GNSS Radio Frequency Interference Detection from Low Earth Orbit

Matthew J. Murrian, Lakshay Narula, Peter Iannucci, and Todd E. Humphreys
Department of Aerospace Engineering and Engineering Mechanics
The University of Texas at Austin
INC 2019, Edinburgh | November 19, 2019
Northern Norway: October 2018
A flexible, science-grade GNSS receiver in low-earth orbit (LEO) would enable continuous global monitoring and characterization of GNSS interference.
Q: What interference EIRP could be detected?

Q: What would be the rate of detection?

Q: How accurately could source be geolocated?
A hypothesis test for interference can be formulated in terms of a common decrease in CINR measurements due to an increase in $I_0$.

Received Power could also be used in place of CINR: no tracking required.
Performance of the interference detection test is completely characterized by the normalized distance between the means of the detection statistic $l(z)$ under $H_0$ and $H_1$. 

$$d \triangleq \frac{E[l|H_0] - E[l|H_1]}{\sqrt{\text{Var}(l|H_0)}} = \delta \sqrt{1^T P^{-1} 1}$$
Detection Sensitivity

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>Minimum Detectable EIRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>C/N0</td>
<td>3.5 dBW</td>
</tr>
<tr>
<td>Received Power</td>
<td>3.5 dBW</td>
</tr>
<tr>
<td>Signal Acquisition</td>
<td>-28.5 dBW</td>
</tr>
</tbody>
</table>

Assumptions:
- $P_F = 10^{-5}$, $P_D > 0.9$
- 4-MHz BW uniform interference at L1
- 3 dB receiver antenna gain, 400 km satellite altitude, transmitter at sea level
- 30 dB-Hz acquisition threshold for signal acquisition.

Matched-code interference can be detected with high-sensitivity by signal acquisition.
Average number of transmitter detections per day by a monitoring satellite on an ISS-like orbit.
Worst-case time between detections:
6.1 dBW EIRP: 4 days
3.7 dBW EIRP: 17 days

Assumptions:
• Space-station-like orbit: 400 km, 55-deg inclination
• Transmitter at sea level
Dual satellites (joint FDOA-TDOA): ~1 km CEP

Single satellite (Doppler positioning): ~3 km CEP

Assumptions:
• Space-station-like orbit: 400 km, 55-deg inclination
• 50-km inter-satellite baseline (for dual satellite scenario)
• Transmitter at sea level
• 100-W EIRP transmitter with low-quality OCXO
• Single flyover
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.
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
Power Spectra

L1: 1575.42 MHz

L2: 1227.6 MHz

3 MHz
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.

Post-fit residuals of Doppler time history assuming estimated transmitter location and clock rate offset.
Doppler time histories can be used to infer transmitter location, assuming a transmitter clock with a constant frequency offset over each 60-second interval.
Khmeimim Air Base, Syria
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 Jan–Nov 2018. The interference source in Syria is clearly evident, with a pattern asymmetry due to the receiver’s antenna pointing aft.
Heat map based on standard 1-Hz L2 C/N0 data from ISS GRID receiver from Jan–Nov 2018. Interference from Syria is evident, as is a persistent signature south of Gobi desert.
Insights (1/2):

a) Russia and China are engaged in wide-area GNSS spoofing and jamming in multiple locations

b) Improved spoofing detection without improved spoofing resilience opens the door to spoofing for denial of service

c) 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 narrow/wideband jammer at the same stand-off distance

d) Cold start remains a necessary capability for many applications of interest
Insights (2/2):

a) A science-grade GNSS receiver in LEO is a power tool for global GNSS interference monitoring

b) Detection of signals as weak as 3.5 dBW (via CINR) and -28.5 dBW (via acquisition) is possible in theory

c) Localization of terrestrial sources is possible to better than a few km

d) We detected wide-area persistent GNSS interference in two locations

e) Interference from Syria is matched-code: potent for DoS