Cooperative GPS Signal Authentication from Unreliable Peers

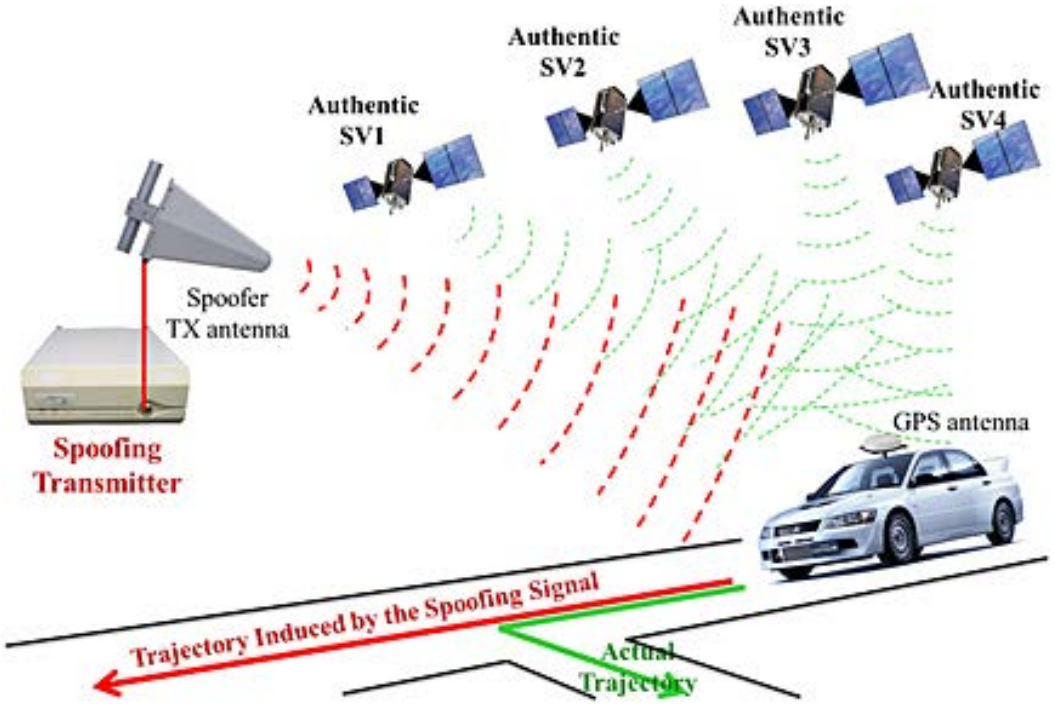
Grace Xingxin Gao

Oct. 30, 2014

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

Civil GPS Signals Are Vulnerable to Jamming and Spoofing

- Civil GPS signals are unencrypted, with their structures explicitly described in publicly-available documents.
- An attacker can broadcast counterfeit GPS signals, and manipulate victim receivers' position and/or time solutions.



(Figure from A. Jafarnia Jahromi et al., 2012)

Our Approach of GNSS Anti-spoofing

Our goal

- Practical: no need to change satellite transmission
- Low cost: no need to have secure reference stations or communication links
- Robustness: tolerate errors

Our approach: cooperative GNSS

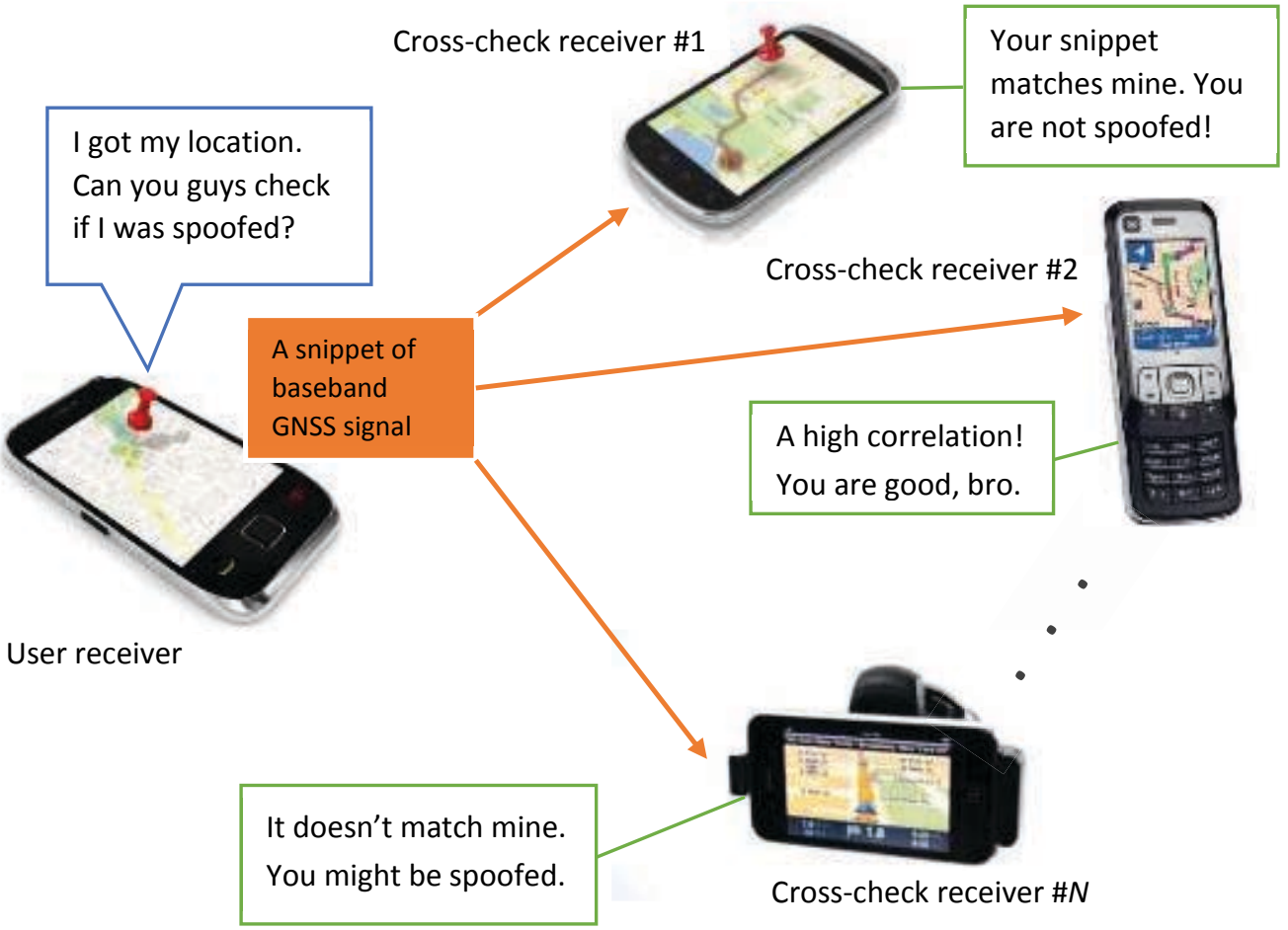
Outline

- Structure of cooperative authentication
- Pairwise check
- Decision aggregation
- Summary

Outline

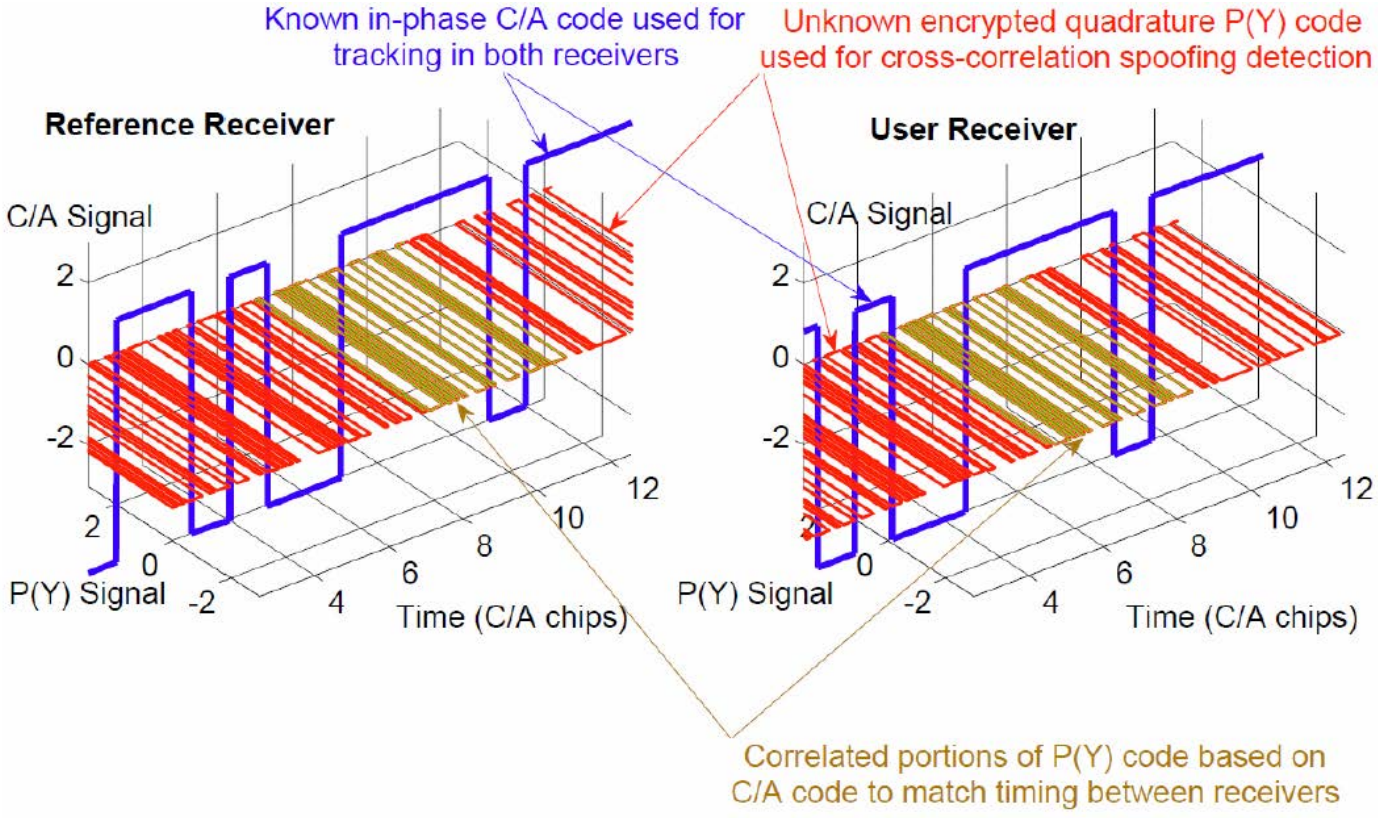
- Structure of cooperative authentication
- Pairwise check
- Decision aggregation
- Summary

Cooperative Authentication: Architecture



Merits: network and geographical redundancy

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

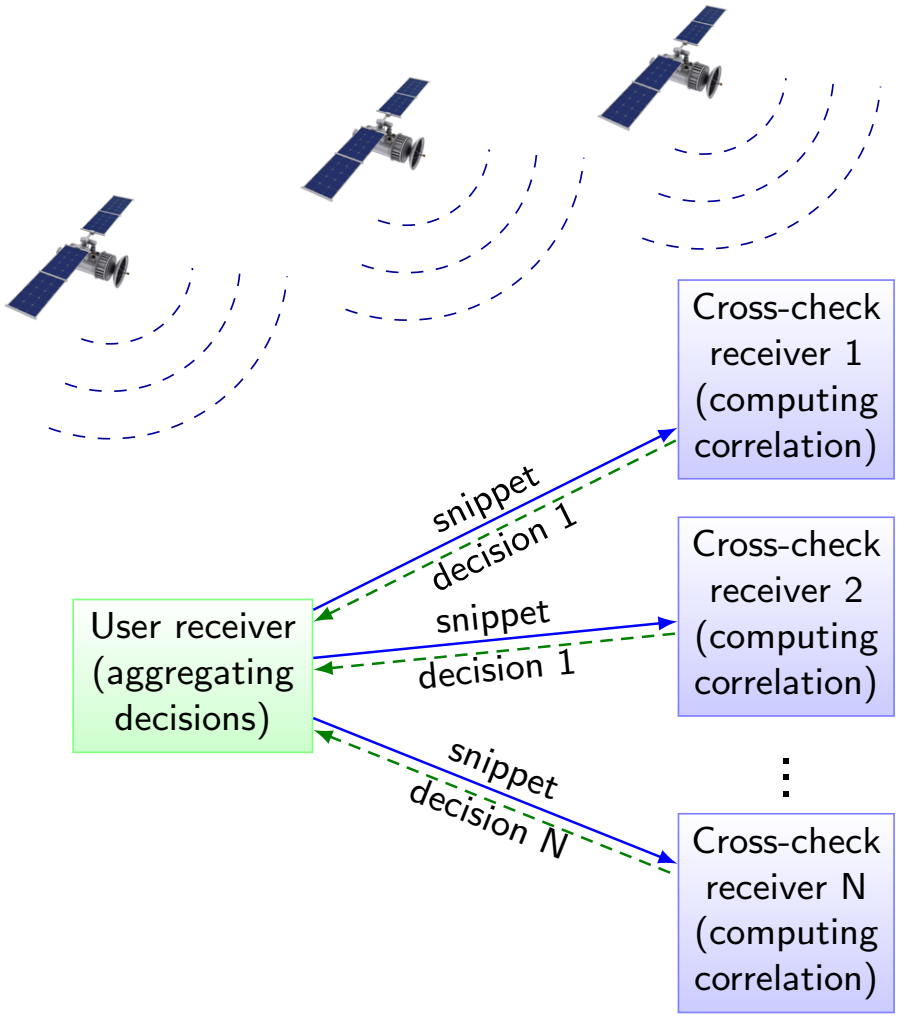


Lo *et al.*, 2009
Psiaki, Humphreys *et al.*, 2013

Two-step Process

Two-step process:

1. Pair-wise check
2. Decision aggregation



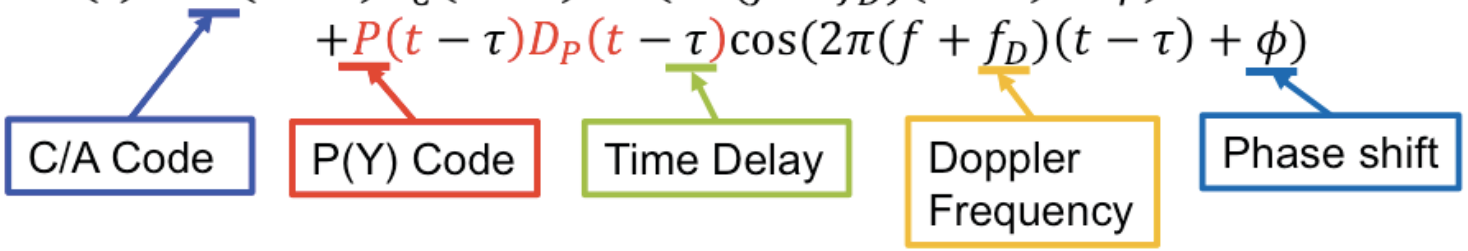
Outline

- Structure of cooperative authentication
- Pairwise check
- Decision aggregation
- Summary

Pairwise Check

Received GPS signal from one satellite:

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



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

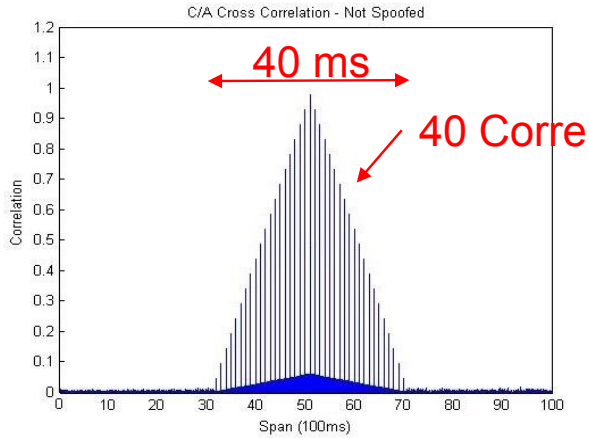
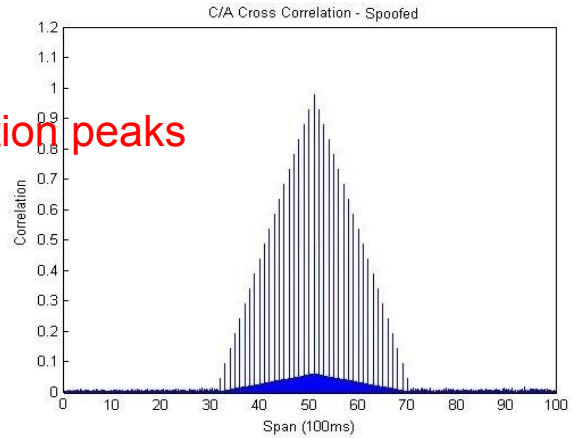
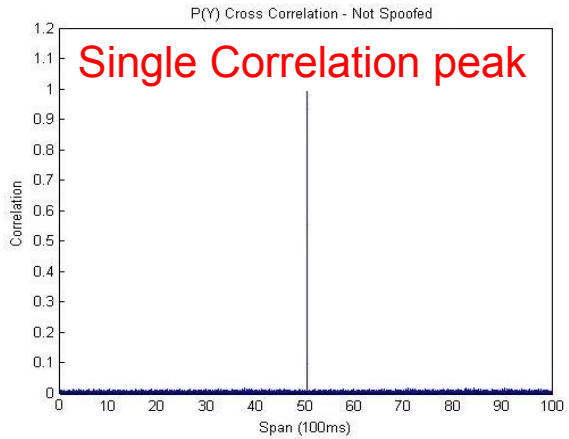
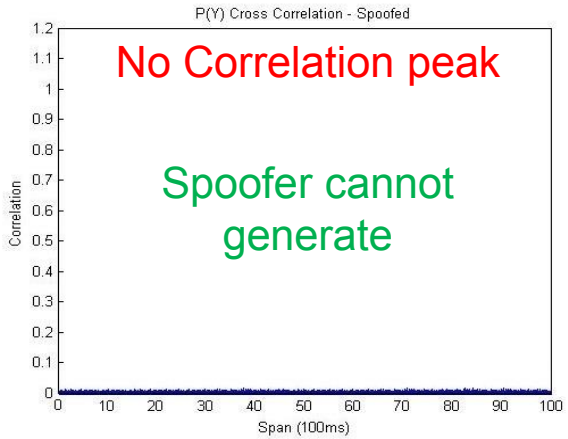
Estimate:

- Doppler frequency, f_D
- Phase shift, ϕ

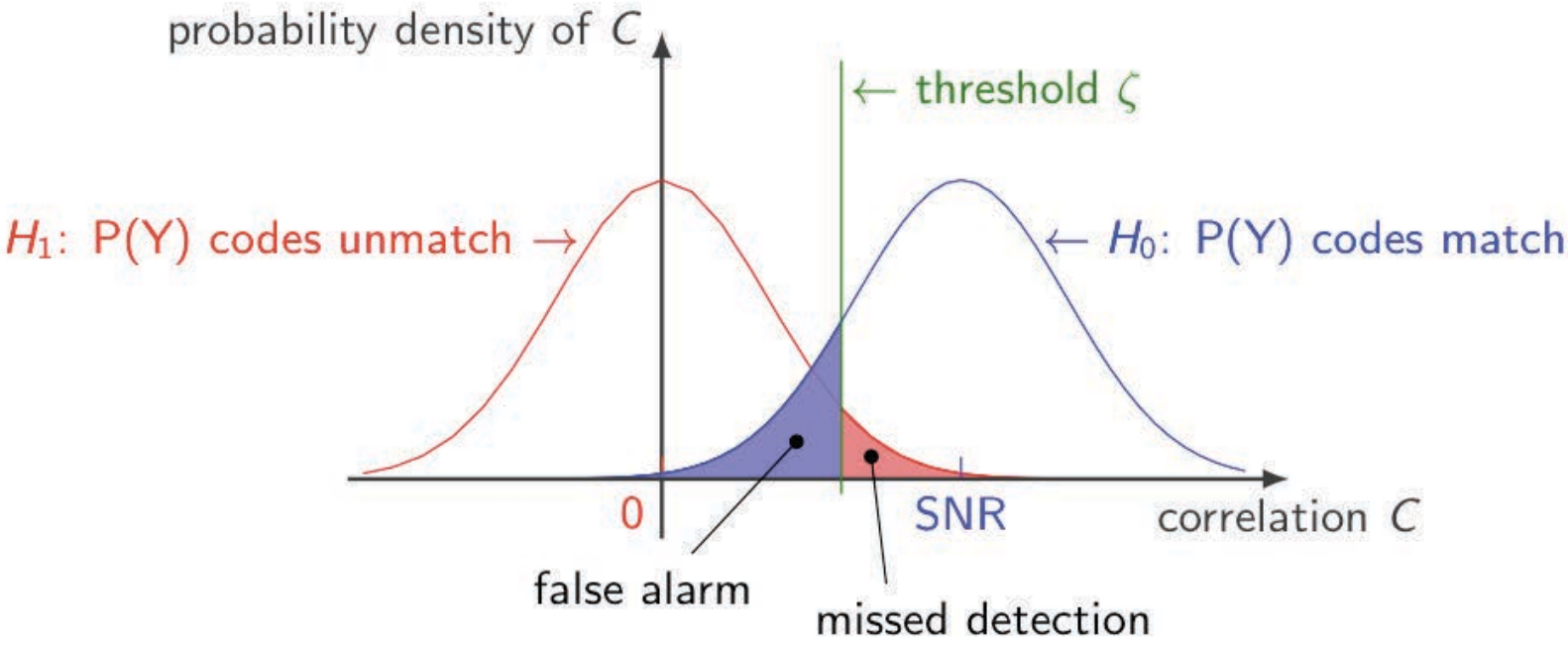
Wipe off Doppler and align phase:

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

Pairwise Check – Ideal Results

	Not Spoofed	Spoofed
In-phase Baseband Correlation (C/A)		
Quadrature-phase Baseband Correlation (P(Y))		

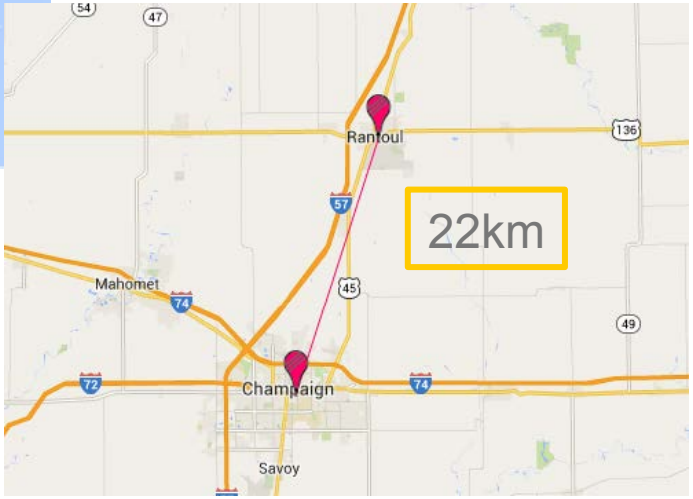
Modeling Pairwise Check



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

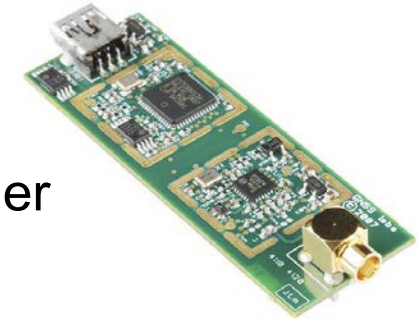
Experiments with Different Separations and Scenarios

San Francisco CA and Champaign IL, static



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

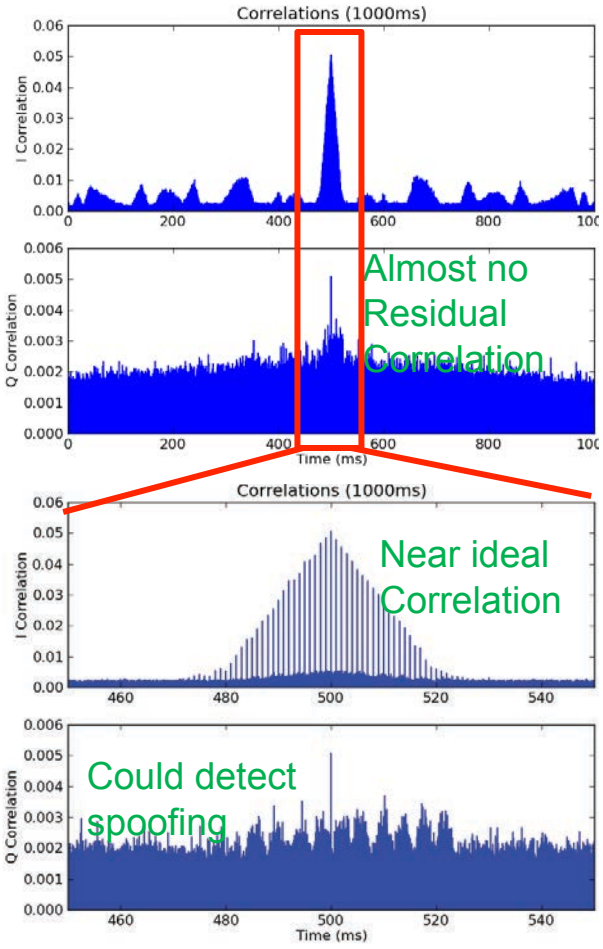
Experiment Setup: San Francisco & UIUC Everitt Lab



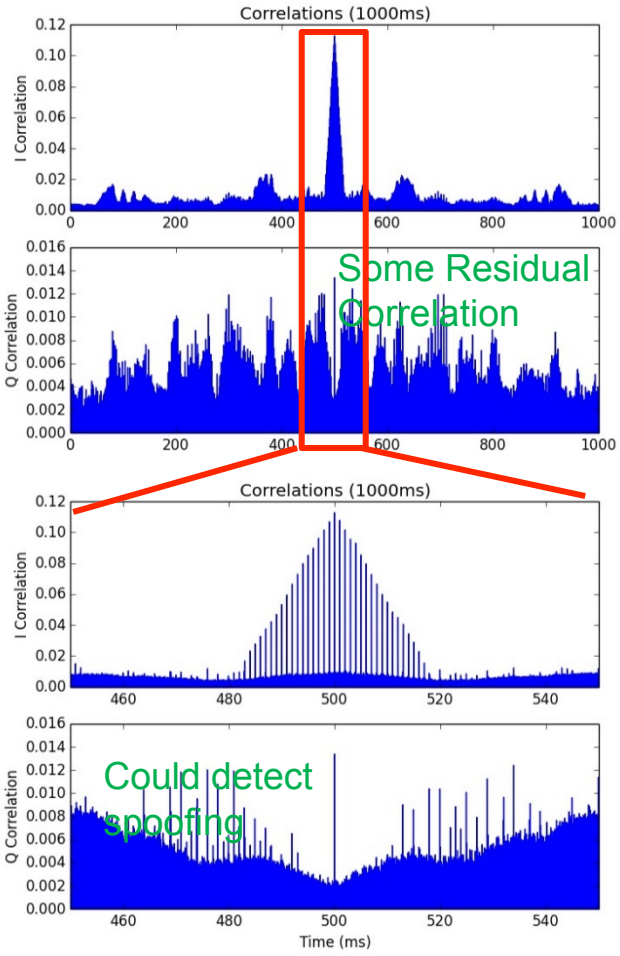
SiGe Sampler

Pairwise Results for Different Separations

3000km separation



22km separation



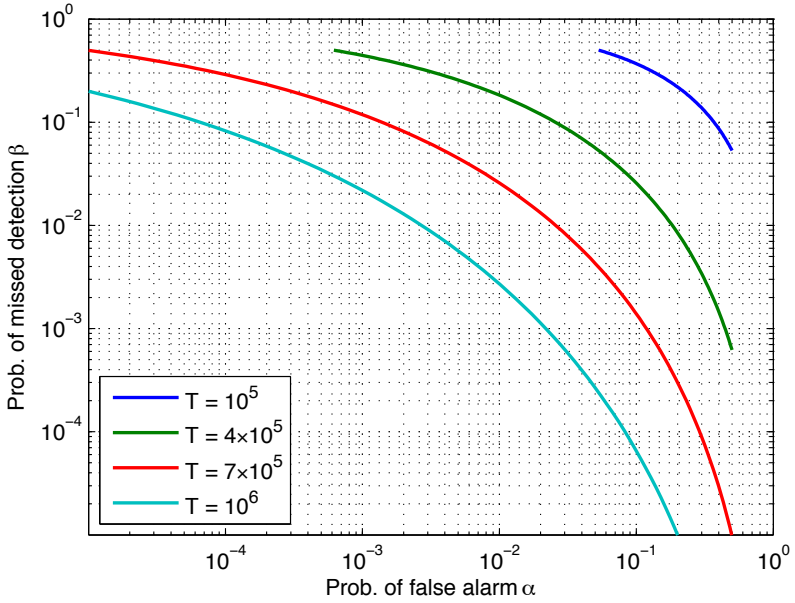
SNR Affects Pair-wise Check Performance

3000 km apart

one receiver in urban canyon

both receivers were static

$C/N_0 = 47$ dB-Hz

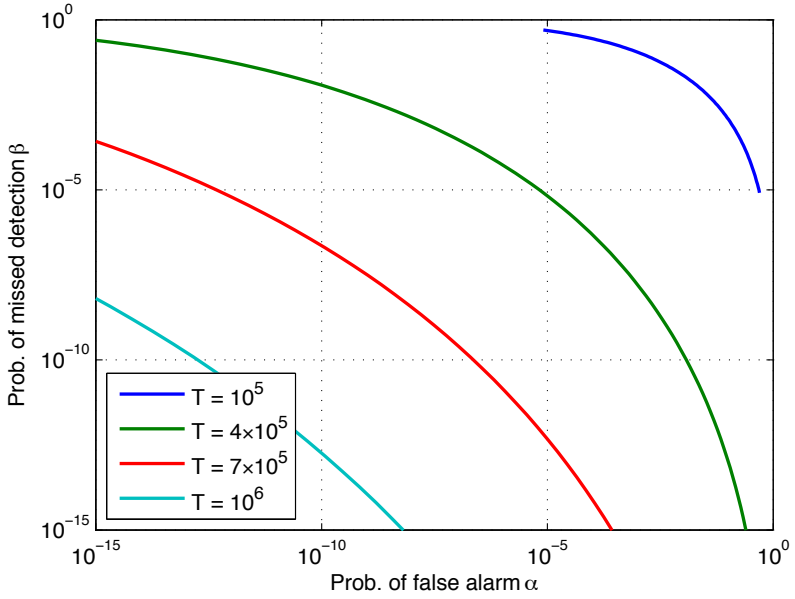


22 km apart

both receivers had an open sky

one receiver was moving at 45 mph

$C/N_0 = 51$ dB-Hz



Outline

- Structure of cooperative Authentication
- Pairwise check
- Decision aggregation
- Summary

Modeling Unreliable Cross-Check Receivers

Definition

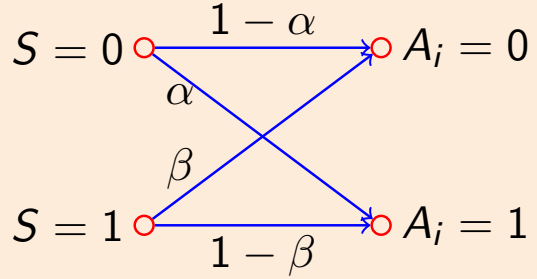
S Actual status of user receiver

A_i Authentication result using the ith cross-check receiver

$= 0$ authentic

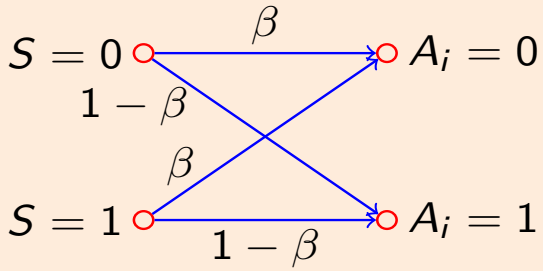
$= 1$ spoofed

Cross-check receiver is authentic



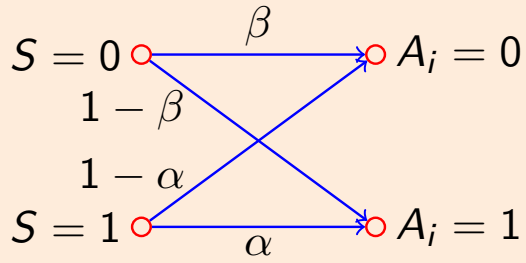
with a probability $1 - P_{SD} - P_{SS}$

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

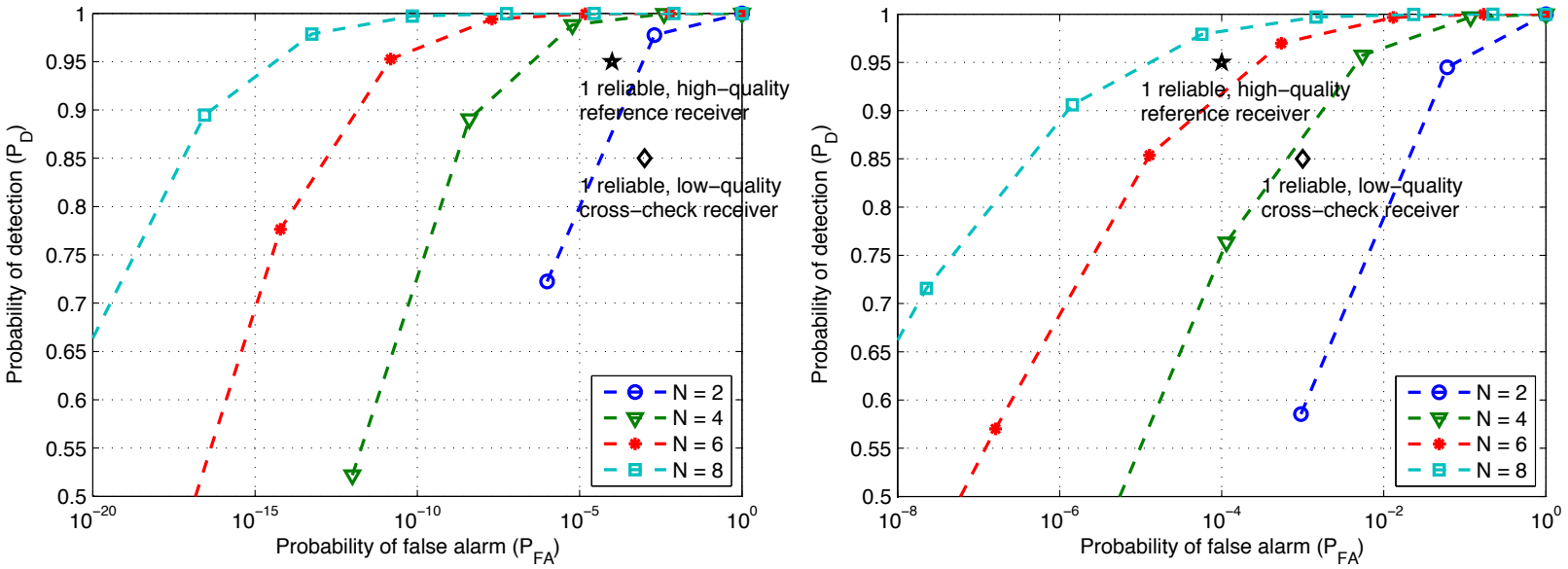
$$P_{FA} = P_{MD} < \exp(-N\lambda^2).$$

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

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.

Receiver Operating Characteristic (ROC) Curves



(a) Reliable cross-check receivers ($P_{SS} = P_{SD} = 0$)

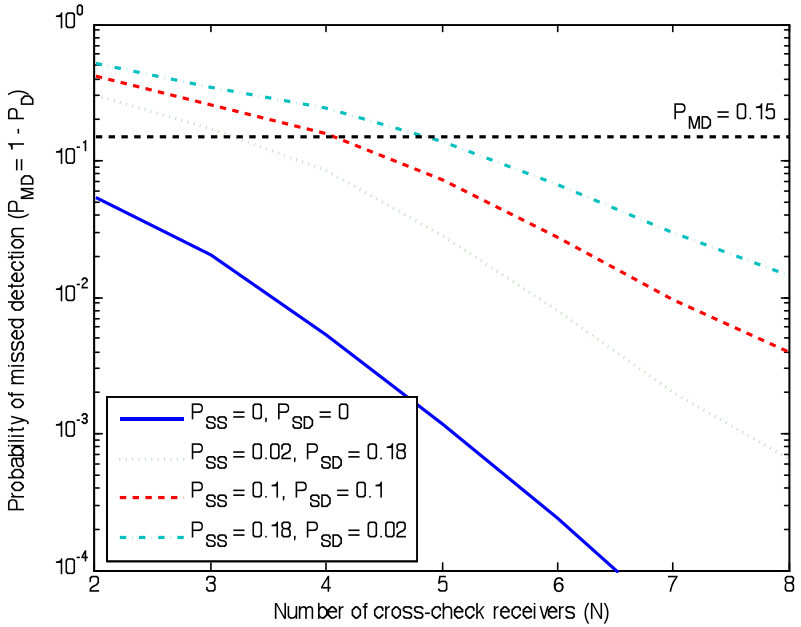
(b) Unreliable cross-check receivers ($P_{SS} = P_{SD} = 0.1$)

Assumptions:

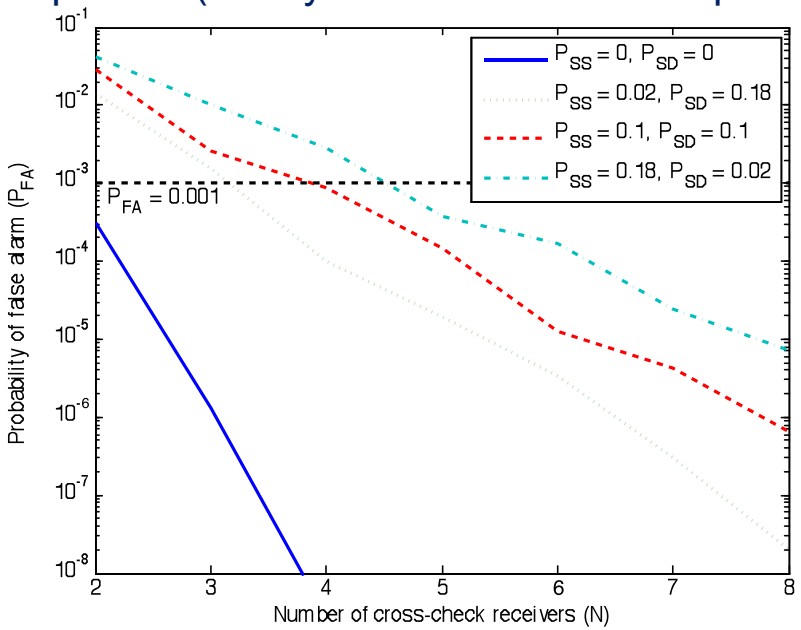
- High-quality reference receiver: $\alpha = 0.0001$ and $\beta = 0.05$.
- Low-quality cross-check receiver: $\alpha = 0.001$ and $\beta = 0.15$.

Performance of Cooperative GPS Authentication

Assume 20% of the cross-check receivers are spoofed (a very conservative 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 a par with a reliable cross-check receiver.

Summary

- Proposed cooperative GNSS authentication
  - Practical: no need to change satellite transmission.
  - Low cost: no need to have secure reference stations or communication links.
  - Robustness: network and geographical redundancy.
- Field tests
  - In San Francisco CA, Rantoul IL, and Champaign IL.
  - Static and dynamic, urban canyon and sub-urban scenarios.
- Key findings
  - 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.

Thank You!

Photo from Prof. Gao's GPS class

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Backup Slides

Challenges: Doppler Leakage from other GPS Satellites

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.

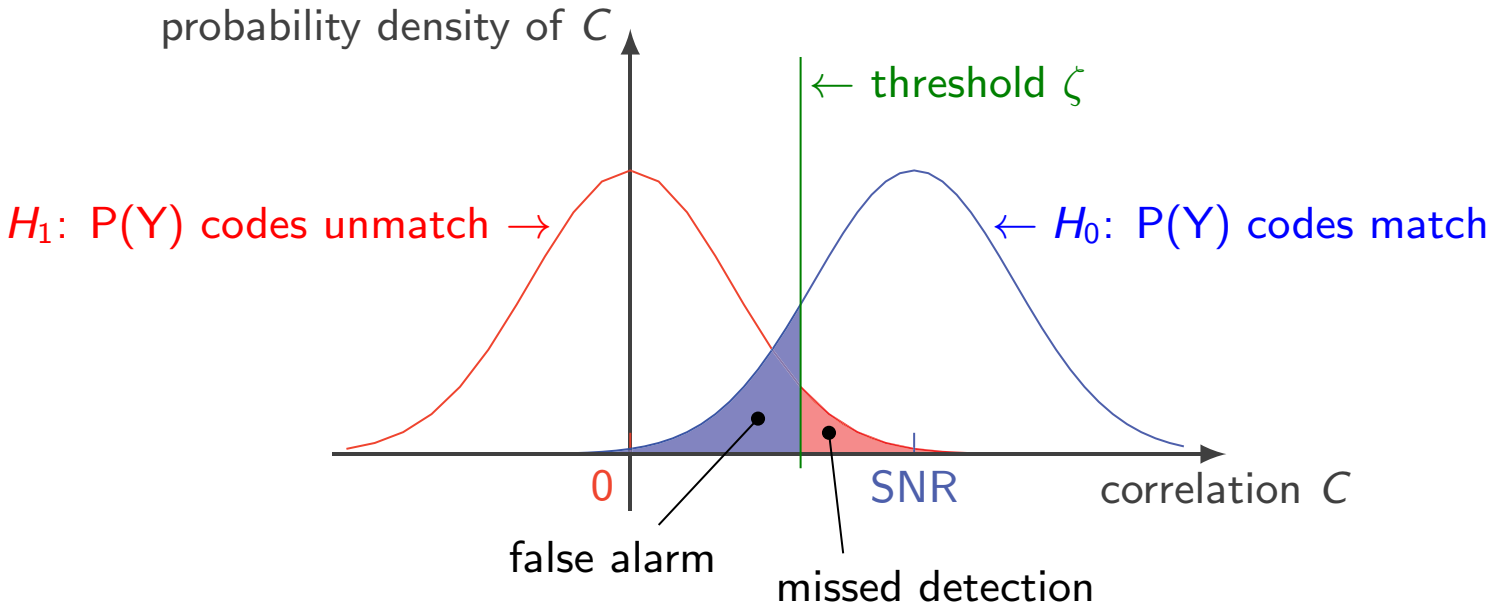
Estimate:

- Doppler frequency, f_D
- Phase shift, ϕ

Wipe off Doppler and align phase:

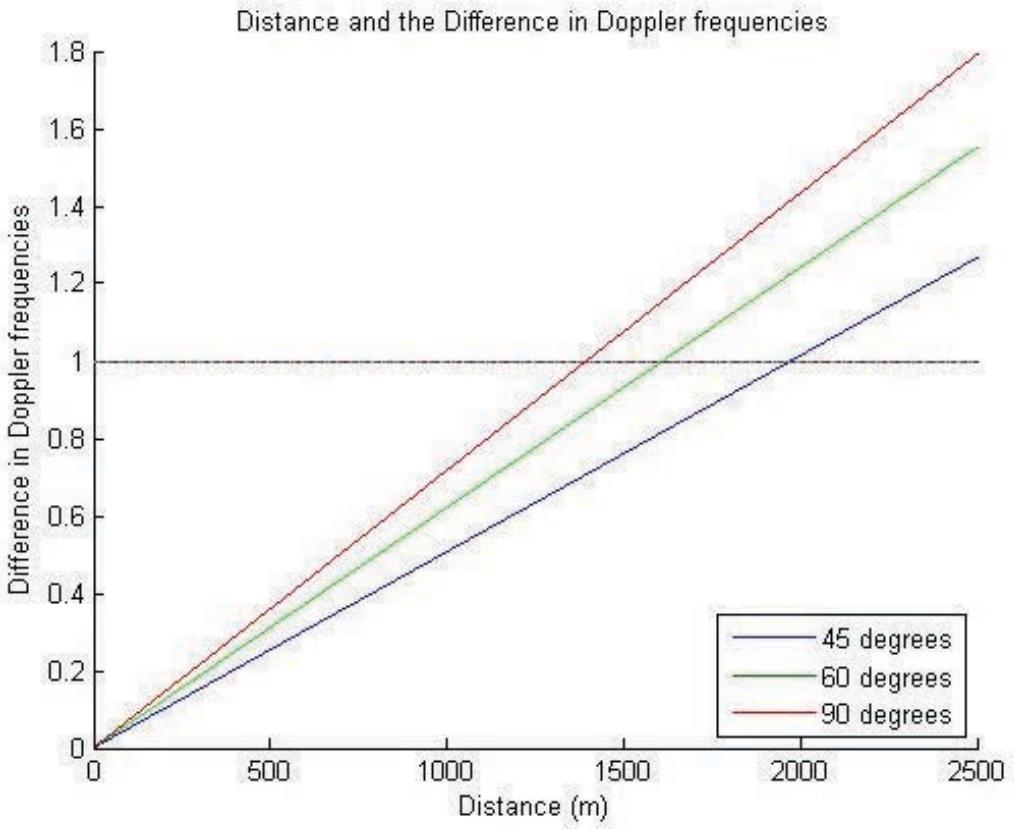
$$P(t-\tau)D_P(t-\tau) = \mathrm{LPF}[\cos(2\pi(f+f_D)(t-\tau)+\phi)\cdot s(t)]$$

Modeling Pairwise Check



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

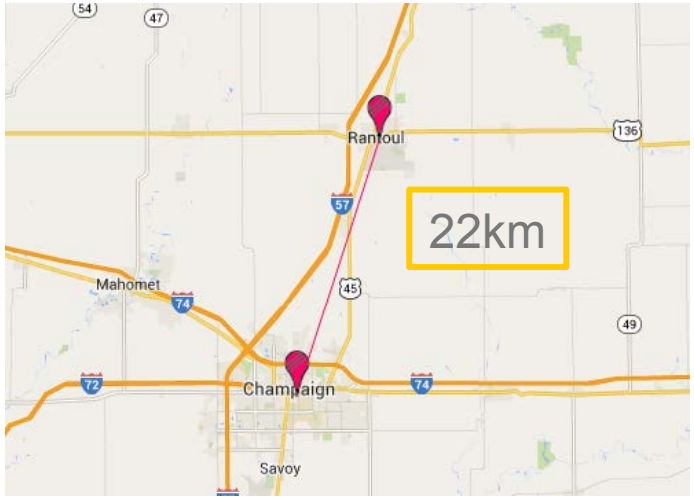
Distance Required Between Receivers

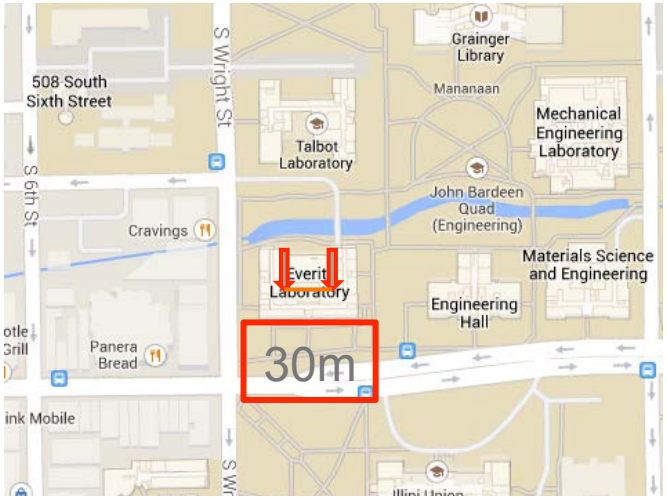


Assumptions made in figure:
- Satellite speed: 3000 m/s
- Receivers are stationary.

Conclusions
- 2-3km separation between receivers is sufficient for a 1Hz difference in the Doppler frequencies of most satellite elevations.

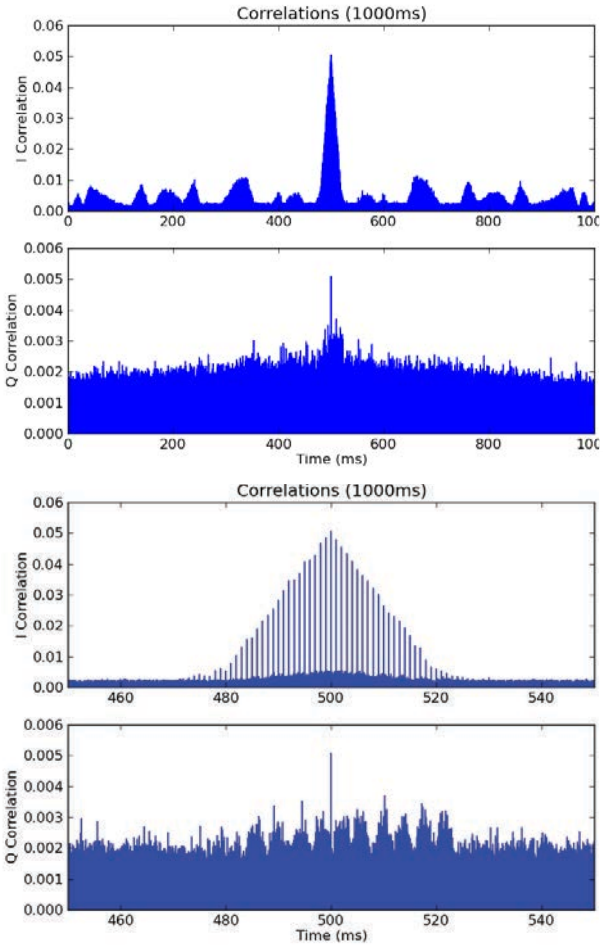
Experiments with Three Different Separations



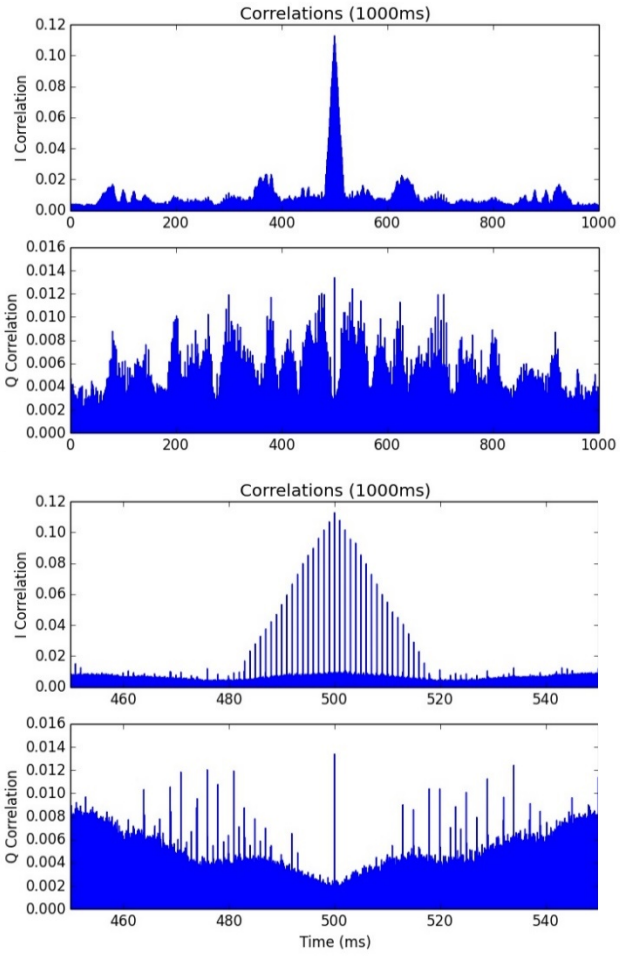


Separation Comparisons

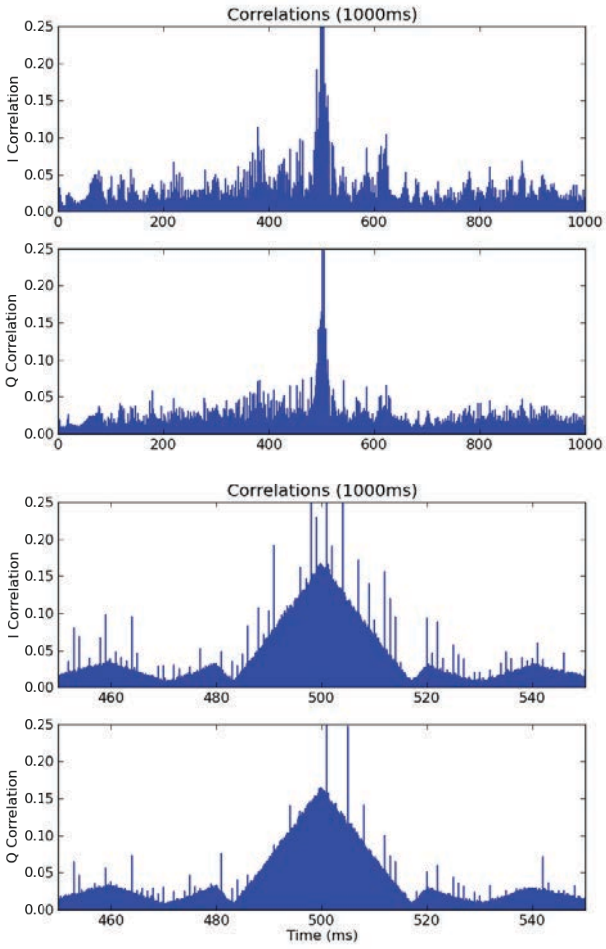
3000km separation



22km separation

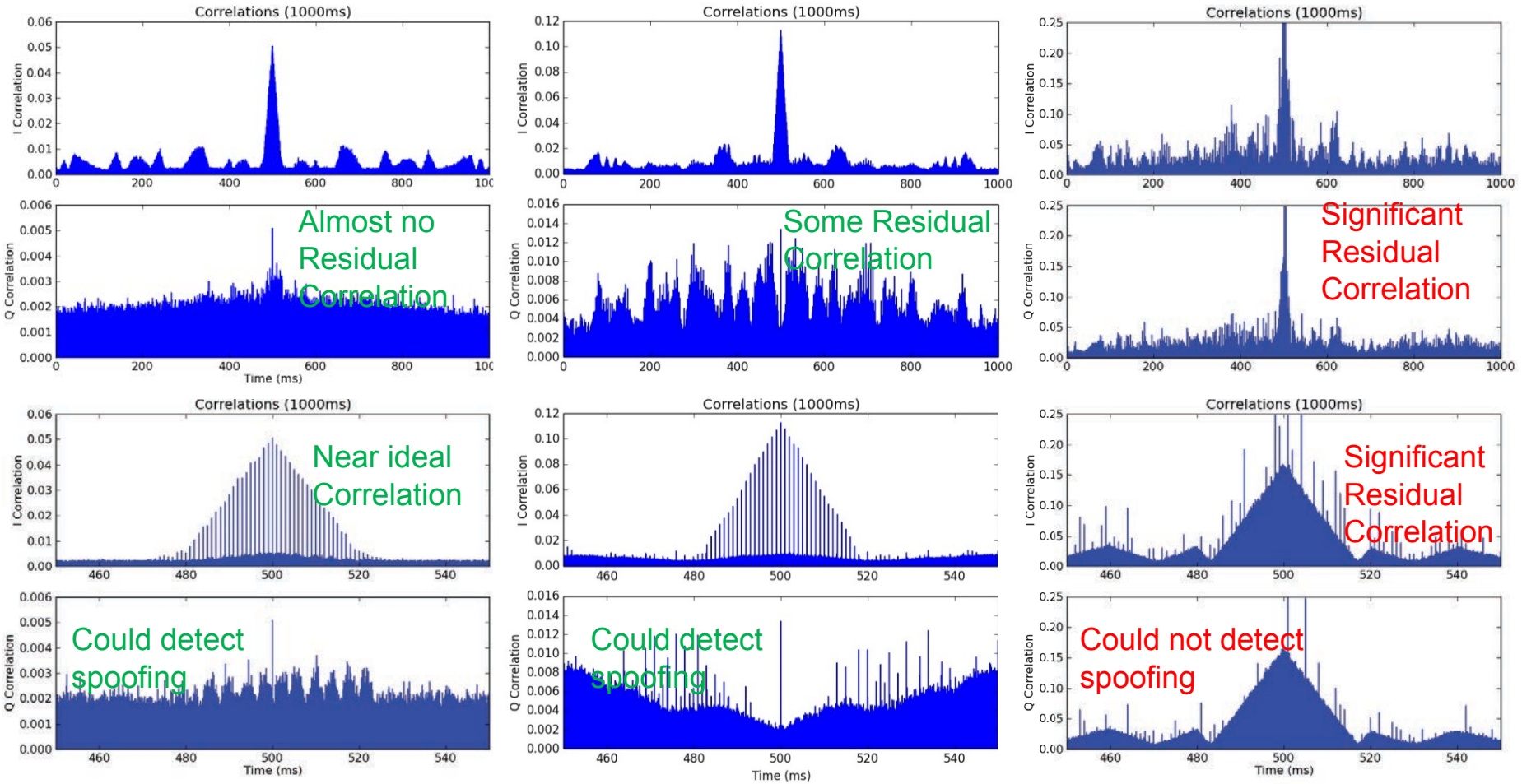


30m separation



ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Separation Comparisons



Detect Spoofing Attacks

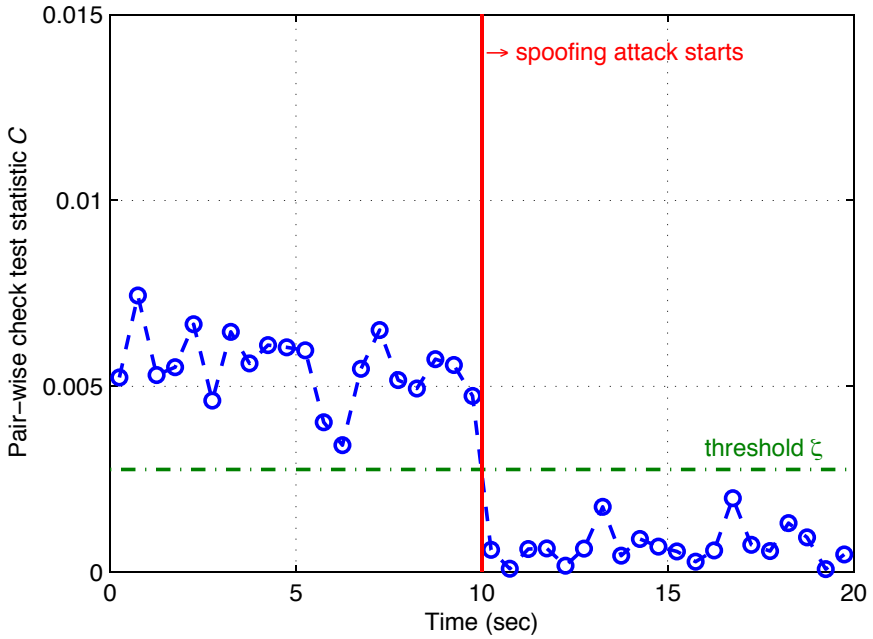


Fig. 10. Experiment 1 (3000 kilometers apart, one receiver in urban canyon): Pair-wise check test statistic over time. Each snippet is 0.5-second long ($T = 2.046 \times 10^6$). Spoofing signal is injected from 10 seconds, with the counterfeit C/A code phase moving away from the authentic C/A code phase at a rate of 0.5 chip per second.

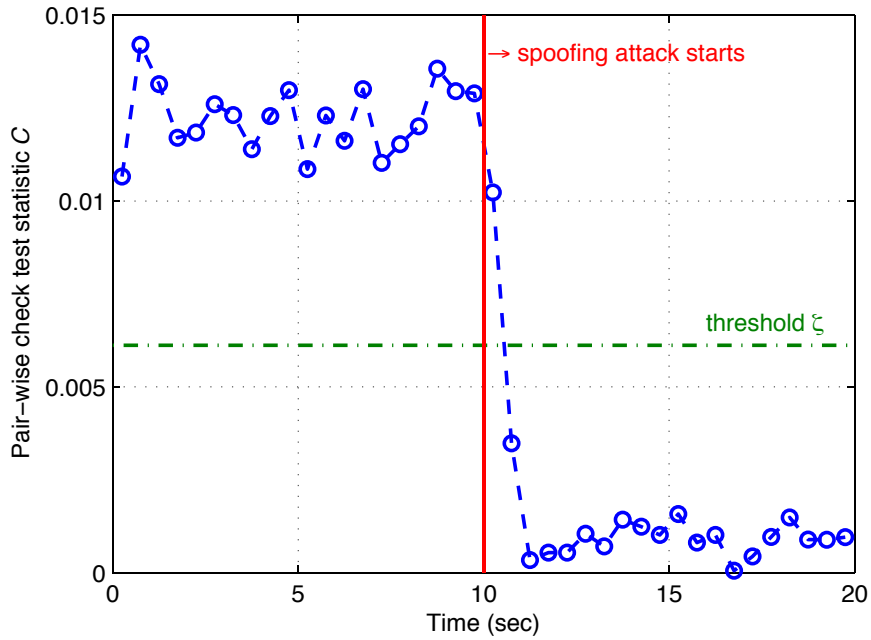


Fig. 11. Experiment 2 (22 kilometers apart, one moving receiver): Pair-wise check test statistic over time. Each snippet is 0.5-second long ($T = 2.728 \times 10^6$). Spoofing signal is injected from 10 seconds, with the counterfeit C/A code phase moving away from the authentic C/A code phase at a rate of 0.375 chip per second.