GNSS Interference Detection and Mitigation for UAV Navigation

May 22$^{nd}$, 2014

Presented in cooperation with GPS World Magazine
Today’s Topics and Panelists

Topics

- GNSS Interference / Denials, Needs and Challenges
- GNSS Interference and Attack Mitigation
- Hybrid Solution for Improving GNSS Reliability and Robustness
- Preliminary HGX Navigation Sensor Test Results

Panelists

- Franck Boynton – VP and CTO, Navtech GPS
- Peter F. MacDoran – Chief Scientist, Loctronix Corporation
- Dr. Michael B. Mathews – CEO and Founder, Loctronix Corporation
- Michael O. Davies – Senior Engineer Loctronix Corporation
GNSS INTERFERENCE / DENIALS, NEEDS AND CHALLENGES

Franck Boynton
Vice President and CTO, NavtechGPS
Fboynton@navtechgps.com
GNSS Vulnerabilities

The received power of GNSS signals at the Earth’s surface is very low

- GNSS signals are internationally protected spectrums
- GNSS signals can be overpowered
- GPS L1 frequency received on Earth at -160dBW
- Galileo L1 and other frequencies received on Earth at -152dBW
- GLONASS L1 frequency received on Earth at -161dBW
- Jamming can occur at any frequency in any location
- Most receivers and antennas are not built with strong AJ qualities
Spoofing

Denial of actual signal and replacement by pseudo signal: typically used to take over navigation of a device

- Typically a problem in non-SAASM Rx
- Difficult to achieve
- Mimic the GNSS signal in real time
- Receiver must transition smoothly from real to false signal
- Must stay locked on
- Claimed to have been used to “hijack” UAV’s
There are many jamming techniques and the more typical techniques for GPS jamming include:

- **Matched Spectral**: Signal with the same PSD (Power Spectral Density) as the target signal. Close match making it difficult to counter.
- **Chirp/Sweep**: A jamming signal is broadcast in a short burst where the frequency of the carrier is changed with respect to time.
- **Random noise**: Generated radio noise of a broad amplitude and bandwidth.
- **Carrier**: Specific attack on a narrow band of spectrum.
- **Natural interference**: Usually low including solar flares and scintillation.
- **With all of these techniques it is still possible to read through parts of the actual signal, process and pull it through**.

High power jammer ~120w, range 150KM claimed range.
Why Jamming?

**Intentional jamming**
- Electronic Warfare
- Terrorism
- Self preservation/evasion
- Security
- Spoofing
- LightSquared, there will be others

200mW personal
2-3W 50km claimed range

Multi-band jammer
Why Jamming?

Unintentional jamming, the reasons are not always obvious

- Out of band interference
- Harmonics
- Bad LNA (Low Noise Amplifier)
- Bad amplifier or other component
- Oscillation from repeater system
- Cell phone jammer that contains GPS jammer
What is typically done?

It depends on who you are.

️ Intrinsically UAV’s have some advantages at elevation
  ❖ Typically jammers are ground based
  ❖ In the air
  ❖ Distance away from ground
  ❖ Antennas mostly point upward and away
  ❖ Can detect and avoid

️ U.S. military and some allies SAASM and ITAR restricted antennas
  ❖ IMU’s
  ❖ Multi frequency bands within GPS
  ❖ AJ antennas, nulling CRPA
  ❖ Filtering

️ Civilian users can use non-ITAR hardware
  ❖ IMU’s
  ❖ CRPA
  ❖ Filtering in antenna, RF front-end and RF cables
  ❖ Multiple frequencies within GPS L1, L2, L2C, L5
  ❖ Change constellations
  ❖ Many frequencies within GPS, GLONASS, Galileo, Compass

KVH CG-5100 FOG
SATIMO CRPA
GPS Networking L1 filter
Vector Nav VN-200

© 2008 Loctronix Corporation, All Rights Reserved
GNSS INTERFERENCE AND ATTACK MITIGATION

Peter F. MacDoran
Chief Scientist, Loctronix Corporation
pete.macdoran@loctronix.com
Jamming Mitigation Techniques

Avoidance Techniques

- **Notch Filter** – Useful against CW or narrowband electronic attacks. Internet available jammers are wideband and target multi-GNSS constellations.

- **SAASM** – Selective Availability Anti-Spoof, not commercially available, DoD COMSEC authorization required and thus not for commercial applications.

- **Null Steering** – CRPA (Controlled Radiation Pattern Antenna), requires additional hardware, power, larger form factor and cost is an issue.

- **Multi-Constellation / Multi-Frequency** – may be of value, but, the jammer suppliers will adapt their “products” to continue jamming.

Preferred Strategy – Acceptance with Survival

- Accept that Jamming / Interference will be a future fact of life.

Design to Survive the Attacks!
Internet available jammers transmit > 4.5 mW EIRP at L1 with 50 MHz bandwidth to attack:

- GPS L1 & L2, and half GLONASS channels
- Jammers cost between $30 and $300, mischief is cheap.

4.5 mW Jammer has ability to:

- Disrupt GPS C/A acquisition at a distance of 117 km.
- A typical COTS C/A receiver has only 20 dB J/S jamming tolerance.
Response to the Jamming Challenge

Explore alternative signal processing techniques

- Achieve resilience comparable to SAASM DAGR DoD receivers
- Desired additional 15-20 dB J/S Margin compared to conventional COTS GPS receivers.

Detect interference early

- Monitoring the GNSS in-channel RF power and presence of interfering source
- Alert system to threat
- Mitigate effect through multiple measures
The significance of superior J/S performance is best illustrated by the Signal Acquisition Denial (SAD) zone.

- Consider even a low power (e.g., 4.5 mW jammer), which might easily be balloon-borne.
- A commercial GPS receiver attacked by a low power jammer will have a 320 square kilometers SAD zone.
- J/S Margins of 35 to 40 dB continues to provide navigation to within 0.9 km of the jammer and reduces the SAD zone area to only 2.4 square kilometers.
The Benefit of Improving Max. J/S Operation

Increased J/S performance significantly reduces effective jammed area.
4.5 mW Balloon-Borne Jammer over Seattle
1. R.H. Mitch, et.al., Cornell University; and J.A. Bhatti, et.al., Univ. of Texas, Austin; ION GNSS 2011

2. H. Kuusniemi, Finnish Geodetic Institute, United Nations, Latvia Workshop on Applications of GNSS, May 2012


HYBRID SOLUTION FOR IMPROVING GNSS RELIABILITY AND ROBUSTNESS

Dr. Michael B. Mathews

CEO / Founder Loctronix Corporation
michael.mathews@loctronix.com
### Robust UAV Navigation Receiver Requirements

#### Basic Interference Detection
- Signal Level (J/S)
- Obstruction detect
- Affected bands and channels

#### Mitigation Capabilities
- 30-40 dB J/S Margin
- Integrated Inertials
- Multi-Frequency / GNSS
- SoOps (advanced)

#### Attack Characterization (Advanced)
- Noise
- Chirp / Sweep
- Carrier
- Matched Spectral
- Spoofing

#### General Capabilities
- 20 dB-Hz Acquisition Sensitivity
- 15 dB-Hz Track Sensitivity
- < 100 ms Latency
- 50 Hz Max Update Rate
- Meter-Level 3-D Accuracy
- < 1s Fast Acquisition/Recovery
HGX – Hybrid Navigation Sensor

Hybrid RF Signal and Sensor Processing
- Combines SCP and Traditional Correlation
- Low Latency Federated Filter
- Integrates Inertial / RF Sensor Observables

Key Features
- Multi-Frequency / Multi-Channel GNSS
- Embeddable Software Defined Radio (SDR) Implementation
- Real-time and Post-Processing Modes
- Interference Simulation Tools
- Integrated Interference Detection and Mitigation Functionality
HGX – Toolkit and Sensor Architecture

HGX SDR Sensor

Sensor Fusion Navigation Engine

- Interference Detection
- SCP Tracking and Acquisition
- Telemetry Extraction
- Interference Mitigation Controller
- Correlation Tracking and Acquisition
- Software Correlators
- Data Sampling
- Software SCP DSP
- High Speed Data Storage

C/C++ Components

- 32/64 Bit Linux/Windows/Custom

Hdw. Logic

- Direct to Baseband DSP RX / TX
- SCP DSP
- Hardware Correlators
- Barometer
- 9 Axis Accelerometer, Gyroscope, Compass

© 2008 Loctronix Corporation, All Rights Reserved
ASR-2300 MIMO SDR / Motion Sensing Module

**RF / Multi-Sensor Signal Processing**
- 2 x 28 MHz Transceivers 300 MHz to 3.8 GHz Full Duplex
- 9 RF Paths: 6 RF inputs / 3 RF outputs (U.FL)
- Integrated L1 GPS and Wi-Fi Antennas
- Integrated 10 axis MEMS sensors (accelerometer / gyroscope / compass / barometer)
- Expansion Port supports for MIMO / Data I/O

**Electrical Interface**
- SuperSpeed USB 3.0 interface at 315 MB/s sustained data transfer
- Very Large Spartan-6 FPGA: 6,822 / 58 DSP slices
- 128 MiB RAM
- 5 Volts @ 1.2 A (6 W) at full utilization.
- 1.2 mbps UART
- Li-Ion Battery external connection w/charger function

**Physical Specifications**
- 9.90 x 6.61 x 0.95 cm (3.898 x 2.60 x 0.375 in)
- Weight ~ 48 grams (1.5 oz).
ASR Workbench™

SDR Integrated Development Environment (IDE)

- Drag-and-drop, real-time DSP modeling tool
- Integrated support for the ASR-2300.
- Freely available for users of the ASR-2300

Features

- Process multiple ASR-2300 baseband I/Q sample streams.
- Record/playback signals, analyze received signals using a variety of demonstration models.
- Optimize the performance and configuration of the ASR-2300 module with a suite of diagnostic tools.
A non-linear operation on a broadband signal that enables extraction of amplitude, frequency, and phase information

GPS example with Delay & Multiply

- Spectral compression applies a delay and multiply operation on P(Y) ranging signals.
- Fundamental chipping rate signals are extracted using an FFT on the Spectral Compressor output.
- Each peak in the FFT (containing amplitude, frequency, and phase) represents a single GPS satellite.
- Doppler frequency shift is used to uniquely identify the specific satellite given a GPS Almanac.
- No complicated tracking loops or correlators are required.
Hybrid SCP and Correlation Has SWaP Advantages

1 Channel of SCP signal processing is equivalent to 16 or more correlation channels

L1 C/A Code-Correlation Receiver (16 Channels)

L1 C/A Receiver Using SCP (1 Channel)

16 Signals=16 Channels

All Satellites In View

LEO Obs.

All-in-View = 1 SCP Channel
HGX Benefits and Roadmap

Interference Mitigation
- Additional 15-20 dB J/S margin compared to conventional GPS
- Multi-frequency capability
- Access to GPS PPS
- Multi-GNSS ready
- Graceful Degradation

Accuracy and Performance
- Meter-level accuracy. Higher accuracy options also a possibility
- Integrated Inertial
- Multi-Frequency / GNSS
- < 100 ms Latency
- 50 Hz Max Update Rate
- < 1s Fast Acquisition/Recovery

HGX Available Summer 2014
- Embedded solution
- Multi-frequency GPS
- Development toolkit w/ASR-2300

See Preview At JNC 2014
- June 16-18th, 2014
- Booth 31
PRELIMINARY HGX NAVIGATION SENSOR TEST RESULTS

Michael O. Davies
Senior Engineer, Loctronix Corporation
michael.davies@loctronix.com
HGX Sensor in the Presence of a Simulated L1 Jammer
A Jammer was simulated and added to the raw data streams collected during drive around.

A Code Correlation Receiver was compared to the Hybrid Receiver in the presence of a jammer.
L1 GPS Data Collection

Collected data driving in a 10 minute loop in Woodinville, WA

The ASR-2300 was used to collect GPS L1 samples and write to disk.

L1 C/A and P(Y) antenna, consumer grade
The Woodinville Loop, COTS GPS Mode

Start, End
Simulating a Jammer

- 2 micro-Watt Power Idealized Isotropic Jammer (direct line of sight)
- Chirp-Sweep Jammer 13 MHz L1
- Signal J/S varies with distance
- Jammer was “placed” close to the drive-around loop to test performance as J/S dynamically changes
Simulating a Jammer

- As jammer gets closer, its power rises above thermal noise floor
- Chirp-Sweep intended to wipe-out L1 C/A Code Correlators
- Similar to commercial jammers: sweep 9 µs, BW = 13 MHz

![L1 Sweep Jammer (9 usec period, ± 13 MHz)](image1)

![L1 C/A Jam Power Spectra (25 dB J/S)](image2)
HGX COTS Mode Operation with Jammer Enabled

Code Correlation Fails, 23 J/S

Code Correlation Recovers
HGX Hybrid Mode Operation with Jammer Enabled

Interference Detected, Enable Mitigation

Disable Mitigation
HGX Preliminary Testing Results

Preliminary Testing Shows:

- Significantly increases J/S margins by 15-20 dB compared to conventional COTS GPS receiver.
- Receiver can detect interference before failure.
- Mitigates failure by seamlessly switching operating modes and data types.

HGX is a Robust and Resilient Solution for Commercial UAV Navigation

- Achieves near-SAASM J/S performance without crypto access requirements.
PLEASE VISIT LOCTRONIX AT
JNC 2014, BOOTH 31

June 16-18, 2014
Orlando, Florida
email: lew.larson@loctrhonix.com
to schedule a meeting
Questions?
Today’s Panelists

Franck Boynton
Vice President and CTO, Navtech GPS
Fboynton@navtechgps.com

Peter F. MacDoran
Chief Scientist, Loctronix Corporation
pete.macdoran@loctronix.com

Dr. Michael B. Mathews
President/Founder, Loctronix Corporation
michael.mathews@loctronix.com

Michael O. Davies
Senior Engineer, Loctronix Corporation
michael.davies@loctronix.com