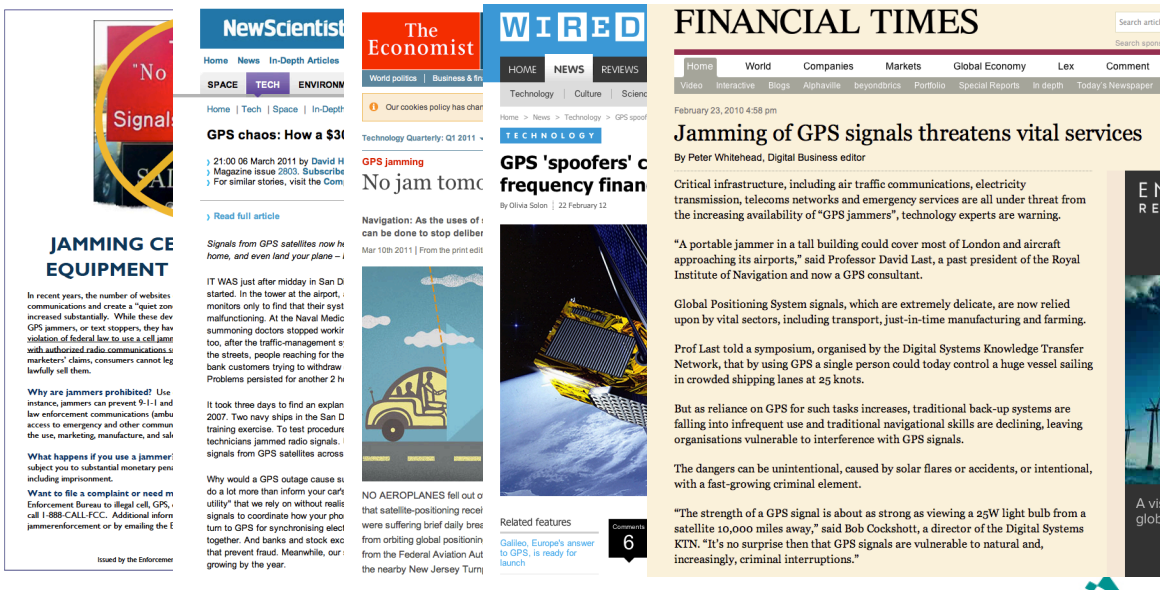
Interference of Anti-Jam Techniques with accurate time determination

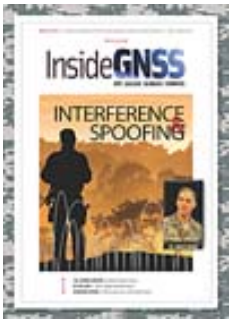
Gordon Jolly
Chief Engineer, Anti-Jam Technologies
NovAtel Inc.
Gordon.Jolly@novatel.com

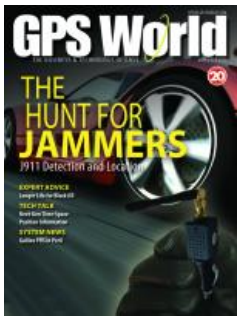
GPS Jammer Headlines

- Mainstream and Industry press make routine pronouncements on the vulnerability of GPS (and other GNSS services) – the "Invisible Utility"



Within the GPS community there is a LOT of concern!





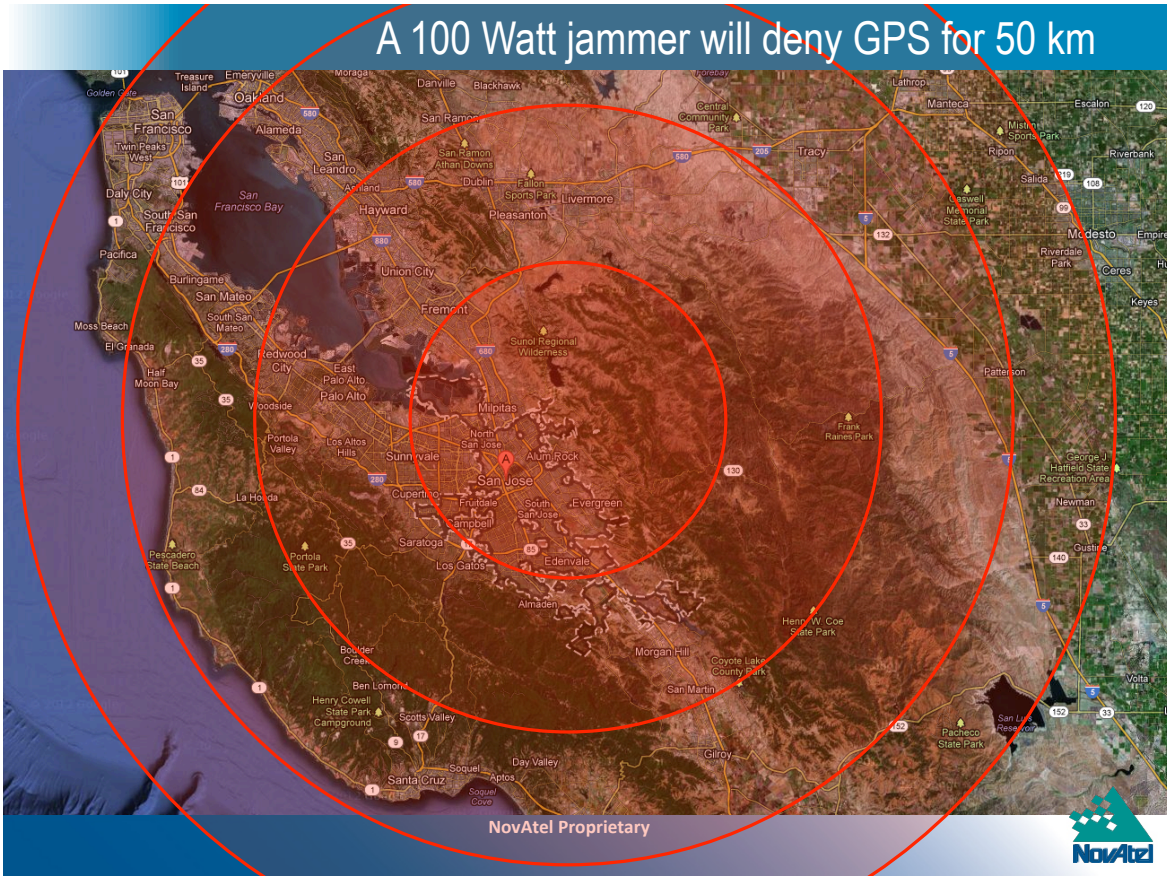
What is the problem

- Power – easy to overwhelm
  - GPS signal at sea level is just 178aW or -127dBm or 178×10^{-18}W
    - from a 25W transmitter on the satellite at an altitude of 21,000km!
- Signal – civilian signals are easy to fake
  - Military signals are encrypted and access is very tightly controlled
  - Civil signals are in the public domain
- Integrity – difficult to validate
  - Military and Augmentation service (e.g. WAAS) include integrity monitoring
  - Civil are unauthenticated – use at your own risk!
- Protection
  - GPS frequency bands are protected by the ITU globally
    - including FCC in the US
  - Detection and enforcement cannot yet be said to be effective

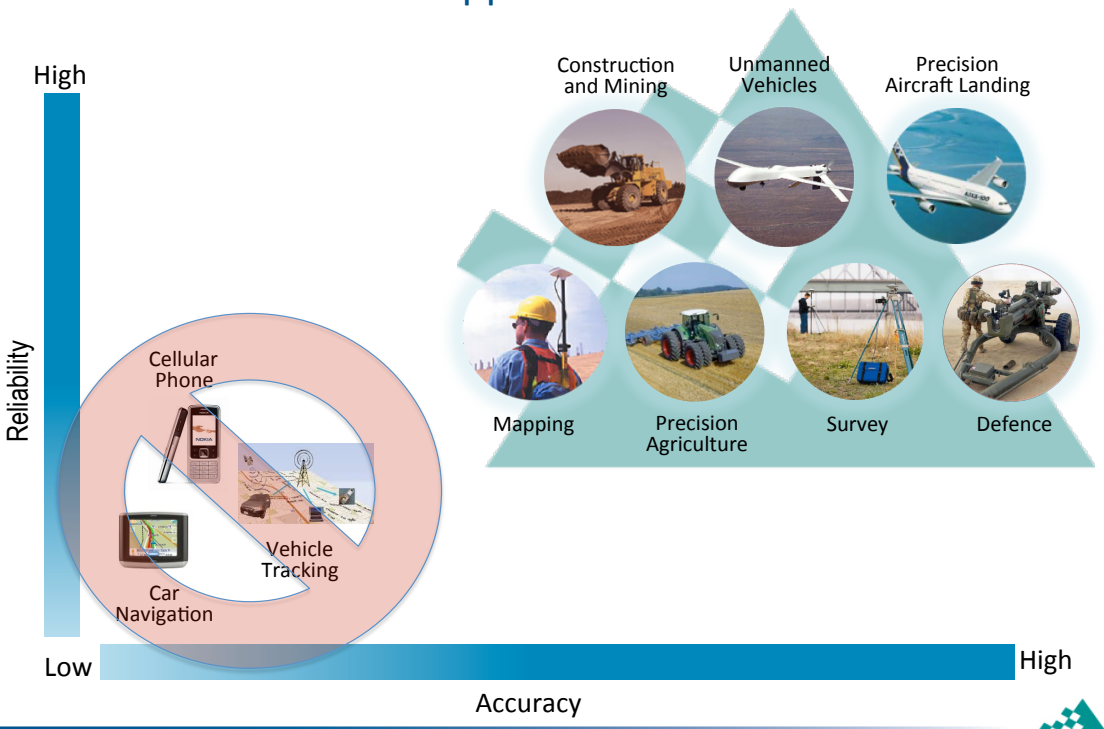
Civil Vulnerabilities

- Jamming sources
  - Accidental emissions
    - Faulty electronics can transmit unwanted signals that disrupt GPS
  - Individuals using 'Personal Privacy Devices' to avoid unwanted location tracking of their movements
    - "eBay jammers" available for $30-$300
    - Claimed ranges of <10m often underestimate impacts
  - In 2012 study by Communications Research Centre Canada focused on downtown Ottawa, prevalence of jammers in vehicles was ~1:70,000
    - 92 jamming incidents logged over 5 weeks (Approx. 3 per day)

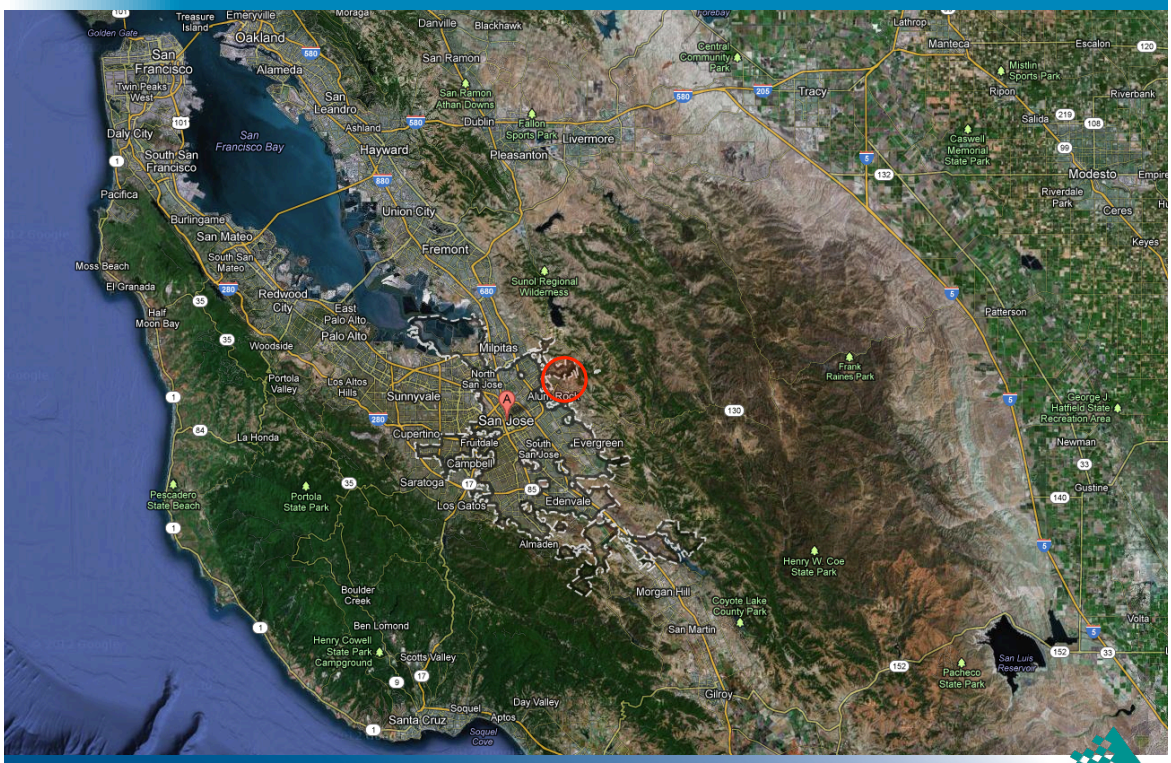
- Timing vulnerabilities
  - Communications
    - LTE and other standards require better than 1µs accuracy
  - Power distribution
    - IEEE C37.118-2005 Synchrophasor Standard specifies better than 1µs accuracy
  - Time stamping
    - NASD requires time stamping accuracy of better than 3 seconds
    - Time stamping for forensic and algorithm evolution better than 1µs



Precision and Critical Applications



40 dB additional protection - navigation to within 400 m of jammer



Effects of jamming and spoofing

- Jamming – noise jamming
  - Obscures legitimate signals ('Loss of Lock')
  - Leads to inadequate data to resolve position and time
    - ≥4 satellites needed for full position & time solution
    - ≥1 satellite needed for fixed and known position to resolve time
  - Limited satellite introduces large geometric errors
  - **Jamming results in *known* loss of operational capability**

- Spoofing – broadcasting a false signal
  - Meaconing – capture and re-broadcast
    - Position & time solution based on Capture Antenna, whose signal is amplified and re-broadcast
    - Target Antenna 'appears' to be at location of Capture Antenna
  - Spoofing – synthesizing signal for broadcast
    - Spoofer can define any position in space and time and apply to Target Antenna
  - **Spoofer capture results in *unknown* loss of operational capability**

Protection options

- Encryption (e.g. SAASM)
- Redundancy (Multiple Rx & other sources)
- Receiver robustness
  - Integrity monitoring
  - Signal strength monitoring
  - Geofencing/dynamic thresholding
- Direct Mitigation
  - Antenna beamshape options
    - Low sensitivity close to horizon
  - Filters
    - Notch filters, adaptive filters and sharp roll-offs
  - **Controlled Radiation Pattern Antenna (CRPA)**
    - **To maintain long-term GPS availability**
    - **Actively suppress unwanted signals (c.f. noise cancelling headphones)**

CRPA-101

- 4-7 elements
- Analog filtering on each channel
- Digital processing to form nulls through destructive interference
- Conversion back to analog signal
- Output to receiver

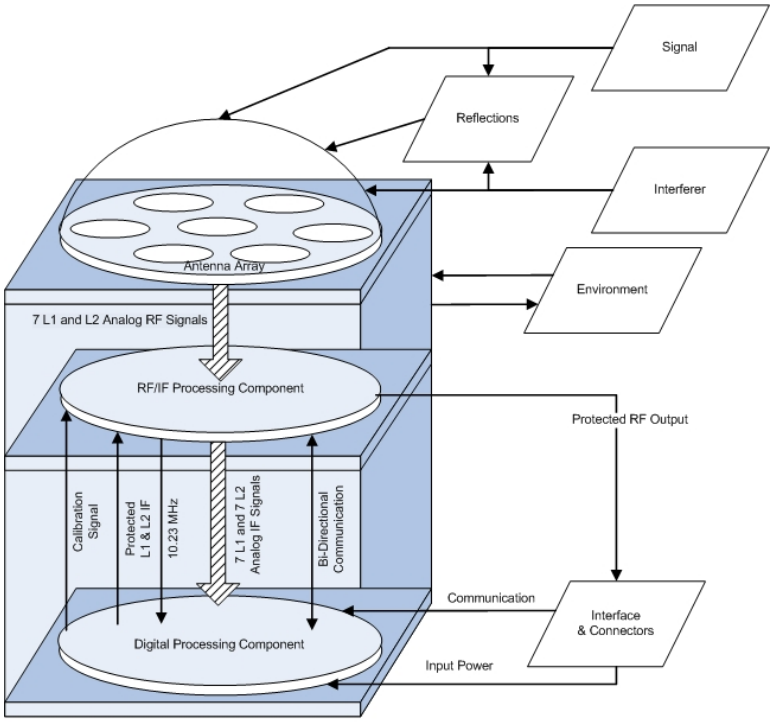


Figure: CAJS Schematic

GAJT: GPS Anti-Jam Technology

GAJT-700ML

- Integrated 7-element CRPA & electronics
- Single-enclosure for direct fit to platforms
- Vehicles and fixed installations
- Available now, off the shelf

GAJT-700ML

GAJT-AE

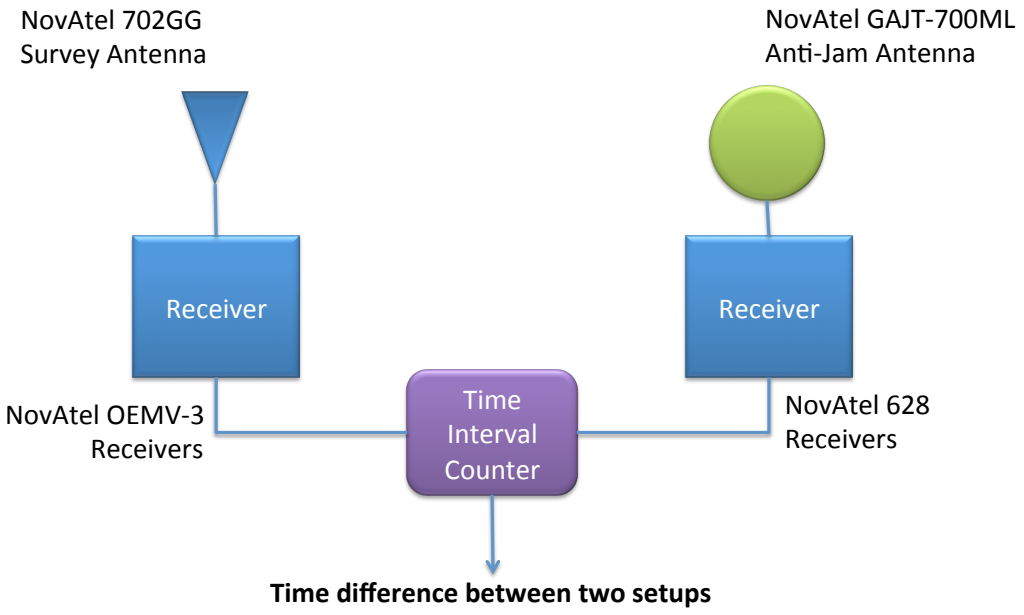
- Compact processing for 4-element CRPA
- Configured
- For integrating into systems:
  UAS, small ground platforms (e.g. UGV)
- Prototype demos achieved TRL-7
- Product release mid-2013

GAJT-AE

Questions and concerns raised about CRPAs

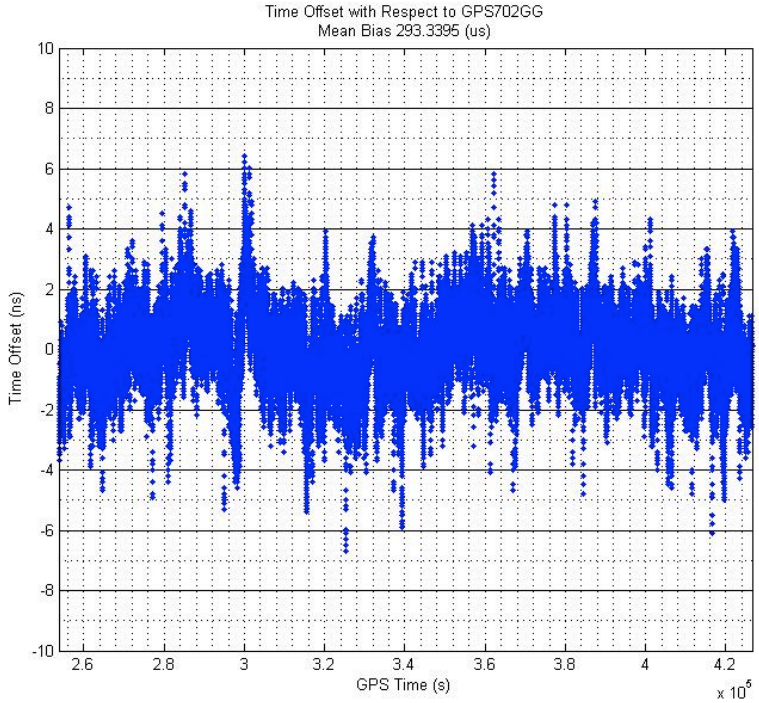
- What is the latency introduced by the CRPA processing?
- Is the latency stable over time?
- What effect does CRPA processing have on the position and time solution

Latency & Stability – Test Set-up



Latency & Stability – results

- Data logged over 48 hours
- Mean offset
  293.3395µs
- Standard deviation
  ±1.2ns



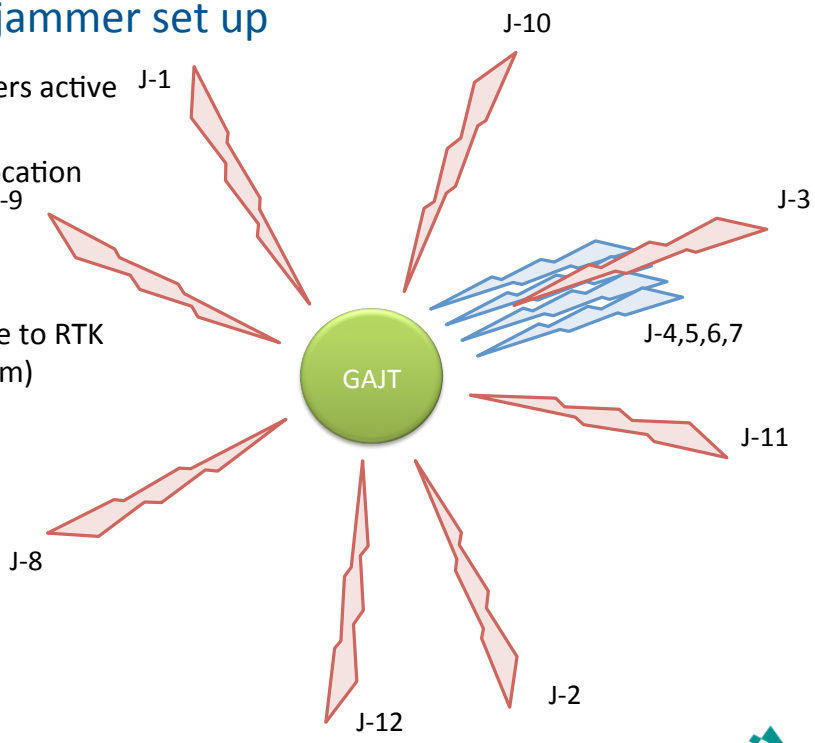
Susceptibility to processing influence

- iNAVFEST 2012, hosted by US Air Force at White Sands Missile Range
- Very high power jammers to exercise military anti-jam systems
- GAJT-AE with 4-element Antcom Antenna Array used for test
- Scenario switched through 12 separate jammers one at a time
- RTK solution obtained from NovAtel base station outside of test range
  - cm-level solution will show any systematic position offsets linked to jammer mitigation
  - No direct timing reference

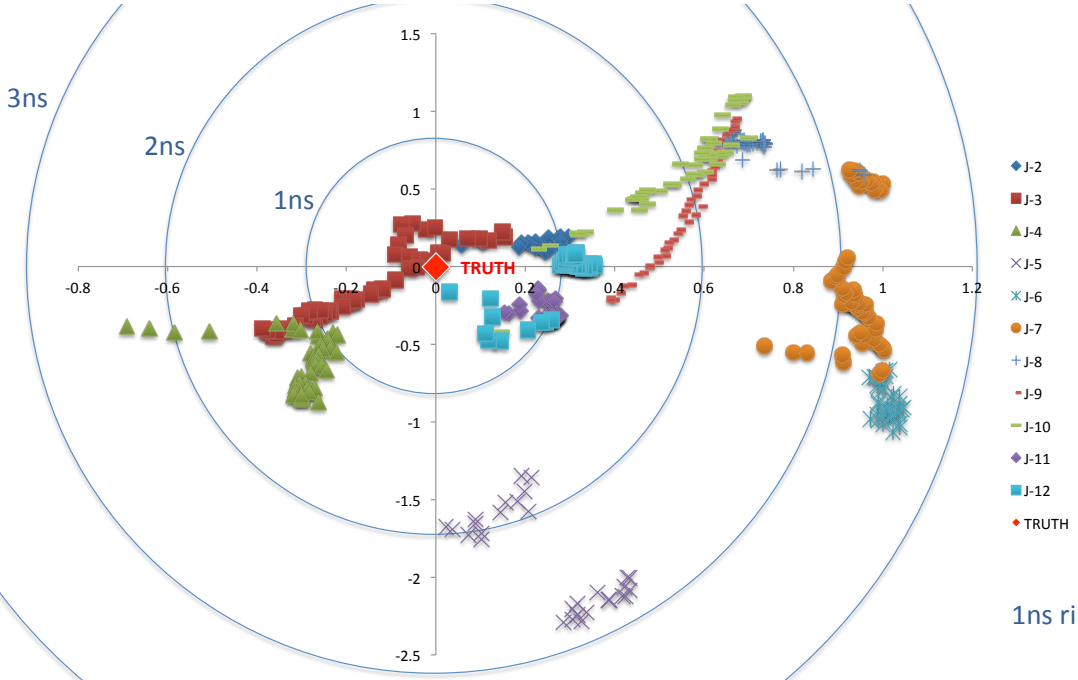
- Hypothesis:
  - *A stable PVT solution (position velocity & time) that shows no statistically significant change in position that correlates with noise jammer status will confirm that CRPA processing does not have a systemic impact on time determination*

Susceptibility jammer set up

- Each of 12 jammers active in turn
- GAJT is in fixed location throughout
- Phase centre of GAJT-AE antenna measured relative to RTK base station (20km)

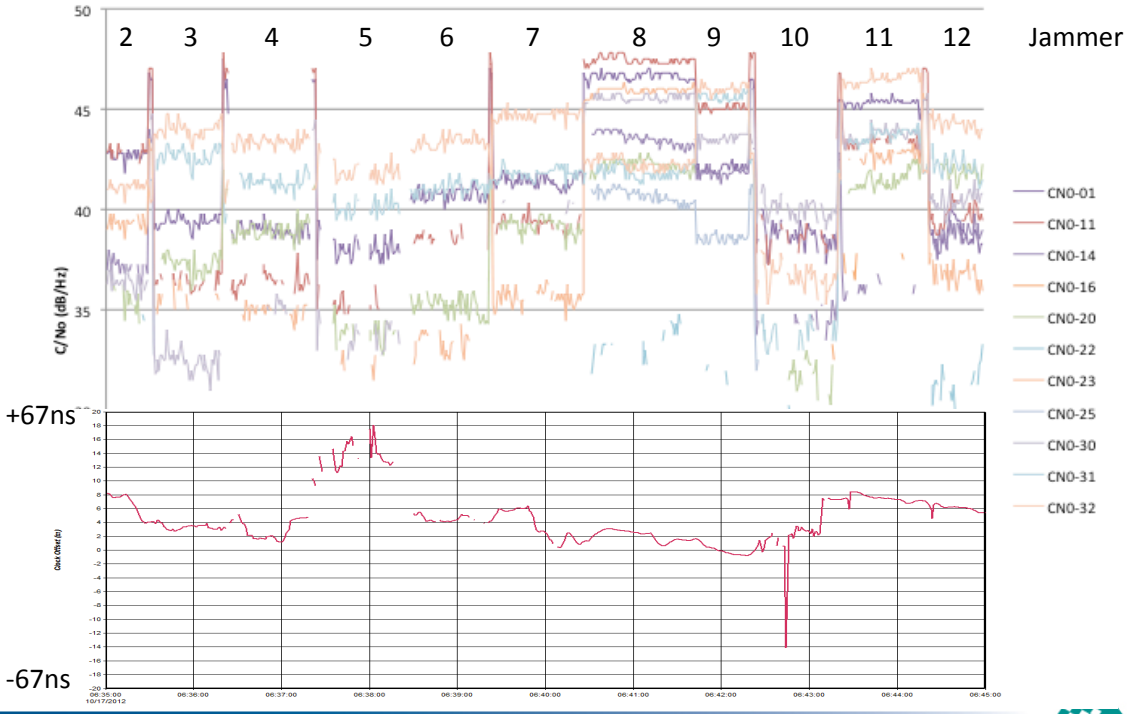


Susceptibility – spatial impact

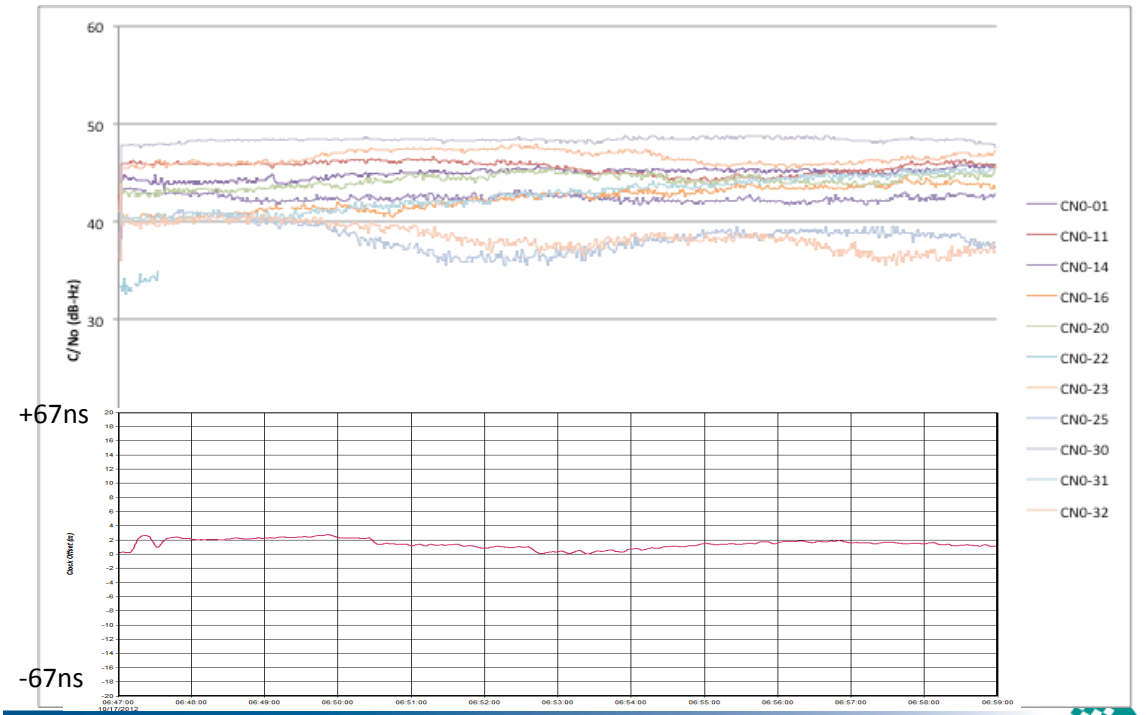


1ns rings

Susceptibility – Time impact (clock adjustments)



Benign time impacts (no jamming)



Timing susceptibility - numbers

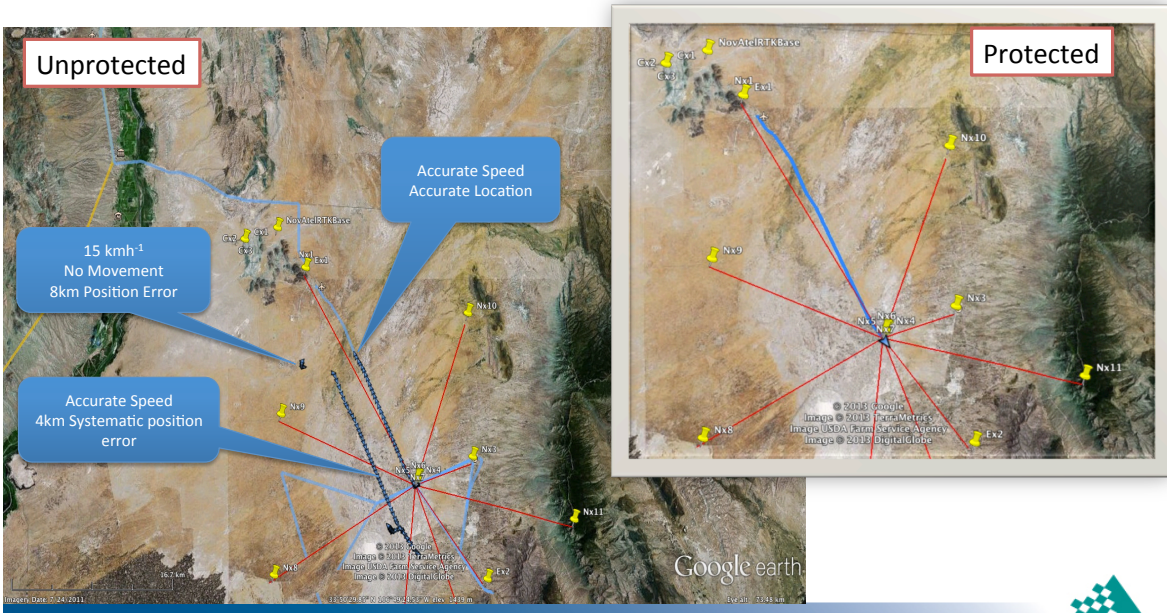
- Jammed conditions
  - Mean 4.30m (14ns)
  - St. Dev. 3.51m (12ns)
  - RMS 5.55m (18ns)

- Benign conditions
  - Mean 1.45m (5ns)
  - St. Dev. 0.64m (2ns)
  - RMS 1.58m (5ns)

N.B. Time constant to steer receiver TCXO is 10-20 seconds. Therefore discrete changes in environment would be seen as impulse response as the TCXO is steered. The absolute magnitude of the change is on the same order of magnitude, i.e. 10s of ns, not hundreds of µs.

Spoofing resistance

- Under some circumstances, a CRPA can also protect against spoofing
  - Results shown for protected and unprotected Garmin receiver



Conclusion

- *What is the latency introduced by the CRPA processing?*
  - **293.3395µs ± 1.2ns**
- *Is the latency stable over time?*
  - **In benign conditions, YES, consistent with 'normal' GPS antenna**
- *What effect does CRPA processing have on the position and time solution*
  - **In severe jamming conditions time shifts of 10-20ns is expected**

- GAJT processing latencies are stable
- For 1µs applications, GAJT protects against noise jammers without contributing significant errors to time determination
- *There is evidence that GAJT also provides a measure of protection against spoofers*
  - *the degree of protection is not yet fully determined*

Question

- IF:
  - Accurate and Available GPS time is a necessary part of Critical Infrastructure
  - GPS time is vulnerable to jamming and spoofing
  - Holdover is effective only over finite time periods
  - Holdover is ineffective against spoofers
- THEN
  - Is robust access to GPS valuable?
  - Are existing mitigations and augmentations adequate?
  - **IS THERE AN ACTIVE CURRENT NEED FOR DIRECT PROTECTION OF GPS SIGNAL ACCESS?**
    - **e.g. through a CRPA or other similar technology**