

# Team member

Ben Wilson

Chi Wong

Devin Lorenzen

Edward Sayers

Hanjae Noh

Capstone 2015

The following document details the purpose of GPS Jamming signal detector and the relevant information is provided to give background knowledge into present prior research efforts in the field. A project plan(schedule) is specified, detailing a series of tasks that will be performed by capstone team.

Table of Contents

[Team member 1](#_Toc412663263)

[Purpose - GPS Jamming detection 2](#_Toc412663264)

[Background – Jamming 3](#_Toc412663265)

[Marketing Requirements 4](#_Toc412663266)

[Must: 4](#_Toc412663267)

[Should: 5](#_Toc412663268)

[May: 5](#_Toc412663269)

[Design specification 5](#_Toc412663270)

[Constraints 6](#_Toc412663271)

[Proposed solution 7](#_Toc412663272)

[Criteria success 7](#_Toc412663273)

[Deliverables 7](#_Toc412663274)

[Project Timetable 7](#_Toc412663275)

[Work Cited 8](#_Toc412663276)

[Revision Table 9](#_Toc412663277)

# Purpose - GPS Jamming detection

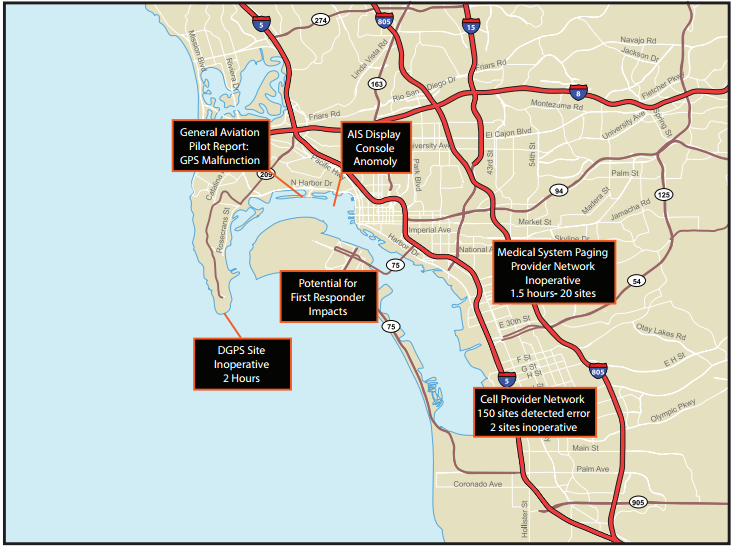
Many trucking companies make use of GPS tracking devices in order to reduce fuel cost, improve driver behavior and increase security and safety. However, there are unscrupulous individuals who want to jam their GPS signal. There are simple ways to jam the GPS signal that is being received by the tracking device located on the truck such as GPS jamming gadgets, metal shields, GPS spoofing gadgets and mobile phone jammer. Whether intentional or inadvertent, jamming GPS signals poses a significant risk to our daily lives. There are couple of examples that highlighted by GPS Jamming(San Diego Harbor in January 2007, Newark Airport in August 2013, and The Stock Market in February 2012 in the U.K.). [1]

figure 1. San Diego Harbor in January 2007 [2]

GPS jammers are illegal to buy, use, or sell due to the potential for criminal or terroristic uses. To help resolve the illegal use of GPS Jammers we would like to design jammer detection when these jamming signals are being utilized.

# Background – Jamming

Global Positioning System (GPS) is a satellites based navigation system. The properties of GPS receiver are

* Center Frequency L1 (1525.42MHz)
* Protected Bandwidth 20.46 MHz
* Precision code (P) Code ≈ -133 dBm
* Course Acquisition (C/A) Code ≈ -130 dBm

Most jamming techniques are divided into three major types (CW, Chirp, and Pulse). The jammer works by adding noise in the L1 band(1575.42MHz ± 10.23MHz) with a power greater than -65dBm [3].

# Marketing Requirements

## Must:

1. Receive I/Q data
2. Determine if a civilian GPS jamming signal is present
3. Notify the user that a jammer has been detected
4. Be fast enough to notify a user that a jammer is present when the jammer is in a moving vehicle

## Should:

1. Be able to detect multiple types of jamming techniques
2. Give indication of jamming method
3. Be implemented on a FPGA
4. Determine the center frequency of the jammer
5. Be portable

## May:

1. Determine the direction of jamming signal
2. Determine the presence of a GPS spoofer
3. Determine the average signal power of jammer

# Design specification

|  |  |  |
| --- | --- | --- |
| Marketing requirements | Engineering Requirements | Justification |
| 1 | 1. The device must accept in-phase and quadrature (I/Q) data through an external interface. | The jamming signals that will be collected and used to test the device will be in a I/Q data format. |
| 2 | 1. The device must be able to detect the presence of a jamming signal in the L1 band. | The primary use of the device is the detection of a jamming signal in the civilian GPS band. |
| 4 | 1. The device needs to notify the user within 1 seconds. | Most receivers can detect a jammer from a range of 20 meters. A car traveling on a three lane highway will pass through the effective in about 1 seconds. |
| 3,5,6 | 1. Must be able to differentiate between continuous, pulse, and chirp jamming. | There are multiple type of jammers. The operator needs to clearly see what type of jamming signal is being used. |
| 7 | 1. The device should be developed on an FPGA. | FPGAs are provided by the project sponsor. |
| 8 | 1. The device should be able to detect the center frequency of the jamming signal. | Many jammers are not very precise and may affect services other than GNSS. Also, detecting the center frequency can aid in determining the variance of cheaply produced jammers. |
| 9 | 1. The device should be less than 8 x 8 x 4 inches. | The detector is likely to be used in a motor vehicle. |

# Constraints

* Processing speed of the zedboard
* Device size: Less than 8 x 8 x 4 inches
* 12 V DC power supply
* Data log size: maximum 1TB
* Budget : maximum 2500$

# Proposed solution

A FPGA should be used in order to quickly perform an FFT on received I/Q data. An impeded processor on the FPGA can run an algorithm to determine if a jammer is present based of the FFT response. The result should be than logged onto an external memory device.

# Criteria success

* A device needs to be able to receive I/Q data
* A technique to determine if jamming signal is present and jamming methods

# Deliverables

The deliverables include a device that can identify at least one jamming method (CW, Pulse, or chirp) from recorded I/Q data on an external memory device.

# Project Timetable

|  |  |
| --- | --- |
| August - September | Industry sponsors submit descriptions of proposed projects |
| September - October | Project descriptions posted on Capstone web site |
| October | Students indicate preferences for projects |
| November | Team and project assignments made.  Faculty advisors assigned. |
| December | Teams meet with industry sponsors, begin research |
| December - January | Teams write project proposals (including PDS and schedules) |
| January - February | Teams present project proposals to industry sponsors |
| February | Teams complete team evaluation and self assessment forms and submit to faculty advisor |
| February - June | Students complete projects |
| June | Final project presentations to industry sponsor and faculty advisor |
| June | Students submit: engineering logbook, project notebook, final project report, second team evaluation and self assessment |
|  |  |

# Work Cited

[1] Jeff Coffed. (2014, Feb). "The threat of GPS Jamming. EXELIS. [Online]. pp. 6. Available: <http://www.exelisinc.com/solutions/signalsentry/Documents/ThreatOfGPSJamming_February2014.pdf>

[2] Logan scott, introduction to GPS interference and Mitigations, January 2015

[3] Gregory D. Rash. (1997). GPS Jamming in A Laboratory Environment. [Online]. pp. 1-4. Available:

http://www.globalsecurity.org/space/library/report/1997/labjam.pdf

# Revision Table

|  |  |  |
| --- | --- | --- |
| Version | Changes Made | Editor |
| 1 | Created First Draft | Hanjae |
| 2 | Added Revision Table Added Member Names  Edited Formatting  Added Table of Contents  Added Citation page | Devin |
| 3 | Constraints | Hanjae |
| 4 | Proposed solution  Criteria success  Deliverables | Devin, hanjae |
|  |  |  |
|  |  |  |