THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Embedded Signal Processing Laboratory
ESPL
The University of Texas at Austin

GPS Spoofing & Implications for Telecom

Kyle Wesson

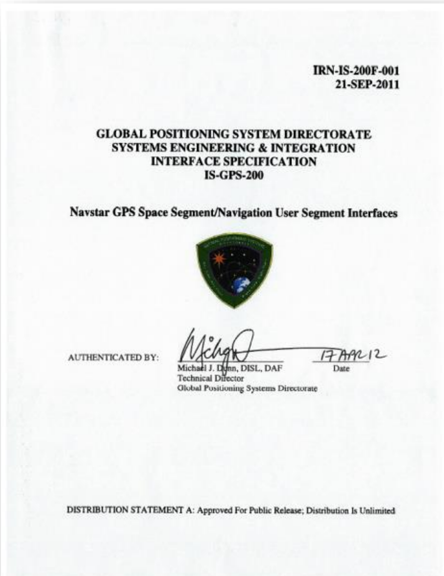
The University of Texas at Austin

Sprint Synchronization Conference | September 18, 2013

Talk Overview

- Civil GPS Spoofing Vulnerability
- Anti-Spoofing Techniques
  - Cryptographic: Navigation Message Authentication
  - Non-Cryptographic: “Sandwich” Defense
- Securing and Testing

Civil GPS is Vulnerable to Spoofing


IRN-IS-200F-001
21-SEP-2011

GLOBAL POSITIONING SYSTEM DIRECTORATE
SYSTEMS ENGINEERING & INTEGRATION
INTERFACE SPECIFICATION
IS-GPS-200

Navstar GPS Space Segment/Navigation User Segment Interfaces

AUTHENTICATED BY: Michael J. Dunn, DISL, DAF, Technical Director, Global Positioning Systems Directorate — 17 APR 12 (Date)

DISTRIBUTION STATEMENT A: Approved For Public Release; Distribution Is Unlimited

An **open GPS standard** makes GPS popular but also vulnerable to **spoofing**


ieee spectrum — INSIDE TECHNOLOGY

AEROSPACE | BIOMEDICAL | COMPUTING | CONSUMER ELECTRONICS | ENERGY

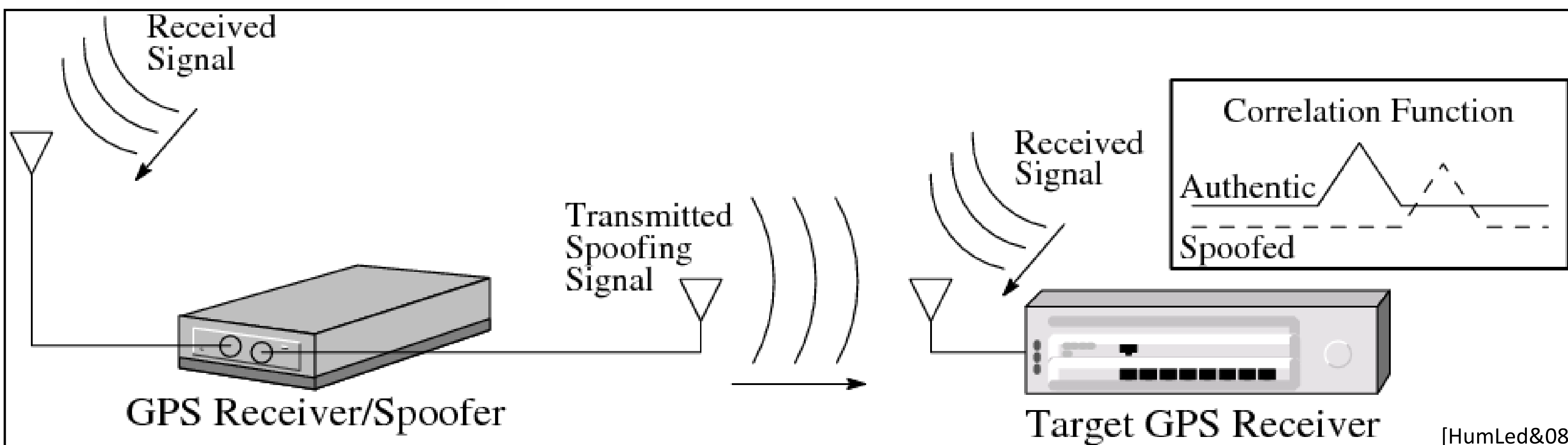
risk factor

BLOGS // THE RISK FACTOR

Commercial Drones and GPS Spoofers a Bad Mix

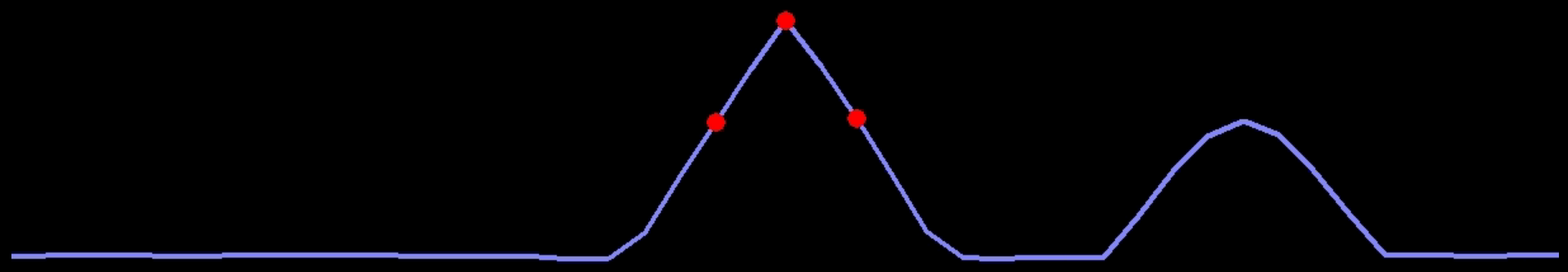
POSTED BY: ROBERT N. CHARETTE / MON, JUNE 25, 2012

Researchers at the University of Texas at Austin Radionavigation Laboratory have successfully demonstrated that a drone with an unencrypted GPS system can be taken over by a person wielding a GPS spoofing device. You can see a video accompanying a Fox News story on it, as well as a video here of an



University of Texas Spoofing Testbed

Inside a Spoofing Attack



Civil GPS Spoofing

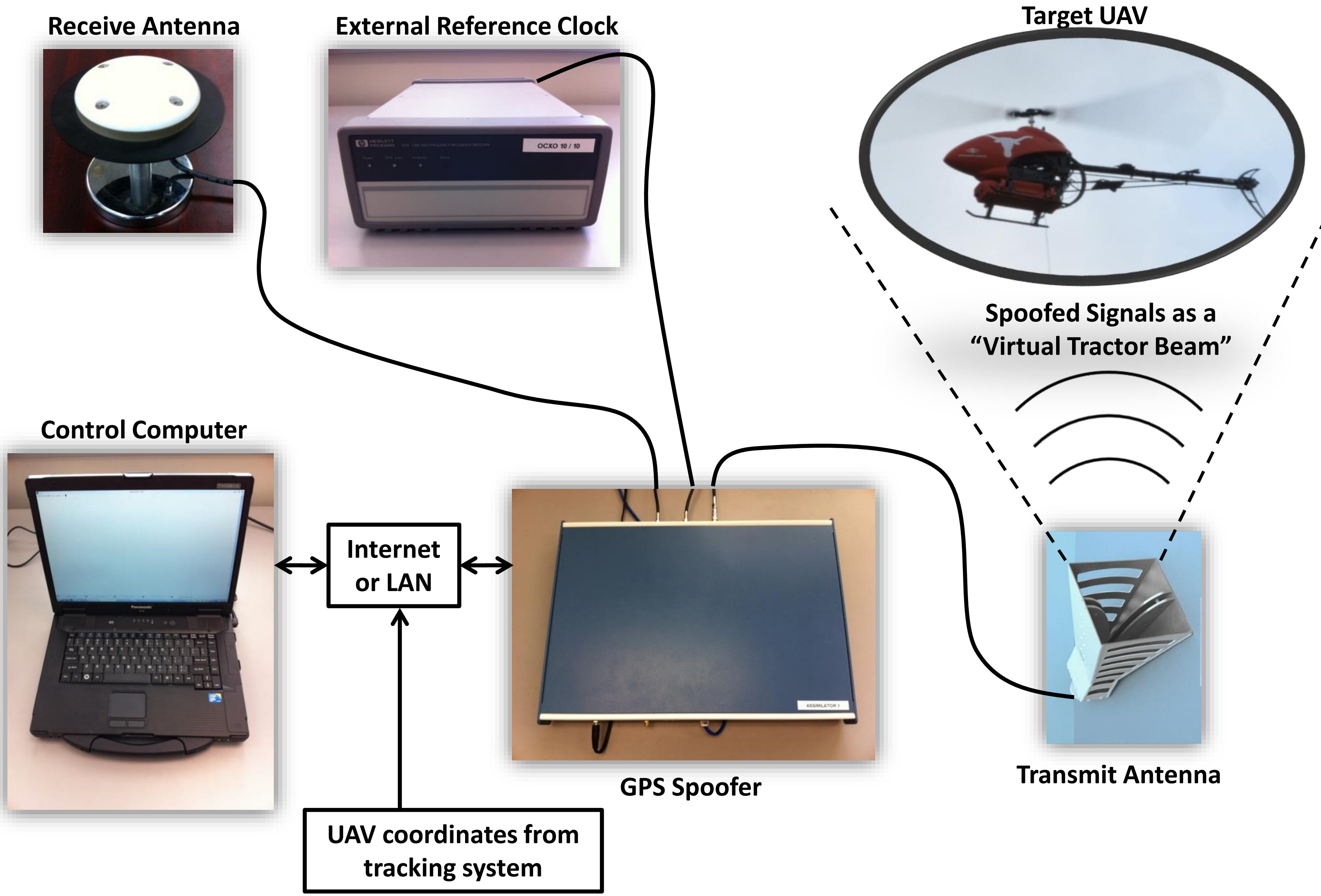
- A discrete spoofing attack typically involves four phases:
  1) Alignment of the authentic and spoofed GPS signals at the target receiver
  2) Increase the power of the spoofed signals above the authentic
  3) Move the spoofed signals slowly away from the authentic signals
  4) Once the spoofed and authentic signals no longer interfere, the spoofer has complete control of the target receiver's PVT solution

- Spoofer-imposed dynamics are limited only by the bandwidth of the target receiver's tracking loops and it's quality indicators

- No receiver we've tested has ever successfully defended against this type of attack

D.P. Shepard and T.E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks," *Proceedings of ION GNSS*, Portland, Oregon, 2011.

Spoofing a UAV (2012)



Surprises (1/2)

- Receiver Autonomous Integrity Monitoring (RAIM) was *helpful* for spoofing: we couldn’t spoof all signals seen by unmanned aerial vehicle (UAV) due to our reference antenna placement, but the Hornet Mini’s uBlox receiver rejected observables from authentic signals, presumably via RAIM
- Overwhelming power is required for clean capture: A gradual takeover leads to large (50-100 m) multipath-type errors as the authentic and counterfeit signals interact
- The UAV’s heavy reliance on altimeter for vertical position was easily overcome by a large vertical GPS velocity

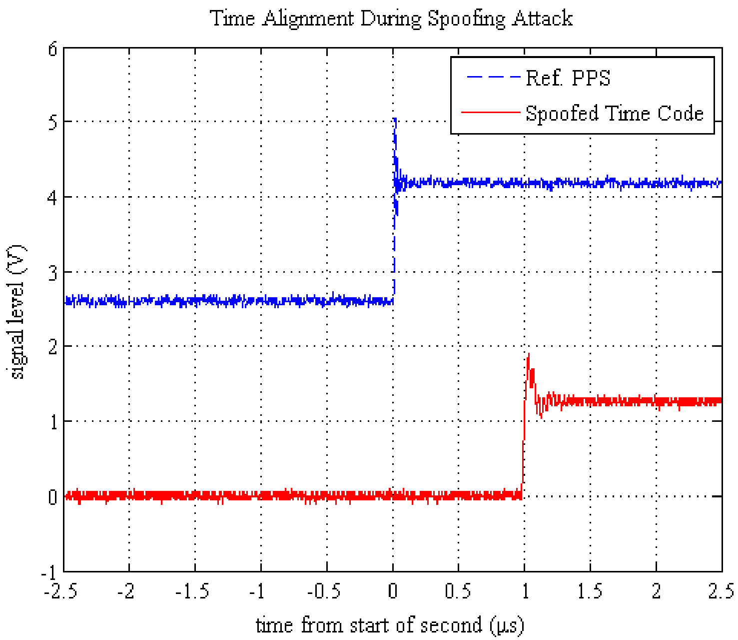
Surprises (2/2)

- Not possible even to station keep with a captured UAV based on visual position estimates: GPS capture breaks flight controller’s feedback loop; now spoofer must play the role formerly assumed by GPS. Implication: An accurate radar or LIDAR system would be required for fine “control” of UAV via spoofing
- Compensating for all system and geometric delays to achieve meter-level alignment is challenging but quite possible

Spoofing a Super Yacht (2013)

Telecom Network Vulnerabilities

Standard	Timing (Air)	Frequency (Transport / Air)
CDMA2000	± 3 – 10 µs	± 16 ppb / ± 50 ppb
GSM	–	± 16 ppb / ± 50 ppb
LTE (FDD)	–	± 16 ppb / ± 50 ppb
LTE (TDD)	± 1.5 µs	± 16 ppb / ± 50 ppb
TD-SCDMA	± 1.5 µs	± 16 ppb / ± 50 ppb



In 35 minutes, spoofer can shift time 10 µs, which would disrupt CDMA2000 call hand-off

Misconceptions about Timing Security (1/2)

- "Holdover" capability of GPS-disciplined oscillator (GPSDO) protects against spoofing
  - Holdover will not be triggered by a sophisticated spoofing attack
- The reference oscillator's drift rate is the upper limit of speed at which a GPSDO can be spoofed (e.g., 1 us per day)
  - Drift rate only matters if GPSDO is configured to alarm on a mismatch between GPS rate and internal clock rate
  - Even then, spoofer can push GPS timing at about 5x the calibrated clock drift rate because of need to keep false alarm rate low

Misconceptions about Timing Security (2/2)

- Timing errors only become a problem at the level of seconds, or maybe milliseconds.
  - Microseconds matter in comm, finance, and energy sectors
- Cross-checking against an atomic clock affords foolproof timing security
  - Rubidium clock with stability of 10^{-12} can be pushed off by about 100 ns per day
- PTP/NTP are a potential solution to GPS spoofing problem
  - These are getting better, but, due to network asymmetry, they still not accurate enough for most demanding applications non-dedicated networks

Recommendations

Humphreys' testimony to House Committee on Homeland Security, July 19, 2012

- ***Require*** navigation systems for UAVs above 18 lbs to be certified "spoof-resistant"
- ***Require*** navigation and timing systems in critical infrastructure to be certified "spoof-resistant"
- "Spoof resistant" defined by *ability to withstand or detect civil GPS spoofing in* a battery of tests performed in a spoofing testbed (e.g., Texas Spoofing Battery)

ANTI-SPOOFING

Spoofing Defenses

Cryptographic

Stand-Alone

SSSC on L1C
(Scott)

NMA on L2C, L5, or L1C
(MITRE, Scott, UT)

SSSC or NMA on WAAS
(Scott, UT)

Networked

P(Y) Cross-Correlation
(Stanford, Cornell)

Non-Cryptographic

J/N Sensing
(Ward, Scott, Calgary)

Sensor Diversity Defense
(DARPA, BAE, UT)

Single-Antenna Spatial Correlation
(Cornell, Calgary)

Correlation Anomaly Defense
(TENCAP, Ledvina, Torino, UT)

Multi-Element Antenna Defense
(Keys, Montgomery, DLR, Stanford)

Anti-Spoofing

CRYPTOGRAPHIC ANTI-SPOOFING

Security-Enhanced GPS Signal Model

$$\begin{aligned} Y_k &= w_k c_k \cos(2\pi f_{IF} t_k + \theta_k) + N_k \\ &= w_k s_k + N_k \end{aligned}$$

- Security code w_k:
  - Generalization of binary modulating sequence
  - Either fully encrypted or contains periodic authentication codes
  - Unpredictable prior to broadcast

Attacking Security-Enhanced GPS Signals

1. **Record and Playback (Meaconing)**: record and re-broadcast RF spectrum

$$Y_k = \boxed{\alpha w_{k-d} s_{k-d} + N_{m,k}} + \boxed{w_k s_k + N_k}$$

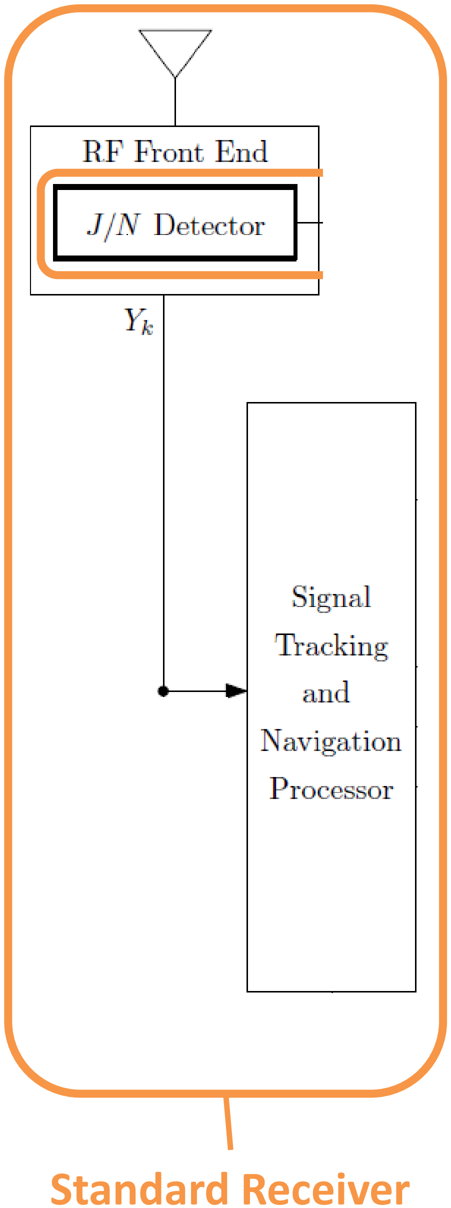
re-broadcast with delay d
and amplitude α

2. **Security Code Estimation and Replay (SCER) Attack**: estimate security code on-the-fly without additional noise

$$Y_k = \boxed{\alpha \hat{w}_{k-d} s_{k-d}} + \boxed{w_k s_k + N_k}$$

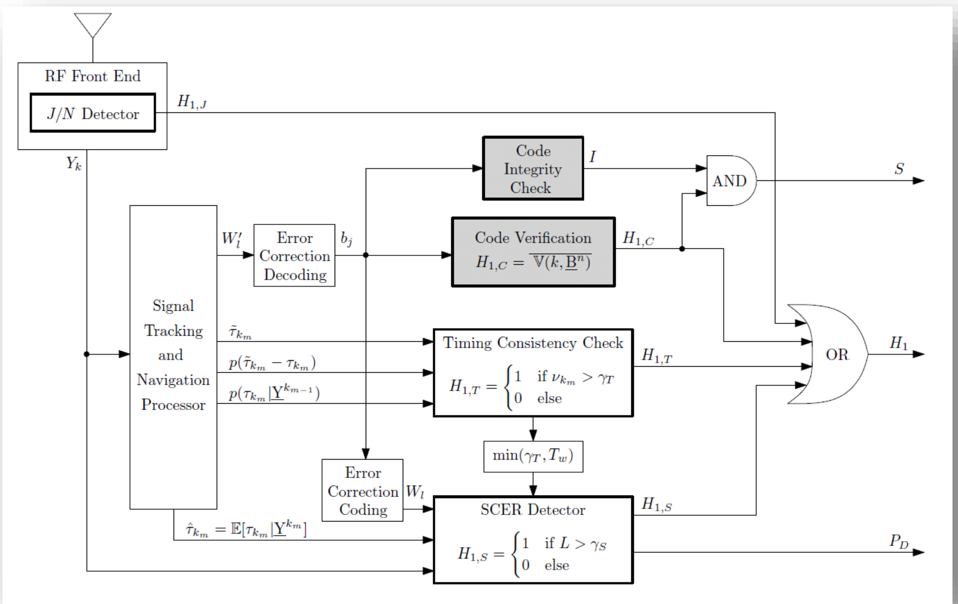
security code
estimate $\hat{w}$

How to authenticate a GPS signal?



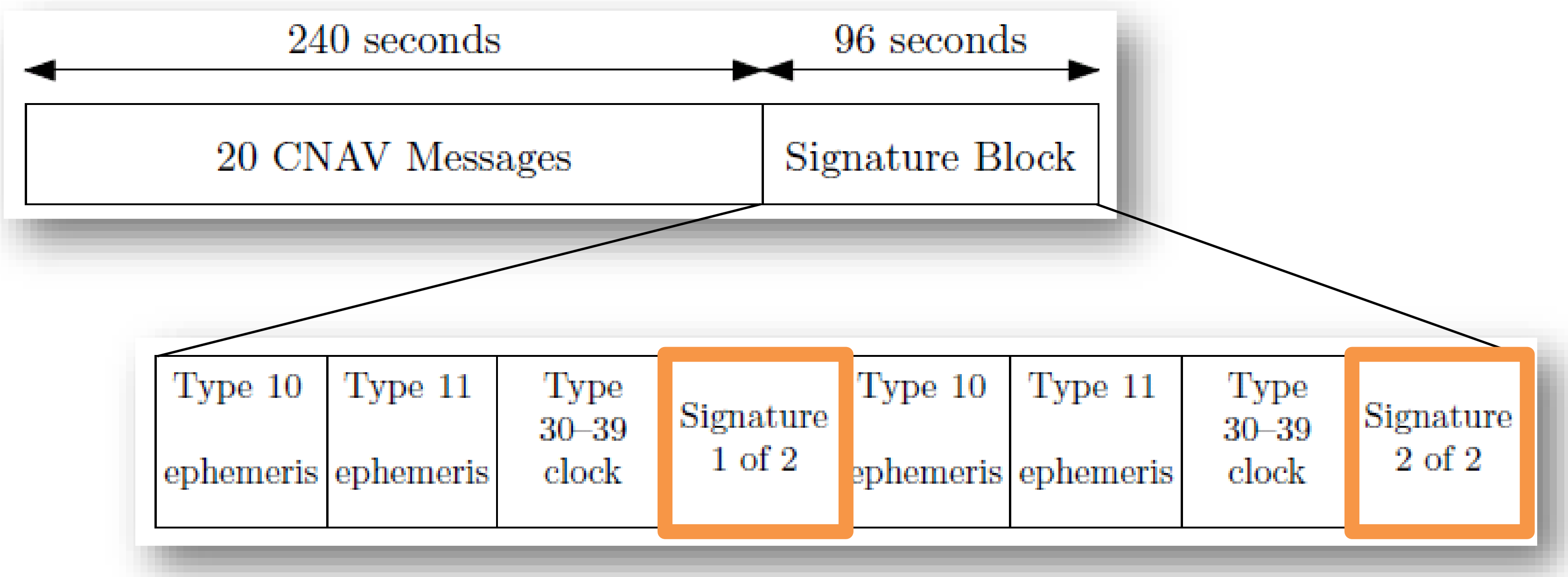
Declaring a Signal Authentic

- From time of verifiable non-spoofing event:
  1. Logical S remained low
  2. Logical H_1 remained low
  3. P_D remains above acceptable threshold



Embedding the Signature

- Civil Navigation (CNAV) Message
  - Flexible & extensible
- Packet-like structure:
  - 300 bits in 12 sec
  - Message Type ID field can identify up to 64 messages of which only 15 are defined



Anti-Spoofing

NON-CRYPTOGRAPHIC ANTI-SPOOFING

Spoofing Requirement and Difficulty

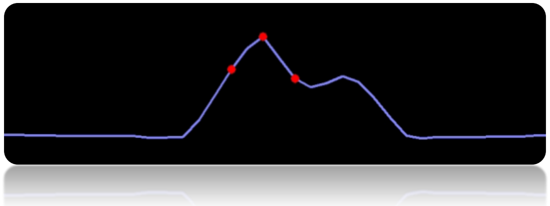
Q: What is a requirement of a successful spoofing attack?

A: Spoofed signal power greater than authentic signal power

$$\eta \triangleq P_S/P_A > 1$$

Q: What is a difficulty of a successful spoofing attack?

A: Suppressing authentic signals while remaining below J/N sensor detector

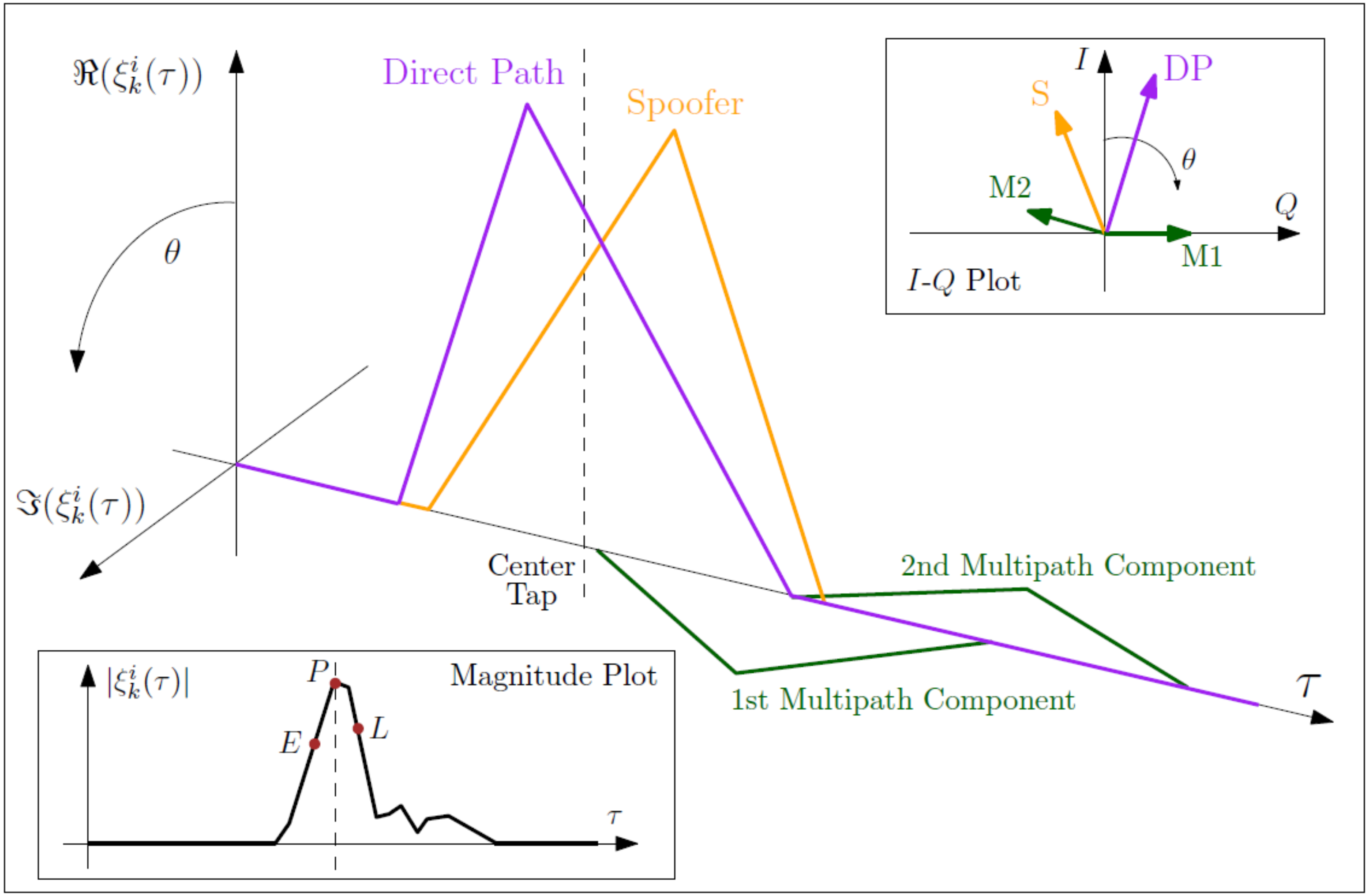


“Sandwich” Defense

- Constrain spoofer between
  1. total in-band received power detector &
  2. cross-correlation function distortion monitor

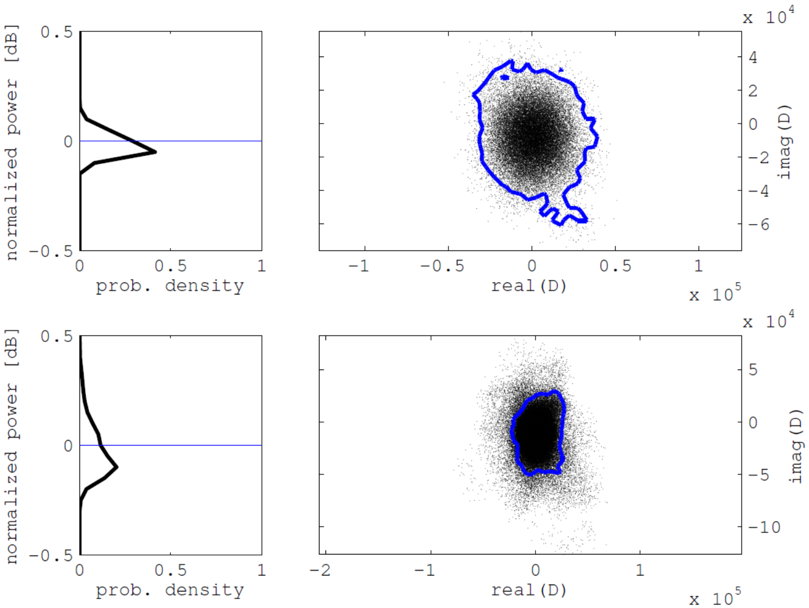
- Features
  - Use multiple correlator taps (RAKE-like)
  - Check multipath signatures across channels
  - Real-time, software defense

Spoofed Signal Distortions

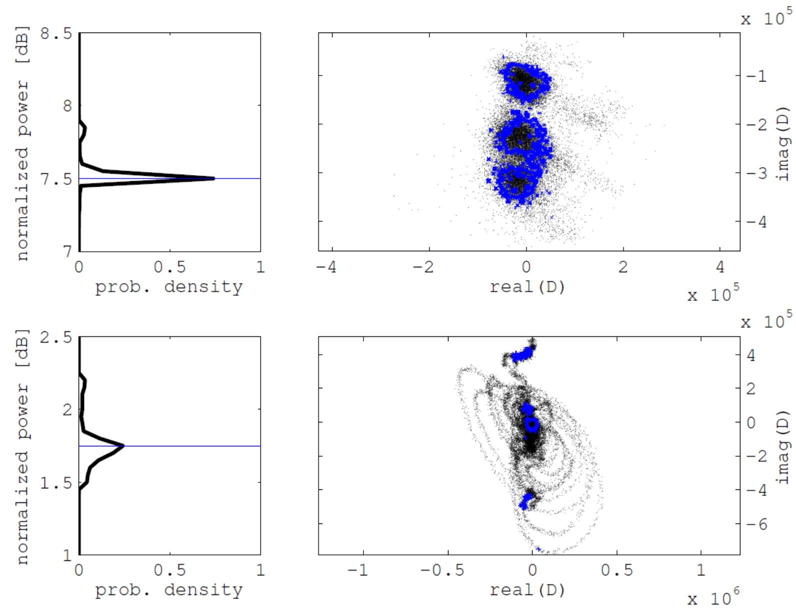


Clean vs. Spoofed Scenarios

Nominal Power and Minimal Distortions



Additional Power and Large Distortions



So what is there to do?

SECURING AND TESTING

Options for Secure ns-Accurate Timing (1/2)

- Obtain required permissions to purchase SAASM-equipped GPSDO
  - Lots of paperwork, special handling
  - Expensive
  - Fairly secure against spoofing
  - Not secure against replay attack
- Wait for GPS Directorate to insert digital signatures into modernized GPS signals
  - They're making progress! (The University of Texas is helping.)
  - Not so strong as SAASM for timing security, but quite effective
  - Eventually inexpensive, but will require new GPSRO

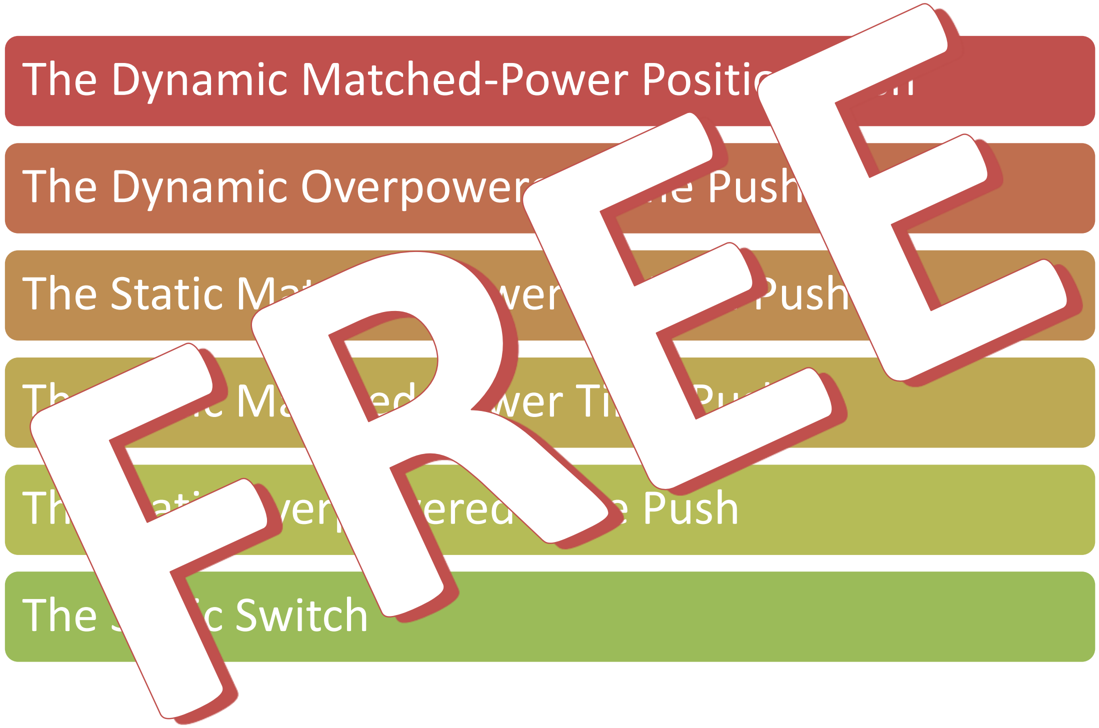
Options for Secure ns-Accurate Timing (2/2)

- Cross-check GPS timing against redundant high-quality (e.g., atomic) clocks
  - Self-contained
  - Expensive
  - Absolutely secure to within about 5x the drift rate of ensemble
- "All Signals" Approach: Develop a GPSDO that pulls in signals from GPS + Glonass + Galileo and rigorously cross-checks these
  - None on market yet (so far as I'm aware)
  - Potentially inexpensive: uBlox LEA-7 runs ~$50
  - Spoofer's job gets much harder with each new signal
- PTP/NTP over a dedicated network

The Texas Spoofing Test Battery (TEXBAT)

Scenario Designation	Spoofing Type	Platform Mobility	Power Adv. (dB)	Frequency Lock	Noise Padding	Size (GB)
1: Static Switch	N/A	Static	N/A	Unlocked	Enabled	43
2: Static Overpowered Time Push	Time	Static	10	Unlocked	Disabled	42.5
3: Static Matched-Power Time Push	Time	Static	1.3	Locked	Disabled	42.6
4: Static Matched-Power Pos. Push	Position	Static	0.4	Locked	Disabled	42.6
5: Dynamic Overpowered Time Push	Time	Dynamic	9.9	Unlocked	Disabled	38.9
6: Dynamic Matched-Power Pos. Push	Position	Dynamic	0.8	Locked	Disabled	38.9

- 6 high-fidelity recordings of live spoofing attacks
  - 20-MHz bandwidth
  - 16-bit quantization
  - Each recording ~7 min. long; ~40 GB
- Can be replayed into any GNSS receiver



The University of Texas Radionavigation Lab
and
National Instruments
jointly offer the **Texas Spoofing Test Battery**
Request: todd.humphreys@mail.utexas.edu

Observations on Defenses

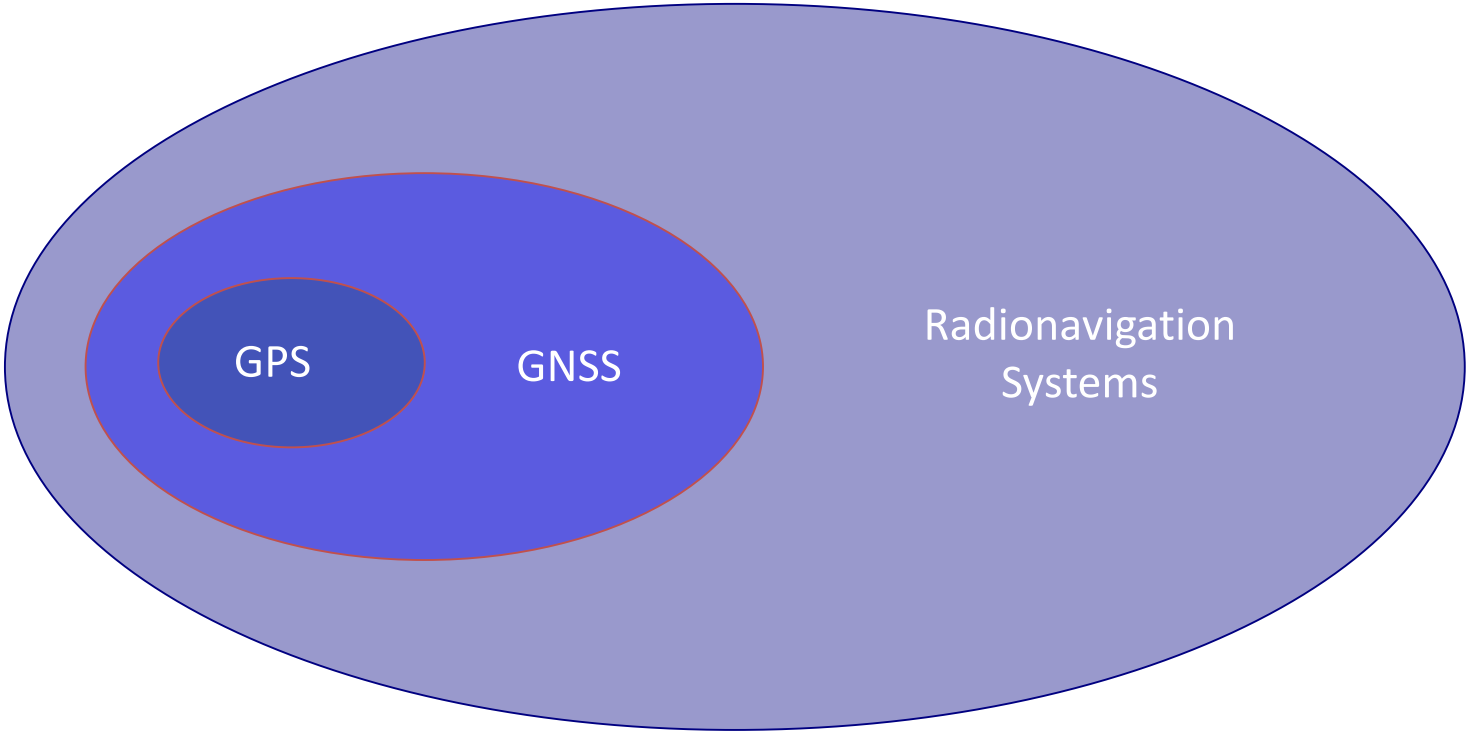
- Crypto defenses not a panacea: Ineffective against near-zero-delay meaconing (entire band record and playback) attacks.
- Non-crypto defenses not so elegant mathematically, but can be quite effective.
- Best shield: a coupled crypto-non-crypto defense.
- When implemented properly, navigation message authentication (NMA) authenticates not only the data message *but also the underlying signal. It is surprisingly effective.*

email: kyle.wesson@utexas.edu

web: http://radionavlab.ae.utexas.edu

THANK YOU

Radionavigation



GPS

GLONASS

Beidou

Galileo

GPS Errors & Accuracy

- Ephemeris errors in r^i: 2 m
- Transmitter clock errors: 2 m
- Residual Ionospheric delay: 4 m*
- Tropospheric delay: 0.5 m
- Multipath (reflected signals): 1 m#
- Receiver noise: 0.5 m
- Multiplicative effect of geometry (GDOP)
- <u>Typical accuracy: 10 m/axis, 30 nsec in time, 0.01 m/sec velocity</u>

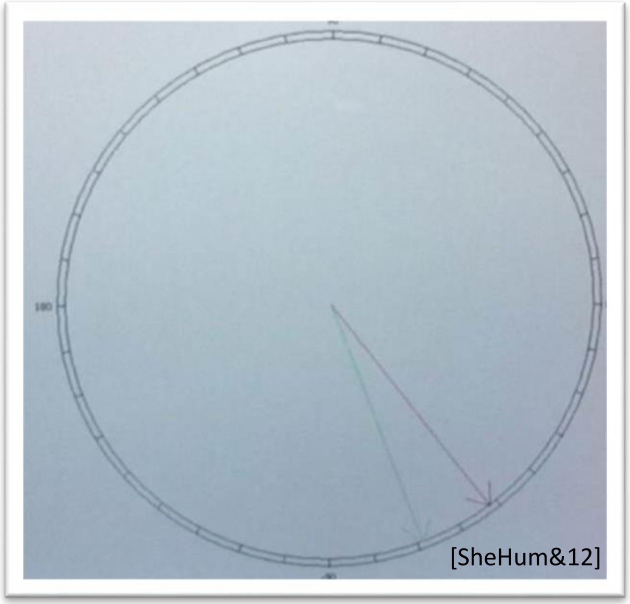
* for single-frequency receiver w/model corrections, error > 15 m possible in unusual ionospheric conditions, low elevation

\# error > 15 m possible in strong multipath environments


RADIONAVIGATION LABORATORY

Smart Grid Vulnerabilities

- Operational system in Mexico on the Chicoasen-Angostura transmission line
  - Automated PMU-based control
  - Connects large hydroelectric generators to large loads
  - Two 400-kV lines and a 115-kV line
- Large phase angle offsets (>10°) induced in minutes
  - Protects against generator instability during double fault by shutting down generators
- Spoofing attack can cause PMUs to violate IEEE C37.118 Standard



Observations on Defenses (1/3)

- Navigation signal authentication is hard. Nothing is foolproof. There are no guarantees. But simple measures can vastly decrease the *probability* of a successful attack. Probability is the language of anti-spoofing.
- Symmetric-key systems (e.g., SAASM) offer short time to authenticate but require key management and tamper-proof hardware: more costly, less convenient. SAASM and M-code will never be a solution for a wide swath of applications (e.g., civil aviation, low-cost location and time authentication).

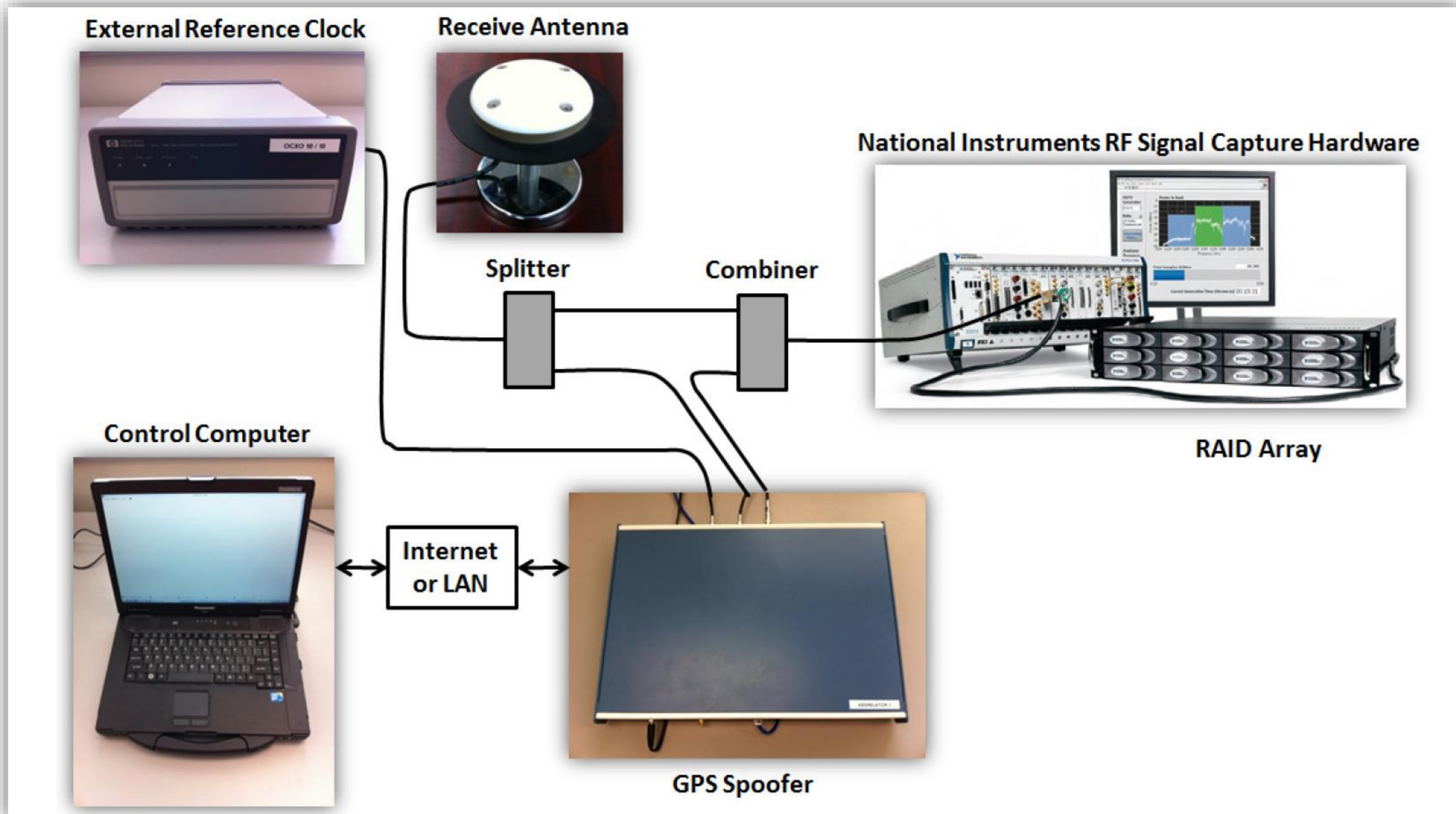
Observations on Defenses (2/3)

- Asymmetric-key (public-private key) systems have an unavoidable delay (e.g., 40 seconds between authentication of any signal) but delay can be accepted in many applications; also, for non-complicit spoofing there is no need to tamper-proof the receiver: cheaper, more convenient.
- Proof of location (proving to you where I am) is emerging as a vital security feature. It's not easy: non-crypto approaches require elaborate tamper proofing; crypto approaches require high-rate security code. Beware black-market vendors with high-gain antennas who will sell an authenticated location.

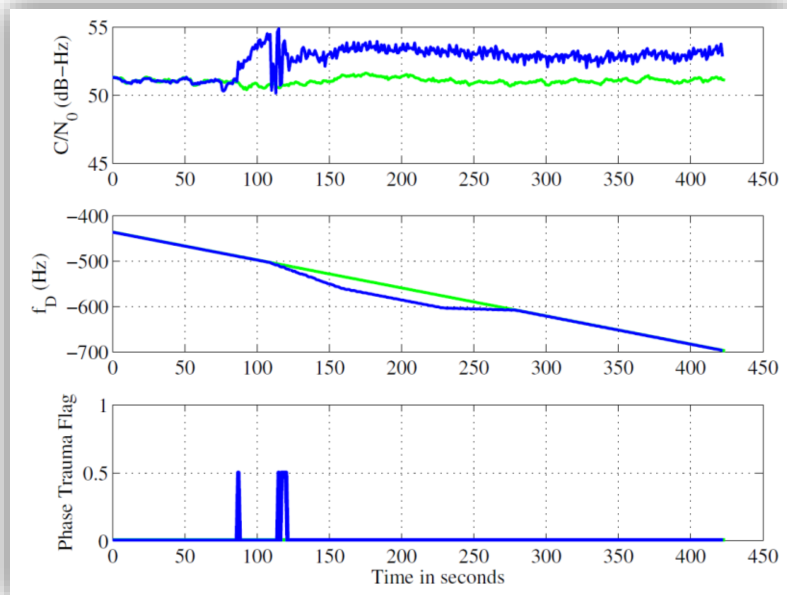
Observations on Defenses (3/3)

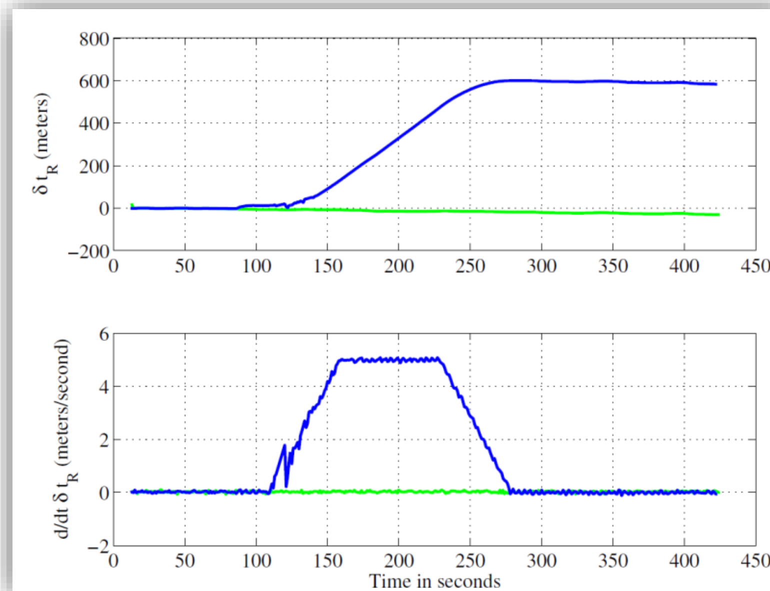
- Crypto defenses not a panacea: Ineffective against near-zero-delay meaconing (entire band record and playback) attacks.
- Non-crypto defenses not so elegant mathematically, but can be quite effective.
- Best shield: a coupled crypto-non-crypto defense.
- When implemented properly, navigation message authentication (NMA) authenticates not only the data message *but also the underlying signal. It is surprisingly effective.*

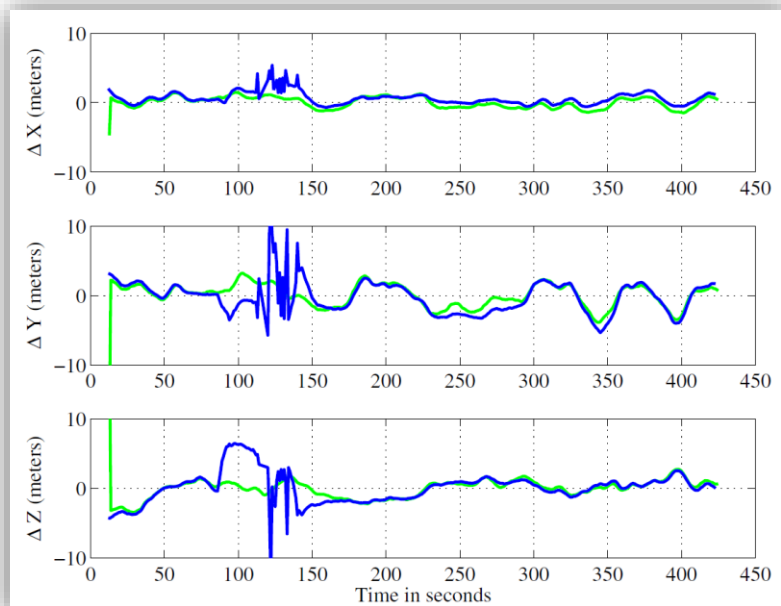
TEXBAT Recording Setup

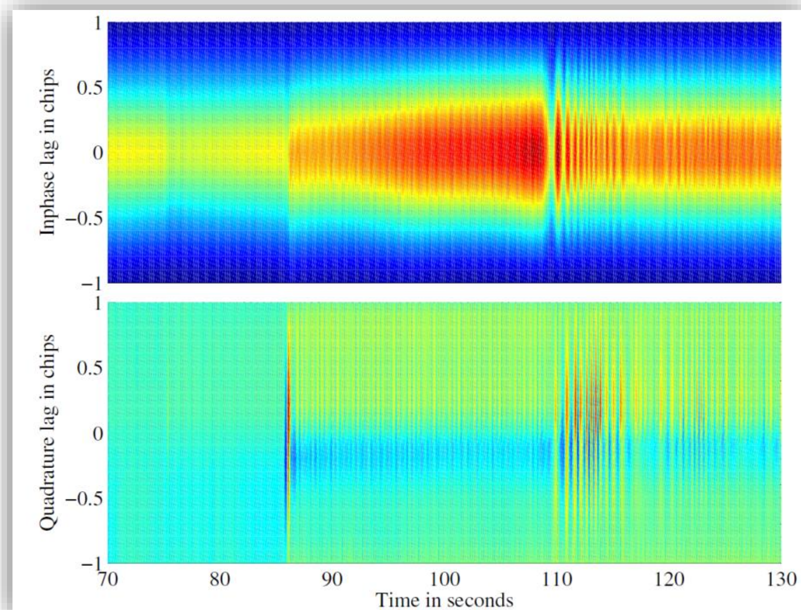


Scenario 2: Static Overpowered Time Push

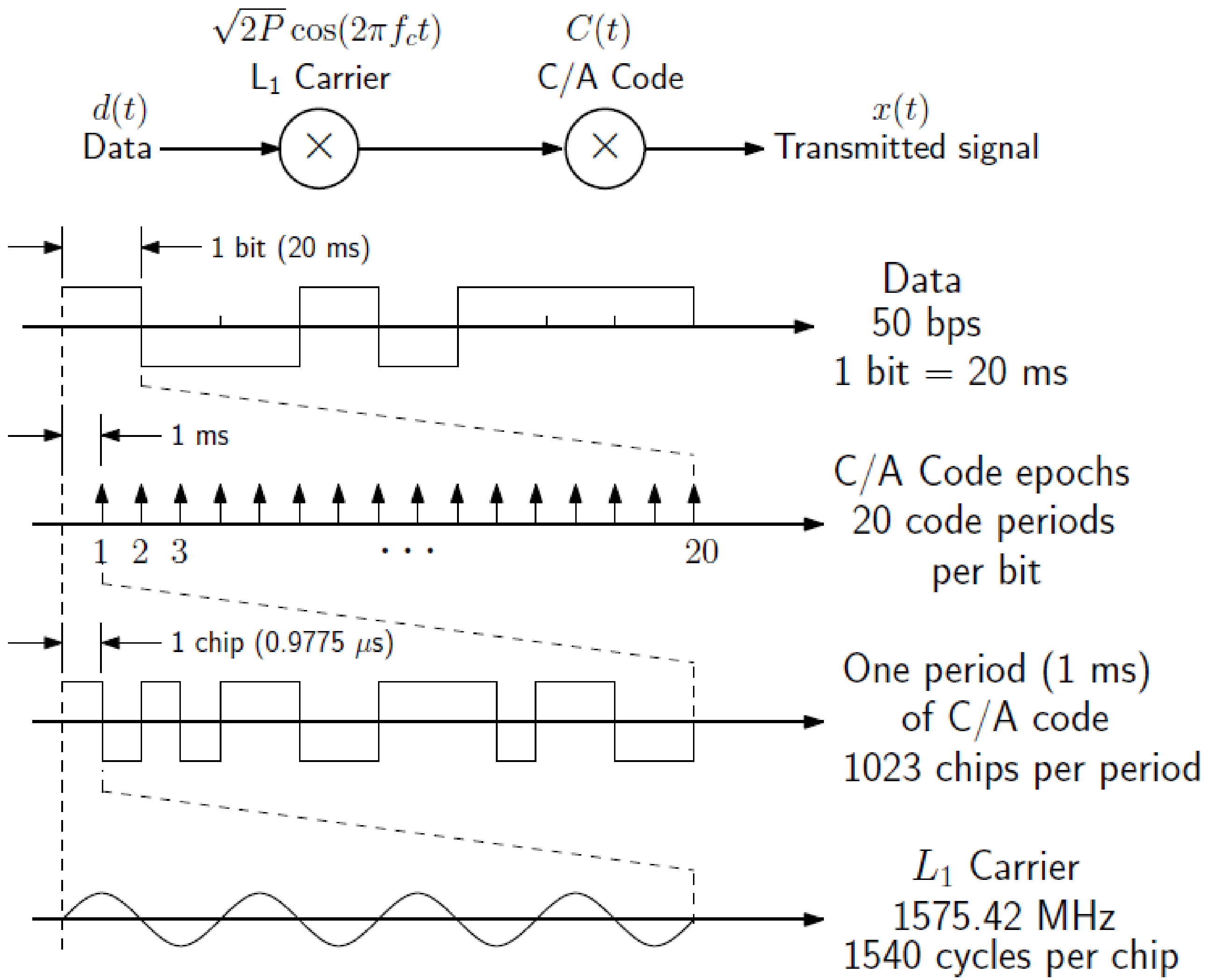








GNSS Signal Processing Basics



GNSS Signal Processing Basics

- GPS baseband signal model:

$$x(j) = A(\tau_j)d\left[\tau_j - t_d(\tau_j)\right]C\left[\tau_j - t_s(\tau_j)\right]\exp\left[i\,\theta(\tau_j)\right] + n(j)$$

- Apparent Doppler frequency shift:

$$f_D(\tau_j) = \frac{1}{2\pi}\frac{d\theta(\tau)}{d\tau}\bigg|_{\tau=\tau_j}$$

- Accumulation Model:

$$S_k = \sum_{j=j_k}^{j_k+N_k-1} x(j)\exp\left[-i\,\hat{\theta}(\tau_j)\right]C\left[\tau_j - \hat{t}_{s,k}\right]$$

GNSS Receiver Block Diagram