Resilient and Robust PNT

Todd Humphreys
With input from Peter Iannucci, Matthew Murrian, and Lakshay Narula
The University of Texas at Austin Radionavigation Lab

JNC Tutorial | August 24, 2021
All material in this presentation is drawn from the open literature. References are provided within and at the end of the presentation.
Fortunately

by REMY CHARLIP

unfortunately
4 billion GNSS devices in use globally

Core global revenue due to GNSS: $76B

Enabled global revenue due to GNSS: $278B

Economic cost to UK of 5-day GNSS outage: $7.2B

“Economic Impact on the UK of a disruption to GNSS,” London Economics, 2017
“Economic Impact on the UK of a disruption to GNSS,” London Economics, 2017
Q: Will GNSS remain the pre-eminent worldwide source for positioning, navigation, and timing (PNT)?
A: Unfortunately, serious GNSS vulnerabilities need addressing; these may be unfixable.
Two schools of thought:
(1) Fix GNSS
(2) Seek stand-alone alternative sources of PNT
“Needed: About 35 dB of additional receiver interference resistance.”

“... we’re looking beyond GPS ... we need to find alternatives for military use that are more resilient and less vulnerable.”

Former Sec. Defense Ash Carter giving Drell Lecture at Stanford in 2015
GNSS Jamming

Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.
1 kW wideband jammer can deny service to the best COTS GNSS receivers over a ~200 km (line-of-sight) effective range
PTA: By (1) deep coupling with inertial sensors, and (2) multi-element antennas we can toughen GNSS receivers enough to withstand 1 kW wideband Gaussian jammer at a distance of 2 km.
Deploying full combination of best current technology could shrink effective range to 2 km. Moreover, the jammer itself becomes a counterstrike target.
But cost asymmetry favors the jammer:

1 kW jammer cost: ~$200

Cost for enough jammers to deny service in 200-km-radius zone: ~$2 M
But cost asymmetry favors the jammer:
1 kW jammer cost: ~$200
Cost for enough jammers to deny service in 200-km-radius zone: ~$2 M
Jamming power now remains constant with altitude
What is more, immunity to $J/S = 84$ dB jamming environment almost certainly requires warm start for encrypted (non-repeating) wideband codes such as M-code: side channel must provide approximate time and location.
A coded jammer (or meacon) is more potent than uncorrelated wideband jammer: Each coded signal produces a correlation peak competitor that must be distinguished from authentic peak.

“Coded” jammer uses authentic spreading codes.

<p>| | | | | | | | | | | | | |</p>
<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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19u</td>
<td>-29228.2</td>
<td>-0.0</td>
<td>0.0</td>
<td>39.3</td>
<td>359.4</td>
<td>-75.1</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>5u</td>
<td>-29228.2</td>
<td>-0.0</td>
<td>0.0</td>
<td>40.2</td>
<td>54.9</td>
<td>-38.4</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>12u</td>
<td>-29228.7</td>
<td>-0.0</td>
<td>0.0</td>
<td>41.3</td>
<td>107.6</td>
<td>-47.8</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>17u</td>
<td>-29226.3</td>
<td>-0.0</td>
<td>0.0</td>
<td>42.9</td>
<td>341.0</td>
<td>-59.1</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2u</td>
<td>-29227.7</td>
<td>-0.0</td>
<td>0.0</td>
<td>42.5</td>
<td>112.4</td>
<td>-58.6</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1u</td>
<td>-29226.9</td>
<td>-0.0</td>
<td>0.0</td>
<td>40.2</td>
<td>281.5</td>
<td>-17.5</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>-31420.0</td>
<td>-2097925.9</td>
<td>23905339.5</td>
<td>42.1</td>
<td>196.6</td>
<td>-4.0</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>-40379.6</td>
<td>2650169.5</td>
<td>2128591.2</td>
<td>35.6</td>
<td>230.0</td>
<td>18.3</td>
<td>5*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>18</td>
<td>-25577.3</td>
<td>1688476.6</td>
<td>17415104.7</td>
<td>38.9</td>
<td>227.7</td>
<td>79.1</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>22</td>
<td>-34506.5</td>
<td>2316331.2</td>
<td>24880641.3</td>
<td>27.3</td>
<td>313.7</td>
<td>-15.2</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>-16254.9</td>
<td>811922.4</td>
<td>24880641.3</td>
<td>27.3</td>
<td>313.7</td>
<td>-15.2</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>8</td>
<td>-10484.9</td>
<td>76068.5</td>
<td>20159639.2</td>
<td>32.0</td>
<td>311.3</td>
<td>29.4</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>-7468.0</td>
<td>328301.5</td>
<td>17415104.7</td>
<td>38.9</td>
<td>227.7</td>
<td>79.1</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Upshot: even 35 dB of additional interference resistance (expensive!) would not prevent a determined adversary from cost-effectively denying GNSS over an area the size of Colorado.
The “fortunately, unfortunately” game can be played with distributed jamming technology: the defender can use the jamming sources as beacons in a “Signal of Opportunity from Interference (SOI) Simultaneous Localization and Mapping (SLAM)” framework.
Q: Could directed energy weapons damage GNSS satellites?
Directed energy: current technology could jam but not damage. Recently-completed Chinese FAST radio telescope is largest in world: 300-meter diameter steerable aperture. If used to focus energy of a massive 466 MW magnetron, power flux at MEO would be only 20 Watts per square meter, less than 1/50 of solar irradiance.
Directed energy: *future technology* (e.g., space lasers) could damage GNSS satellites
“[An influential view within China] is that this next phase [of warfare] will be characterized by combining manipulations of “Big Data” and increasing autonomy/artificial intelligence, with directed energy weapons at the core.”

Q: Could direct-ascent kinetic ASAT weapons destroy GNSS satellites?
May 2013: Chinese launched experimental direct-ascent ASAT weapon that reached beyond GPS orbit.

Direct-ascent ASAT could destroy individual satellites, but it would be impractical to take out full GPS constellation.
GNSS SPOOFING

Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops.
GPS Spoofer
GPS Spoofer
GPS Spoofer
GPS Spoofer
Q: Is the GNSS spoofing vulnerability only theoretical, or has it been proven by experiment?
Building the first publicly-acknowledged GPS spoofer, 2008

First target: personal iPhone
Could false GNSS signals cause UAV to believe it’s at the spoofer-simulated location, allowing full 3D hostile control of UAV?
$60k Hornet Mini’s navigation system sensors: civil GNSS + baro + IMU + magnetometer
White Rose of Drachs: 65-meter, $80M research laboratory in the Mediterranean
Datum: W84
N 38°02.0768
E 22°48.1772
Local time: Saturday 29
June 2013
Altitude: -415.3m (3D)
Variation: 3.3° E
COG 126°
SOG 15.1Kn
14:34:09
How Vulnerable is G.P.S.?

An engineering professor has proved—and exploited—its vulnerabilities.

By Greg Milner
August 6, 2020

Profile of UT Radionavigation Lab’s research in GNSS vulnerabilities over past decade: The New Yorker, August 2020.
Q: Are GNSS vulnerabilities being exploited in the wild, or are they only laboratory phenomena?
C4ADS “Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria.”
Capable turnkey GNSS spoofer can now be purchased for less than $300
Q: Can LEO SVs be used for global GNSS interference monitoring?
A flexible, science-grade GNSS receiver in low-earth orbit (LEO) would enable continuous global monitoring and characterization of GNSS interference.
February 2017: FOTON SDR installed on International Space Station
Science mission: Ionospheric sensing via radio occultation and airglow meas.
Collaborators: Naval Research Lab, Cornell, University of Texas, Aerospace Corp.
Software-defined radio is a key asset for agile and assured PNT. The University of Texas GRID receiver is the result of 14 years of development.
Q: Is Black Sea spoofing detectable in raw IF data captured on the ISS?
March-May 2018: Raw IF samples captured near Black Sea on 3 separate days
60-second recordings sent via NASA’s communications backbone to NRL and thence to UT for processing with latest version of GRID
250 kHz rounded prominence at L1 waxes and wanes with an approximately 5 sec. period.
The Syrian interference source employs coded jamming. Its purpose appears to be denial of GPS service, but it achieves this by spoofing each of the GPS L1 C/A PRN codes (albeit without LNAV modulation).
Data-Wiped 100-Hz IQ accumulations

False signal

Authentic signal in interference

Authentic signal under clean conditions

Unexplained fading
Doppler time history for false PRN 10 signal from day 144 capture

Doppler model nonlinearly related to transmitter position, but also strongly affected by transmitter clock error rate.

\[ f_D = -\hat{r}^T \nu_R / \lambda - c \left[ \delta t_R - \delta t_T \left( 1 - \delta t_R \right) \right] / \lambda + w \]
Doppler time history for false PRN 10 signal from day 144 capture

Marginal contribution of TX frequency instability to a single-pass geolocation error ellipse semi major (a) and semi minor (b) axes

<table>
<thead>
<tr>
<th>Clock Quality</th>
<th>$h_{-2}$</th>
<th>$a$ (m)</th>
<th>$b$ (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCXO</td>
<td>$3 \times 10^{-21}$</td>
<td>6900</td>
<td>690</td>
</tr>
<tr>
<td>Low-quality OCXO</td>
<td>$3 \times 10^{-23}$</td>
<td>720</td>
<td>72</td>
</tr>
<tr>
<td>OCXO</td>
<td>$3 \times 10^{-25}$</td>
<td>67</td>
<td>7.4</td>
</tr>
</tbody>
</table>
Doppler time history for false PRN 10 signal from day 144 capture

Post-fit residuals of Doppler time history assuming estimated transmitter location and clock rate offset
Analysis of the estimated clock frequency rate for days 74 and 144 revealed an Allan deviation consistent with an OCXO.

Post-fit residuals of Doppler time history assuming estimated transmitter location and clock rate offset.

\[ \sigma_y(2, \tau, \tau) = 1.6 \times 10^{-11} \]
Khmeimim Air Base, Syria

35.4099 N, 35.9431 E
April 2018: “[Syria is] the most aggressive electronic warfare environment on the planet.”

Gen. Raymond Thomas, commander
U.S. Special Operations Command
Interference from Syria is also evident in the carrier-to-noise-ratio observables continuously produced by the GRID receiver under normal operation.
To maximize detectability, CINR observations must be pre-processed to compensate for predictable variations due to PRN ($j$), frequency ($f$), range ($r_{sr}$), satellite off-boresight angle ($z_s$), and receiver off-boresight angle ($z_r$).
Model-compensated receiver-reported CINR as ISS overflies interference zones
Heat map based on standard 1-Hz L1 C/N0 data from ISS GRID receiver from March 2017 to June 2020. The interference source in Syria is clearly evident, with a pattern asymmetry due to the receiver’s antenna pointing aft. A second source near Libya is also evident.
Heat map based on standard 1-Hz L2 C/N0 data from ISS GRID receiver from March 2017 to June 2020. Interference from Syria is evident, as is a persistent signature in mainland China at approximately 32 N, 114 E.

Q: How does one calculate the effect of a given interference waveform on an GNSS receiver?
Received signal is a mixture of signal, interference, and noise

\[ r(t) = r_s(t) + r_I(t) + n(t) \]

\[ P_T = P_S + P_I + P_n \]
Received signal is multiplied by a local replica and accumulated. In the frequency domain, the interference component of $Y(t)$ is a convolution of the psds of the desired code, the interference signal, and a delta fcn at the Doppler estimate estimate.
psd of desired signal’s spreading code

psd of interference signal

psd of $I(t)$, the interference component of $Y(t)$

$I_0$ is what makes it through into the receiver’s tracking loops
CINR_i = \frac{P_i}{N_0 + M_{0i} + I_0}

I_0 := \int_{-\frac{W_{FE}}{2}}^{\frac{W_{FE}}{2}} S_{r_I}(f) S_{C_l}(f) \, df

M_{0i} = \frac{2T_C}{3} \sum_{j \in \mathcal{I}(t) \setminus i} P_{A,j}
Q: What waveform is most potent for jamming? In other words, for a fixed interference power $P_I$ what $S_{r_I}$ maximizes $I_0$?

\[ I_0 := \int_{-W_{FE}/2}^{W_{FE}/2} S_{r_I}(f) S_{C_l}(f) \, df \]
A: A pure tone jammer aligned with the highest point on the desired signal’s psd:

\[ S_{r_I} = P_I \delta(\hat{f}_D) \]

\[ I_0 := \int_{-W_{FE}/2}^{W_{FE}/2} S_{r_I}(f) S_{C_I}(f) \, df \]

\[ CINR_i = \frac{P_i}{N_0 + M_{0i} + I_0} \]
Q: Then why isn’t the jammer in Syria using this most potent waveform?
Q: Then why isn’t the jammer in Syria using this most potent waveform?

A: It’s too easy to defeat: a simple notch filter will do the trick.
To be both power-efficient and effective (hard to reject), the jamming signal has to produce high $I_0$ but avoid being sparse in some domain (e.g., time, frequency, code space, direction of arrival). A continuous matched-spectrum signal coming from multiple directions is both power-efficient and non-sparse (difficult to excise).
It takes very little interference power to present a cold-starting receiver with a conundrum: which peak does it choose?
Against civil receivers performing cold start, spoofing is more efficient for denial of service than jamming: a 1W spoofer is more potent than a 1kW matched-spectrum jammer at the same stand-off distance.

\[
\frac{P_I}{C} = - \left[ \eta + 10 \log_{10} \left( \frac{2T_C}{3} \right) \right]
\]

For a typical CINR acquisition threshold of \( \eta = 30 \text{ dB-Hz} \), the received jamming-to-signal power ratio must be 31.8 dB to deny service. For DOS via spoofing it need only be 0 dB.
Q: What desired-signal spreading code is most effective for resisting interference? In other words, what $S_{Cl}$ minimizes $I_0$?

$$I_0 := \int_{-W_{FE}/2}^{W_{FE}/2} S_{rI}(f) S_{Cl}(f) \, df$$
A: The wider the better. M-Code BOC(10,5) is an excellent example.
Q: How do we build a resilient PNT box?
Q: First, how do we authenticate GNSS signals?
There are many spoofing detection and mitigation techniques. None is perfect. The practical objective is to price your adversary out of the game.

Q: Next, how do we prevent denial of PNT?
PTA: By (1) deep coupling with inertial sensors, and (2) multi-element antennas we can toughen GNSS receivers enough to withstand 1 kW wideband Gaussian jammer at a distance of 2 km.
Robust, precise, high-integrity PNT for self-driving cars
University of Texas Sensorium
Emphasis on high-integrity PNT: Precise dual-antenna GNSS, three radar units, stereo cameras, inertial sensing, stable internal clock, LTE comms.
Ground Truth:

Forward-backward smoothed solution from iXblue ATLANS-C connected to the test antenna

The ATLANS-C “smartly” couples a tactical-grade IMU with a Septentrio RTK receiver

1-sigma reported uncertainty ranged from 2cm to 20cm
CDGNSS (when available), vehicle dynamics, and radar are fused to constrain drift of IMU.
Must determine vehicle’s center of rotation in order to apply zero-sideslip constraint
Must model and calibrate radar sensors
Periodic 5-minute GNSS outages: High-end MEMS IMU drifts up to 2km
Now with vehicle motion model constraints (zero sideslip, ZUPD). High-end MEMS IMU drifts less than 40 meters.
Additionally with radar range rate constraints (no prior map). High-end MEMS IMU drifts less than 20 meters.
Further constrain with a prior radar map
A prior radar map enables 60-minute GNSS-denied vehicle positioning to better than 0.5 meters.


THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY