Techniques for Spoofing and for Spoofing Mitigation

Mark L. Psiaki

*Sibley School of Mechanical & Aerospace Engineering, Cornell University, Ithaca, NY, USA*
The Problem: Surreptitious Receiver Channel Capture & Consistent Drag-Off

- Received Signal
- Transmitted Spoofing Signal
- Correlation Function
  - Authentic
  - Spoofed

GPS Receiver/Spoof

Target GPS Receiver

Known

ENAC/SIGNAV Nov. ‘15
The Problem: Spoofer Field Tests & Alleged “In-the-Wild” Spy Drone Capture


Exclusive: Iran hijacked US drone, says Iranian engineer (CS Monitor 15 Dec 2011)

GPS Spoofing Experiment Knocks Ship off Course: University of Texas at Austin team repeats spoofing demonstration with a superyacht. (Inside GNSS 31 July 2013)
Presentation Outline

I. Potential spoofing attack strategies
II. Effective spoofing detection methods
III. Ranking of attack & detection “costs” and identification of appropriate detection methods for given attack strategies
IV. Re-acquisition of true signals & navigation capability after attack detection
V. Recommendations for COTS GNSS receiver spoofing defenses
Open-Loop Signal Simulator Attack

- Initially jam receiver to unlock tracking loops from true signals
- Generate consistent spoofer signals using GNSS signal simulator & broadcast overpowered versions
Receiver/Spoofer with Known Geometry Relative to Victim (as already shown)

Receiver tracking points
Total signal
Spoofer signal
Completed drag-off
Meaconing Attack

Meacon's small phased array of GPS receiver antennas

Meacon (i.e., replay-with-delay) signal processor w/independently steerable channel reception gain patterns, replay delays, & replay gains

Meacon/spoofer signal (has correct versions of all encryptions)
True-Signal Nulling Attack

- Total signal
- Nulling signal
- Spoofer signal
- Completed drag-off
- Cancellation of true & nulling signals

ENAC/SIGNAV Nov. '15
Multi-Transmitter Attack

Single-channel receiver/spoofers (possibly carried on air vehicles)

Spoofed signals of individual satellites with realistic direction-of-arrival diversity
Received Power Monitoring (RPM)

$\times 10^9$

**Power Spectral Density**

**Frequency Offset (MHz)**

- **Spoofed Signal**
- **Non-Spoofed Signal**
Jump in $[I;Q]$ Accumulation Phasor

Sudden $[I;Q]$ jump at onset of spoofing attack
Sudden Jump in Doppler Rate of Change

Onset of spoofing attack

Onset of drag-off (sudden 0.02 g increment in carrier acceleration/ Doppler rate)
Distortion of Complex Correlations

No apparent spoofed distortion in correlation magnitude vs. code offset

Telltale spoofer/true-signal interaction distortion: complex autocorrelation is non-planar
Encryption-Based Defenses

- Symmetric key encryption, e.g., GPS P(Y) & M codes
- Cross-correlation of unknown symmetric key codes between a secured reference receiver & a potential victim
- Navigation Message Authentication (NMA): digitally signed unpredictable navigation bits
- Spread Spectrum Security Code (SSSC): Short encrypted segments received, stored, & checked against a digitally signed key that is broadcast later
Spoofing Detection via Inter-Receiver Correlation of Unknown P(Y) Code

- GPS Satellite
- GEO “bent-pipe” transceiver
- Secure uplink of delayed, digitally-signed P(Y) features
- Broadcast segments of delayed, digitally-signed P(Y) features
- Secure antenna/receiver w/processing to estimate P(Y) features (or a single antenna or a distributed set of single-antennas)

UE with
- receiver for delayed, digitally-signed P(Y) features
- delayed processing to detect spoofing via P(Y) feature correlation
Semi-Codeless Spoofing Detection using Unknown P(Y) code Receiver Cross-Correlation

- Onset of spoofing attack
- Successful detection of spoofing when dashed green threshold crosses above solid blue detection statistic
- Build-up of significant spoofed C/A code-phase error
Drift-Based Defenses

- Monitor drift of computed receiver clock offset & compare with known oscillator stability
- Monitor nav. solution motion using an inertial measurement unit
- Declare a spoofing alert if either clock drift or nav. solution acceleration are physically unreasonable based on *a priori* knowledge or independent sensor data
DOA/Interferometric Methods, Non-Spoofed Case

Alternate system w/partial DOA determination:

Antenna A  Antenna B

\[ \hat{\rho}_j \]

\[ \hat{\rho}_{j-1} \]

\[ \hat{\rho}_{j+1} \]
DOA/Interferometric Methods, Spoofed Case

Single-transmit-antenna spoofer that sends false signals for GNSS satellites \(..., j-1, j, j+1, \ldots\)

\[ \hat{\rho}_{\text{to2antsys}}^{sp} \]

\[ \hat{\rho}_{\text{to4antsys}}^{sp} \]

Alternate system with full DOA determination:
Test of 2-Antenna Defense Against Live Spoofing Attack on White Rose of Drachs

- Receiver/spoofer signal processor amidships
- 2-antenna spoofing detector near bow
- Spoofer transmission antenna

Spoofer reception antenna at stern of yacht
Single-Differenced Carrier Phase Responses to Spoofing Attack against Dual-Antenna System

Initial Attack

Code Drag-Off

Fractional Part of $\Delta \phi_{BA}$ (cycles)

Receiver Clock Time (sec)
Complementary Detection Strategy Examples

- **Power/signal-distortion/drift**
  - Distortion less obvious w/high-power spoofer or rapid drag-off
  - Power & drift monitors constrain spoofer to allow recognizable signal distortion during a long drag-off phase

- **NMA/SCER-detection/clock-drift**
  - NMA forces Security Code Estimation & Replay attack
  - Clock drift monitoring constrains initial spoofed signal delays
  - Constrained delays force spoofer to fake early parts of NMA bits; faked initial bit portions are detectable

- **DOA/continual signal re-acquisition**
  - Re-acquisition finds multiple copies of same signal
  - DOA distinguishes true & spoofed versions of same signal
Relative “Cost” Ranking of Attack Strategies

- Meaconing, single RCVR ant, single TRANS ant
- Jammer/open-loop signal simulator
- RCVR/SPFR, 1 TRANS ant
- Meaconing, multi RCVR ants, 1 TRANS ant
- Nulling RCVR/SPFR, 1 TRANS ant
- RCVR/SPFR, multi TRANS ants
- Meaconing, multi RCVR ants, multi TRANS ant
- Nulling RCVR/SPFR, multi TRANS ants
Relative “Cost” Ranking of Detection Strategies

- Observables & received power monitoring (RPM)
- Correlation function distortion monitoring
- Drift monitoring (clock offset, IMU/position)
- Observables, RPM, distortion, & drift monitoring
- NMA or Delayed symmetric-key SSSC
- NMA, SCER detection, RPM, & drift monitoring
- Dual-RCVR keyless correlation of unknown SSSC codes
- Symmetric-key SSSC, e.g., P(Y) or equivalent
Ineffective Defense/Attack Paring Examples

- Pseudorange-based RAIM defense:
  - Ineffective against all reported attack strategies

- RPM & observables monitoring
  - Receiver/spoofer w/1 TRANS ant -- if designed carefully

- NMA (w/o or w/SCER detection), dual-receiver keyless correlation of unknown SSSC, or symmetric-key SSSC
  - Any type of meaconing

- Correlation function distortion monitoring
  - Any type of signal-nulling attack

- DOA-based methods
  - Methods using multiple spoofer transmission antennas
Effective Defense/Attack Paring Examples

- RPM w/monitoring of observables, drift, & correlation function distortion
  - Any spoofing method w/o signal nulling – if caught at onset
- DOA-based methods
  - All spoofing methods with a single transmission antenna
- NMA, dual-receiver keyless correlation of unknown SSSC, or symmetric-key SSSC
  - All non-meaconing/non-SCER spoofing methods
### Cost-Ranked GNSS Attack/Detection Matrix

**TABLE I: Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D2</td>
<td>~</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>X</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>D3</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D4</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D5</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D6</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D7</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D8</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D9</td>
<td>~</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D10</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D12</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>D13</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Attack Techniques Key**
- A1: Meaconing, single RX ant, single TX ant
- A2: Open-loop signal simulator
- A3: RX/SP, single TX ant, no SCER
- A4: RX/SP, single TX ant, SCER
- A5: Meaconing, multi. RX ants., single TX ant.
- A6: Nulling RX/SP, single TX ant, no SCER
- A7: Nulling RX/SP, single TX ant, SCER
- A8: RX/SP, single TX ant, sensing of victim ant. motion
- A9: RX/SP, multi. TX ants., no SCER
- A10: RX/SP, multi. TX ants., SCER
- A11: Meaconing, multi. RX ants., multi. TX ants.
- A12: Nulling RX/SP, multi. TX ants., no SCER
- A13: Nulling RX/SP, multi. TX ants., SCER

**Detection Techniques Key**
- D1: Pseudorange-based RAIM
- D2: Observables and RPM
- D3: Correlation function distortion monitoring
- D4: Drift monitoring (clock offset, IMU/position)
- D5: Observables, RPM, distortion, and drift monitoring
- D6: NMA
- D7: NMA* and SCER detection
- D8: Delayed symmetric-key SSSC*
- D9: NMA*, SCER detection, RPM, and drift monitoring
- D10: Multiple RX antennas
- D11: Moving RX antenna
- D12: Dual-RX keyless correlation of unknown SSSC codes
- D13: Symmetric-key SSSC* [e.g., P(Y) equiv.]
Navigation Recovery after Attack Detection

- Bulk of research to date concentrates on detection
- Need to go beyond “Warning: Spoofing Attack; GNSS navigation fix unreliable”, to “Authentic GNSS signals recovered; navigation fix reliable”
- Problem involves seeking, re-acquiring, & authenticating true signals
- Hampered by spoofer strength (acts as a jammer)
- Weak-signal techniques useable if spoofer transmits authentic navigation bits – enables very long coherent integration intervals for authentic signals
Authentic Signal Re-Acquisition “During” the White Rose of Drachs Libya Attack

Spoofed Signal, 0.94 sec Coherent Integration

True Signal, 0.94 sec Coherent Integration
Recommendations to COTS Receiver Mfg’s.

- Implement something beyond simple pseudorange-based RAIM detection methods
  - Apparently no COTS receivers defend against current threats
- Implement simplest detection methods first, ones that require mostly firmware upgrades
  - Monitoring of received power (needs AGC gain input if not available), observables anomalies, correlation function distortion, & clock drift.
- Implement stronger detection methods as time, money, & market/perceived threat allow or demand
  - Existing multi-antenna systems could implement DOA methods via firmware upgrades
- Constellations should add NMA or SSSC segs w/delayed keys
- Use hypothesis testing machinery in detection tests
- Enable re-acquisition of authentic signals/navigation capability