Spoof Detection and Mitigation Technologies

Sherman Lo
(and GPS Lab colleagues)
Stanford University

June 24, 2020

DSIAC
Defense Systems
Information Analysis Center

DSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC), with policy oversight provided by the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E). DSIAC is operated by the SURVICE Engineering Company.

Bottom Line, Up Front

- Deliberate threats (jamming & spoofing) to the Global Navigation Satellite system (GNSS) are more likely due to increasing incentives and ease of implementing attacks.

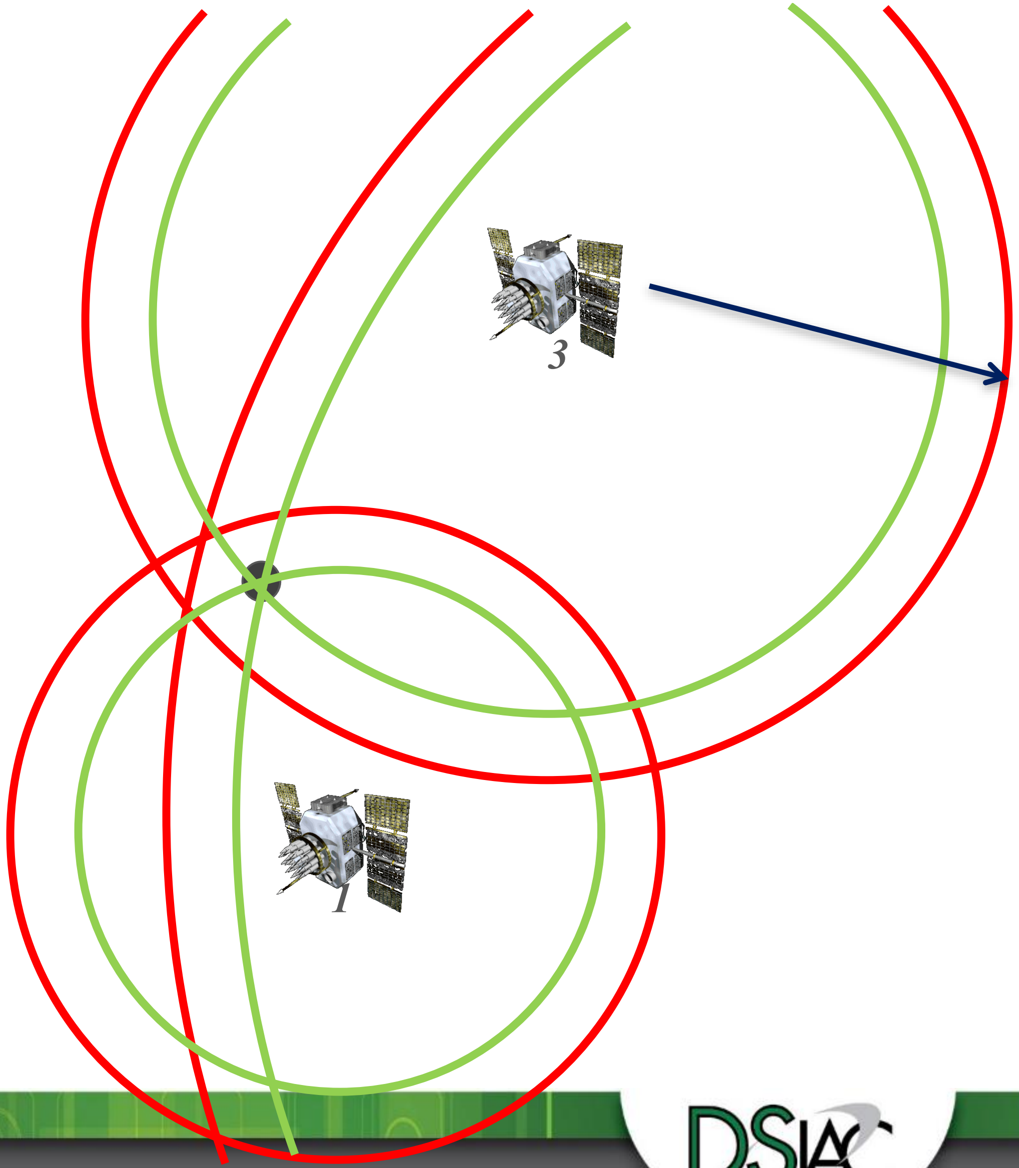
- Develop reasonable GNSS spoof detection methods to protect applications, such as safety of life (aviation & autonomous vehicles), as part of an overall GNSS resiliency strategy.

- Need to mature these technologies and develop best combinations adapted for the characteristics of each application.

Outline

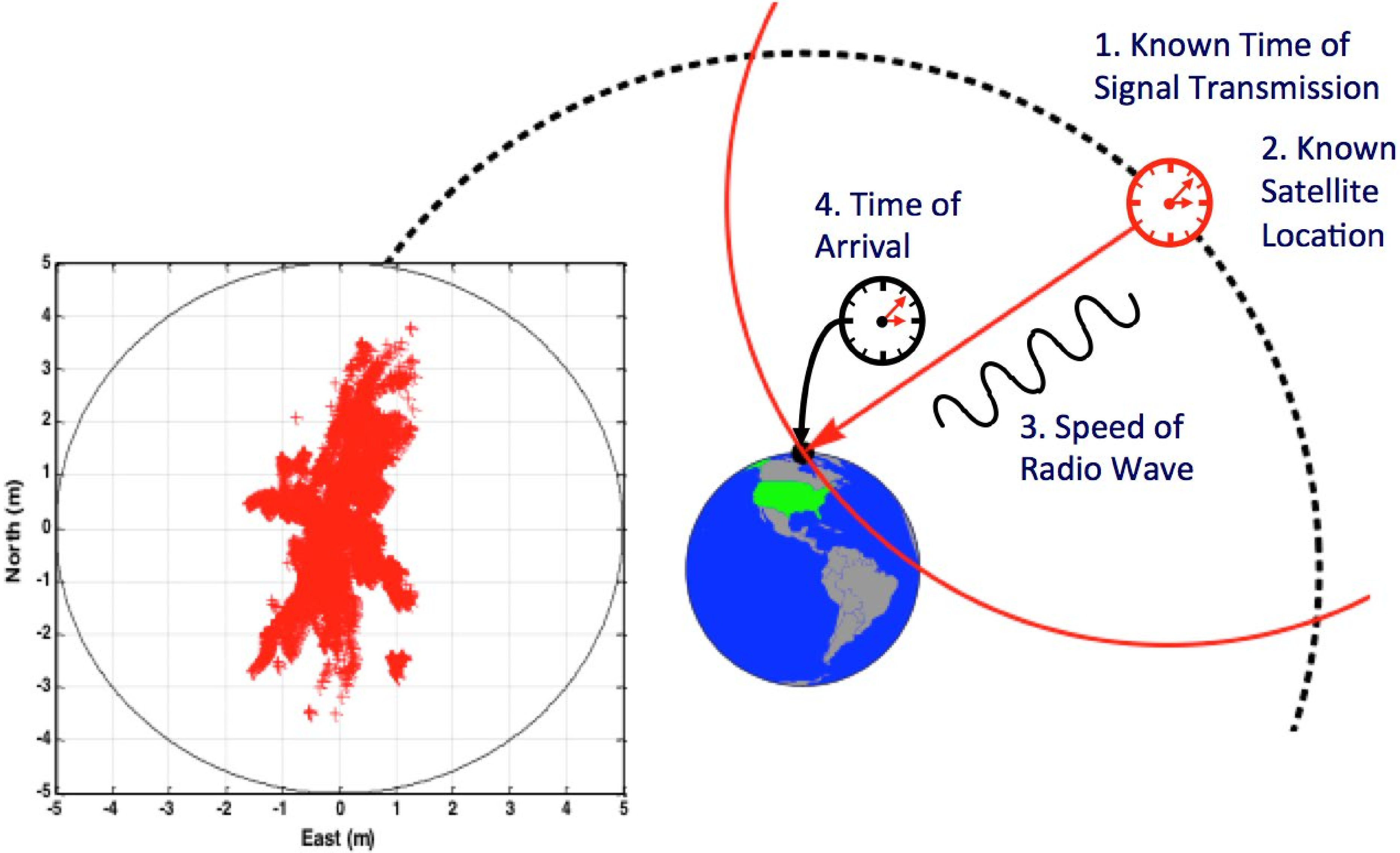
- Background on the Global Positioning System (GPS)/GPS Lab
- The Spoofing Threat
- Spoof Mitigation Techniques

How GPS Works: Principle of "Multilateration"



"Pseudo" range ρ_3

Elements of GPS



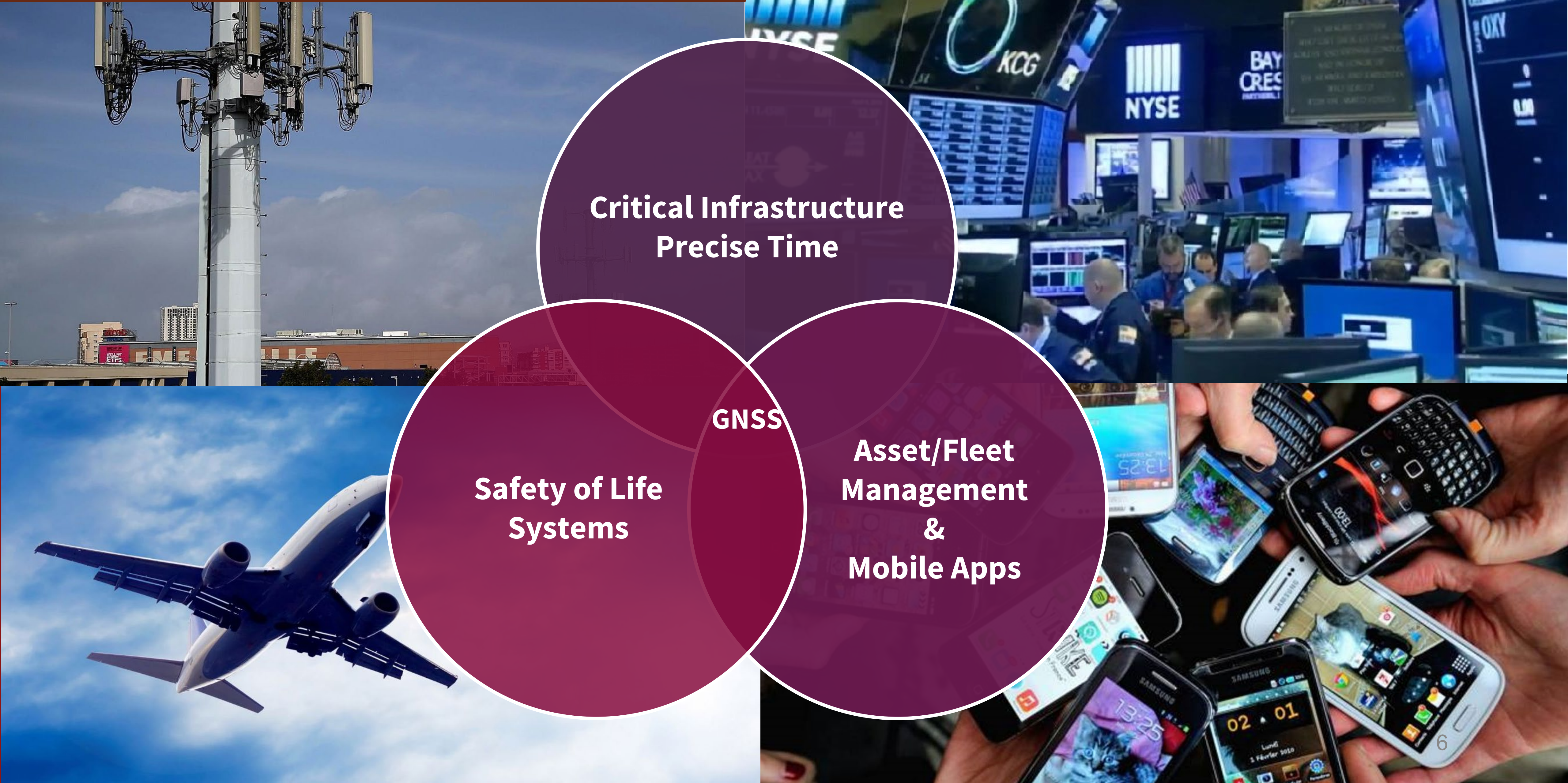
1. Known Time of Signal Transmission

2. Known Satellite Location

3. Speed of Radio Wave

4. Time of Arrival

Critical Uses for GNSS



Critical Infrastructure Precise Time

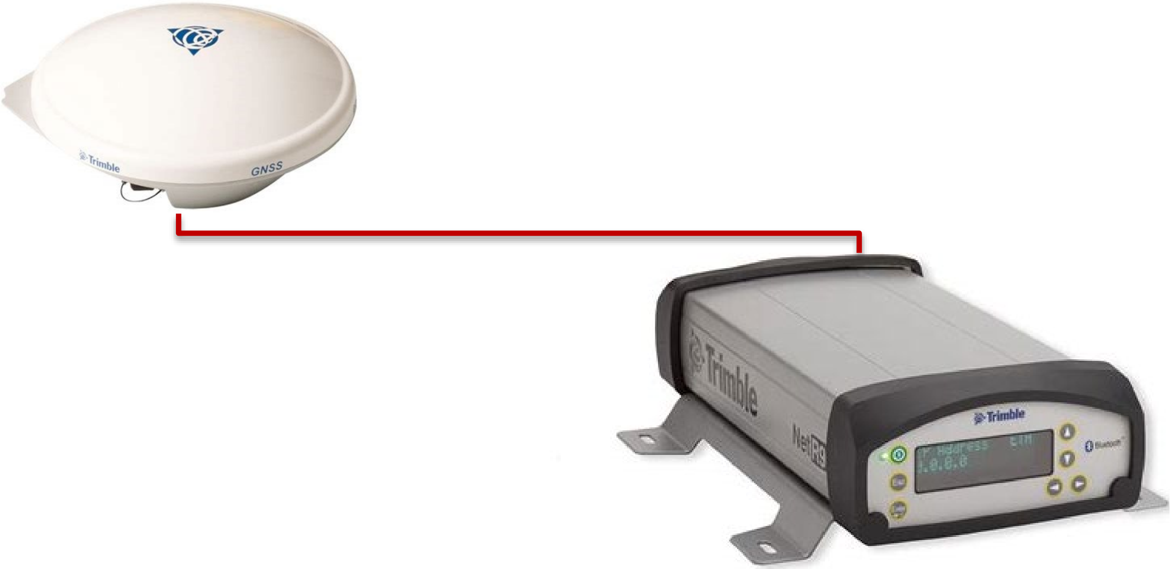
Safety of Life Systems

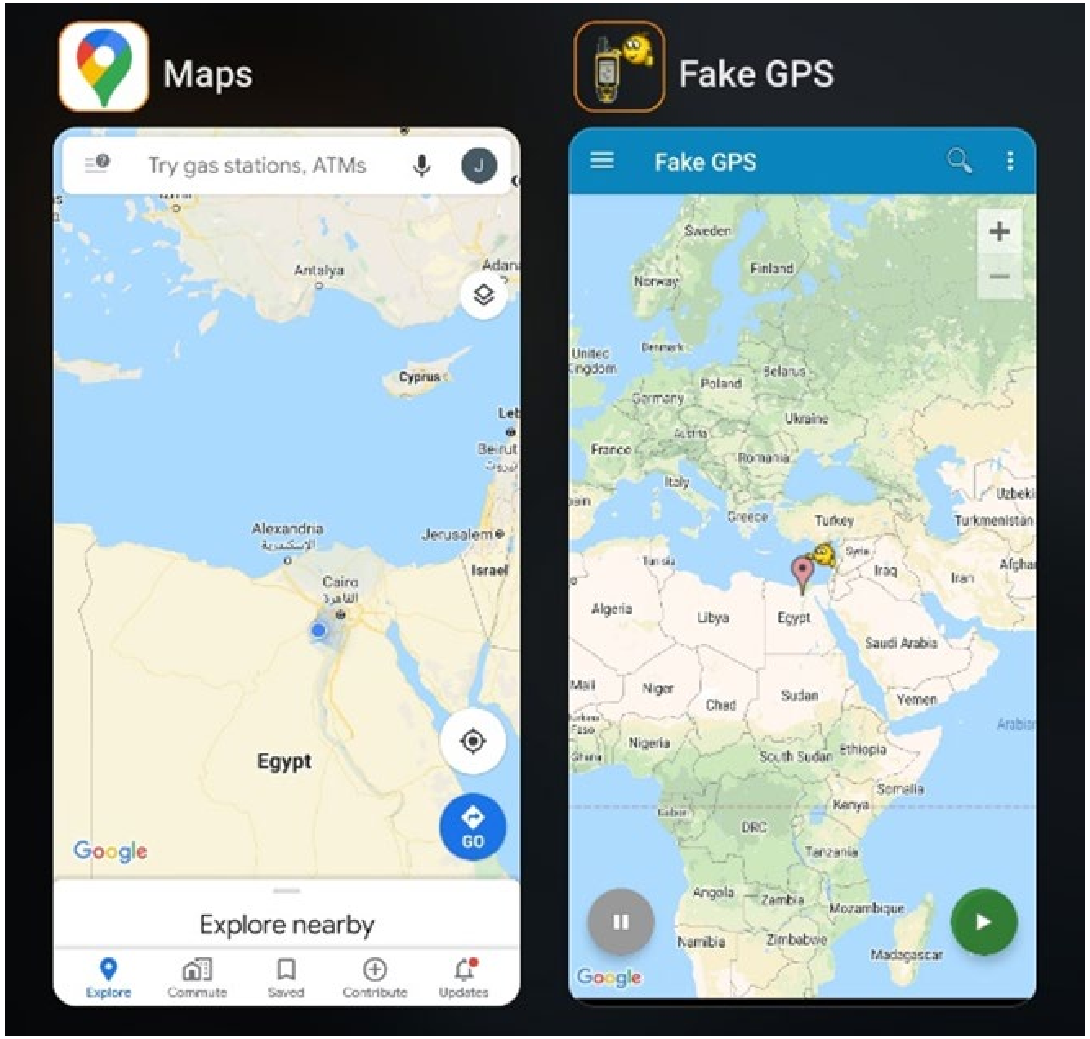
Asset/Fleet Management & Mobile Apps

GNSS

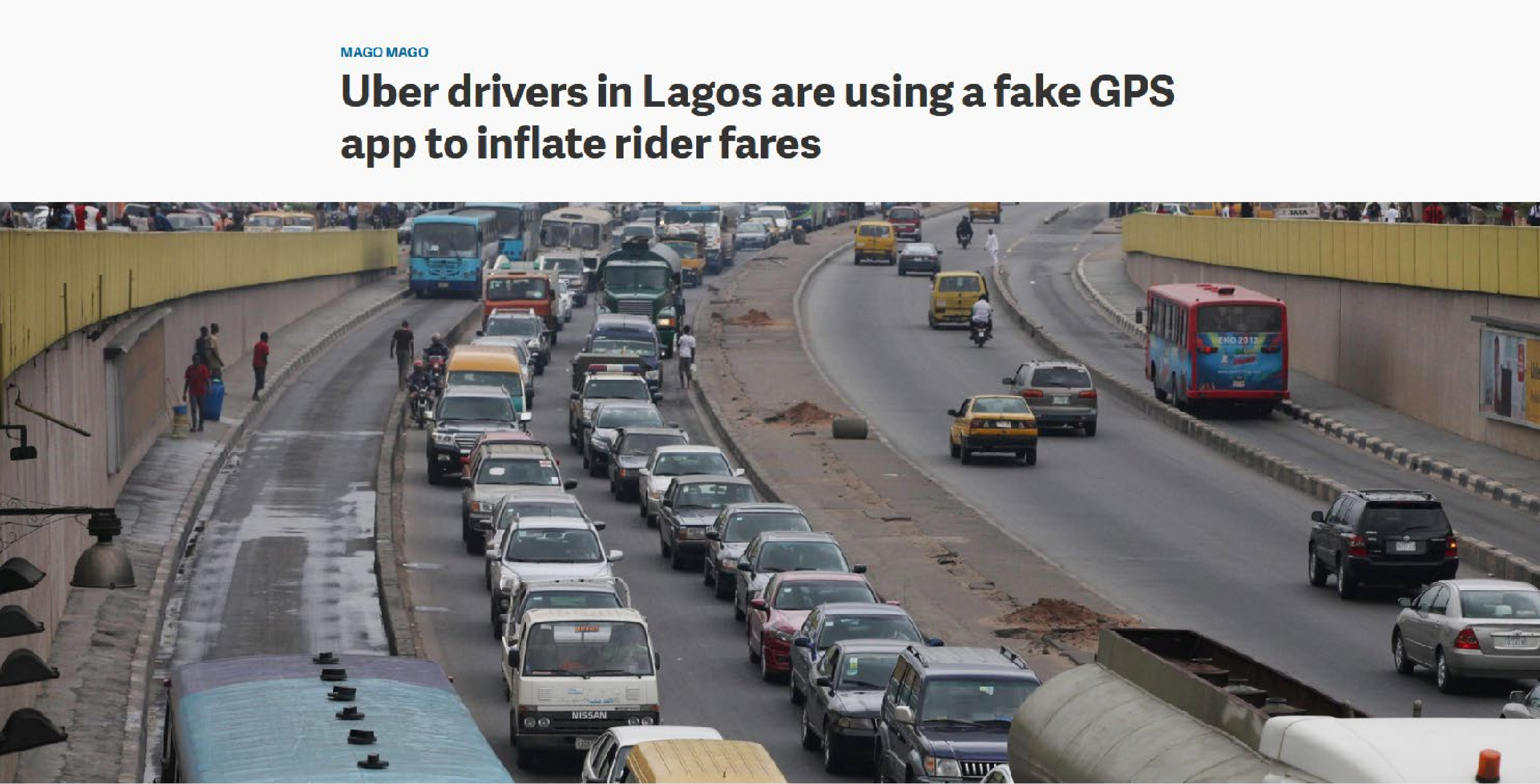
GNSS Spoofing

- **Spoofing GNSS Receiver Input**
    - Signal spoofing
    - Alter ranges and data
- **Spoofing GNSS Receiver Output**
    - Traditional computer security





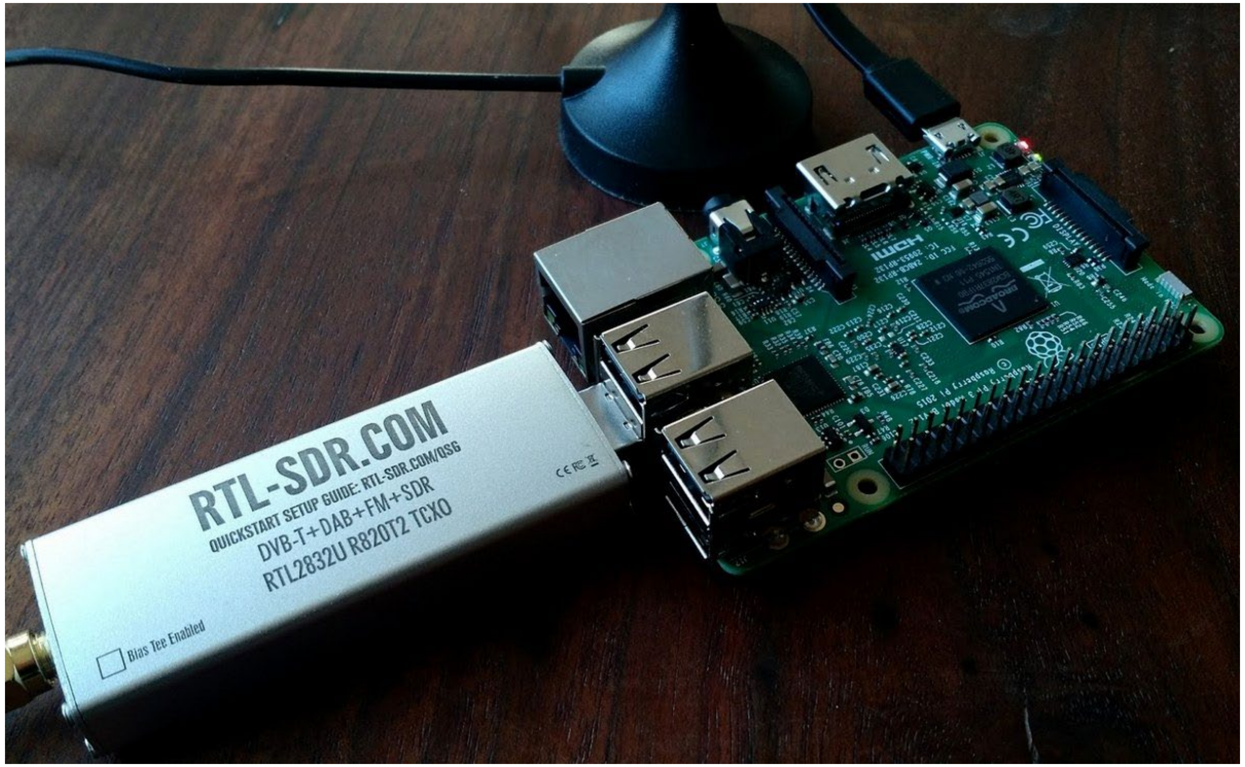
Many Incentives to Spoof GNSS Already Exist

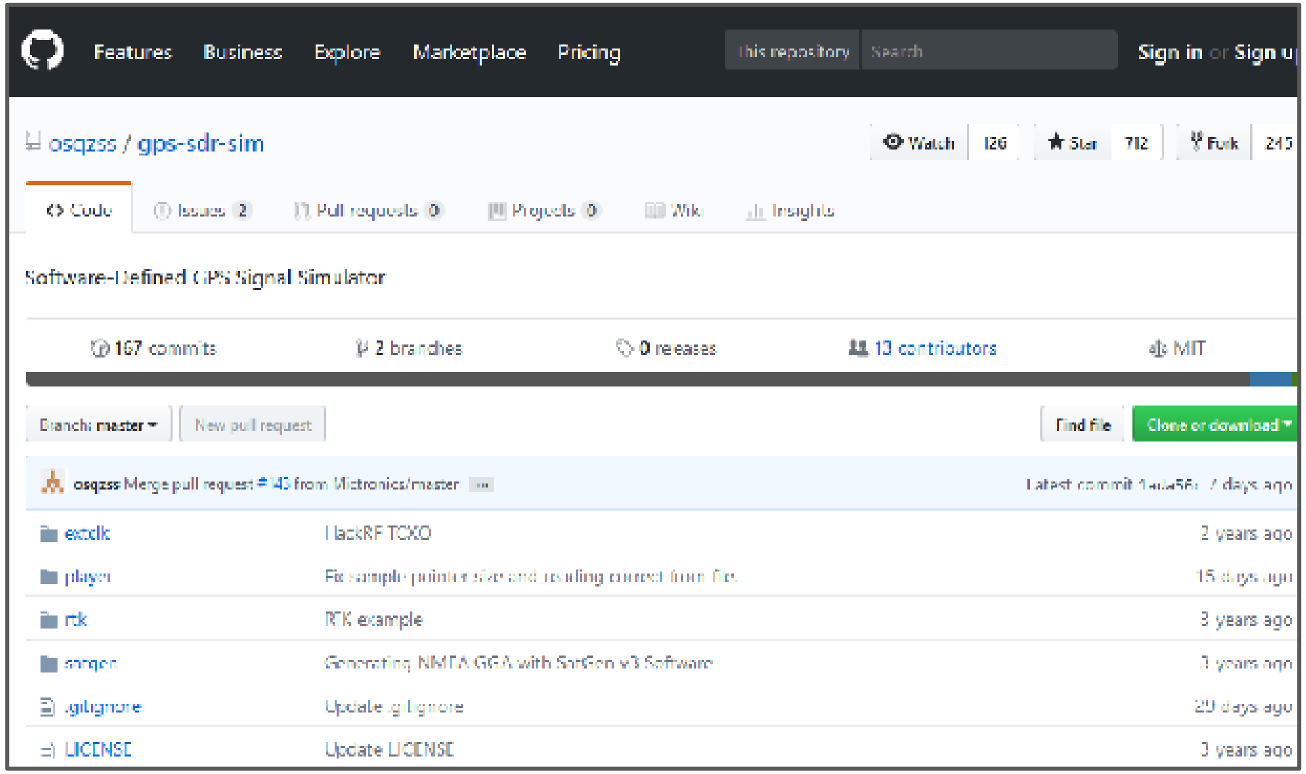


MAGO MAGO

Uber drivers in Lagos are using a fake GPS app to inflate rider fares

Spoofing Can Be Cheap ($30)





osqzss / gps-sdr-sim

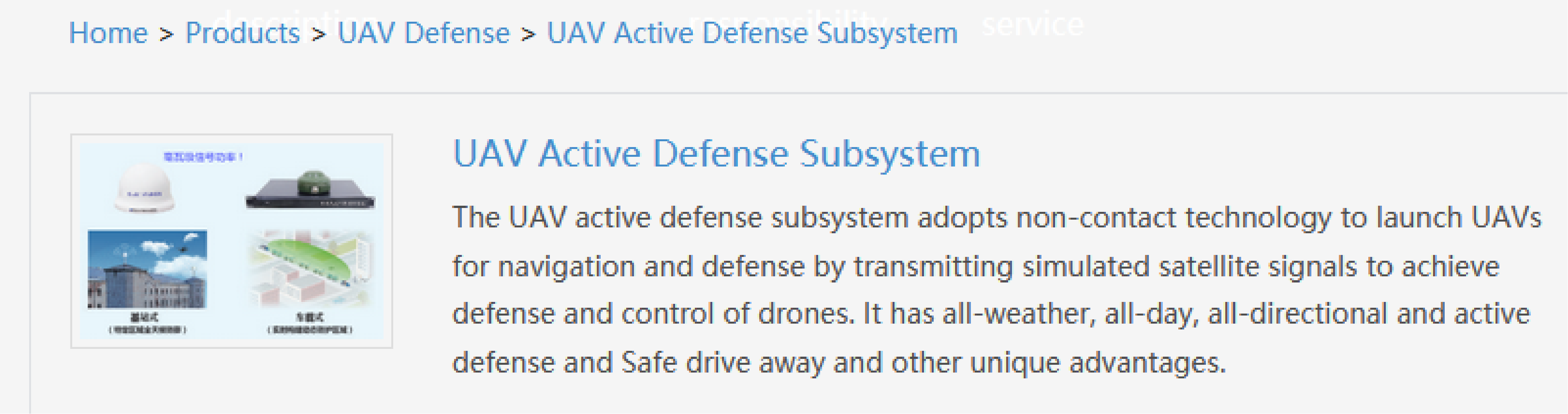
Software-Defined GPS Signal Simulator

167 commits | 2 branches | 0 releases | 13 contributors | MIT

osqzss Merge pull request #143 from Mictronics/master … Latest commit 1a4a56… 7 days ago

extclk	HackRF TCXO	2 years ago
player	Fix sample pointer size and reading correct from file.	15 days ago
rtk	RTK example	3 years ago
satgen	Generating NMEA GGA with SatGen v3 Software	3 years ago
.gitignore	Update .gitignore	29 days ago
LICENSE	Update LICENSE	3 years ago

Spoofing Products Being Sold as Defense



Home > Products > UAV Defense > UAV Active Defense Subsystem

UAV Active Defense Subsystem

The UAV active defense subsystem adopts non-contact technology to launch UAVs for navigation and defense by transmitting simulated satellite signals to achieve defense and control of drones. It has all-weather, all-day, all-directional and active defense and Safe drive away and other unique advantages.

Spoof Detection & Mitigation Characteristics

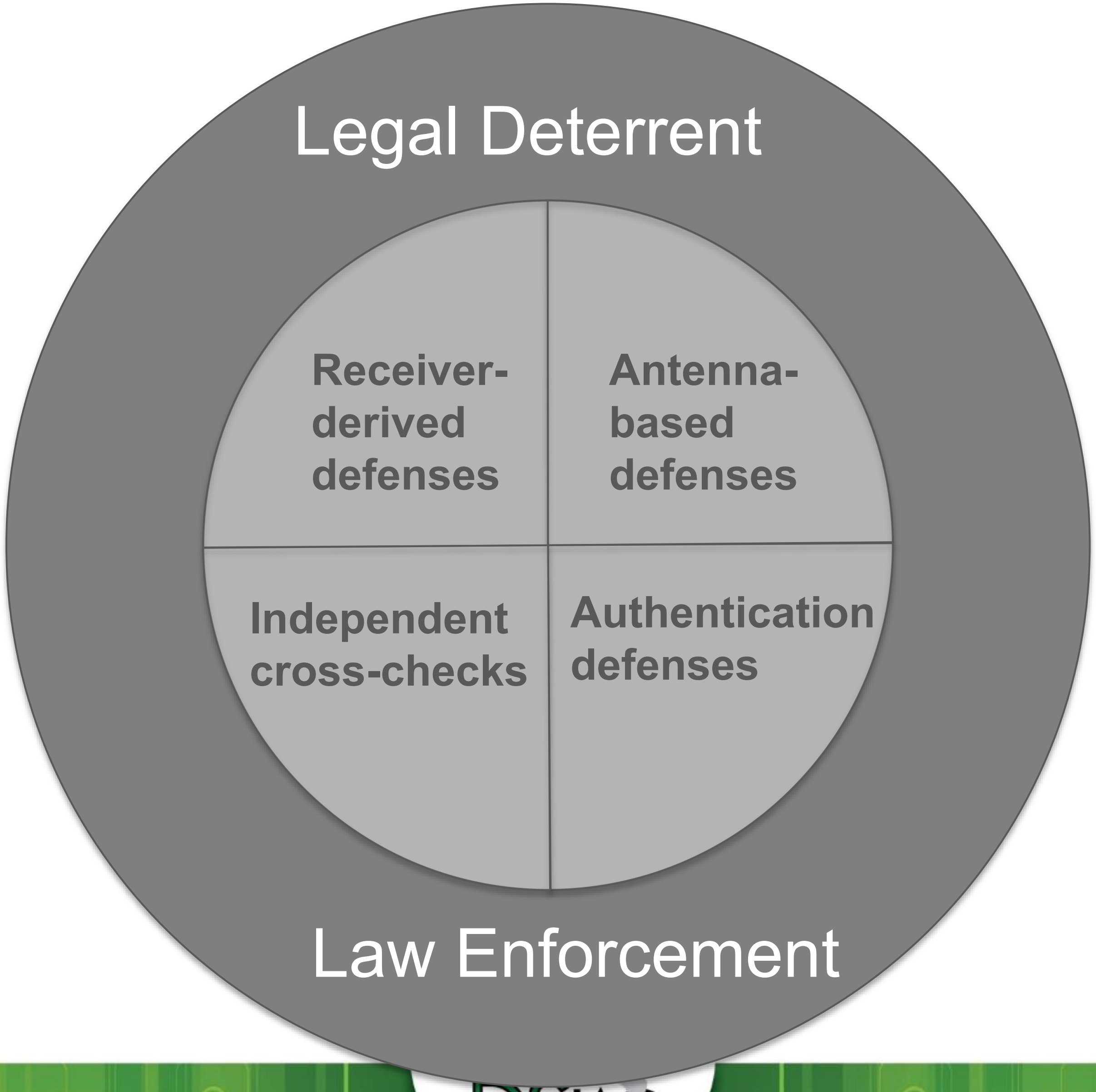
- Practical – reasonable to implement.

- Robust – low false alert and missed detection rate.

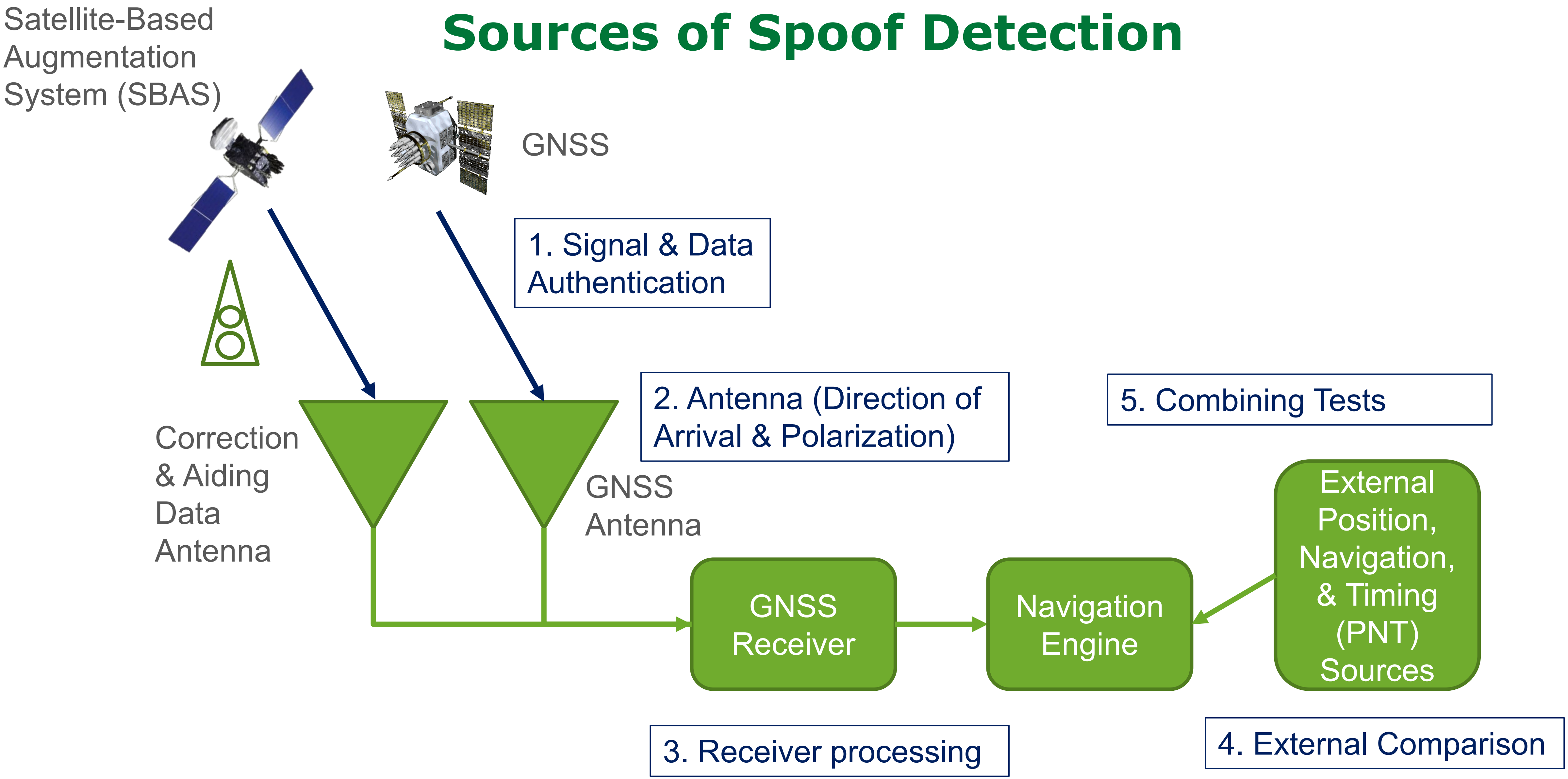
- There are NO SILVER BULLETS.

- Combine several techniques as driven by application needs.

Defense in Depth for Spoofing



Sources of Spoof Detection



Satellite-Based Augmentation System (SBAS)

GNSS

1. Signal & Data Authentication

2. Antenna (Direction of Arrival & Polarization)

5. Combining Tests

Correction & Aiding Data Antenna

GNSS Antenna

GNSS Receiver

Navigation Engine

External Position, Navigation, & Timing (PNT) Sources

3. Receiver processing

4. External Comparison

Spoof Detection Technology Overview

1. Authentication Signal Design: Current State of the Art

- Data authentication, signal authentication, network-based authentication

2. Antenna-Based Spoof Detection Based on Direction of Arrival

- Dual-polarization antenna, controlled reception pattern antenna

3. Receiver Measurement-Based Detection

- Power, residual & consistency, correlator residuals (floating correlator), continuity

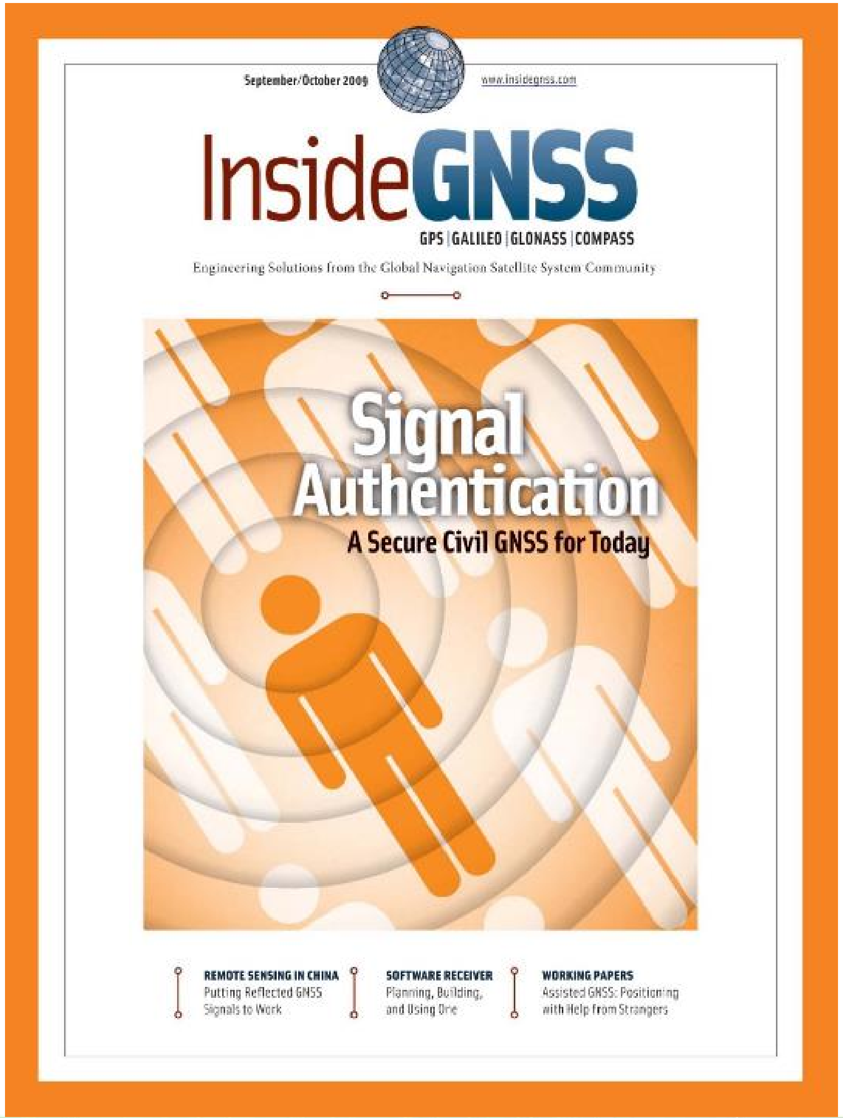
4. Comparison With Independent PNT Sources

- Inertials, alternative navigation systems, odometry (wheel counter & visual), etc.

5. Combining Tests

1. Authentication Signal: Current State of the Art

- Signal Authentication – develop signal whose source/ranges can be verified.
- Encrypted (Hidden) Signals – requires user/user equipment that can keep a secret.
- Networked-Based Authentication – use signal comparison of hidden signal components with a trusted source.
- Civil signal authentication cannot rely on secure user equipment – CHIMERA being proposed as public signal authentication.
- Data Authentication – verify that data has been unadulterated.



September/October 2009 www.insidegnss.com

InsideGNSS

GPS | GALILEO | GLONASS | COMPASS

Engineering Solutions from the Global Navigation Satellite System Community

Signal Authentication

A Secure Civil GNSS for Today

REMOTE SENSING IN CHINA
Putting Reflected GNSS Signals to Work

SOFTWARE RECEIVER
Planning, Building, and Using One

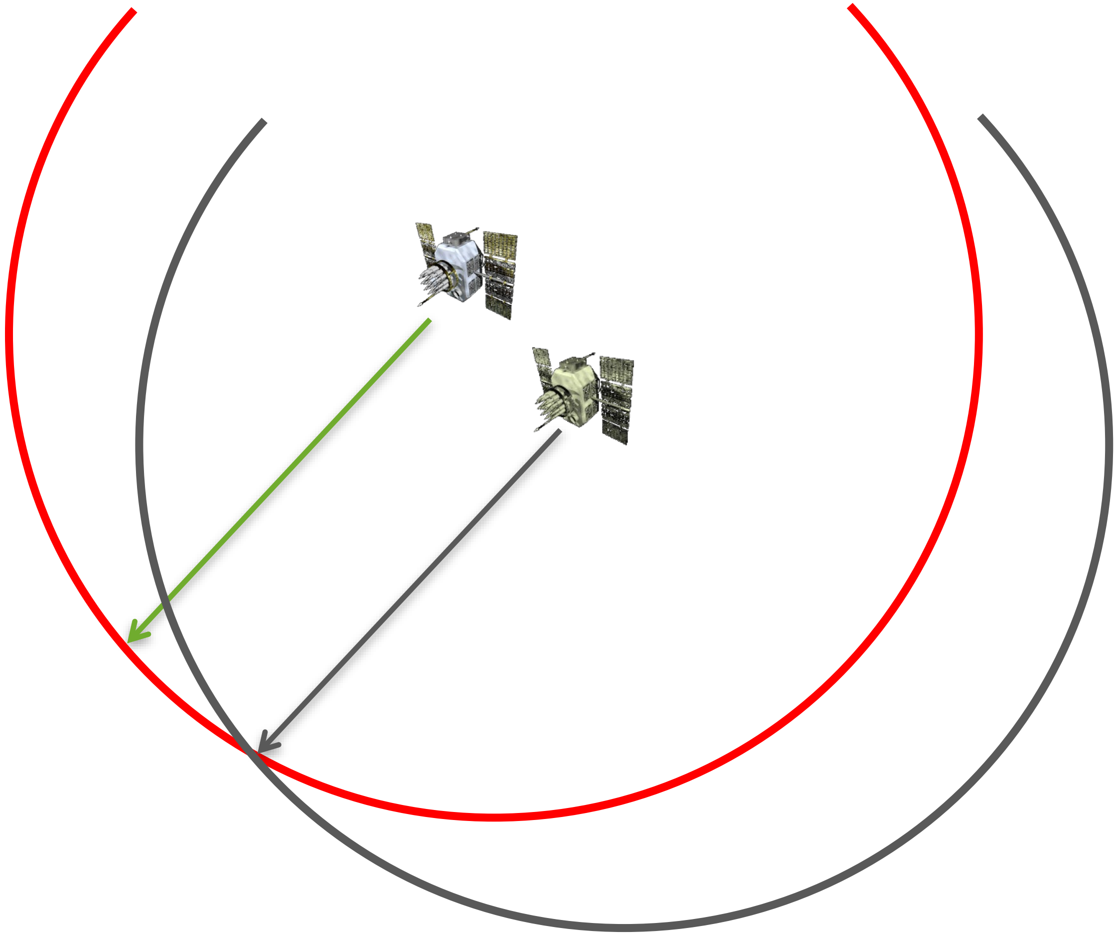
WORKING PAPERS
Assisted GNSS: Positioning with Help from Strangers

Data Authentication

- Altering transmitted data can change calculated position.

- Need as building block to civil signal authentication.

- Designing data authentication for aviation GNSS systems.

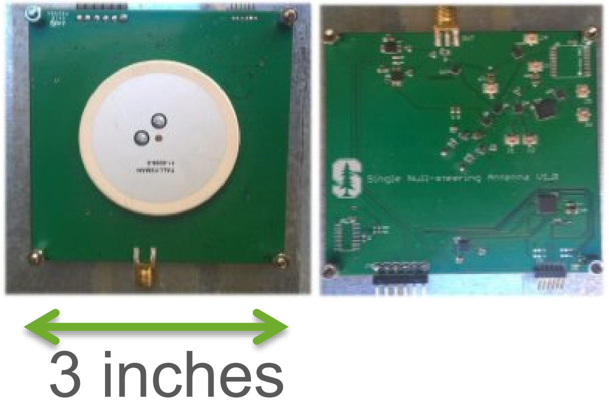


2. Antenna-Based Spoof Detection Based on Direction of Arrival

- **Antenna technologies can be used to identify physical characteristics of the genuine signal that the attacker may not replicate.**
  - Direction of arrival (DOA)

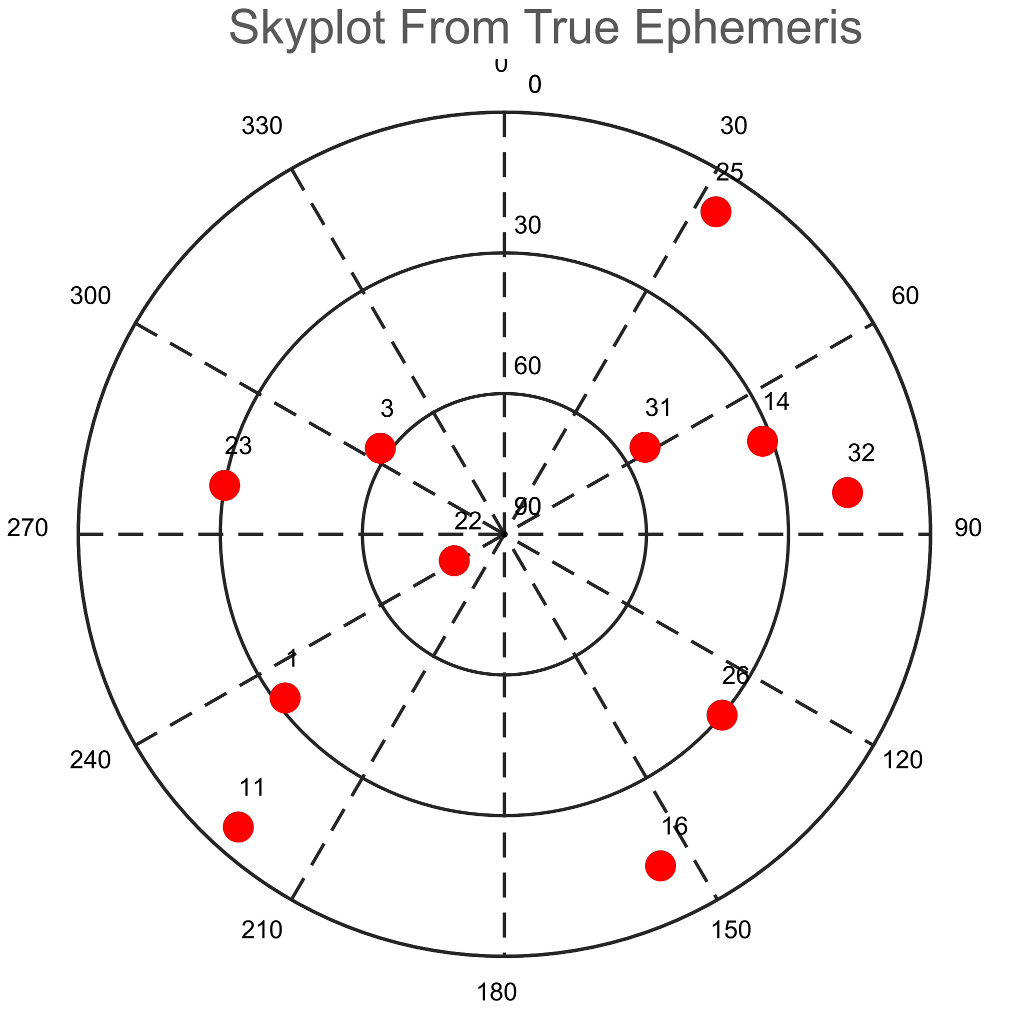
- **Enhanced antenna technologies include multielement antennas & polarization antenna.**
  - International Traffic in Arms Regulations now allows three-element antennas.

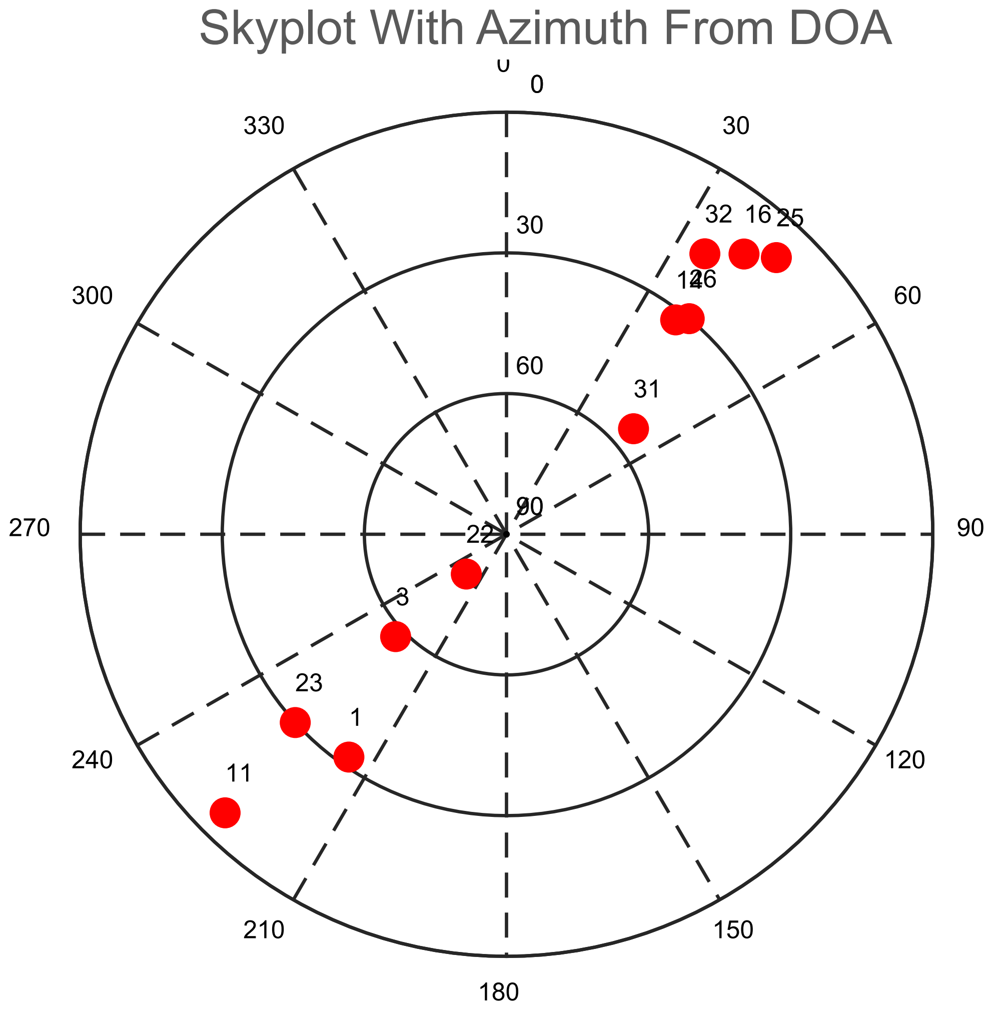
- **Developing small single antenna to support DOA.**



Reference: McMilin, E. "Single Antenna Null Steering for GPS & GNSS Aerial Applications." Ph.D., Stanford, 2016.

Direction of Arrival Estimates


Skyplot From True Ephemeris


Skyplot With Azimuth From DOA

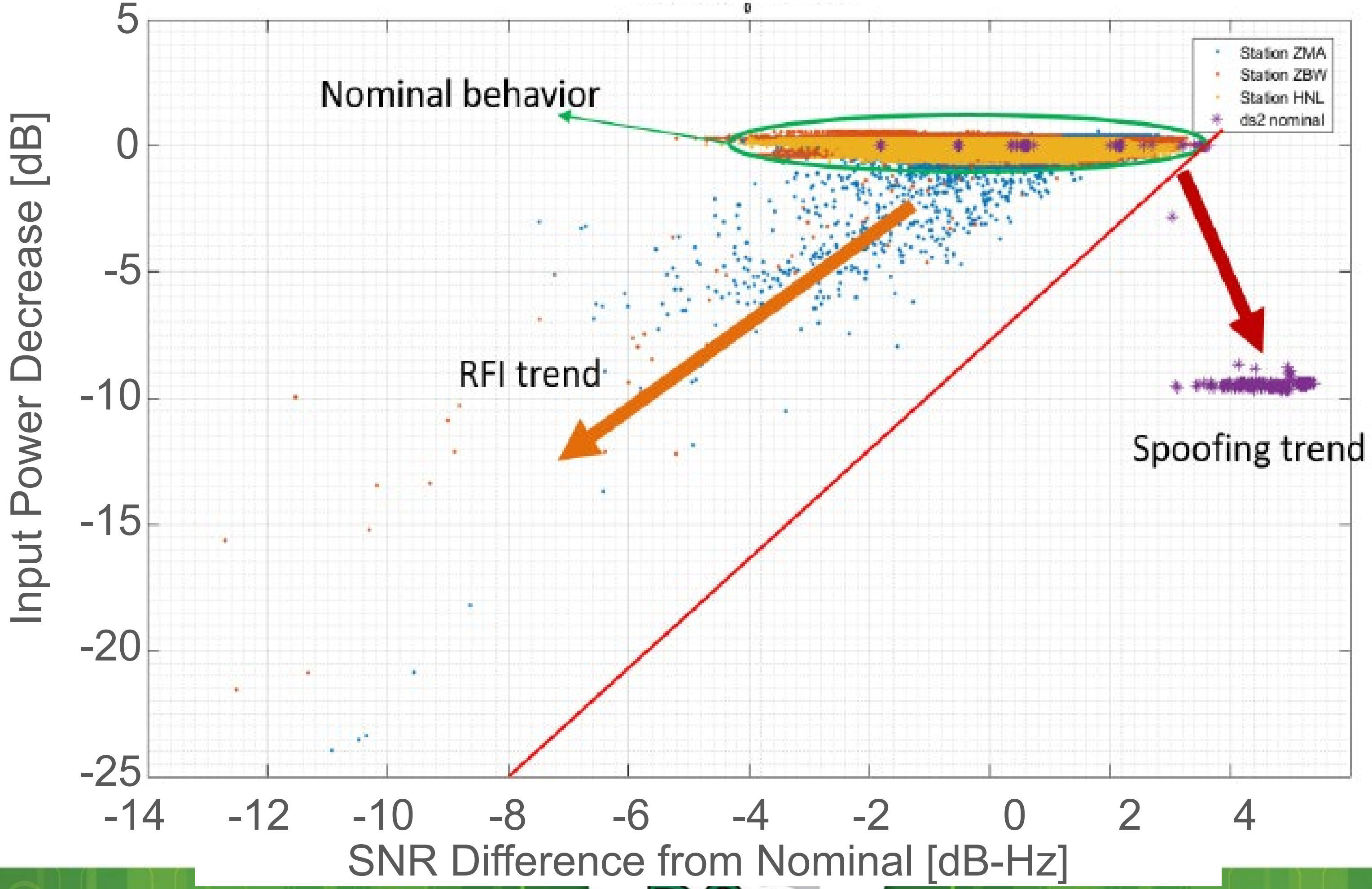
Chen et al. "Demonstrating Single Element Null Steering Antenna Direction Finding for Interference Detection." ION ITM, 2018.

3. Receiver Measurement-Based Detection

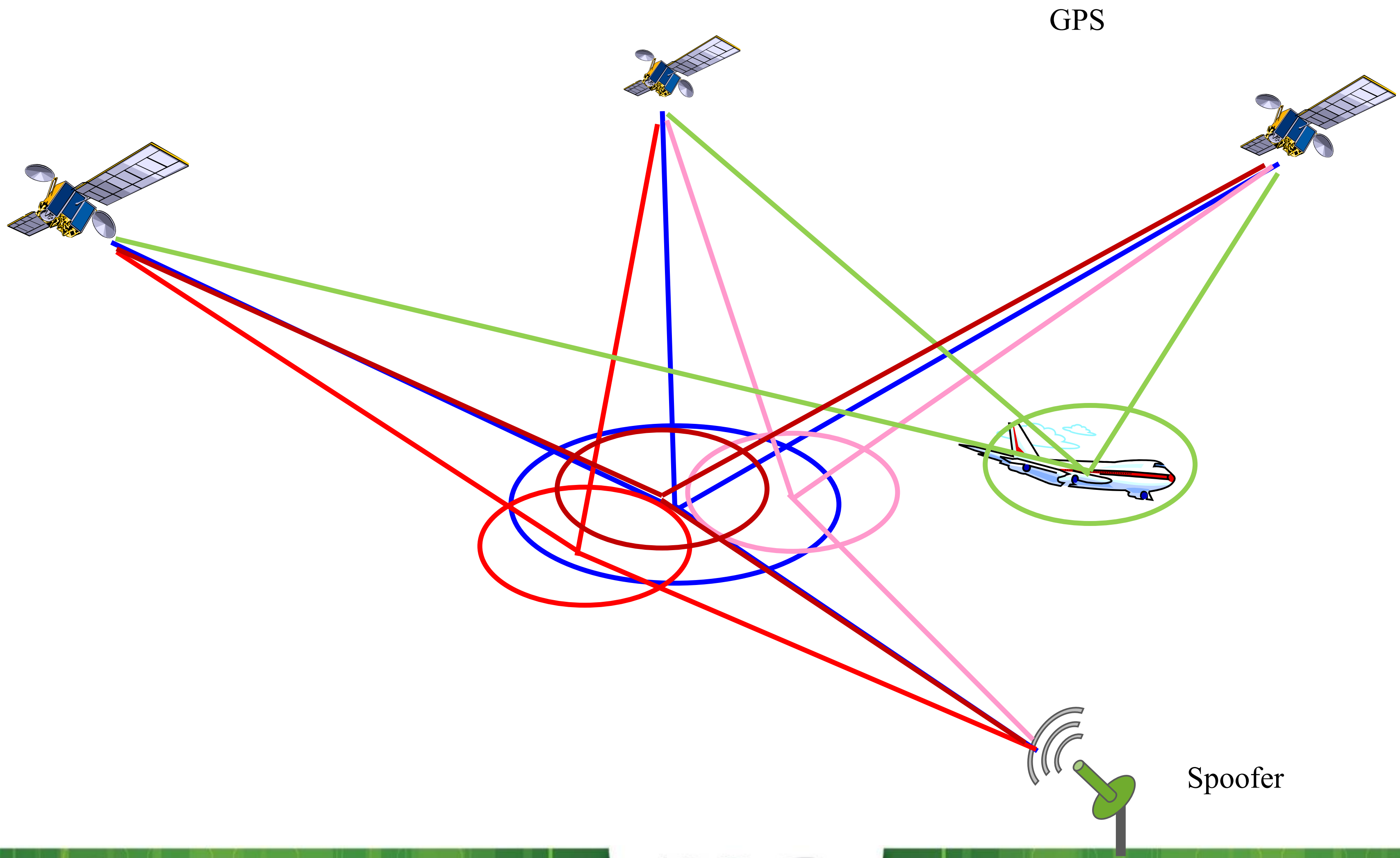
- Power Monitoring: input power & signal-to-noise ratio (SNR).
- Consistency Check: examine consistency of ranges from each satellite.
- Others - Floating Correlator/Complex Ambiguity Function: examine for additional signals from the same satellite.

Input Power and SNR

- Receivers already measure input power (mostly thermal noise).
- SNR measures power ratio of GPS to noise.



Basic Concept of Redundancy (Residuals) Check

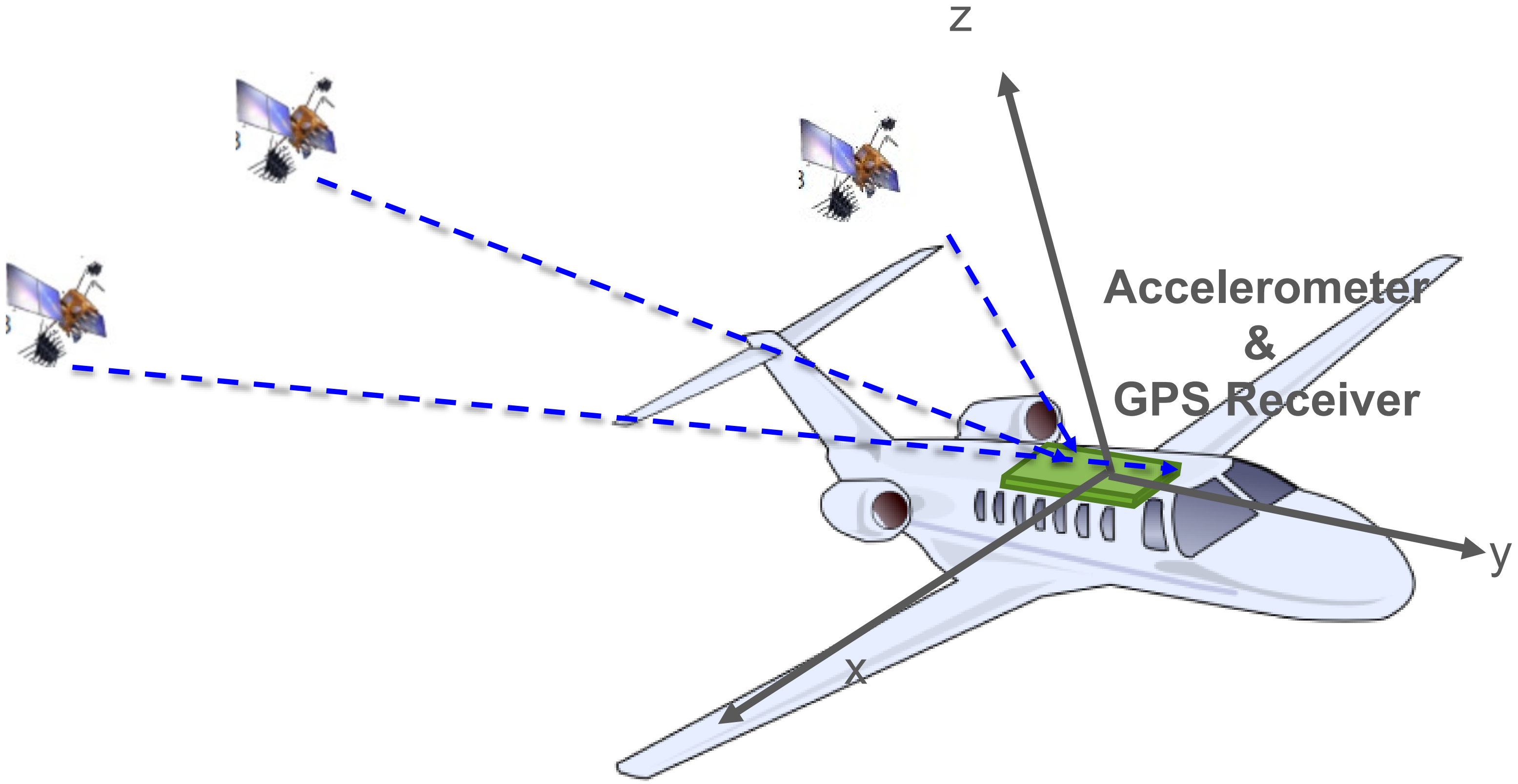


4. Comparison With Independent PNT sources

- **Compare position solutions with independent position solution.**
  - Inertial navigation system, other radio navigation (Loran, DME, cellular, etc.).

- **Compare intermediate measurement results: acceleration from accelerometer with GNSS acceleration, range rate from satellites.**

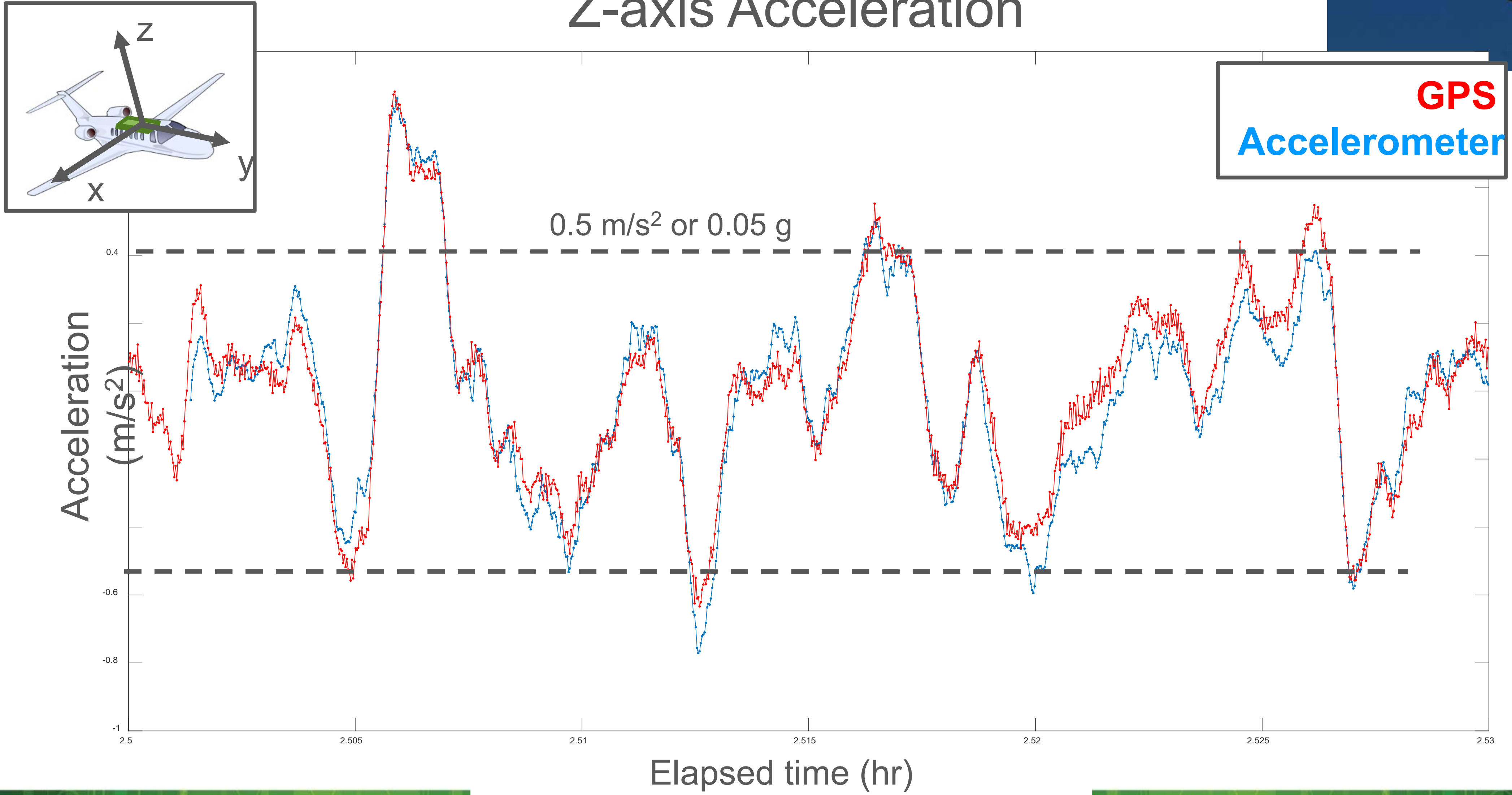
Antispoofing via User Motion: Low-Cost Accelerometer Integration



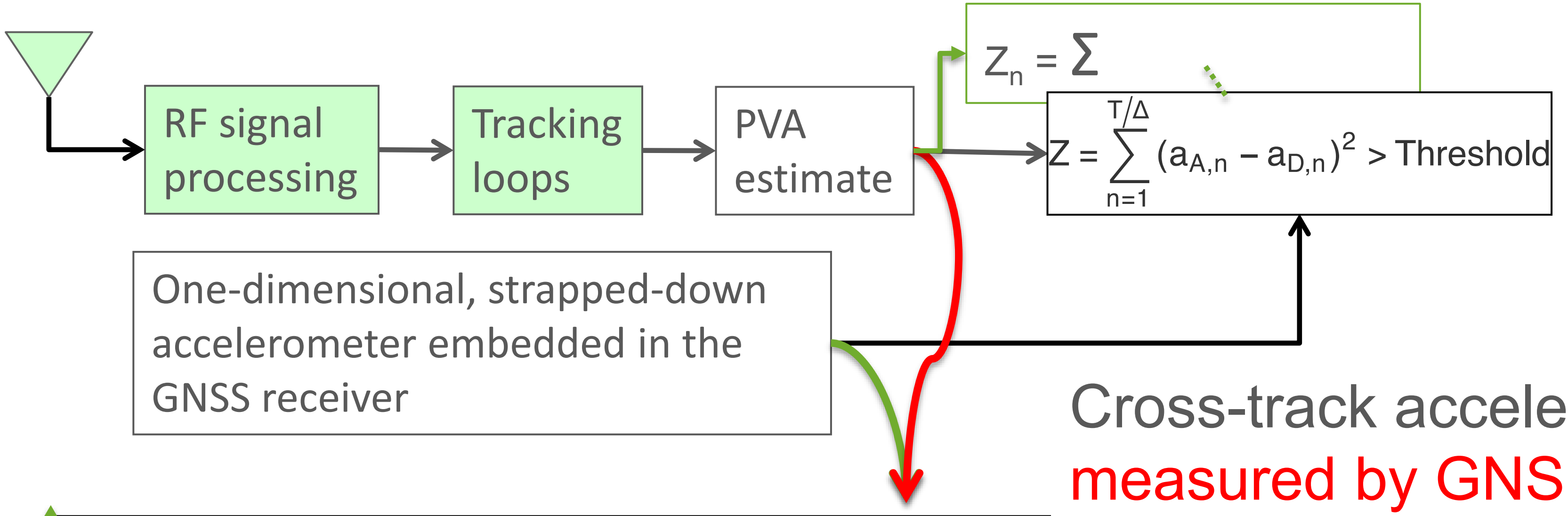
Accelerometers can provide an independent measure of user motion.

Motions that deviate from expected can indicate GPS spoofing.

Spoof Detection From Low-Cost Accels in Flight



Spoof Detection From Low-Cost Accels in Cars

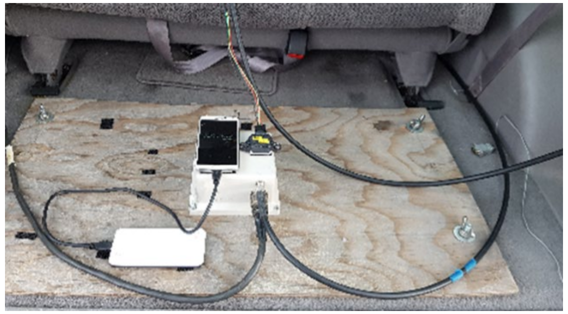


Test Statistics

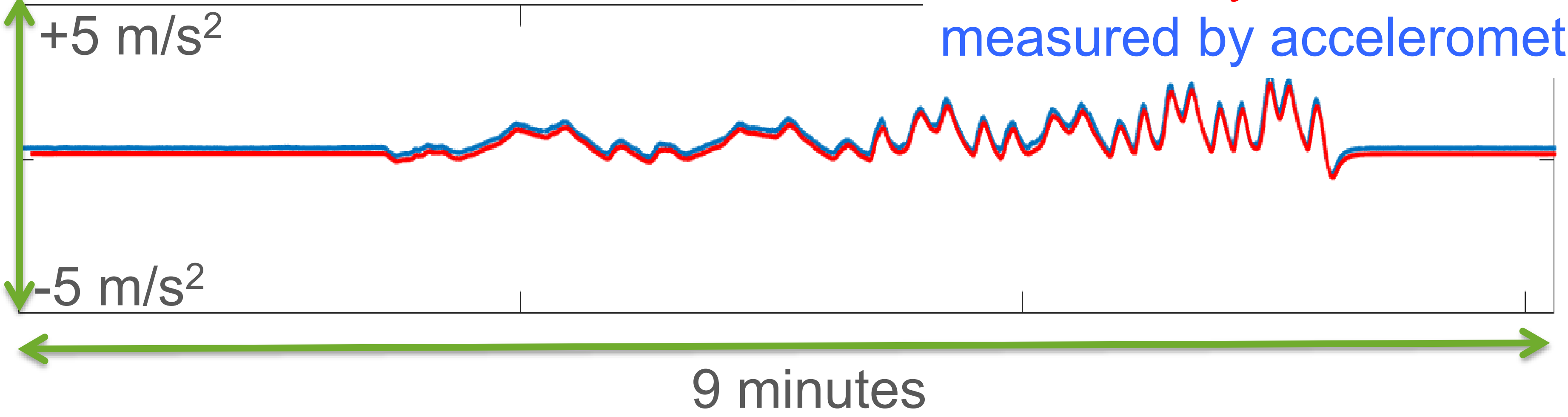
$Z_n = \Sigma$

$$Z = \sum_{n=1}^{T/\Delta} (a_{A,n} - a_{D,n})^2 > \text{Threshold}$$

One-dimensional, strapped-down accelerometer embedded in the GNSS receiver



Cross-track acceleration
measured by GNSS in red
measured by accelerometer in blue



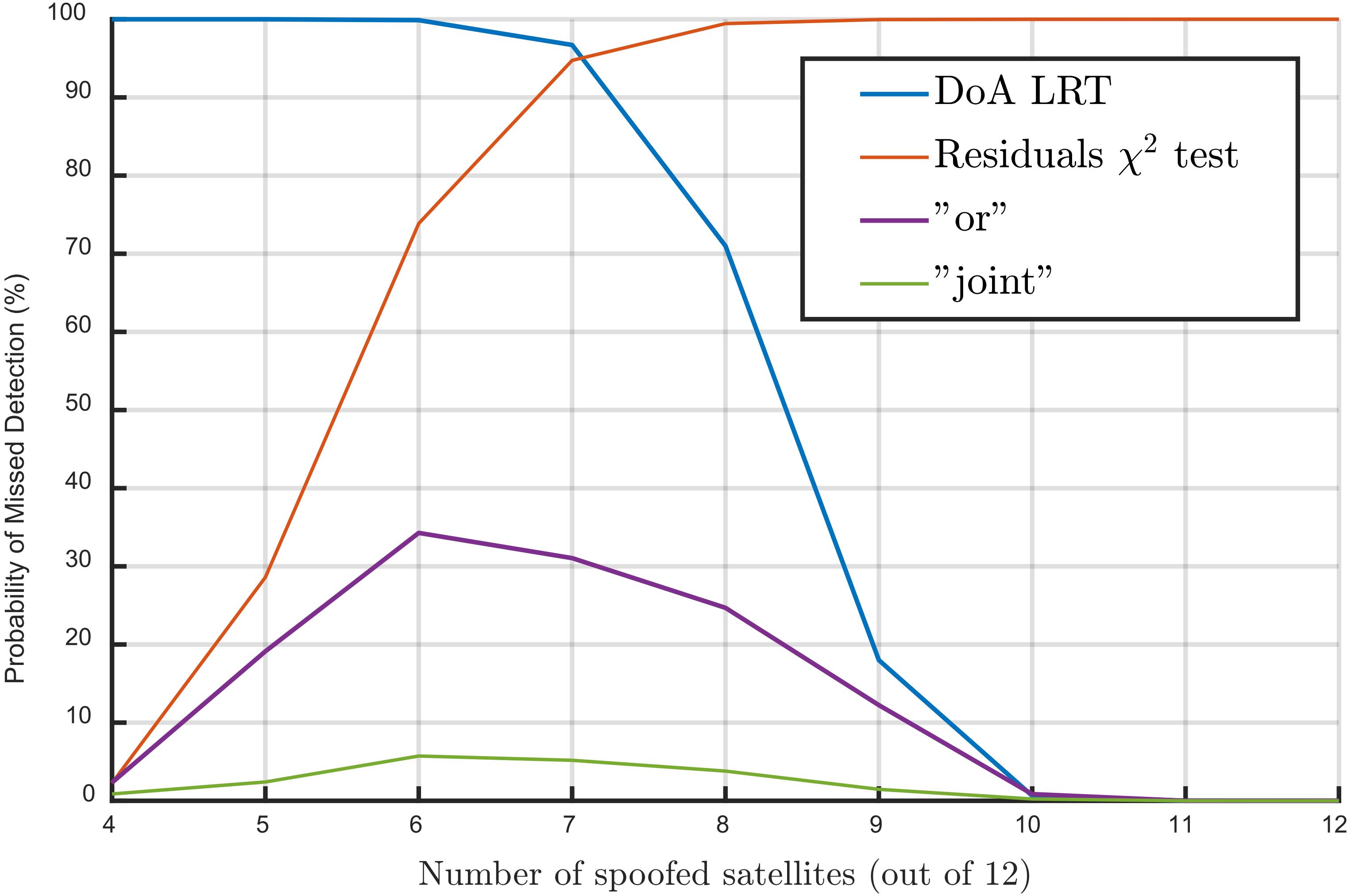
5. Combining Tests

- **Detection tests can be dependent (similar or complimentary) or independent.**

- **Example: power/SNR test good against high-power spoofing signal quality & residuals test good against equal power; DOA is good against high power but also can be useful at equal powers.**

- **How do we combine tests to maximize their effectiveness?**
  - Simply "OR" the tests.
  - We can do much better with a smarter combination.

Generalized Likelihood Ratio Test (GLRT)



Rothmaier, F., L. Sherman, and T. Walter. "A Framework for Multi-metric GNSS Spoof Detection With Provable Performance." Submission to Navigation Journal.

Summary & Conclusion

- GNSS spoofing is a growing threat that needs to be mitigated as we increase reliance on GNSS for safety and infrastructure.

- Many mitigations have been developed – we covered a sample of them here. Mitigations should form part of an overall strategy to handle GNSS vulnerabilities.

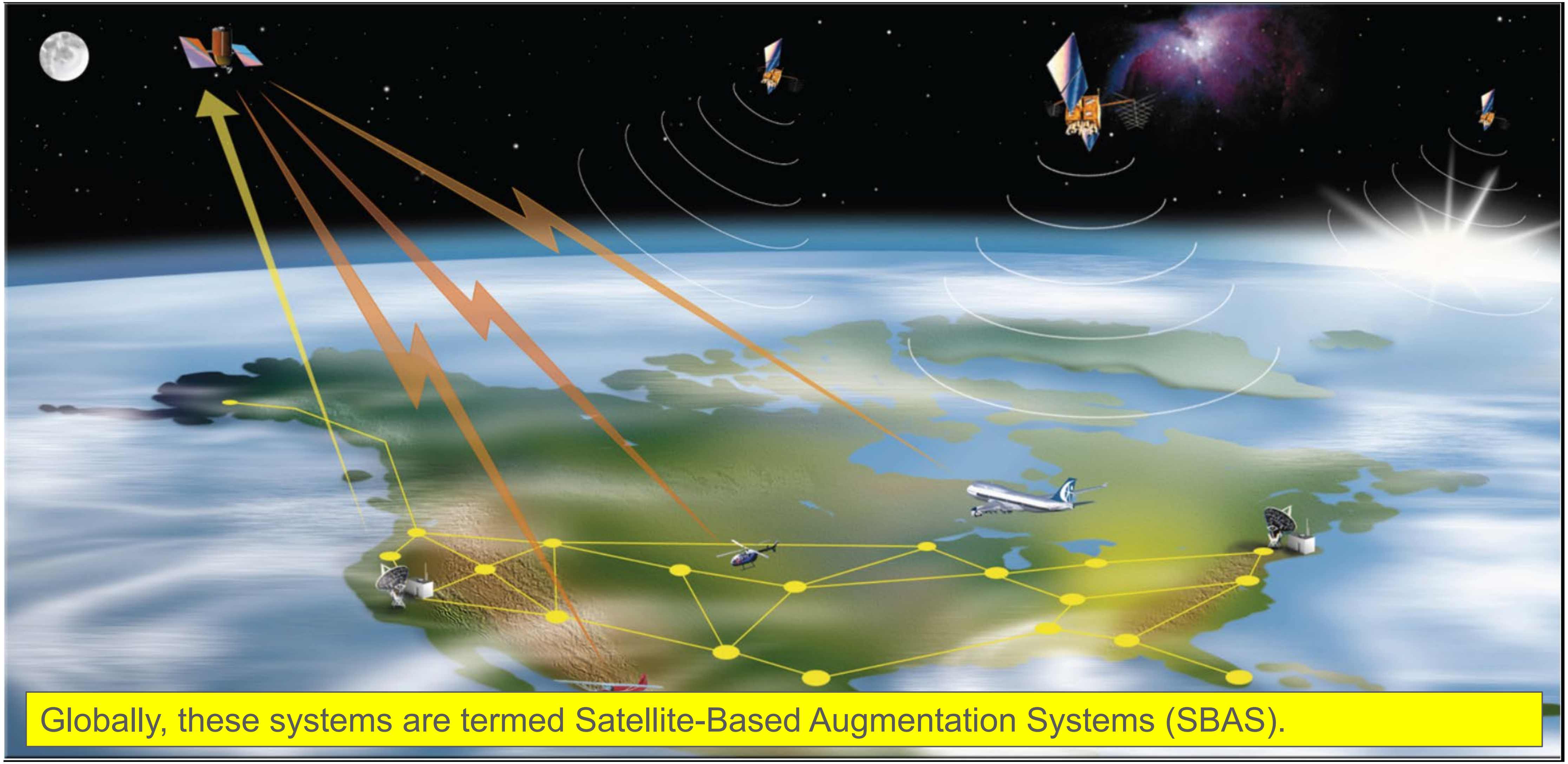
- Need to mature these technologies and develop best combinations adapted for the characteristics of each application.

ADDITIONAL INFORMATION

GNSS for Safety of Life Applications

- Use of GNSS safety of life applications requires integrity.
- Integrity is given by a high confidence on bound position error.
- Traditionally derived from analysis and monitoring of GNSS of natural and accidental sources of errors.
- Today, integrity must also encompass deliberate or accidental spoofing threats.

Wide Area Augmentation System (WAAS)



Globally, these systems are termed Satellite-Based Augmentation Systems (SBAS).

Source: FAA

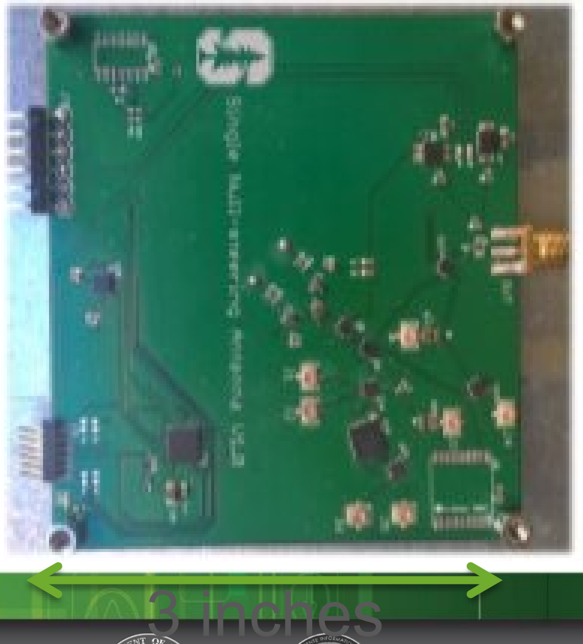
Dual Polarization Antenna (DPA)

- DPA is a patch antenna that can receive and distinguish right-hand circular polarization (RHCP) and left-hand circular polarization (LHCP) signals; it uses this to determine direction of arrival (DOA).

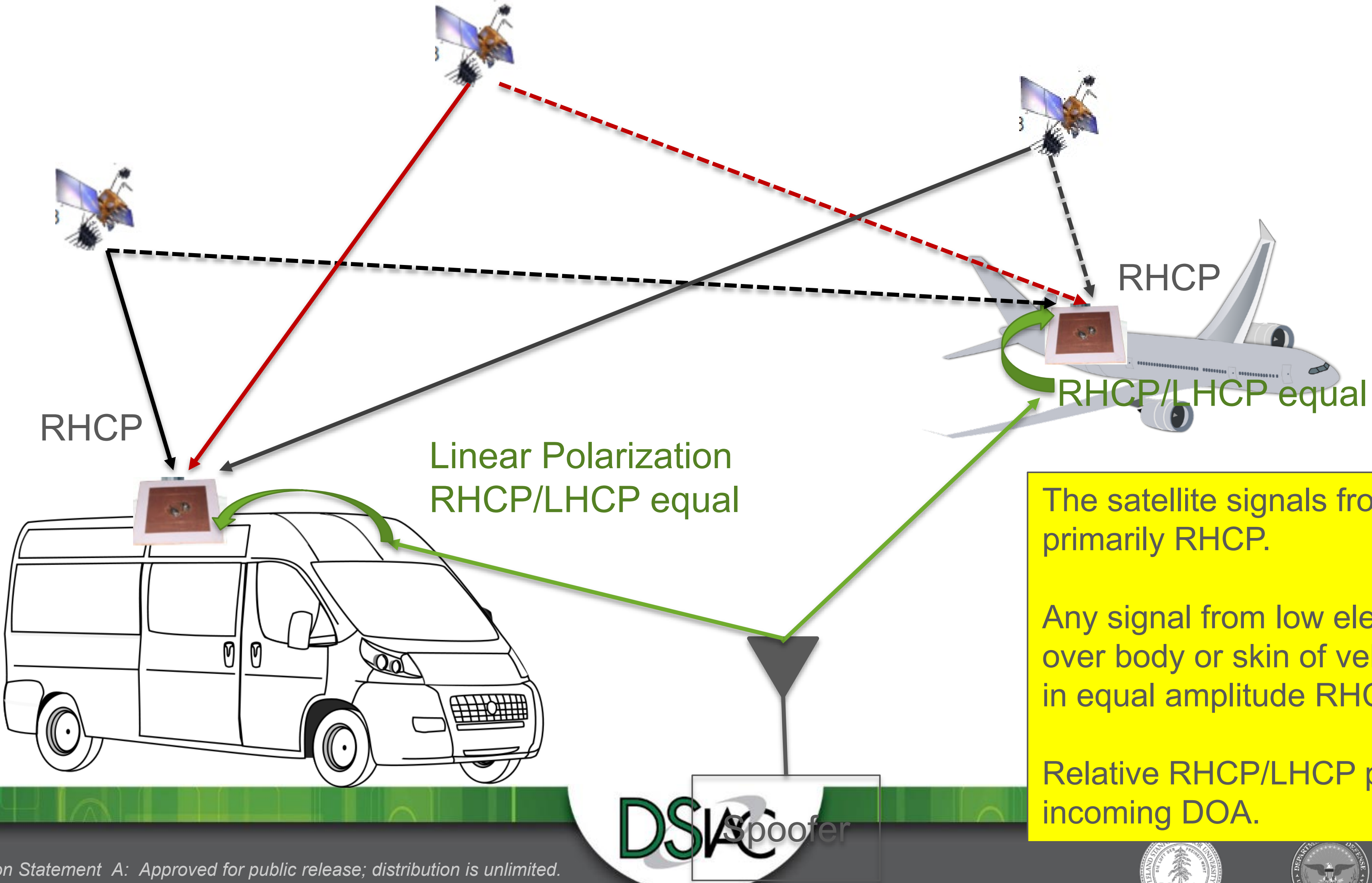
- Allows determining DOA of signals impinging on the ground plane.

- Important Characteristics:
  - Spoof detection & jamming mitigation, direction finding
  - Small form factor & single antenna & can be built from commercial off-the-shelf components
  - Only needs one cable (useful for aviation and other applications)

Reference: McMilin, E. "Single Antenna Null Steering for GPS & GNSS Aerial Applications." Ph.D., Stanford, 2016.



Polarization of Different Signals

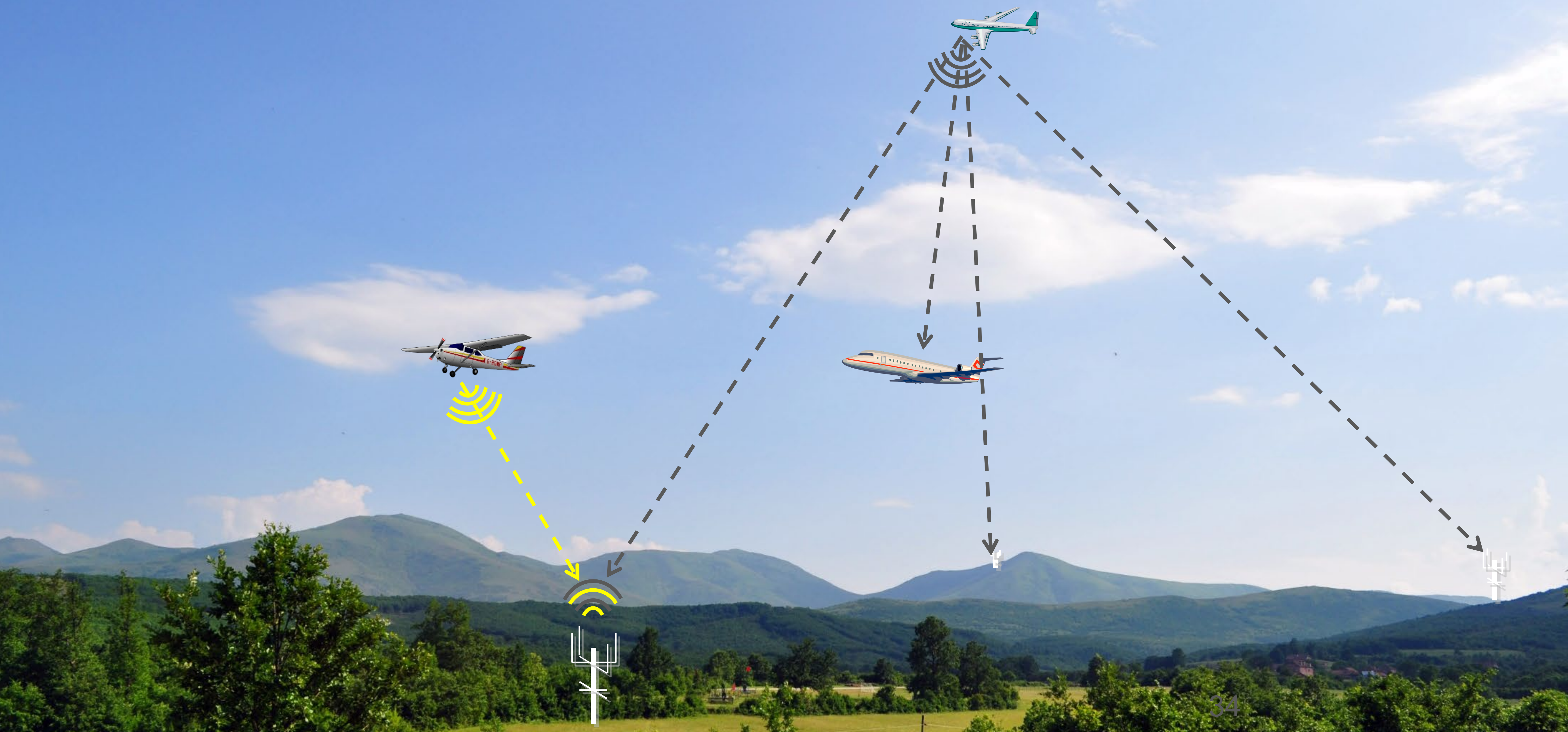


The satellite signals from above are primarily RHCP.

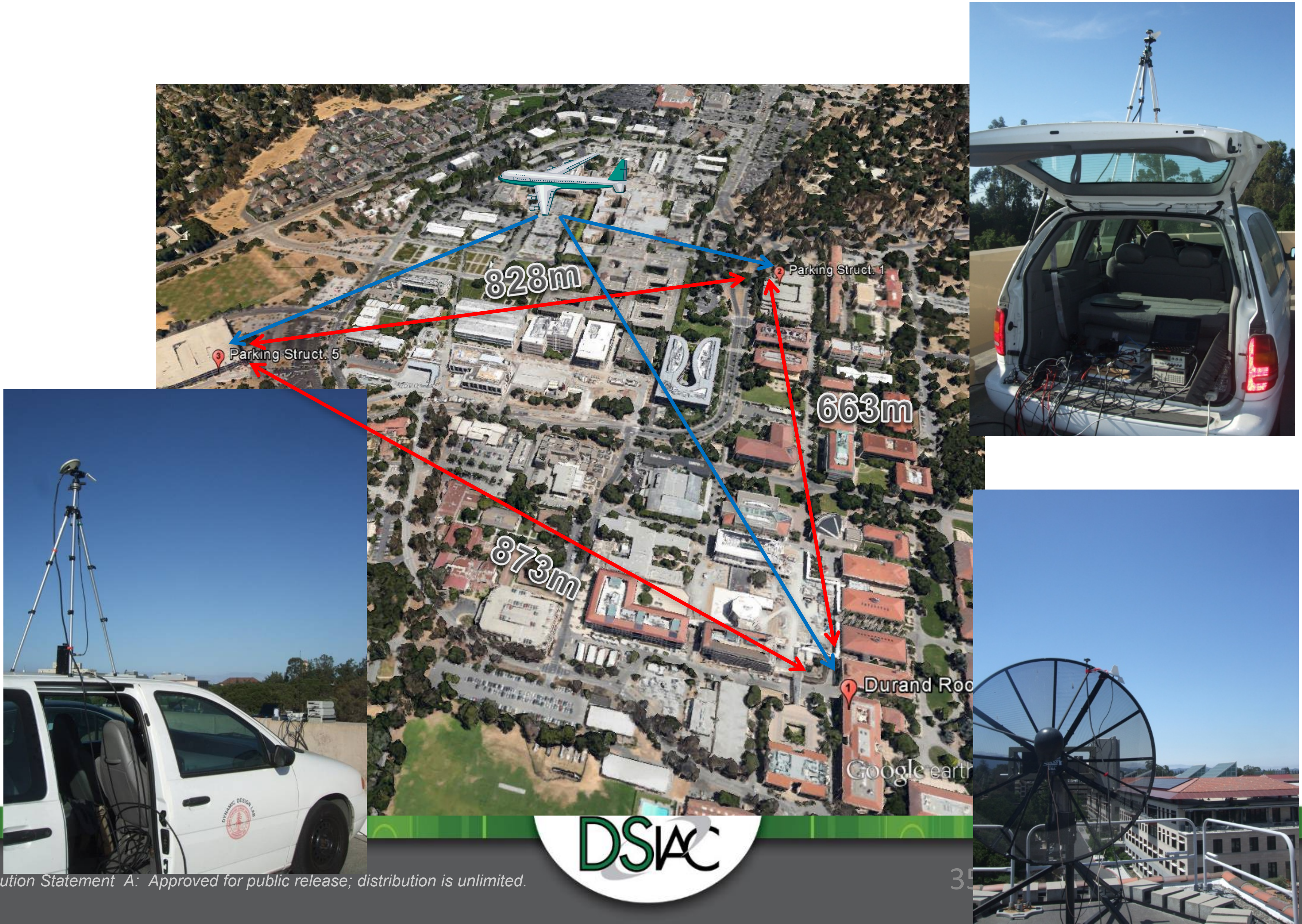
Any signal from low elevation that goes over body or skin of vehicle frame results in equal amplitude RHCP/LHCP.

Relative RHCP/LHCP phase related to incoming DOA.

Multilateration to Verify GNSS Position of Automatic, Dependent Surveillance Broadcast (ADS-B)



ADS-B Multilateration/Passive Ranging Data Collection Setup



Position Calculation

Positioning using time difference of arrival and aircraft’s altitude

$$c \times (TOA_1 - TOA_2) = \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2} - \sqrt{(x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2}$$

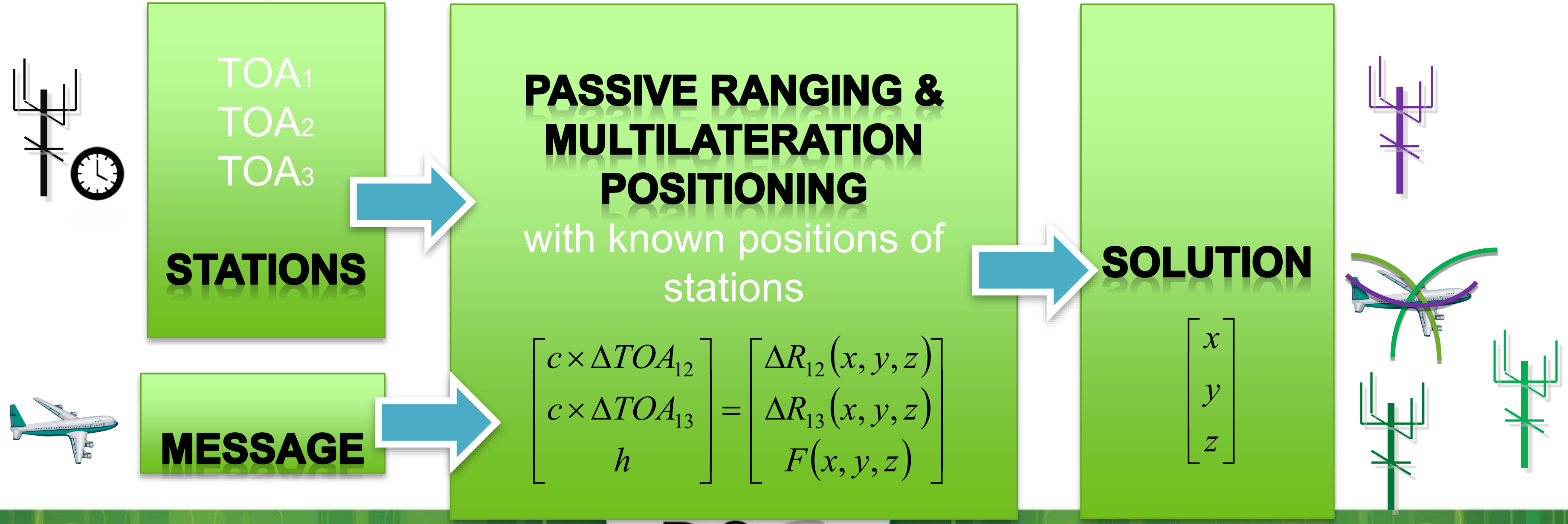
$$c \times (TOA_1 - TOA_3) = \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2} - \sqrt{(x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2}$$

$$h = F(x, y, z)$$

x, y, z is the aircraft's position

x_k, y_k, z_k is k$^{\text{th}}$ ground station's position

h is barometric altitude



TOA1
TOA2
TOA3

STATIONS

MESSAGE

PASSIVE RANGING & MULTILATERATION POSITIONING

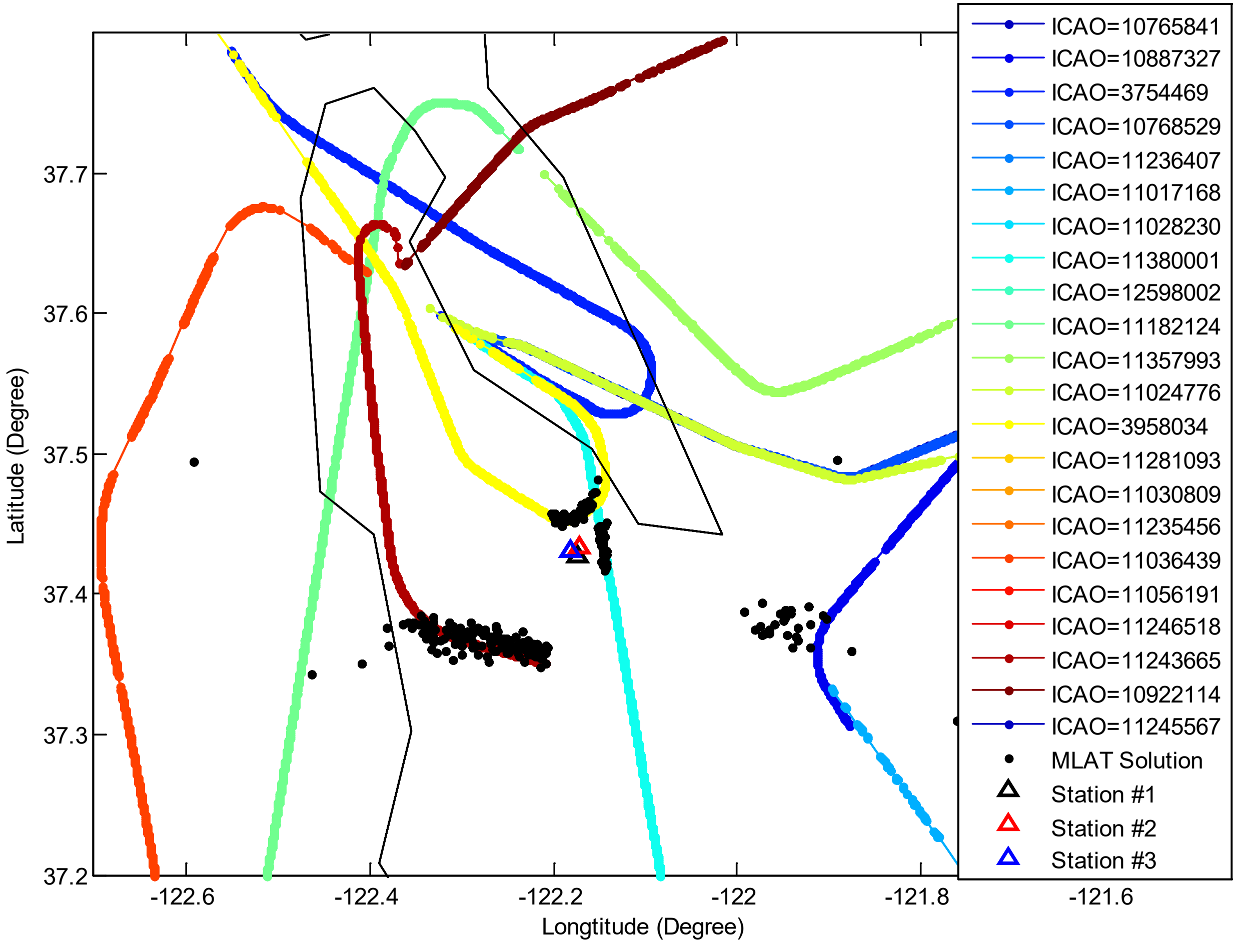
with known positions of stations

$$\begin{bmatrix} c \times \Delta TOA_{12} \\ c \times \Delta TOA_{13} \\ h \end{bmatrix} = \begin{bmatrix} \Delta R_{12}(x, y, z) \\ \Delta R_{13}(x, y, z) \\ F(x, y, z) \end{bmatrix}$$

SOLUTION

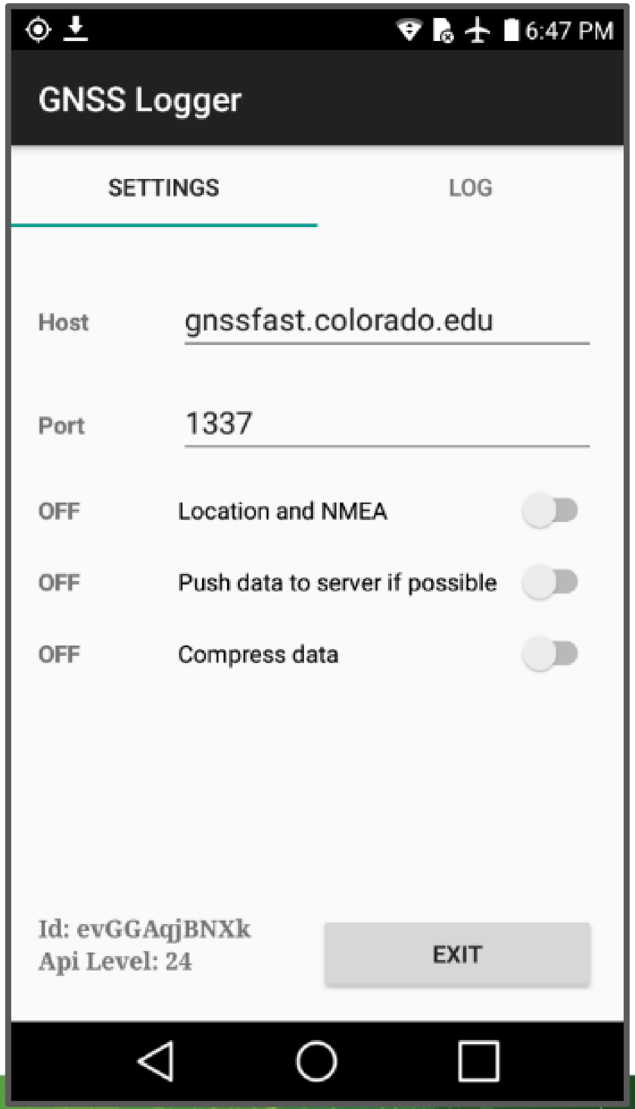
$$\begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

Multilateration Positioning Results vs. Reported Position



Crowdsourced Smartphone for Jamming & Spoofing Location

- Benefits of multiple, dispersed smartphone measurements for detection & localization
- Available metrics: position, C/No, pseudo range*, AGC*
- Other equipment to measure AGC due to smartphone limitations



Host gnssfast.colorado.edu

Port 1337

OFF Location and NMEA

OFF Push data to server if possible

OFF Compress data

Id: evGGAqjBNXk
Api Level: 24

* Available on some phones with Android 7.0 or later OS

Recognizing and Responding to the Threats to GNSS

- Johns Hopkins GPS Risk Assessment (1999)

- From Presidential Policy Directive 21 (PPD-21) (2013):

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

- From Executive Order 13800 (EO 13800):

"...known, but unmitigated vulnerabilities are among the highest cybersecurity risks."

Based on Executive Order 13905, Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services, "It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services. To this end, the Federal Government shall engage the public and private sectors and promote the responsible use of PNT services."

Source: Conner, K. "Resiliency in Design, Implementation and Operations for Critical Infrastructure," 57th CGSIC.