sponsored by spirent™ Promise. Assured.

InsideGNSS
GPS | GALILEO | GLONASS | BEIDOU

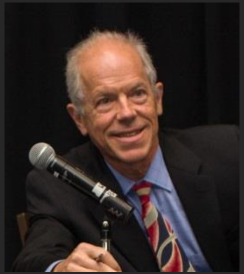
inside unmanned systems
INSIDE ENGINEERING, POLICY AND PRACTICE

GNSS VULNERABILITY TESTING AND THE CONTROLLED RECEPTION PATTERN ANTENNA (CRPA)

Wednesday, March 25, 2020

WELCOME TO

GNSS Vulnerability Testing and the Controlled Reception Pattern Antenna (CRPA)



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Kimon Voutsis
Product Manager
High-end PNT Test Solutions
Spirent Communications, UK

Oscar Pozzobon
Technical Director
Qascom, Italy

Sherman Lo
Research Engineer
Aeronautics and Astronautics
Stanford University

Co-Moderator: Lori Dearman, Executive Webinar Producer

Who's In the Audience?

A diverse audience of over 500 professionals registered from 49 countries, representing the following industries:

28% Military and defense

8% Transportation/logistics/asset tracking

7% Automotive

4% Machine control/mining/construction

1% Precision Agriculture

52% Other

Welcome from *Inside Unmanned Systems*

Richard Fischer
Publisher
Inside GNSS
Inside Unmanned Systems

A word from the sponsor

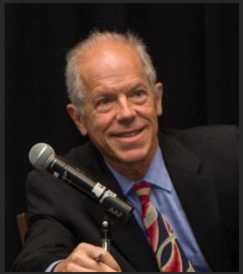
Adam Price
Director of Product Management & Business Development
PT Business unit at Spirent Communications

Today's Moderator

Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Today's Panel

GNSS Vulnerability Testing and the Controlled Reception Pattern Antenna (CRPA)



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Kimon Voutsis
Product Manager
High-end PNT Test Solutions
Spirent Communications, UK

Oscar Pozzobon
Technical Director
Qascom, Italy

Sherman Lo
Senior Research Engineer
Aeronautics and Astronautics
Stanford University

QUICKPOLL

What one type of RF interference have you encountered most frequently in the past year?

Poll Results (single answer required):

unintentional jamming	31%
intentional jamming	29%
spoofing	10%
self-interference	9%
none in the past year	21%

Efficient Testing for GNSS Vulnerabilities (Interference)

Kimon Voutsis, PhD
Product Manager
Spirent

Outline

- GNSS vulnerabilities overview

- Why simulate?

- User applications

- RFI testing (CRPA)

- Summary

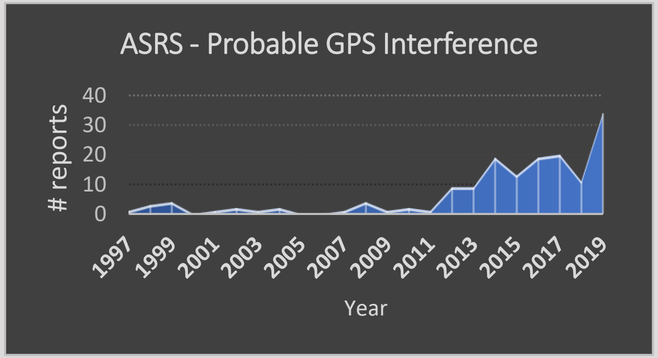
GNSS Vulnerabilities Overview

Why Simulate?

Method / attribute	Live-sky	Simulation	Record & playback system
Realistic	✓	Representative	✓
Repeatable	✗	✓	✓
Controllable	✗	✓	Partially
Truth reference & error budget	✗	✓	✗

User application examples

Performance	Resilience
Fundamentals System Interoperability Multipath/obscuration Hardware-in-the-loop Sensor fusion Regulatory conformance Timing	Atmospherics & Space Weather Spoofing **Interference & Jamming**

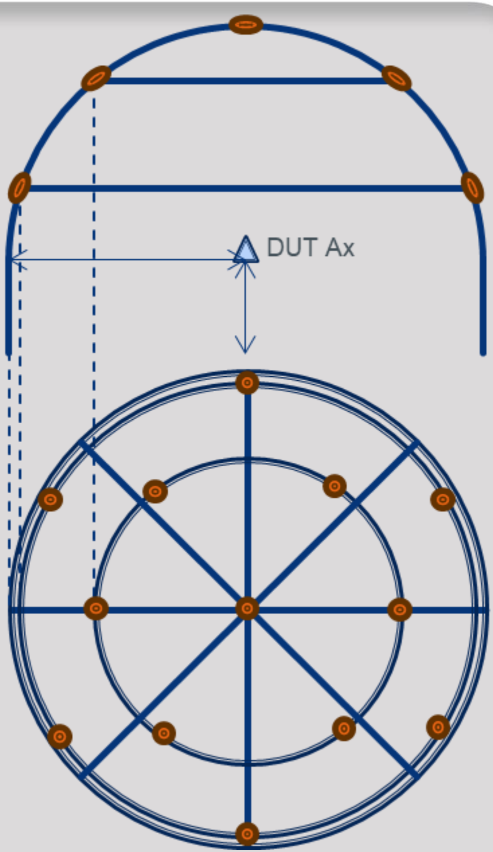


Source: https://asrs.arc.nasa.gov/index.html

- Over the air (anechoic chamber)

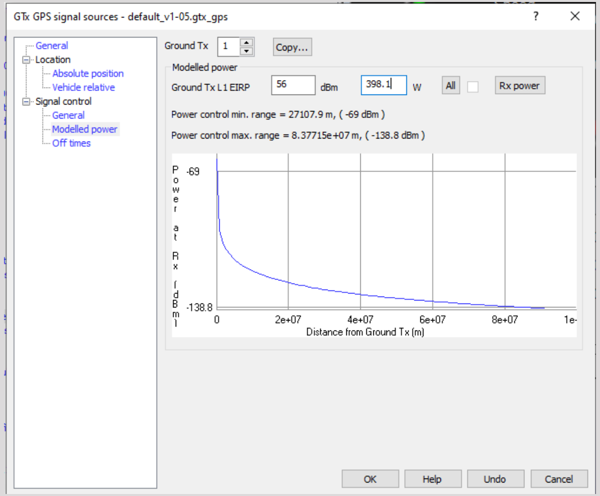
- Conductively

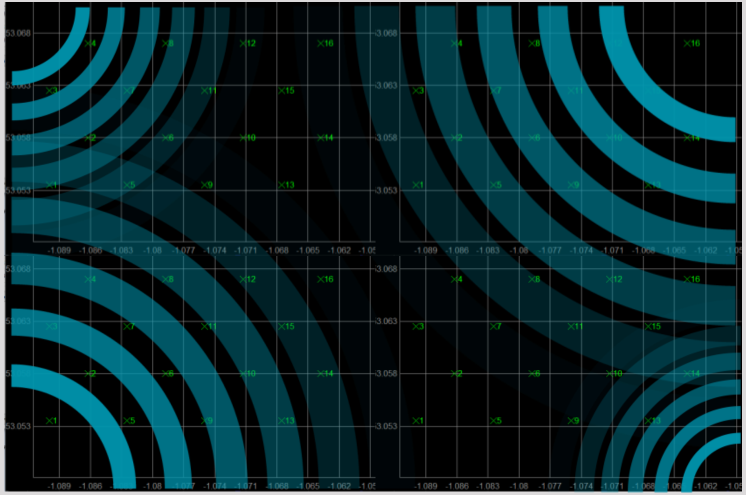
- Example applications
  - CRPA testing: military & civil applications (recently)
  - Regulatory compliance, e.g. RTCA DO-229, ETSI RED.



Efficient RFI simulation testing

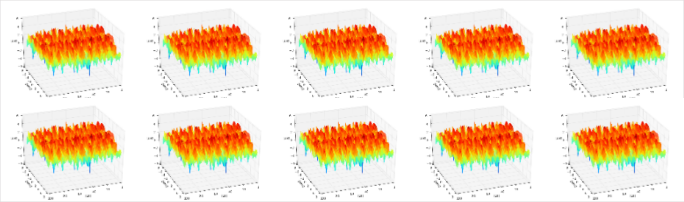
- Accurate power calibration, modelling and control
  - High incident power (e.g. 0 dBm)
  - Low noise floor, High J/S (+130dB)
- Radiation field - # of Tx’s
- Multi-constellation/frequency, realistic wavefront

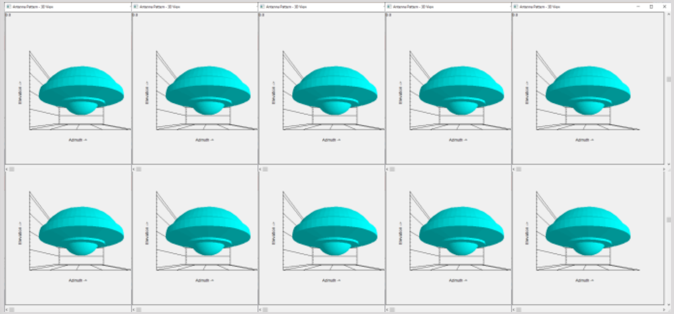




Efficient RFI simulation testing

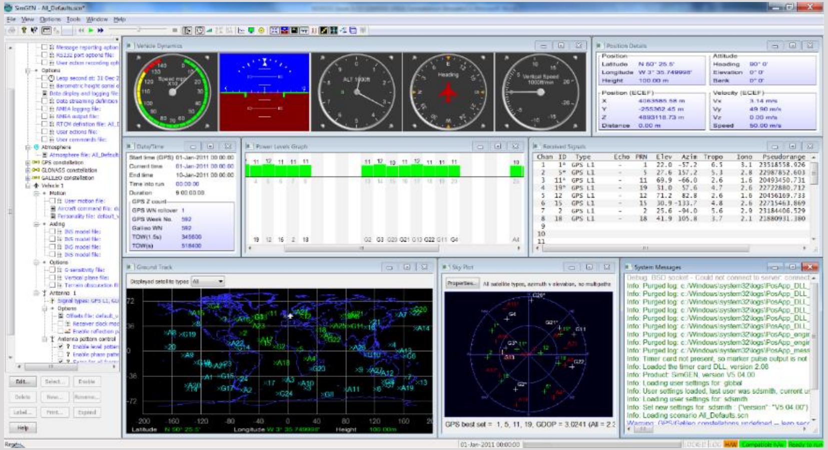
- Accurate carrier-phase calibration (degree-level)
  - Multiple carrier frequencies
  - No. of RF outputs (one per CRPA element)
- Antenna amplitude & phase patterns
  - Depending on carrier frequency (L1/L2/L5)
- Waveforms
  - CW/BPSK/AM/FM/PM/AWGN

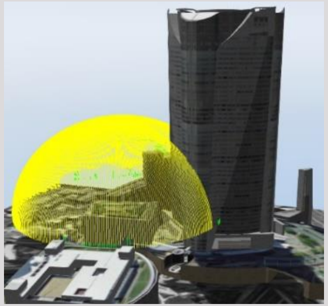


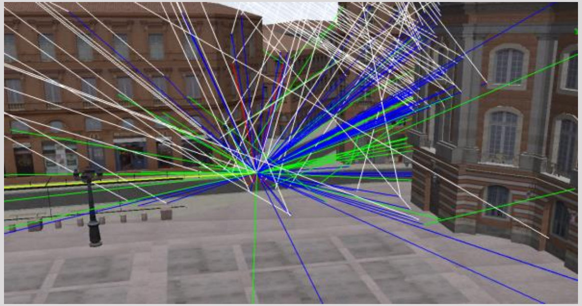


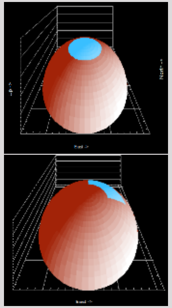
Efficient RFI simulation testing

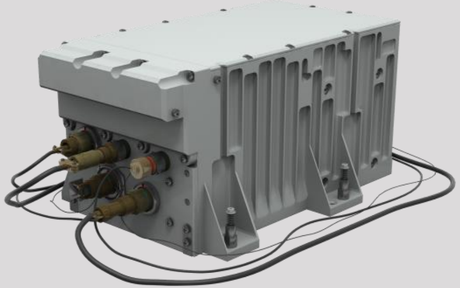
- Scalability
- HUR/SIR (e.g. >1kHz)
- User-friendly scenario creation
- Automation
- HIL (low latency)
- Other sensors











Summary

- GNSS vulnerabilities
  - Ensure testing is repeatable and accurate

- RFI testing key parameters
  - Power/carrier-phase calibration
  - Multi-frequency/constellation support
  - Signal fidelity/Spectrum purity
  - Low noise floor, high J/S
  - Scalability
  - Update rate
  - Automation
  - HIL
  - Other sensors

GNSS Vulnerability Testing

Oscar Pozzobon
Technical Director
Qascom, Italy

GNSS Threats: the past, the present and the future

- GNSS threats are evolving
- The challenge is to predict
- Tomorrow Likelihood of occurence -> Today's product design

1990: **Availability**

2000: **SA OFF**, **Jamming**

2010: **Jamming**, **+Spoofing**

2020: **Jamming**, **Spoofing**, **+Cyberattacks**

2030: **Jamming**, **Spoofing**, **Cyberattacks**, **+Authentication**

2040: **?**

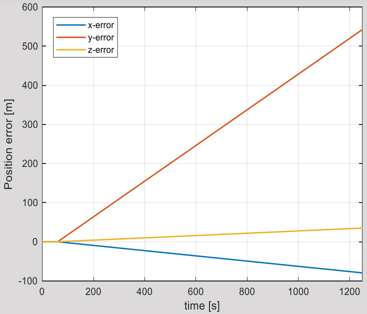
GNSS Threats: the past, the present and the future

- Threat classification and categorization will be the need for the future
- Attacks shall be considered in all layers (signal, coding, data, protocol)

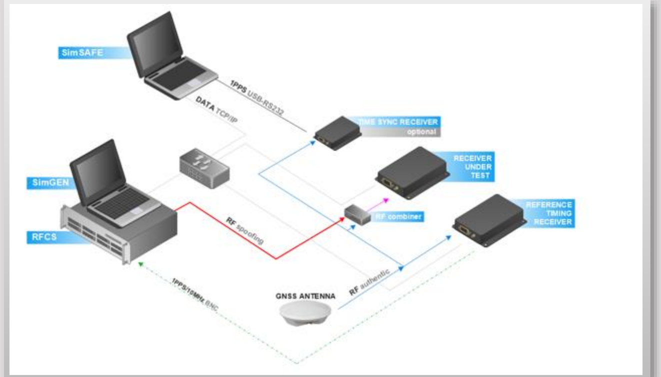
Protocol Layer	Security exploits
Data Layer	Spoofing, Smart Jamming
Coding Layer	Jamming, Spoofing
Signal Layer	Jamming, Spoofing, Meaconing

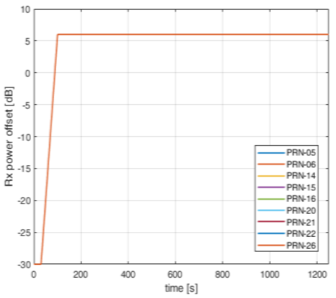
Example of synchronized spoofing attack

- Targets position deviation without position fix loss
- Requires synchronization with live signals and knowledge of target location and dynamics

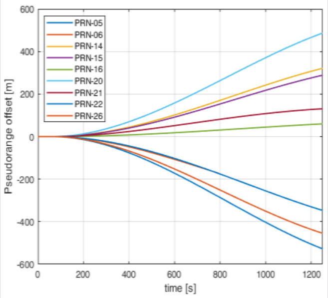


Position Error





Spoofing signals relative power

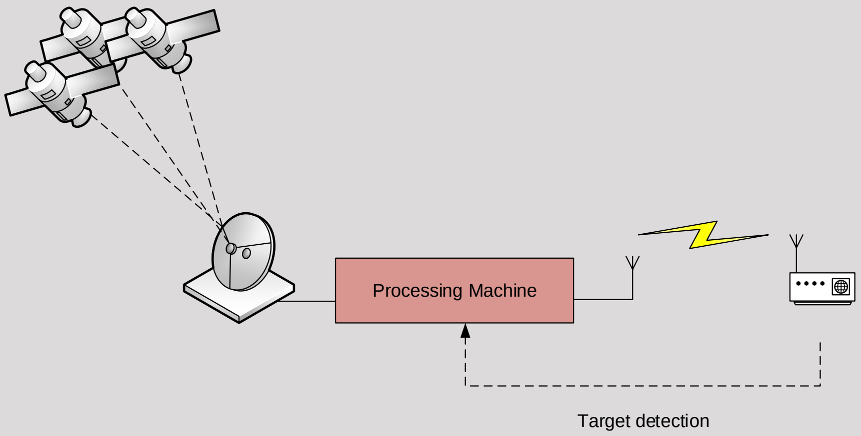


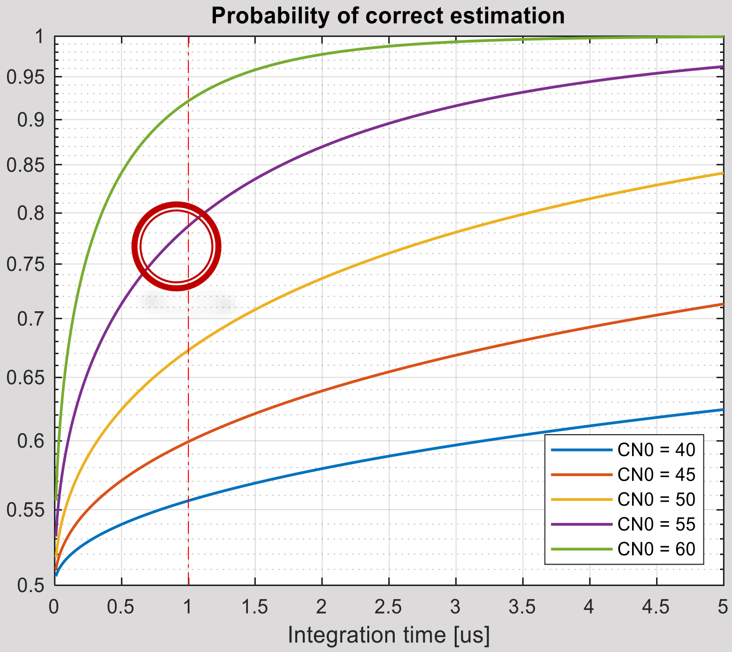
Pseudorange error

Future attacks: Replay Attack simulation

- Signals are first estimated with a receiver like technology
- Signals are then re-generated with the predicted information

- 1us integration allows up to 80% of correct estimation
- Effective on any radio frequency signals





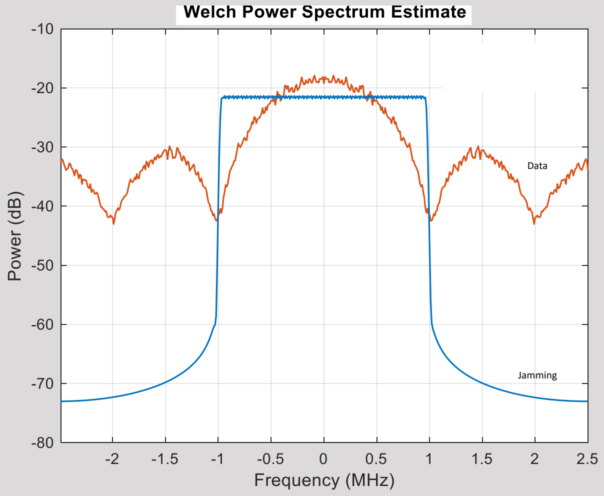
The need for sophisticated equipment

- Simple White noise channel simulation
  - Theory is bright
  - Anti jam / Anti spoof Detection is perfect
  - High probability of detection, low probability of false alarm

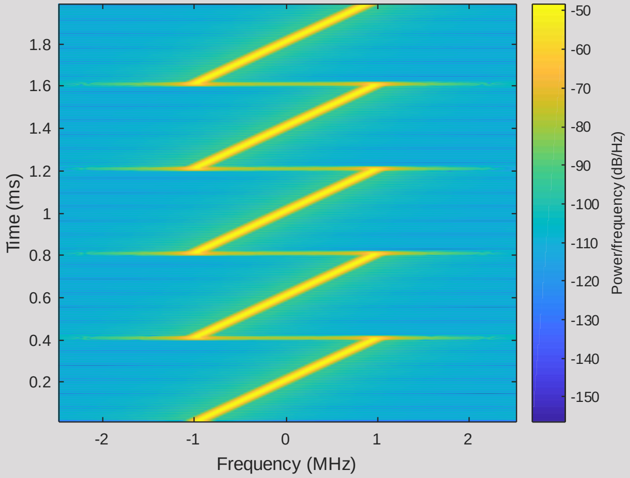
- Realistic RF Environment simulation
  - urban/suburban, indoor highly impacts vulnerability testing
  - Low probability of detection, High probability of false alarm
  - Required for CRPA testing
  - Fundamental for fine risk assessment evaluation

Selective Jamming

- Selective Jamming refers to jamming of some specific data / symbols for specific objectives
- Performed for Denial of Service, Spoof only some services,etc



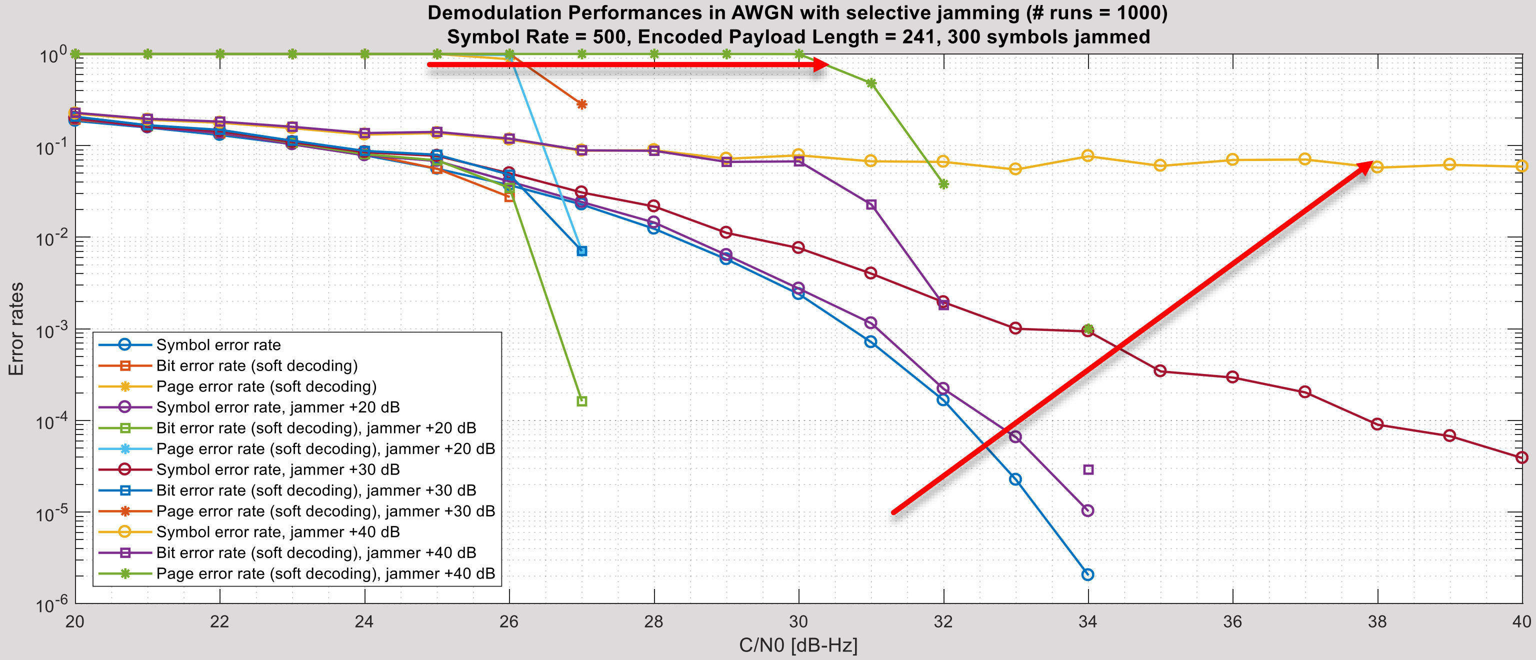
Channel data and jamming signal spectral shaping



Jamming signal spectrogram

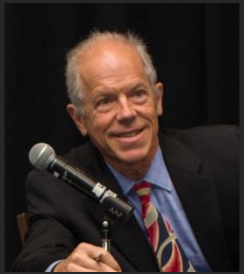
Impact of Selective Jamming

- Pages and Symbols are impacted differently in selective jamming.
- C/N0 plays a role in robustness



Ask the Experts Part I

GNSS Vulnerability Testing and the Controlled Reception Pattern Antenna (CRPA)



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Kimon Voutsis
Product Manager
High-end PNT Test Solutions
Spirent Communications, UK

Oscar Pozzobon
Technical Director
Qascom, Italy

Sherman Lo
Senior Research Engineer
Aeronautics and Astronautics
Stanford University

QUICKPOLL

What is your level of experience with simulation testing for signal vulnerability?

Poll Results (single answer required):

incorporating simulation testing for signal vulnerability	38%
Have not done so, and have no plans to do so	16%
Have not yet done so but wish to take this step	29%
Not yet accomplished but have taken steps in this direction	18%

GNSS Vulnerability Testing- Part II

Oscar Pozzobon
Technical Director
Qascom, Italy

Why testing in simulation

- Prevent threats before occurrence
- Support risks assessment, Analyze impact on the receiver
- Check impact on specific environment
- Play in repeatable ways → Massive vulnerability testing

- Threats to consider
  - Denial of Service
    - Jamming
    - Smart Jamming / Selective Jamming
    - Data spoofing
    - Cyberattacks (crash of receiver)
  - Deception
    - Spoofing
    - Meaconing
    - Replay attacks

Vulnerability test planning

Attacks

Vulnerabilities

Nominal KPI

Security KPI

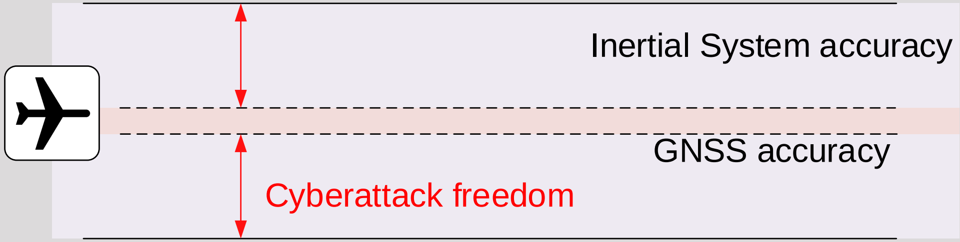
Different vulnerability analyses approaches

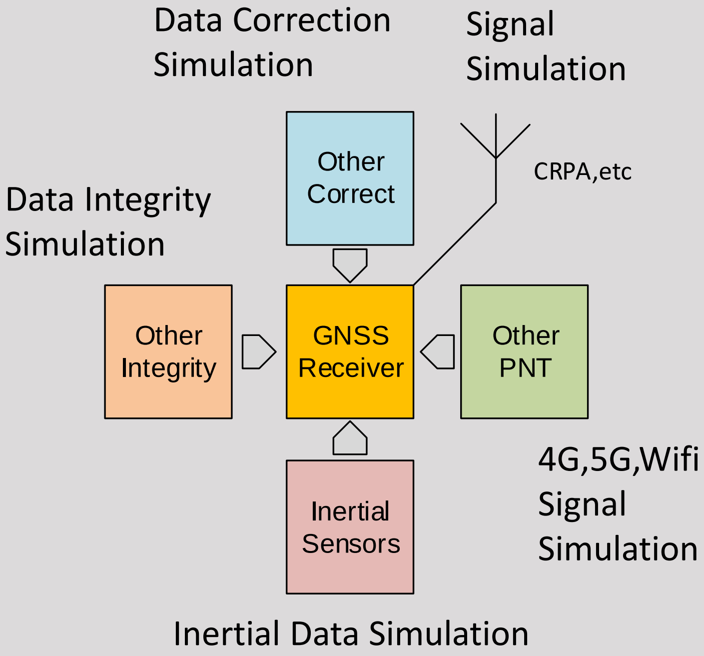
- **Test by Known Attacks**
- **Test by Known Vulnerabilities**
- **Test by Security Objectives**
- **Test by nominal KPI**
  - Availability
  - Integrity
  - Precision / Accuracy
- **Test by security KPI**
  - Probability of false alarm
  - Probability of Miss Detection
  - Time to Alert
  - Other

Vulnerability test planning

- **Define the Simulation Realism**
  - Attacker location
  - Attacker Dynamics
  - Attacker Channel Conditions
  - Attacker antenna
- **Define sensor fusion simulation**

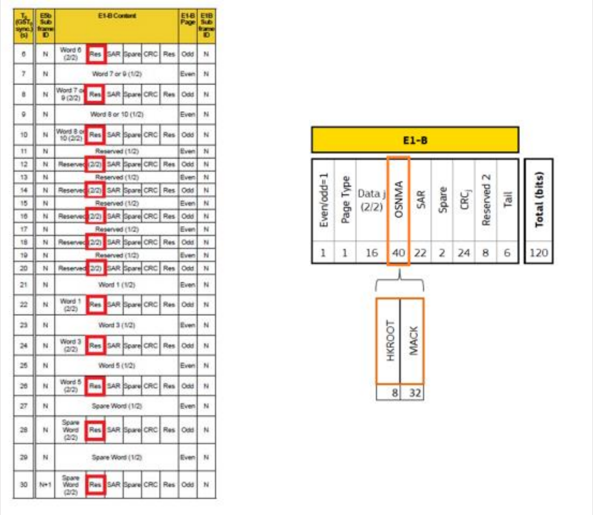
E.g.: Application level risk assessment





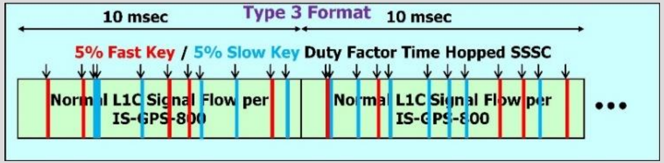
Future Authentication Services

- Authentication is going to be introduced in all major systems
  - Open Service Navigation Message Authentication (OSNMA) For Galileo
  - Chip Message Robust Authentication (CHIMERA) for GPS
  - Other proposal under discussion
- Authentication will be an opportunity to test receiver based anti-spoofing with System based services



Galileo OSNMA

Source: www.gsa.europa.eu/



GPS Chimera

Conclusions

- Security is a continuous process, new protections means new threats
- The need for vulnerability testing is a fundamental part of the security process
- Security requirements shall define the level of sophistication and realism required, including application level realism
- Authentication Services will be next decade opportunity to test protection mechanisms

Basic Control Reception Pattern Antenna (CRPA) for Civil Applications

Sherman Lo
Senior Research Engineer
GPS Laboratory
Stanford University

Outline

- CRPA for civil applications
- Overview of fundamental concepts
- Research and Development of Civil CRPA

Civil Controlled Reception Pattern Antenna (CRPA)

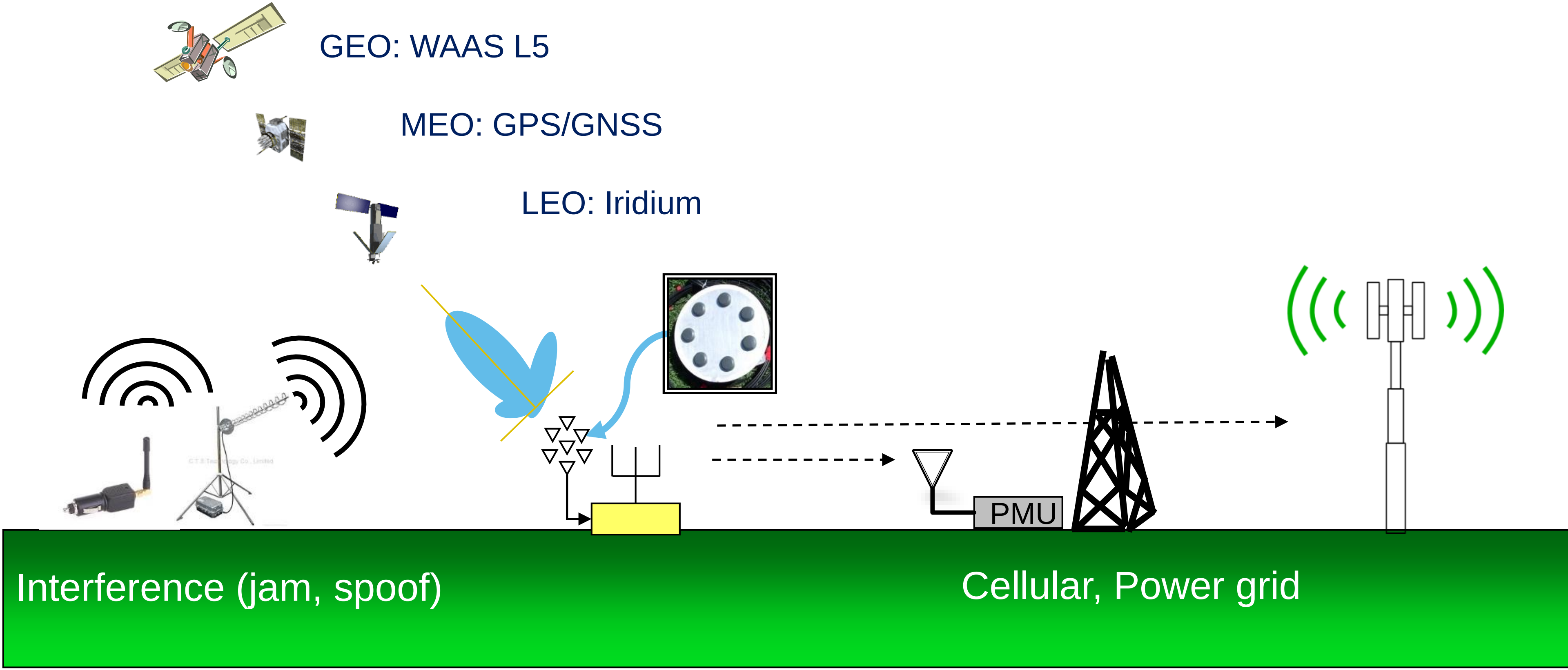
- CRPA used in military aircraft to overcome jamming by hostile forces
  - High end systems
- Is there a place for CRPA in the civilian world?
- Can we create a CRPA appropriate for civil use?



NYSE
KCG
NYSE
OXY


CRH

Example: Robust Satellite Based Time Synchronization for Civil Infrastructure



International Traffic in Arms Regulations (ITAR)

- GNSS adaptive antennas are export-controlled by many countries
  - U.S. ITAR and EAR – 22 CFR 120 – 130, 15 CFR 730 -
  - Europe – by Commission Delegated Regulation (EU) 2018/1922 of 10 October 2018
  - Canada – Export Control List
- Current ITAR provides some commercial opportunities
  - Restrictions apply to 4+ element CRPA with beams & nulls switching faster than 50 ms
  - See regulation for more details

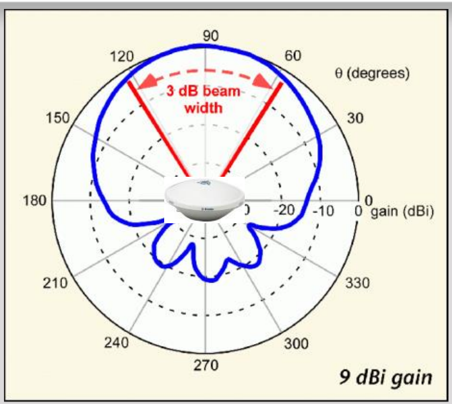
Outline

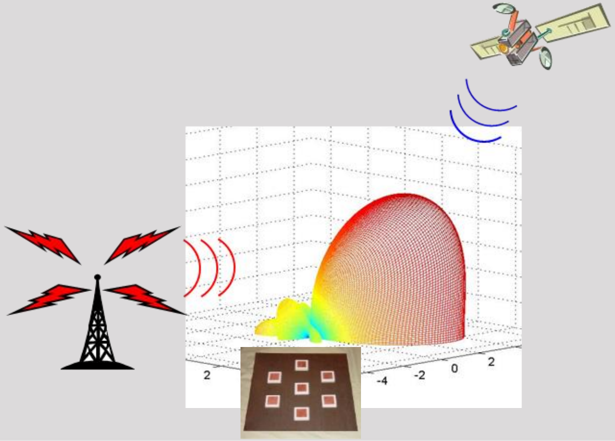
- CRPA for civil applications
- Overview of fundamental concepts
- Research & Development of Civil CRPA

Fixed vs Controlled Reception Pattern Antenna

- FRPA – traditional single element antenna
  - Gain pattern fixed

- CRPA technology generically describes adaptive gain pattern capabilities
  - Electronically steered based on weighting each antenna element

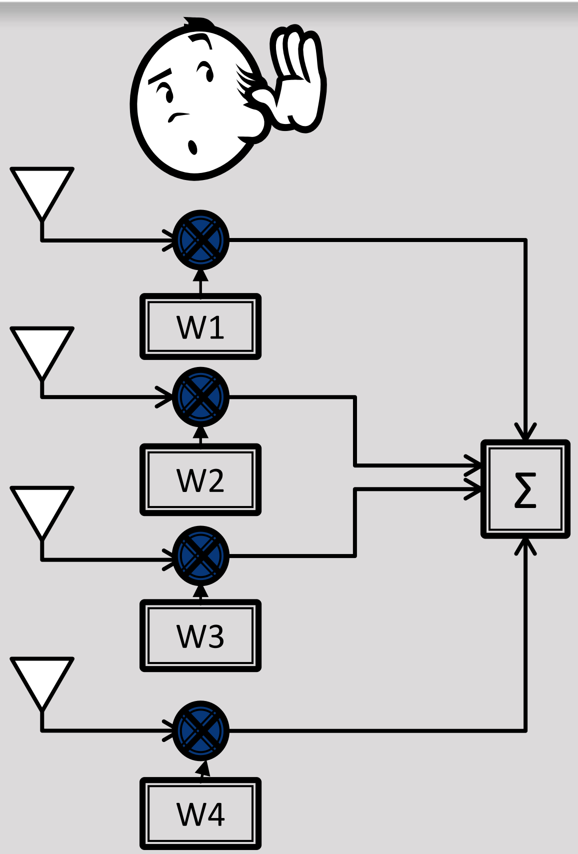




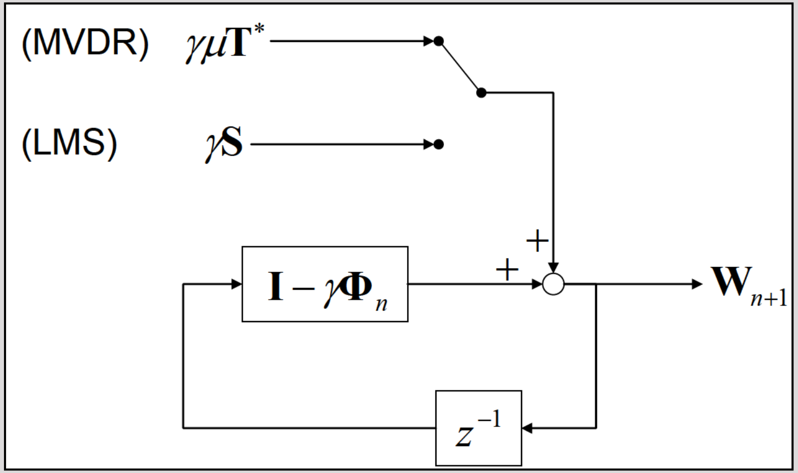
Source: http://www.navipedia.net, Stanford University

- Adapt phase weights to change how CRPA listens
- Null forming: pure nulling is unconstrained & single output
- Beam forming: 2 classes of constraint, different constraint per sat/signal
  - Maximize Signal to Interference + Noise Ratio (SINR)
  - Minimize Mean Square Error (MSE)

$$\boxed{s(t) = \sum_{k=1}^{n} s_k(t) * w_k(t)}$$

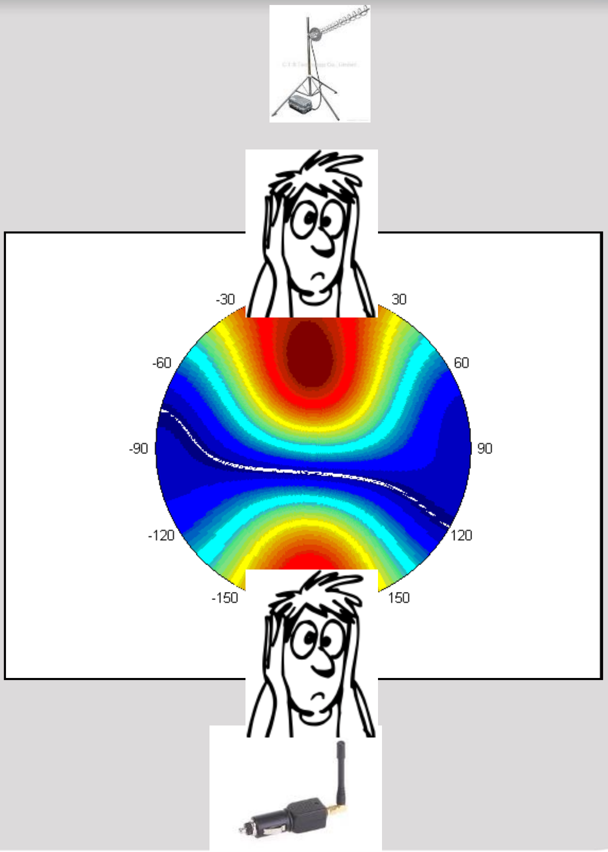


- Minimum Variance Distortionless Response (MVDR): SINR class
  - Constraint is a look direction
- Least Mean Squared (LMS): MSE class
  - Constraint is a specific signal
- Both techniques straightforward to implement iteratively
  - Can update each epoch



Null forming

- Unconstrained (no beam forming)
  - Minimize overall power
  - Useful for GNSS as GNSS below noise floor
- Power constraint (from beam forming)
  - Keeps energy in beam but reduces it elsewhere



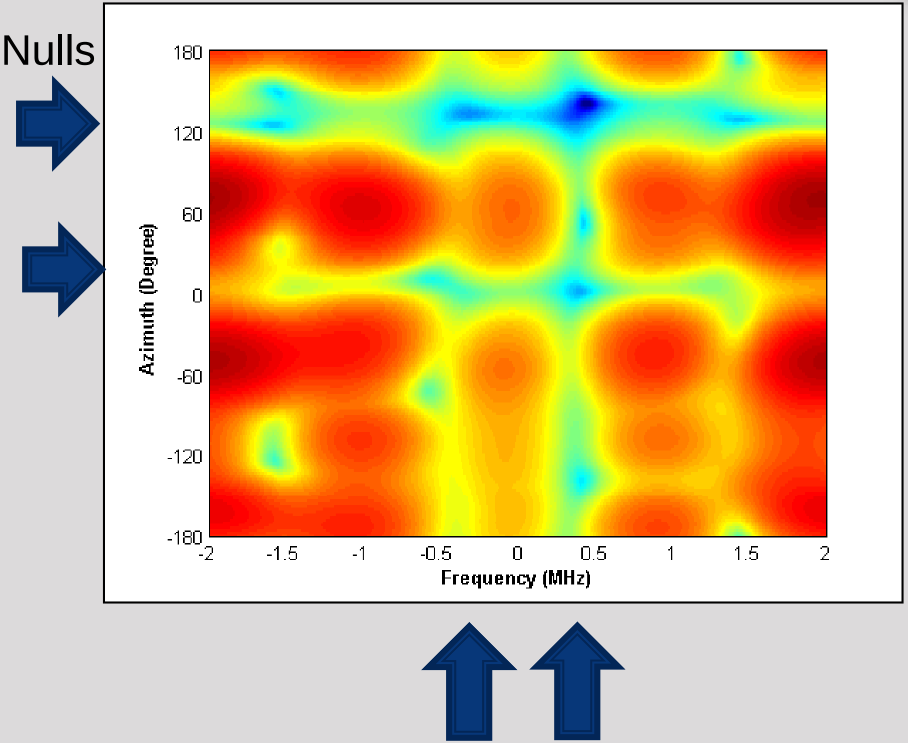
Beam forming vs Nulling Only

- Beam forming gets concentrate more signal energy
  - Requires an additional constraint, so loses a degree of freedom for nulls
  - Separate calculation & output for each satellite or signal
  - More computationally intensive
- Nulling (only) does not concentrate satellite energy
  - Single output (powermin), easy to fit into existing receivers
  - Less effective as GNSS approaches noise floor

CRPA STAP Processing

- Spatial Time Adaptive Processing (STAP) combines adaptive reception pattern & time processing
- Combination improves interference rejection (number and power)

Spatial Nulls

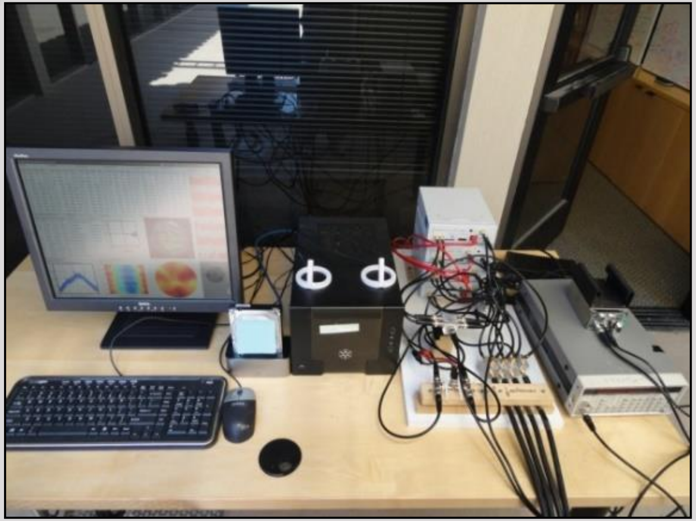


Spectral Nulls

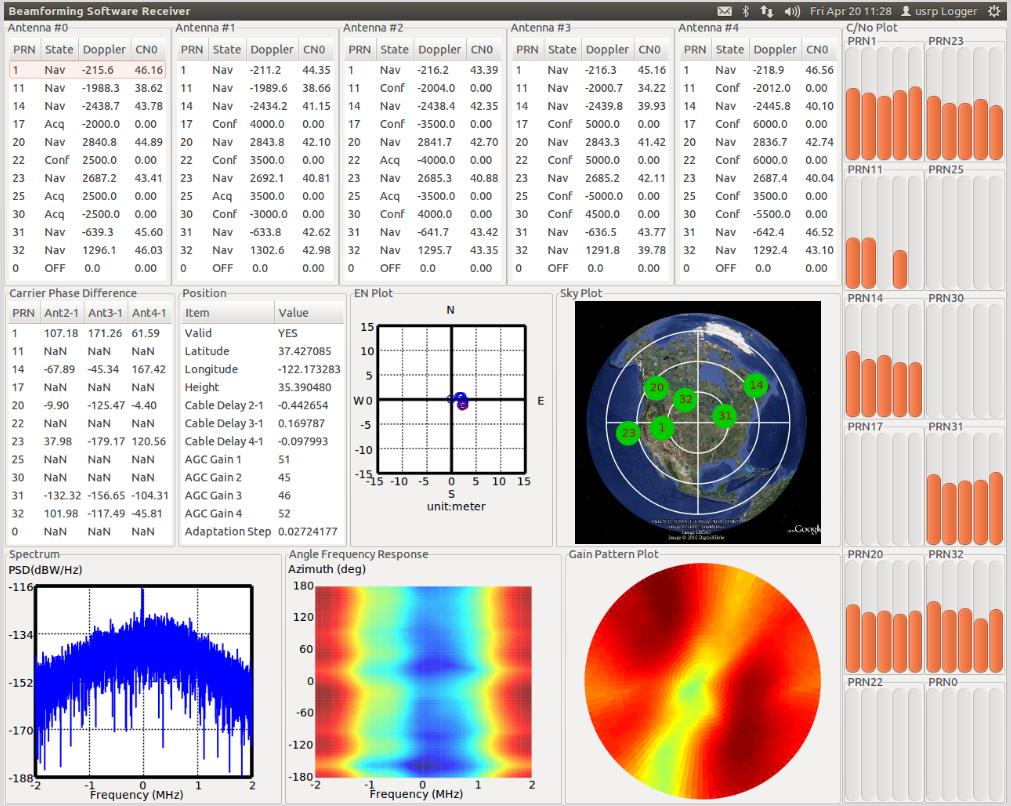
Outline

- CRPA for civil applications
- Overview of fundamental concepts
- Research & Development of Civil CRPA

An All COTS CRPA for Civil Applications (2010-2015)



Controlled reception pattern antenna (CRPA) receiver & data collector developed by Y.H. Chen



Dual Polarization Antenna (DPA) for CRPA

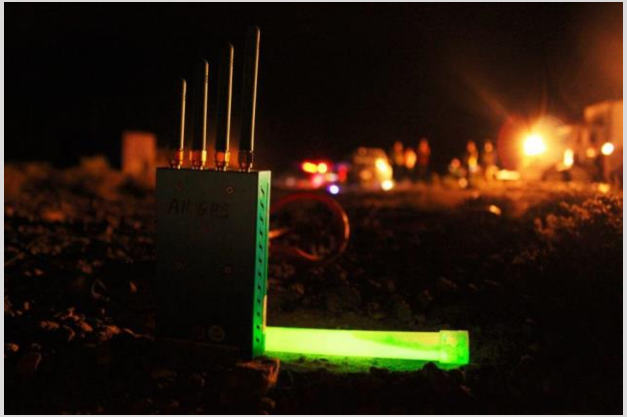
- DPA provides LHCP & RHCP signals; can be built with a patch with 2 feeds
- DPA can use LHCP & RHCP combinations to create a null in one direction
- CRPA using DPAs have more degrees of freedom for improved accuracy & robustness
  - Accuracy from improved C/No
  - Track signals at higher jamming levels than with single polarization implementation

1. Y.H. Chen, et al, “Demonstrating Single Element Null Steering Antenna Direction Finding for Interference Detection,” ION ITM 2018

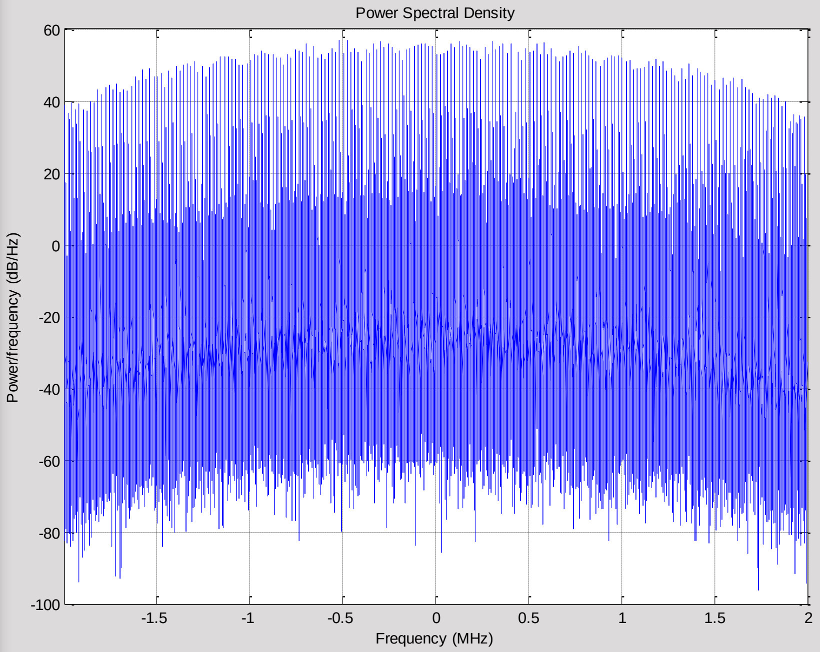
2. Matteo Sgammini, et al, “Interference mitigation using a dual-polarized antenna array in a real environment,” Navigation, Journal of ION, 2019

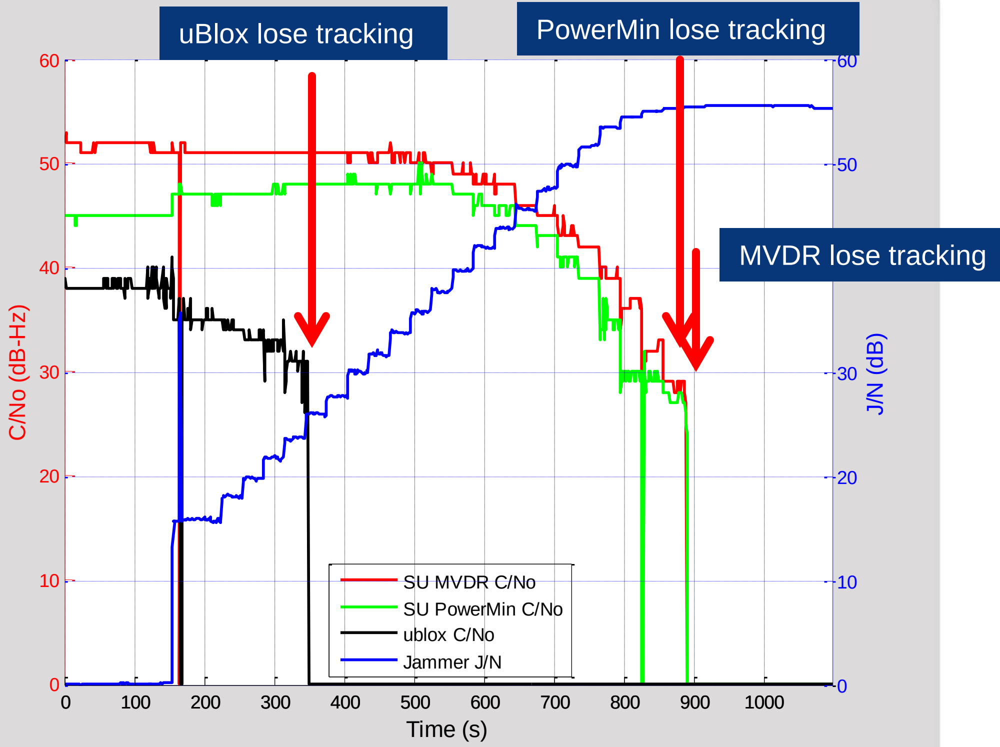
Interference Exercises for CRPA & DPA Testing

Interference Exercise	Date
NAVFEST, White Sands	Feb 2011
RFN, Sweden	Oct 2011
DHS Gypsy, White Sands	June 2012
RFN, Sweden	Oct 2012
DHS JamX & GET-CI, Idaho	2017
DT NAVFEST, Mojave Desert, CA	Sept 2019



Broadband Noise





Summary

Spirent InsideGNSS Inside Unmanned Systems

- CRPA for the civil market is both achievable and practical
- Many forms and implementations of basic CRPA technology including beam steering, null steering, time/frequency processing
- Research and commercial development of CRPA ongoing and require many means of testing

Resources

eBook: Choosing a GNSS Simulator

https://www.spirent.com/assets/eb/eb_choosing-a-gnss-simulator

eBook: How to Construct a GPS/GNSS Test Plan

https://www.spirent.com/assets/eb/eb_how-to-construct-gps-gnss-test-plan

Data Sheet GSS9000 Series

https://www.spirent.com/-/media/datasheets/positioning/gss9000.pdf

QUICKPOLL

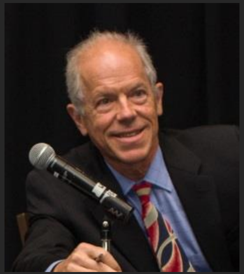
What is the most common threat affecting GNSS signals?

Poll Results (single answer required):

short-range jamming	55%
area-wide or region-wide deliberate GNSS attack	30%
spoofing for criminal or other law-evading purposes	10%
scheduled signal operator outages	2%
other	4%

Ask the Experts

GNSS Vulnerability Testing and the Controlled Reception Pattern Antenna (CRPA)



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Kimon Voutsis
Product Manager
High-end PNT Test Solutions
Spirent Communications, UK

Oscar Pozzobon
Technical Director
Qascom, Italy

Sherman Lo
Senior Research Engineer
Aeronautics and Astronautics
Stanford University