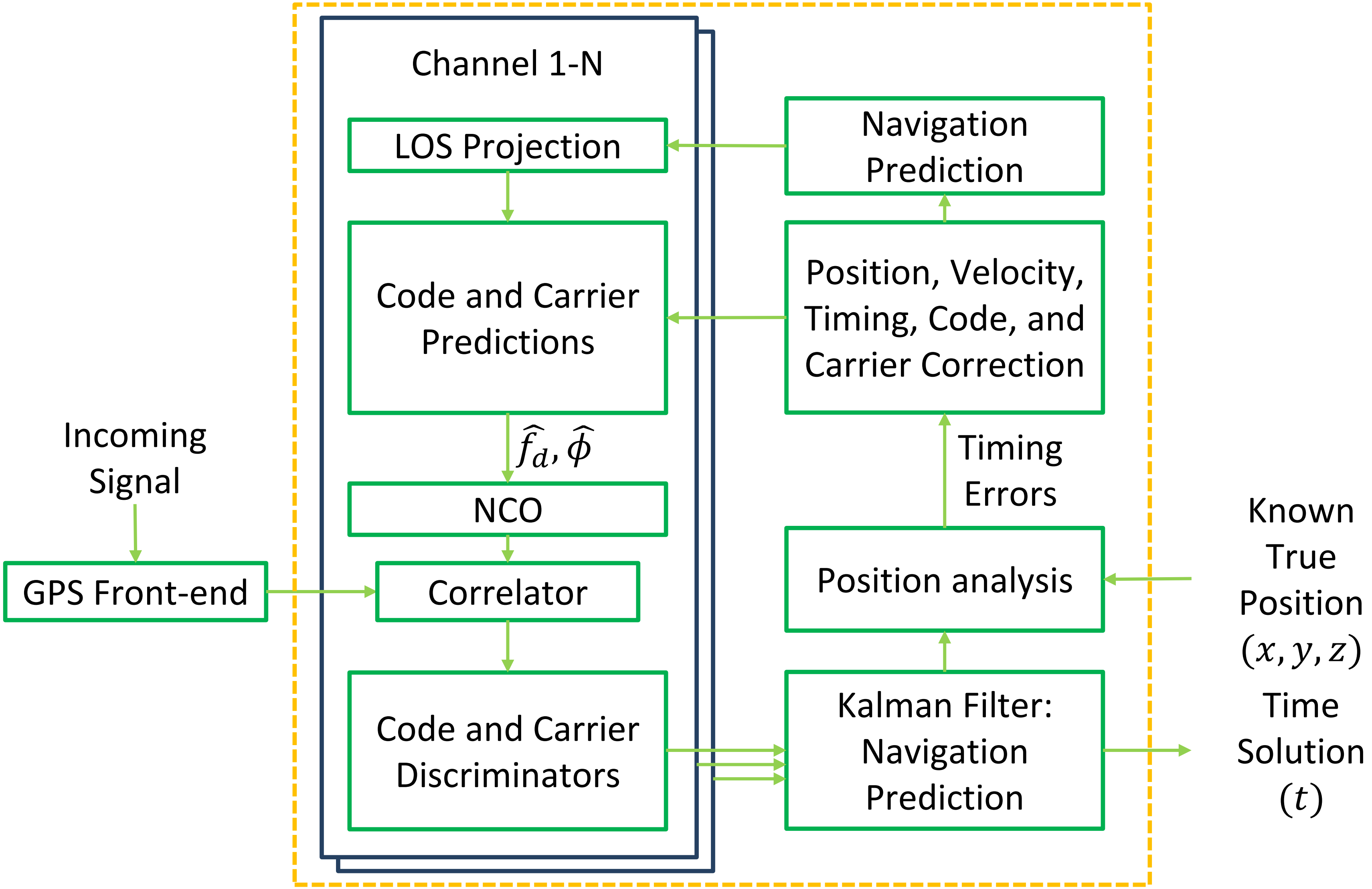
Approach:

- Vector tracking
- Reduces the search space
  - Aided by the true position
- Kalman filtering
  - Recursively predict and update the errors
- Narrowband loop filter

Scalar Tracking



Implementation: P.I.A. Vector Tracking



Implementation: Kalman Filter

- States: $\delta X, \delta V, \delta t_b, \delta t_d$
- State Transition Matrix

$$F_k = \begin{bmatrix} 0 & 0 & 0 & \Delta t & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \Delta t & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \Delta t \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad X_{state} = \begin{bmatrix} \delta x \\ \delta y \\ \delta z \\ \delta v_x \\ \delta v_y \\ \delta v_z \\ \delta t_b \\ \delta t_d \end{bmatrix}$$

- Predictions:
  - $\delta X_{k+1} = X_{True} - (X_k + V_k \Delta t)$
  - $\delta V_{k+1} = V_{True} - V_k$
- Calculation of receiver clock bias:

$$t_b = \frac{1}{\sum_{k=1}^{K} \omega_k} \sum_{k=1}^{K} \omega_k \left(\tilde{\rho}^{(k)} - \left| x^{(k)} - x \right| \right)$$

$1/var\left(\epsilon^{(k)}\right)$ — ω_k

Psuedorange — $\tilde{\rho}^{(k)}$

Satellite Position — $x^{(k)}$

Known true position — x

P.I.A. Vector Tracking Improves Accuracy

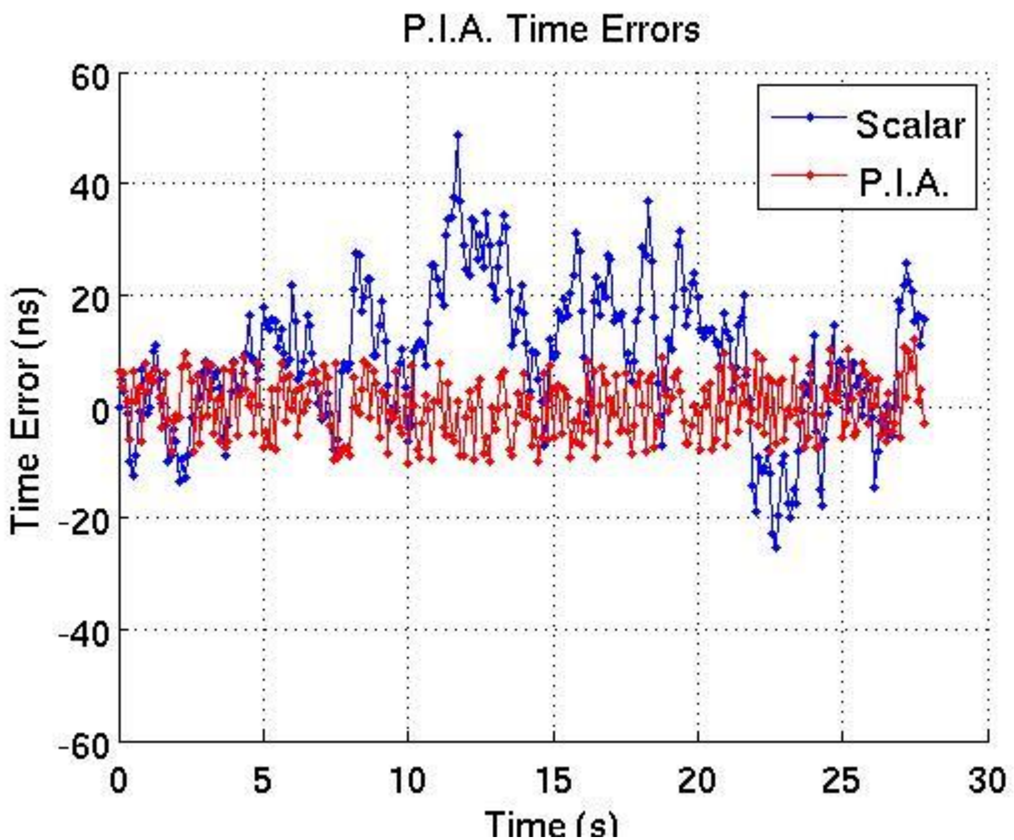
– Loop filter bandwidth of 5Hz for both scalar and P.I.A tracking loops.

– 9 satellites in view

Maximum errors:

– Traditional tracking
  - ~50ns

– Proposed vector tracking
  - ~15ns



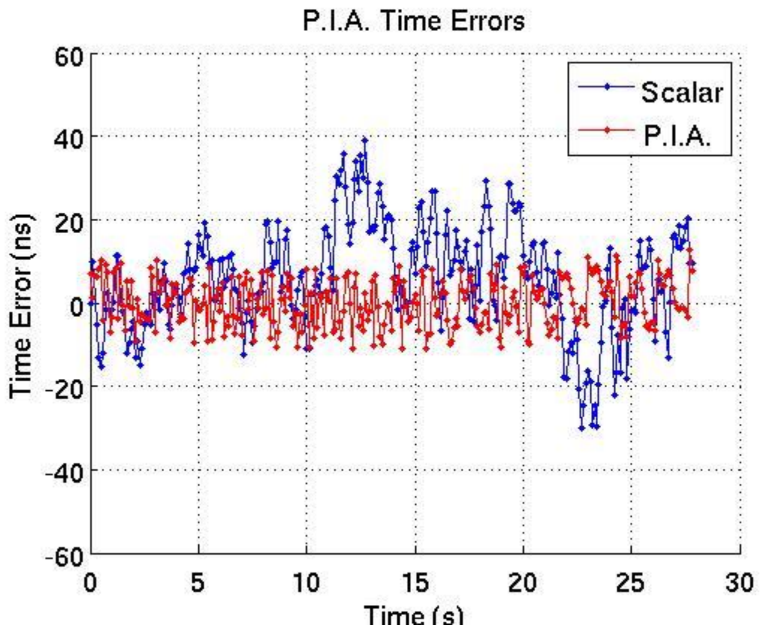
No Noise Added

P.I.A. Tracking Increases Noise Tolerance

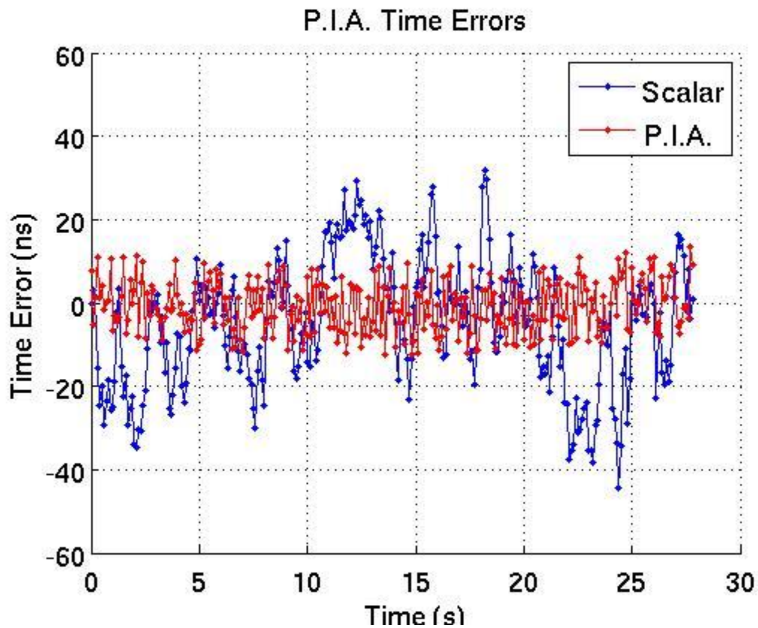
- Increased noise leads to loss of lock in scalar tracking.
- At 4 dB of additional noise, the scalar tracking was able to produce navigation bits for 4 satellites.

Noise Added	# of Satellites Tracked
0 dB	9
1 dB	8
3 dB	5
4 dB	4

1 dB Noise Added



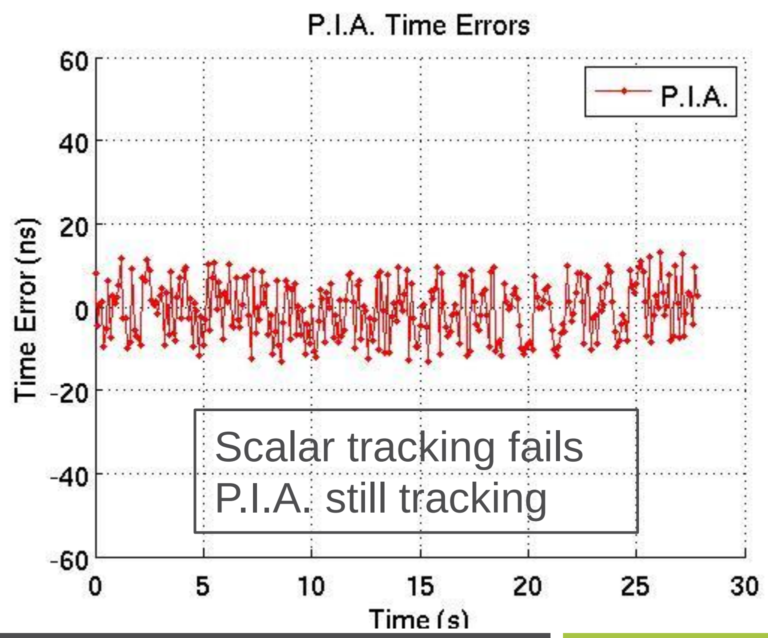
4 dB Noise Added



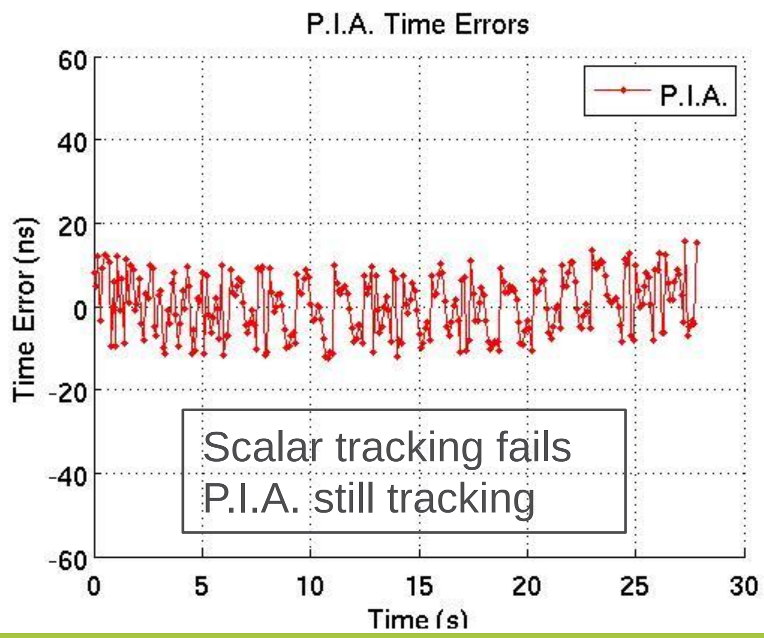
P.I.A. Tracking is Robust Against Jamming

- Scalar tracking fails at 5 dB of added noise.
- P.I.A. Vector Tracking continued to operate up until 9 dB of additional noise (5 dB more noise tolerance over scalar tracking)
- Reduces a jammer's effective radius.

5 dB Noise Added

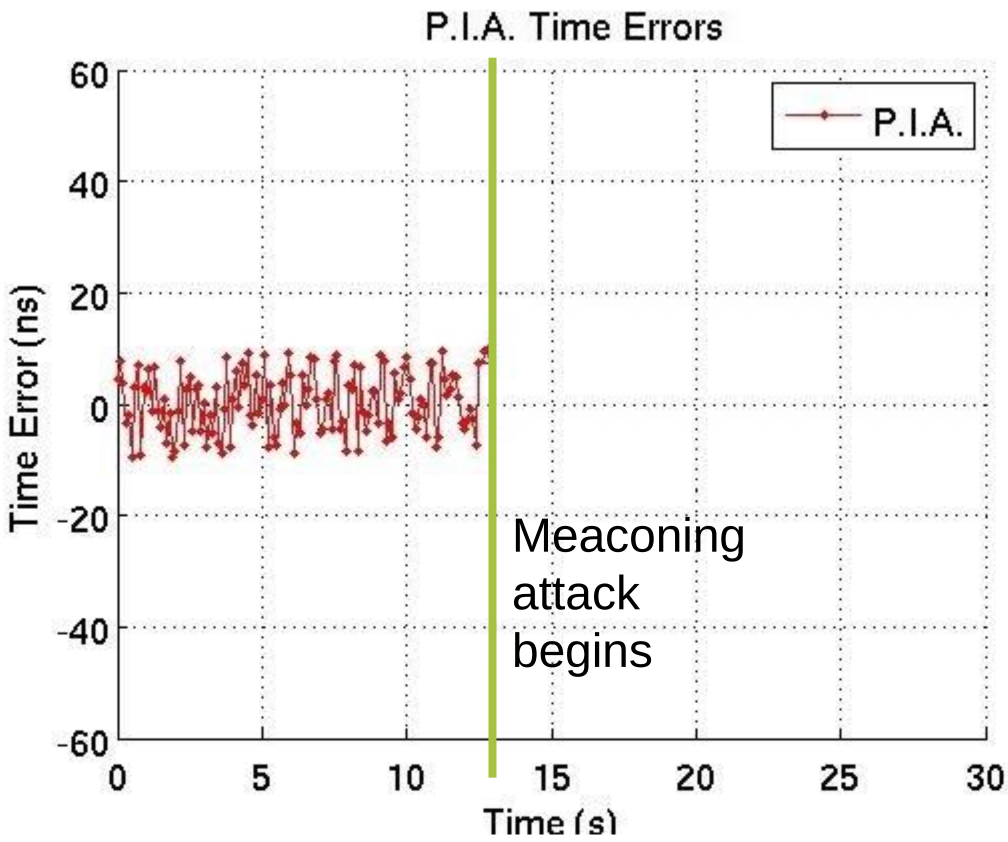


9 dB Noise Added



P.I.A. Tracking Detects Meaconing

- Meaconing: record and replay legitimate GPS signal.
- Meaconing attack simulated.
- P.I.A. Vector Tracking loop fails to converge in the event of a meaconing attack.
- 200 meter difference in known position and meaconing position.



Outline

- GPS Cooperative Authentication
  - Pairwise check
  - Decision aggregation

- Position-Information-Aided Vector Tracking
  - Approach
  - Implementation
  - Experimental Results

- Conclusions

Conclusions

- GPS cooperative authentication
  - A modest number of low-reliable cross-check receivers outperform a high-quality reliable receiver.
  - Robustness grows exponentially with the number of cross-check receivers.

- Position-Information-Aided Vector
  - Robust against jamming (5dB more noise tolerance compared with scalar tracking);
  - Successfully detects meaconing attacks;
  - Improves the accuracy of the timing solutions (15 ns vs 50 ns).

Acknowledgement

- Prof. Jonathan Makela
- TCIPG

References

- 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.

- Liang Heng, Daniel B. Work, and Grace Xingxin Gao, “GNSS Signal Authentication from Cooperative Peers,” IEEE Transactions on Intelligent Transportation Systems, submitted.

Backup Slides

Multi-layer Countermeasures

Signal conditioning

[C1] Check signal power

Code & carrier tracking

[C2] Cross-correlation of military P(Y) code between receivers

[C3] Narrow-band tracking loops

[C4] Multi-receiver vector tracking loops

Navigation data decoding

[C5] Check navigation data against external archives

[C6] Reverse-calculate satellite positions and compare them with navigation data

Position & time calculation

[C7] Check position solution against known PMU locations

[C8] Check time solution against learnt statistics of receiver clocks