GNSS RFI/Spoofing: Detection, Localization, & Mitigation

Stanford's 2012 PNT Challenges and Opportunities Symposium

14 - November - 2012

Dennis M. Akos

University of Colorado/Stanford University

with contributions from many at CU and Stanford

Presentation Overview

- *Motivation & Background*
- *Concept & Experimental Results*
  - *I. RFI Detection/Characterization*
  - *II. Spoofer Detection*
  - *III. RFI/Spoofer Localization*
  - *IV. RFI/Spoofer Mitigation via CPRA*
- *Summary & Conclusions*

Presentation Overview

- ***Motivation & Background***
- *Concept & Experimental Results*
  - *I. RFI Detection/Characterization*
  - *II. Spoofer Detection*
  - *III. RFI/Spoofer Localization*
  - *IV. RFI/Spoofer Mitigation via CPRA*
- *Summary & Conclusions*

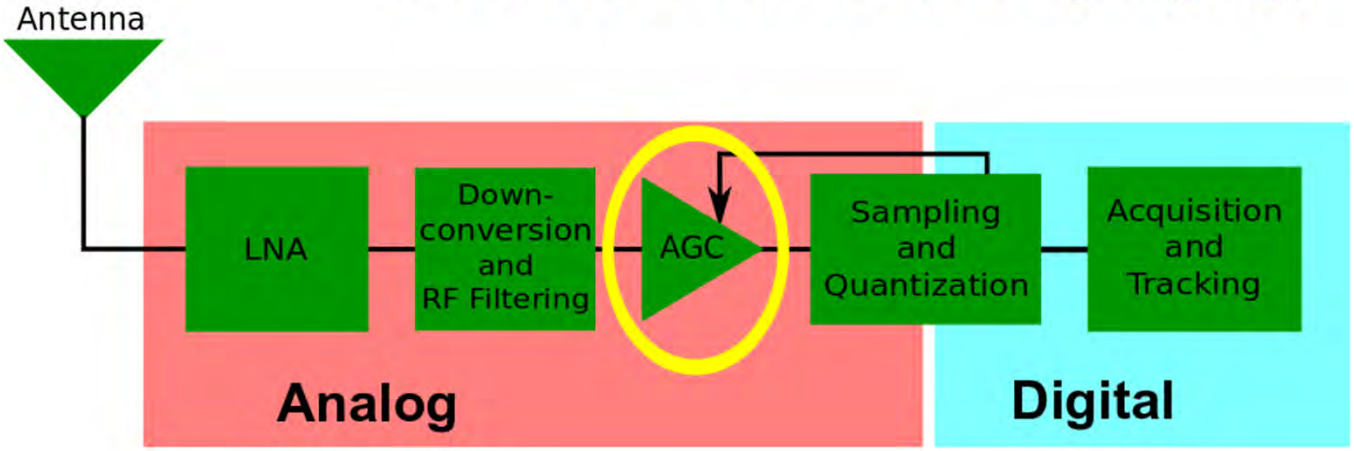
Background & Motivation

- *GPS/GNSS signals need robustness and integrity for critical applications*
- *Personal privacy devices (PPD) appear to be proliferating*
- *Simplistic/sophisticated GPS spoofing has been demonstrated*

$15 GPS Jammer

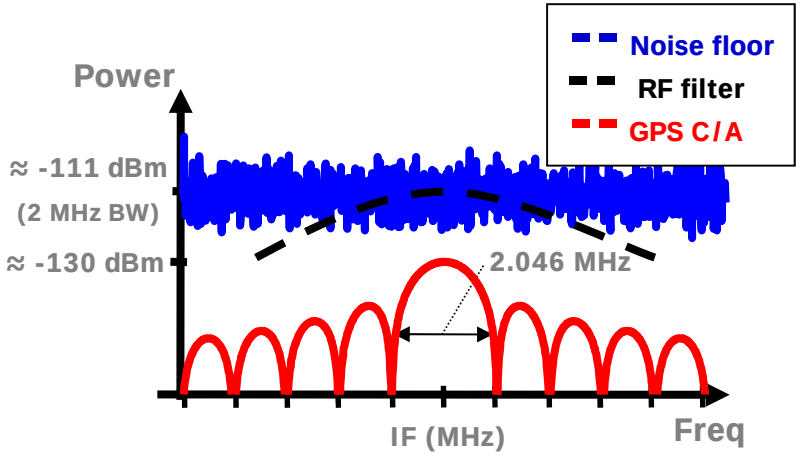
- *Leverage the receiver's automatic gain control (AGC) for "event" detection and confidence in the integrity of measurements*

Where to Detect RFI/Spoofing: AGC



To minimize losses the amplitude of the received signal has to be adjusted to the range of the ADC

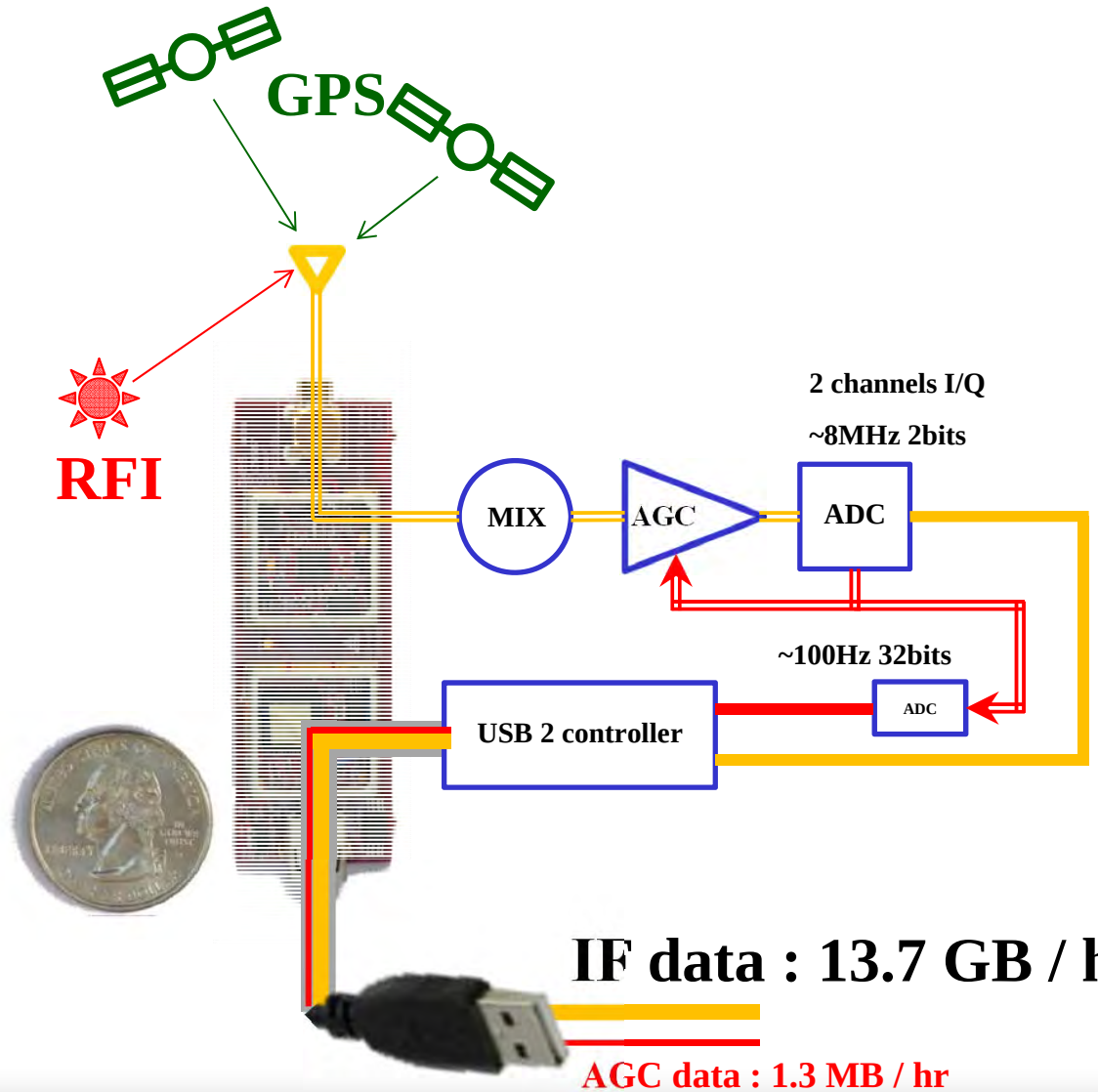
- *AGC measures the noise floor of the antenna/receiver (signal captured in the ADC)*
- *Any additional energy (RFI or spoofing) in the band will result in an AGC change*
- *Very low computational metric available on any multibit GPS/GNSS receiver*

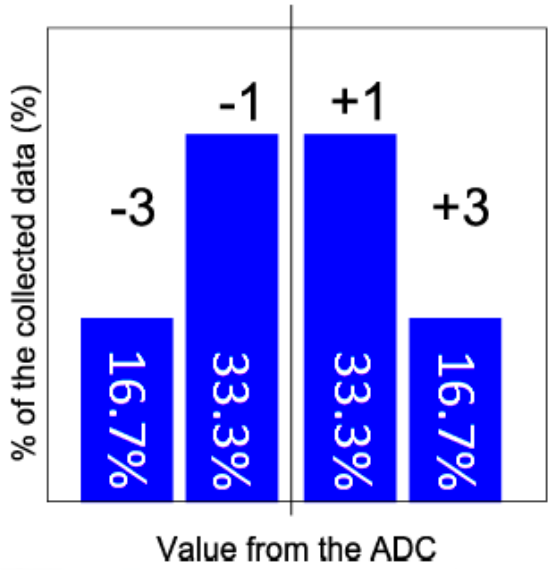


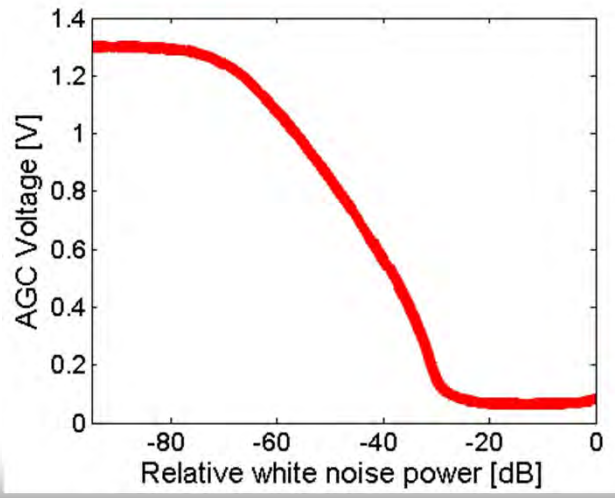
Presentation Overview

- Motivation & Background
- **Concept & Experimental Results**
  - I. RFI Detection/Characterization
  - II. Spoofer Detection
  - III. RFI/Spoofer Localization
  - IV. RFI/Spoofer Mitigation via CPRA
- Summary & Conclusions

Low-Cost GPS RFI Detection/Characterization Sensor







Add Notebook PC for Complete System

Laptop
Low computational requirements
Low cost CPU + 3GB RAM

IF data : 13.7 GB / hr

AGC data : 1.3 MB / hr

Circular buffers (100sec)

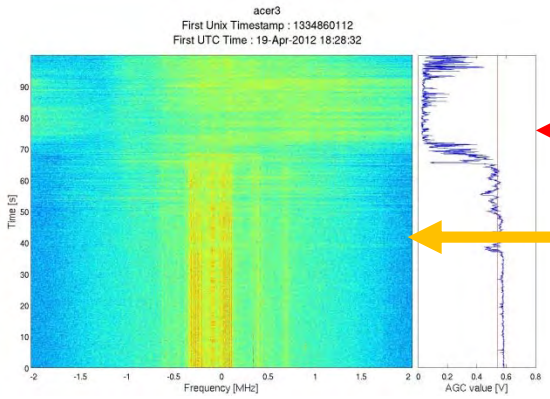
Trigger

Recording program

IF file 100sec

AGC file 100sec

AGC file Continuous



AGC plot

Spectrogram generation

Post processing
Report generator script

System Deployment at Two Airports

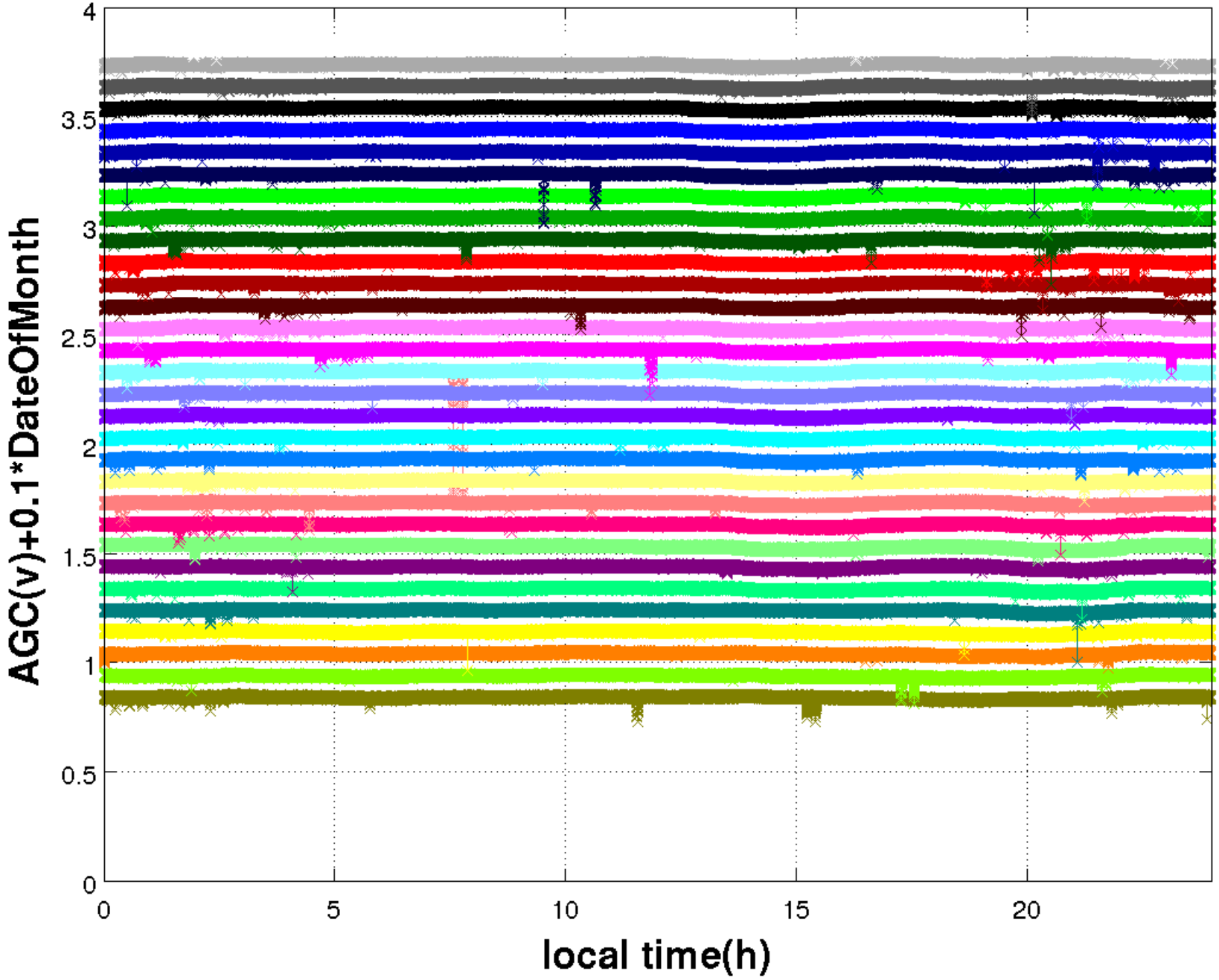
- **Systems were deployed at two different airports and data logged during Aug-2011**
  - » *LLA – Luleå, Sweden*
  - » *KHH - Kaohsiung, Taiwan*

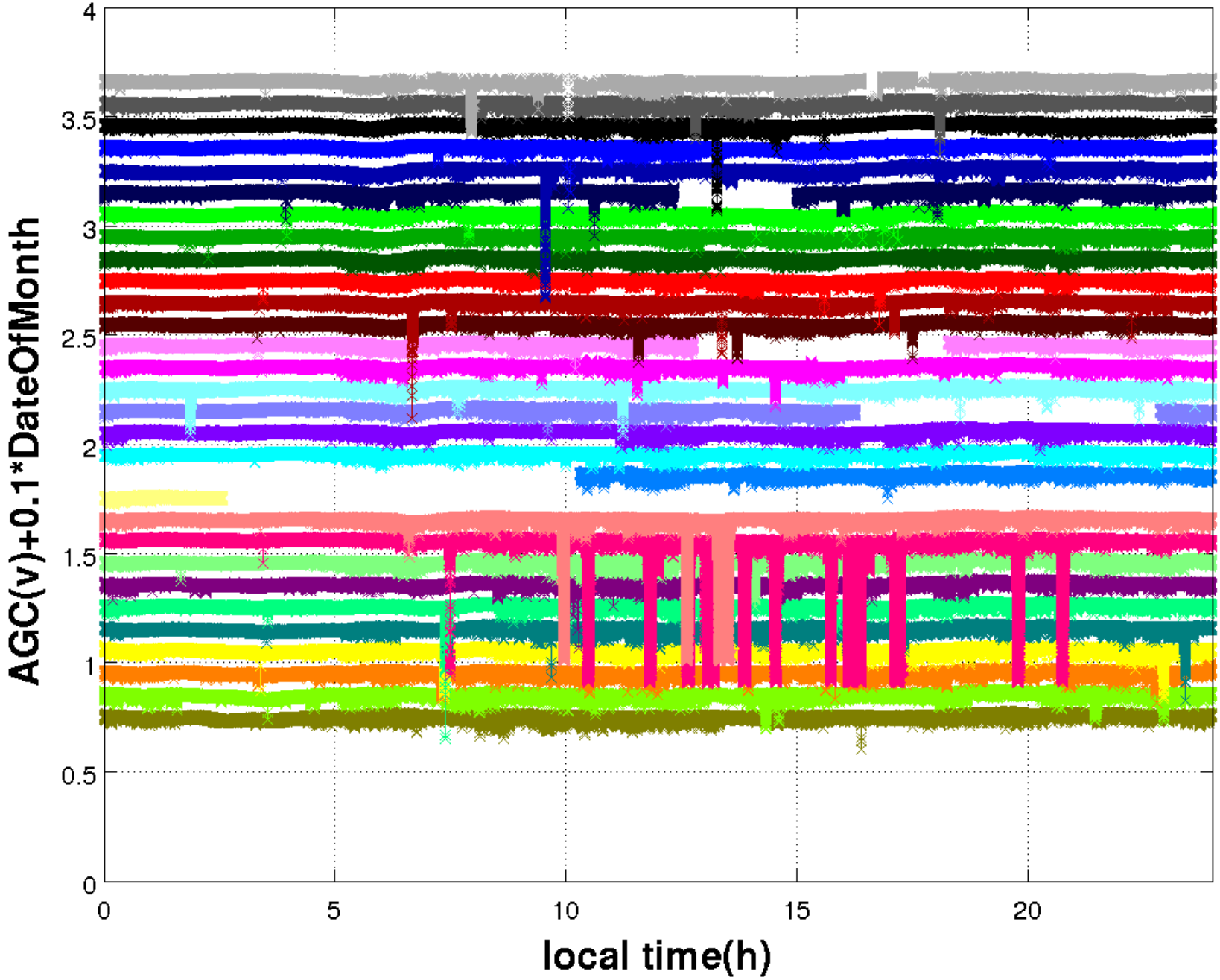
Description of Luleå, Sweden [LLA]

- *Position : 65.550N, 22.122E*
- *~ 900k passengers in 2010*
- *7km from the town of Luleå*
- *No highways within 5km*
- *Significant marine traffic in the area*

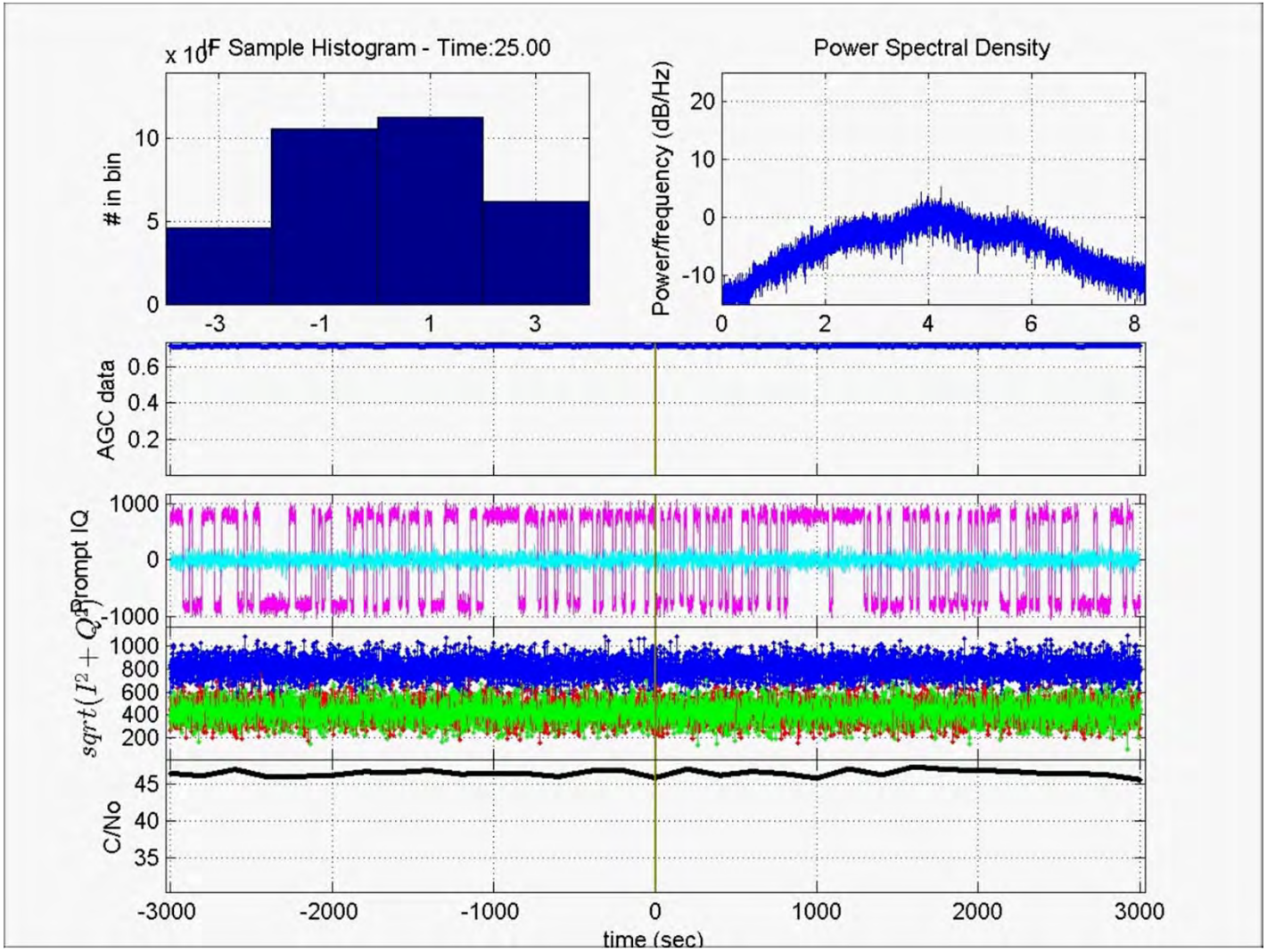
Description of Kaohsiung, Taiwan [KHH]

- *Position: 22.580N,120.332E*
- *~4000k passengers in 2010*
- *Locate at the downtown of Kaohsiung city*
- *Neighbors with the Kaohsiung harbor*
- *Surrounded by several major roads*
- *Heavy traffic nearby*


AGC from LLA (Sweden) 1/8-31/8
AGC(v)+0.1*DateOfMonth
local time(h)
0
0.5
1
1.5
2
2.5
3
3.5
4
0
5
10
15
20


AGC from KHH (Taiwan) 1/8-31/8
AGC(v)+0.1*DateOfMonth
local time(h)
0
0.5
1
1.5
2
2.5
3
3.5
4
0
5
10
15
20

Animation of a KHH Trigger/Capture



In addition to spectrogram, it is possible to animate the captured data

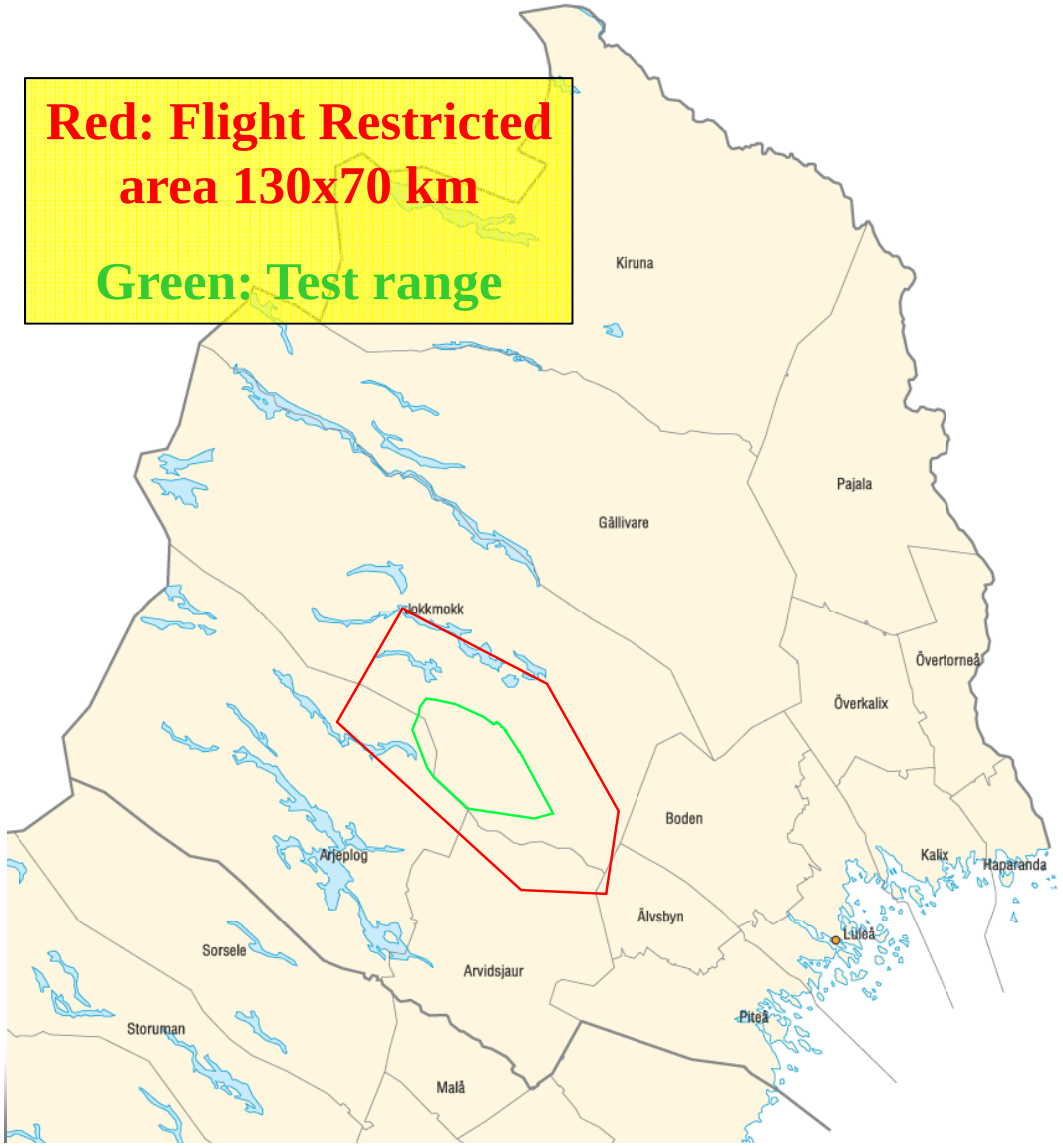
Summary

- *Developed and deployed a low-cost computationally efficient GPS RFI detection & characterization system*
- *Currently operating 5 different stations*

Presentation Overview

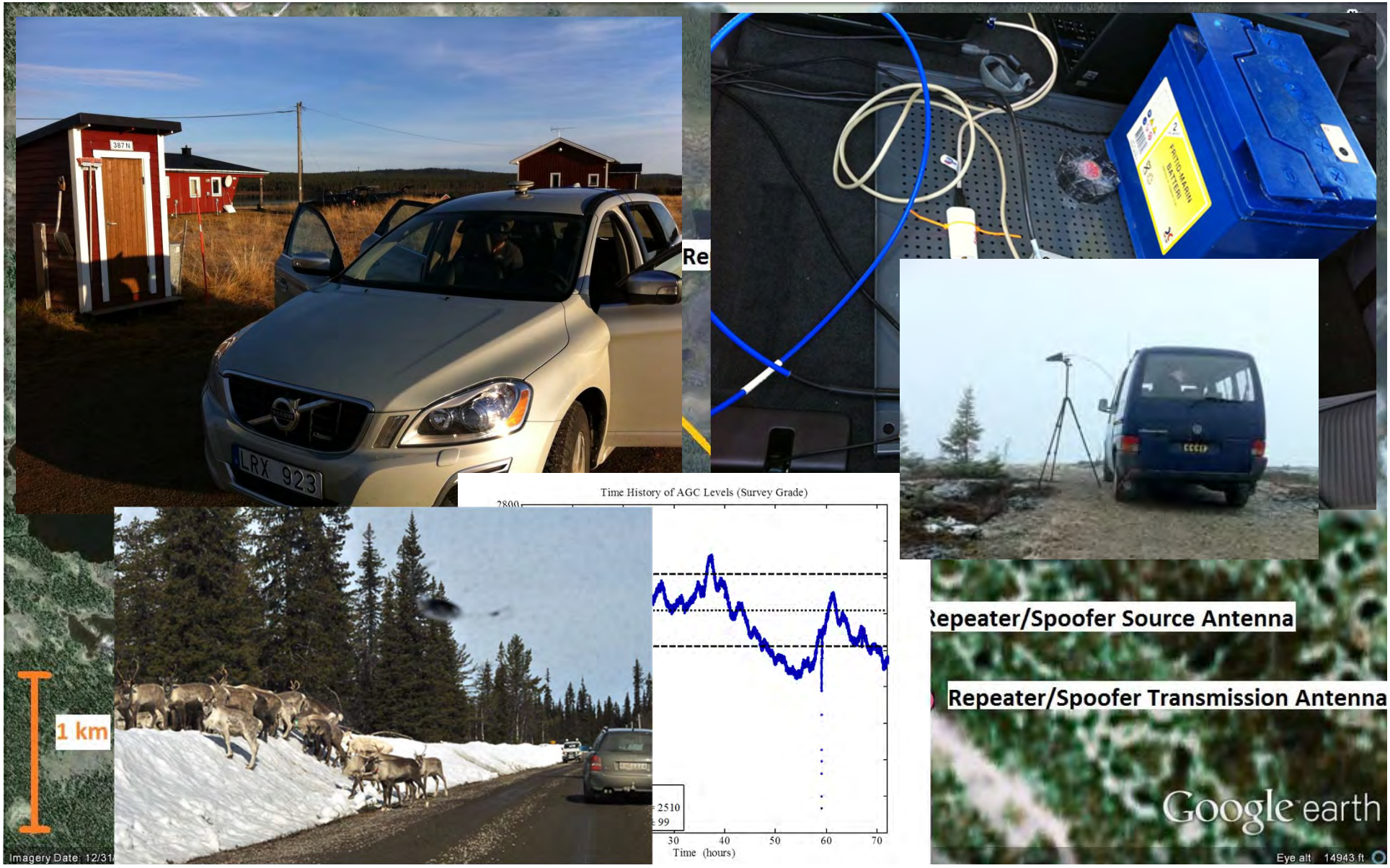
- Motivation & Background
- **Concept & Experimental Results**
  - I. RFI Detection/Characterization
  - **II. Spoofer Detection**
  - III. RFI/Spoofer Localization
  - IV. RFI/Spoofer Mitigation via CPRA
- Summary & Conclusions

Swedish Military Test Range: Robotförsökplats Norrland (RFN)

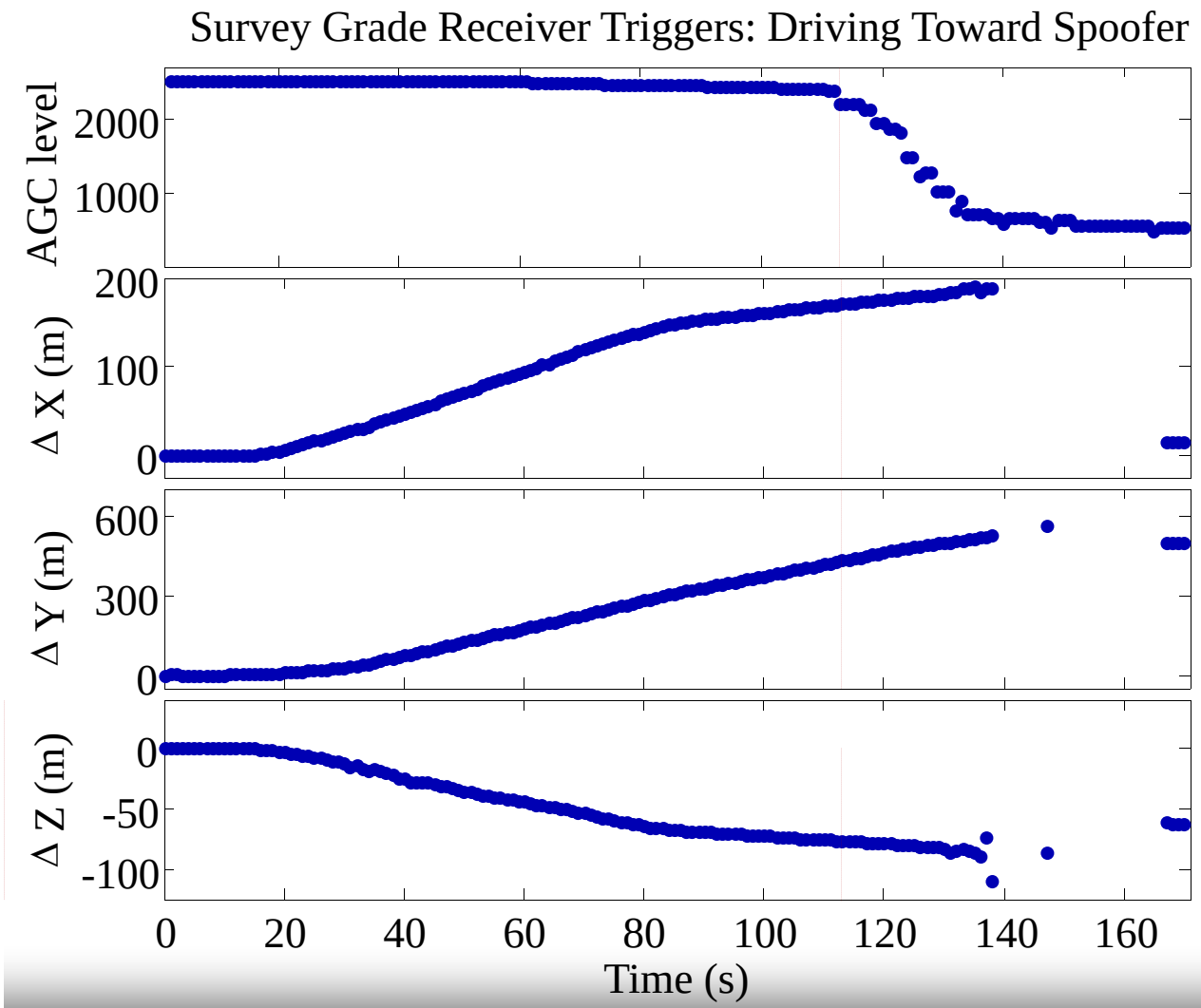


- *Developed experiment to assess AGC's ability to detect spoofing*
- *Difficult to perform such experiments outside of a laboratory environment*
- *Utilize a simplistic repeater spoofer (meaconing) in live testing*

AGC Spoofer Detection Experiment

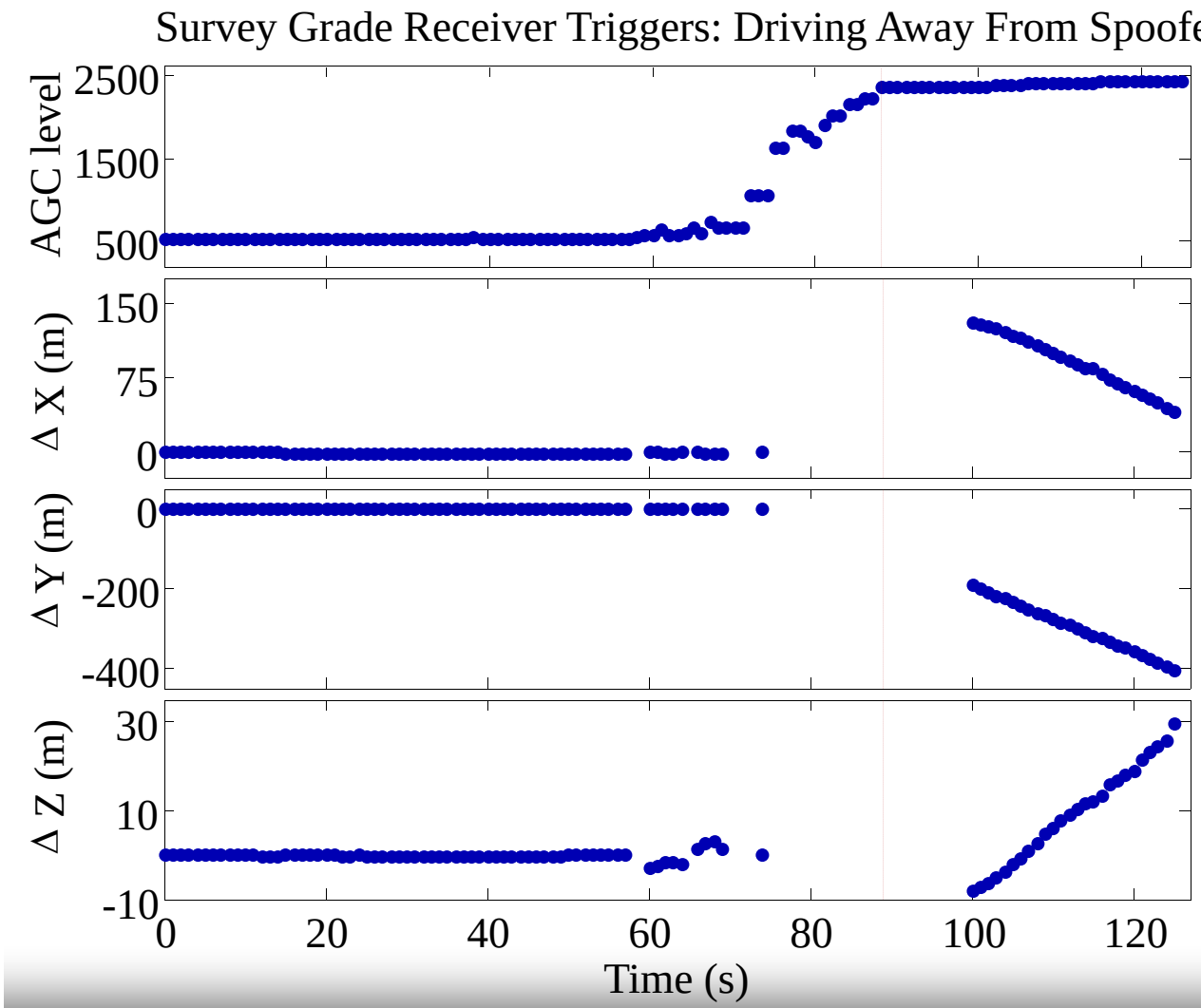


GPS AGC & XYZ Position Data - Driving Toward Spoofer



- ***AGC 2-sigma threshold flagged well before GPS RX is captured by spoofer***
- ***Other receivers under test showed similar results***

GPS AGC & XYZ Position Data - Driving Away Spoofer



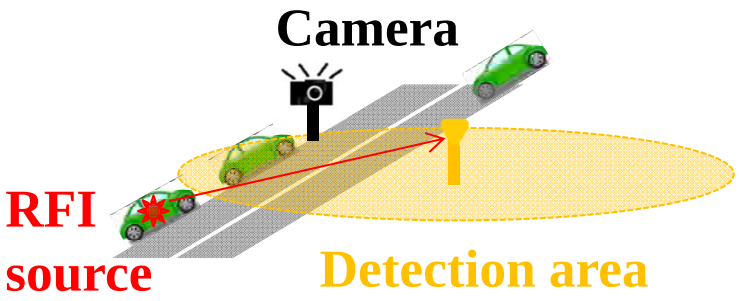
- ***AGC 2-sigma threshold exceed when receiver is powered on***
- ***True position only after AGC returns to normal levels***
- ***Other receivers under test showed similar results***

Presentation Overview

- Motivation & Background
- **Concept & Experimental Results**
  - I. RFI Detection/Characterization
  - II. Spoofer Detection
  - **III. RFI/Spoofer Localization**
  - IV. RFI/Spoofer Mitigation via CPRA
- Summary & Conclusions

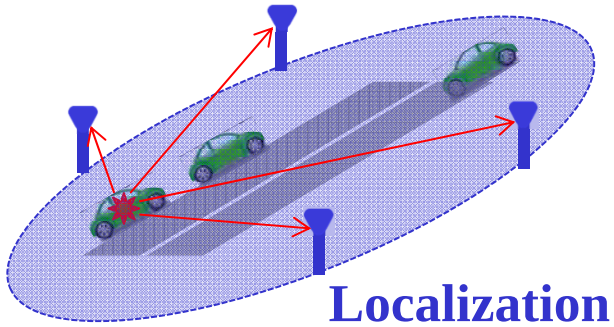
Update Detection System for Localization

Detection configuration

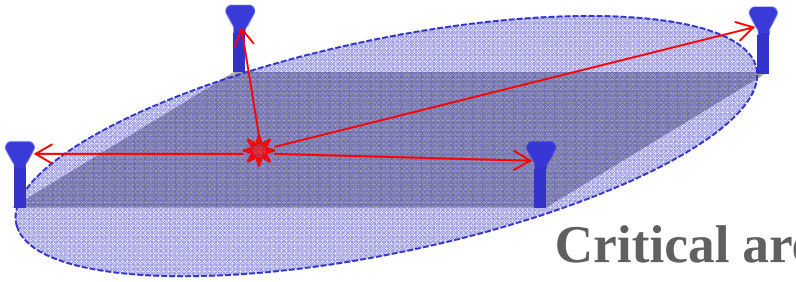


- *How often does RFI occur ?*
- *What kind of RFI (CW, narrowband, white noise) ?*
- *Add camera capability*

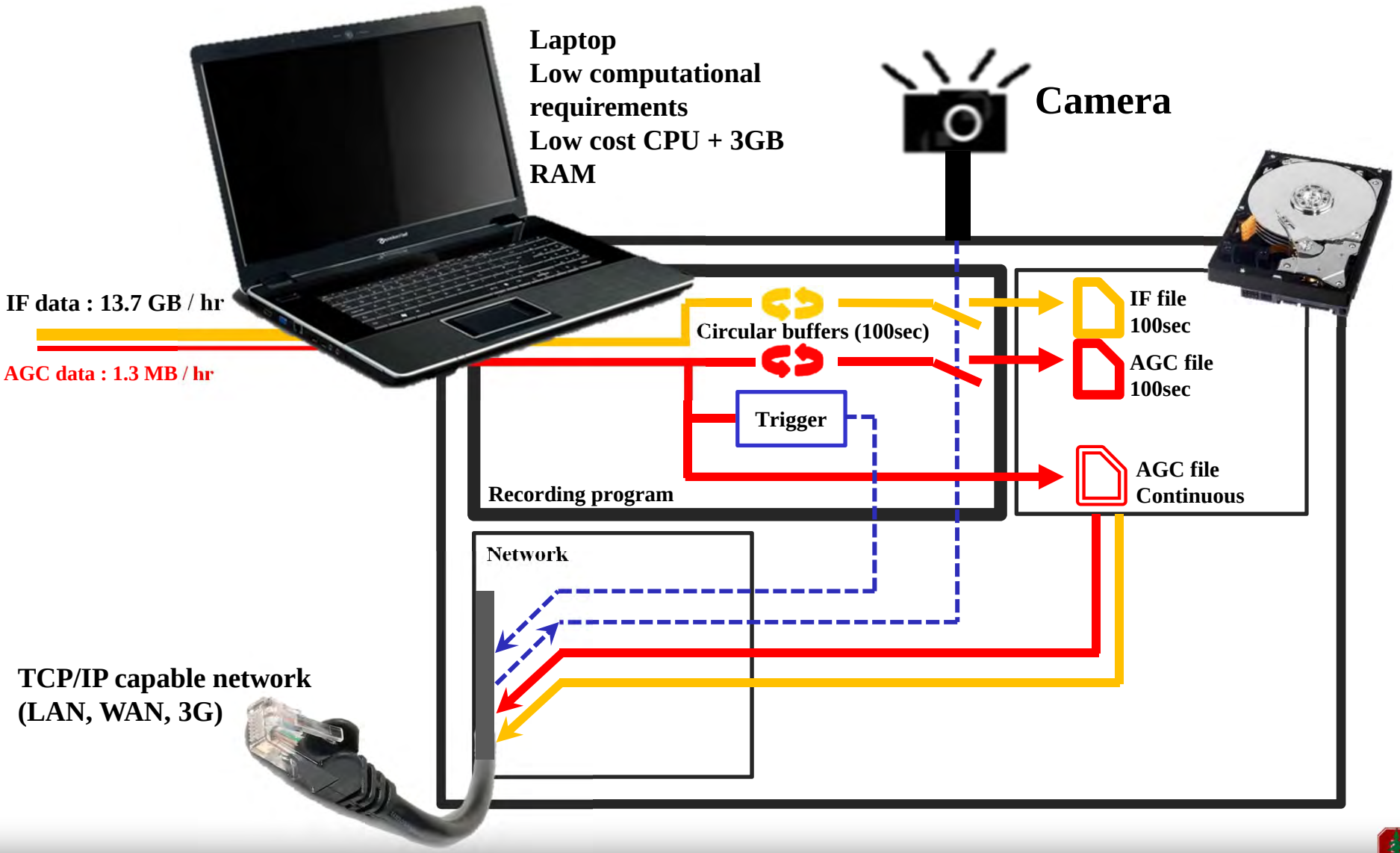
Localization configuration



- *Type of vehicle (car, truck, motorcycle)*
- *Quickly identify spurious RFI sources*



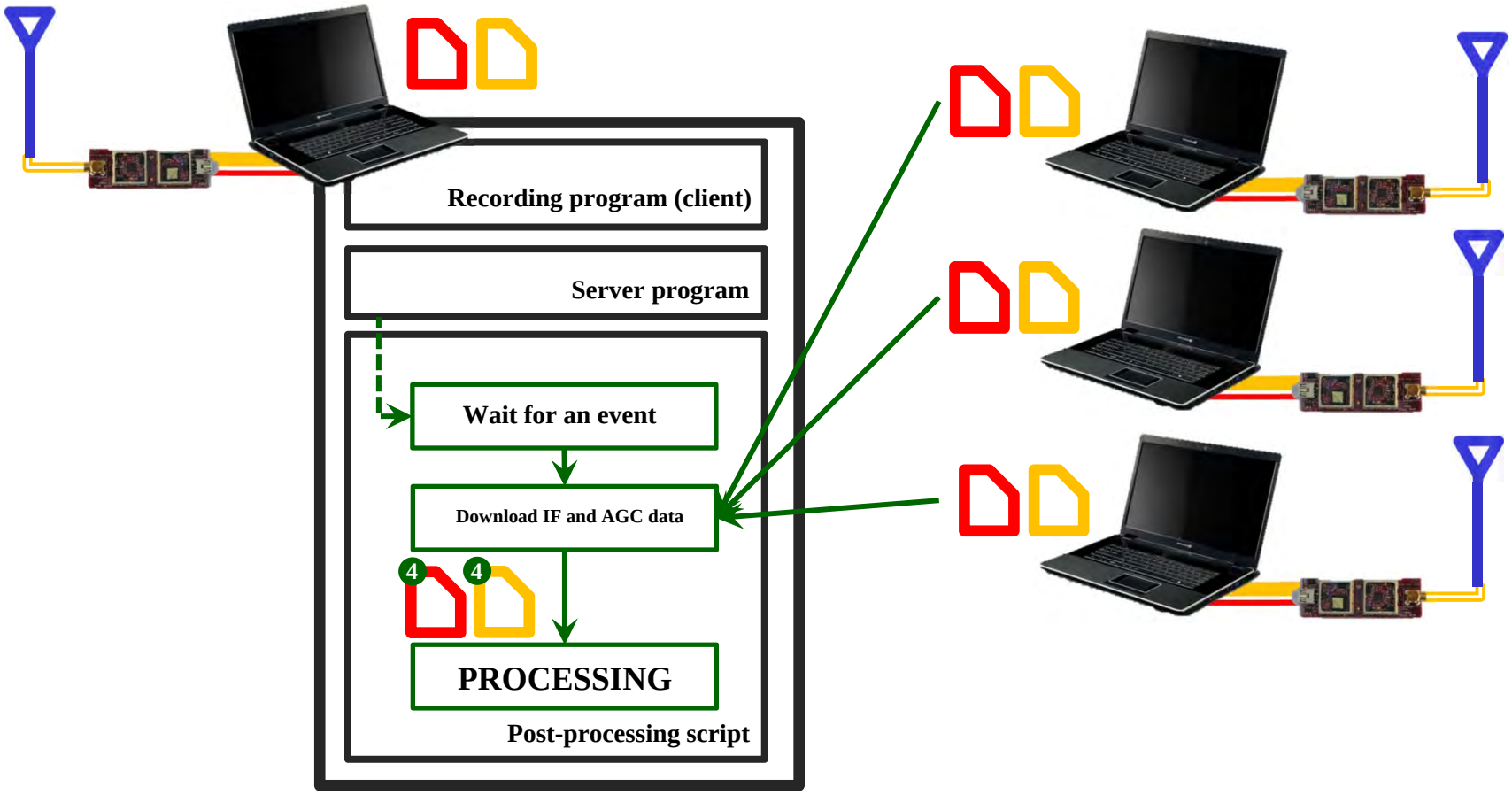
System : Host Computer for Localization



System : Network Operation

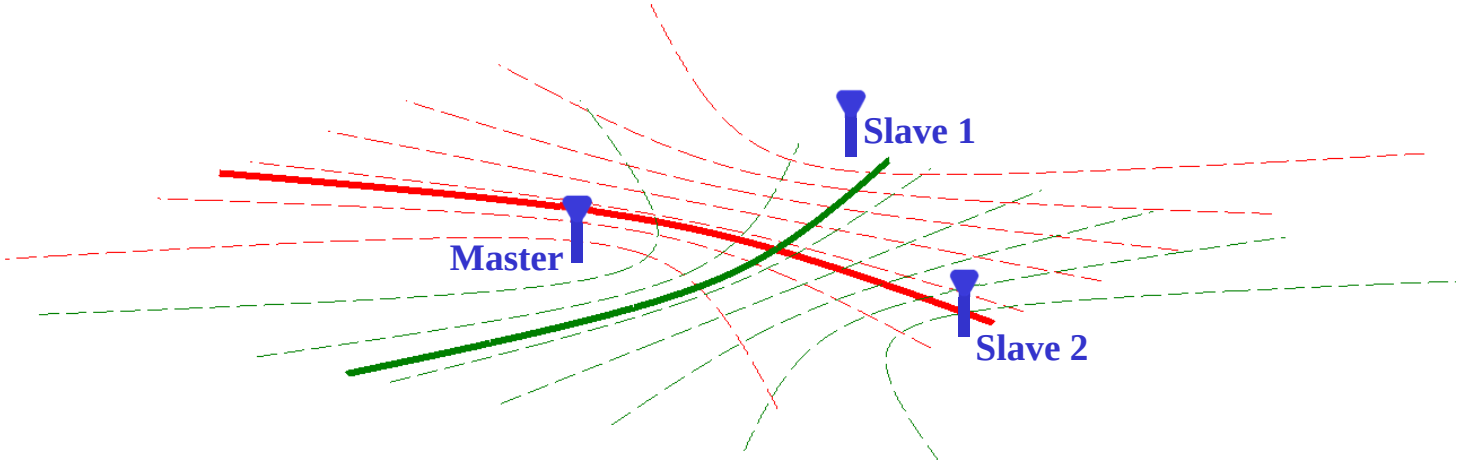
Running as a client + server

Running as clients



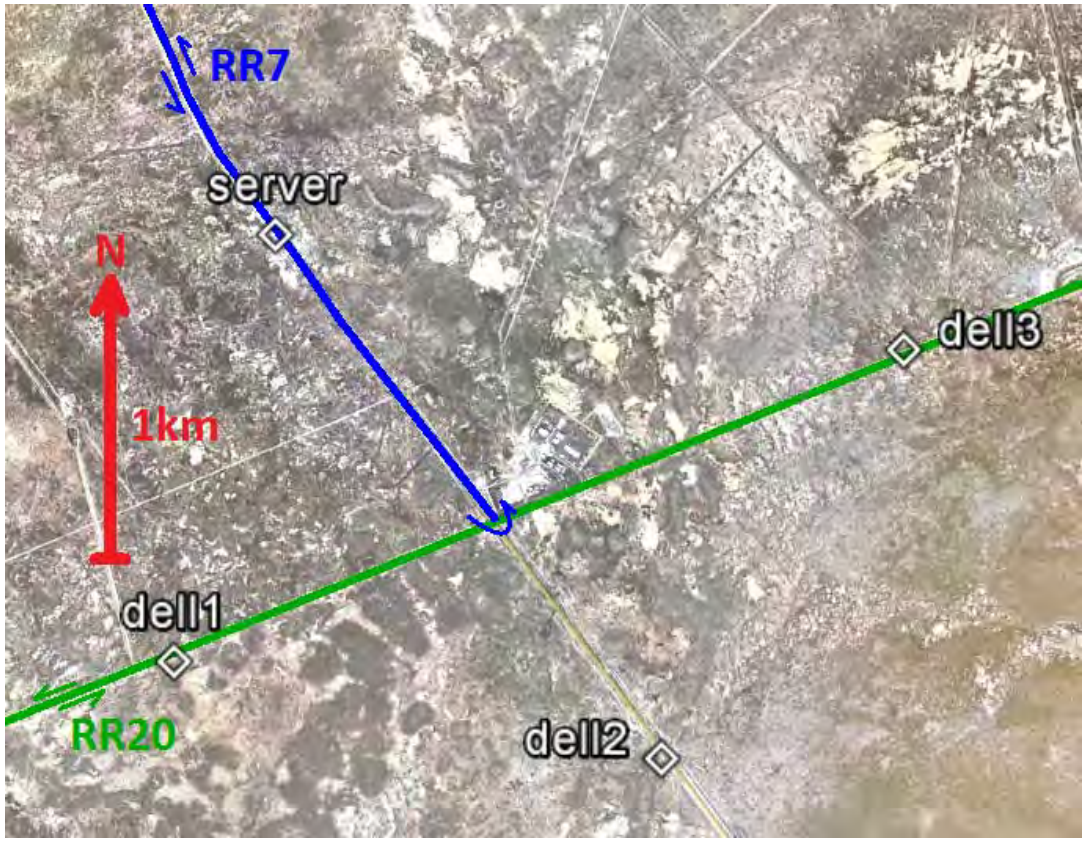
Processing Principles

- *Two possible methods*
  - » *Time Difference of Arrival : cross-correlation*
  - » *Power Difference of Arrival : AGC processing*
- *Both result in hyperbolic equations (like LORAN)*



- *Cross-correlation requires coherent signals*
  - » *File alignment & clock error model leverage "clean" 40 sec of GPS data*

Department of Homeland Security (DHS) GPS Jammer Testing at White Sands Missile Range (WSMR) – 18-22 June 2012



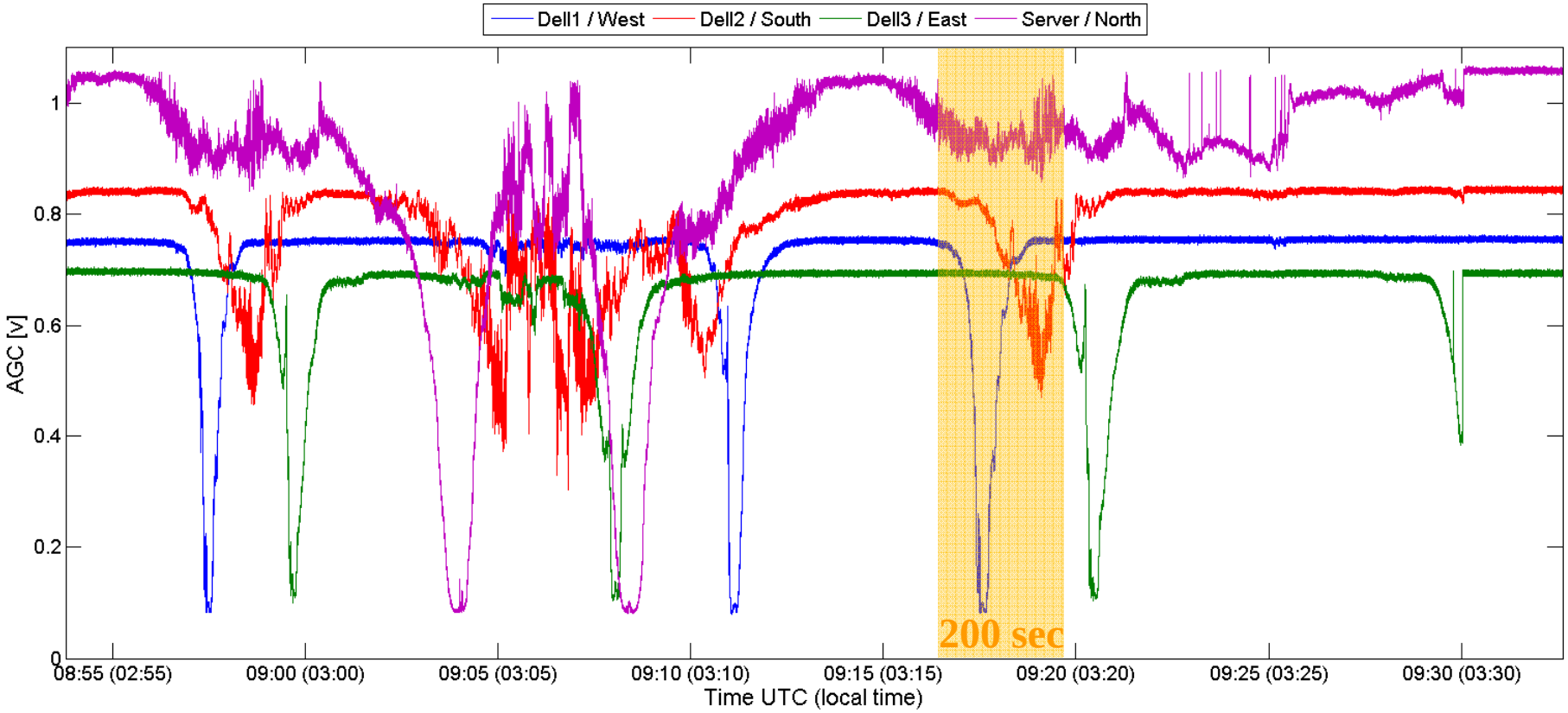
Station

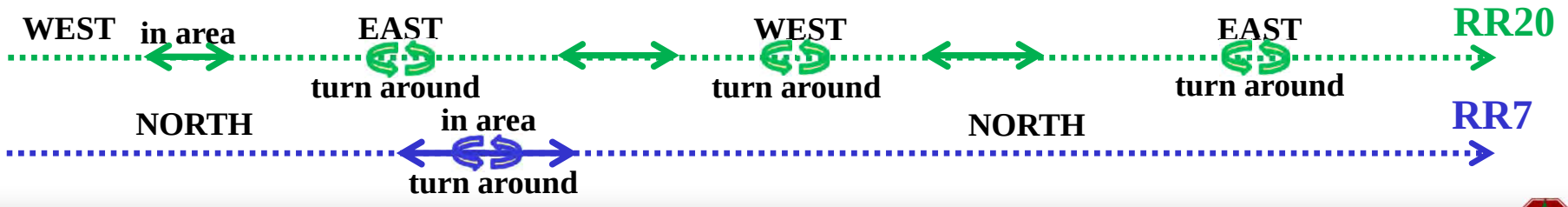
Jammer's path

Focused on two testing days

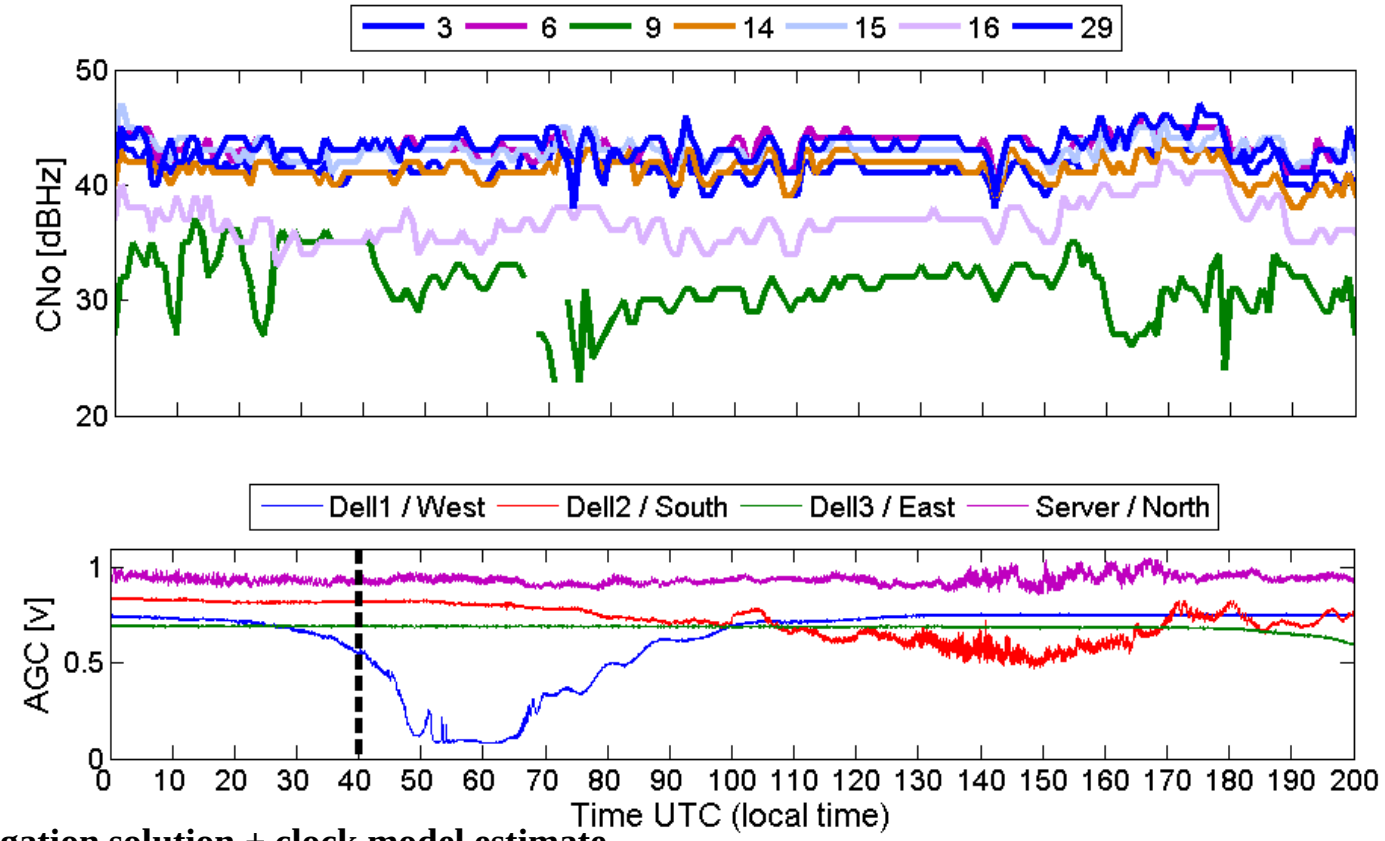
- ***20-June-2012: Dynamic 250mW/2.5W jammers***
  - » ***Station deployment : ~1.8km apart***
    - Scenario 3 02:45 to 03:30
      - 1 vehicle RR7
      - 1 vehicle RR20
      - 2.5W jammers
- ***22-June-2012: Stationary 25W jammers***
  - » ***Station deployment : ~15km apart (9.4 mi)***

Experiment : Dynamic 250mW/2.5W jammers





Zoomed View: Dynamic 2.5W jammers



Navigation solution + clock model estimate

Cross-correlation + jammer localization

Localization Results: Animation

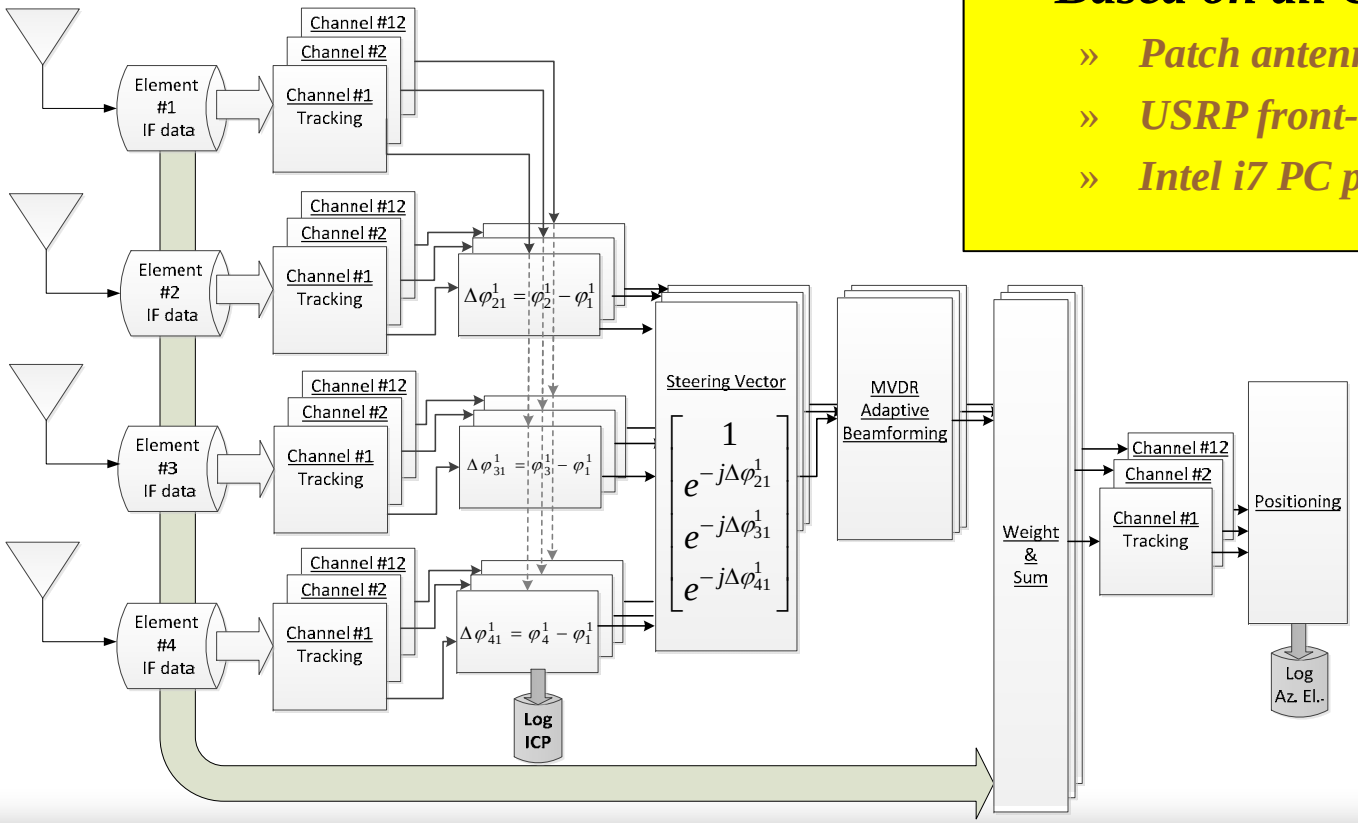
Presentation Overview

- Motivation & Background
- **Concept & Experimental Results**
  - I. RFI Detection/Characterization
  - II. Spoofer Detection
  - III. RFI/Spoofer Localization
  - **IV. RFI/Spoofer Mitigation via CPRA**
- Summary & Conclusions

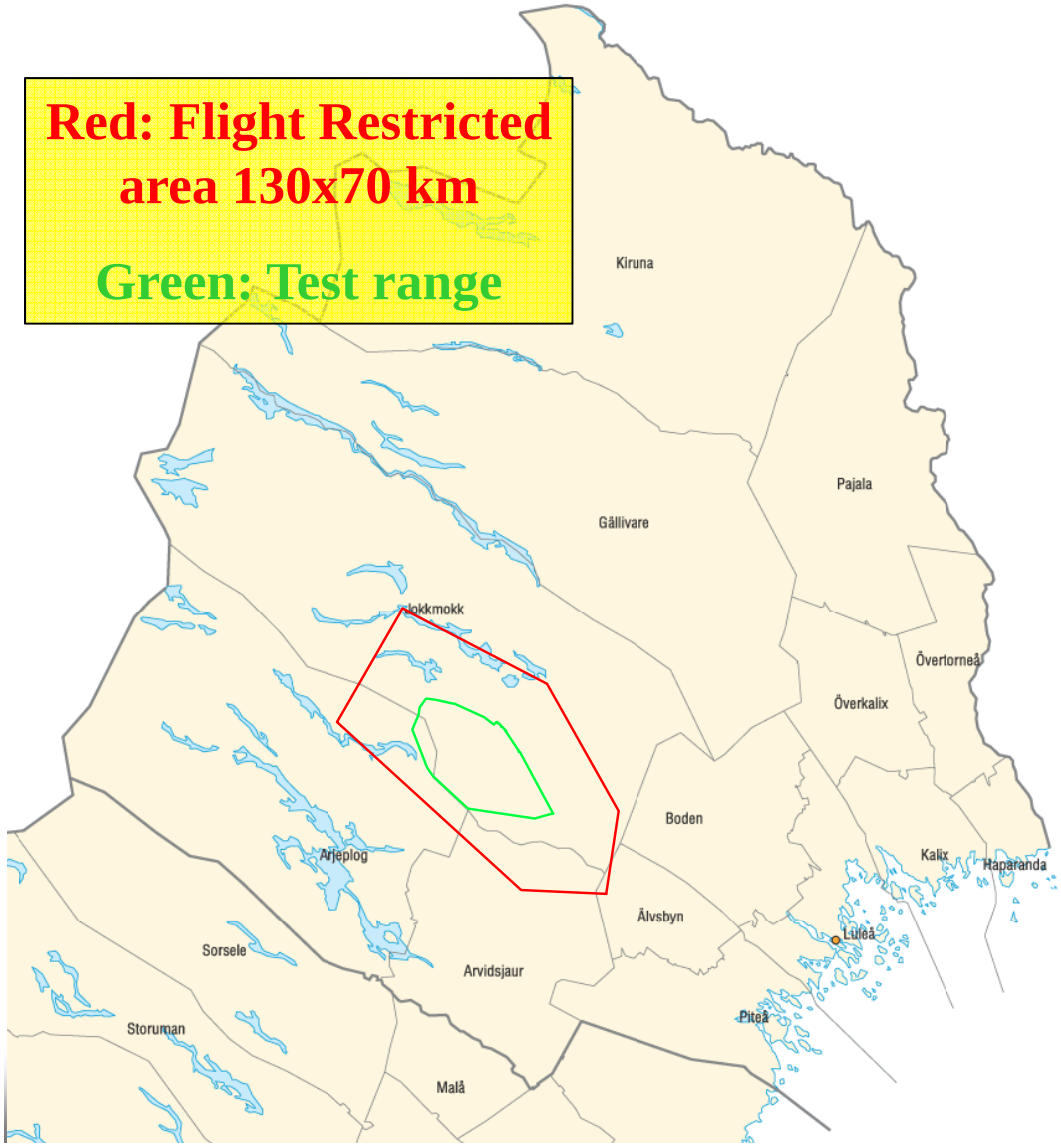
Controlled Radiation Pattern Antenna (CRPA) Software Receiver

- ***All-in-view real-time CRPA software receiver for GPS/WAAS L1 C/A***
  - » *4 elements, 12 channels, 4 MHz sampling rate, 14 bits ADC resolution for I/Q*
  - » *Minimum Variance Distortionless Response (MVDR) & power minimization algorithms*

- ***Based on all COTS components***
  - » *Patch antennas*
  - » *USRP front-ends*
  - » *Intel i7 PC processing computer*



Return to Swedish RFN Test Range: Oct 2012

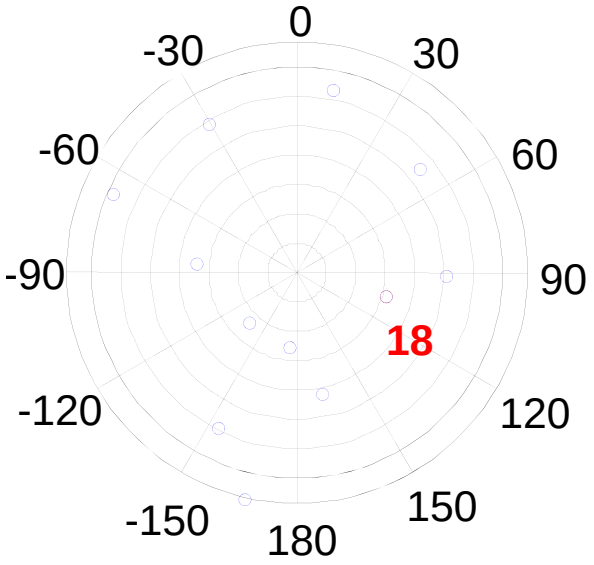


- *Testing Panavia Tornado aircraft with munitions in GPS denied conditions*
  - » *"Piggybacking" on this test*
- *Operating Stanford 4 element CRPA in parallel with mass market RX*
  - » *Provides real time operation & IF recording*
- *Assess/compare performance in RFI environment*

RFN Antenna Array Testing – Oct 2012

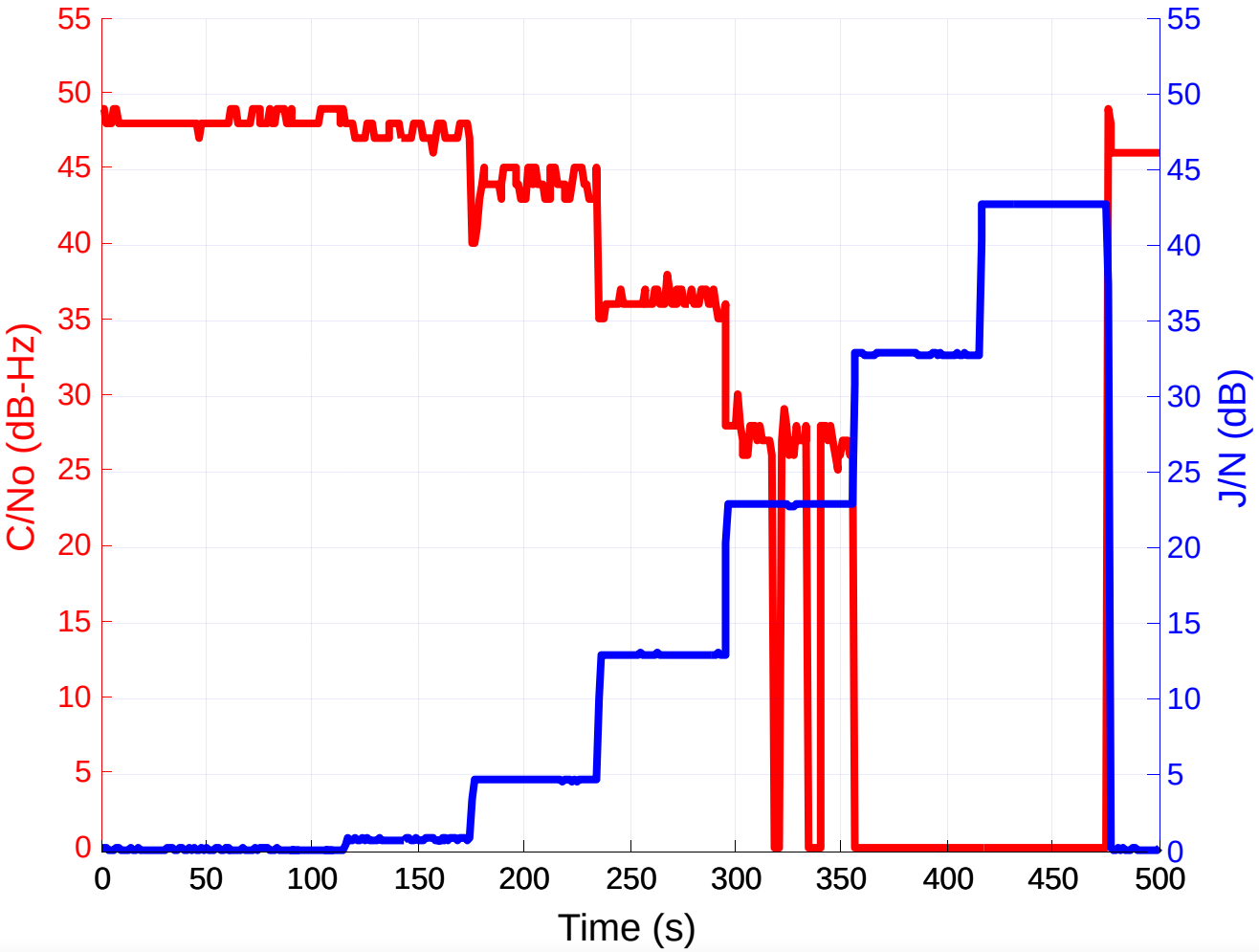
RFN Antenna Array Testing – 14-Oct-2012

J/N & PRN18 C/No for Power Ramp Test



- ***Shown are the J/N and C/No (PRN18 - mass market GPS RX) for stepped BBN jamming***

- ***Assess/compare performance of CRPA processing***



Beamforming Software Receiver

MVDR

PRN	STA	FRQ	CN0
3	Lock	4304	55.3
16	Nav	816	48.1
18	Lock	4698	52.5
19	Nav	6441	51.6
6	Lock	3270	52.4
7	Lock	1982	40.5
15	Lock	4601	47.3
21	Nav	1725	50.4
30	Lock	-45	36.6
8	Nav	4610	43.5
26	Nav	2533	43.8
22	Nav	6993	52.7

PoweMin

PRN	STA	FRQ	CN0
3	Lock	4292	43.9
16	Lock	806	44.2
18	Lock	4698	43.1
19	Nav	6439	42.2
6	Lock	3264	43.6
7	Lock	2001	0.0
15	Lock	4600	39.7
21	Lock	1717	42.1
30	Lock	-62	33.2
8	Nav	4619	40.9
26	Nav	2491	37.4
22	Lock	7008	43.4

Antenna #1

PRN	STA	FRQ	CN0
3	Lock	4303	45.6
16	Nav	816	48.1
18	Lock	4694	47.6
19	Nav	6434	43.5
6	Lock	3267	46.4
7	Lock	1957	40.5
15	Lock	4600	41.5
21	Nav	1717	45.1
30	Lock	-45	36.6
8	Nav	4613	43.5
26	Nav	2519	39.0
22	Nav	6992	48.4

Antenna #2

PRN	STA	FRQ	CN0
3	Lock	4303	50.3
16	Nav	816	39.8
18	Lock	4701	48.6
19	Nav	6450	45.9
6	Lock	3261	43.9
7	Lock	1968	43.6
15	Lock	4606	46.1
21	Nav	1727	45.4
30	Conf	-99	0.0
8	Lock	4557	29.7
26	Nav	2540	39.1
22	Nav	6994	46.8

Antenna #3

PRN	STA	FRQ	CN0
3	Lock	4305	51.9
16	Lock	817	42.7
18	Lock	4691	44.1
19	Nav	6443	46.6
6	Lock	3276	48.2
7	Pull	1973	0.0
15	Lock	4593	38.7
21	Nav	1726	43.2
30	Lock	-46	36.7
8	Nav	4603	42.4
26	Nav	2531	36.8
22	Nav	6987	45.8

Antenna #4

PRN	STA	FRQ	CN0
3	Lock	4309	51.2
16	Lock	815	47.3
18	Lock	4710	44.3
19	Nav	6437	48.1
6	Lock	3270	46.6
7	Lock	1971	41.5
15	Lock	4594	42.2
21	Nav	1727	45.9
30	Nav	-45	33.7
8	Nav	4596	40.1
26	Nav	2526	37.4
22	Nav	6998	49.7

Antenna Layout

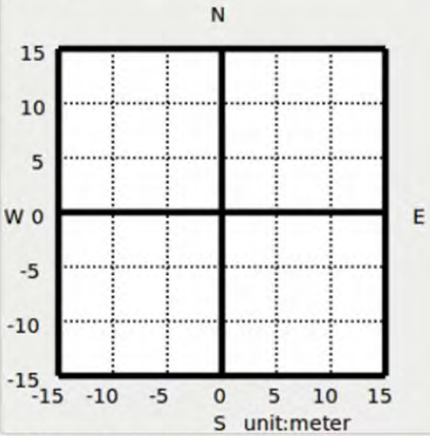
Carrier Phase Difference

PRN	Ant2-1	Ant3-1	Ant4-1
3	-129.25	-170.66	-134.99
16	-137.42	160.82	6.21
18	23.48	64.29	-152.46
19	-156.70	-82.88	-141.88
6	-112.28	121.07	-132.23
7	NaN	NaN	NaN
15	89.75	129.54	93.02
21	51.53	19.60	128.79
30	NaN	NaN	NaN
8	NaN	NaN	NaN
26	23.85	-122.34	22.91
22	-6.35	77.74	-5.76

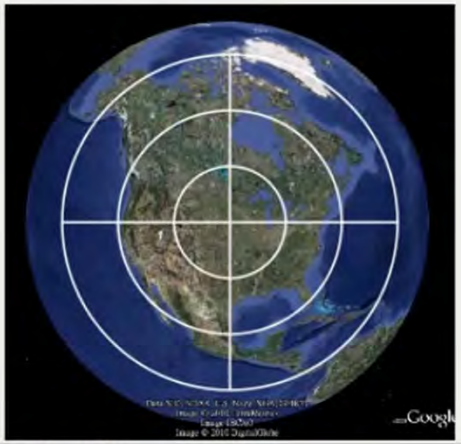
Position

Item	Value
Streaming Time(s)	14
Latitude	0.0
Longitude	0.0
Height	0.0
Cable Delay 2-1	0.000000
Cable Delay 3-1	0.000000
Cable Delay 4-1	0.000000
AGC Gain 1	841
AGC Gain 2	715
AGC Gain 3	727
AGC Gain 4	611
Adaptation Step	0.00182432

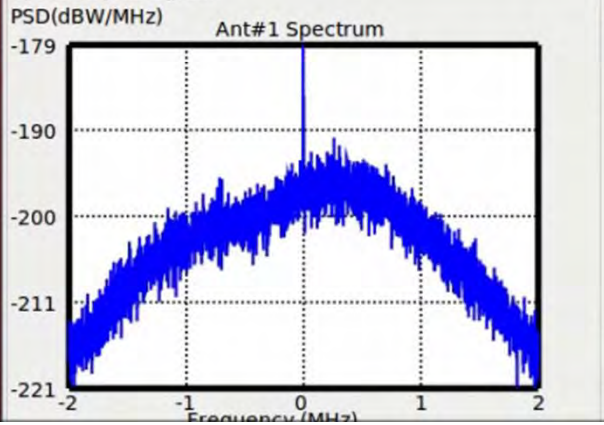
EN Plot



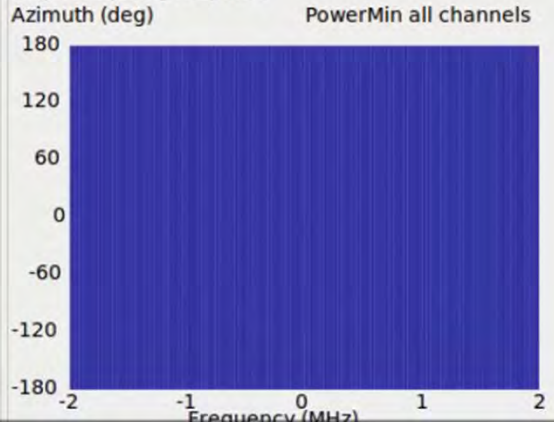
Sky Plot



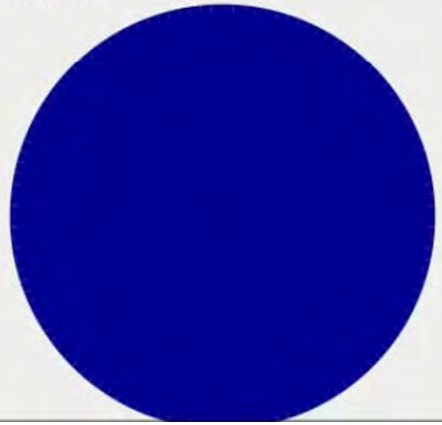
Spectrum/Histogram



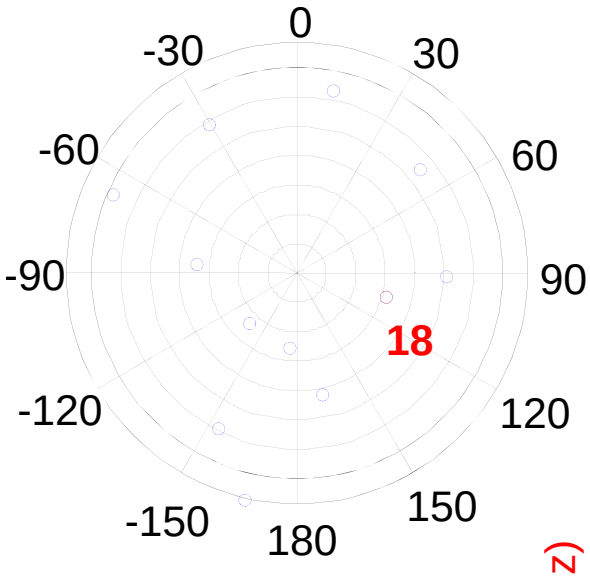
Angle Frequency Response



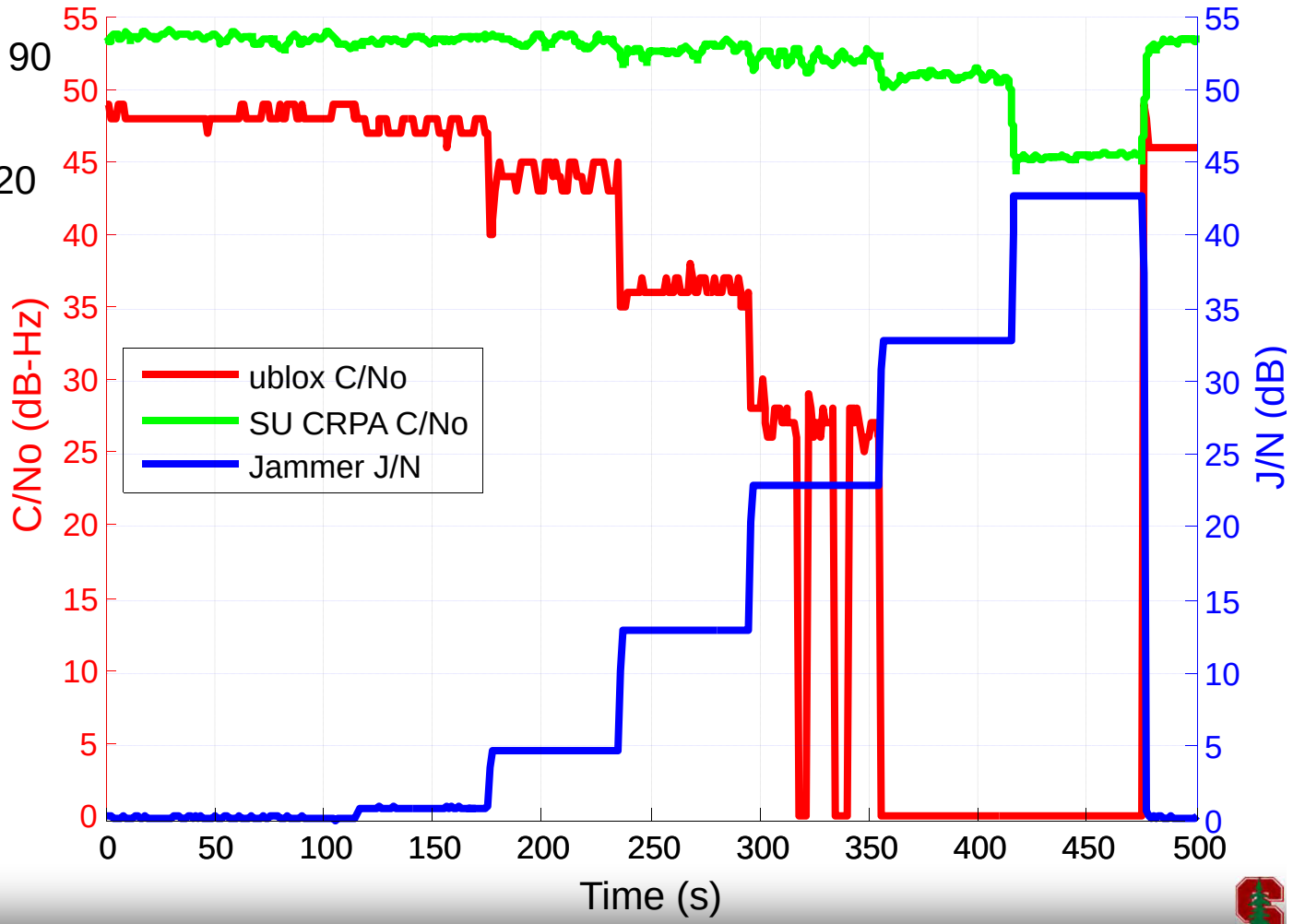
Gain Pattern Plot



J/N & PRN18 C/No for Power Ramp Test



- ***SU CRPA (MVDR) maintained lock for the entire jamming cycle***
- ***SDR implementation using low cost COTS components***



Presentation Overview

- Motivation & Background
- Concept & Experimental Results
  - I. RFI Detection/Characterization
  - II. Spoofer Detection
  - III. RFI/Spoofer Localization
  - IV. RFI/Spoofer Mitigation via CPRA
- **Summary & Conclusions**

Summary & Conclusions

- *Automatic Gain Control (AGC) is a powerful yet computational simplistic means to detect RFI/spoofing*

- *Localization of RFI/spoofing sources can be done effectively, easily and low-cost via time/power difference of arrival*

- *CRPAs can be developed using COTS hardware and provide a powerful tool to mitigate RFI/spoofing*