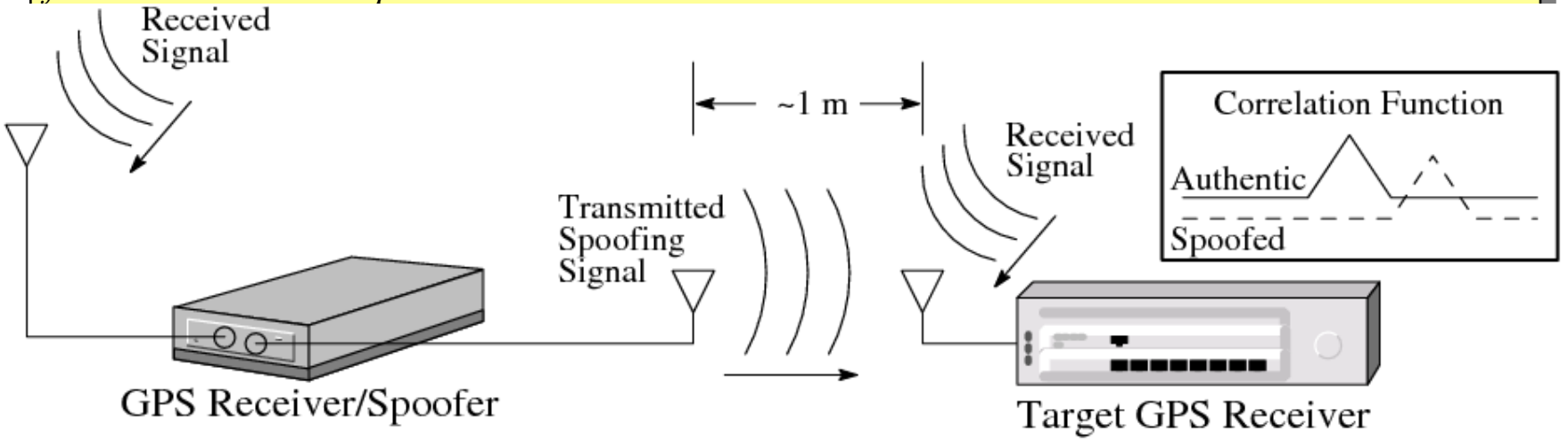
Assessing the Civil GPS Spoofing Threat

Todd Humphreys, Jahshan Bhatti, University of Texas at Austin
Brent Ledvina, Virginia Tech/Coherent Navigation
Mark Psiaki, Brady O' Hanlon, Paul Kintner, Cornell University
Paul Montgomery, Novariant

Spoofing Threat Overview

"As GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups, or countries hostile to the U.S." -- 2001 DOT Volpe Report

- *"There also is no open information on ... the expected capabilities of spoofing systems made from commercial components."*

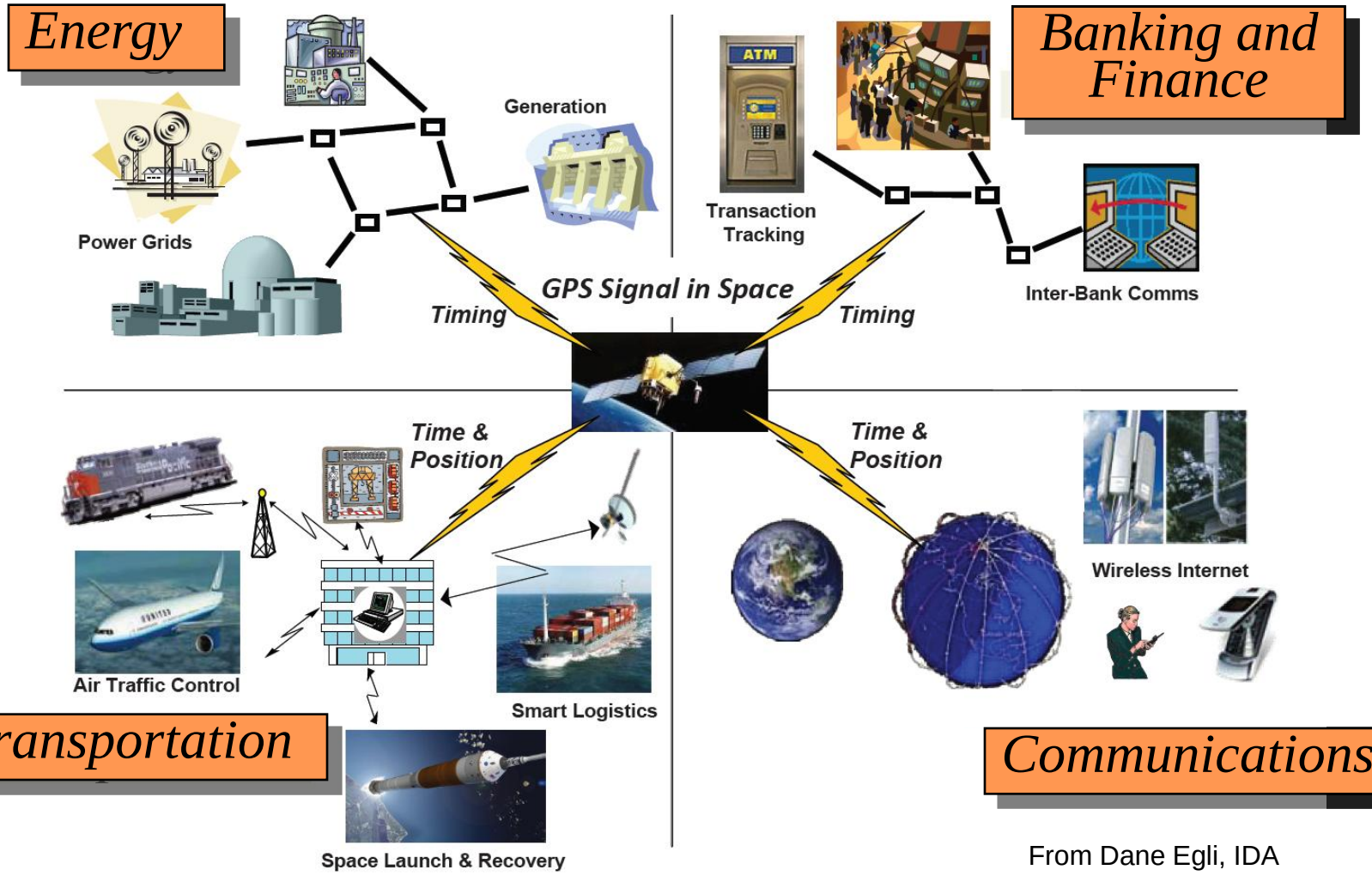


GPS World, July 2007

September 2008: Humphreys, Ledvina et al. present work on civil spoofer.

December 2009: Civilian GPS receivers as vulnerable as ever.

GPS: Dependency Begets Vulnerability



From Dane Egli, IDA

Suggested Spoofing Countermeasures

Suggested by Dept.of Homeland Security

- ~~Monitor the relative GPS signal strength~~
- ~~Monitor satellite identification codes and the number of satellite signals received~~
- ~~Check the time intervals~~
- ~~Do a time comparison (look at code phase jitter)~~
- Perform a sanity check (compare with IMU)
- Monitor the absolute GPS signal strength

Warner and Johnston, "GPS Spoofing Countermeasures," 2003
http:/www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html

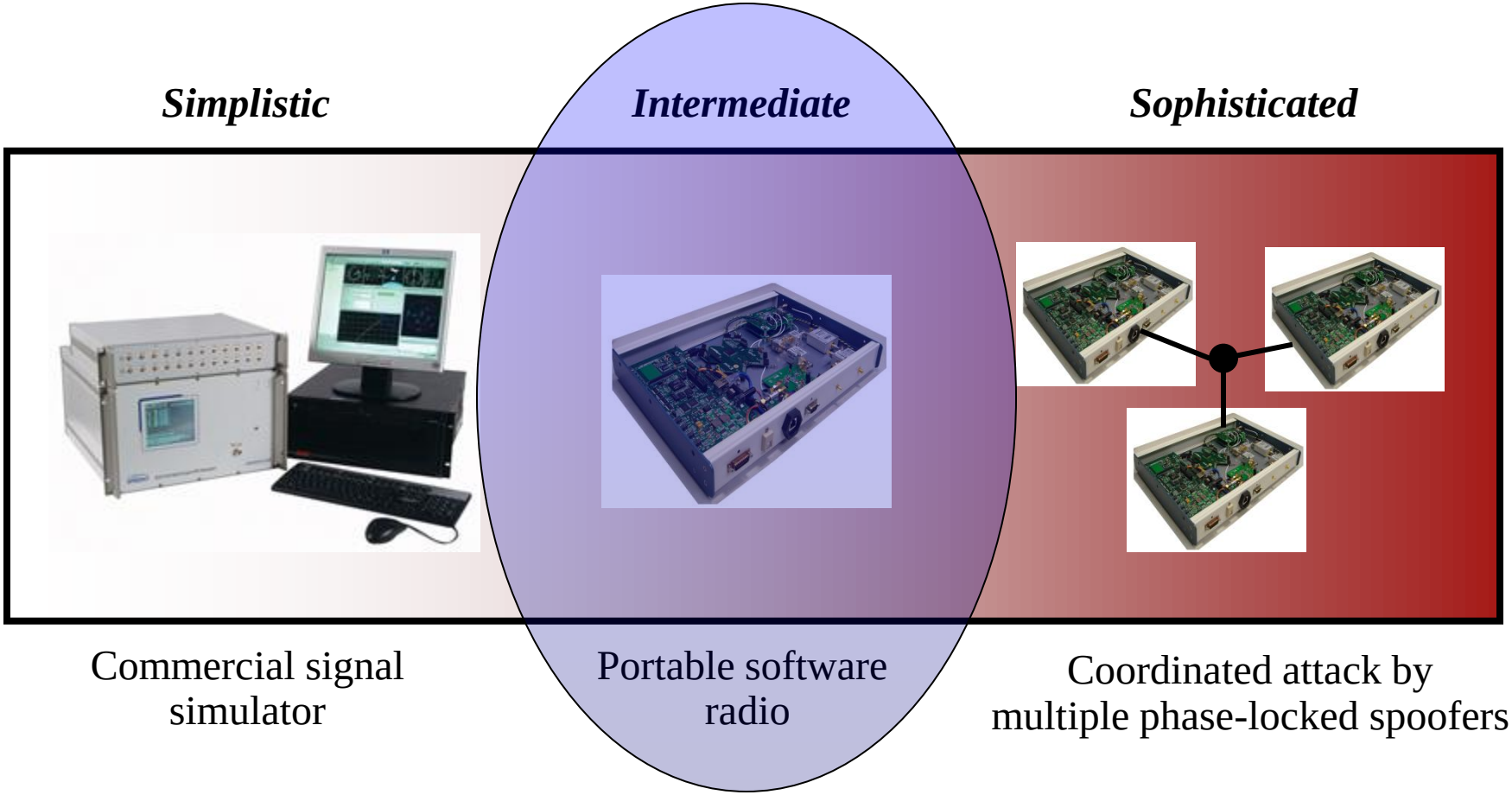
Other Suggested Techniques

- Employ two antennas; check relative phase against known satellite directions
- *To accurately assess the spoofing threat and to design effective practical countermeasures, we concluded that it was necessary to go through the exercise of building a civilian GPS spoofer*

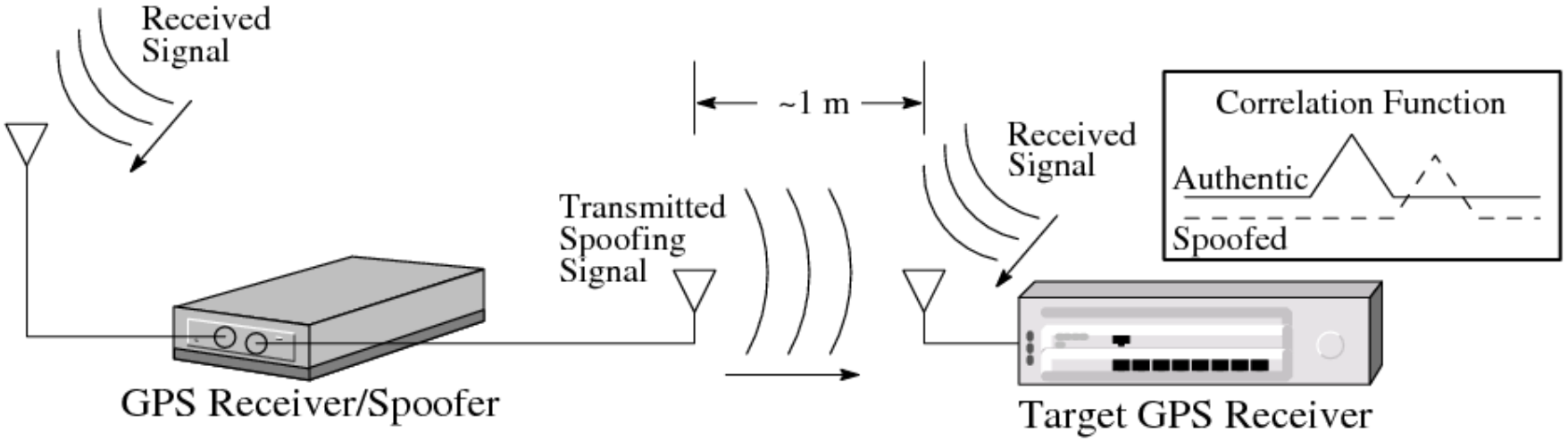
Goals

- Assess the spoofing threat:
  - Build a civilian GPS spoofer
  - Q: How hard is it to mount a spoofing attack?
  - Q: How easy is it to detect a spoofing attack?
- Investigate spoofing countermeasures:
  - Stand-alone receiver-based defenses
  - More exotic defenses

Spoofing Threat Continuum

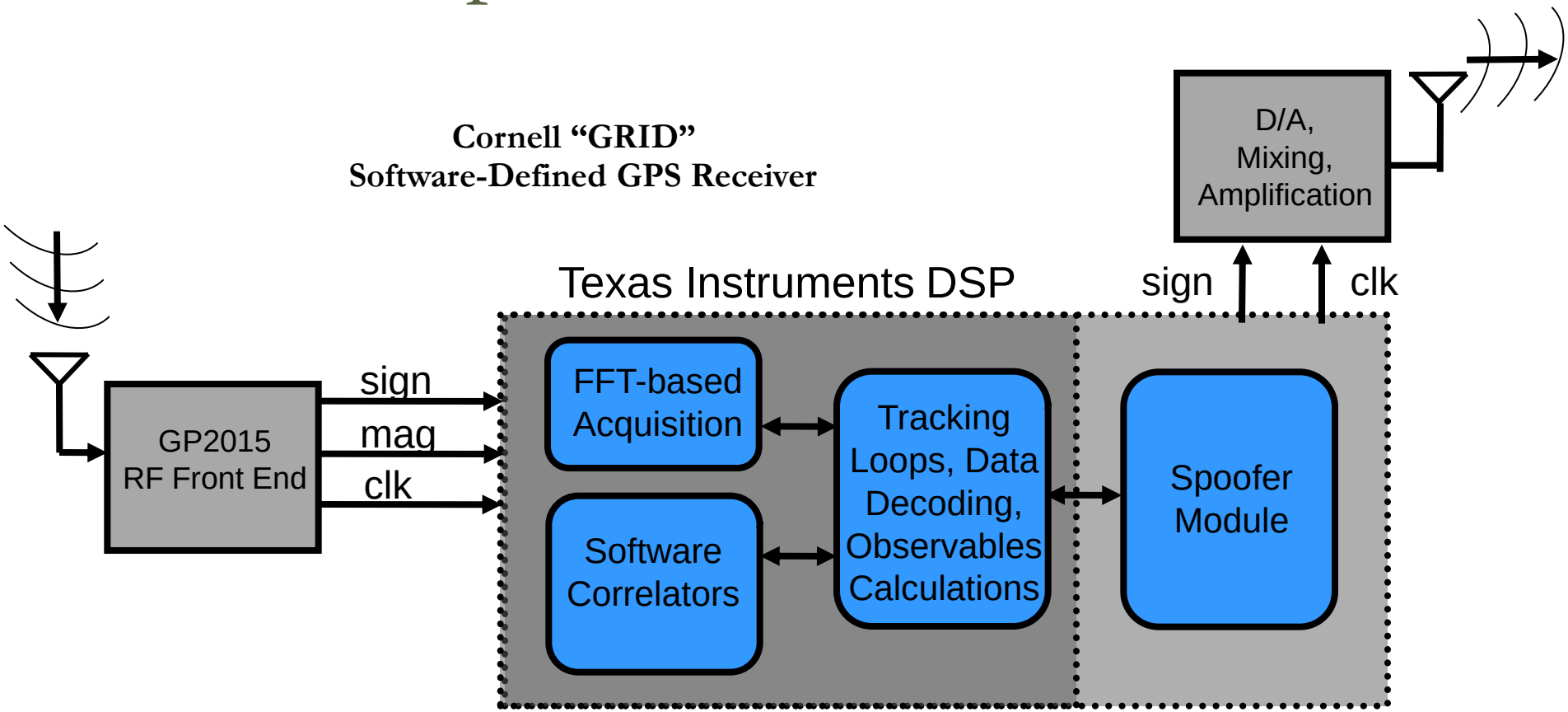


The Most Likely Threat: A Portable Receiver-Spoofer



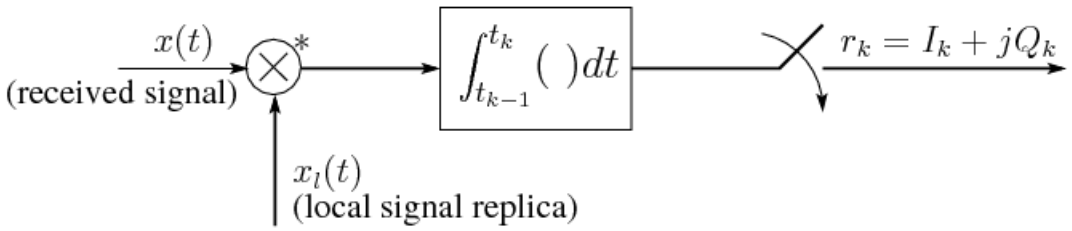
The portable receiver-spoofer architecture simplifies a spoofing attack

Receiver-Spoofer Architecture

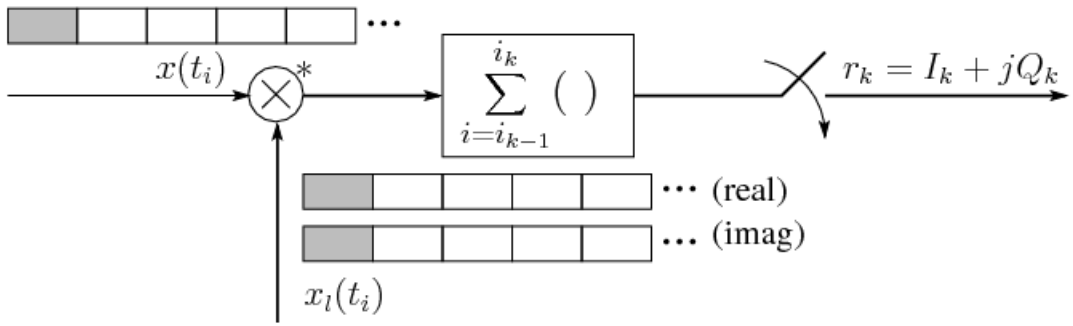


Signal Correlation Techniques (1/2)

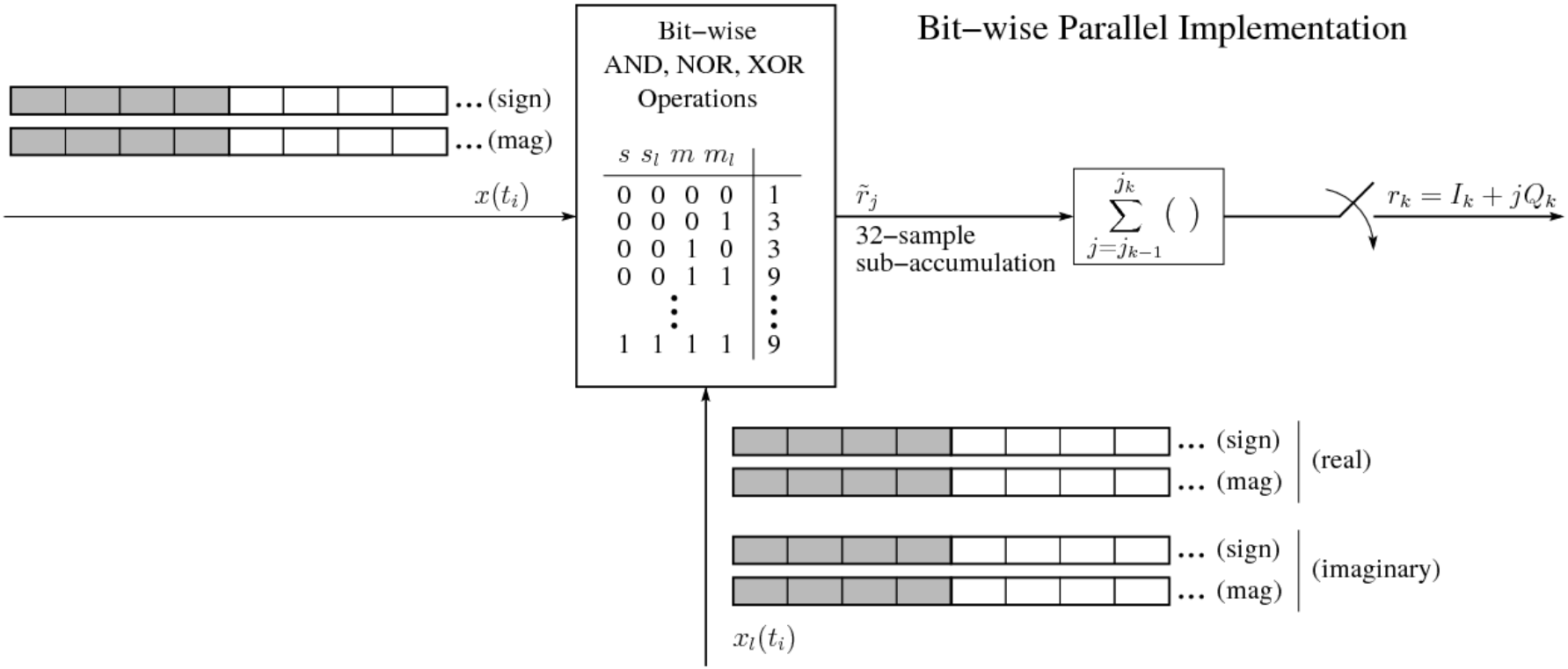
Standard Correlation Operation



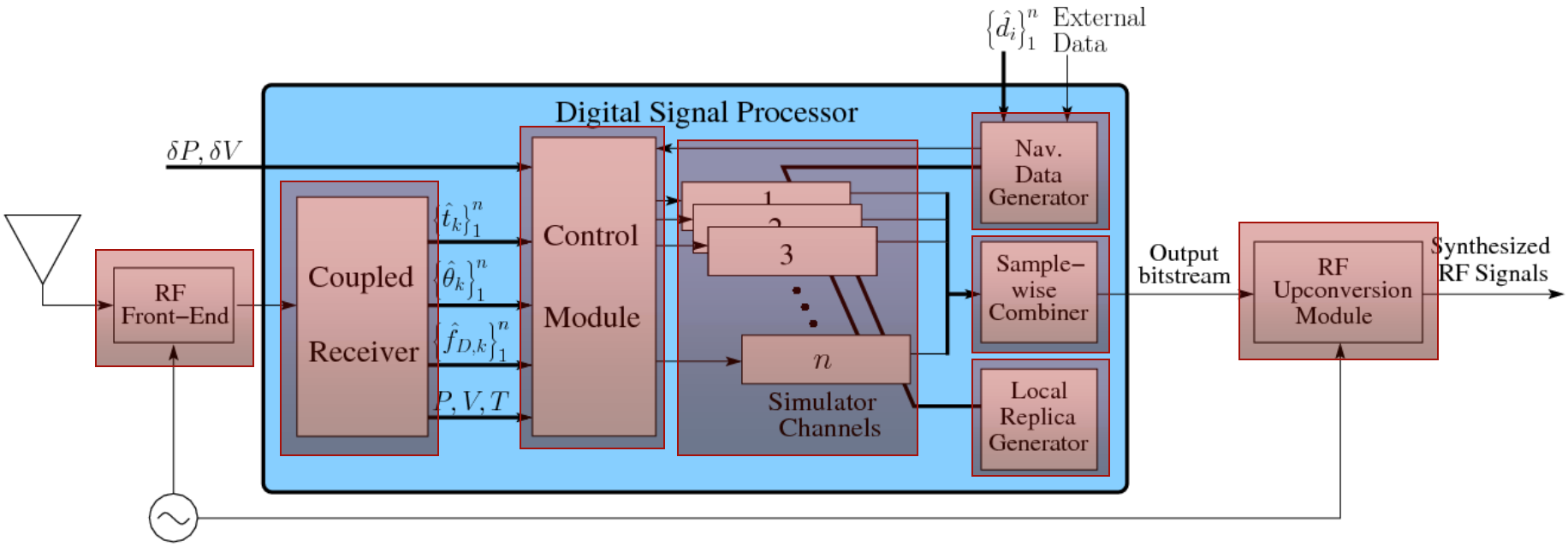
Byte–wise Implementation



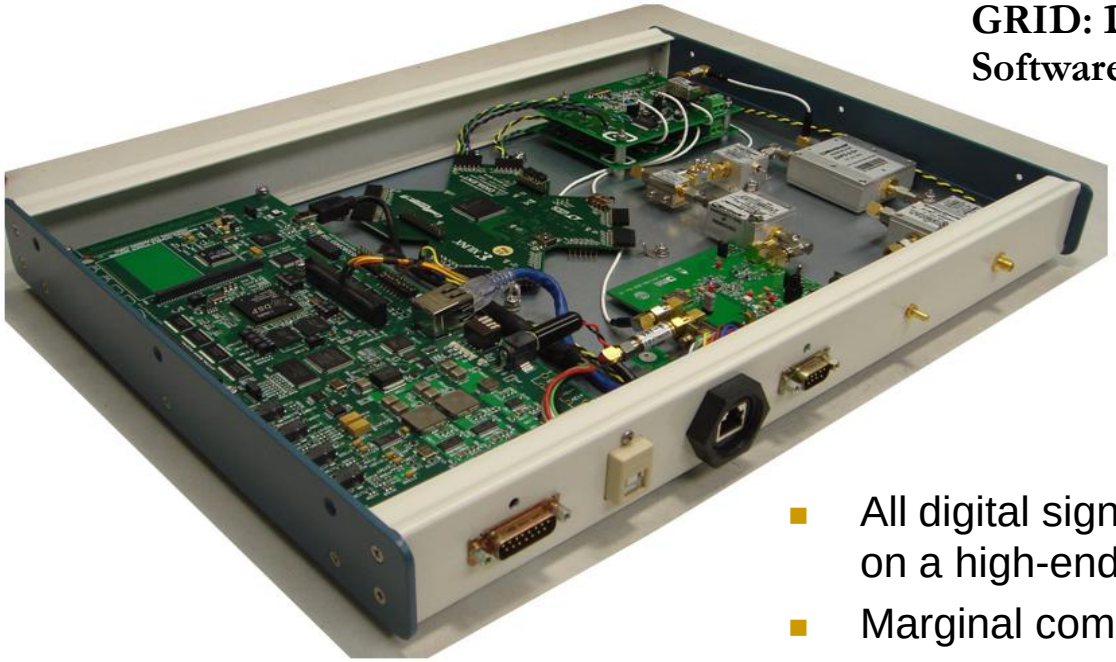
Signal Correlation Techniques (2/2)



Details of Receiver-Spoofer



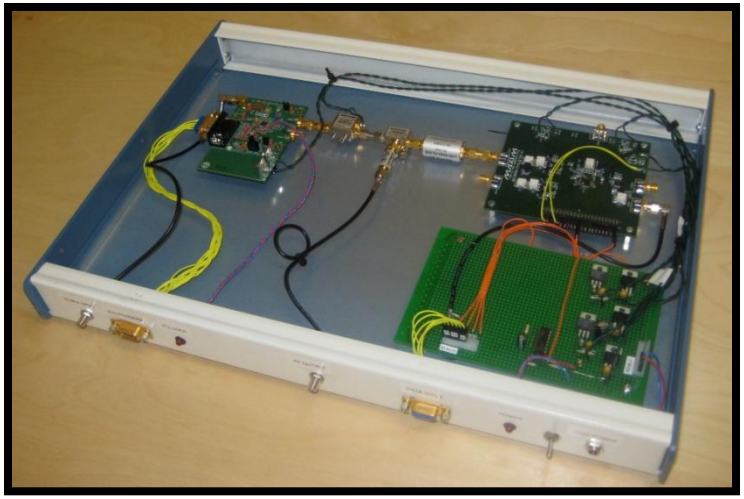
Receiver-Spoofer Hardware – DSP Box

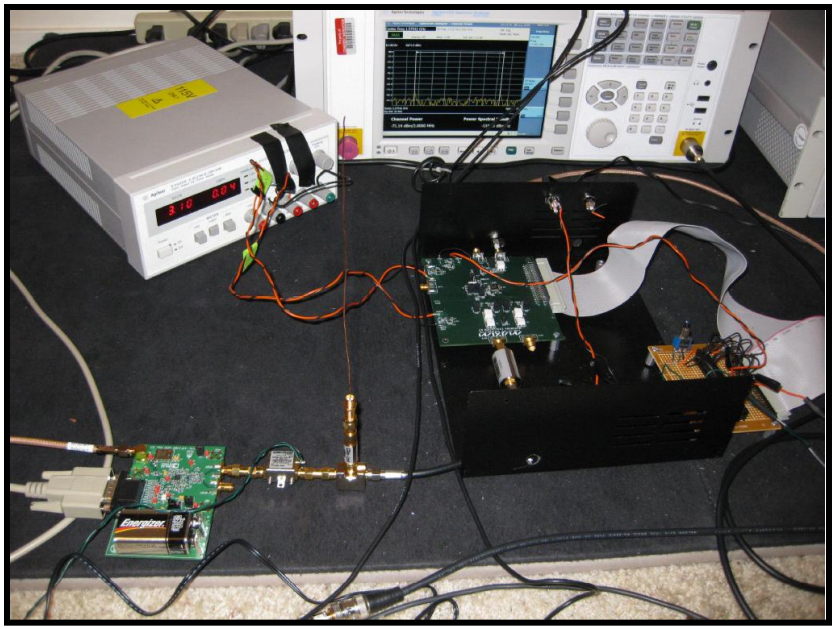


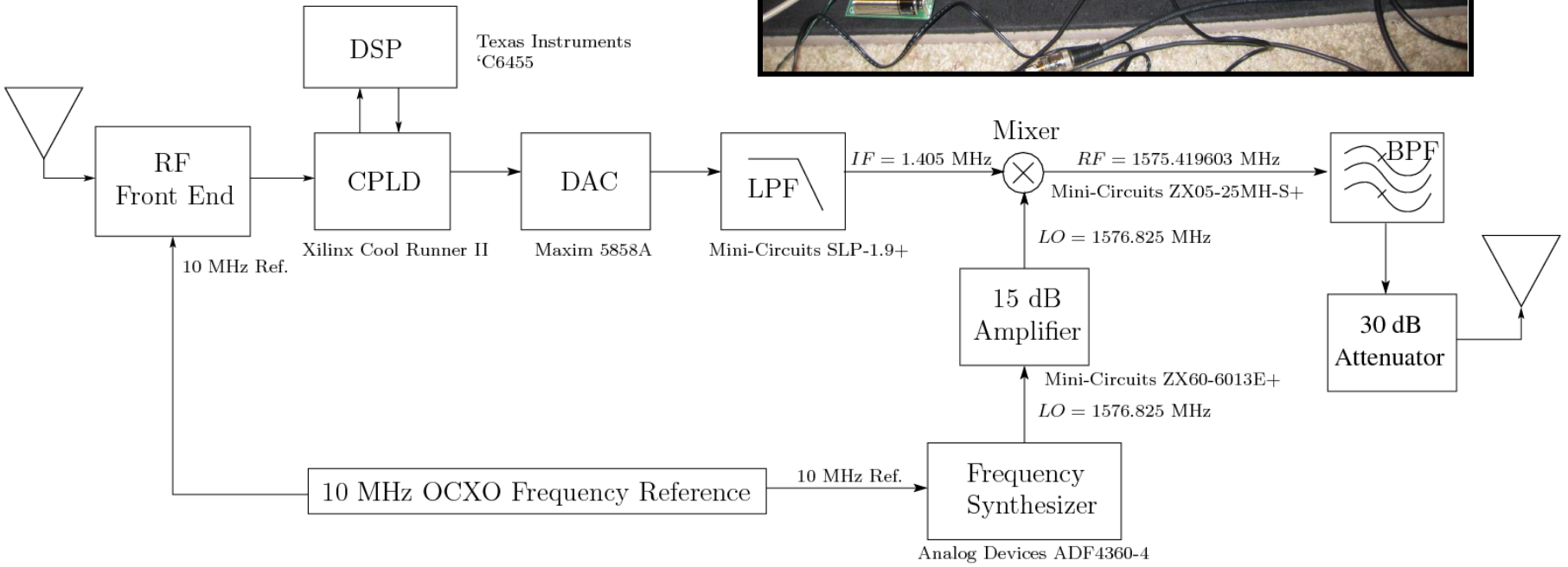
GRID: Dual-Frequency Software-Defined GPS Receiver

- All digital signal processing implemented in C++ on a high-end DSP
- Marginal computational demands:
  - Tracking: ~1.2% of DSP per channel
  - Spoofing: ~4% of DSP per channel

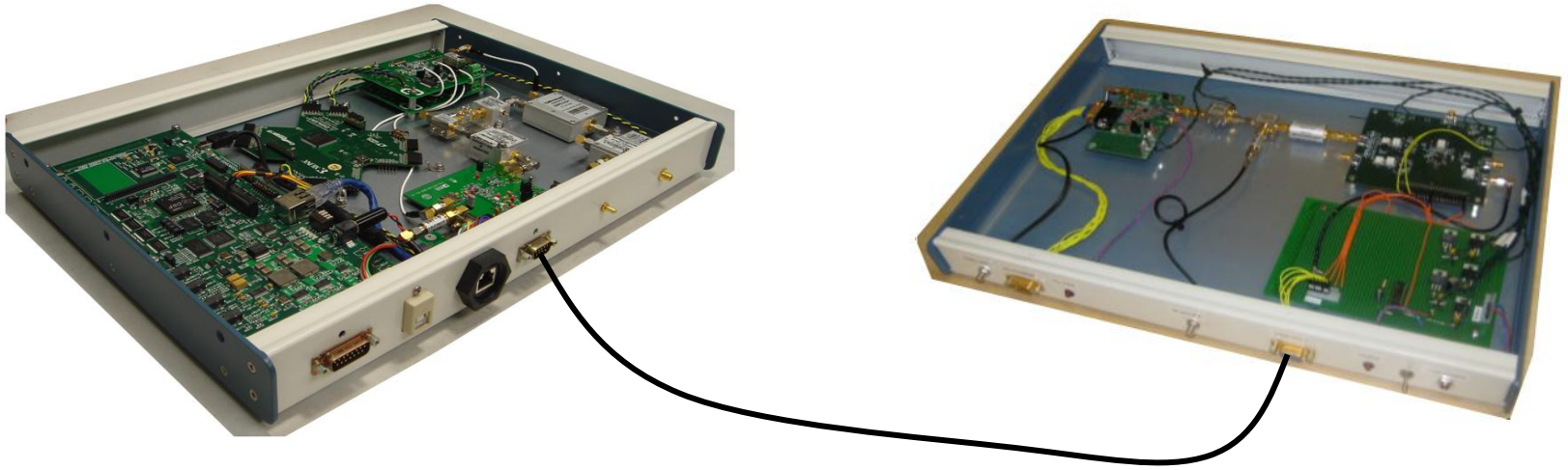
Spoofer RF Transmission Hardware







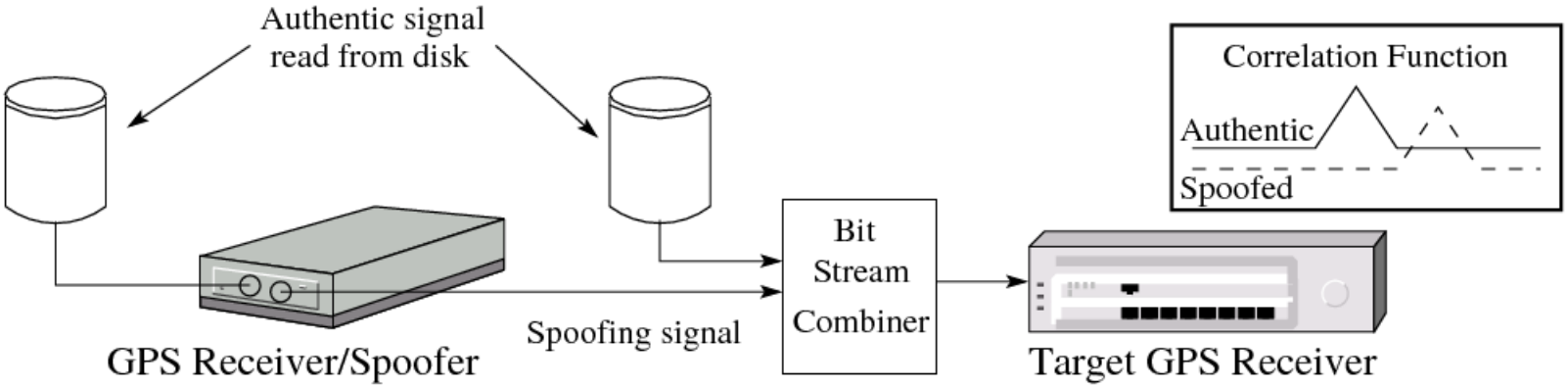
Full Receiver-Spoofer

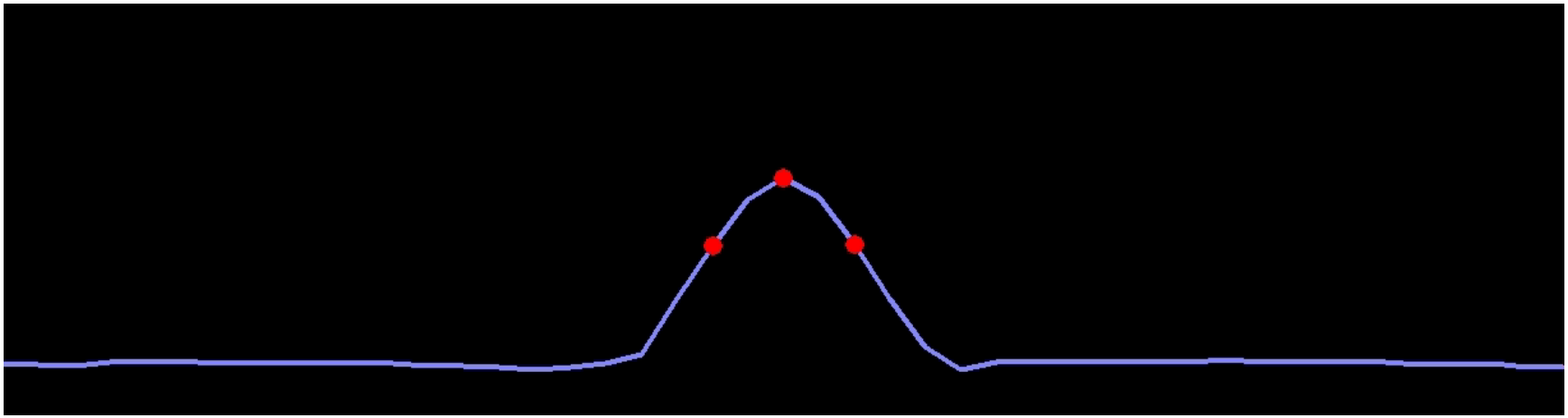


Full capability:

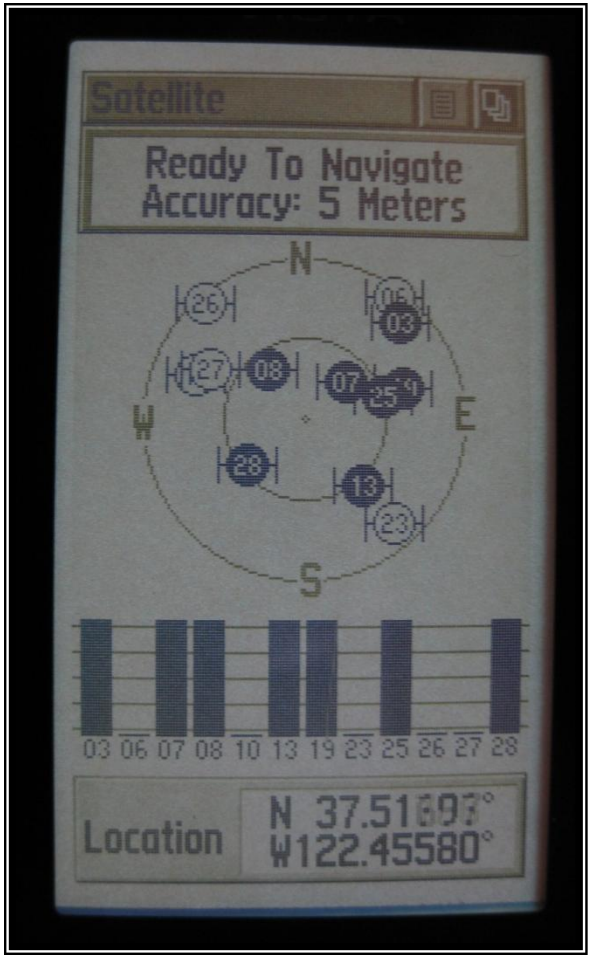
- 12 L1 C/A & 10 L2C tracking channels
- 10 L1 C/A simulation channels
- 1 Hz navigation solution
- Acquisition in background

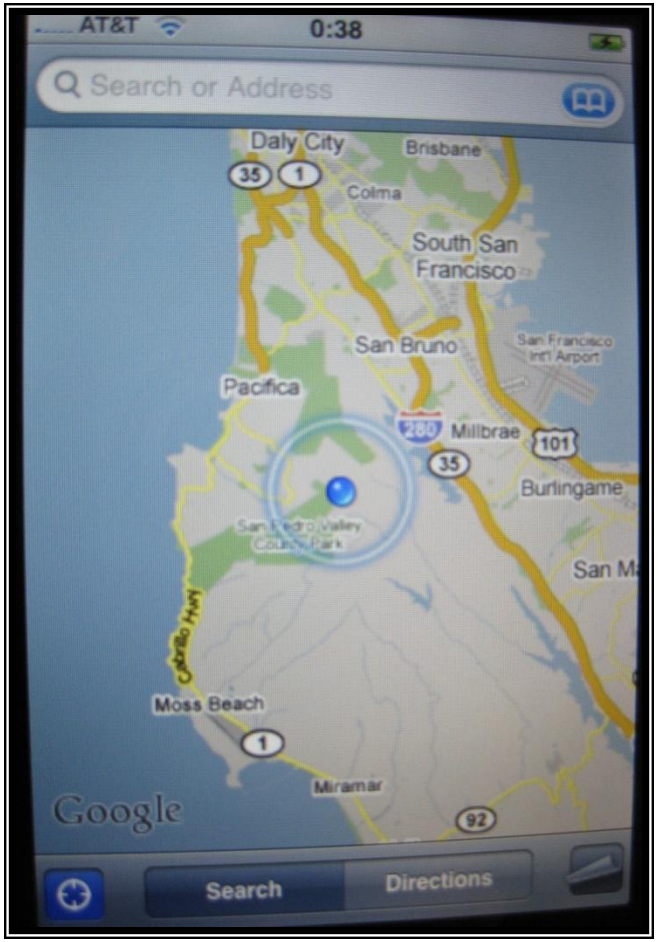
Spoofing Attack Demonstration (offline)



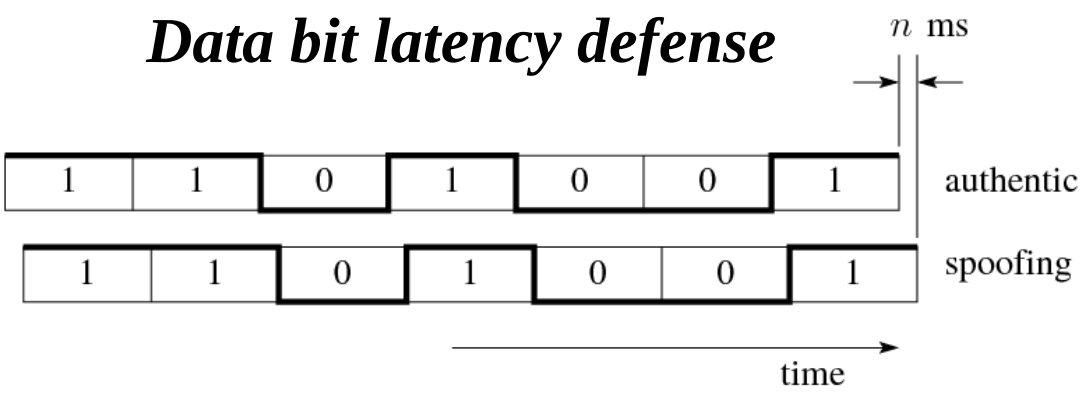


Spoofing Attack Demonstration (real-time, over-the-air)





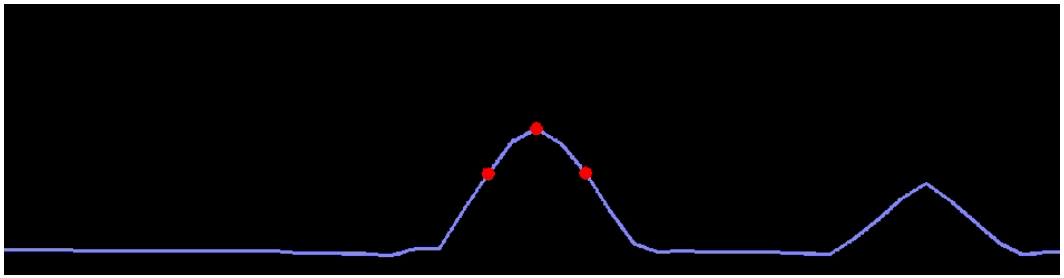
Countermeasures (1/5)



- Hard to retransmit data bits with < 1ms latency
- ***Jam first, then spoof***
- Jam-then-spoof attack may raise alarm
- ***Predict data bits***
- Hard to predict data bits during protected words and at ephemeris update boundaries
- ***Arbitrarily populate protected words, continue across ephemeris boundary with old data***
- No stand-alone countermeasure – must appeal to data bit aiding

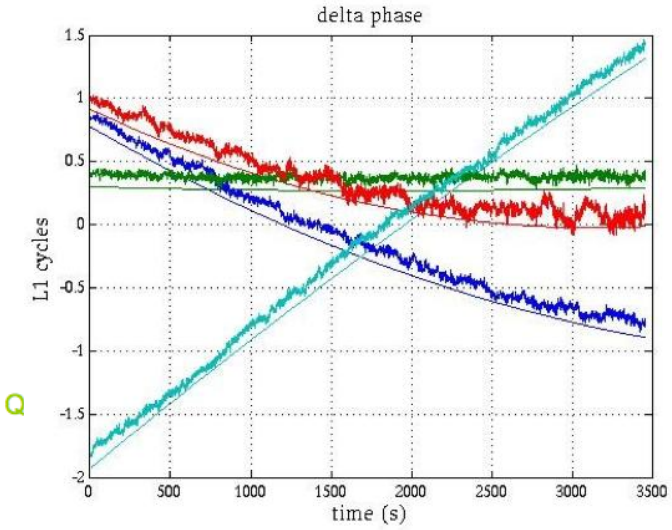
Countermeasures (2/5)

Vestigial signal defense

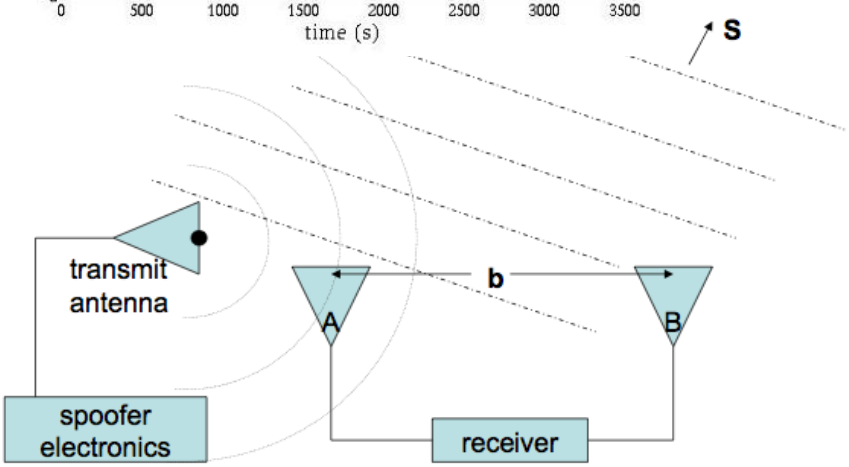


- Hard to conceal telltale peak in autocorrelation function
- ***Masquerade as multipath***
- Limits perturbation to < 1 chip
- ***Suppress authentic peak***
- Requires phase alignment for each signal at target antenna

Countermeasures (3/5) *Multi-antenna defense*

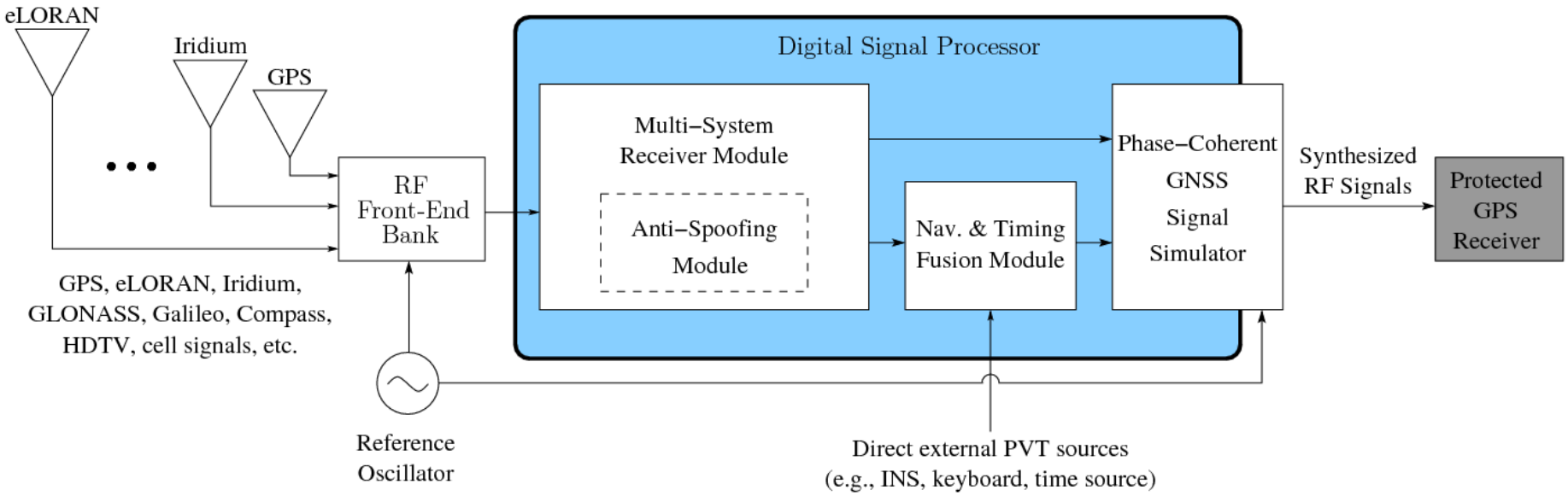


48 channel L1/L2 Quad Antenna



AutoFarm roof array with 146 cm baseline

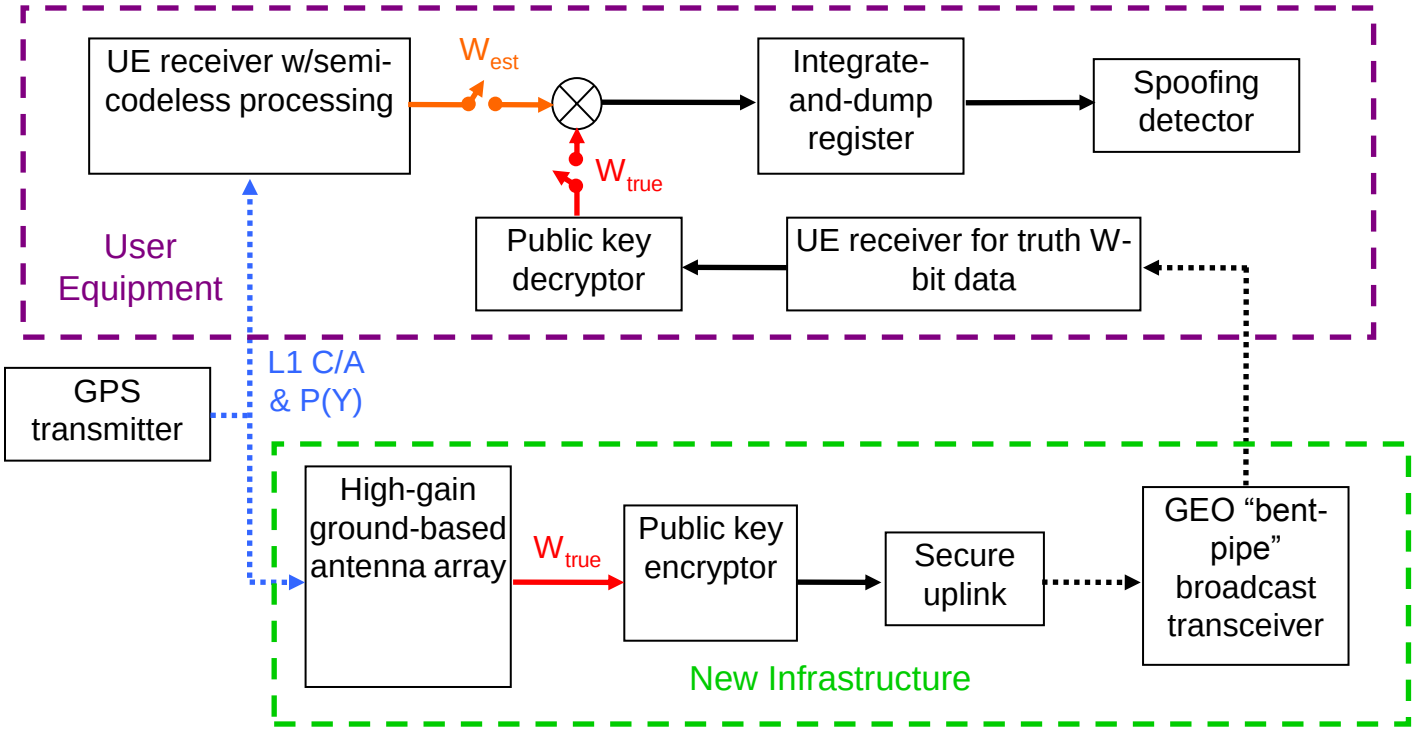
Countermeasures (4/5) ***Assimilative defense***



The GPS Assimilator modernizes and makes existing GPS equipment resistant to jamming and spoofing without requiring hardware or software changes to the equipment

Countermeasures (5/5)

Cryptographic defense based on estimation of W-bits



Findings (1/2)

- Bad news:
  - It's straighforward to mount an intermediate-level spoofing attack
- Good news:
  - It's hard to mount a sophisticated spoofing attack, and there appear to be inexpensive defenses against lesser attacks
- Bad news:
  - There is no defense short of embedding cryptographic signatures in the spreading codes that will defeat a sophisticated spoofing attack

Findings (2/2)

- Good news:
  - With the addition of each new modernized GNSS signal, the cost of mounting a spoofing attack rises markedly
- Bad news:
  - FPGAs or faster DSPs would make multi-signal attacks possible
- More bad news:
  - There will remain many single-frequency L1 C/A code receivers in critical applications in the years ahead

Are We Safe Yet?

- No. There is much much work to be done:
  - Characterization of spoofing signatures in full RF attack
  - Development and testing of more effective countermeasures, including stand-alone countermeasures and and network-based cryptographic countermeasures
  - Encourage commercial receiver manufacturers to adopt spoofing countermeasures