GNSS Spoof Detection to Protect Civilian Aviation

for the Stanford Symposium on Position Navigation and Time
November 3, 2016

by Prof. Per Enge with wonderful help from:
• FAA Navigation Directorate
• FAA Technical Center
• Dr. Yu-Hsuan Chen
• Dr. Sherman Lo
• Dr. Emily McMilen
• Dr. Eric Phelts
• Dr. Todd Walter
Spoofers

• Defcon is “the world’s longest running and largest underground hacking conference.”
  – How to spoof the sensors being considered for autonomous cars (camera, lidar, ultrasound & radar)
  – How to build a GPS spoofer

• Spoofing in Russia
  – Protect the Kremlin
  – Persuade UAVs that they are in a no-fly zone by spoofing to the airport
  – Nationwide protection against drones & cruise missiles

• Korea

• Catch any Pokémon from your couch
Requirements for Spoof Detection

We seek spoofing detection with the following properties:
• Twenty to 30 years of lifetime for civilian avionics
• Export for international use
• Easily installed (same hole pattern & cable run)
• Extremely low false alarm rate. Selective against
  • scintillation
  • radio frequency interference
  • banking
## Outline

<table>
<thead>
<tr>
<th>Topic</th>
<th># of slides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>5</td>
</tr>
<tr>
<td>• Mono-pipe</td>
<td></td>
</tr>
<tr>
<td>• Multi-pipe</td>
<td></td>
</tr>
<tr>
<td>Transient Tells</td>
<td>4</td>
</tr>
<tr>
<td>Acceleration as a Signature</td>
<td>7</td>
</tr>
<tr>
<td>Polarization as a Signature</td>
<td>3</td>
</tr>
<tr>
<td>Go Forward Plan</td>
<td>1</td>
</tr>
</tbody>
</table>
Mono-Pipe, On-Horizon Spoofing Attack With Signature Stripping

Separate SV signals
- beam steering
- frequency domain

Victim simulation operating on live SV signals

SV 1: Delay & Doppler

SV k: Delay & Doppler
Multi-Pipe Above-Horizon Attack (Stereo Attack From UAVs)

Bad Actor
- attack scenario
- compute pseudo-ranges

Complicated attack! Eventually obviated by multi-constellation receivers
GNSS on Orbit

Year

Number of SVs


0  5  10  15  20  25  30

GPS

GLONASS

Galileo

Beidou IGSO
Beidou MEO
Beidou GEO
# Outline

<table>
<thead>
<tr>
<th>Topic</th>
<th># of slides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>5</td>
</tr>
<tr>
<td>Transient Tells</td>
<td>4</td>
</tr>
<tr>
<td>• C/N₀ &amp; AGC</td>
<td></td>
</tr>
<tr>
<td>• Correlation Peak</td>
<td></td>
</tr>
<tr>
<td>Acceleration as a Signature</td>
<td>7</td>
</tr>
<tr>
<td>Polarization as a Signature</td>
<td>3</td>
</tr>
<tr>
<td>Go Forward Plan</td>
<td>1</td>
</tr>
</tbody>
</table>
Transient “Tell”
Due to Interference of the Radio Waves

Victim simulation operating on live SV signals

SV 1: Delay & Doppler

SV k: Delay & Doppler

Separate SV signals
• beam steering
• frequency domain

Due to Interference of the Radio Waves

November 7, 2016
Stanford University
Amplitude Signature Appears in AGC & C/N₀
Phase Difference Introduces a Tell in the Correlation Peak

Above described signatures are transient. They are also sensitive, but not selective.
## Outline

<table>
<thead>
<tr>
<th>Topic</th>
<th># of slides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>5</td>
</tr>
<tr>
<td>Transient Tells</td>
<td>4</td>
</tr>
<tr>
<td><strong>Acceleration as a Signature</strong></td>
<td>7</td>
</tr>
<tr>
<td>Polarization as a Signature</td>
<td>3</td>
</tr>
<tr>
<td>Go Forward Plan</td>
<td>1</td>
</tr>
</tbody>
</table>
Acceleration Signatures Recorded During Flight Trials with FAATC in August of 2016
GPS Altitude for 72 Minutes of Flight

Approach 1:
Hr 2.24-2.3

Approach 2:
Hr 2.5-2.53

Approach 3:
Hr 2.78-2.825

Approach 4:
Hr 2.98-3.03

approx. 72 minutes

approx. 2000 m
GNSS Acceleration (red) & Accelerometer (blue) During Approach 1

Z Acceleration (no pitch corr) from Accel & PPP GPS on 08/24/16

2.254 Turn
0.05 g or 0.5 m/s²

approx. 4 minutes

Acceleration is appealing, because a bad actor cannot readily measure acceleration without latency.
GNSS Acceleration (red) & Accelerometer (blue) During Approach 2

Z Acceleration (no pitch corr) from Accel & PPP GPS on 08/24/16

- 0.05 g or 0.5 m/s²
- -0.05 g or -0.5 m/s²

approx. 2 minutes

Time since start (hr); Start 24-Aug-2016 06:51:47
GNSS Acceleration (red) & Accelerometer (blue) During Approach 3

Z Acceleration (no pitch corr) from Accel & PPP GPS on 08/24/16

0.05 g or 0.5 m/s²

-0.05 g or -0.5 m/s²

approx. 3 minutes

Time since start (hr); Start 24-Aug-2016 06:51:47

11/7/16
GNSS Acceleration (red) & Accelerometer (blue) During Approach 4

Z Acceleration (no pitch corr) from Accel & PPP GPS on 08/24/16

-0.05 g or -0.5 m/s²

0.05 g or 0.5 m/s²

approx. 3 minutes

Take Off

On Ground

Time since start (hr); Start 24-Aug-2016 06:51:47

11/7/16
Vertical Acceleration Errors

C/N₀ (dB–Hz)

<table>
<thead>
<tr>
<th>C/N₀ (dB–Hz)</th>
<th>Acceleration Error (m/s²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>0.100</td>
</tr>
<tr>
<td>35</td>
<td>0.050</td>
</tr>
<tr>
<td>40</td>
<td>0.005</td>
</tr>
<tr>
<td>45</td>
<td>0.001</td>
</tr>
<tr>
<td>50</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Body Frame Attitude Shake (degrees)

Smart Phones, 2015
STMicro & Invensense
GNSS Receiver, 2015

NXP & Fairchild

Automotive, 2015

BW_PLL = 5 Hz, Tₛ = 0.4 s, T_coh = 20 ms
BW_PLL = 10 Hz, Tₛ = 0.4 s, T_coh = 20 ms

11/7/16
## Outline

<table>
<thead>
<tr>
<th>Topic</th>
<th># of slides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>5</td>
</tr>
<tr>
<td>Transient Tells</td>
<td>4</td>
</tr>
<tr>
<td>Acceleration as a Signature</td>
<td>7</td>
</tr>
<tr>
<td>Polarization as a Signature</td>
<td>3</td>
</tr>
<tr>
<td>Go Forward Plan</td>
<td>1</td>
</tr>
</tbody>
</table>
Emily’s Antenna
(Yu-Hsuan’s Version)
XPD Polarization Test for Spoofing

XPD (Cross Polarization Discrimination) is antenna gain difference between RHCP and LHCP.
## Cross Polarization Discrimination

### Summary of Three Measurements on Skyline Boulevard in September of 2016

<table>
<thead>
<tr>
<th>Elevation (Deg)</th>
<th>XPD (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>35~90</td>
<td>10~20</td>
</tr>
<tr>
<td>15~35</td>
<td>5~10</td>
</tr>
<tr>
<td>&lt;15</td>
<td>~0</td>
</tr>
</tbody>
</table>

![Diagram showing XPD values]

**XPD ≈ 20dB**

**XPD ≈ 0dB**
Go-Forward Plan
Backup Slides
GNSS for Highly Automated Automobiles
# New Constellations & Frequencies

<table>
<thead>
<tr>
<th>Frequency (MHz)</th>
<th>1200</th>
<th>1300</th>
<th>1400</th>
<th>1500</th>
<th>1600</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeiDou B5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BeiDou B6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Galileo E5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Galileo E6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GLONASS G5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS L2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GLONASS G2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS L1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GLONASS G1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Go Forward Plan

1) Test the individual spoof detection elements
   a) Constructive/destructive interference
   b) Acceleration signatures
   c) Polarization signatures

2) Determine the domain for each candidate element
   a) Prob(missed detection) against threat model
   b) Prob(false alarm) against nominal background
   c) Protection level
   d) Cost

3) Design a synthesis of the above

4) Build a safe test scenario (Camp Roberts or End Station III or White Sands or a combination??)

5) Tests on a car! (when?)