Innovation, Science and Economic Development Canada / Innovation, Sciences et Développement économique Canada
Communications Research Centre Canada / Centre de recherches sur les communications Canada

Wireless USRP Backhaul Network: Geolocate a GPS Jammer in Near Real-Time

CRC Interference Geolocation

Alexis Bose

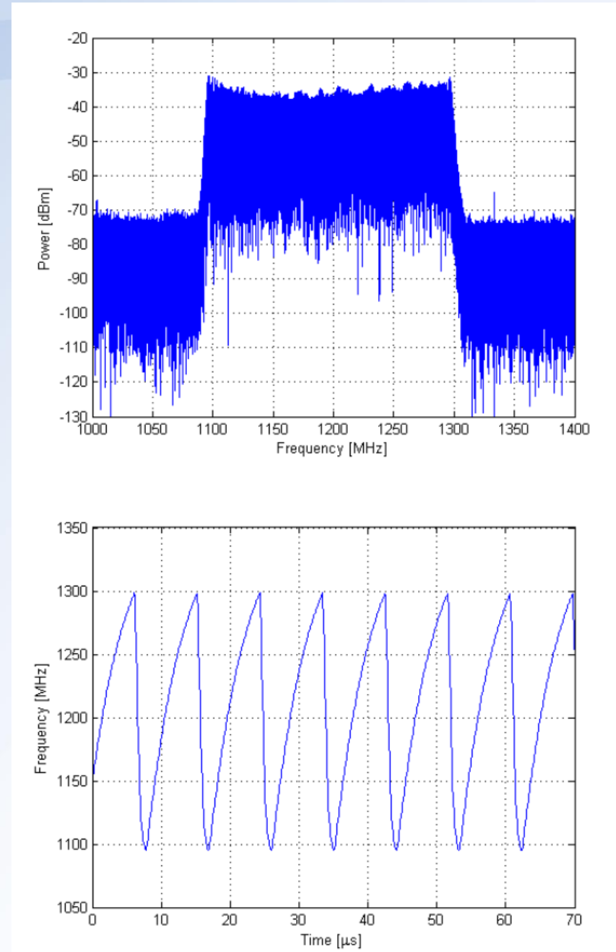
September 11, 2017

Communication Research Centre Canada

- Research to advance efficient usage of the Radio Spectrum
- Canadian government lab that provides long-term technical advice for spectrum management, regulation and policy
- Support critical wireless telecommunications operational requirements of other government departments
- R&D collaborations to leverage CRC research

Introduction

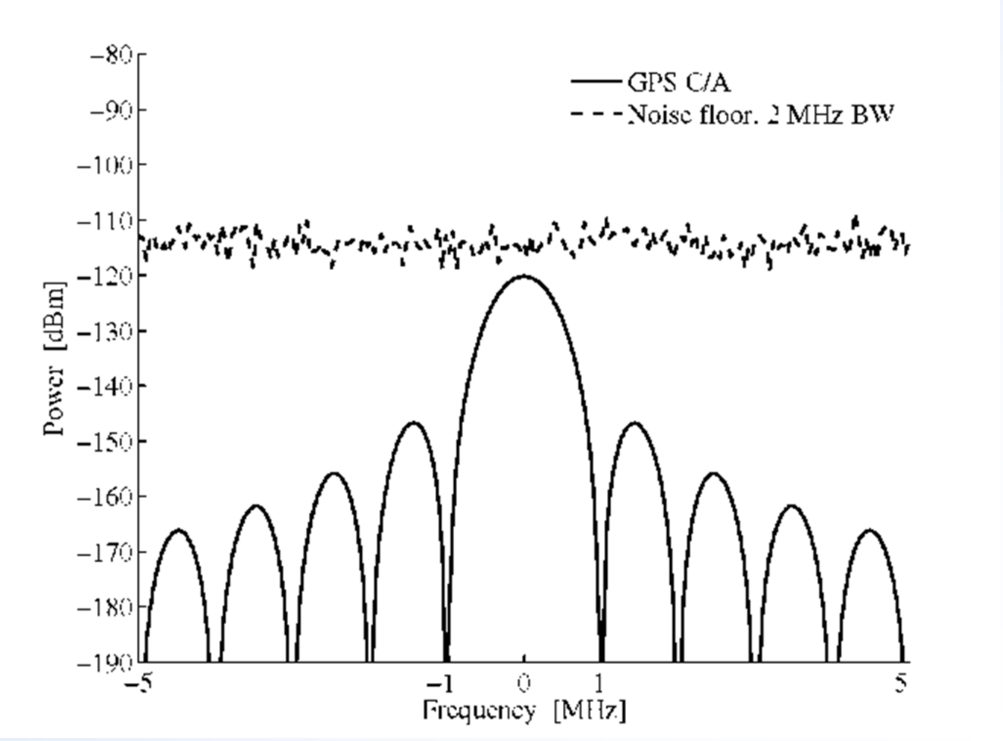
- What is a Jammer ?



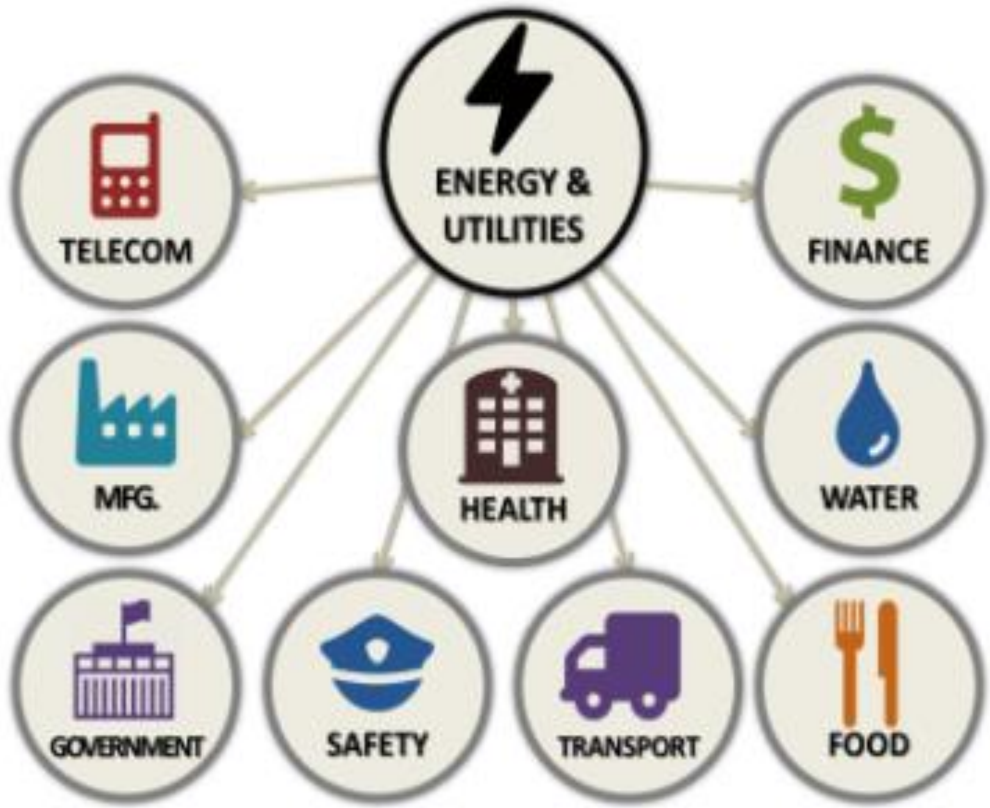
- Why are GPS Jammers used?

Why so Vulnerable?

Received GPS signal power is about -120 dBm



What is the big deal?



Canada's 10 Critical Infrastructure Sectors

- Critical Infrastructure -

2.5m - boat min requirement (7.5ns) to enter harbour

20 ns - internet time (PTP)

40 ns - aeronautical (Comms)

30 ns - aeronautical (ADS-B)

50 ns - electrical grid
(phase measurement)

How frequent are jammers ?

- CRC work:

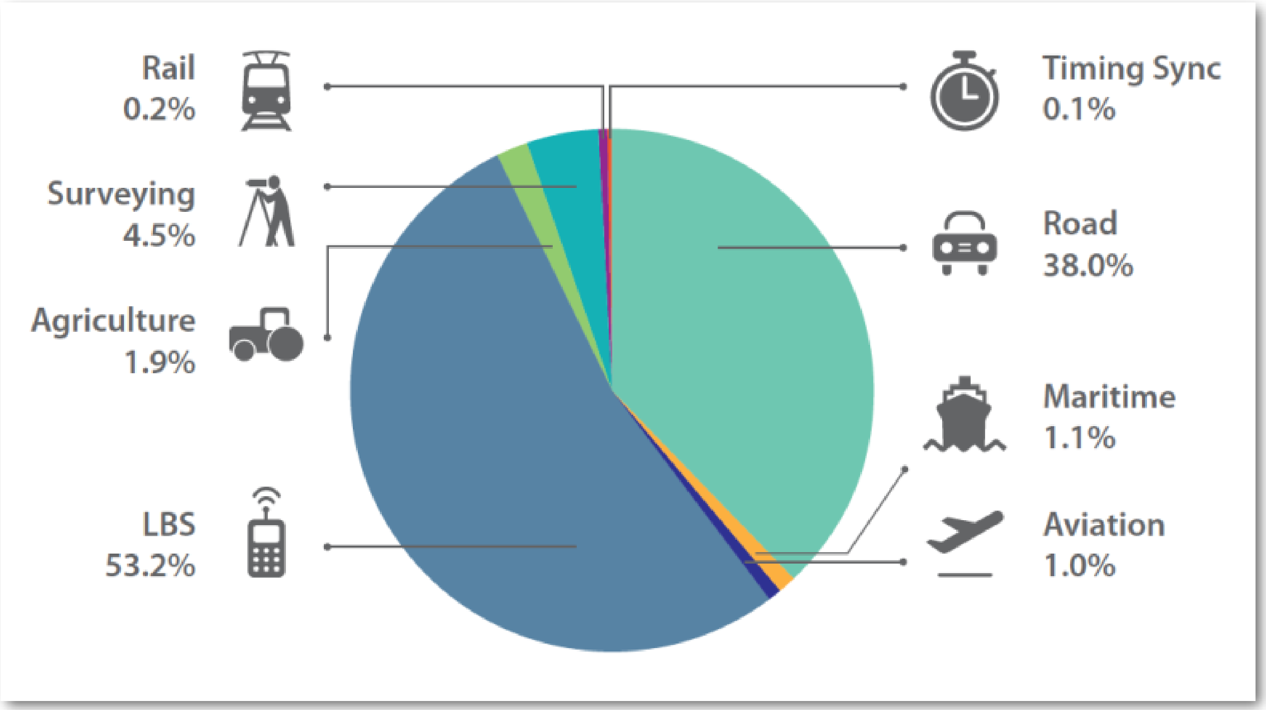
➢ 2011 Ottawa Highway: 2-4 jammers/day for 3 weeks

➢ 2012 Montreal Airport: 3-4 jammers/day for 2 weeks

➢ April 2017 - present Ottawa Highway: 5-8 events/day (24/7 monitoring)

GNSS (GPS, GLONASS, Galileo) supporting Industry

Cumulative Core Revenue 2013-2023
Valued at approximately **€2.8T**, or **$4.1T CAD**

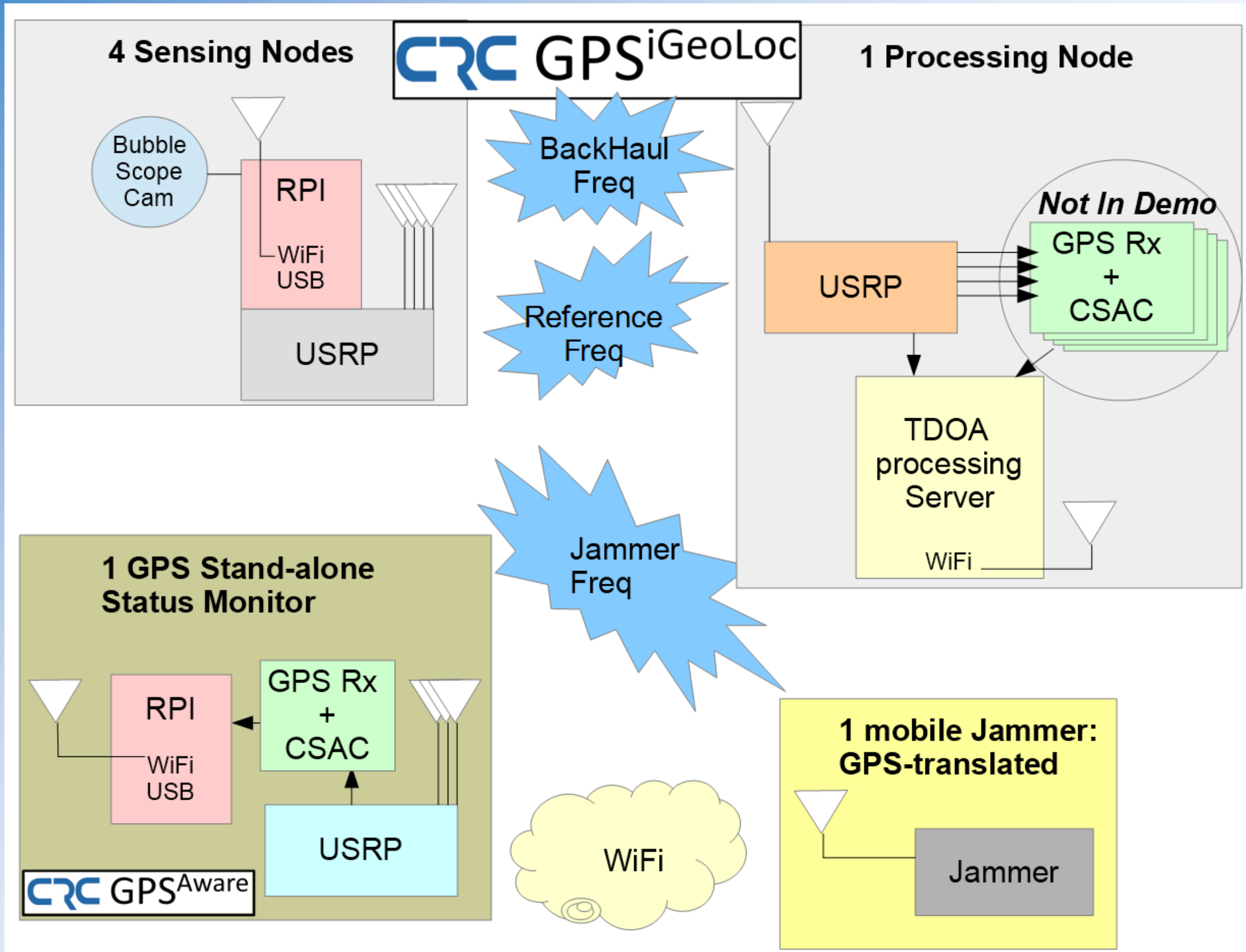


Source: European GNSS Agency (2015) *GNSS Market Report*, Issue 4

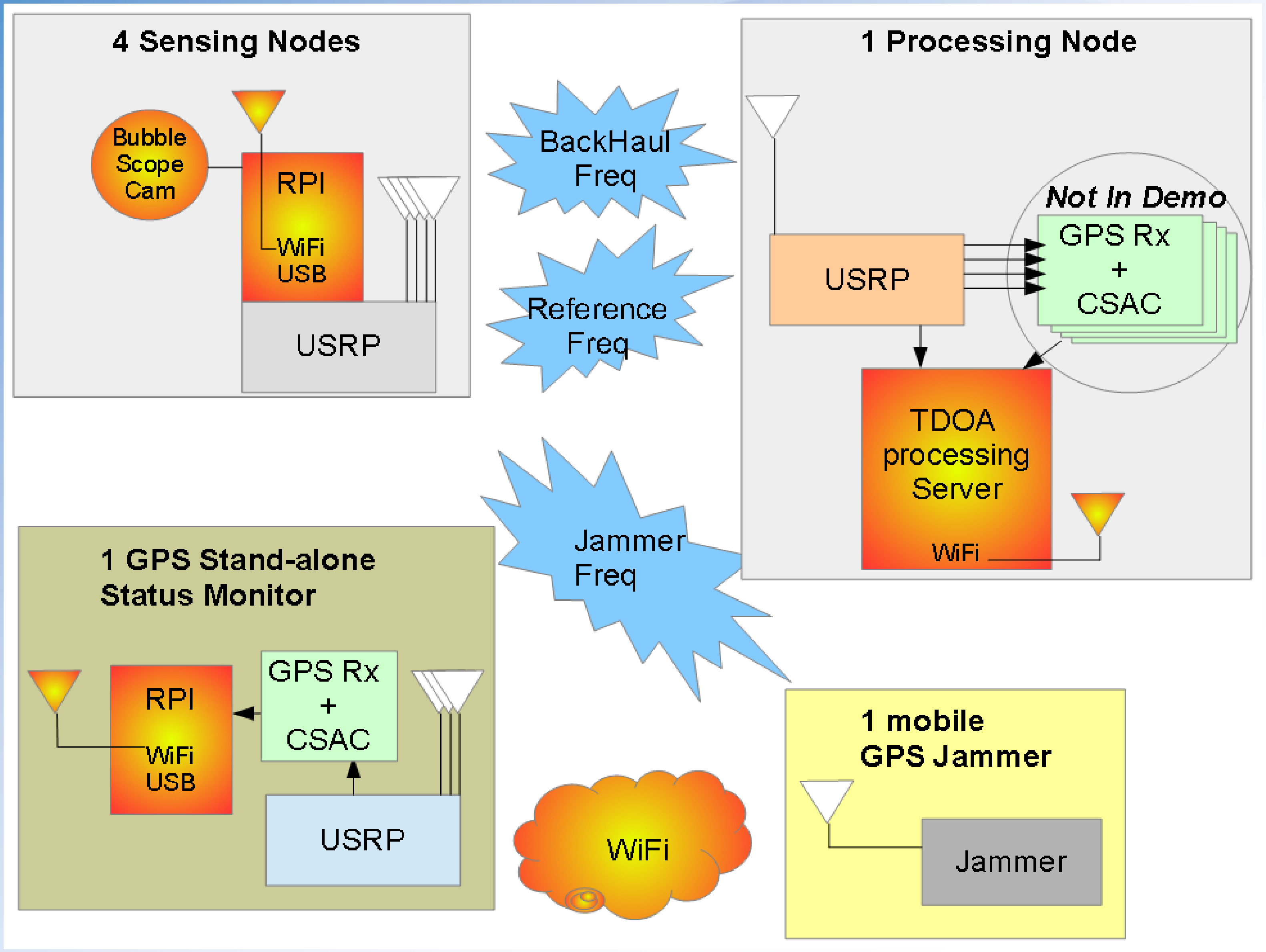
Project Objectives

- Demonstrate near real-time geolocation of GPS Jammers using the Time Difference of Arrival (TDOA).
- Leverage project experience as inputs into other CRC projects
- Demonstrate a low-cost field deployable spectrum monitoring application

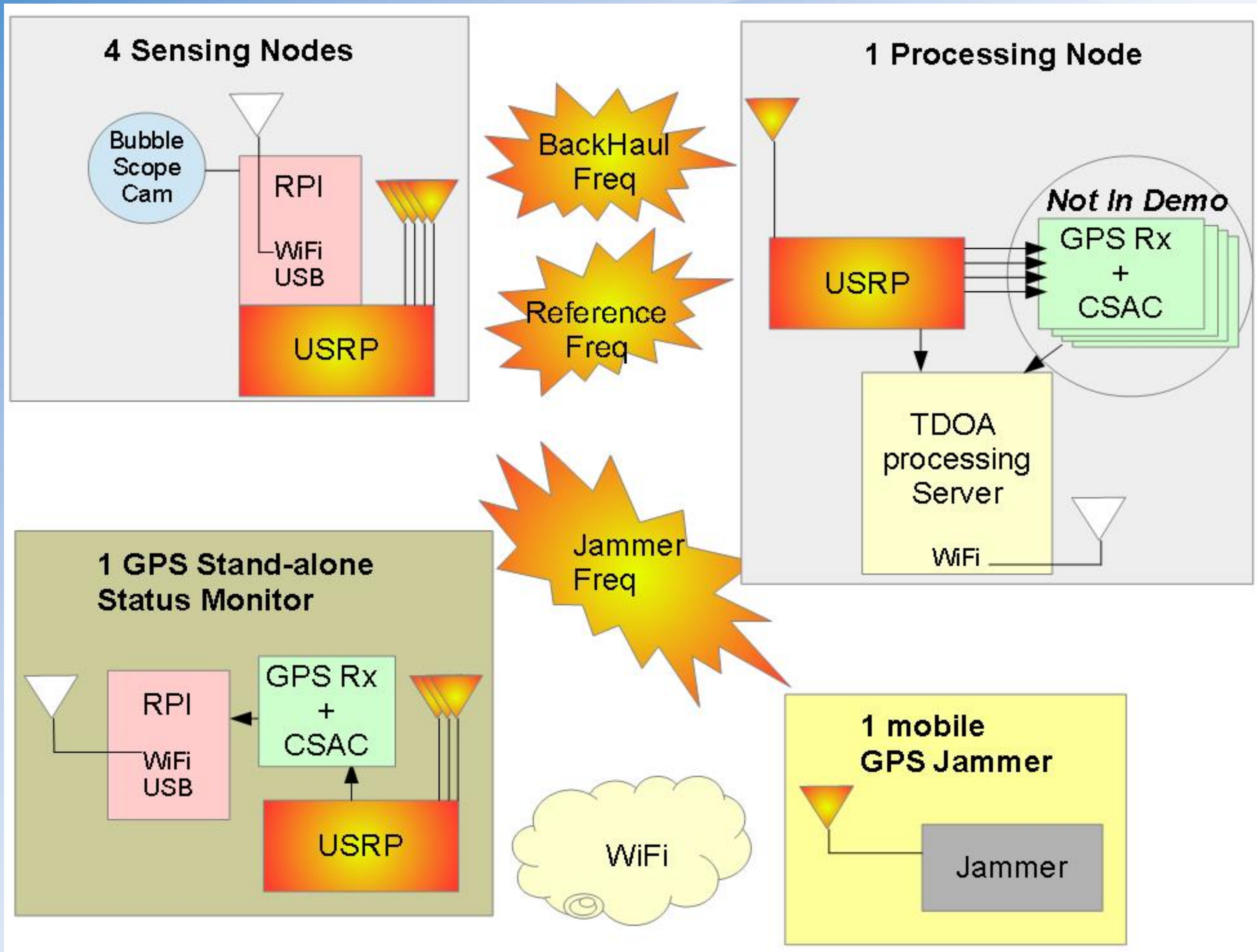
System Diagrams


GPSiGeoLoc
4 Sensing Nodes
Bubble Scope Cam
RPI
WiFi
USB
USRP
BackHaul Freq
Reference Freq
1 Processing Node
Not In Demo
GPS Rx + CSAC
USRP
TDOA processing Server
WiFi
1 GPS Stand-alone Status Monitor
RPI
WiFi
USB
GPS Rx + CSAC
USRP
GPSAware
Jammer Freq
WiFi
1 mobile Jammer: GPS-translated
Jammer

Control-Network in Orange

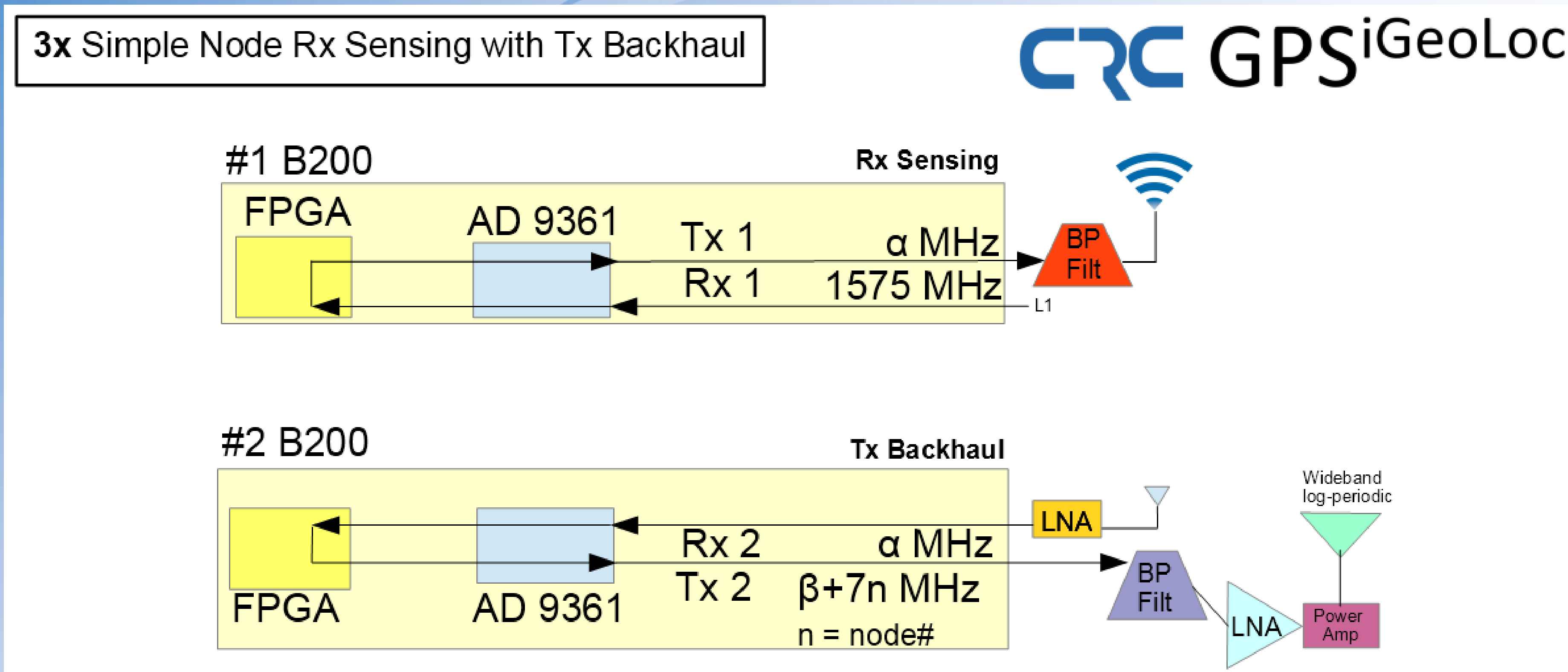


Data-Network in Orange

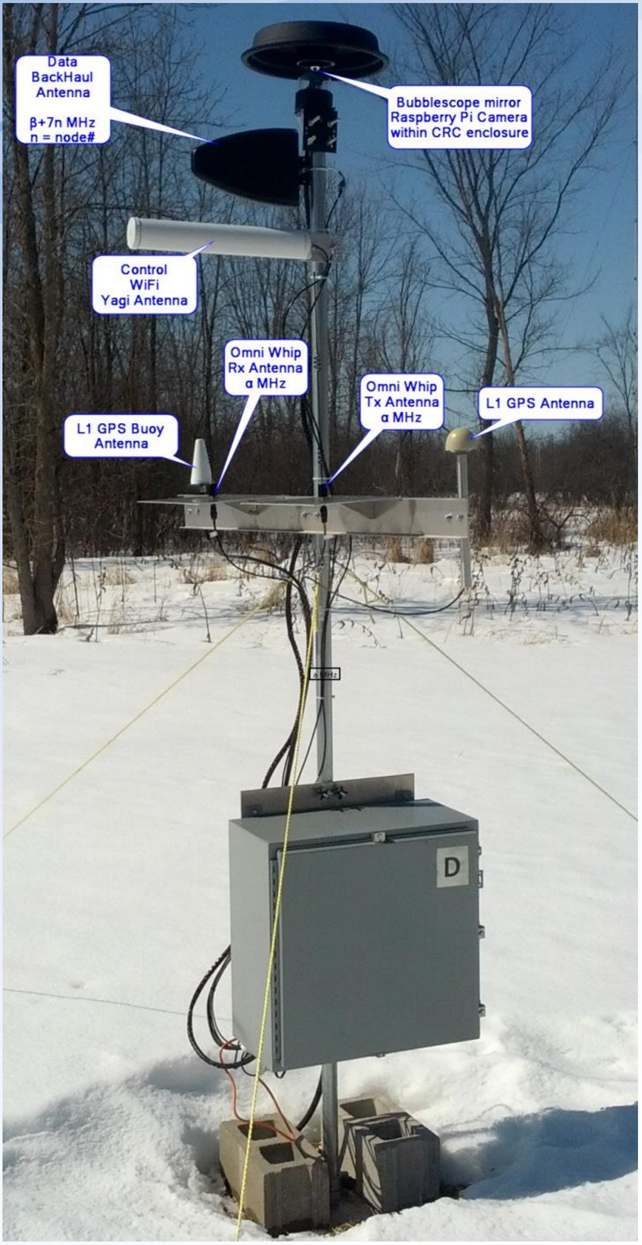


GPS-Translated Jammer Setup

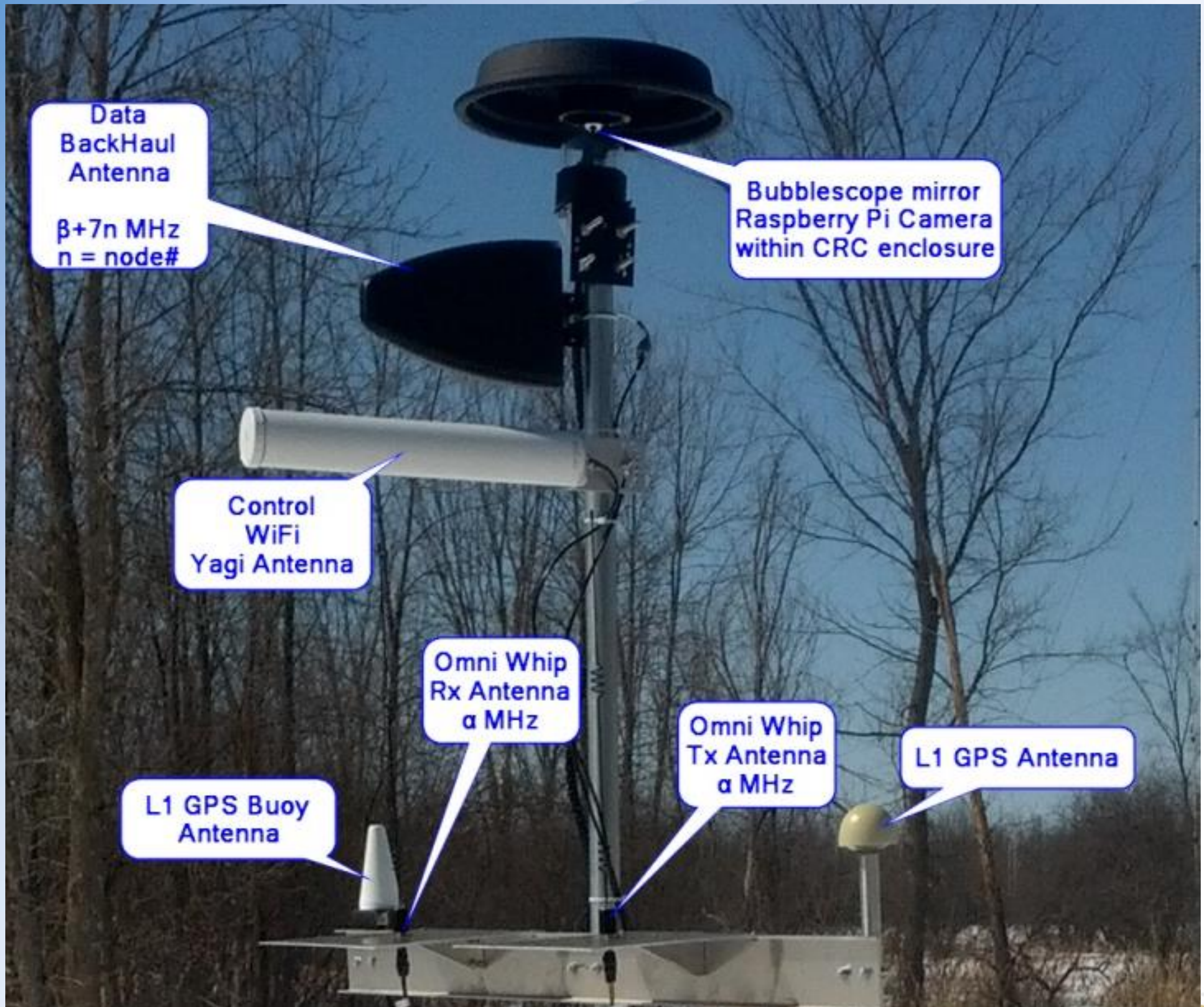
Detailed Diagram – Sensor Nodes



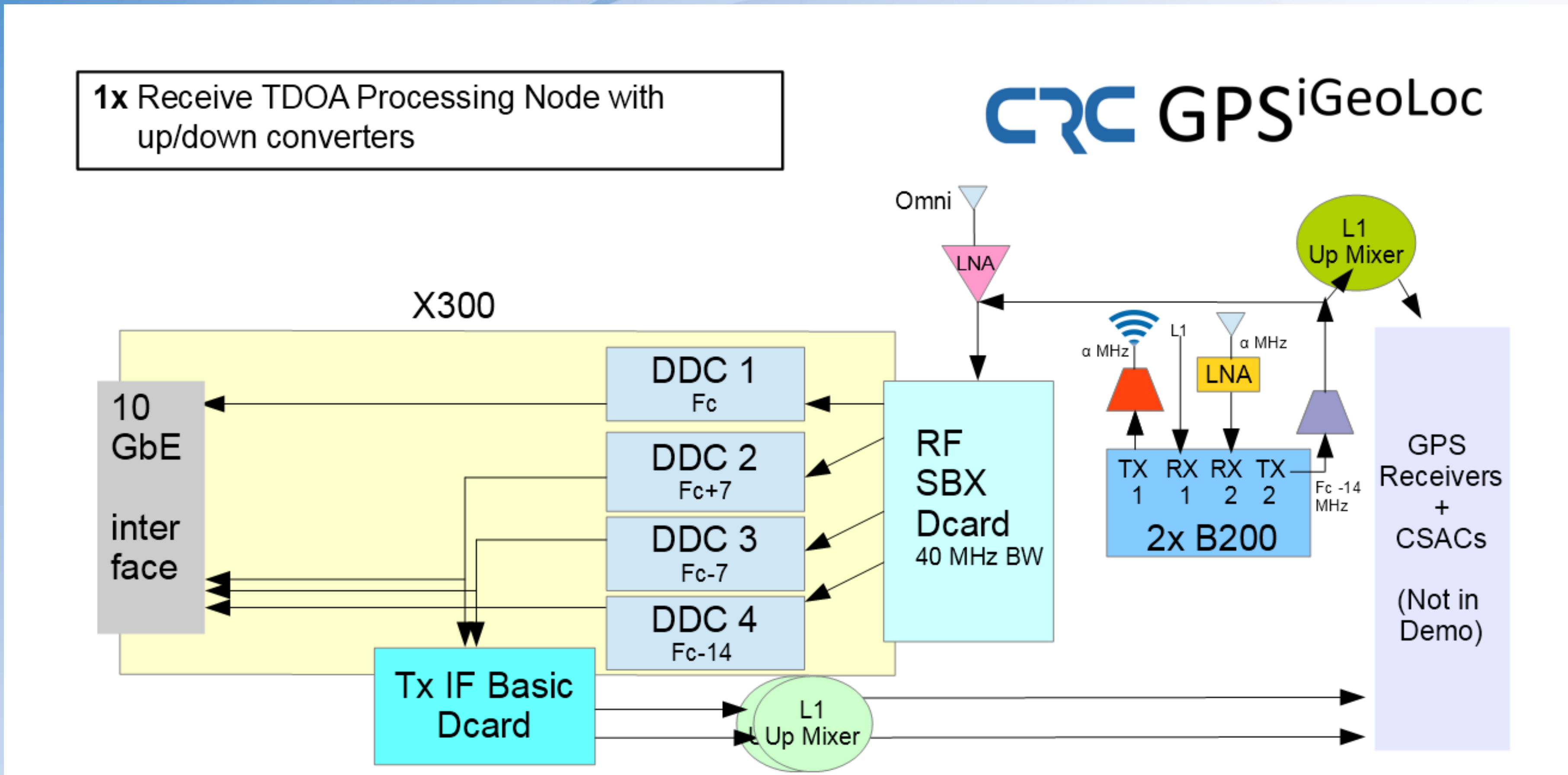
Sensor Node Setup



Sensor Node Setup



Detailed Diagram – TDOA Processor Node



Processing Node Setup

Calibration Example

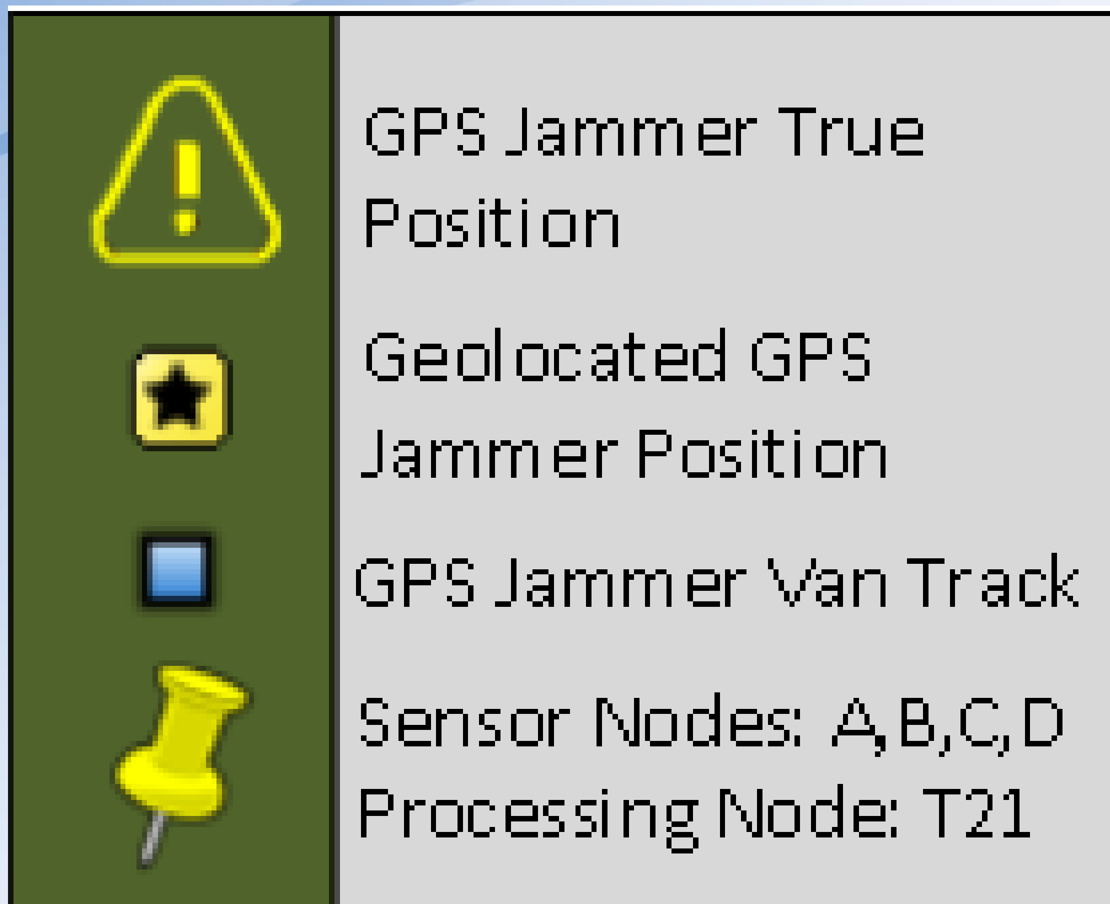
All paths = Transmitter to Sensing Node (A,B,C,D) to Processing Node (T21)

$$
\begin{aligned}
A_{node} - D_{node} &= 2\ (empirical) \\
A_{node} - B_{node} &= -1\ (empirical) \\
C_{node} - A_{node} &= 0\ (empirical)
\end{aligned}
$$

$$
\begin{aligned}
C_{node} - B_{node} &= (C_{node} - A_{node}) + (A_{node} - B_{node}) = -1 \\
B_{node} - D_{node} &= (A_{node} - D_{node}) - (A_{node} - B_{node}) = 3 \\
C_{node} - D_{node} &= (C_{node} - A_{node}) + (A_{node} - D_{node}) = 2
\end{aligned}
$$

units 200ns or 59.95 meters(65.56 yd) based on 5 MHz BW

Demonstration

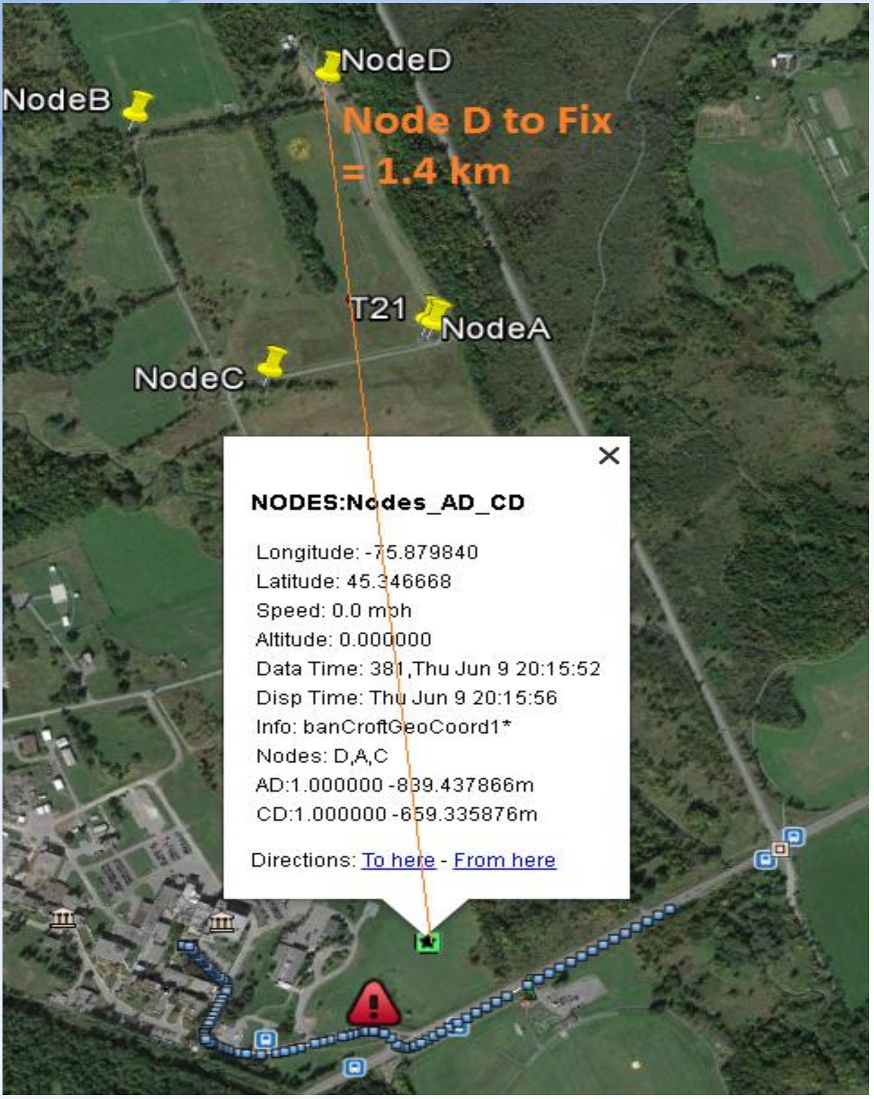


Raw Signal Processing Results 😐

Raw Signal Processing + snap to road filter ☺

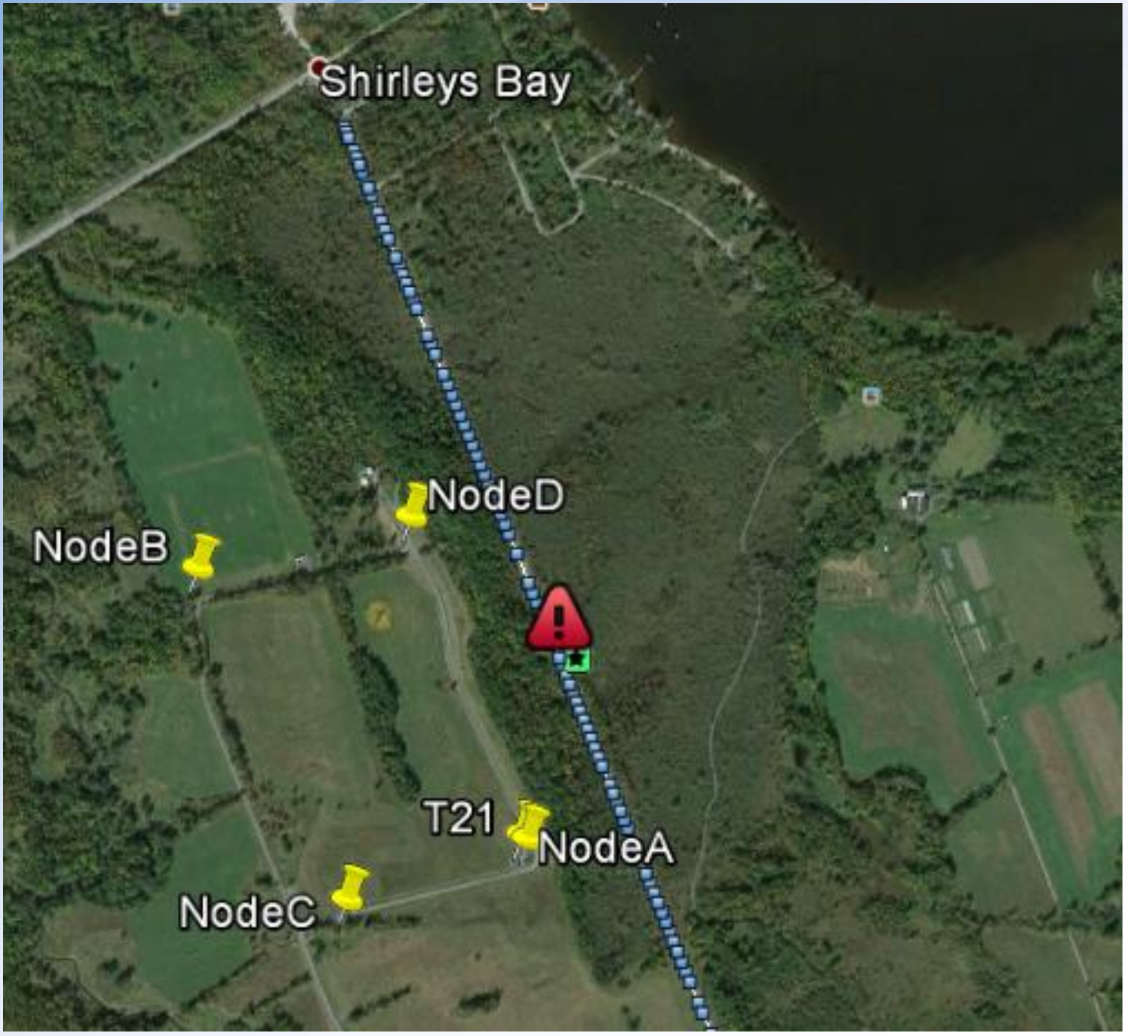
CRC GPS^{iGeoLoc}

Range Example (1.2 W)



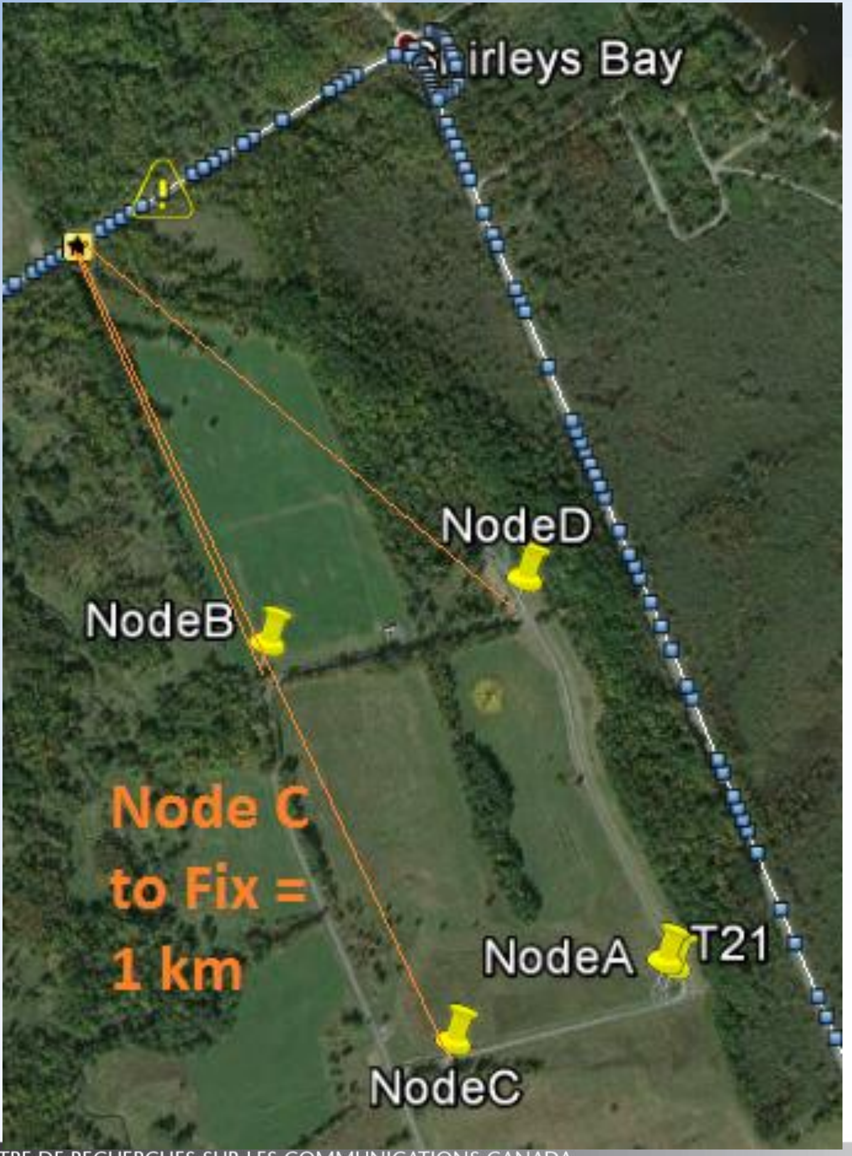
GPS[iGeoLoc]

Range Example (1.2 W)



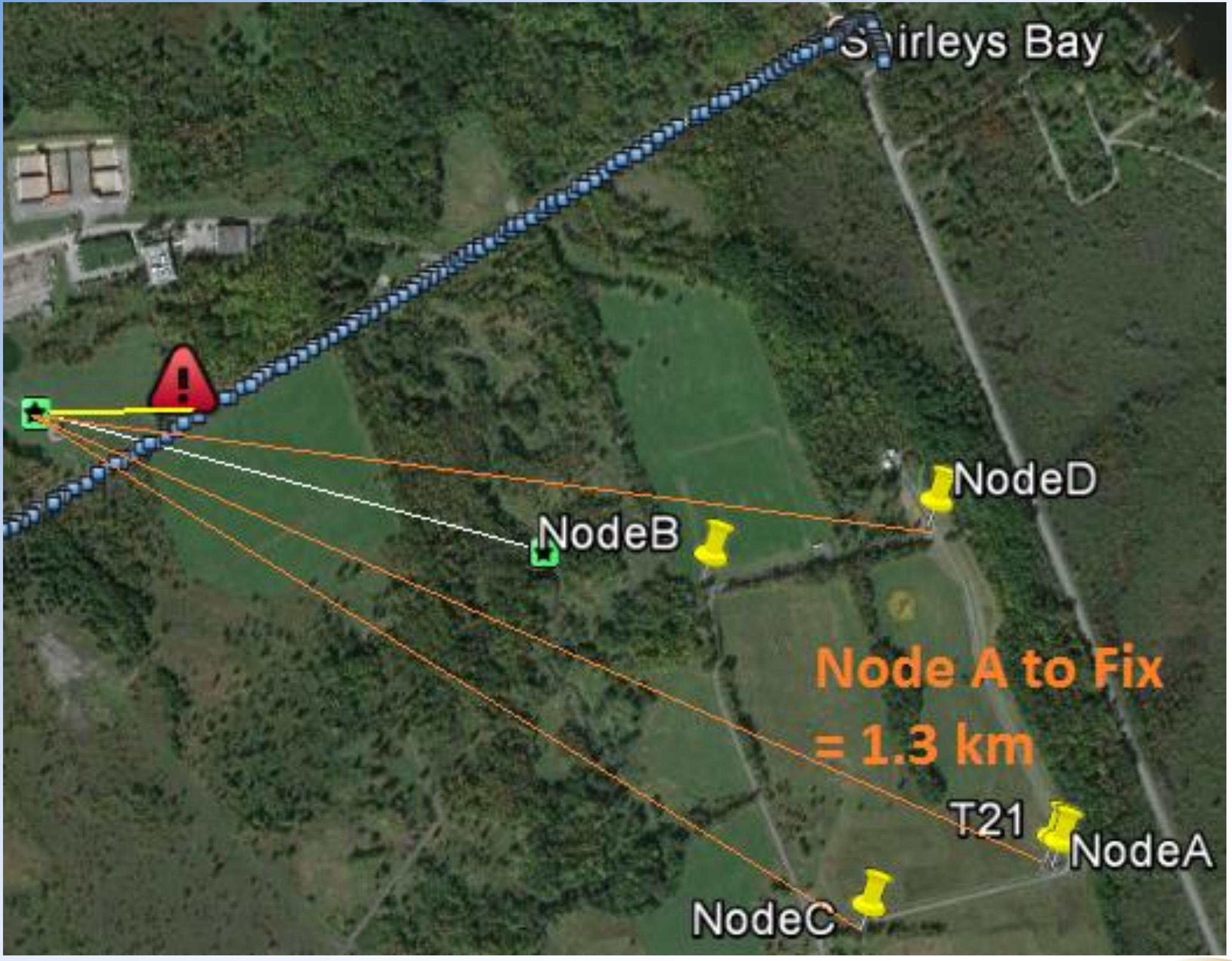
GPS^{iGeoLoc}

Range Example (1.2 W)



GPS iGeoLoc

Range Example (1.2 W)



Performance of Other Existing Systems

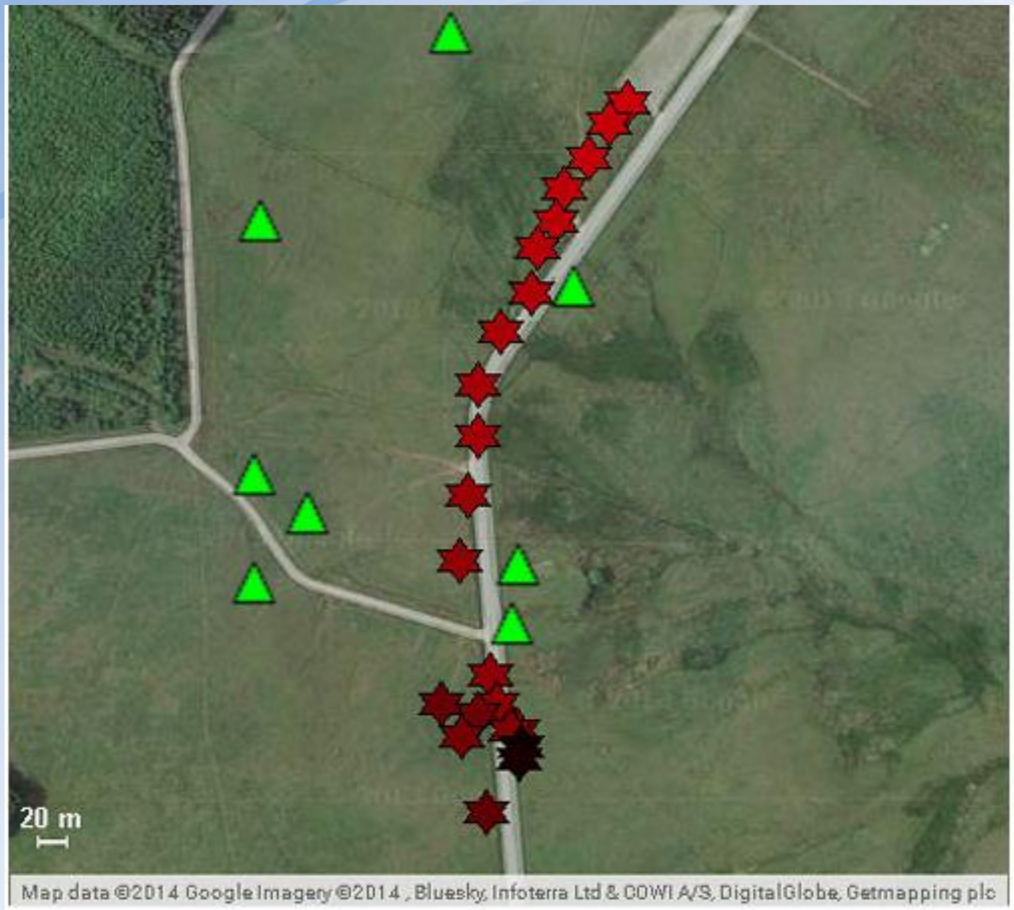


FIGURE 3. Jammer locations detected by Signal Sentry, when jammer was driven at 50 miles per hour, north to south. Green triangles denote sensor locations.

GPS^{iGeoLoc}

Results

CRC GPS^{iGeoLoc}

- Track *<u>route</u>* of a mobile 200mW GPS jammer
- 4 sensing nodes covering a:
  450m (yd) x 300m (yd) track
- ~10 second delay, with a 0-20 meter (yd) error

CRC GPS^{iGeoLoc} Range

- Track *<u>position</u>* of mobile 1200mW GPS jammer
- Some detections at 1.4 km (0.87 mi) away,
  with a ~150 meter (yd) error

Novel Achievements: CRC GPS^{iGeoLoc}

- No jammer waveform assumptions
- No time-stamping
- Local reference (27 MHz)
- Small datasets: 10MB of data per sensing node
- Less than 30 seconds calibration
- 4 to 20 seconds time to geo-locate
- Snap to Road Filter
- Low Cost $4K/sens node + $15K/proc node

Novel Achievements: CRC GPS^{Aware}

- < $4K/box
- Ease of Use
- 1 second detection time
- measure actual GPS outage time

Signal Processing and Geolocation

Cross-correlation and Processing

- 2^{18} number of complex samples at 5 MHz bandwidth used for stationary assumption at highway speeds

- Overlapped cross-correlation of multiples of 8192 blocks of complex samples

- 5 MHz bandwidth allows a peak resolution of 200ns (or 59.95 meters (65.56 yd))

Cross-correlation and Processing

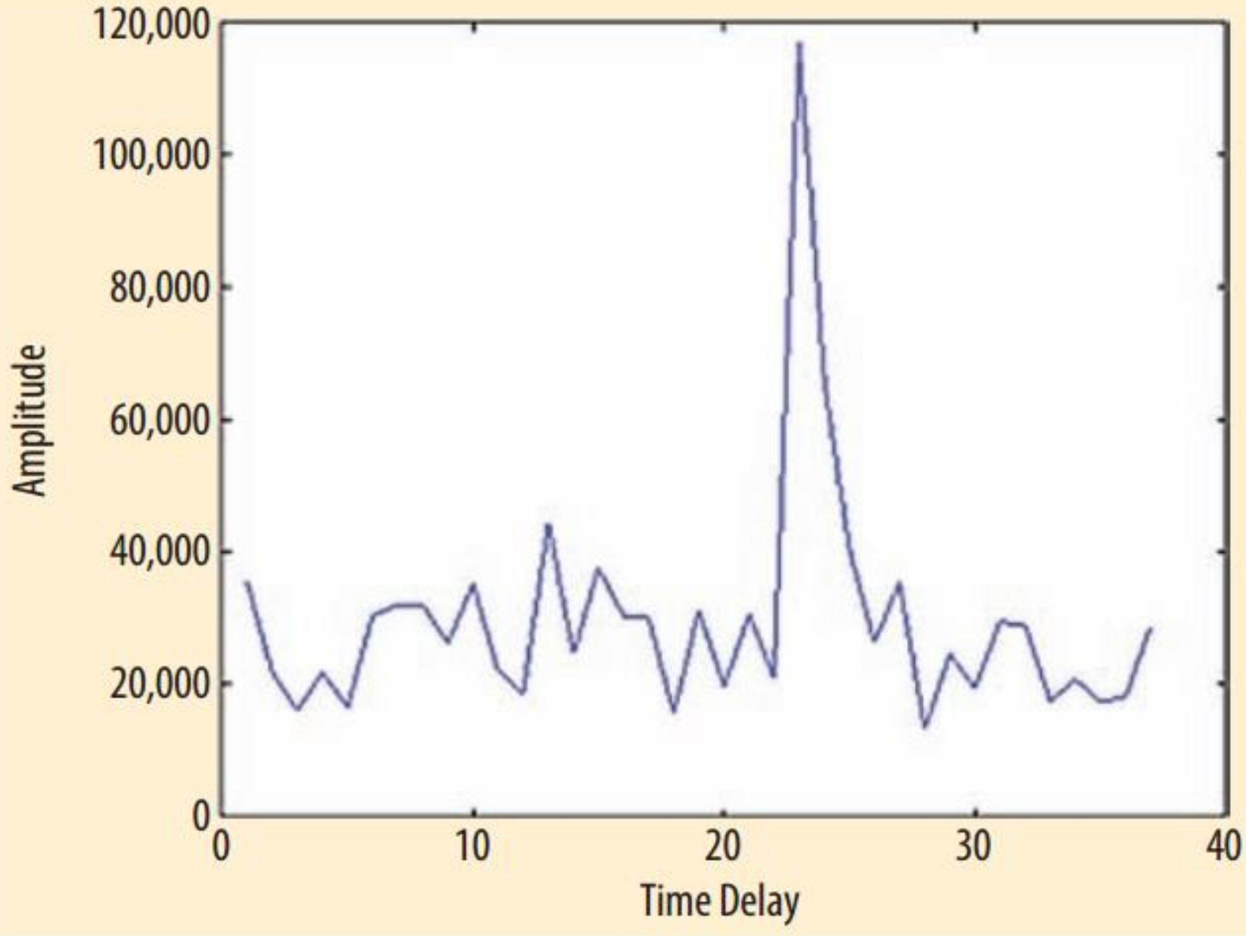


FIGURE 3 Cross-correlation output

Mode Filtering

- True correlation peak should be more common than noise
- Only if the mode of the overlapped cross-correlations > 70 % occurrence, then it is used as node pair time difference.

Multipath Mitigation

- Metric = *magPeak1 – magPeak2*
- Only peaks above a noise level (NL) are used.
- The NL = first peak, in descending order, which is at most 2/3 amplitude of the previous peak.
- Peak with least delay of the two max peaks above NL
- Parabolic interpolation (valleys between peaks)

Multipath Mitigation

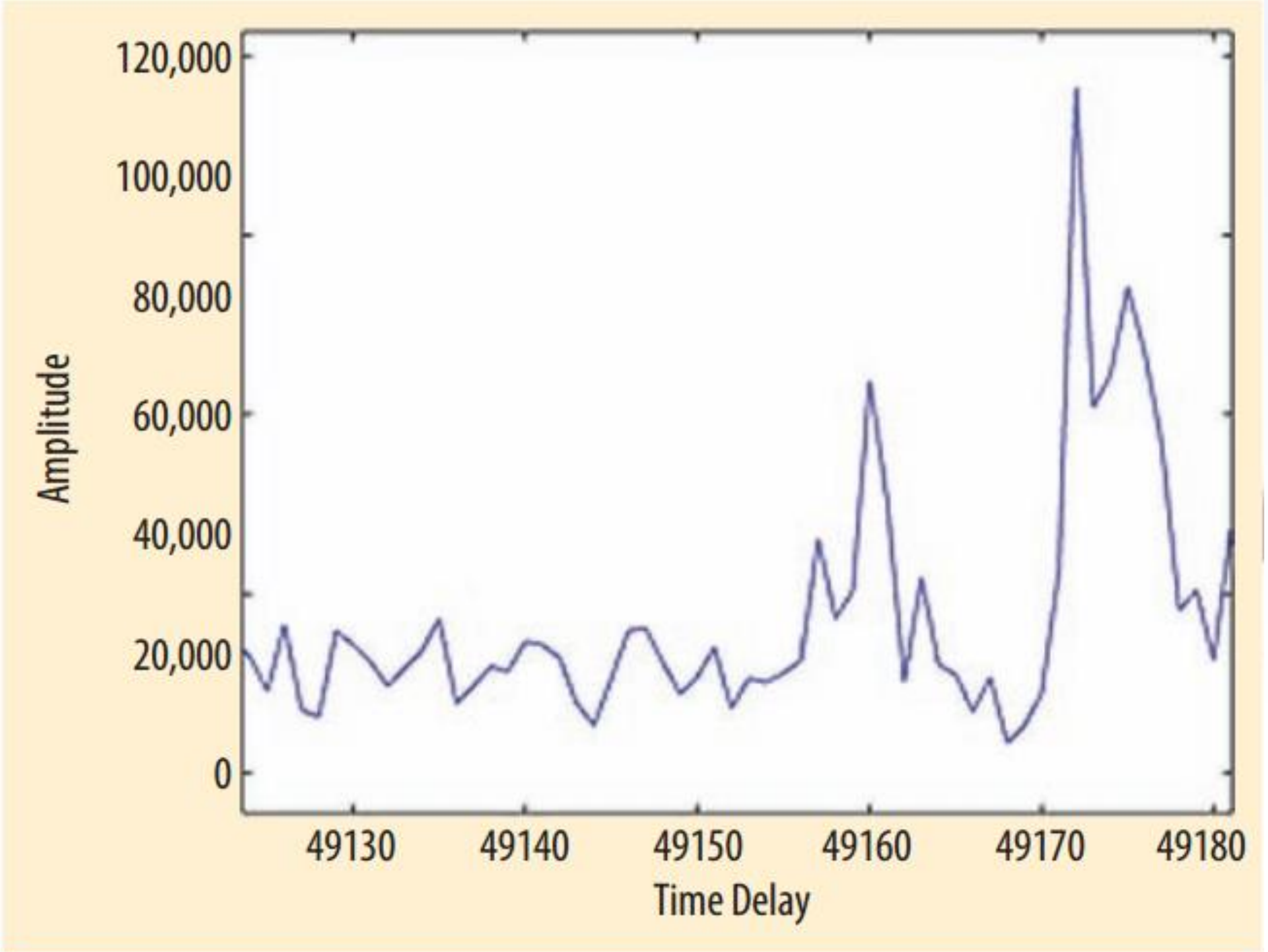


FIGURE 4 Cross-Correlation result with multiple peaks

Geolocation: Hyperbolic intersection

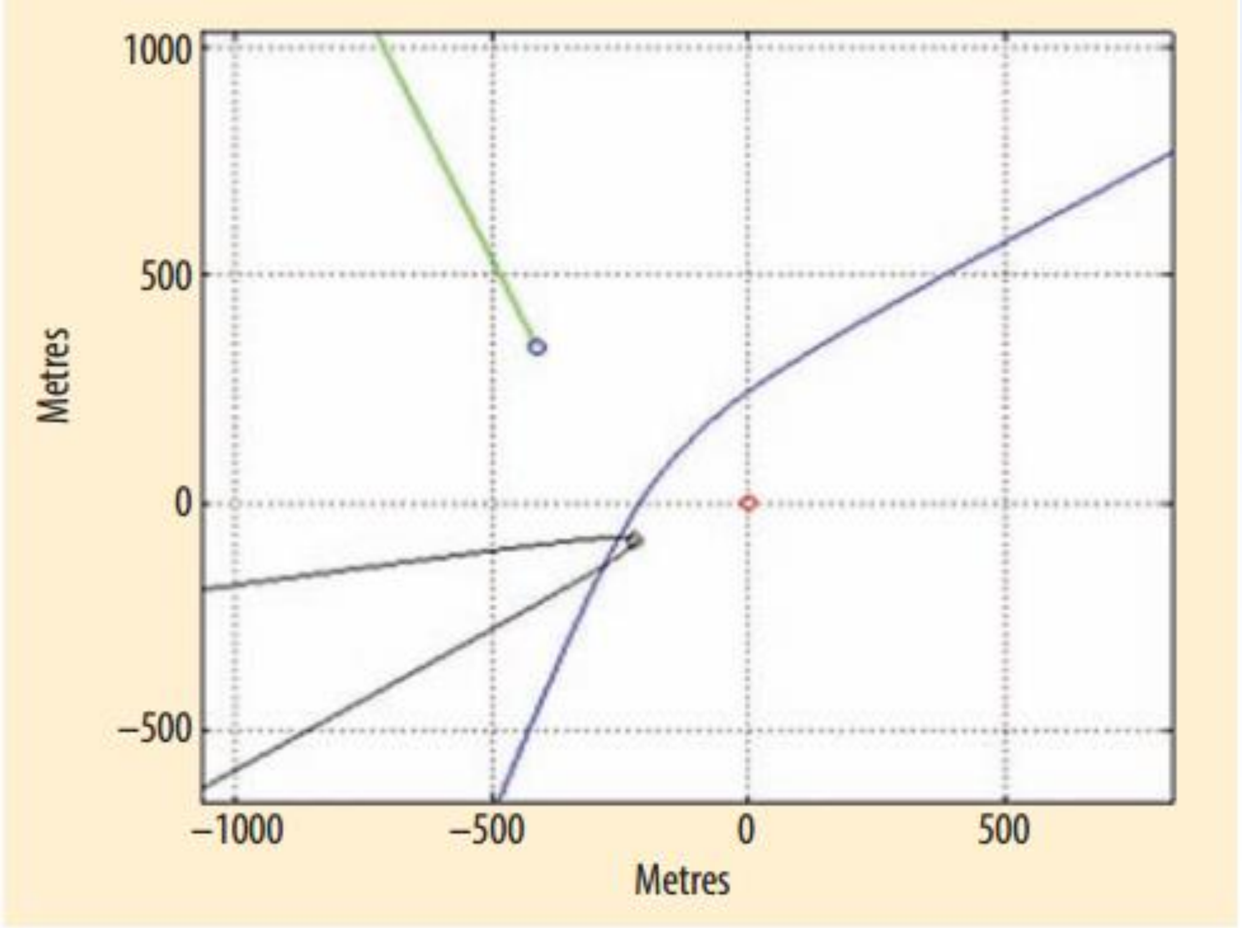


FIGURE 5 Multiple Solutions due to Hyperbolic intersections Sensing Nodes (A,B,C) are circles. Blue and black hyperbolas intersect at two points.

Bancroft multilateration for GPS

$$\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + b = p_i$$

i = satellites > 3 to get (x,y,z,t) result

p_i = satellite pseudorange

b = error in receiver clock

Lorentz inner product trans (2x) to solve analytically

Bancroft multilateration for jammer detection

$$\sqrt{(x_i - x)^2 + (y_i - y)^2} + \mathrm{b} = p_{\mathrm{i}}$$

i = sensor node = 3 to get position (x,y,t)

p_{i} = jammer pseudorange

b = error in receiver clock

Lorentz inner product trans (2x) to solve analytically

Filtering Recap

When does data get thrown out?

- Mode of all cross-correlations is < 70% of results
- Multipath: > 2 peaks above NL
- Bancroft Algorithm does not find a solution
- Snap to Road geo-located point is not possible in route

Future Optimization

- Overcome backhaul limitation with spread spectrum
- Upgrade Ettus SBX Daughtercard to TwinRx for X300 in processing node (superhet better sensitivity)
- Open alternative to the Intel I.P.P.

Recognition

Team

Wayne Brett (RF wireless)

Paul Guinand (geolocation, domain expert)

Russell Matt (mech, thermal, power, network)

Communication Research Centre Canada's Expertise

Ettus Research (NI)

past and present employees

Open Source Community

OSRM, PF_Ring, BubbleScopeCL, GNURadio…

Thank you

Merci

Is it possible to build a low-cost system to detect and locate a single GNSS jammer in near-real time?

http://www.insidegnss.com/node/5307