Assured GNSS

Attacks and Countermeasures

Stefan Söderholm

23 October 2023
Outline

Septentrio

Spoofing

Test campaign

Jamming
In Septentrio

RELIABLE & ACCURATE
GPS/GNSS POSITIONING

APPLICATION KNOW HOW

YOUR OEM PARTNER

Assured PNT is key for our customers

Experts in Localization technology

@ Interleuvenlaan Heverlee

Autonomous Vehicles
Marine
Construction & Mining
UAV
Reference Networks

Accuracy + Reliability + Availability + Security

Modules
Boards
Housed receivers
Smart antenna
Scientific Receivers
Jamming
Jamming

• Jamming, to jam = “squeeze or pack tightly into a specified space”
• Jamming is always malicious and intentional
• The interfering signal does not contain any information
• Cause GNSS receivers to stop working or suffer in performance by adding an interfering signal to the GNSS frequency band that saturates the radio frontend.

• Jammers is often referred to as PPD’s (Personal Privacy Devices)
• Especially in US it was considered OK to protect your own privacy by blocking any GPS receiver your employee might have installed in your car.
Chirp Jammers

- Sinewave with Changing Frequency
- Wipes out GPS band(s)

- 10 mW over ~20 MHz => 63 dBm/Hz
  Noise Floor: -172 dBm/Hz

Voltage Controlled Oscillator (VCO)

Low Frequency Oscillator 555-timer

100 mW

Range: 2.5 km

10-100 MHz

8-40 µs
Jamming Mitigation: Concept

- General Concept:
  - GPS normally dominated by thermal noise
  - And GPS signals also look like noise

→ So, remove anything which doesn't look like noise
Mitigation Techniques: Chirp Jammers

- Method 1: **Mimick the signal**, and subtract
  - Parameter estimation: frequency-range, chirp-rate, phase
  - Problem: can't deal well with reflections

- Method 2: **FFT** – set peaks to zero - **IFFT**
  - = **FDAF**: Frequency Domain Adaptive Filter
Military Grade Anti-Jamming: Beam Forming

- Random Noise at Main Lobes
  - Structure cannot be exploited
- Exploit Geometry
- Multiple Antenna Elements

Typically uses 4 to 7 antenna elements

CRPA: Controlled Radiation Pattern Antenna

Deduced from cross-correlation A1 and A2 signal

\[ \text{Rest of the Receiver} \]

\[ \text{GPS.(1-exp(2.\pi.j.D/\lambda)) + (Noise-Noise)} \]

\[ \text{exp(2.\pi.j.D/\lambda)} \]

\[ \text{Noise.exp(-2.\pi.j.D/\lambda)} \]
Spoofing
Spoofing

• Spoofing, to spoof = “imitate something, hoax or trick someone”
• Spoofing is always malicious and intentional.
• The interfering signal tries to generate and transmit false GNSS signals.
• Fool a receiver to think it is at different position than it really is.

Pizza Time!
A spoofer need to:

- Generate **true GNSS signals** including data, modulation and timing.
- Maintain **time synchronization** close to true GNSS time.
- Adapt the **signal power levels** to match those of the true signals.
Detection of Spoofing

- Detect excessive power
  - But can also come from high-gain antenna...
- Detect correlation profile deformation
  - But can also come from multipath...
- Detect divergence
  - But can also come from ionospheric scintillation...
- Detect wrong angle-of-arrival (2 antenna-receivers)
  - But can be reflection....
- Navigation data authentication
Code-Carrier Divergence

- Both Represent Range → Equal
- Only Slow Divergence Expected
  - Ionosphere, Phase Wind Up
- Most SDR:s → Huge Code-carrier Divergence
Wrong Angle of arrival

- A spoofer transmits all signals from the same location => Same angle of arrival
- Satellite signals arrive from different angles
- Spoofed measurement from two antennas will not match

Single Difference Phase
GALILEO Open Service Navigation Message Authentication

- First Cryptographic Service
- Now running on MOSAIC module

Accurate: Authentication wrong → Spoofing!
Coherent Attack Protection

Latency: 30 seconds
NTP-Dependency

Spoofing detected (Galileo OSNMA)
Test Campaign
The Norway Jamming/Spoofing test

- **Organizers:** Norwegian Governmental Organizations, coordination via Testnor

- **When:** September 18th till the 20th 2023

- **Where:** Andøya, Norway

- **Who attended:** 300 participants from various industries
Attack Type: Non-Coherent Attack

- Introduce *jump* of position or time
- Use jamming to *obfuscate* attack

Receiver acquires on higher peak
Chirp Jammer: WIMU in Action

Receiver 1: WIMU Off → L1 mostly gone

Receiver 2: WIMU On → L1 is back!
Response to Multi-frequency Chirp Jammer Attack

WIMU Disabled

Receiver: Mosaic-mini
Dual antenna config
Hi-Target antenna

WIMU Enabled

Receiver: Mosaic-mini
Single antenna config
Hi-Target antenna

WIMU Enabled + low-elev lock-out antenna

Receiver: Mosaic-T
Single antenna config
AJ977XF antenna
OSNMA and Atomichron

Position affected with only OSNMA

GPS Spoofing

Galileo Spoofing
Did we detect the spoofing?

Undetected spoofing epochs with an error > 10m

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Total (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitor 1</td>
<td>67%</td>
</tr>
<tr>
<td>Competitor 2</td>
<td>45%</td>
</tr>
<tr>
<td>Competitor 3</td>
<td>26%</td>
</tr>
<tr>
<td>Septentrio</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

Spoofing flag captures the big outliers!

Spoofing flags is set for all big outliers!
EMEA (HQ)
Greenhill Campus
Interleuvenlaan 15i,
3001 Leuven, Belgium

Americas
Los Angeles, USA

Asia-Pacific
Melbourne, Australia
Shanghai, China
Yokohama, Japan

septentrio.com
sales@septentrio.com