**GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules**

Jonas Lindström, Dennis M. Akos, Oscar Isoz and Marcus Junered  
*Luleå University of Technology*

**BIOGRAPHY**

**Jonas Lindström** has finished his M.Sc. studies with the department of Computer Science and Electrical Engineering at Luleå University of Technology in 2007. Satellite navigation is a great interest and topics covered are GNSS hardware design and GNSS signal processing.

**Dennis M. Akos** completed the Ph.D. degree in Electrical Engineering at Ohio University within the Avionics Engineering Center. He has since served as a faculty member with Luleå University of Technology and currently with the Aerospace Engineering Science Department at University of Colorado at Boulder. Also he has done research at the GPS Laboratory at Stanford.

**Oscar Isoz** is an M.Sc. student at Luleå University of Technology. He is specialized in embedded systems and satellite navigation technologies.

**Marcus Junered** is a Ph.D. student with the department of Computer Science and Electrical Engineering at Luleå University of Technology in Luleå, Sweden. He received his Licentiate in Industrial Electronics in 2007. Research interests include embedded design and hardware synthesis with FPGAs for GNSS applications.

**INTRODUCTION**

The expanding fields of usage for global satellite navigation systems (GNSS) have been made possible thanks to the general technological progress.

The forthcoming advent of the European Galileo system increases the availability to the user of possible GNSS ranging sources, which even further will increase the interest in using satellite navigation applications.

Even so, fundamental problems about satellite navigation persist. One primary issue is that the signals are weak and thus subject to interference, intentional as well as unintentional, especially under delicate conditions.

GNSS serves both Safety of Life applications and the rapidly increasing market of Location Based Services. Both areas are dependant on GNSS availability. Discussed in here are available tools, possible methods and a proposed solution for mitigating the possible decrease in GNSS availability due to interference sources.

The final result, a network based sensor grid, will demonstrate how such low cost modules can be deployed over a wide geographic area and be used to quickly detect and isolate sources of interference in areas where GNSS operation would be considered critical.

Each monitoring station in the grid is built around a low-cost L1 band GNSS receiver and a hosting PC. Software used originates in open source project and has been modified to some extent for this work.

**ABSTRACT**

This paper discusses the set-up of a network of low cost ASIC front-end modules for detection of interference and localization of interference sources in GNSS L1/E1 band. Such a system has been designed to not only provide an IF-data stream but also gain control level samples. These two information channels combined provide the ability of detection and localization of both weak and strong signals. Presented herein are the theory and mathematics used along with validation from tests where the position of the interference source is known.
CONCEPTUAL APPROACH

In past efforts – see [1], [2] and [3] – the interference subject has been covered from various aspects. This paper presents a partially new approach to the GNSS interference topic. We will present the outlines and simulations of a network of independent low-cost sensors capable of detecting and localizing interference sources within the GNSS L1/E1 band.

The investigated methods include one algorithm for detection of an interference turning on and two different ways for localizing a GNSS interference source by calculating a 2D position solution. Most of the effort has been on developing the method for AGC Power Localization of an interference source.

Network Design

Key idea is to deploy a number of independent monitoring stations and one central server, as depicted in Figure 1. Detection of interference at a monitoring station is reported to a central server, then collecting data from several stations for processing interference source localization.

Interference Detection

Thanks to the L1-band is reserved for GNSS-signals only, it is considerably easy to detect any interference. Each of the satellites contribute with below-the-noise-floor levels of energy and they are transmitting continuously why any sudden increase or decrease in power level has to have its origin in something that should not be there, by definition an interference source.

There are slow changes in the AGC level coming from changes in antenna temperature and changes in number of visible satellites. These differences should not trigger a system designed for detecting interference sources going on/off and so the detection system has to be designed such it filters those changes out.

The sampled AGC-level is relatively noisy, why the power increase of 0.5 dB in Figure 2 may not be easily distinguished. By applying a median filter with a following weighted summation, as shown in Figure 3, even this small change generates a clearly detectable metric.

AGC monitoring concept

AGC level as an interference assessment tool has been investigated before. In [1] an extensive research and investigation around frequency band L5 is presented. When GNSS signals themselves reside below thermal noise floor and the L1 frequency band has no other legitimate signals the spectra should appear silent and consistent.
**AGC Power Localization**

By monitoring the impact on automatic gain control voltage for a set of minimum three monitoring stations it is possible to solve for the 2D-position of the interference source. This method may be described by the analogy of adjusting the sizes of three circles to attain a common point of intersection as depicted in Figure 4.

### Description of Method

The read out voltages as a function of emitted power and distance is described by the equation system in Figure 5.

- \( V_{\text{AGC},N} \) – AGC voltage difference from each monitoring station.
- \( X, Y, P \) – Unknowns: Geographic position and interference source emitted power.
- \( V_{0,N} \) – Individual calibration constants
- \( P_{0,N} \) – Background power level at antenna

An algebraic solution to the problem is way beyond the ambitions of this paper, thanks to the triple non-linearity in equations. A much simpler grid search has been implemented for verification presented later.

### Considerations of Method

The non-linearities involved call for some careful consideration of the dynamics involved. The combination power/distance impact on AGC voltage is shown simulated in Figure 6. It shows there are a couple of things to consider.

1. The AGC may saturate.
2. AGC voltage relation to distance may be insufficient for low power emitted.
3. AGC voltage relation to power may be insufficient for long distances.
4. A preferred region should be defined where these issues are avoided.

The result from using measurements having bad properties is that position solution may become very noisy or ultimately there is no position solution at all, as illustrated in Figure 7.

### Equation

\[
V_{\text{AGC},N} = k_N \cdot \log_{10} \left( \frac{P_{0,N} + P}{(X - X_N)^2 + (Y - Y_N)^2} \right) - V_{0,N} ; N \geq 3
\]

**Figure 4 – Analogy to method of adjusting circles**

**Figure 5 – Mathematic relationship describing the nature of the AGC voltage metrics**

**Figure 6 – AGC voltage as a function of interference source power and distance**

**Figure 7 – No solution due to bad geometric properties**
Hyperbolic Localization

Hyperbolic navigation systems have been in use since World War II. Still operational is the LORAN system, updated to eLORAN. The basic principle is determining the user’s position by calculating two intersecting hyperbolas defined each by a TDOA-estimate for a defined transmitter pair. This is illustrated in Figure 8.

Figure 8 – Intersecting hyperbolas define a position

Description of Method

Our implementation of hyperbolic localization utilizes the same math as any hyperbolic navigation system. The only difference is that there is only one transmitter and multiple receivers instead. This is introduced in [4].

TDOA-estimates are done by cross-correlating data sets from pairs of monitoring stations, see Figure 9. Time scales for the data sets are aligned by processing them for a GNSS navigation solution since this also produces accurate timing information down to sample level. In [2] the same process is used, however, synchronized at sampling level.

Data Processing

Presumably this method is suitable for very weak signals. For such a case, the GNSS signals in the band may distort the correlation of the interference signal searched for.

Two different methods, described only briefly here, for counteracting their influence have been investigated. For wider spread sensor grids this becomes less of a problem.

First method is for counteracting the effect of C/A-codes generating correlation energy added to the interference source. That is done by applying a 2 MHz band-stop filter taking out the main lobe of the C/A-code, and such most of its energy. The effect is demonstrated as the difference between Figure 10 and Figure 11.

Figure 10 – Original spectrum and correlation vector

Second method for enhancing correlation has to do with remainders of the P(Y)-codes, also correlating between data sets. This is dealt with by subtracting the amount of correlation energy experienced just before detection of interference. The correlation peak has a fingery look due to band limitations from the previous band stop filter.

Figure 11 – Filtered spectrum and correlation vector

Figure 12 – Resulting vector (blue) is difference between measured (green) and reference (red)
HARDWARE AND SOFTWARE

**RnD 4120 Front-End**

The RnD 4120 board, shown in Figure 13, is the result from an effort to develop a low-cost GNSS front-end with AGC monitoring capability. It is built around the SiGe SE4120L front-end.

A Cypress USB-interface provides board control and data transfers. The board provides IF-data samples in various real and I/Q modes in up to 16.368 MHz. The sampling rate of the AGC level is defined by the software.

![RnD 4120 front-end board with AGC monitoring capability – shield cans opened](image)

**GN3S Software**

This software is the outcome of series of student projects and is licensed under GNU general public license. The bundle consists of two basic parts, a host software being the user interface as well as storing data to disk and a firmware operating the front-end board from the Intel 8051 implementation in the USB circuit. The code base originates from the GNUradio project [5].

**GNSS Software Defined Radio**

This Matlab based software defined radio implementation post-processes saved GNSS IF-data and provides a full position solution if the prerequisites are fulfilled. It has been developed at Aalborg University and University of Colorado under GNU GPL. Small modifications have been made to extract additional information necessary for timing required by the Hyperbolic Localization.

![Figure 14 – Data collection field map and relative coordinates in meters](image)

FOI JAMMING EXPERIMENT

This paper presents results based on data from an intentional GNSS jamming campaign carried out in cooperation with Totalförsvarets forskningsinstitut, FOI [6], a Swedish Military research organization. The campaign was carried out during the summer 2007 commissioned by Swedish military forces.

Luleå University of Technology was invited by FOI to participate in the campaign. The invitation was accepted for the purpose of collecting data to be used in the verifications presented in this paper.

DATA COLLECTION

Data was collected using five monitoring stations comprising each a laptop PC, an RnD 4120 front-end module and a generic GPS antenna.

**Data Collection Field Overview**

Static positions of the monitoring stations (M) and alternating positions of the jammer (J) are shown in Figure 14 and their coordinates are listed in Table 1.
### Table 1 – Field coordinates

<table>
<thead>
<tr>
<th>Position</th>
<th>East</th>
<th>North</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>103</td>
<td>284</td>
</tr>
<tr>
<td>M2</td>
<td>78</td>
<td>485</td>
</tr>
<tr>
<td>M3</td>
<td>46</td>
<td>141</td>
</tr>
<tr>
<td>M4</td>
<td>237</td>
<td>455</td>
</tr>
<tr>
<td>M5</td>
<td>194</td>
<td>274</td>
</tr>
<tr>
<td>J1</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>J2</td>
<td>63</td>
<td>209</td>
</tr>
<tr>
<td>J3</td>
<td>146</td>
<td>367</td>
</tr>
</tbody>
</table>

Relative coordinates in meters

### Data Collection Cases

For each position of the jammer, data sets are collected synchronously by all stations. Each data set is four minutes long with the jammer turned on after one minute and remaining on for two minutes.

Such, the start and end of each data set are jammer free and used for reference. As a backup, the process is repeated twice for each jammer position.

Three subsets of the data collected have been selected for verification of the two localization methods. These sets are presented in Table 2.

### Table 2 – Data sets used for verification

<table>
<thead>
<tr>
<th>Label</th>
<th>Method</th>
<th>Monitoring stations</th>
<th>Jammer position</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>AGC Power</td>
<td>M1, M2, M4 and M5</td>
<td>J3</td>
</tr>
<tr>
<td>P2</td>
<td>AGC Power</td>
<td>M2, M3 and M5</td>
<td>J2</td>
</tr>
<tr>
<td>H1</td>
<td>Hyperbolic</td>
<td>M4 and M5</td>
<td>J1</td>
</tr>
</tbody>
</table>

### VERIFICATION OF ALGORITHMS

From the data collected different subsets are chosen for verification of the localization algorithms. No further verification of the interference detection is done than what is presented in the theoretical description.

For AGC Power Localization two various sets have been selected from available combinations and for Hyperbolic Localization one set with the option of different combinations has been picked out.

### AGC Power Localization

The two sets used for verification of AGC Power Localization are selected to differ in geometric properties. The first set comprises four monitoring stations with the jammer well within the polygonial boundary defined by the positions of the monitoring stations.

The second selection is a set of three monitoring stations with a less advantageous geometry where the jammer is considerably closer to one of the stations.

### Method

A grid search for the position, represented by \( X \) and \( Y \) coordinates, and power \( P \) emitted from the jammer. Full calibration data has not been available, why simplifications have been made, based partially on assumptions.

It is assumed that the power from background radiation affects each antenna equally. Also the linearity constants of the front-end boards AGC circuitry are considered being equal. Furthermore, calculating the true power output from the jammer is not of interest, only the position. Thus, the jammer power is handled in the simulation in relation to the unknown, but everywhere equal, background.

Validation metrics are generated from available data sets by comparing mean values from no jammer and jammer present groups within each AGC data set. The difference between those mean values will serve as each station’s metric. This is demonstrated in Figure 15.
Position Solutions from AGC Power Localization

By looking for the lowest point in the error plot over the geographic area a position in X and Y representing least possible error for available data is found. This is also the position estimate for the measurement. This is illustrated for the two data sets investigated in Figure 16 and Figure 17, respectively. Vertical lines in surf plots represent monitoring stations (M), localization solutions (S) and known positions (J).

Hyperbolic Localization

This method is designed for weaker interference signals than those experienced in available data sets. The number of suitable data sets available for verification is therefore limited. It is however possible to use different subsets, separated by seconds in time, of the same data to get a statistic overview.

The method has therefore been examined for one pair of monitoring stations only on a TDOA level approach as depicted in Figure 18, which also shows an example for how the correlation peak may look. In Table 3 is found the statistics for the calculations.

<table>
<thead>
<tr>
<th>Monitoring stations</th>
<th>M4 and M5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jammer position</td>
<td>J1</td>
</tr>
<tr>
<td>Expected TDOA in meters</td>
<td>177</td>
</tr>
<tr>
<td>Number of trials</td>
<td>5</td>
</tr>
<tr>
<td>Measured TDOA in meters std.dev. in parentheses</td>
<td>198 (40)</td>
</tr>
</tbody>
</table>

Table 3 – Statistics for case of verifying TDOA correlation
SUMMARY AND CONCLUSIONS

A low-cost and easy-to-use GNSS front-end module has been developed. The module uses existing open source software with minor modifications. Algorithms for detection and localization have been developed and implemented in Matlab. Focus has been on verifying the AGC Power Based method for localization.

During jamming campaign carried out by FOI data has been collected later used to verify algorithms and methods developed. Despite limited time for planning and no prior knowledge of the test site properties data sets collected have been very useful for verification.

Both localization methods are verified to produce results within a few tens of meters, which is considered being a promising result, given the prerequisites.

Future Efforts

Automatic centralized data collection and processing are still to be implemented. This comprises development of detection and method selection logic and also calls for a back-tracking buffer of data at the monitoring stations.

One part not being investigated at all for this paper is the antennas used. It is certain that the generic GPS antenna has a beam form that is not optimal for this kind of investigation. For further work in this area it has been proposed to investigate other kinds of antennas that have other beam patterns forms. A candidate for such is the half wavelength dipole.

ACKNOWLEDGEMENTS

Thanks to Fredrik Eklöf and his staff at FOI for enabling the field-testing presented in this paper. Also the following people have been of great help and support during this work: Staffan Backén, Sirish Jetti, Tore Lindgren, Christopher Treib and Eric Vinande. Many thanks to all of you!

REFERENCES

[3] Homepage: http://www.engineering.leeds.ac.uk/i3s/research/Sat_Nav_wire/qgn_project.shtml