RFI Mitigation for Civil Navigation

TODD WALTER

(WITH HELP FROM MANY COLLEAGUES)

STANFORD UNIVERSITY

ITSNT

November 16, 2018

RFI Concerns

- Global Navigation Satellite System (GNSS) signals are weak
  - 10^{-16} W or -160 dBW
  - Can easily be overwhelmed by terrestrial signals
- Signal designs are open and unencrypted
  - Anyone can generate signals that are perceived as valid
- Many motivations to interfere with GNSS
  - Privacy, economic, criminal, military, …

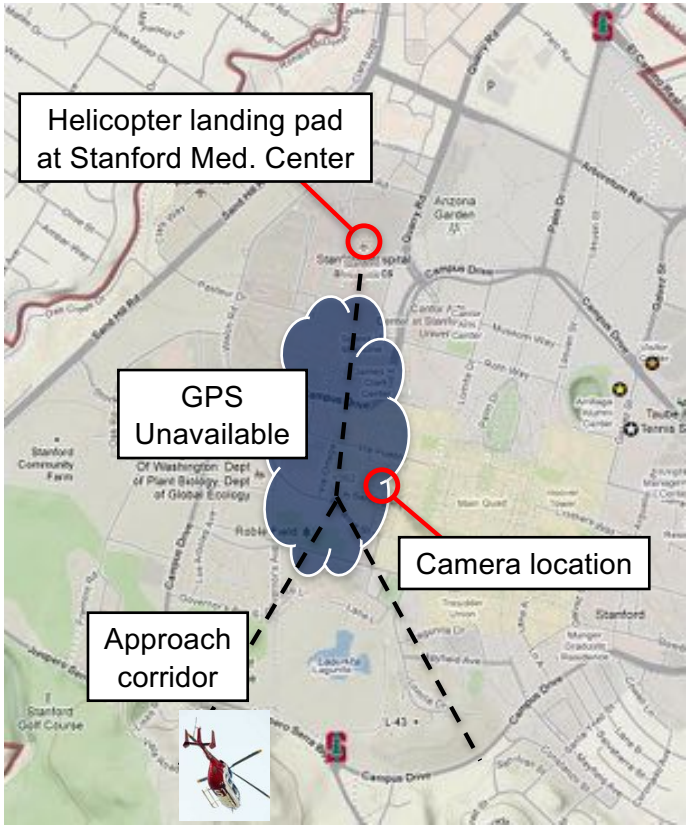
GNSS Interference

- Interference is defined by the ITU as: "The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy[1]""
  - **Jamming:** denial of GNSS through the addition of noise or other signals in the spectrum
  - **Spoofing:** emissions of GNSS-like signals that may be acquired and tracked in combination with or instead of the intended signals
  - **Unintentional:** inadvertent, collateral, spurious energy, …
  - **Intentional:** denial of service, hacking, privacy, theft, terror, …

[1] International Telecommunication Union (ITU) Radio Regulations (Vol 1, Art I, Sect VII)

1999: GPS "Jammer" on the Medevac Approach to Stanford Medical Center

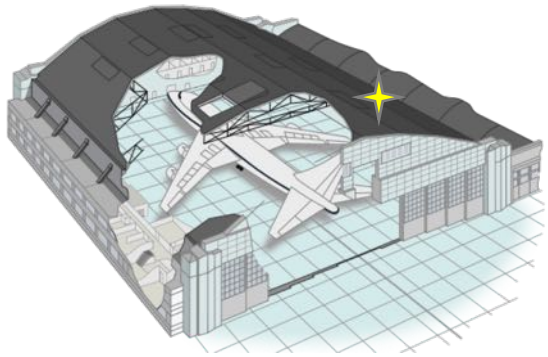
- Medevac rescue pilots report loss of GPS navigation on final approach; GPS Lab notice receiver degradation
- GPS Laboratory personnel localize
- Networked camera to document a campus construction project radiated in the GPS/L1-band



November 2009: Jamming at Liberty Airport in Newark, N.J. Personal Privacy Devices (PPD) Affect Aircraft Operations

Unintentional Spoofing from a Re-radiator

- GPS re-radiators may be used, with authorization, in the United States and many other countries
- Inappropriately modified systems have resulted in unintentional spoofing or disruption of aviation GNSS receivers in several instances to date



Typical Installation

Commercial GPS Re-radiator System

Examples of aviation impacts:

- March 2007 - Loss of STARS & DVRS at Des Moines IAP
- May 2010 - Spoofing incident in Germany caused erroneous Ground Proximity Warning System alert
- July 2010 - Loss of WAAS vertical guidance during approaches into Sanford, FL airport

Financial Incentives to Spoof GNSS Already Exist

RF Interference Effect on Aircraft

- Existing aviation receivers require that the system:
  - is able to acquire and accurately track true signals when the actual interference is not worse than a specified environment
  - will not output misleading information for interference that exceeds the specified environment.
    - A note labels this as only applying to unintentional interference
    - RF Interference environment is described in Appendix C of the requirements

- Work is underway to strengthen the interference requirements for the next set of aviation standards
  - PPDs and repeaters have been observed to affect aircraft and ground systems

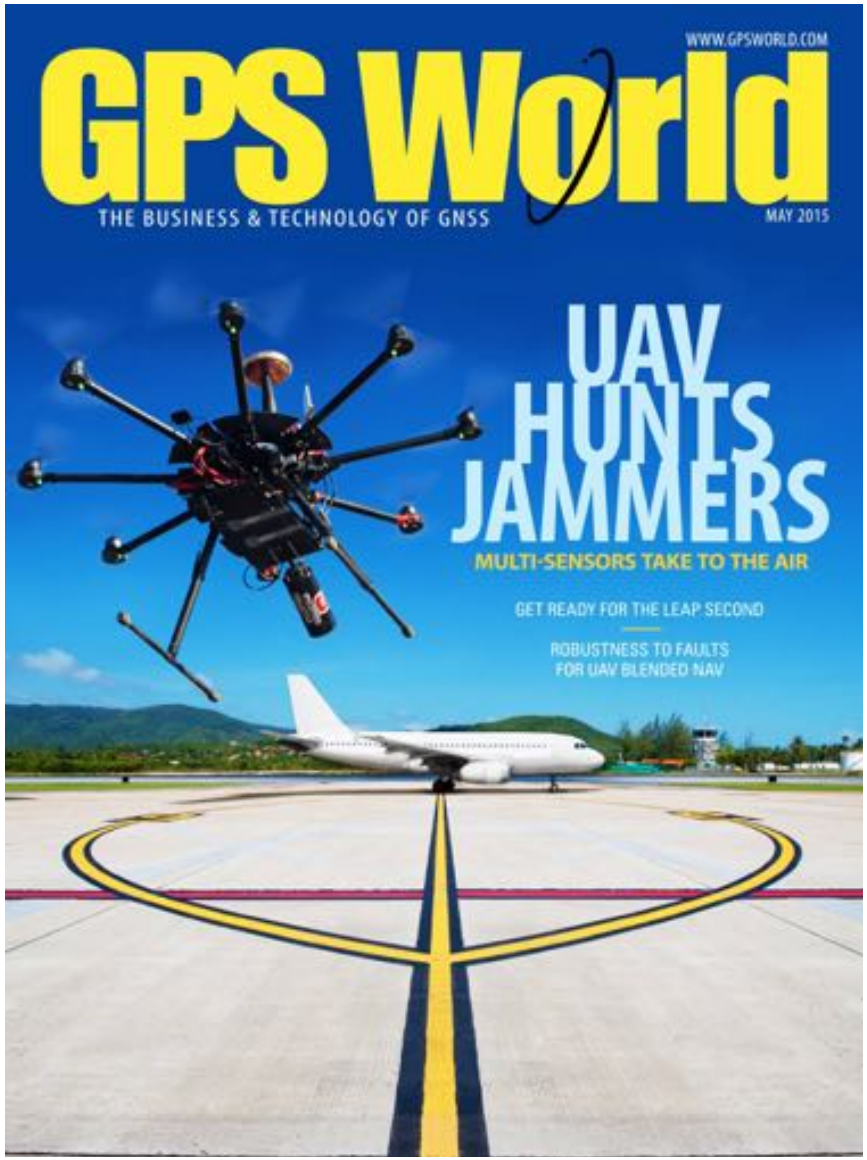
Collateral, Targeted, & Sophisticated

- These words are typically understood as how the spoofer operates rather than what can be distinguished by the receiver
  - The words are useful for receiver requirements, but they need to be clarified
- **Collateral** – the position, code chip phase, power levels etc. are unlikely to be aligned with truth at the user antenna. Therefore large positioning and pseudorange jumps can be expected as well as power levels that are often too weak or too strong
- **Targeted** – some effort (TBD) has been made to align these items so that errors may not be obvious at the receiver
- **Sophisticated** – The spoofing signals are at their hardest to detect conditions, multiple signals may be arriving from different directions, including overhead

How do we deal with interference?

- Protect
  - Detect and localize interferences sources
  - Create legal and financial disincentives to disruption
  - “Jammers are illegal to market, sell, or use in the United States.” GPS.GOV
- Toughen
  - Transmitted signal (more power, multiple frequencies)
  - Antenna technology
  - Improve GNSS receiver
- Augment
  - Coasting with relative navigation (precise clocks, inertials)
  - Independent navigation systems (terrestrial navigation aids)

Detection of Interference With a Directional Antenna

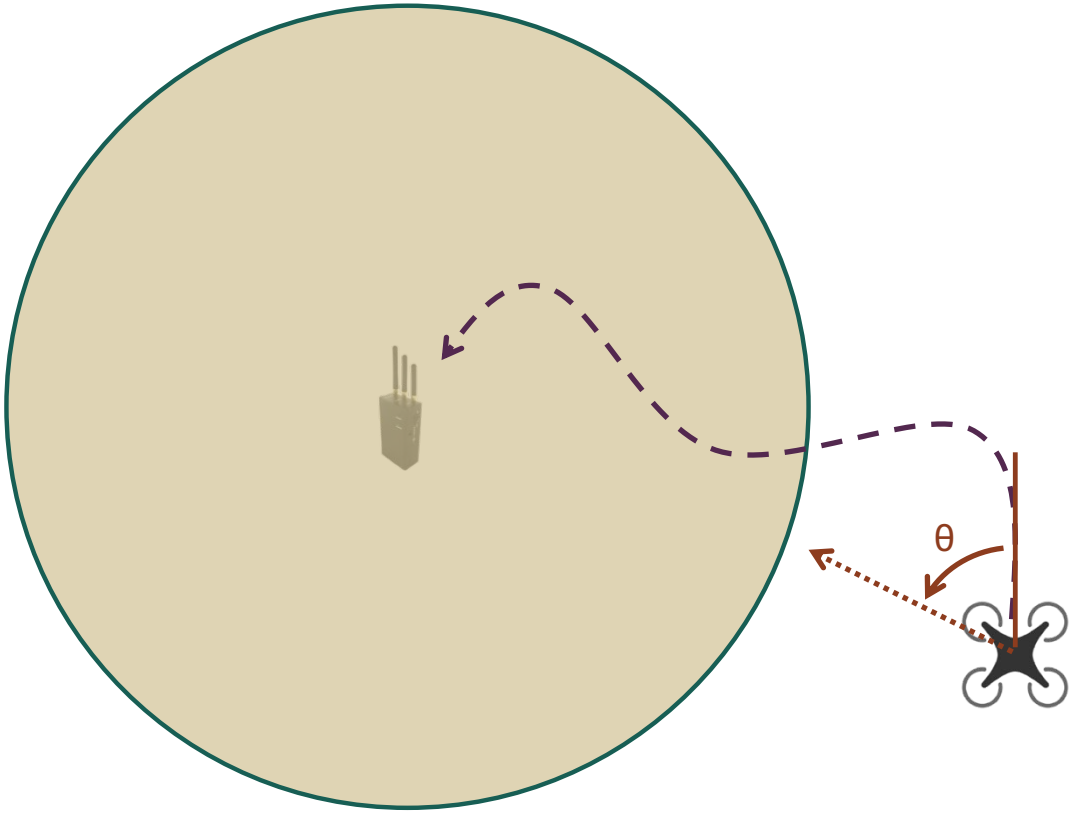


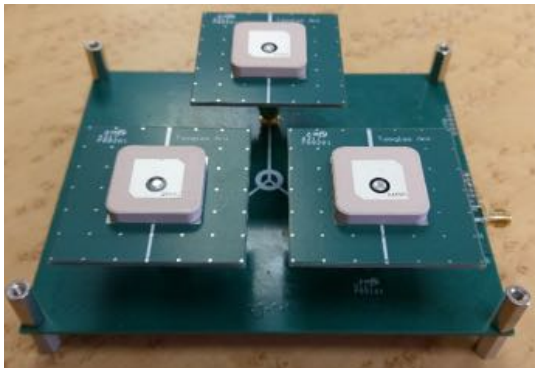
Improving Detection with UAV

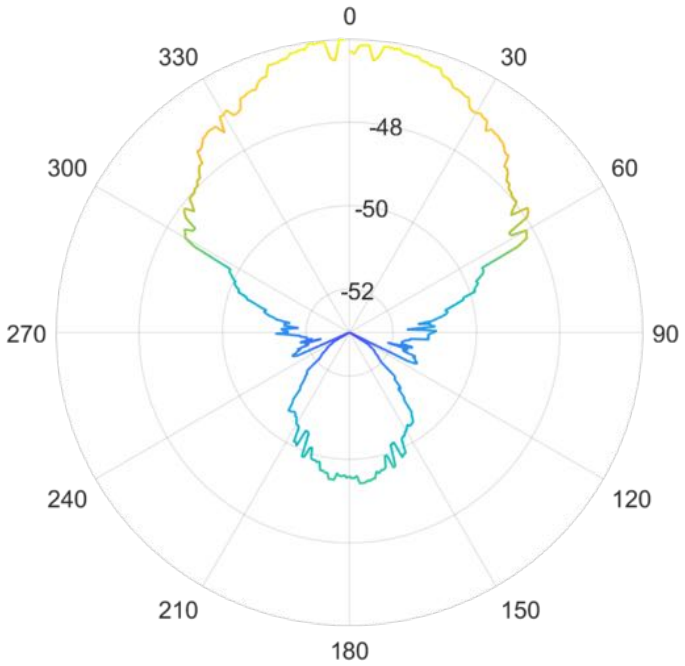
- UAV can be rapidly deployed and are maneuverable (quick direction finding)
- Jammer Acquisition with GPS Exploration and Reconnaissance (JAGER) testbed for interference localization algorithm
- Interference detection (direction finding)
- Robust navigation
- Rapid interference localization strategies

JAGER

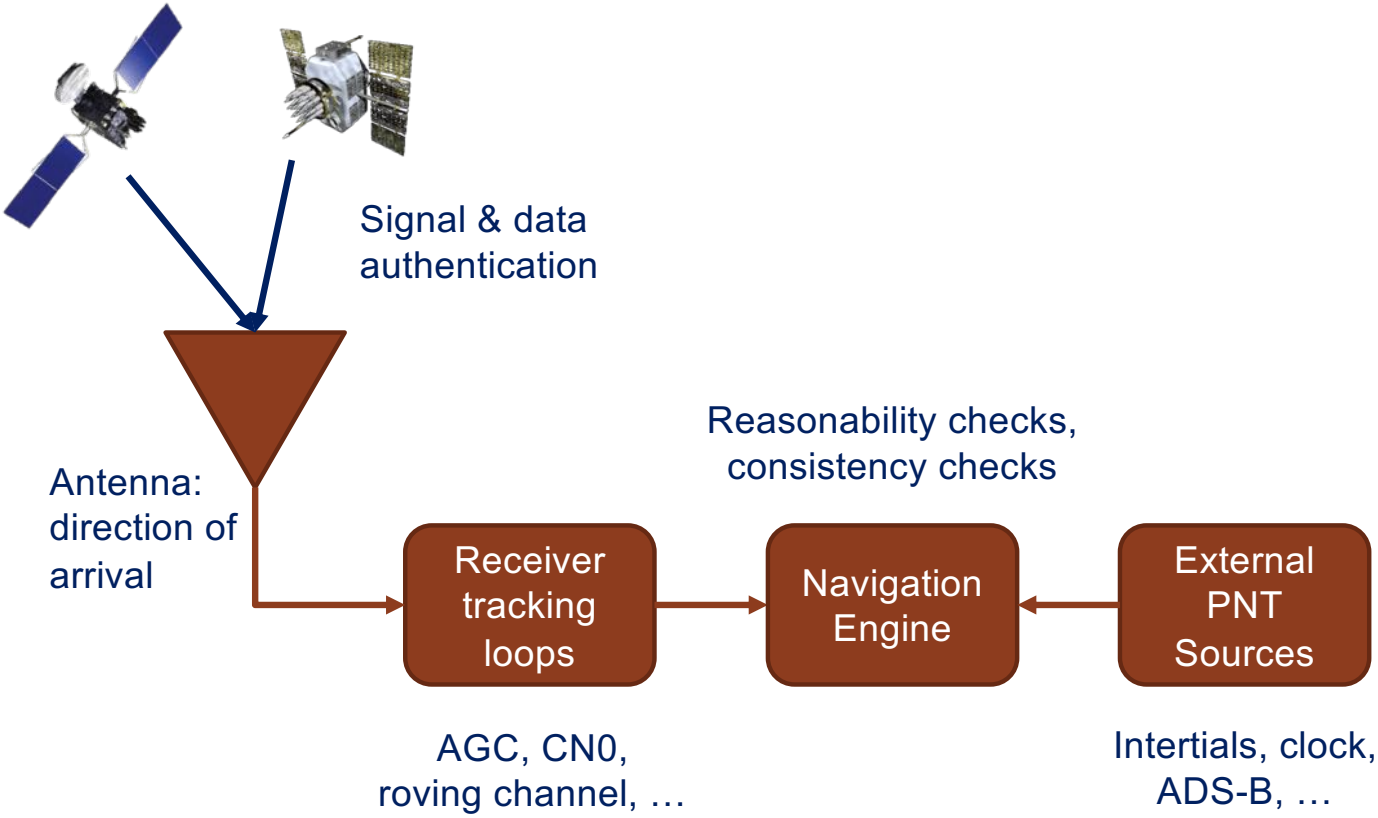
Bearing to the jammer is the observation of interest







RFI Detection and Mitigation



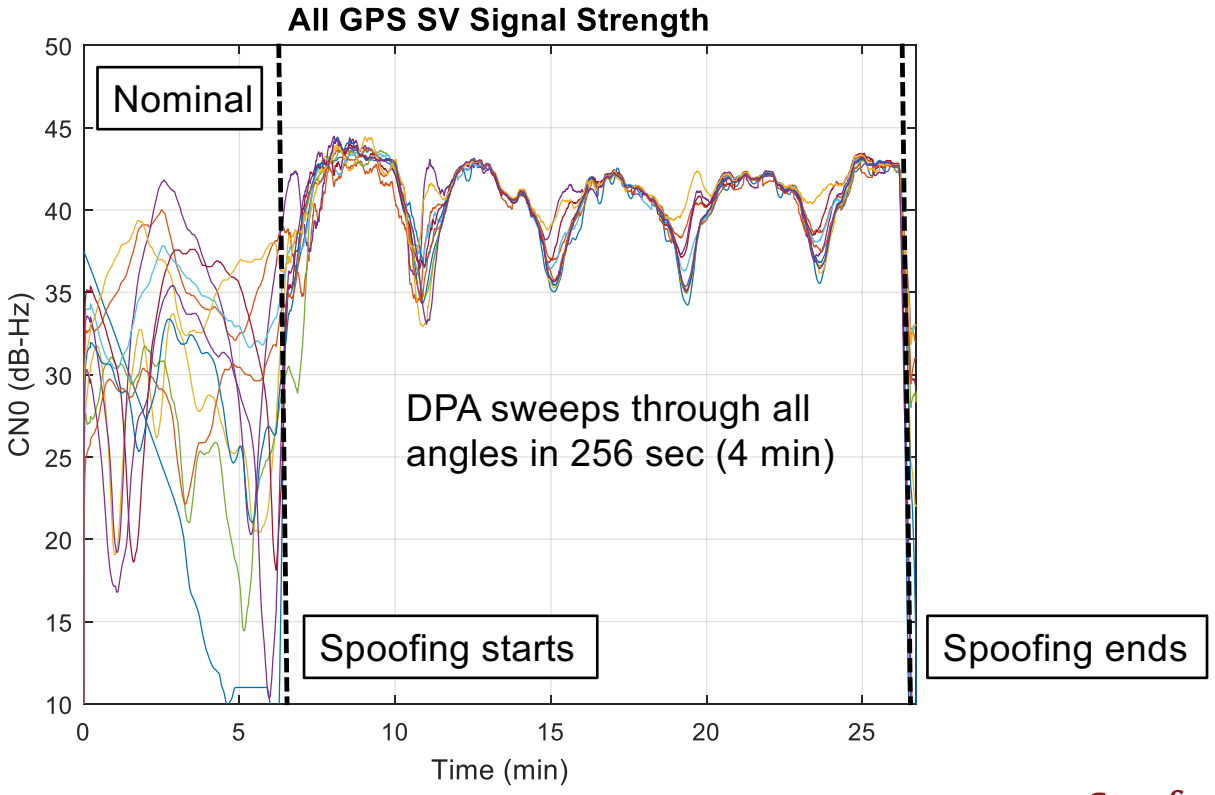
Dual Polarization Antenna (DPA)

- DPA is a patch antenna that can receive and distinguish right and left hand circularly polarized signals; it uses this to determine direction of arrival
- Allow for determining direction of arrival 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 (COTS) components
  - only needs one cable (useful for aviation and other applications)

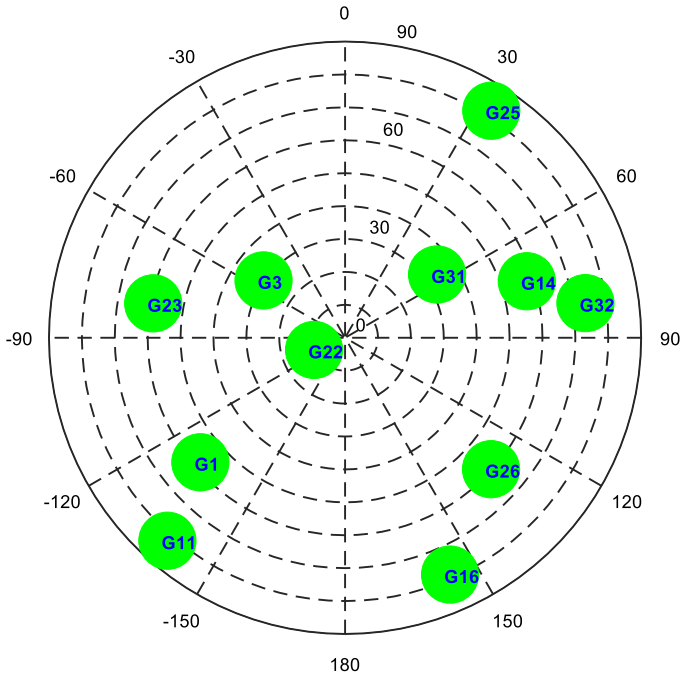
3 inches

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

GPS C/No During Live Spoofing Test

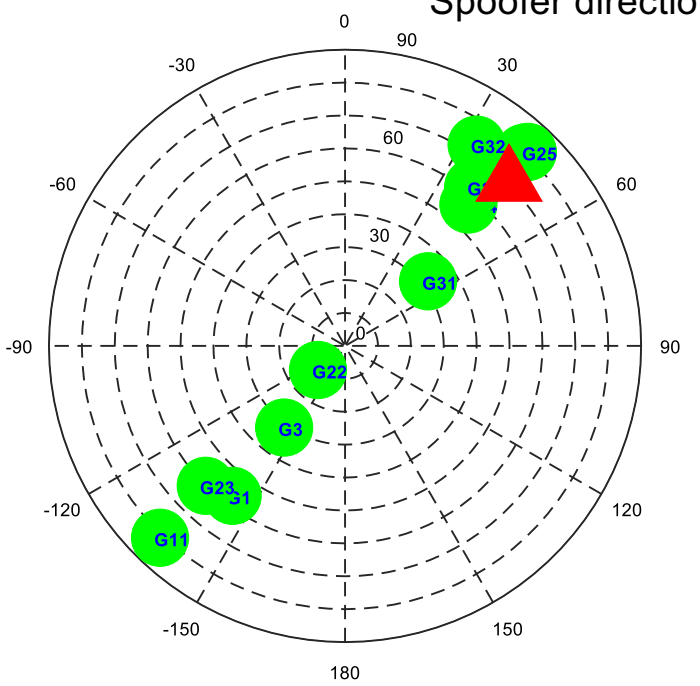


Direction of Arrival Estimates



Skyplot from true ephemeris

Spoofer direction



Skyplot with azimuth from DOA
& elevation from ephemeris

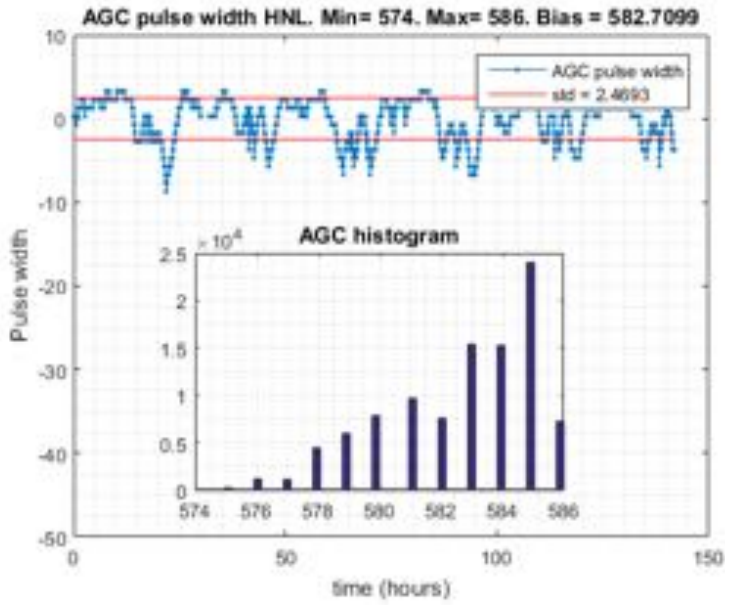
Automatic Gain Control (AGC)

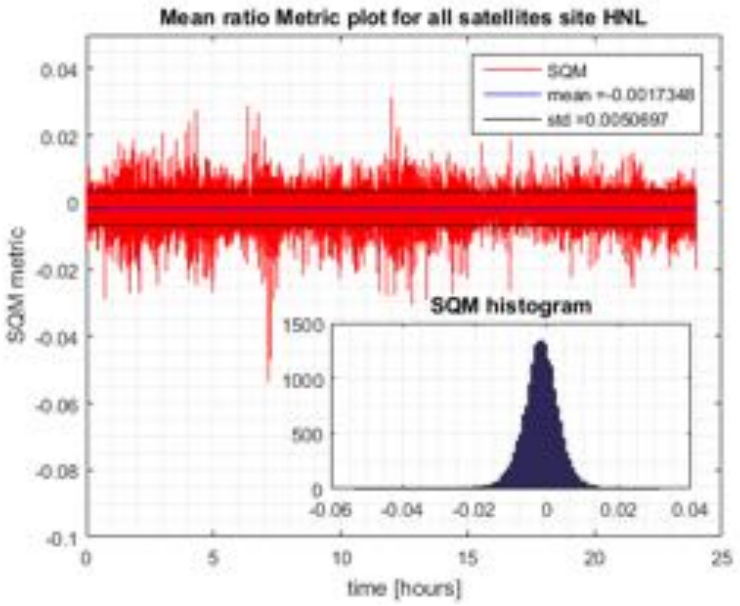
- The AGC adjusts the amplification of the analog input signal prior to conversion to digital
- It is designed minimize quantization loss by ensuring that the full range of the digital sampling is properly utilized
- The sampled distribution is usually driven by thermal noise and follows a Gaussian distribution
  - The GNSS signals are below the noise floor
- Interference will disturb this expected distribution, often putting energy beyond the dynamic range of the sampling
  - In response the AGC lowers the gain until the observed signals fit within expectation

WAAS station HNL

WAAS station HNL

- Around 150 hours of data of AGC measurements and 24 hours of SQM measurements



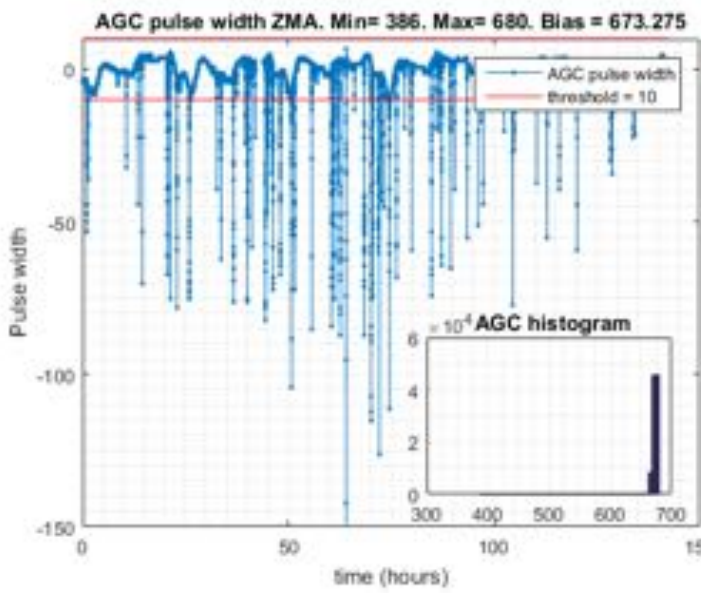


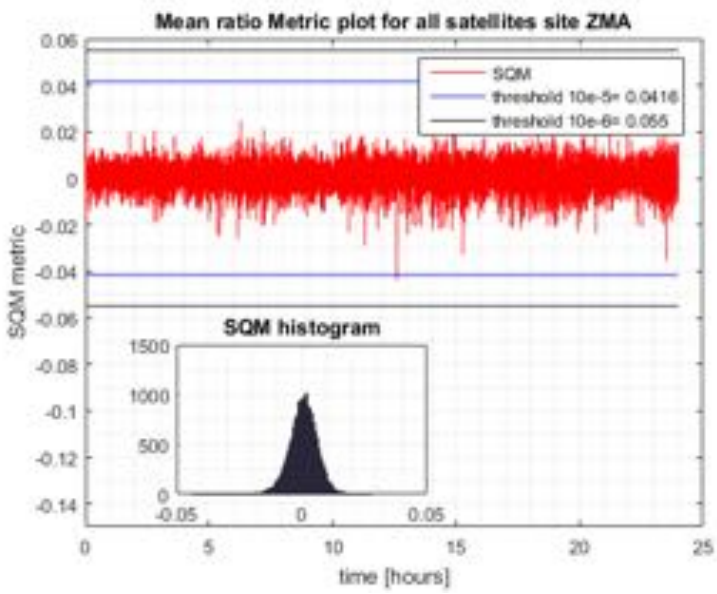
WAAS station ZMA

- Location in Deep Urban/ heavy traffic area

WAAS station ZMA (w/ RFI)

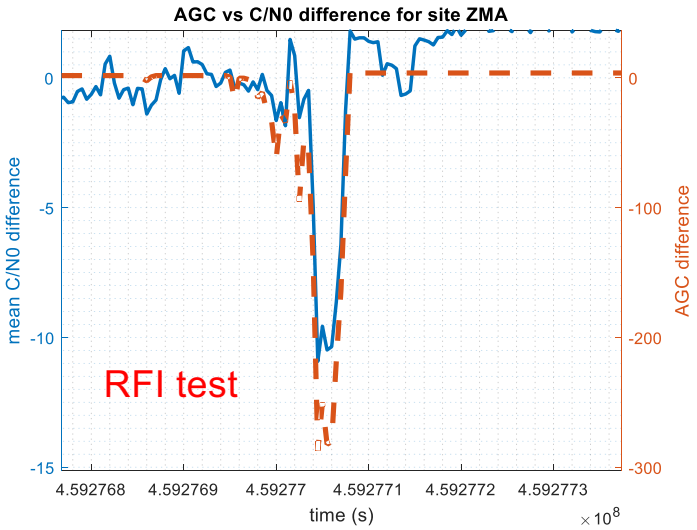
- Similar behavior to overpowered attacks, only reflected on AGC and not on the SQM, could lead to false alarms

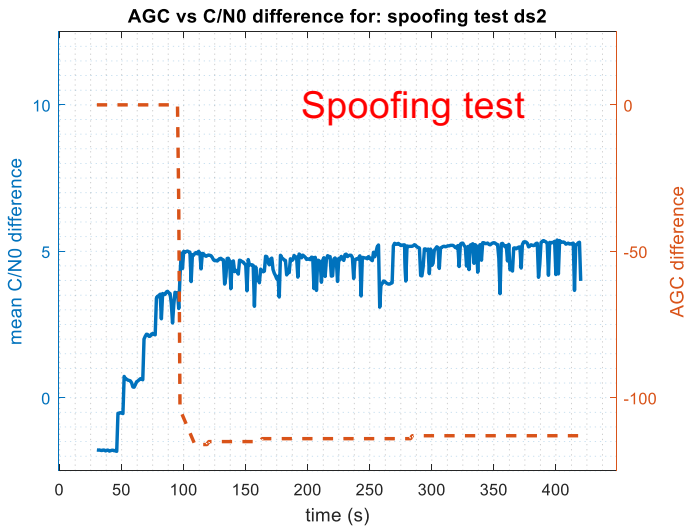




What if We Look at the AGC and C/N0 Together?

- Direct link between AGC behavior and C/N0 when affected by RFI. This is not true during spoofing attacks

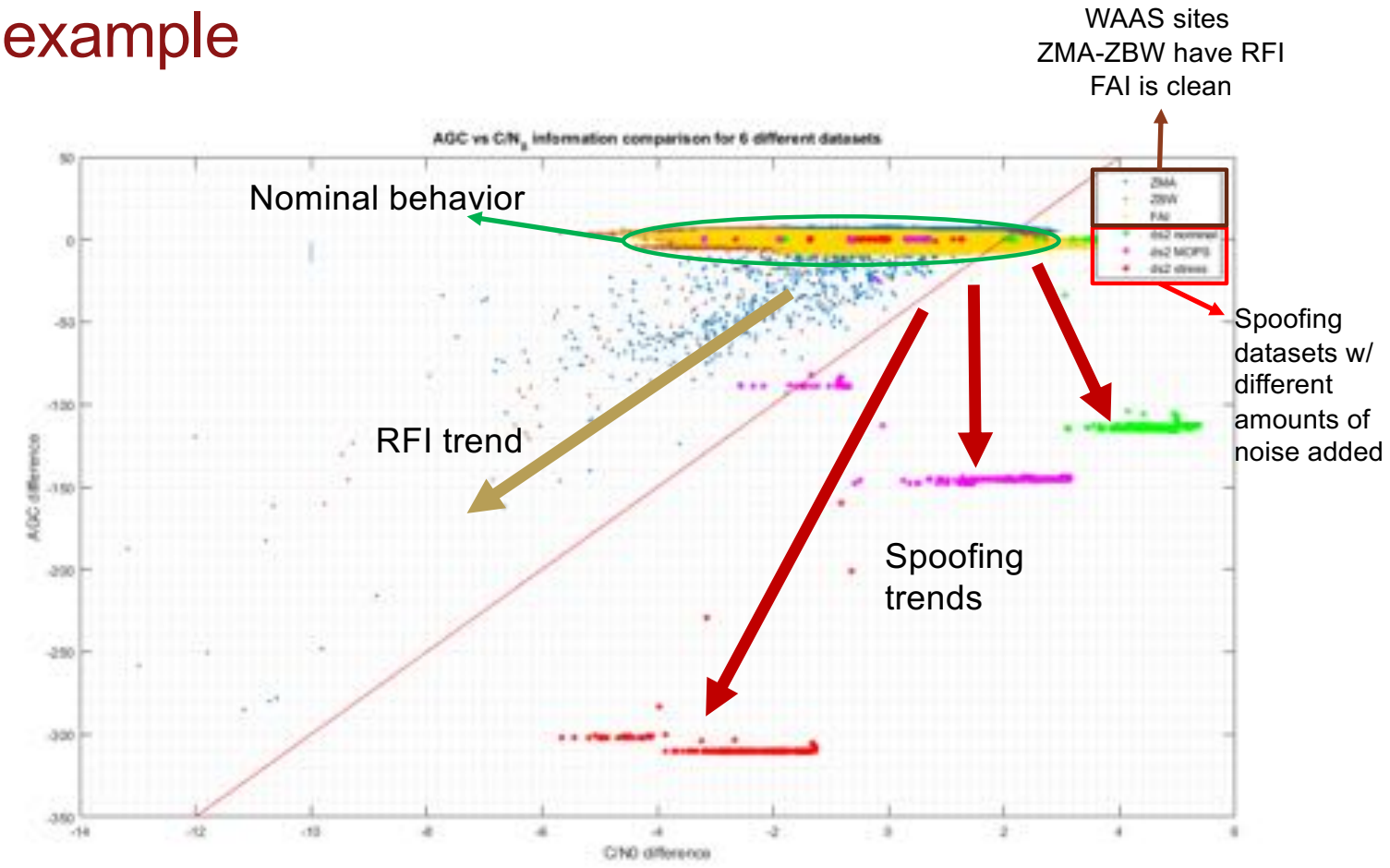




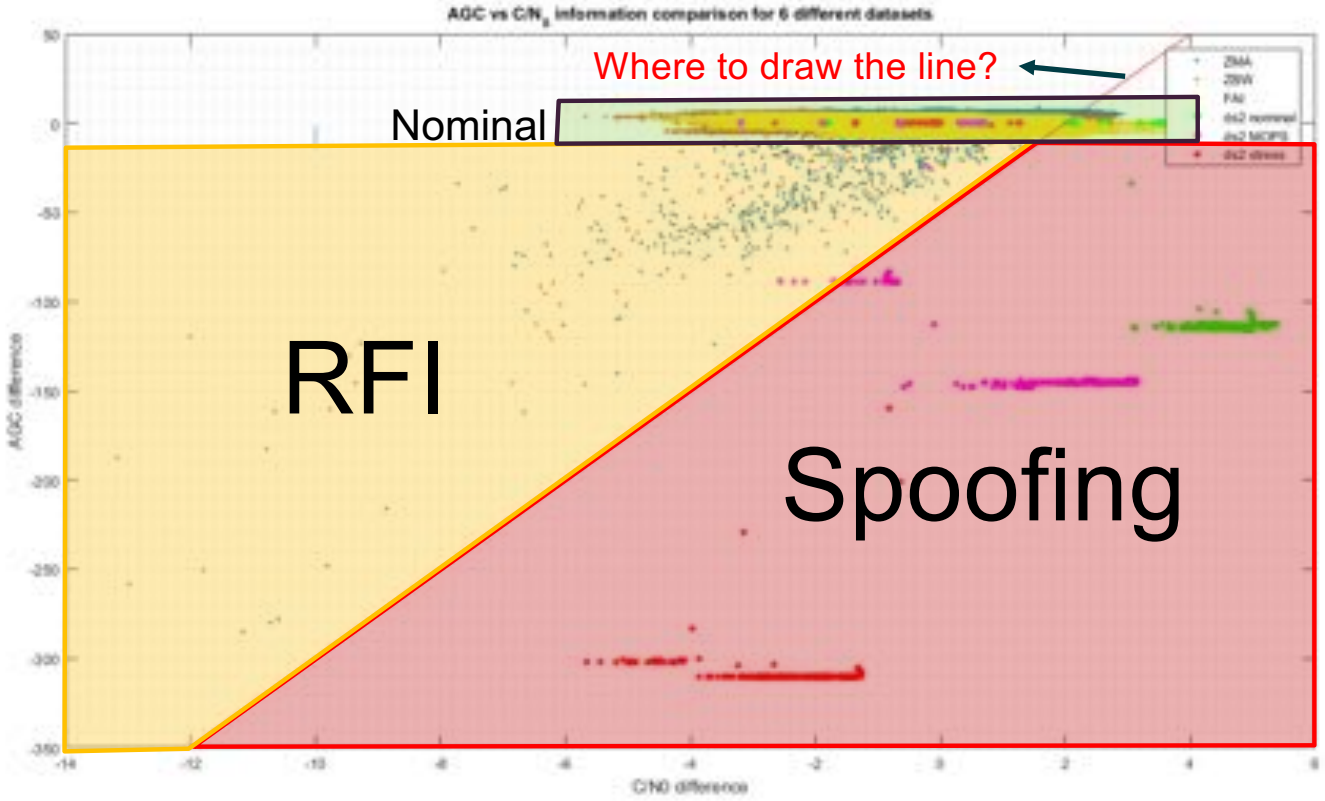
GPS Receiver Measurements

- What happens?
  - During RFI, noise is added to the GPS band, so the AGC lowers its gain value. This means that N0 will be larger and the C/N0 will decrease
  - During a spoofing attack, a signal that is specifically aligned with the carrier signal of the GNSS. This means that C will be larger and C/N0 will increase
- What if the spoofer adds extra noise?
  - A smart spoofer may be able to maintain the C/N0, or even decrease it by adding additional noise
  - But, the AGC will respond to larger amounts of power being inserted, and the C/N0 will not decrease with the expected trend

An example


WAAS sites
ZMA-ZBW have RFI
FAI is clean
AGC vs C/N0 information comparison for 6 different datasets
Nominal behavior
RFI trend
Spoofing
trends
Spoofing
datasets w/
different
amounts of
noise added
AGC difference
C/N0 difference

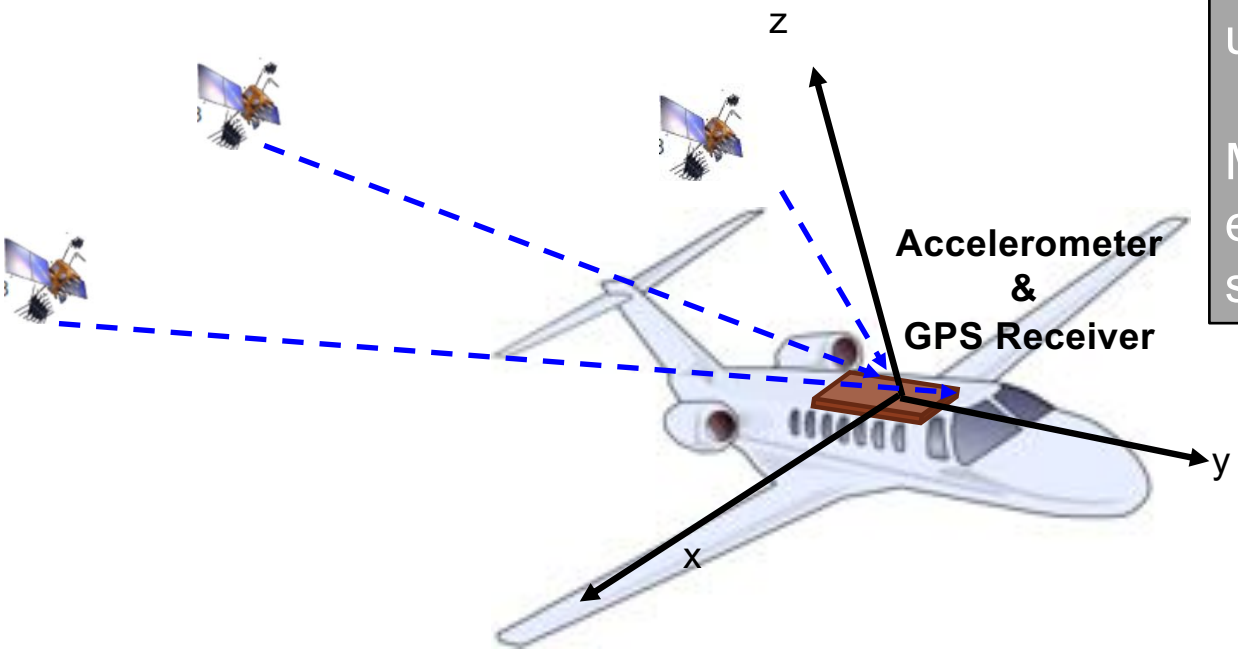
We can define three zones



Reasonability Checks

- Are the positions reasonable?
  - Not well outside expected operating region
- Are the velocities reasonable?
  - Not below stall speed of the aircraft or above maximum for vehicle
- Are the position and velocity estimates consistent?
  - Sudden jumps may indicate spoofing
- Are the tracking loops and data well behaved
  - Excessive cycle slips, poor data demodulation or inconsistent navigation data could indicate spoofing
- Not necessarily definitive on their own, but can be combined with other measures indicating spoofing

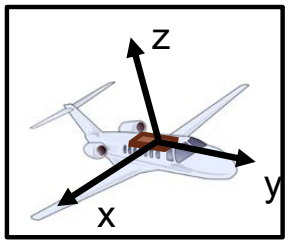
Anti-Spoofing via User Motion: Low-cost Accelerometer Integration



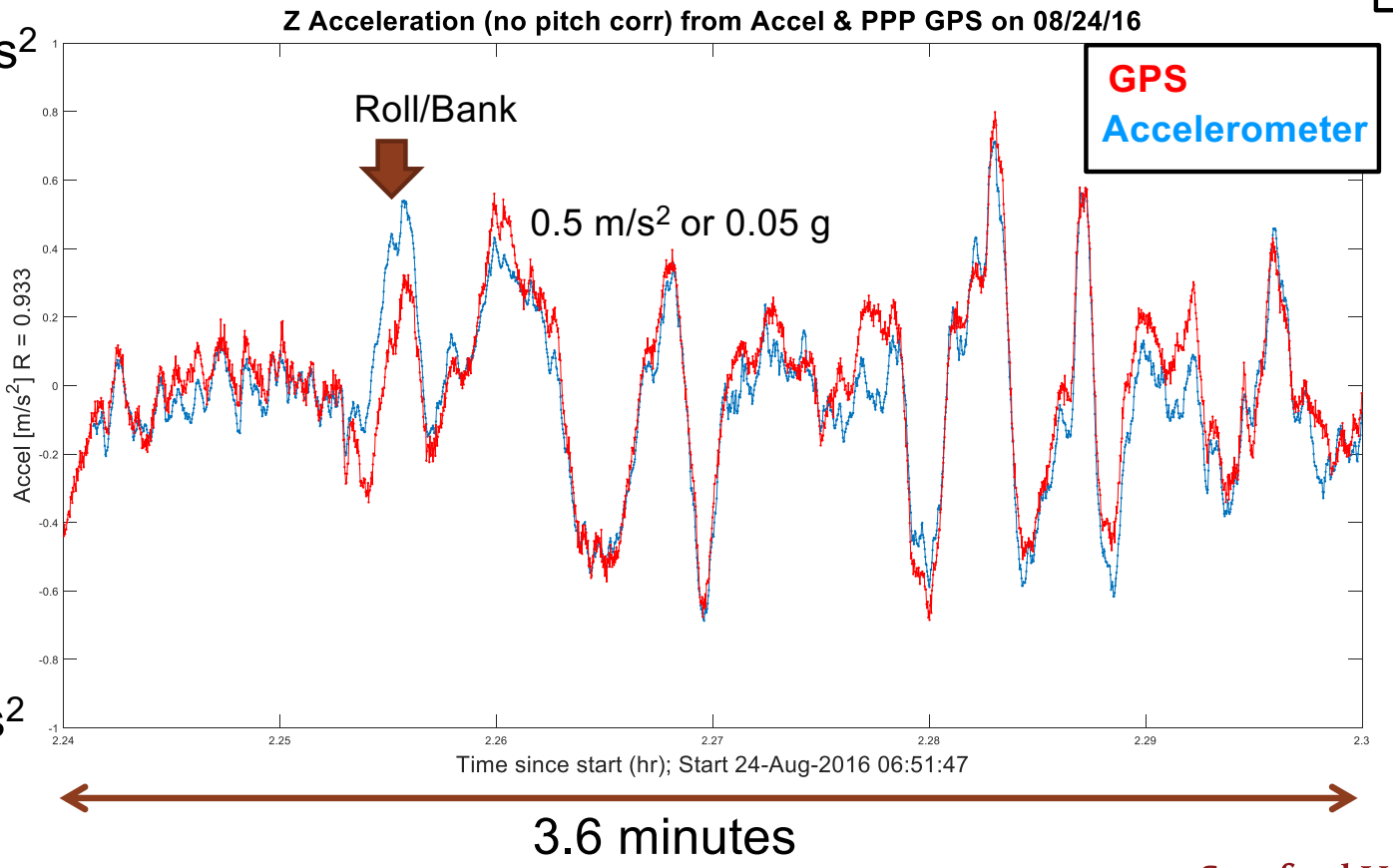
Accelerometers can provide an independent measure of user motion.

Motions that deviate from expected can indicate GPS spoofing.

Z axis (Vertical) Acceleration Comparison



+1 m/s^2



-1 m/s^2

Summary

- GNSS signals are weak and easily overwhelmed
- Jamming and spoofing are becoming cheaper, easier, and more common
- It is increasingly important to protect, toughen, and augment GNSS receivers against the effects of RFI
- Many promising mitigations exist
  - Their cost and operational impact must be balanced against the likelihood and severity of the perceived threats
  - Best choices are still being decided for different applications