[[1]](#footnote-1)

Detection of GPS Jamming Signals in the L1 Band

Devin Lorenzen, Hanjae Noh, Edward Sayers, Ben Wilson and Chi King Wong

*Abstract*— GPS jamming has become an increasing problem in today’s society. While some may think that they are protecting their right to privacy they are actually breaking the law by illegally transmitting signals in the L1 band that affect other nearby systems. This project is designed to help reduce the use of illegal GPS jammers by identifying jammer signals and characterizing them on a FPGA from captured IQ data.  MATLAB was used to simulate and verify the correct operation of the algorithm.

# INTRODUCTION

T

HE majority of GPS jammer users consists of commercial drivers. For instance, Taxi drivers will use a GPS jammer in order to steal clients from other drivers working for the same company [1]. Similarly truck drivers can jam their GPS in order to drive longer than the maximum amount of time aloud. This is because many truck drivers are paid by the mile [2]. Criminals also Use GPS jammers in order to hide the movement of a stolen car as they drive it to a chop shop [3].

While the concept of detection has been around since the electromagnetic spectrum was discovered, law enforcement still rely on third party reports of possible jamming [4]. Because of this, it is hard to track down GPS Jammers [5]. While Chris Vallance for BBC News Reports “In one location the Sentinel study recorded more than 60 GPS jamming incidents in six months” [6].

The intention of this project is to help study the use of GPS jammers by exploring methods of detection and characterization for the different method of jamming. This project was designed to be a software module of a standalone jammer detector that could be placed in high traffic areas to determine jammer use patterns and help pinpoint potential offenders.

# Theory

GPS operates with a center frequency of 1575.42 MHZ and has a protected bandwidth of 20.46 MHz and a received power of about -130dBm [7].this suggests that the L1 band should be completely quiet and any signal picked up could be treated as a potential jammer. The majority of jammers on the market utilize the chirp method of jamming. This jamming method works by sweeping across a frequency range as a function of time.

# IMPLEMENTATION

## Algorithm

There are several meaningful ways to detect the presence of an interfering signal. The simplest way is to measure the energy of the frequency spectrum and determine if a signal is present [8, 9].  Another method is to look for cyclostationary features in a signal. A third method is to use a waveform based detection algorithm that assumes basic properties of the jamming signal [9].  Due to the fact that the jammer captures used in this project were all some form of chirp, it was decided that a waveform based detection would be the best approach.

The essential idea of detecting a GPS jammer is to determine if a signal in the L1 band is a GPS signal or not.  Fortunately, the GPS signals are so weak at the receiver that they are under the noise floor and cannot be seen with a spectrum analyzer. This means that any signal that is visible above the noise floor should not be present and would be considered a jammer.  With this information in mind the first step in the detection algorithm is to perform a fast Fourier transform (FFT) of the incoming signal and verify that no frequency component is noticeably above the noise floor.  If a frequency component is above the some threshold, the detector is triggered (see figure 1) and begins the characterization step.

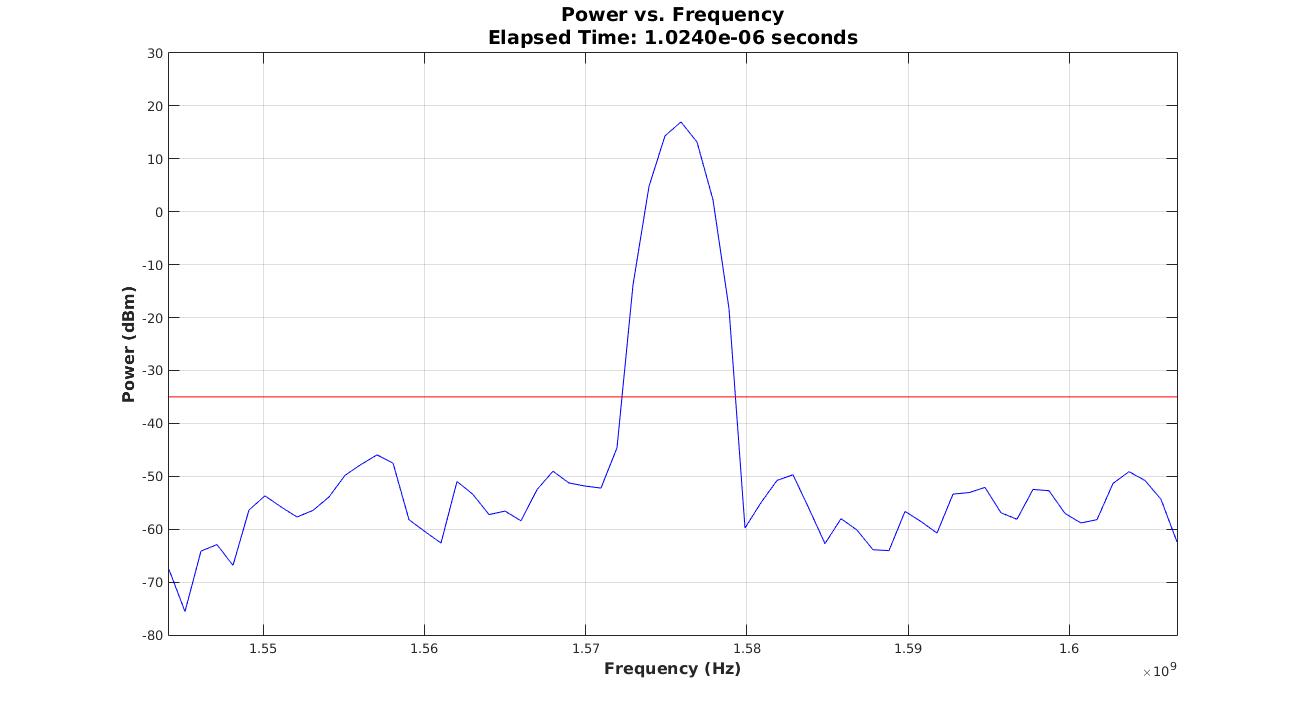


Figure 1- 64 point FFT of a jammer capture

Once the detector has been triggered, the algorithm will assume the interfering signal is a chirp and will try to determine the bandwidth and chirp rate of the jammer.  To do this the algorithm takes many small FFTs of the incoming signal and records the frequency corresponding to the maximum power level.  If the interfering signal is actually a chirp, it would be expected that the recorded values would start at some minimum frequency and increase monotonically to some maximum frequency before jumping back to the original minimum frequency (see figure 2).  As this trend is recorded over several chirps a periodic pattern will emerge.  The chirp rate can be calculated by performing an FFT on these records and returning the maximum value (see figure 3).  The bandwidth of the interfering signal can be computed by calculating the difference between the maximum and minimum frequencies.

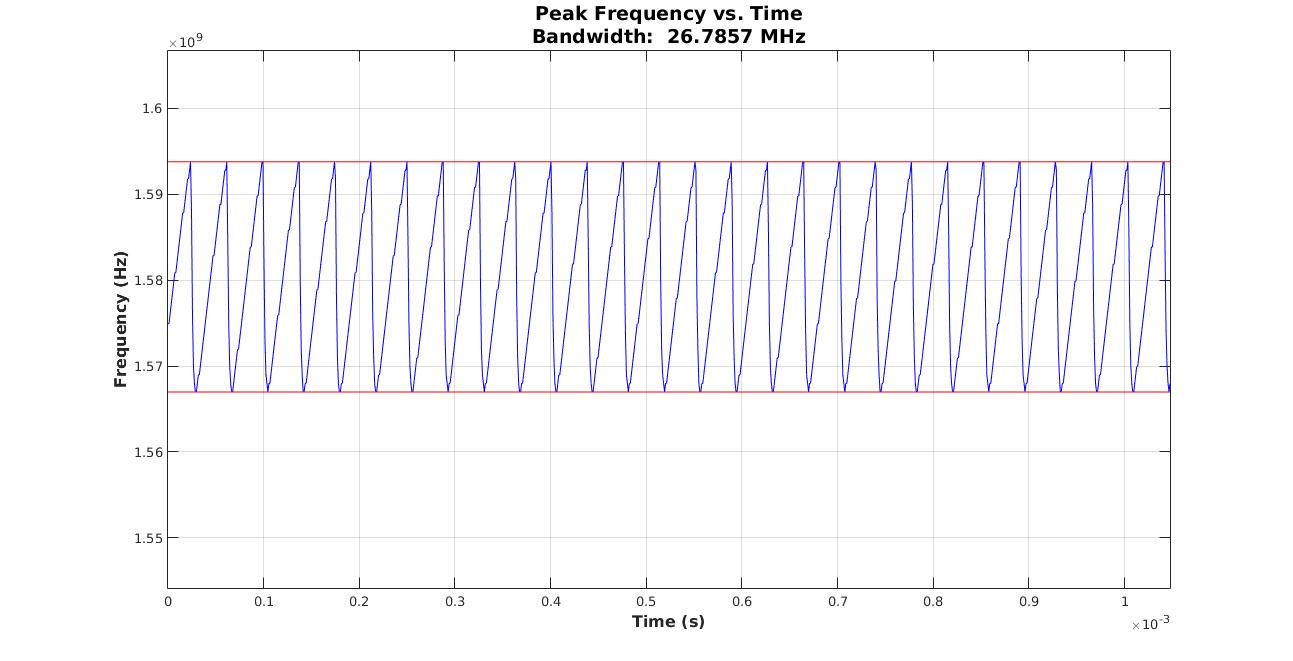


Figure 2 - Tracking the peak frequency of a chirp over time results in a sawtooth waveform

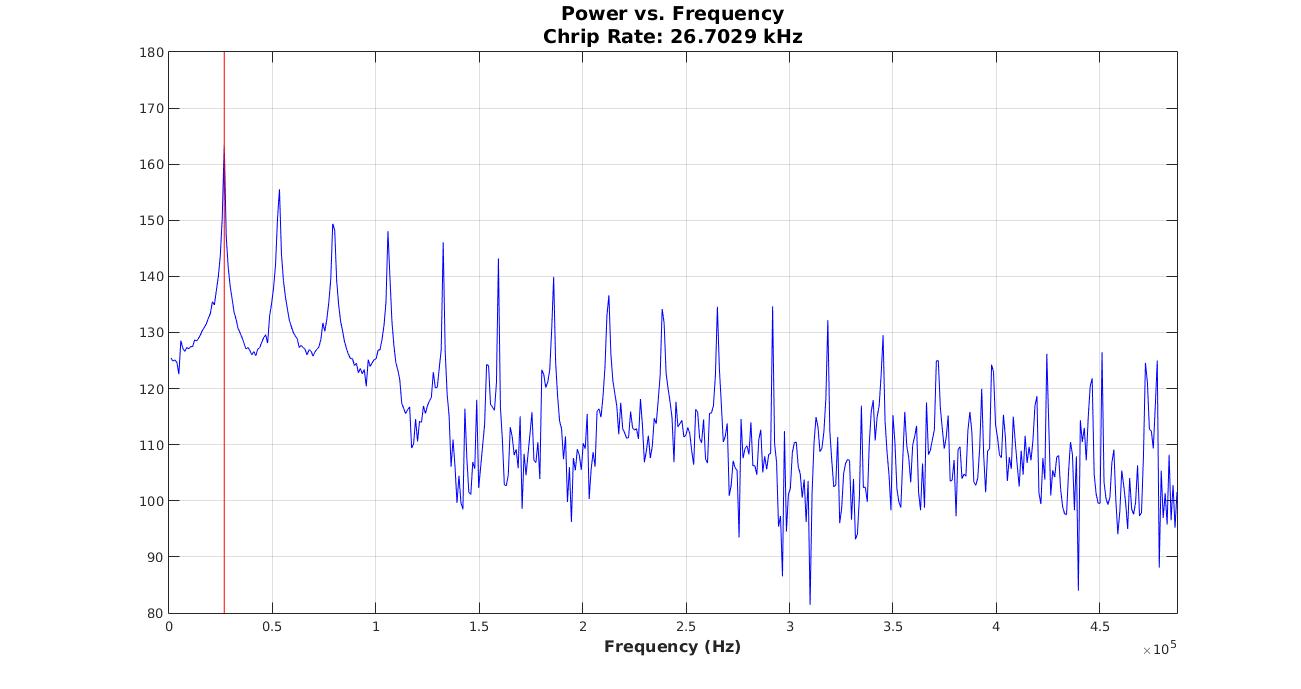


Figure 3 - The Fourier Transform of figure 2 returns the chirp rate of the jammer

## Hardware

The final hardware design is implemented on a ZedBoard. Collected IQ data can be streamed to the board from an external client program over a TCP connection. The data is then processed using the previously described algorithm. When a jamming signal is detected, an LED is activated to notify the user and the characterizing information is relayed via the COM port.

  Design was done in two stages. First, the FPGA hardware layout was designed using Vivado. Then, software was written to implement the design.

 The FPGA design centers on the Zynq 7000 processing system. Connected to the processing system are two GPIO controllers and a DMA controller via the AXI bus. The first GPIO controller is connected to eight LEDs on ZedBoard to allow rudimentary communication with the user. The second GPIO controller is connected to eight switches on the ZedBoard. These switches would allow a form of user input, but were not used in the final design. The DMA controller is connected to an IP block that implements an FFT algorithm. The FFT block was to be used to offload some of the work from the main processor, but there was no time to implement the software side of the setup.

  The processing system uses the FreeRTOS operating system along with the lwip TCP/IP stack to act as a server accepting TCP connections over Ethernet. A client program connected to the device takes data in the iq.tar format and transmits it to the server. That data is then run through the detection algorithm. If a jamming signal is determined to be present, the user is notified.

# Conclusion

In this paper we have described a GPS jammer detection based on our algorithms. Our algorithms seek simple power detection above a threshold value. We collected frequency spectrum by taking FFT from I/Q data and evaluated the algorithms in terms of threshold value. When the measurements (spectrum of I/Q data) at Receiver are collected, all performed algorithms on Matlab have good performance and are able to detect jamming signal.

## Retrospective

In hindsight there are better ways to determine the presence of a jamming signal. One of the limitations of the proposed algorithm is that it can only detect signals that are above the noise floor. Other methods, such as cross correlation can work even when the signal has a negative SNR. An alternate solution would be to cross correlate and normalize the current set of capture data with the previous set. If a periodic signal is present there will be peaks corresponding to the lags where the two signals are in phase. By measuring the distance between peaks it would be possible to determine the chirp rate. This method would not be able to determine the bandwidth of the jamming signal, but that information is not as meaningful.

## Contributions

Devin Lorenzen – Project lead/administration

Ben Wilson – Algorithm design, MATLAB simulations

Edward Sayers – FPGA implementation

Chi King Wong – Testing

Hanjae Noh – Techbench development

## Lessons learned

**What went well with the project?**

As a whole, the team worked well with each other and maintained a professional level of respect throughout the project. Everyone handled criticism well and there was never any need for mediation among the team. Along with that, the team met regularly with each other to discuss current status and also met weekly with the industry sponsor.

**What was the most frustrating part of the project?**

There were times where one or more team members were uncertain of what they should have been doing and more direction, from other team members as well as faculty advisor, would have been appreciate.

Over the course of the project, the scope was changed a few time in order to narrow the focus of the project. While these adjustments were clearly necessary in hindsight, it did cause some frustration.

Another cause of frustration was due to the fact that much of our early research didn’t directly relate to the goal of the project and there was substantial time wasted while researching topics that would not contribute to the successful completion of the project.

**How can this be prevented in the future?**

We should have been more organized in the beginning and been more upfront when we needed help. Many people were researching things that were interesting to that individual, but not helpful for the project. Instead, we should have been working towards an achievable short term goal and building on that towards completion of the final product.

**Where the goals of the project clear?**

The project was clear, but left open ended to account for more creative solutions. As the term progressed and time became more of a luxury the goals came into sharp focus and everyone knew what was needed to succeed.

**Was the project well outlined, how can it be improved?**

The project was well outlined from the beginning, but we didn’t give it as much consideration as we became busier. In hindsight, we should have been referring to the schedule more frequently.

**Was the schedule realistic?**

The scope was realistic, but due to inexperience with DSP and FPGAs we had difficulty meeting goals.

**Was the workload reasonable?**

The workload could have been more evenly distributed. There were times when one or two team members had a heavy workload while others were looking for tasks to perform.

**Was the test plan sufficient?**

It is unclear if the test plan was sufficient due to the fact that device testing wasn’t thoroughly implemented. Testing could have been more thorough during MATLAB simulations and we could have tested more on the FPGA.

It would have been nice to have more test benches ready so that optimization could have been done in MATLAB.

**What changes could have been made to make the team more effective?**

The workload could have been broken up more efficiently and break the team into two smaller teams so that we could team up to work on major sections together.

References

1. H. A. Collier Karen, "Taxi Cheats Using GPS Jammers To Steal Fares," Heraldsun, 08 November 2013. [Online]. Available: http://www.heraldsun.com.au/news/law-order/taxi-cheats-using-gps-jammers-to-steal-fares/story-fni0fee2-1226756138559. [Accessed 11 June 2015].
2. Truckers Report, "The Truckers Report," 23 February 2004. [Online]. Available: http://www.thetruckersreport.com/truck-driver-facts/. [Accessed 11 June 2015].
3. C. Arthur, "Thousands Using GPS Jammers On UK Roads Pose Risks, Say Experts," The Guardian, 13 February 2013. [Online]. Available: http://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks. [Accessed 11 June 2015].
4. L. Northrup, "FCC Catches Vigilante Highway Cell Phone Jammer, Wants To Fine Him $48K," Consumerist, 02 May 2014. [Online]. Available: http://consumerist.com/2014/05/02/fcc-catches-vigilante-highway-cell-phone-jammer-wants-to-fine-him-48k/. [Accessed 11 June 2015].
5. L. Scott, Introducing GPS Interference and Mitigation (Presentation)*,* Portland, 2015.
6. V. Chris, "Sentinel Project Research Reveals OK GPS Jammer Use," 08 March 2012. [Online]. Available: http://www.bbc.com/news/technology-17119768. [Accessed 11 June 2015].
7. T. Y. Bao James, "GPS C/A Code Signal Structure," in *Fundamentals of Global Positioning System Receivers: A Software Approach*, John Wiley & Sons, Inc., 2000, pp. 74,75.
8. Urkowitz, Harry, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE* , vol.55, no.4, pp.523,531, April 1967
9. Yucek, T.; Arslan, H., "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys & Tutorials, IEEE* , vol.11, no.1, pp.116,130, First Quarter 2009

1. [↑](#footnote-ref-1)