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

GNSS Solutions is a regular column featuring questions and answers about technical aspects of GNSS. Readers are invited to send their questions to the columnist, **Dr. Mark Petovello**, Department of Geomatics Engineering, University of Calgary, who will find experts to answer them. His e-mail address can be found with his biography below.

MARK PETOVELLO is a Professor in the Department of Geomatics Engineering at the University of Calgary. He has been actively involved in many aspects of positioning and navigation since 1997 including GNSS algorithm development, inertial navigation, sensor integration, and software development. Email: mark.petovello@ucalgary.ca

GNSS jammers are an ongoing threat to the reliable use of GNSS. The problem of geolocating GNSS jammers can be addressed using a time-difference-of-arrival (TDOA) processing technique; however, this problem is quite different than geolocating jammers in other radio frequency systems. The two main differences are:

(1) No GNSS are available to use as a timing reference.

(2) The signal of interest (i.e., the GNSS signals) are weak. This contrast with other applications (e.g., mobile phone jamming) where the signal of interest is much stronger.

The first point forces the TDOA technique to be unconventional, but still possible. The second point eliminates the complexities of having to discern desired versus undesired signals in the band.

To address these issues the Communications Research Centre (CRC) Canada, which is the Government of Canada's primary laboratory for wireless research, has been doing work in this area. Two complementary systems were devised to solve the problem of geolocating a single GPS jammer: *iGeoLoc*$_{GPS}$ (interference Geolocation) and *jAware*$_{GPS}$ (jammer situational awareness). *iGeoLoc*$_{GPS}$ can geolocate GPS band interference, but the effect on a GPS receiver is unknown. *jAware*$_{GPS}$ can indicate if a GPS receiver is jammed, but not geolocate the jammer source.

The *iGeoLoc*$_{GPS}$ uses a 5 MHz bandwidth centered at GPS L1. The *jAware*$_{GPS}$ examines all outputs of a GPS timing receiver for both timing and position errors and other irregularities.

In order to facilitate testing with an illegal device, a typical GPS chirp jammer was frequency-translated to a nearby experimental-licensed band and will be referred to as the translated-jammer. The "jammer" will refer to a signal source originating from either an intentional jammer device or a source of unintentional interference. Intentional or not, both sources can degrade a GPS receiver.

System Level

First, let's take a look at the overall jammer detection systems under consideration.

***jAware*$_{GPS}$ Description.** In some cases only awareness that the on-site GPS signal is being disrupted is required. *jAware*$_{GPS}$ is meant to answer the question: "Do we have a jamming problem?"

This stationary sensor uses the number and received power of satellites, positional drift, GPS receiver lock status, and the accuracy of the pulse-per-second (PPS) output to determine the status of a GPS receiver. The PPS error is measured using the internal phase meter of a chip scale atomic clock (CSAC).

The phase meter measures the time difference, with a resolution of 450 picoseconds, between the internal CSAC 1 PPS and the externally applied PPS from the GPS receiver. In order to use the phase meter the CSAC is always configured in 1 PPS discipline mode with a 10-second time constant, and the PPS time difference is reported once a second (cycle to cycle) in nanoseconds. If the PPS time difference exceeds 10 nanoseconds, the position drifts more than a threshold, or a sudden change occurs in satellite informa-

tion, a GPS outage is reported until the signals are stable for 10 seconds.

***iGeoLoc*$_{GPS}$ Description.** The current *iGeoLoc*$_{GPS}$ (**Figure 1**) uses four semi-transportable *sensing nodes* (A, B, C and D) connected in two separate networks: a real-time data network and a Wi-Fi control network.

Each sensing node receives the translated-jammer band and retransmits it in its own dedicated backhaul band to the processing node (**Figure 6, 8, and 9**). This continuous real-time frequency translation is referred to as the *data network*.

The jammer geolocation is calculated at the processing node using a TDOA technique followed by a geolocation algorithm. No waveform assumptions are used. A blind cross-correlation is computed between all pairs of sensing node datasets to determine their relative time differences of arrival.

A common jammer signal must be detected by at least three sensing nodes. This permits at least two time differences to be calculated and then used to generate possible hyperbolic intersections and hence possible geolocation points (in the horizontal plane).

The TDOA cross-correlation and geolocation processing works with 218 complex samples per node and has a latency of 6 to 10 seconds. As the processing node continuously receives all sensing node data, geolocation points can be continuously produced with the aforementioned latency.

In order to achieve greater sensitivity, the low-level processing is required to do overlapped cross-correlations of different sizes across all three combinations of sensing node data. These cross-correlations are then mode filtered, multipath-filtered, parabolically interpolated, and given a quality metric.

Cross-correlation qualities that are greater than a predefined threshold are then fed into the Bancroft geolocation algorithm, which enable one to obtain a direct solution of the receiver position and the clock offset without requesting any *a priori* knowledge for the receiver location. The geolocation results can then be enhanced by an optional snap to the road filter. We will provide details of these steps in the following sections.

***iGeoLoc*$_{GPS}$ Sensing Nodes.** Each sensing node contains two software-defined radios and the necessary RF filters and amplifiers to perform the previously mentioned frequency translation for the data network. Each sensing node is controlled by a small micro-processing computer that controls and configures both the radios and a camera attached to a panoramic lens. A panoramic photo is taken once a second, providing context to the geolocation results. The computer communicates on the Wi-Fi control network. The component cost of a sensing node is approximately $5,000 CAD (about US$3,777). (See **Figure 2**)

***iGeoLoc*$_{GPS}$ Processing Node.** The processing node uses an appropriate RF antenna, filters and amplifiers to

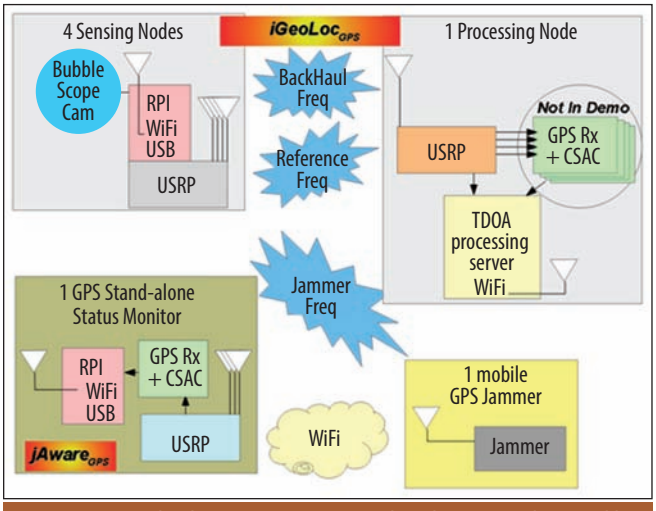

FIGURE 1 CRC Testbed *iGeoLoc*$_{GPS}$: one translated-jammer, detected by four sensing nodes, processed at one node for geolocation using separate data and control networks. *jAware*$_{GPS}$: actual GPS outage monitor

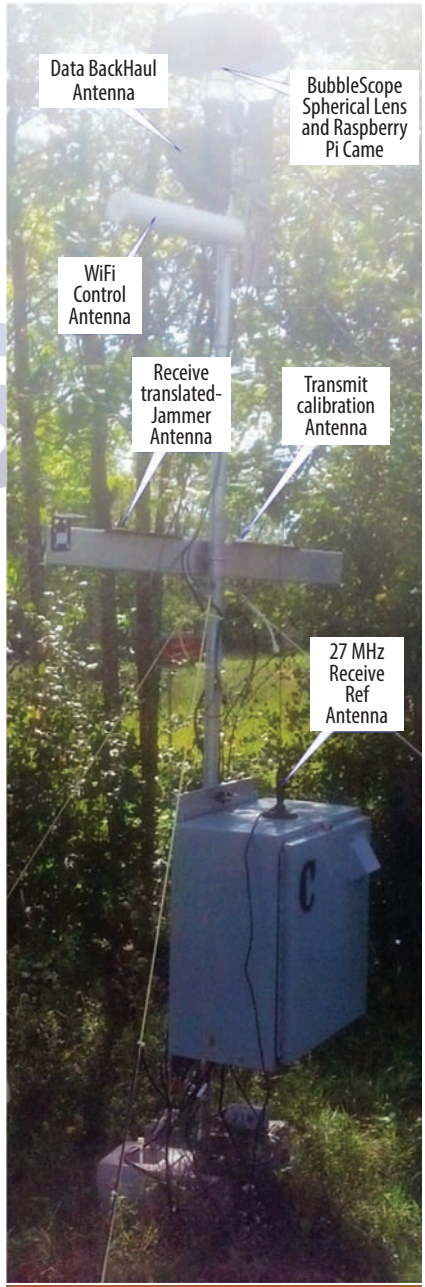

FIGURE 2 Sensing Node

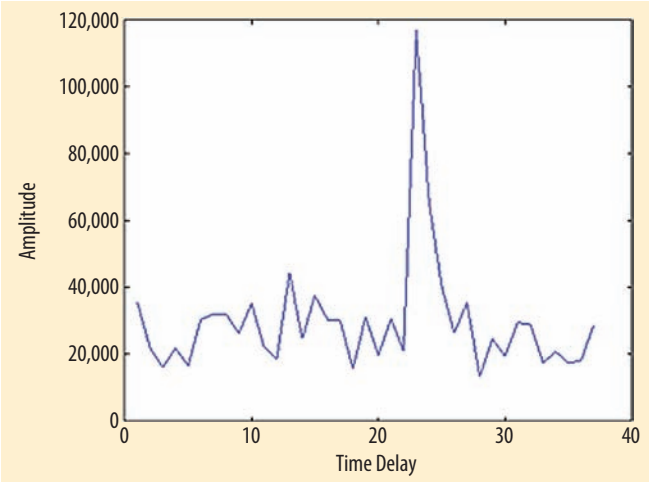

FIGURE 3 Cross-correlation output

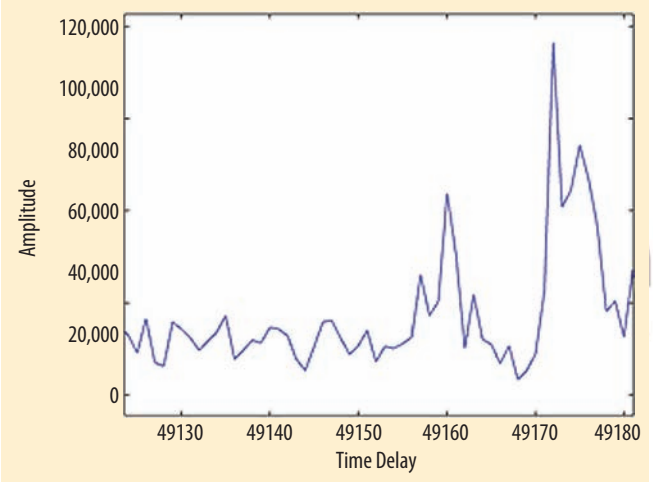

FIGURE 4 Cross-Correlation result with multiple peaks

allow a software-defined radio with a custom field-programmable gate array (FPGA) design to receive the four sensing node backhaul bands and digitally down-convert them synchronously to baseband. The previously described processing chain (cross-correlation through geolocation) is then performed. The component cost of the processing node was approximately $20,000 CAD (about US$15,108), which can be reduced by using a low-cost alternative to a server-class computer for signal processing.

Reference Frequency – 27 Megahertz. The sensing nodes' radios have RF local oscillators (LOs) that can drift relative to each other unless provided with a common reference. To avoid this, the processing node generates and transmits a continuous one-watt constant 27-megahertz tone as the reference signal. The 27-megahertz tone is in an industrial, scientific, and medical (ISM) RF band and in the range of the radios' acceptable reference phase locked loop (PLL) frequency (5 to 104 megahertz). The implementation of this reference scheme encountered standard HF difficulties, of large antenna dimensions and high RF power.

Cross-Correlation Processing. Traditionally TDOA is performed by calculating the difference of arrival between two signals with absolute timestamps. Since a difference is a relative measure, it does not need to be derived from two absolute measurements; the difference can be obtained from a cross-correlation process with a known relative offset between the two signals. A calibration process (described later) ensures that the offsets in a set of node-pair differences form a consistent set of equations for computing the jammer's location.

The cross-correlations are performed using 262,144 complex samples. With a bandwidth of five megahertz, a stationary assumption can be used for a source travelling at highway speeds. An overlapped method that varies the data block size by multiples of 8,192 complex samples was created to generate more cross-correlation results over the dataset that could then be used for the mode filtering (described later).

The five-megahertz sensing bandwidth also allows for cross-correlation peak determination with a resolution of 200 nanoseconds (59.95 meters). **Figure 3** shows an example cross-correlation result.

Multipath Mitigation. CRC developed a cross-correlation quality metric to ensure that only reliable data is used for locating the jammer. The metric is defined to be the magnitude difference between the highest and second-highest cross-correlation peaks in the cross-correlation function.

To illustrate the need for this metric, **Figure 4** shows how multiple cross-correlation peaks can result from multipath effects. These can sometimes be discerned based on having longer delays than the true signal, but this is not always possible. The peaks considered were above a noise level where the noise level is defined as the first peak, sorted in descending order (by magnitude), that is at most two-thirds the amplitude of the next-highest peak.

The system considered a maximum of two peaks and took the peak with the least delay; otherwise the cross-correlation was not used. Finally, a parabolic interpolation between samples was done to provide accuracies better than the 59.95-meter resolution mentioned earlier.

Mode Filtering. Low-level data processing involves mode filtering. In order to distinguish it from noise, a true cross-correlation peak should be consistent through a great majority of all the overlapped cross-correlations in the dataset. The geolocation algorithm only uses cross-correlations with a mode value greater than 70 percent occurrence.

Calibration of Sensing Node's Local Oscillators. The 27-megahertz common reference frequency locks (synchronizes) all the sensing nodes; however, it will arrive at the nodes at different phases. The phase difference between nodes will be a constant error. The system can calibrate out any constant errors as the TDOA technique is based on a difference in time that is relative. The calibration stage produces an offset for each combination of node pairs that compensates for all constant errors. A recalibration is required every time

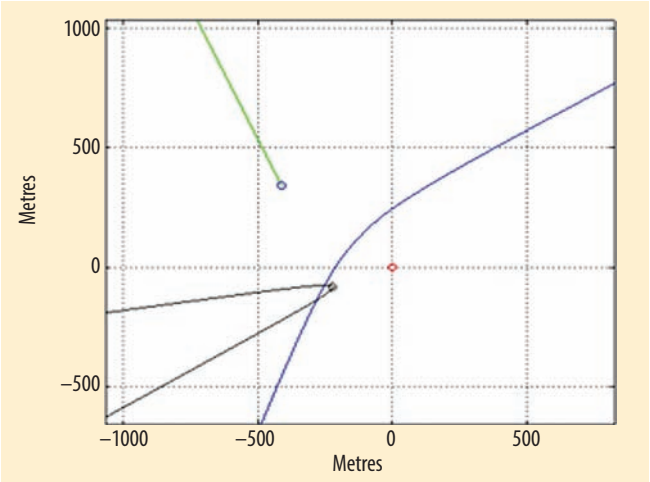

FIGURE 5 Multiple Solutions due to Hyperbolic intersections Sensing Nodes (A,B,C) are circles. Blue and black hyperbolas intersect at two points.

the radios' LO changes, which is on reconfiguration, restart or reboot.

A linear system of equations is empirically obtained by transmitting white noise in the translated-jammer band, from one node at a time and cross correlating the receiving nodes to get the corresponding delay. This noise is generated by a pseudorandom bit sequence (PRBS) in the software-define radios of the sensing nodes. A minimum of three node pairs are required to be determined empirically, and the others can be solved analytically.

Geolocation Algorithm. The geolocation is accomplished using Bancroft's Algorithm to solve the multilateration equations. However, this can result in multiple solutions due to the multiple points of intersecting hyperbolas, an example of which is shown in **Figure 5**.

A simple clustering algorithm is used to determine the best points. The clustering criterion is the number of neighbors within a pre-defined threshold distance. The remaining points can also be displayed, as shown in **Figure 6**. The clustering is only meant to aid a system operator and suffices for a stationary jammer, as the best points should be close together. However, if the jammer is believed to be mobile, a snap-to-road filter can be employed.

The snap-to-road filter uses the OSRM (open source routing machine) project (<https://github.com/Project-OSRM/osrm-backend>). Offline maps are generated for use with the OSRM algorithm, which uses a Hidden Markov Model as the probabilistic approach in determining route feasibilities. "No U-turns" is the only constraint used with the OSRM routing algorithm. **Figure 7** shows the estimated jammer position after applying the snap-to-road filter.

Geolocation to Google Earth – Testbed Visualization

In order to visualize the system, the processing node creates keyhole markup language (KML) files that describe the translated-jammer's position and the generated geolocation point(s). These KML files along with the sensor nodes' photos are sent over a one-kilometer Wi-Fi link to an office computer to display the results in Google Earth in near real-time (**Figure 8** and **Figure 9**).

FIGURE 6 Color clustering multiple results for one geolocation (red caution = jammer position, green stars = best solutions, white stars = other solutions). The blue trajectory illustrates the true jammer trajectory.

FIGURE 7 Jammer location after applying the snap-to-road filter

Interference Geolocation – *iGeoLoc*$_{GPS}$ Results

Parameters and results from recent experimentation performed at the CRC Testbed for the geolocation were as follows:

iGeoLoc$_{GPS}$ (interference geolocation)

- Tracked *route* of a mobile 200-megawatt GPS jammer
- Four sensing nodes covering a 450x300–meter track
- ~10second latency, with a 0–20-meter error

These excellent performance results led to some further validation tests outside of the CRC testbed, where we expected very poor performance due to the large network size and poor measurement geometry and obstructed propagation paths. The results were as follows:

iGeoLoc$_{GPS}$ Range

- Tracked approximate *position* of mobile 1,200-megawatt GPS jammer
- Some detections were 1.4 kilometers away (**Figure 10**)

Jammer Situational Awareness – (*jAware*$_{GPS}$) Results

The results for the situational awareness are:

jAware$_{GPS}$ (jammer situational awareness)

- detected only disruptive GPS jammers up to 200–250 meters away at highway speeds
- one-second delay, measured actual GPS outage time

To validate the previously described translated jammer testbed, *jAware*$_{GPS}$ was brought to a site along the highway in Ottawa where illegal GPS jammers were initially found in 2011. The *jAware*$_{GPS}$ sensor was used to trigger a low-cost spectrum recorder, with a multi-second ring buffer, upon jammer detection. A post-processing algorithm found some chirp jammers in the triggered spectrum collection. However, other unknown events were detected that resulted in similar GPS outage periods, as were caused by

FIGURE 8 CRC Testbed showing iGeoLoc Geolocation and jAware Detection. jAware at the processing node (which is hidden by the message box) detects the translated-jammer, and iGeoLoc geolocates it close to Node C.

FIGURE 9 CRC Testbed showing iGeoLoc Geolocation with Photo. iGeoLoc geolocates the translated-jammer close to Node D and is spotted on camera.

the identified GPS jammers. Further investigation is warranted and is being undertaken. **Figure 12** illustrates a correlation amplitude of a *jAware*$_{GPS}$-detected chirp jammer event and can be contrasted against **Figure 11** where no jammer is present.

A GPS status report across the country, similar to a weather report, could be generated by networking *jAware*$_{GPS}$ sensors along major highways to report current and forecast future GPS status. If such a system were in place, a GPS outage could be seen moving along a highway, and an outage forecast could be generated for critical infrastructure (e.g., outage approaching airports).

Conclusions

This effort has proven that it is possible to build a low-cost system to detect and locate GNSS jammers in near-real time. In just more than one year CRC has designed, built, and tested such a system using many novel and sophisticated techniques to achieve impressive results. The *iGeoLoc*$_{GPS}$ and *jAware*$_{GPS}$ systems are new tools that can protect GNSS from the perils of jammers. The GNSS community can now employ these tools, empowering its spectral awareness.

Manufacturers

The GPS timing receiver used was the Mini-T GPS Disciplined Clock Board from **Trimble**, Sunnyvale, California

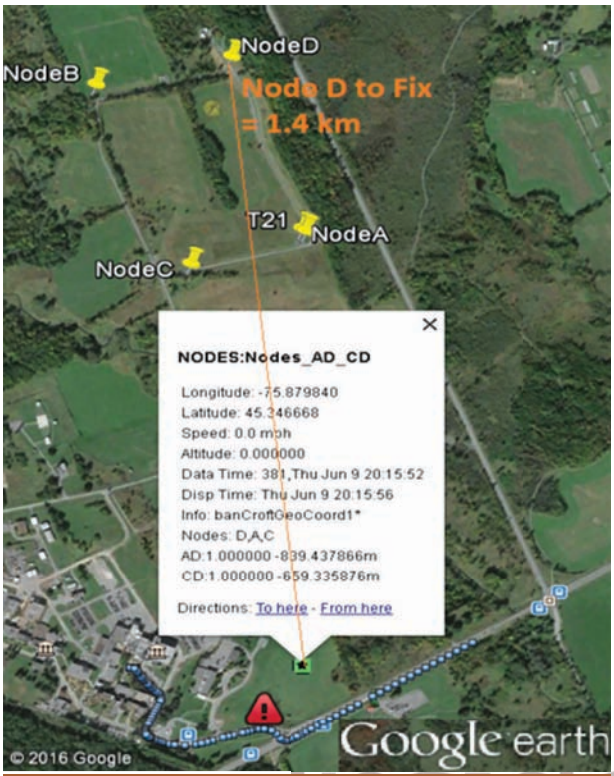

FIGURE 10 *iGeoLoc*$_{GPS}$ Range result processed in four seconds (red caution = jammer position, green star = only solution)

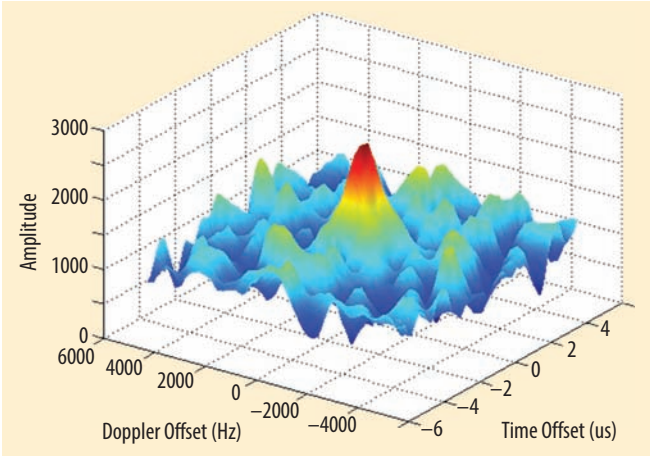

FIGURE 11 *jAware*$_{GPS}$ correlation amplitude, no jammer PRN Response, 5-ms integration time

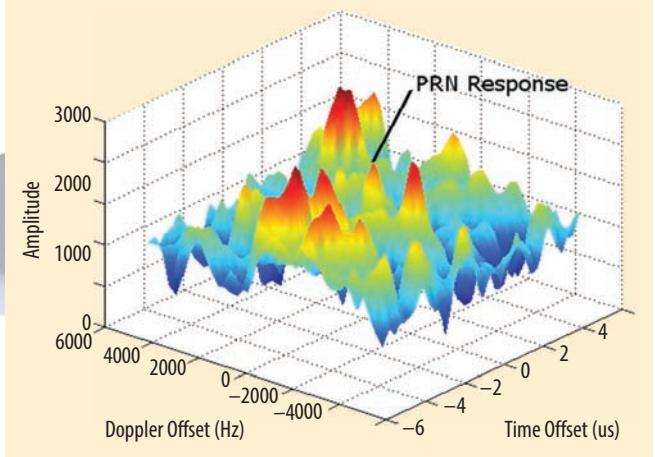

FIGURE 12 *jAware*$_{GPS}$ correlation amplitude, highway jammer effect on PRN response, 5-ms integration time

USA. The software-defined radios in the iGeoLocGPS sensing nodes and the processing node were, respectively, B200 USRP boards and X300 USRP units, from **Ettus Research** (a National Instruments (NI) company), Santa Clara, California USA. The sensing nodes were also equipped with Raspberry Pi computers to control the units, and the imaging was done using Raspberry Pi cameras from the **Raspberry Pi Foundation**, Cambridge, United Kingdom, attached to BubbleScope lenses by BubblePix Ltd., Newcastle-upon-Tyne, United Kingdom. The chip-scale atomic clock is the Quantum SA.45s from **Microsemi Corporation**, Aliso Viejo, California USA.

Acknowledgement

The author would like to thank the dedicated team members — Wayne Brett, Dr. Paul Guinand, and Russell Matt—as well as the CRC for making this project a success.

Author

Alexis Bose is a system design engineer from the University of Waterloo. Although he was accepted to the University of McGill for a Master's in Signal Processing, Alexis chose to work as a DSP/FPGA Engineer for eight years and as a research engineer at the Communications Research Centre (CRC) Canada for the last five years. Alexis enjoys solving real world problems, by developing a concept and carrying it through to implementation. He recently was the Project Manager and Technical Authority for the Geolocation of Jammers project at CRC. He received a Director General Award of Merit for this geolocation project. IG