sponsored by

NovAtel

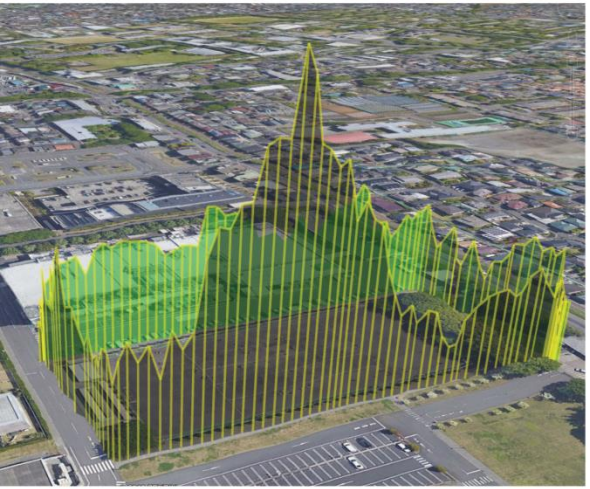
InsideGNSS

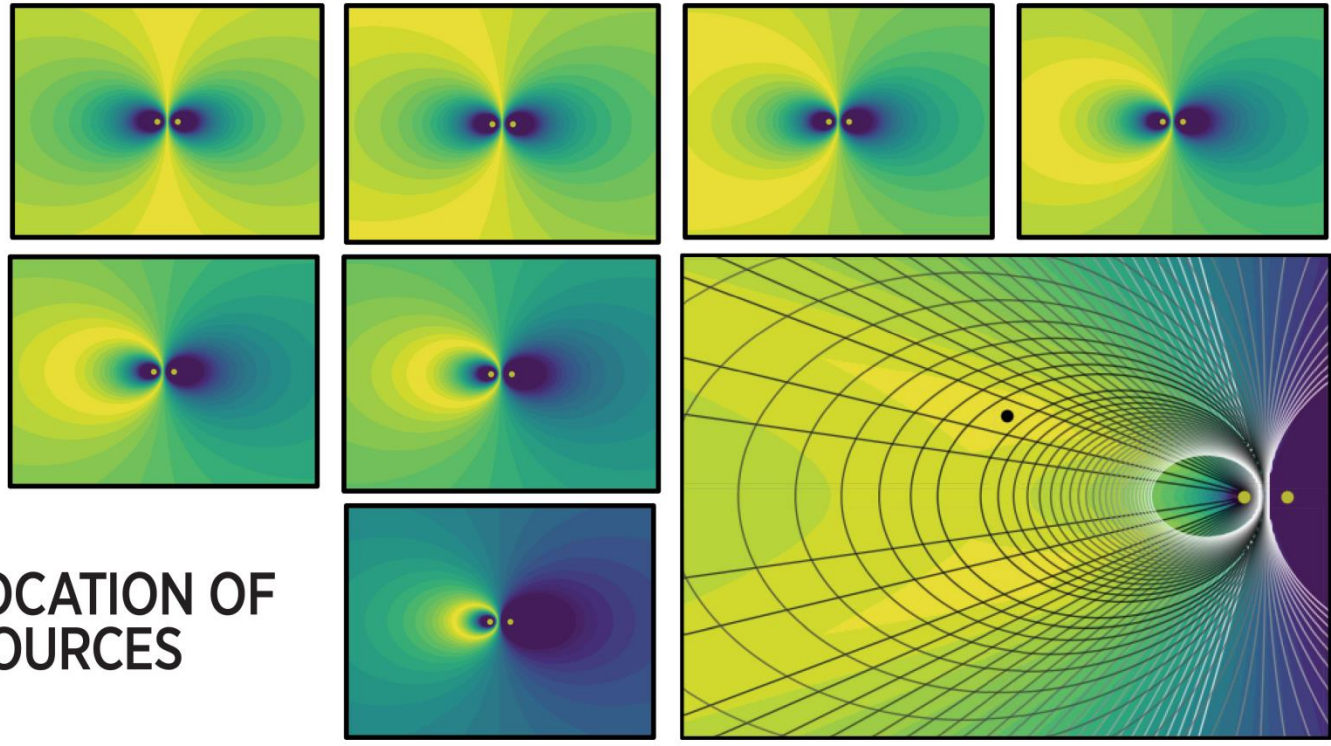
GPS | GALILEO | GLONASS | BEIDOU

Wed, Oct 30, 2019

10 a.m. PT • 12 a.m. CT

1 p.m. ET • 11 p.m. PT

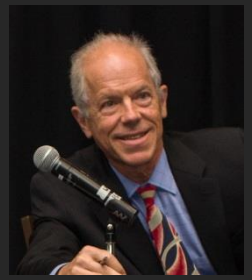




DETECTION AND GEOLOCATION OF GNSS INTERFERENCE SOURCES

WELCOME TO

Detection and Geolocation of GNSS Interference Sources



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Fabio Dovis
Associate Professor
Politecnico di Torino

Guy Buesnel
PNT Security Technologist
Spirent

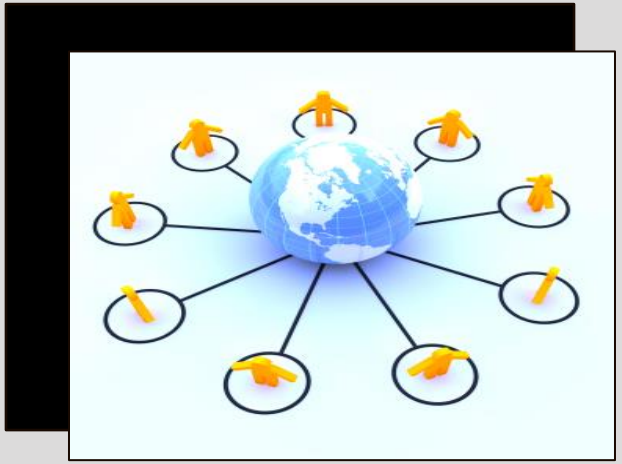
Paul Alves
Technology Manager
Correction Services
NovAtel

Co-Moderator: Lori Dearman, Executive Webinar Producer

Who's In the Audience?

A diverse audience of over 500 professionals registered from 47 countries, representing the following industries:

- 19% GNSS Equipment Manufacturer
- 15% System Integrator
- 16% Government
- 15% Professional User
- 14% Product/Application Designer
- 21% Other



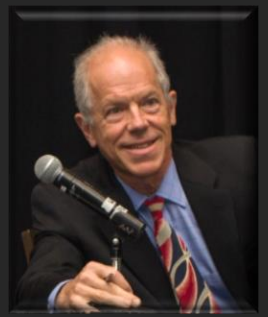
Welcome from *Inside GNSS*

Richard Fischer
Publisher
Inside GNSS
Inside Unmanned Systems

A Word from our Sponsor

Dean Kemp, PhD, MBA
Defense Segment Manager
NovAtel

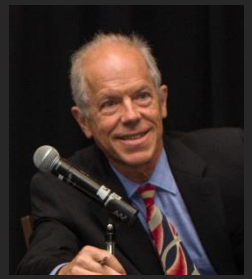
Today's Moderator



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Today's Panel

Detection and Geolocation of GNSS Interference Sources



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Fabio Dovis
Associate Professor
Politecnico di Torino

Guy Buesnel
PNT Security Technologist
Spirent

Paul Alves
Technology Manager
Correction Services
NovAtel

Co-Moderator: Lori Dearman, Executive Webinar Producer

Poll #1

How often have you personally encountered real-world GNSS jamming or spoofing in your work or application? (select one)

A. *Never*
B. *Once*
C. *2 to 4 times*
D. *5 times or more*

How easy is it to interfere GNSS consumer devices?

POLITECNICO DI TORINO

Dipartimento di Elettronica e Telecomunicazioni

Fabio Dovis
Associate Professor
Politecnico di Torino

Talking of Jamming and Spoofing

- In the past years regarding jamming and spoofing started to be considered as a potential serious threat for GNSS

> *«The spoofing of GNSS signals is a controversial and divisive topic within the satellite navigation community. Some believe that **spoofing is virtually infeasible,** while other industry insiders believe that **spoofing is actually trivial**.»*

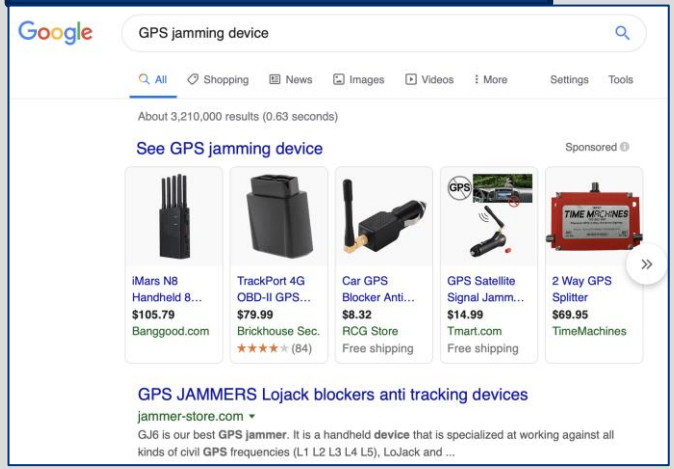
Curran J, Morrison A, O'Driscoll C. (In)Feasibility of Multi- Frequency Spoofing - Inside GNSS June 2018

- There are serious concerns for critical infrastructure and professional applications, that may be subject to structured jamming and spoofing attacks
- How realistic is the risk for consumer devices and applications?

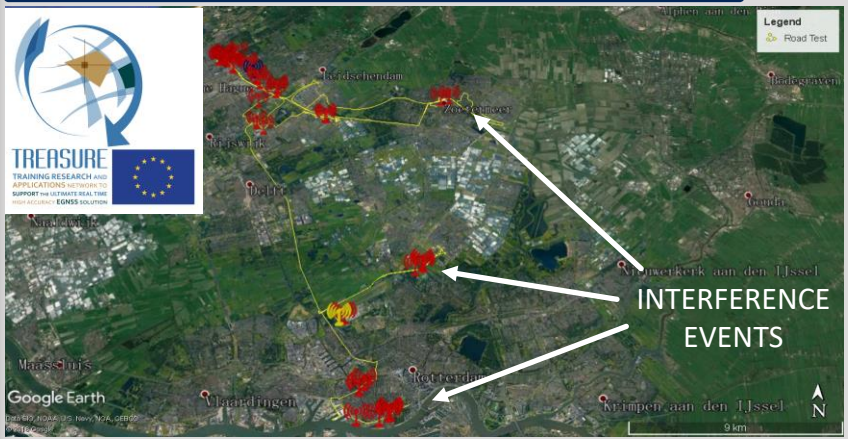
Popularity Index OF Jamming

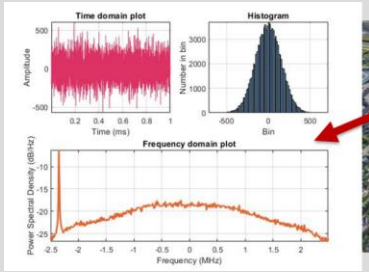
«*PERSONAL PRIVACY DEVICES*»
ARE INDEED POPULAR

EASY PURCHASE



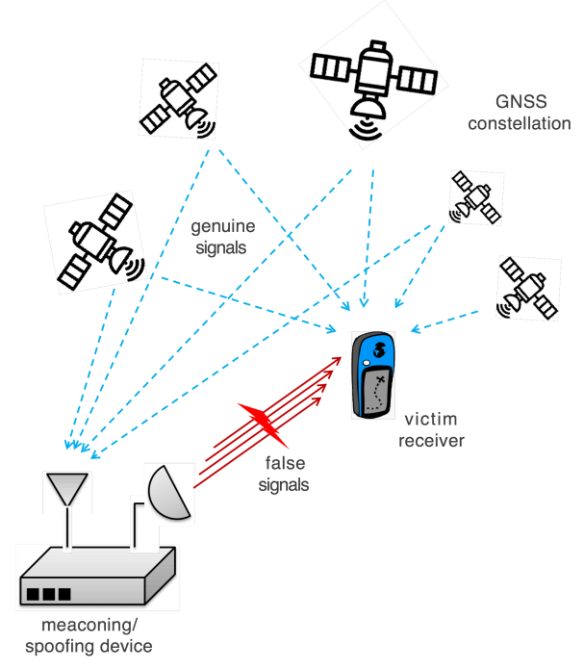
JAMMING CASES COMMONLY REPORTED





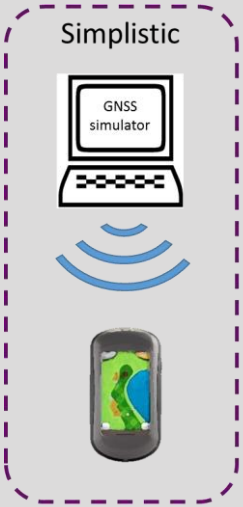
Spoofing VS. Jamming

- Jamming is not the only possible form of intentional interference
- RF spoofing attack deceives the target receiver with a **false copy of the GNSS signals**
  - More malicious than jamming: the false signals **take control of the target receiver** and the victim is fooled without any notice
  - Jamming is easily detectable
- Better have a deny of service than a fake position
- Attacks can be very effective depending on the quality of the generated signal

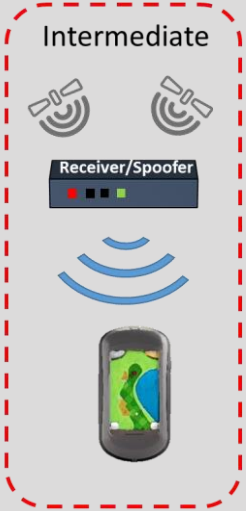


Picture taken from: D. Margaria, B. Motella, M. Anghileri, J.J. Floch, I. Fernández-Hernández, M. Paonni, Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives (2017) IEEE Signal Processing Magazine, 34 (5), art. no. 8026200, pp. 27-37

Spoofing Attacks



- signals **not consistent** with the satellites signals
- HW GNSS signal generator
- high cost and easily detectable



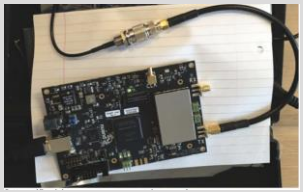
- signals **consistent** with the satellites signals
- requires a GNSS receiver
- lower cost and more difficult to detect

- signals **consistent** with the satellites signals
- requires GNSS receiver and multiple transmitting antennas
- high implementation complexity

Popularity Index of Spoofing

CHEAP TECHNOLOGIES FOR SIMPLISTIC/INTERMEDIATE SPOOFING

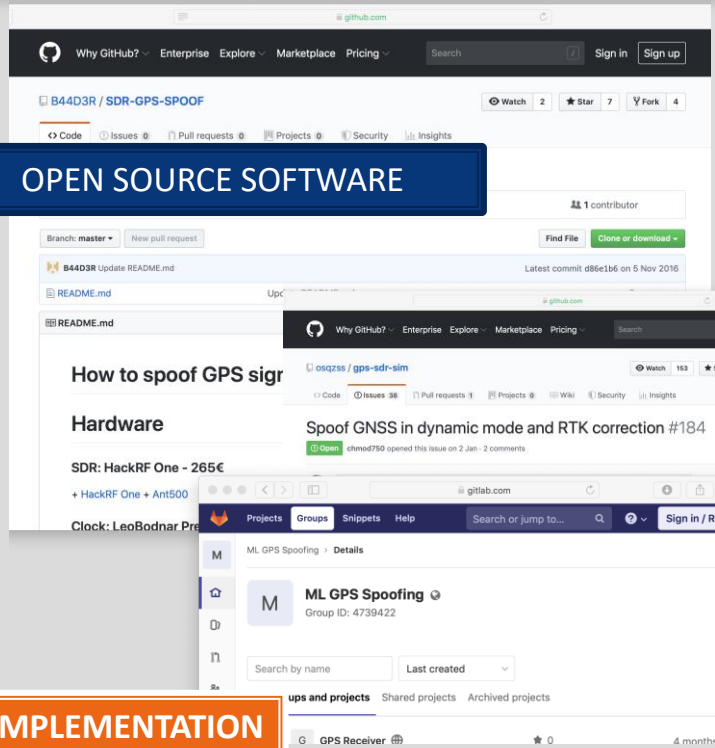
CHEAP HARDWARE AVAILABLE



SPOOFING IS FUN!

SPOOFING NEEDS ALSO A LOT OF KNOWLEDGE!

OPEN SOURCE SOFTWARE

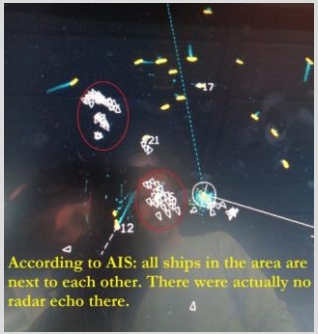


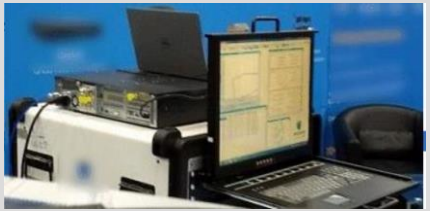
IMPLEMENTATION

USE

How Popular is the Spoofing?

- …If we don't consider very complex attacks requiring advanced capabilities and resources
- …If we dont consider ad-hoc attacks, and scenario built on purpose for feasibility demonstration
- …if we dont consider incidental, unintentional spoofing -> see ION GNSS+ 2017

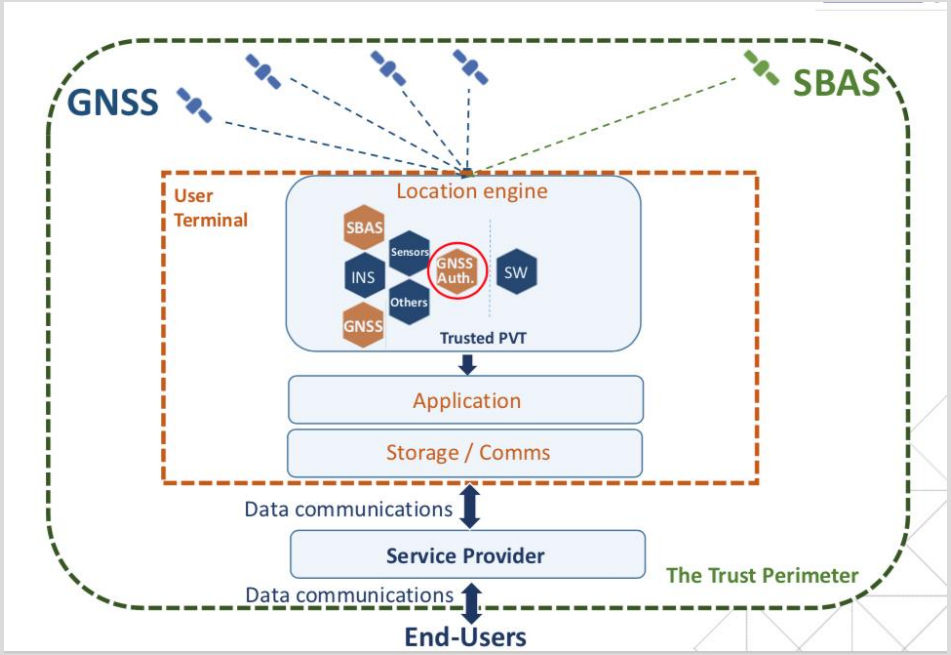


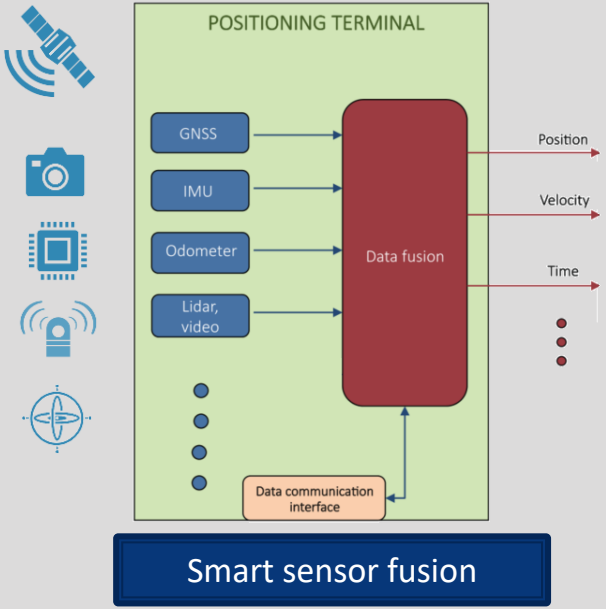


How likely is it to have effective spoofing of mass-market (consumer) equipment at GNSS signal level?

How robust are such devices to possible spoofing attacks?

- Mass-market devices are not pure GNSS receivers and more and more GNSS is just a part of them





Source: GSA

Insurance Boxes

Company claiming to have installed «Millions of boxes»

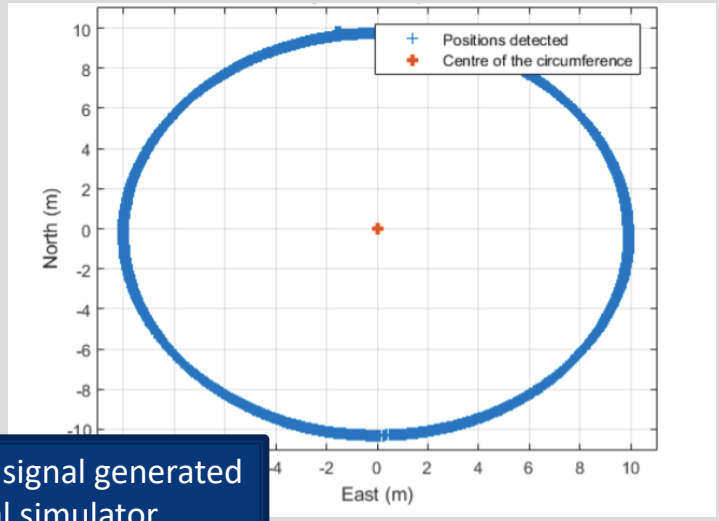
GNSS Unit

INS unit

Buffering window

COM Interface to data center

No protection against jamming



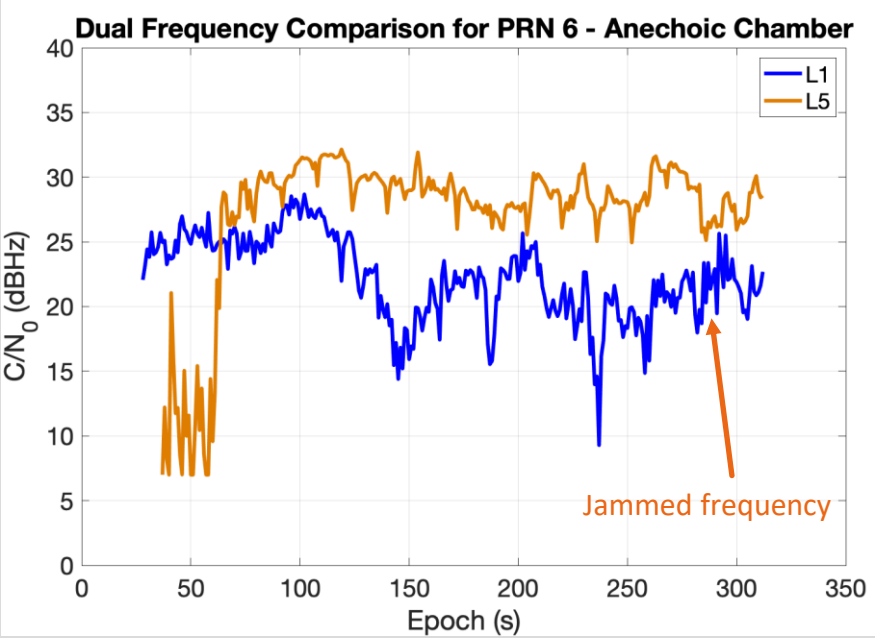
Static box fed with the signal generated by a simple GNSS signal simulator

NOTE: Image is not showing the actual box analyzed and it is just for illustrative purposes

Easily spoofable, not even cross-checks between INS and GNSS outputs

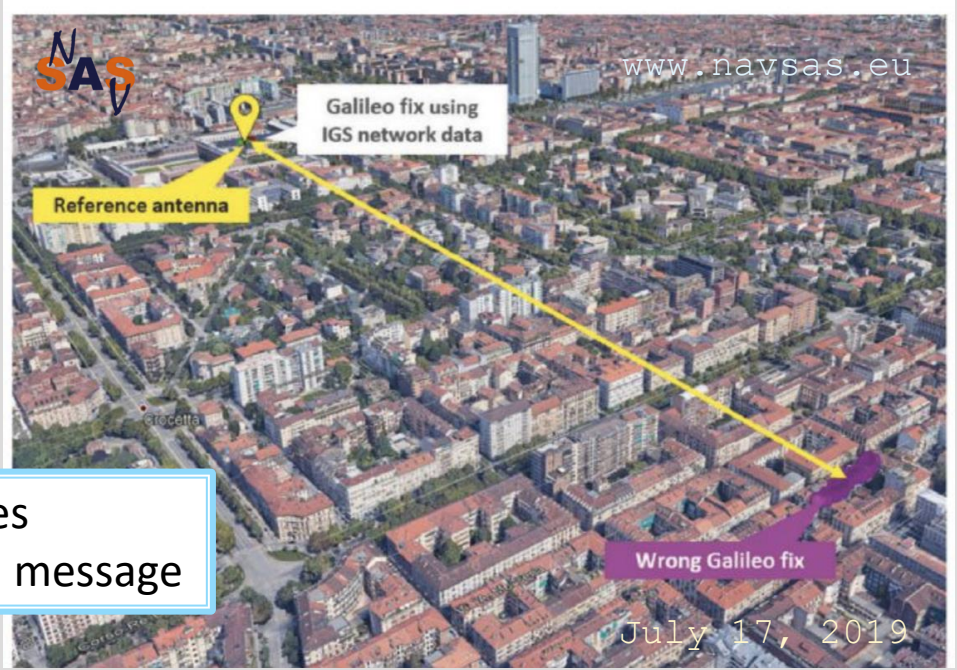
Smartphones Under Jamming (L1)

- With strong jamming power -> no solution
- Hard to find cases in which the position is significantly affected but not fully blinded
- Robustness of double frequency chipsets
- In Android if no ToW is obtained the data are not even logged.



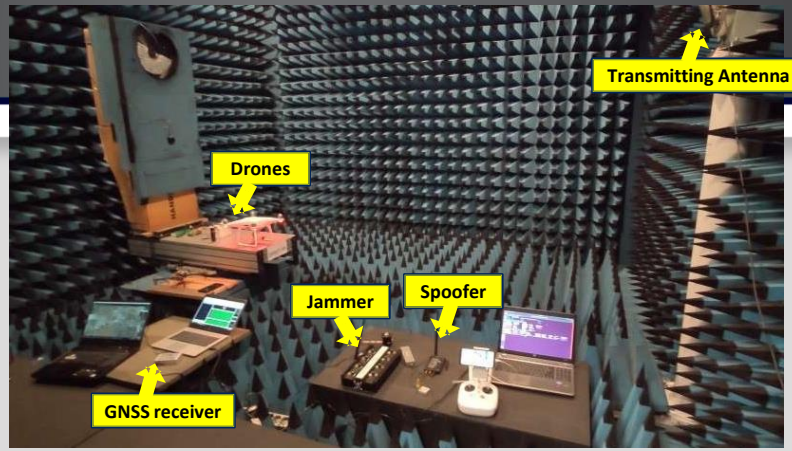
C/N0 values for a double frequency smartphone L1/L5 under attack of the swept-frequency jammer on L1

- During the Galileo outage in July 2019 all enabled smartphones we were observing were not providing any Galileo only solution
  - Basically impossible to force them to use the valid ephemerides retrieved from the IGS network
  - It is hard to bypass the retrieval of the almanac from the assistance network



It is not easy to force the smartphones to trust and use a spoofed navigation message

Jamming a Drone

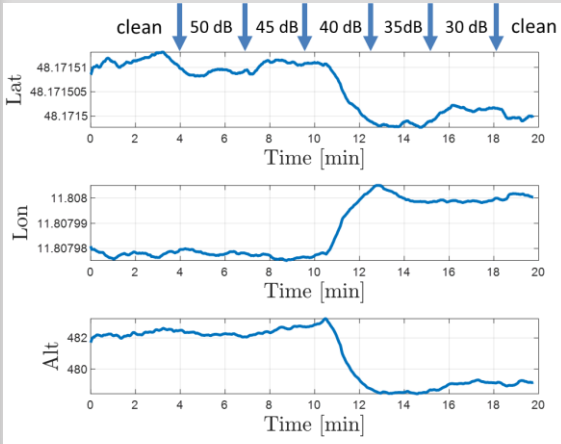


POLITECNICO DI TORINO

PIC4SeR

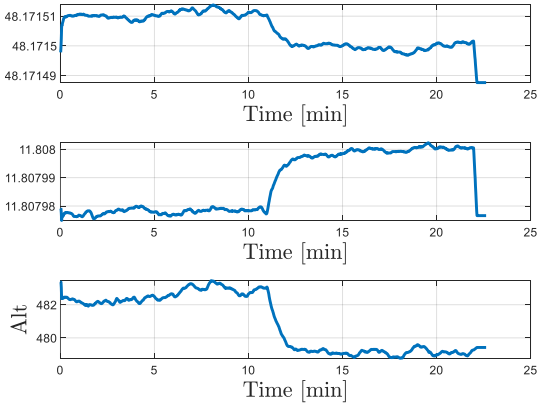
PoliTo Interdeprtmental Center for Service Robotics

Jamming attenuation

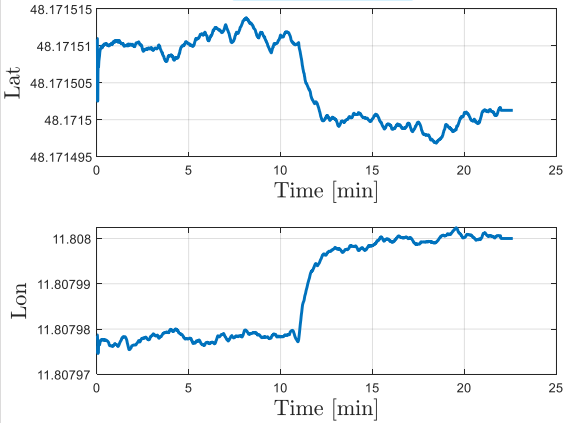


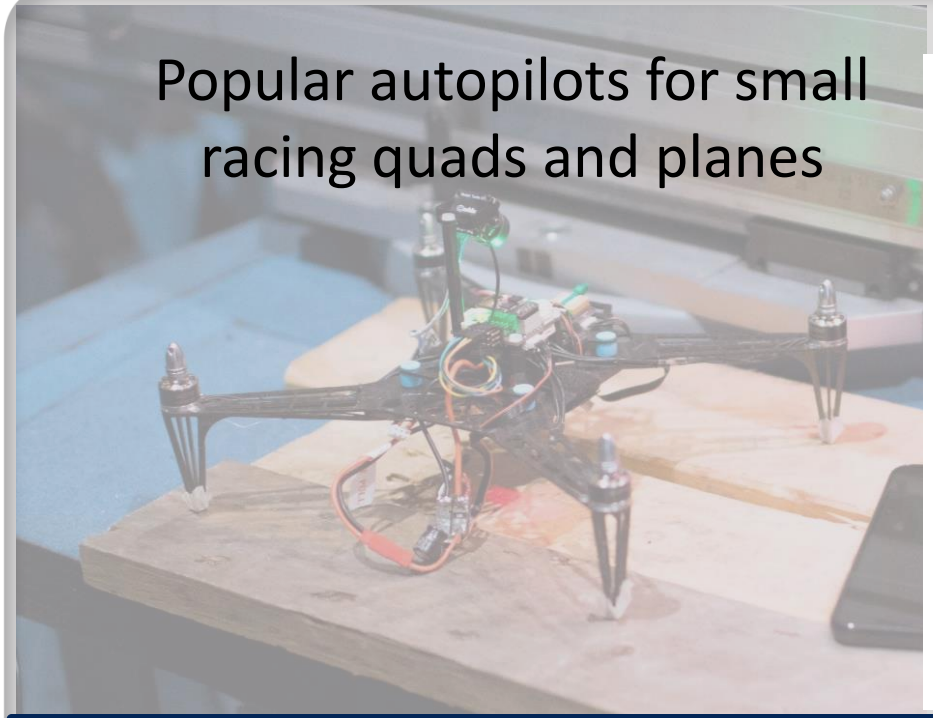
REFERENCE RECEIVER

GPS Unit

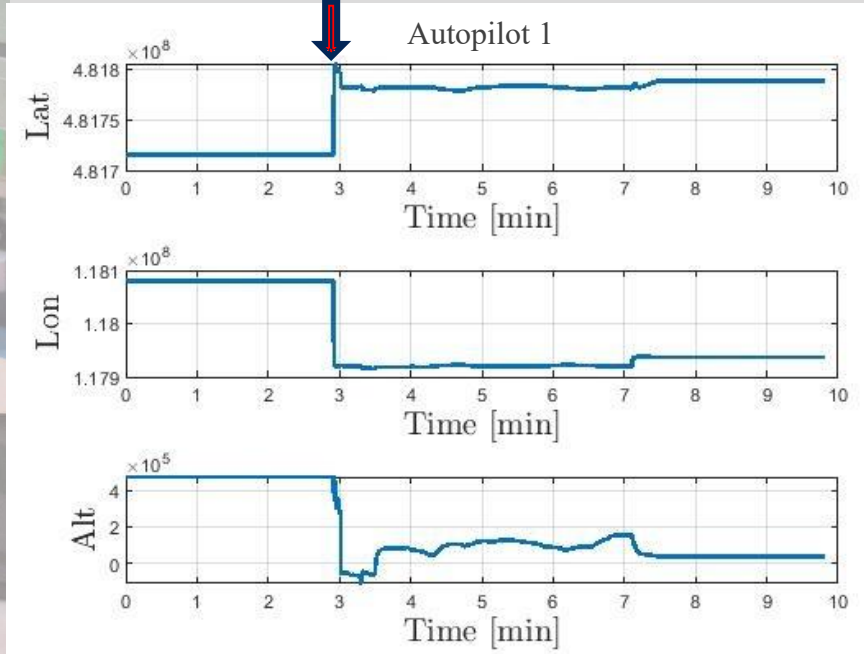


IMU Unit





Spoofing starts here



THE JAMMER BLINDS THE GNSS UNIT – AUTOPILOT IS BLOCKED
A HARD SIMPLISTIC SPOOFING ATTACK IS SUCCESSFULL

Spoofing Does Exist…

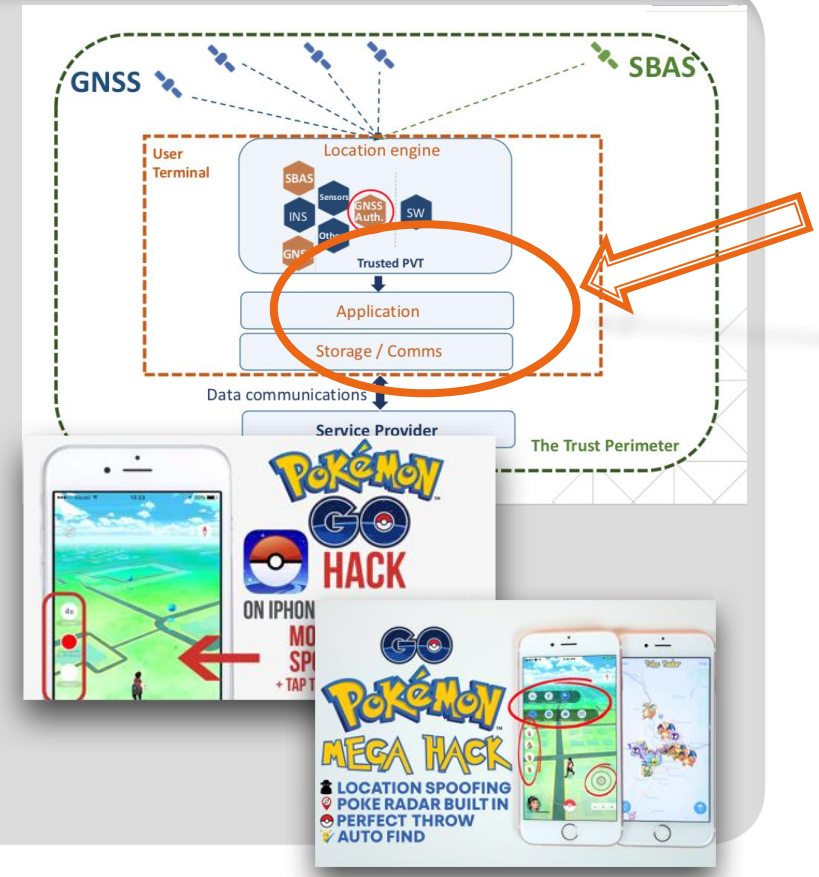
- It is already occurring nowadays
- Spoofing devices can be built in lab combining a software receiver and a simple RF front end
- Self-made spoofers might be used to launch effective attacks against civilian receivers in the near future, even if technical knowledge to create spoofers still not widespread

However…

- I am still undecided if spoofing is ***virtually infeasible***, or spoofing is actually ***trivial*** for **consumer equipments**, i.e. if spoofing at signal level is a real and realistic threat
- Consumer electronics may be weak to spoofing and be vulnerable.
  - **They should not be used** outisde of the «leisure» field for more serious and **critical applications**
- Whatever makes the signals more robust is welcome, but a simple **jammer** can cause sufficient damage

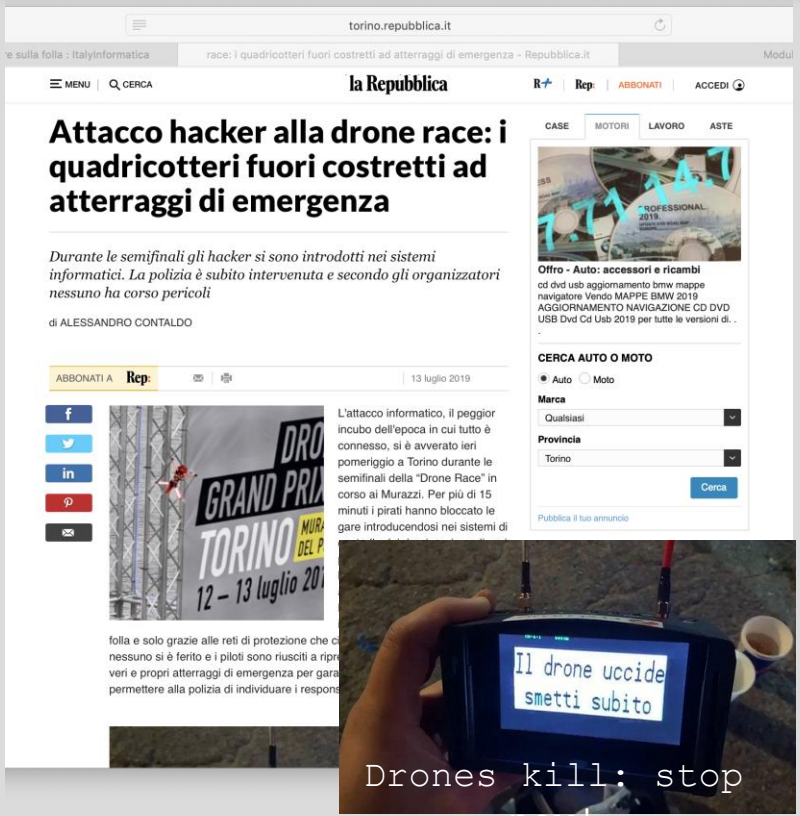
Conclusions

- **Multifrequency GNSS** chipsets for smartphones provide some robustness to jamming
- Smartphones are **hard to spoof at signal level**
  - Almanac is often downloaded from the network
  - A complex spoofing attack would have the same effect of a cheap jammer
- I would rather hire a **good cyber-hacker** than a GNSS specialist!
  - Replacing the position by a a man-in-the-middle could be easier than signal spoofing



Conclusions

- **Multifrequency GNSS** chipsets for smartphones provide some robustness to jamming
- Smartphones are **hard to spoof at signal level**
  - Almanac is often downloaded from the network
  - A complex spoofing attack would have the same effect of a cheap jammer
- I would rather hire a **good cyber-hacker** than a GNSS specialist!
  - Replacing the position by a a man-in-the-middle could be easier than signal spoofing



GNSS Interference sources – Impacts and Characterization (Part I)

Guy Buesnel
PNT Security Technologist
Spirent

spirent™
Promise. Assured.

GNSS Interference

Not just about low powered cigarette lighter jammers….

Adjacent band interferers

Nation State jamming

Drone disruptor

GNSS Interference now a reality in many commercial sectors
Example–Commercial Aviation

- Space-based position and navigation enables three-dimensional position determination for all phases of flight from departure, en- route, and arrival, to airport surface navigation
- Increasing reliance on GNSS for aRea NAV (en-route and approaches) GPS also an essential component for many other aviation systems, such as the Enhanced Ground Proximity Warning System (EGPWS) and ADS-B
- Interference to systems reliant on GNSS is a real issue–many recent examples of disruption…

Background…

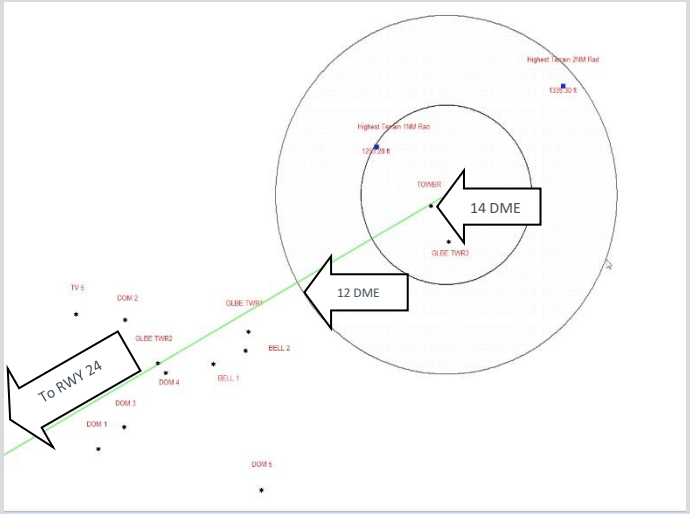
- More than 250 incidents of GPS disruption reported by pilots through NASA's Aviation Safety Reporting System (ASRS) since 2013
- 815 incidents of GPS disruption reported to Eurocontrol so far in 2018 (Europe and adjoining areas)
- Significant disruption can result – missed approaches, delays, cancellations….

Typical Flight Crew report
17-JUL-16, Ben Gurion International Airport, Israel
During the GEFFEN 1C Arrival/ILS X RWY 26, we experienced intermittent GPS/ADS-B Signal Interruption due to NOTAM military operations present in the Tel Aviv FIR. Just as we were about to intercept the RWY 26 localizer, we had a Nav Unavailable RNP. Since we were in VFR conditions with 8 miles visibility and the airport area in sight, we continued to intercept the localizer and proceeded to a normal landing. There was some map shift note as compared to the localizer course raw data.

Case Study – Nina Aquino International Airport (NAIA)

Multiple reports of GPS interference on approach to Runway 24 at Manila International Airport More than 50 reports in the 2nd quarter of 2016

Loss of on-board GNSS functionality
[GPS-L INVALID] and/or [GPS-R INVALID] messages appear.
Decrease in navigation performance leading to RNP alert through increasing aircraft horizontal error, Actual Navigation Performance (ANP) decreases beyond RNP requirement. – [NAV UNABLE RNP] message appears.
This sometimes has led to missed approaches



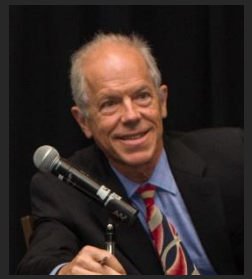
in some aircraft, navigation reverted to inertial (IRU) or DME/DME after GNSS loss. Impact on Navigation Display a large “map shift” was observed. Impact on GPWS - [TERR POS] and [EICAS TERRAIN POSITION] messages appear.
Loss of auto-land and ADS reporting capabilities

Case Study – Nina Aquino International Airport (NAIA)

- First suspect was a TV broadcasting station tower
- Second suspect two Cellphone towers - both initially indicated emitting transmissions on the GPS frequency itself
- Third suspect was another Digital TV broadcasting station
- The Digital TV broadcasting station (Suspect Three) was repaired after bullet damage was discovered–The GNSS interference then ceased
  Aircraft operators resumed utilization of RNAV approaches to both runways in August 2017

(details published in ICAO information paper FSMP-WG/5 IP/9) 2017-09-07

Ask the Experts



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Fabio Dovis
Associate Professor
Politecnico di Torino

Guy Buesnel
PNT Security Technologist
Spirent

Paul Alves
Technology Manager
Correction Services
NovAtel

Poll #2

Which of the following are you most concerned about?(select one)

A. Intentional/malicious jamming

B. General wireless communication interference

C. Self-induced system interference

D. Another type of interference not mentioned above

E. None

GNSS Interference sources – Impacts and Characterization (Part II)

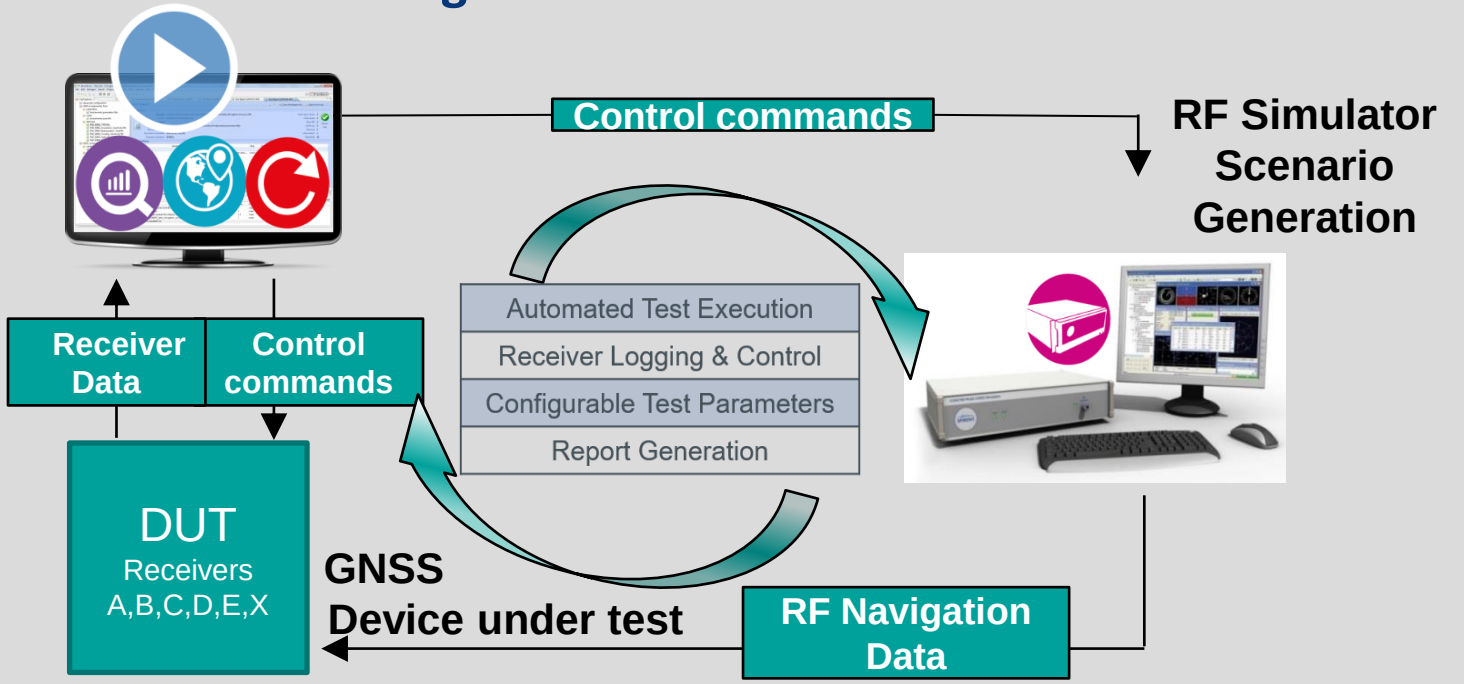
Guy Buesnel
PNT Security Technologist
Spirent

spirent™
Promise. Assured.

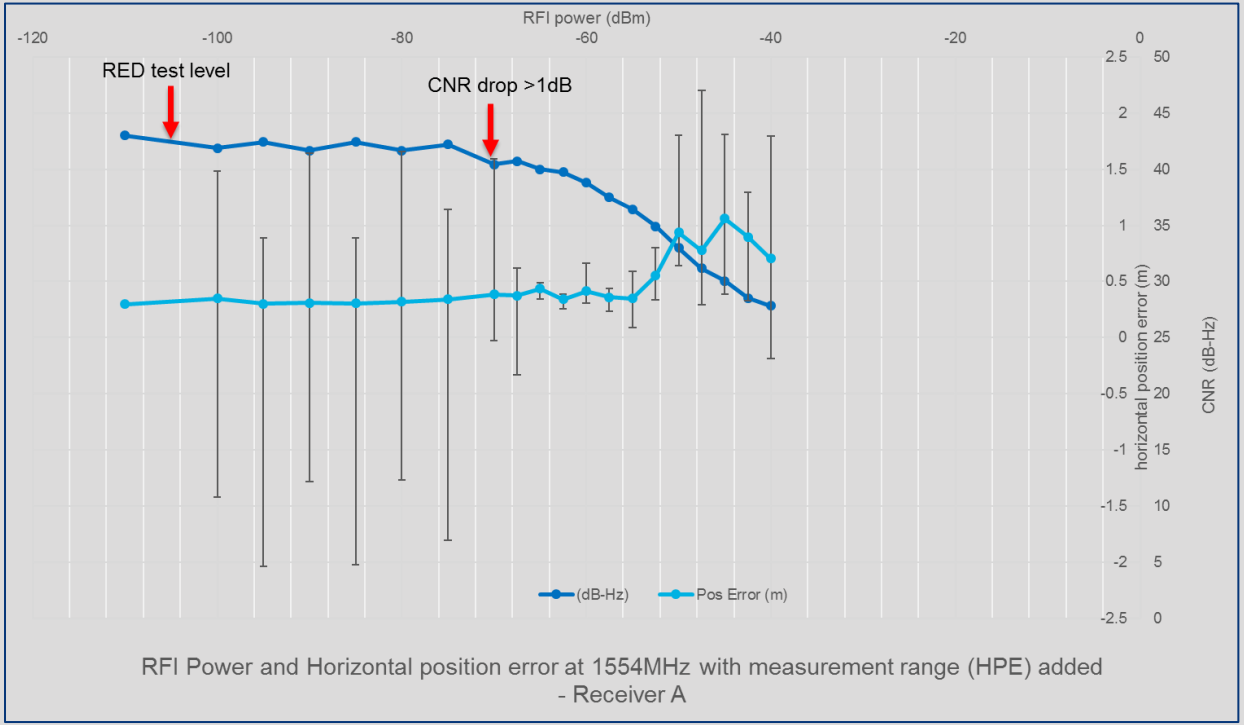
GNSS Interference – evaluating impact on receivers

- Relatively easy to emulate different interferer types – as long as can generate sufficient J/S – and inject into simulation
- Also possible to record and replay RF environment (recorder needs high enough bit depth to capture interference as well as GNSS signals)
- Allowing a 1 dB decrease in C/N0 due to the aggregate interference from all non-RNSS sources equates to limiting the aggregate interfering signal power to 6 dB below the noise level of the GPS receiver
- Use of 1dB decrease in C/N0 has long and well-established history as most appropriate metric for GPS Interference Protection Criterion (IPC) – in international use (including EC RED GNSS Adjacent Band Compatibility testing)
- Receiver parameters like HPE/TTFF all require a “harmful” level of interference to be injected into receiver (not really a level playing field….)

Evaluating Impact of 1dB C/N0 decrease on a selection of GNSS Receivers using PNT Test Bench

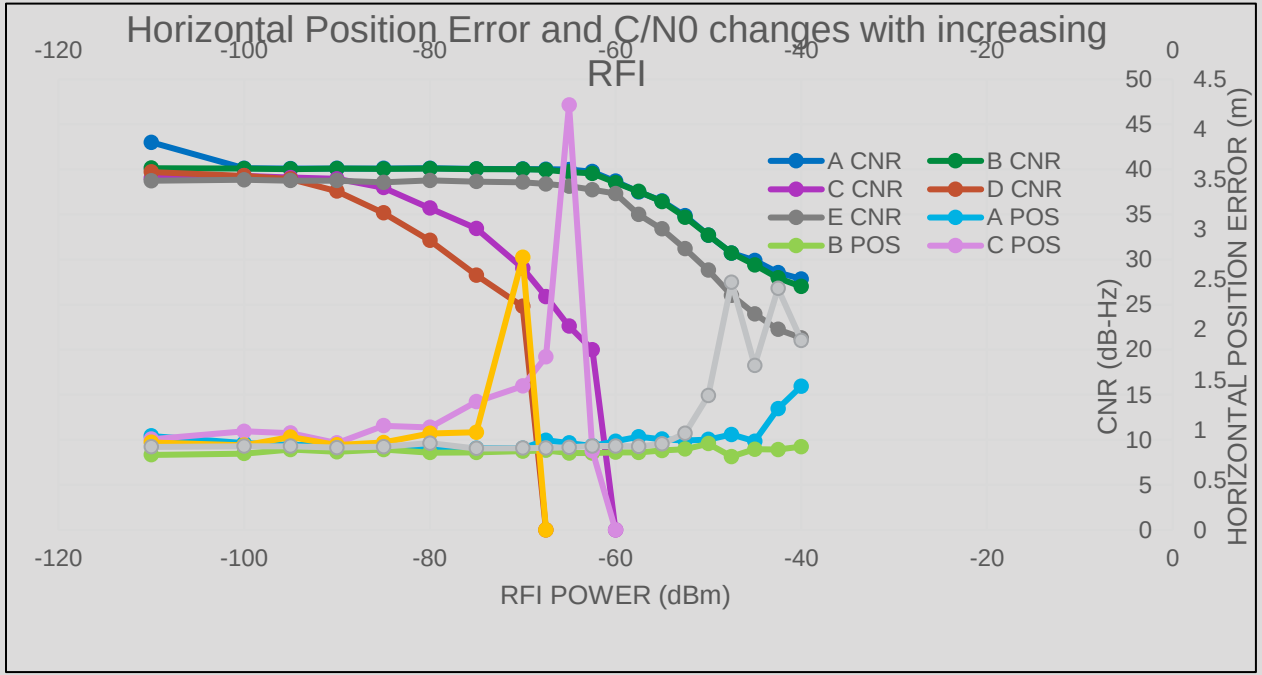


RFI effects on C/N0 and HPE – Single Receiver



RFI Power and Horizontal position error at 1554MHz with measurement range (HPE) added - Receiver A

RFI effects on C/N0 and HPE – 5 GNSS Receivers tested in lab



- 1554 MHz Out of band RFI
- C/N0 drop off (for all 5 Receivers) occurs before HPE starts to fluctuate..
- Some Receivers clearly much more susceptible to the RFI than others….

Insights

- Effects of GNSS interference being experienced in many application areas
- Most often the interference is collateral – not targeted
- Need for risk assessment when deploying GNSS dependent systems – unexpected behaviour likely to result otherwise – impacts can be very significant
- Our test results confirm that under test conditions a 1dB degradation in C/N0 is always a precursor to reduced or erratic performance (HPE etc…) in GPS receivers so it is a good metric to use when evaluating Receiver performance under RFI
- There is a need to detect and locate sources of GNSS interference in a timely manner where disruption occurs

How to locate GNSS interference?

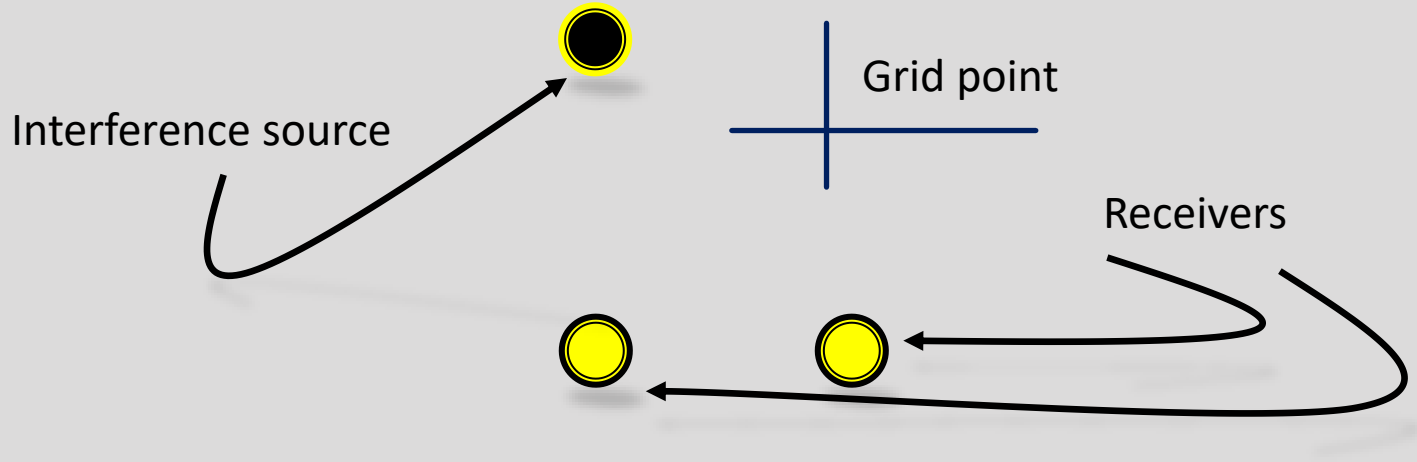
Paul Alves
Technology Manager
Correction Services
NovAtel

Interference Finding Techniques

- Angle of Arrival (AOA) or Direction of Arrival (DOA)
  - Antenna array is used to determine the phase offset of the signals.
    - E.g. NovAtel GAJT-410
- Time Difference of Arrival (TDOA)
  - Front end data from multiple receivers is correlated to estimate the time offset between the signals.
    - E.g. NovAtel OEM7 Sprinkler
- Power Difference of Arrival (PDOA)
  - Received power from multiple receivers is compared to estimate the range to the transmitter.
    - E.g. NovAtel ITK

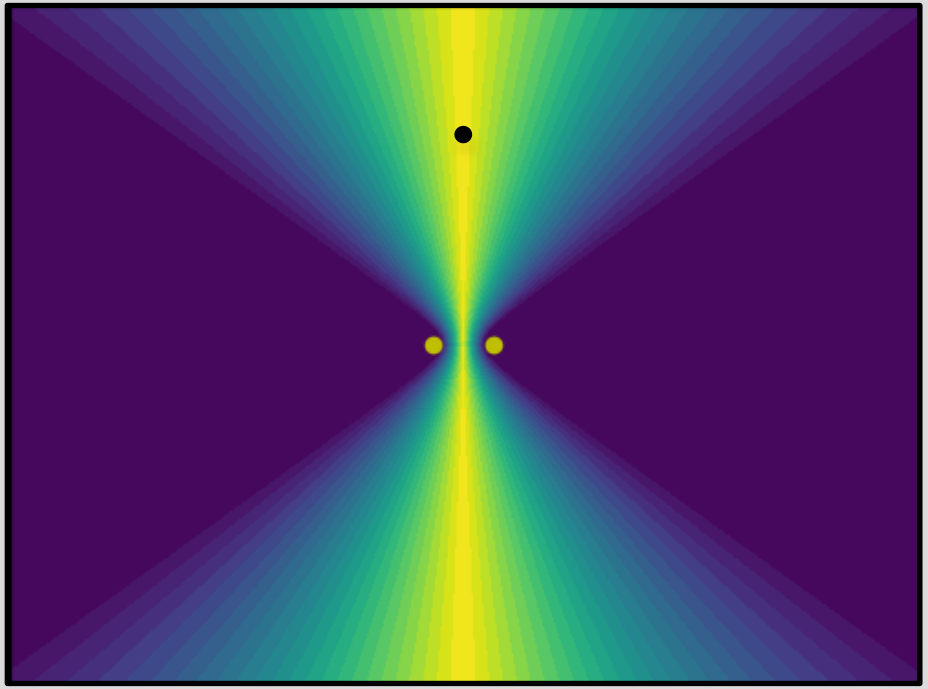
We can see what information we get from these measurements.

1. Determine the location of receivers and transmitters.
2. Calculate the time and/or power difference at the receivers.
3. Create a grid
4. For each grid point calculate the time and/or power difference from this location.
5. Plot the RMS agreement between the actual (calculated in 2.) and the measurements from this location.

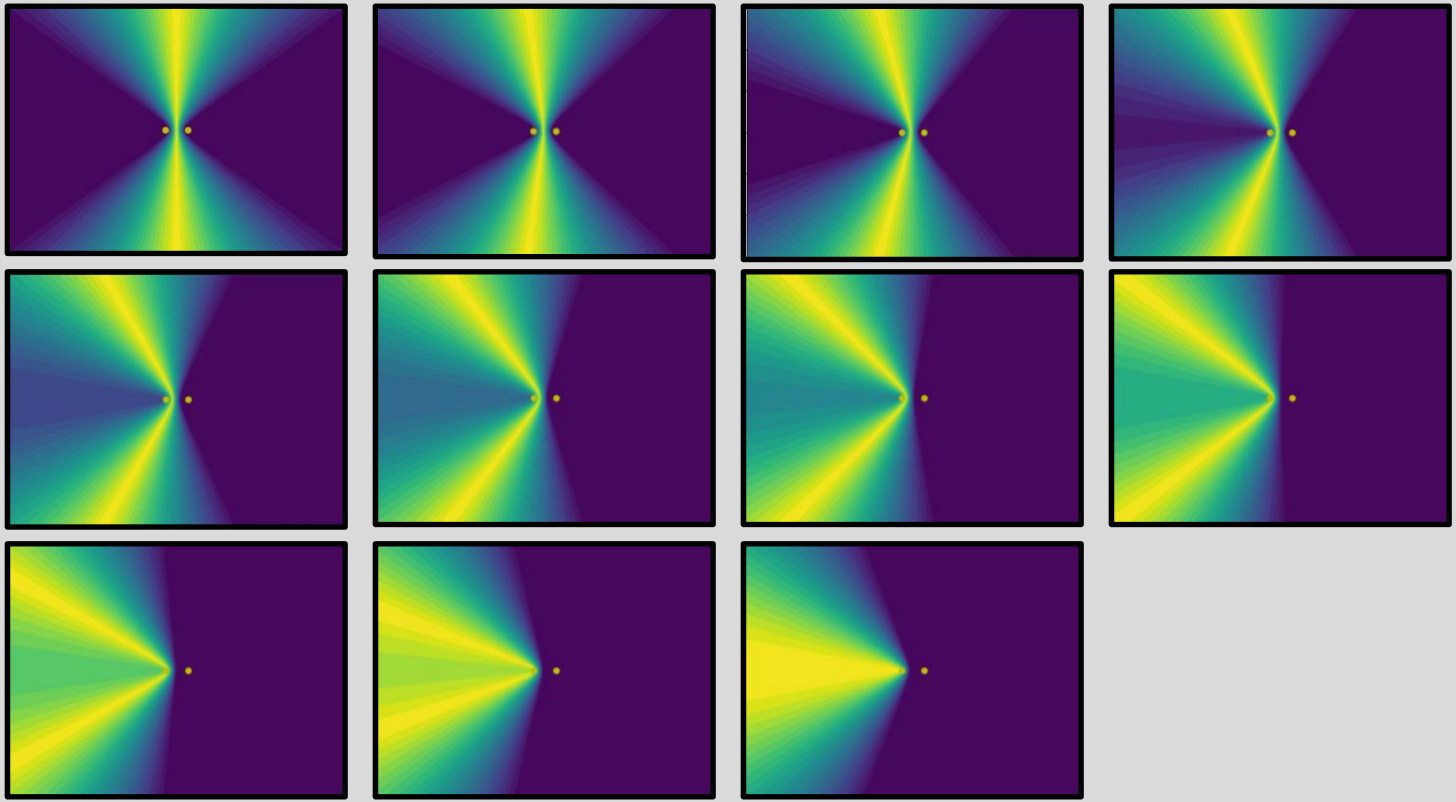


Time Difference of Arrival

- Yellow dots are receiver locations.
- Black dot is the interference source location.
- The contour is the agreement between measurements from that location and the measurement from interference source to receivers.
- Lighter mean more likely and darker is less likely.



Time Difference of Arrival



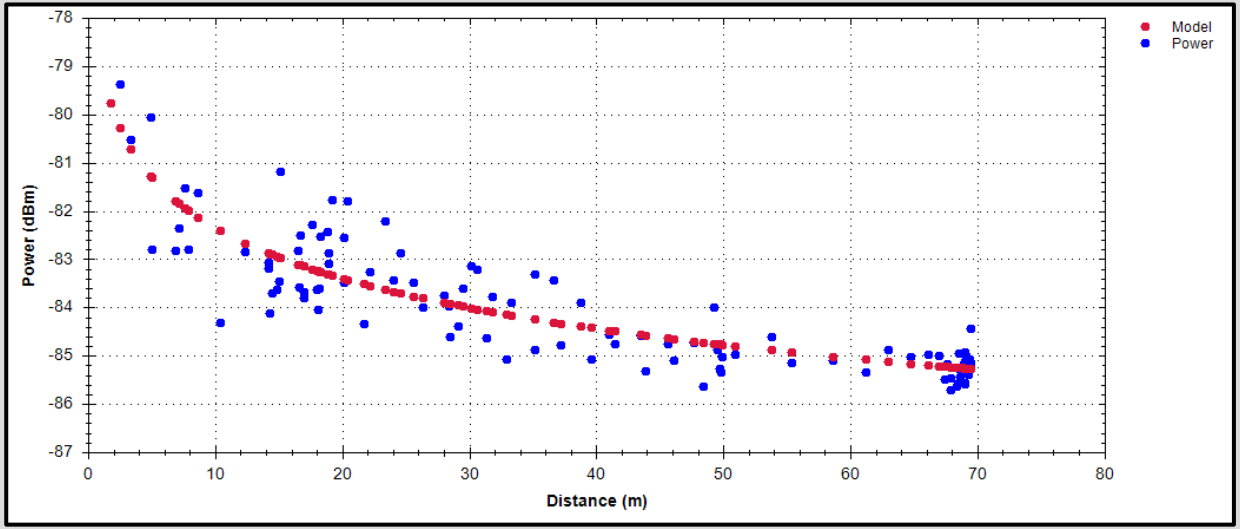
Free space loss

$$P_r = P_t - 20\log(d) - 20\log(f) + 147.55$$

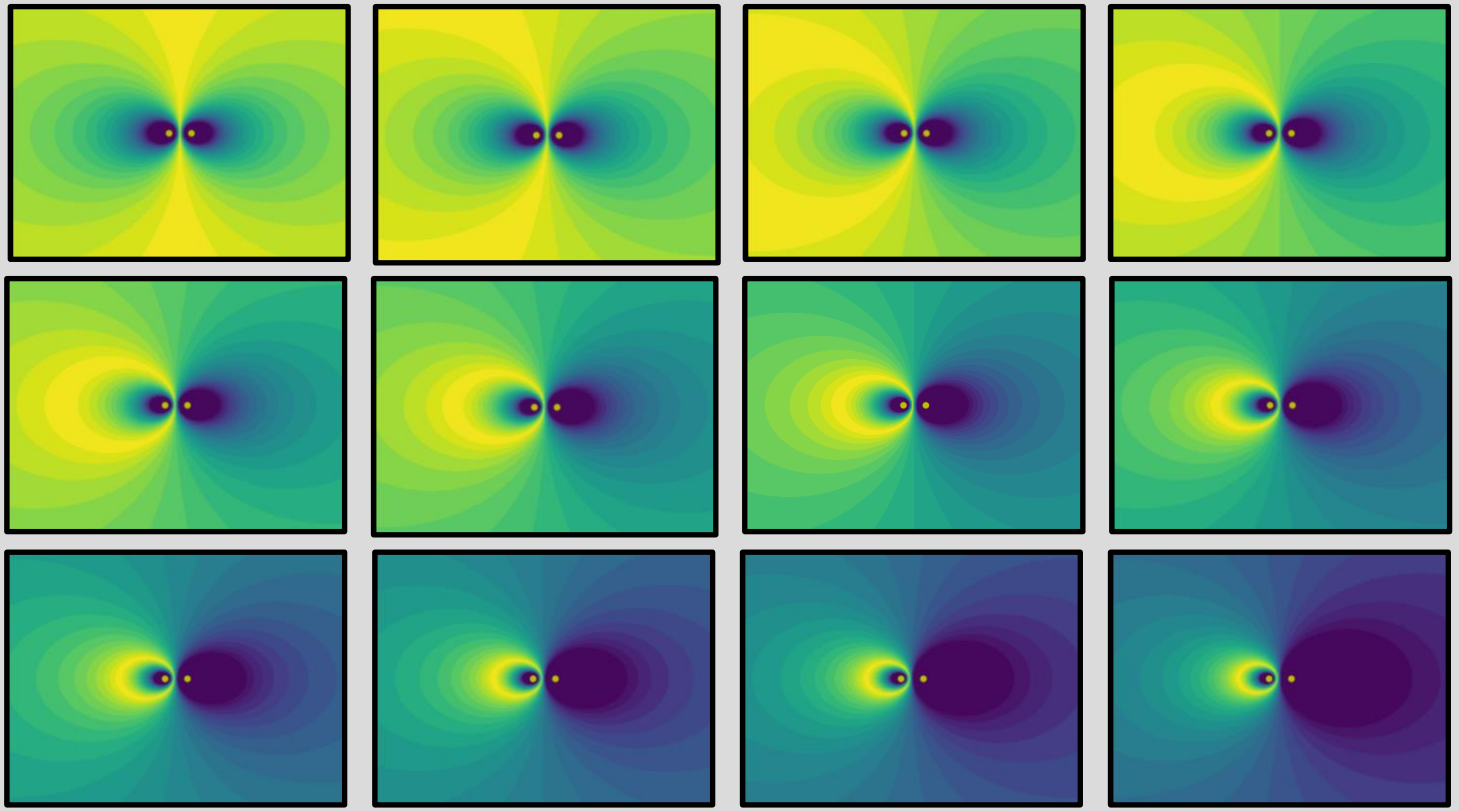
Where,

- P_r - received power
- P_t - transmit power
- L_p - power loss function
- d - distance
- f - frequency

Actual power loss

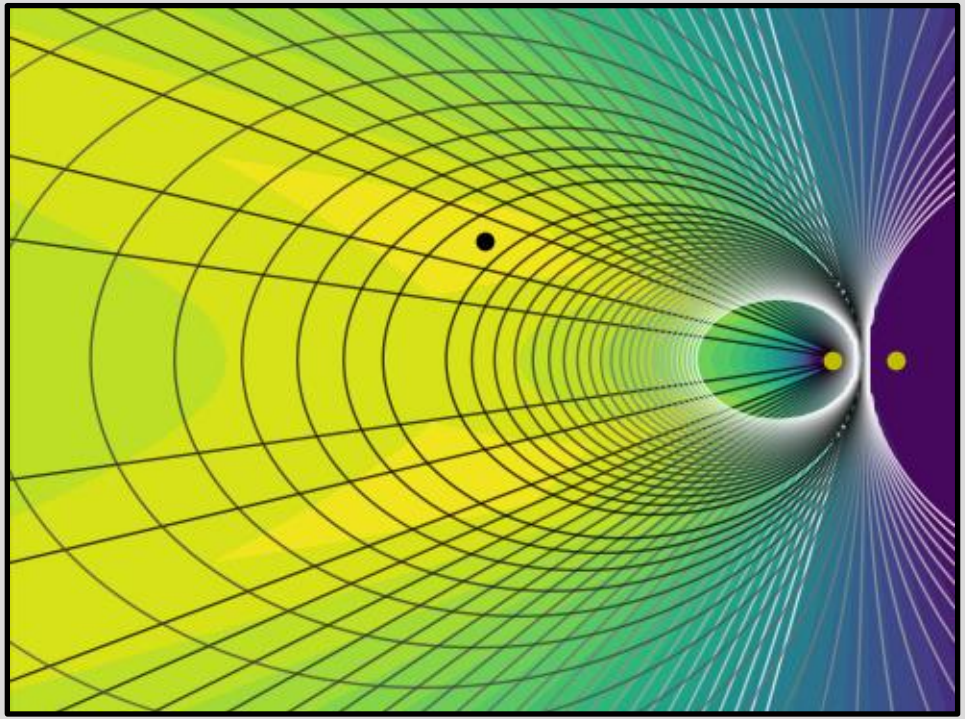


Power Difference of Arrival

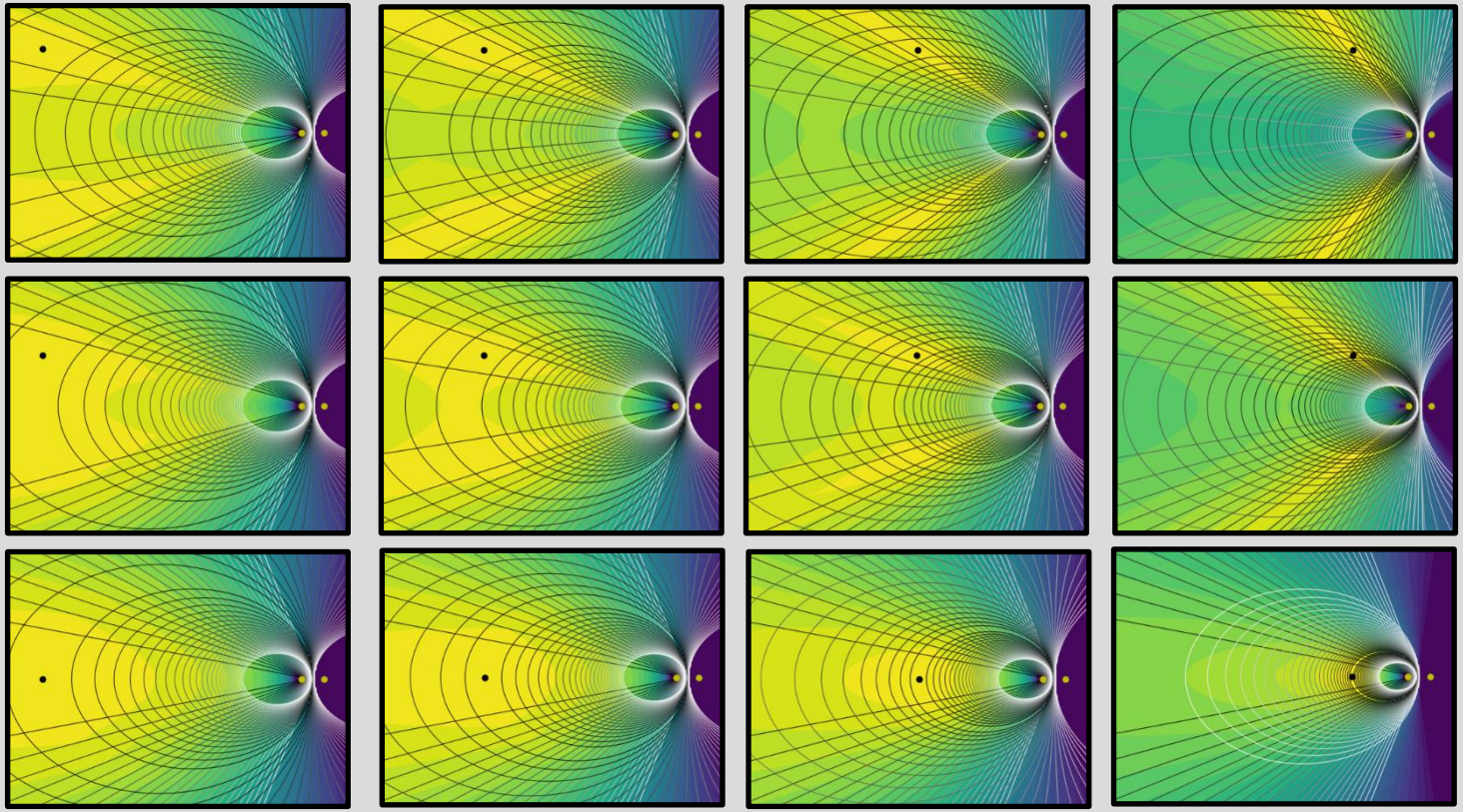


Time and Power Difference of Arrival

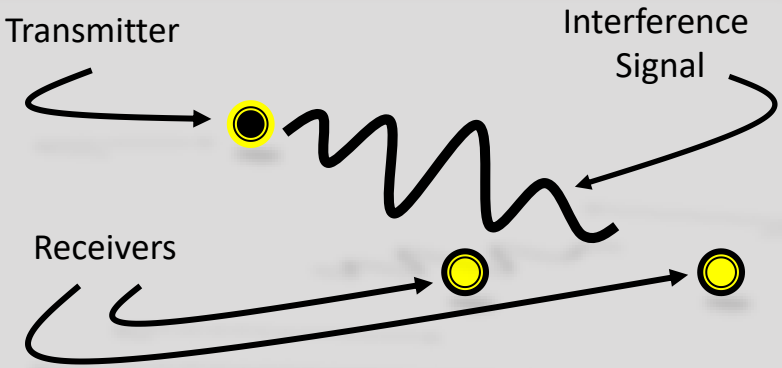
- Measurements can be combined.
- The straight lines show the TDOA measurements where darker is more likely.
- The curved lines show the PDOA measurements where darker is more likely.
- The contour plot shows the combined location likelihood with lighter representing more likely.



Time and Power Difference of Arrival



GPS Rx time tagging of ‘pre-correlation” data

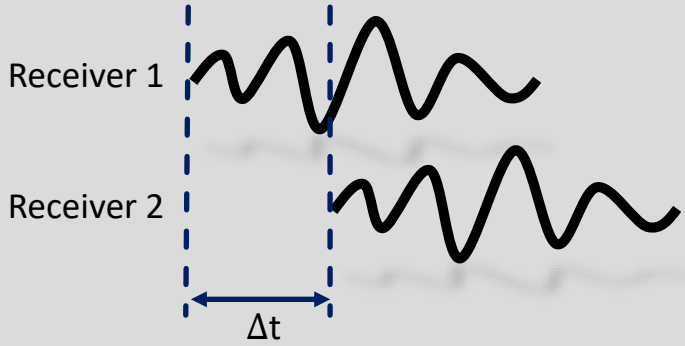


Prototype code name “Sprinkler” circa 2014

- Small snapshots of data every second
- Custom firmware on production OEM628 receiver card
- 1 bit complex data from single post-decimated RF path
- Snapshots of 64k samples every 1 second
- 5.6 ms at 12.5 million samples per second
- Choose from GPS L1, GPS L2, GLONASS L1, or GLONASS L2

Sprinkler is available on OEM7.

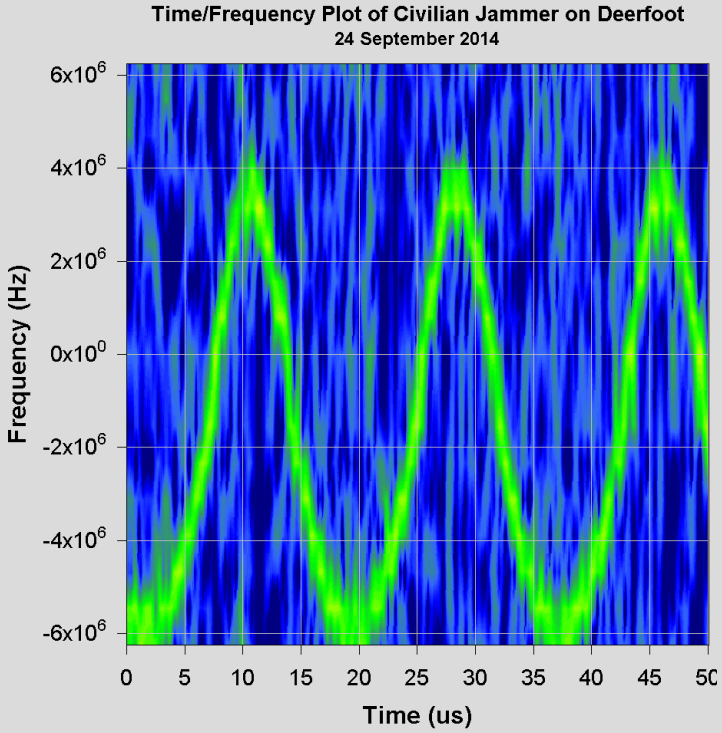
Special firmware is required



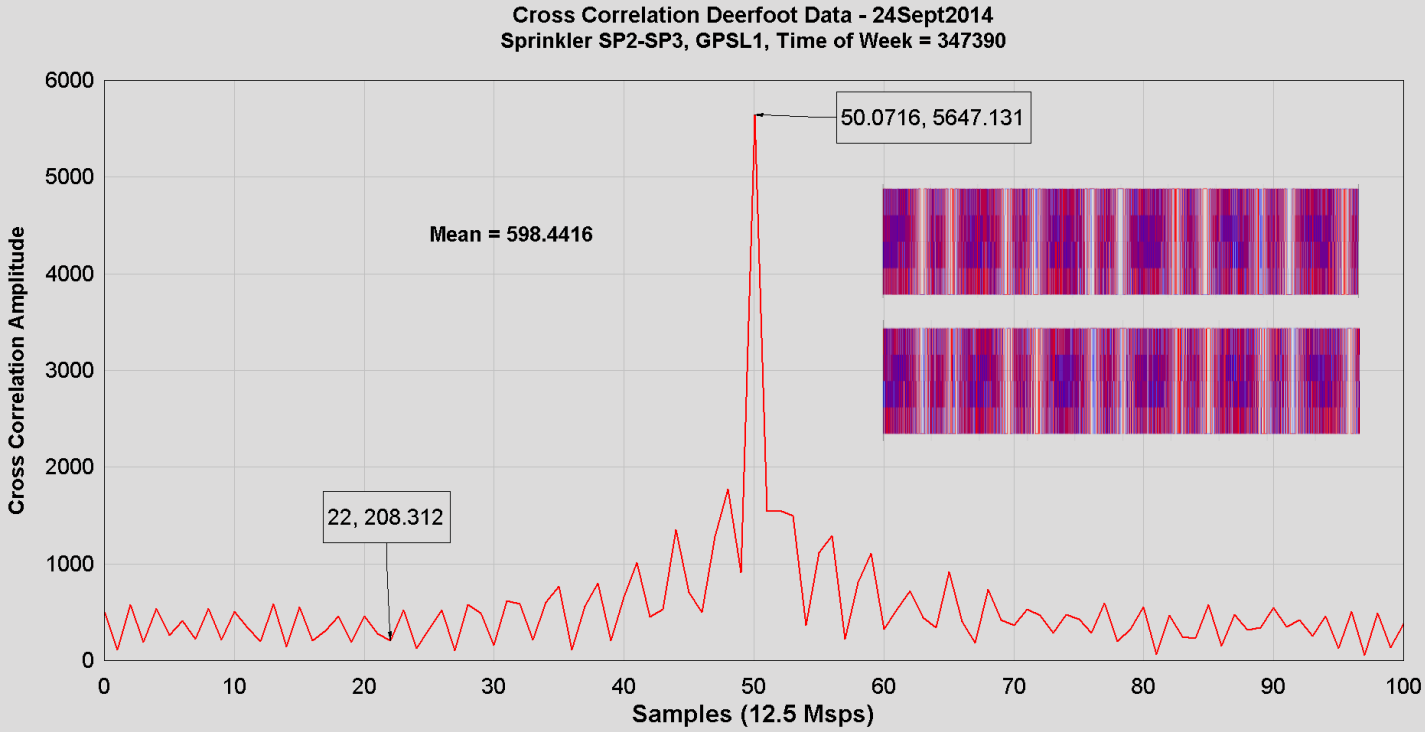
Detection Array – Both Sides of Deerfoot Trail

Civilian Jammer

- Intentional Jammer
- Civilian Style
- Chirp Type Jammer
- 58 KHz repetition
- L1, 1 MHz offset
- 10 MHz Wide

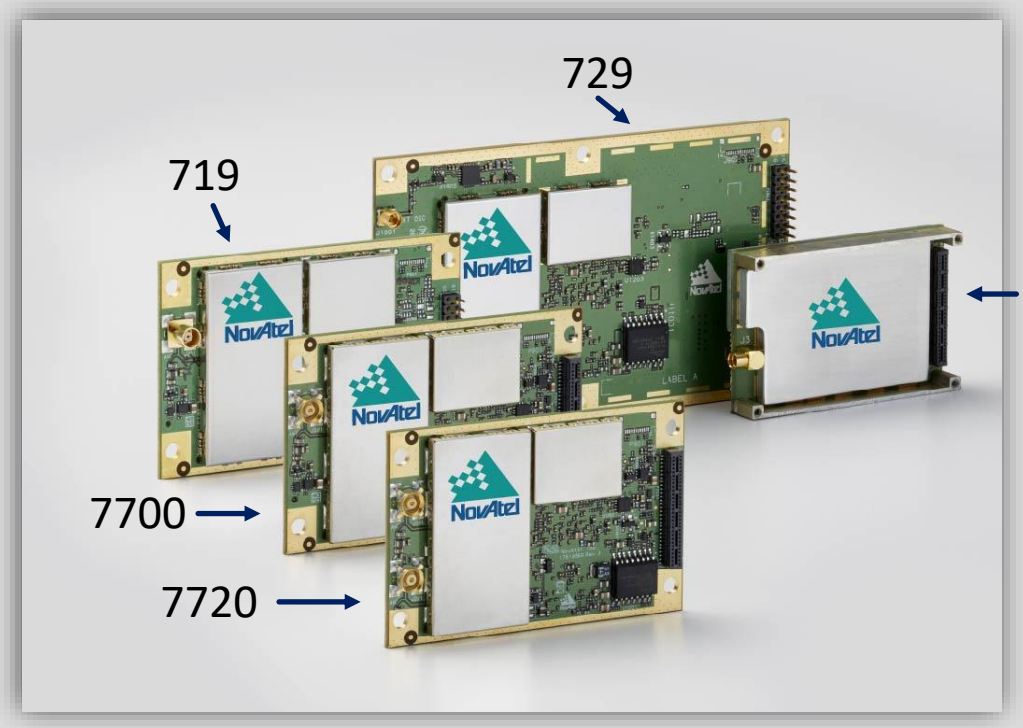


Cross-correlation of I/Q data from Rx #2 and Rx #3



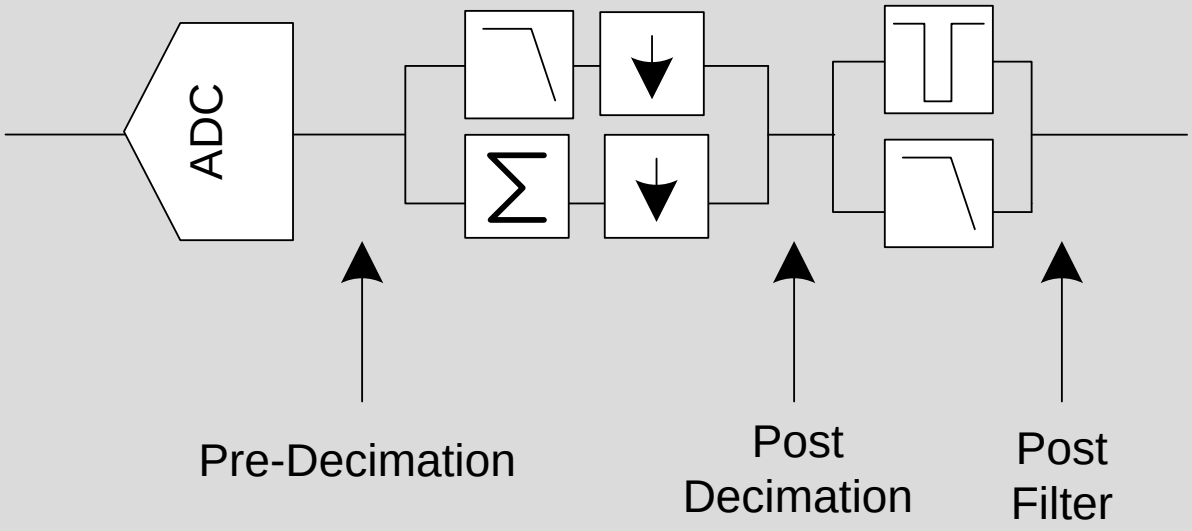
Probable Jammer Host Vehicle 18:29:32.5

Probable Jammer Host Vehicle 18:29:33.5

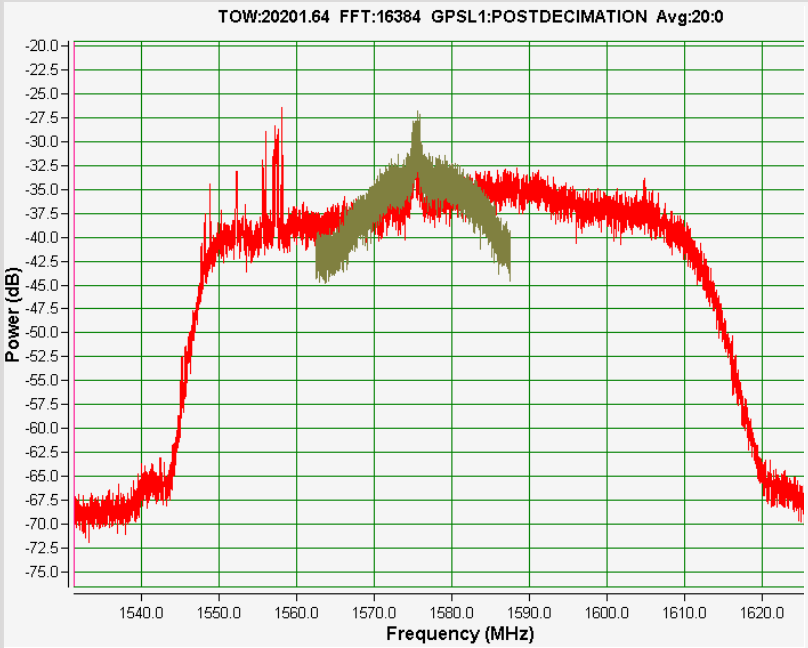


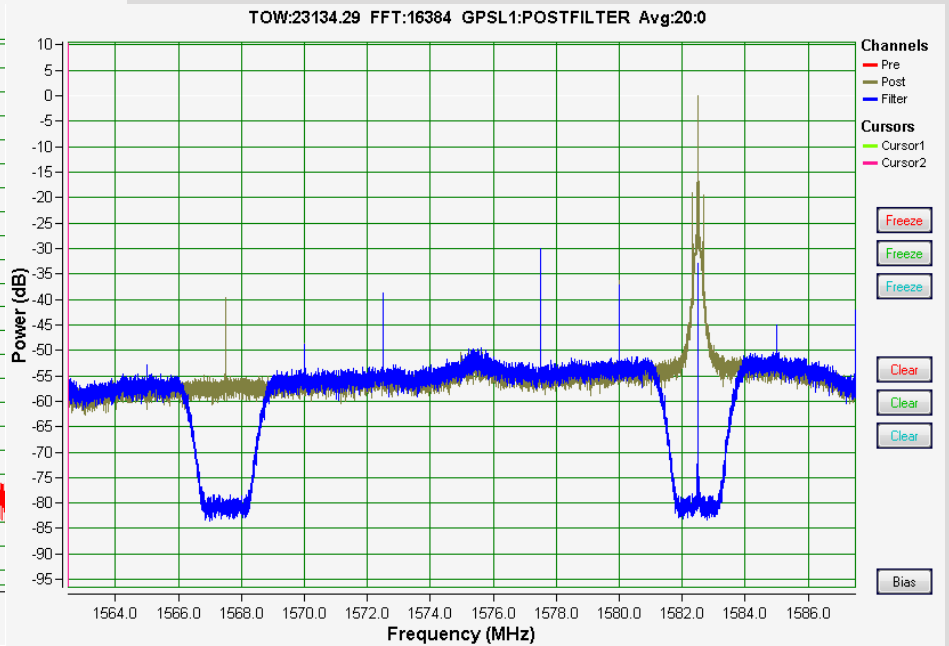
Interference Toolkit (ITK)

Spectral Analysis



Power Spectrum Examples



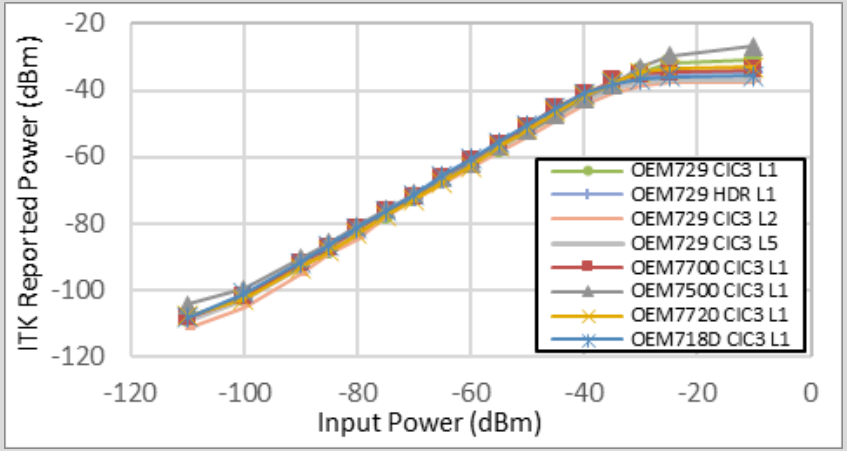


Automatic Gain Control (AGC) vs ITK Absolute Power

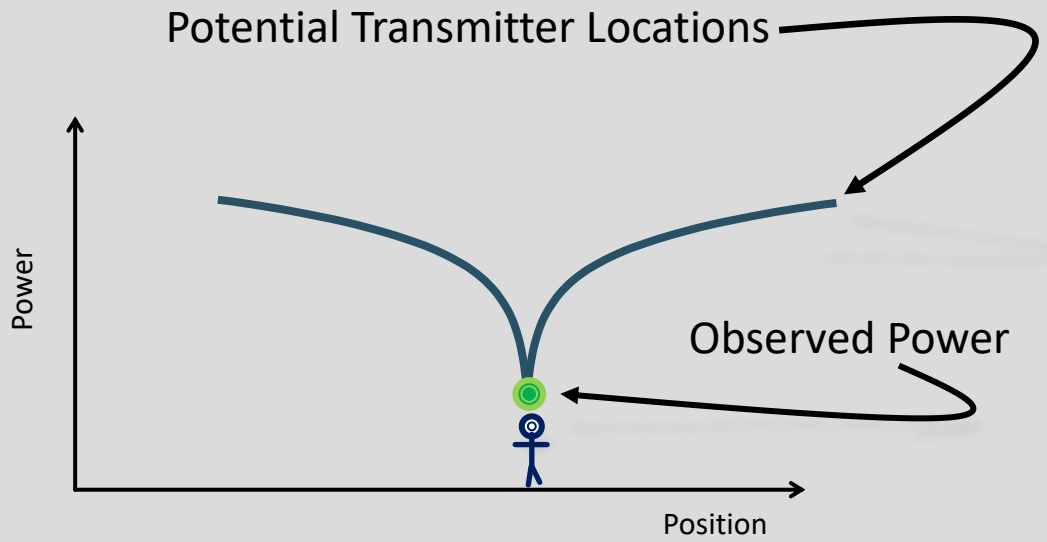
ITK provides absolute power within 5 dB accuracy independent of:

- Temperature
- Receiver design
- Interference type
- Interference frequency band (in-band/out-of-band)
- Receiver model
- Manufacturing variance

ITK Absolute Power

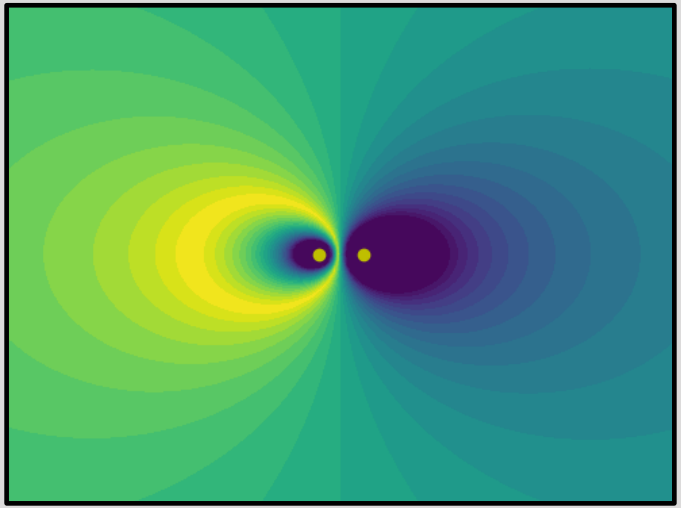


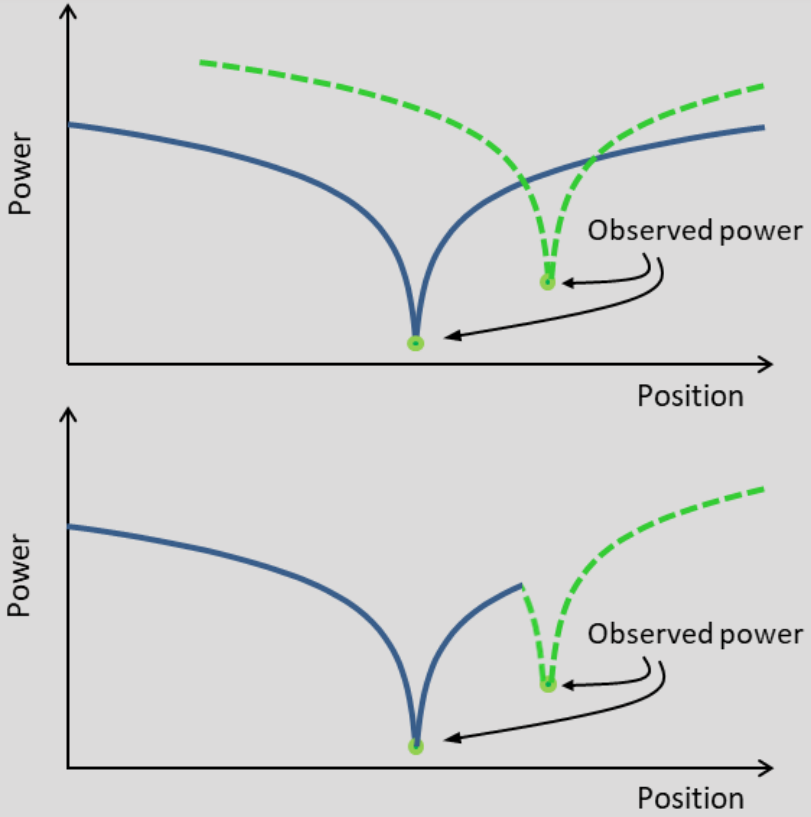
Mapping a Single Observation



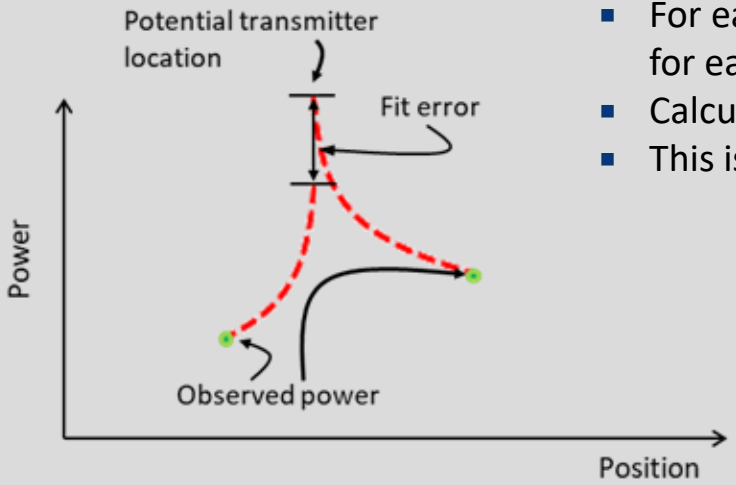
Adding More Observations

- Multiple observations are combined.
- Many options for mixing/combining measurements.





Goodness of Fit - New Version



- Create a grid of locations.
- For each location, calculate the expected transmit power for each measurement
- Calculate the RMS fit error for all measurements.
- This is called the Fit Map

Received Power for Free Space Loss

$$P_r = P_t - L_p(dB)$$

$$P_r = P_t - 20\log(d) - 20\log(f) + 147.55$$

$$P_r = x_0 + x_1\log(d)$$

Where,

P_r	- received power
P_t	- transmit power
L_p	- power loss function
d	- distance
f	- frequency

Estimation Model

Physical model

$$P_r = P_t - 20\log(d) - 20\log(f) + 147.55$$

Functional model

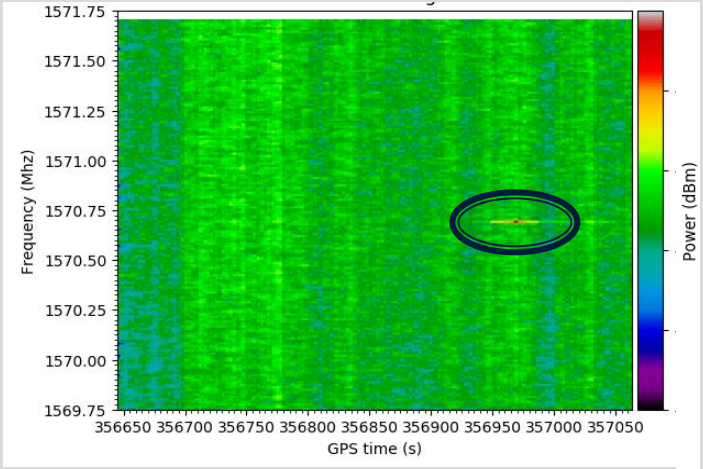
$$P_r = x_0 + x_1\log(d)$$

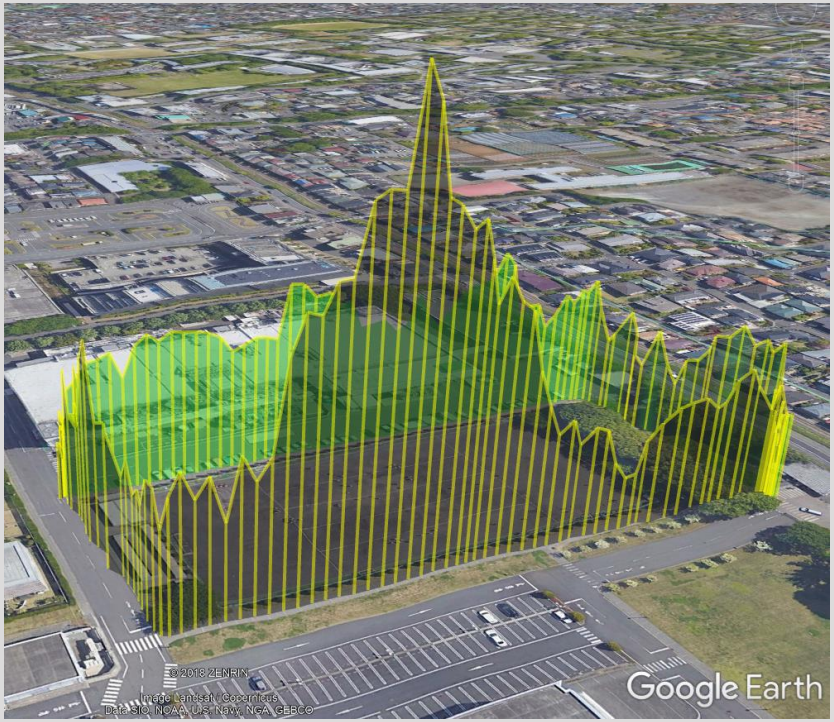
Design matrix

$$A = [1 \quad \log(d)]$$

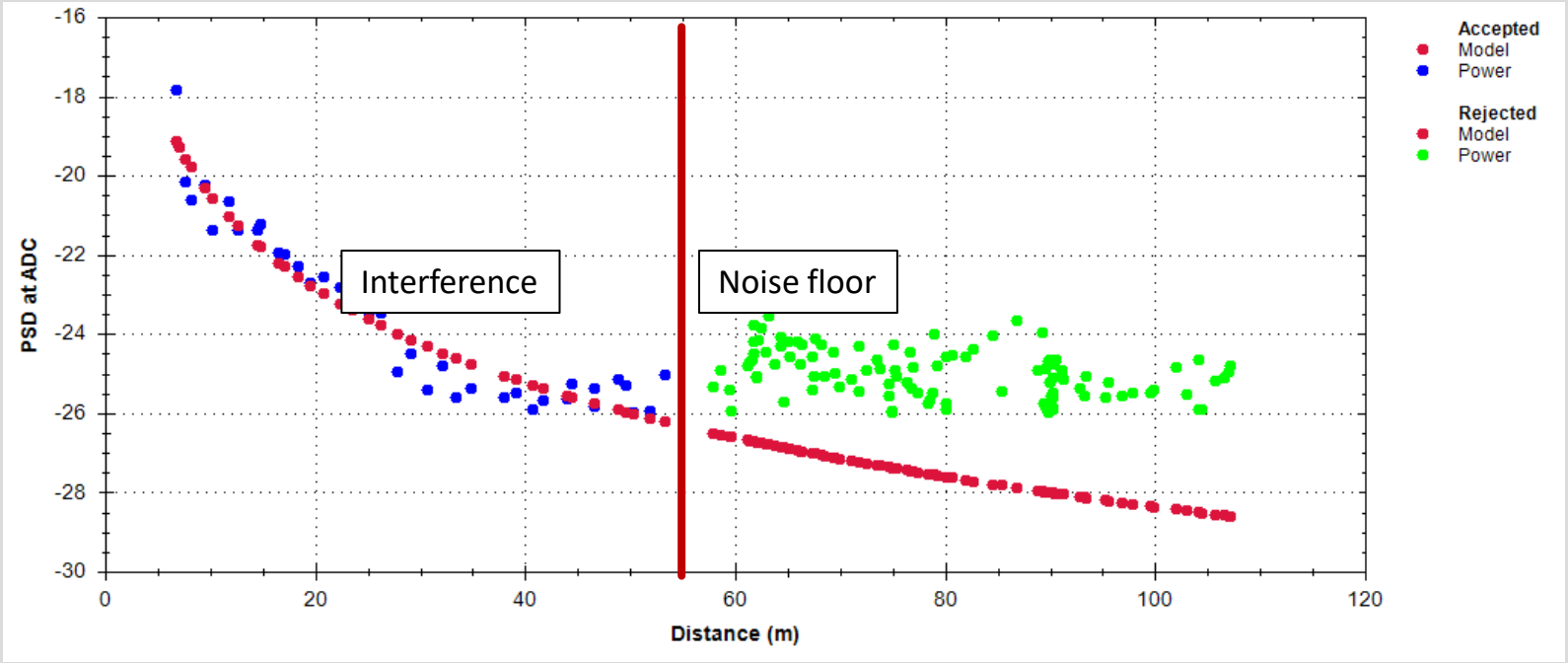
Received Power Measurements

- Power calculated by integrating the PSD across the interference bandwidth.
- Yellow line is the roller-coaster plot of the interference from a dataset in Japan. The power increases as we approach the interference source.

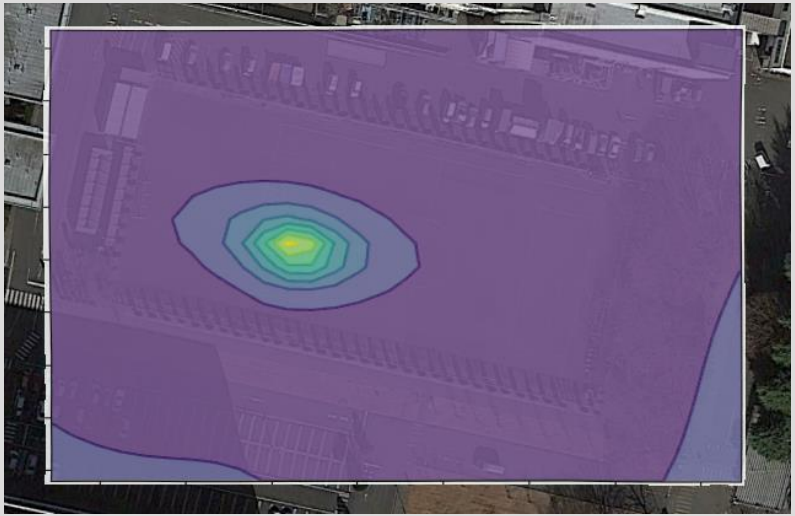




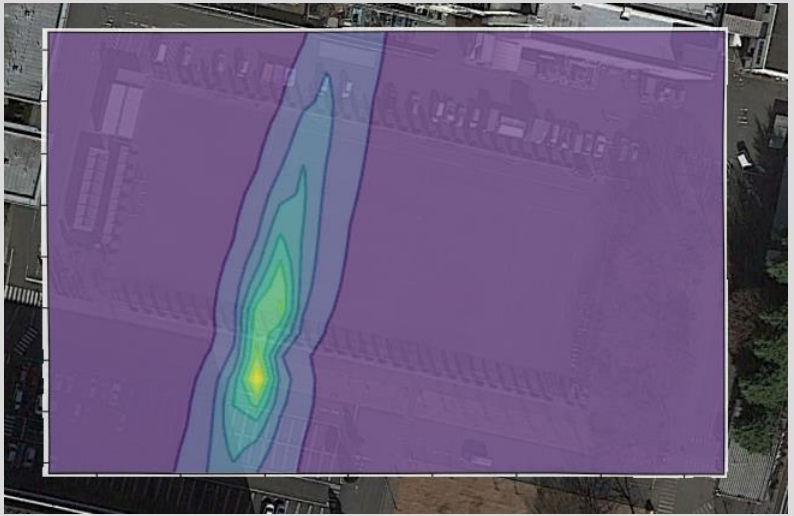
Tokyo—Power vs Distance



Fit Map



Estimation Map



(Map data: ZENRIN)

Interference Tool Kit (ITK)

- http://docs.novatel.com/OEM7/Content/Operation/Interference_Toolkit.htm

ION Publications

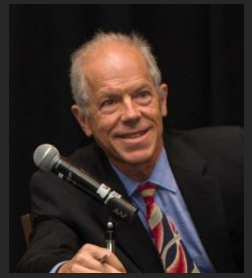
- Demonstrated Interference Detection and Mitigation with a Multi-frequency High Precision Receiver
  http://www.ion.org/publications/abstract.cfm?articleID=14743
- Interference Likelihood Mapping with Case Studies
  http://www.ion.org/publications/abstract.cfm?articleID=15582
- Interference Mapping Using Received Power
  http://www.ion.org/publications/abstract.cfm?articleID=16007

Poll #3

Which option on a GNSS receiver would most influence your purchasing decision? (select one)

A. Interference detection
B. Interference mitigation
C. Interference geolocation

Ask the Experts – Part 2



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Fabio Dovis
Associate Professor
Politecnico di Torino

Guy Buesnel
PNT Security Technologist
Spirent

Paul Alves
Technology Manager
Correction Services
NovAtel

www.insidegnss.com
www.novatel.com/defense