Signal Characteristics of Civil GPS Jammers

Ryan H. Mitch, Ryan C. Dougherty, Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon,
Cornell University, Ithaca, NY

Jahshan A. Bhatti and Todd E. Humphreys,
University of Texas, Austin, TX

BIOGRAPHIES

Ryan H. Mitch is a graduate student in the Sibley School of Mechanical and Aerospace Engineering at Cornell University. He received his B.S. in Mechanical Engineering from the University of Pittsburgh. His current research interests are in the areas of GNSS technologies, estimation and filtering.

Ryan C. Dougherty is a graduate student in the Sibley School of Mechanical and Aerospace Engineering at Cornell University. After earning his B.S. in Aerospace Engineering from the University of Southern California, he worked in propulsion systems engineering first at the Jet Propulsion Laboratory, then at Space Systems/Loral. His research interests are in estimation and filtering.

Mark L. Psiaki is a Professor in the Sibley School of Mechanical and Aerospace Engineering. He received a B.A. in Physics and M.A. and Ph.D. degrees in Mechanical and Aerospace Engineering from Princeton University. His research interests are in the areas of GNSS technology and applications, spacecraft attitude and orbit determination, and general estimation, filtering, and detection.

Steven P. Powell is a Senior Engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in Electrical Engineering from Cornell University. He has been involved with the design, fabrication, testing, and launch activities of many scientific experiments that have flown on high altitude balloons, sounding rockets, and small satellites. He has designed ground-based and space-based custom GPS receiving systems primarily for scientific applications.

Brady W. O'Hanlon is a graduate student in the School of Electrical and Computer Engineering at Cornell University. He received a B.S. in Electrical and Computer Engineering from Cornell University. His interests are in the areas of GNSS technology and applications, GNSS security, and GNSS as a tool for space weather research.

Jahshan A. Bhatti is pursuing a Ph.D. in the Department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin, where he also received his M.S. and B.S. He is a member of the UT Radionavigation Laboratory. His research interests are in the development of small satellites, software-defined radio applications, space weather, and GNSS security and integrity

Todd E. Humphreys is an assistant professor in the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin and Director of the UT Radionavigation Laboratory. He received a B.S. and M.S. in Electrical and Computer Engineering from Utah State University and a Ph.D. in Aerospace Engineering from Cornell University. His research interests are in estimation and filtering, GNSS technology, GNSS-based study of the ionosphere and neutral atmosphere, and GNSS security and integrity.

ABSTRACT

This paper surveys the signal properties of 18 commercially available GPS jammers based on experimental data. The paper is divided into two distinct tests. The first characterizes the jamming signals, and the second test determines the effective range of 4 of the jammers. The first test uses power spectra from discrete Fourier transforms (DFTs) of the time series data to show that all the jammers employ approximately

Preprint from ION GNSS 2011

the same jamming method, *i.e.* linear frequency modulation of a single tone. The spectra also show that there are significant jammer-to-jammer variations, including between jammers of the same model, and that a given jammer's signal may vary over time. The first test also includes measurements of signal power within frequency bands centered at the L1 and L2 frequencies, along with the sweep periods and the sweep range at both frequencies. The second test presents measurements of the attenuation of the jamming signal necessary to allow a commercially available GPS receiver to acquire and track signals from a GPS simulator. From the attenuation levels and some assumptions about the antennas used, upper limits on the effective jamming ranges are calculated for 4 of the jammers, with a resulting maximum range of 6–9 km.

1 INTRODUCTION

The Global Positioning System (GPS) has become increasingly incorporated into civilian life, especially since selective availability was turned off on 2 May 2000 [1]. GPS is now used in aircraft navigation [2], trucking and shipping, personal navigation and tracking devices [3], and other applications. The increase in GPS-integrated systems has caused a proportional increase in the vulnerability of these systems to jamming and interference. The interests of individuals or groups willing to break the law may be served by interfering with the normal operation of GPS-enabled systems. As a result, in recent years many GPS jamming devices have become available for purchase over the internet. These widely available and relatively cheap devices, some costing significantly less than a GPS receiver, pose a significant risk to the normal operation of many systems reliant on GPS.

There are many types of radio frequency (RF) interference, including tones, swept waveforms, pulse, narrowband noise, broadband noise and other multi-frequency and time-varying versions of most of the same methods [4]. There are a number of methods for mitigating the effects of jamming and interference in general [4], and specifically for GPS [5] and swept tones or chirp signals [6]. The methods listed in references [7] and [8] can be used in situations where the location of the interference source is to be determined. These mitigation and location methods can be improved by use of *a priori* information about the interference source. This paper attempts to provide that *a priori* information in addition to evaluating the effective range of some of the GPS jammers.

The rest of the paper is organized as follows. Section 2 provides a brief description of the availability and purveyor claims of the jamming devices and attempts to categorize them. The same section also mentions the affected frequencies and the antennas used by the jammers. The remainder of the paper is broadly separated into two tests, the first being an attempt to characterize the jammer signals and the second to determine some of the jammers' effective ranges. Section 3 provides an overview of the equipment and Section 4 gives the detailed procedure for the first test. Section 5 presents the jammer signal characteristics resulting from the first test. Section 6 provides an overview of the equipment used during the second test, and Section 7 outlines the testing procedure. Section 8 presents the results of the second test. The paper's summary and conclusions are presented in Section 9.

This paper examines 18 currently available civil GPS jammers, but there are other types of GPS jammers for sale that were not tested and civil jammer behavior and design will evolve over time. This paper draws conclusions based only on the jammers that were tested.

2 OVERVIEW OF CIVIL GPS JAMMERS

2.1 Availability and Claims

Devices which claim to jam or "block" GPS signals are widely available through a number of websites and online entities. The cost of these devices ranges from a few tens of dollars to several hundred. Their price does not seem to correlate with the claims made by the purveyors of these devices regarding the features and effectiveness of the product in question. Effective ranges from a few meters to several tens of meters are advertised, but it will be shown that the actual effective ranges are significantly greater. Claimed and true power consumptions range from a fraction of a Watt to several Watts.

2.2 Categories

The GPS jammers examined in this paper are grouped into three categories based on power source and antenna type. The first is a group of jammers designed to plug into an automotive cigarette lighter 12-Volt supply; this type of jammer is referred to in the remainder of this paper as Cigarette Lighter Jammers, or Group 1. A typical Group 1 jammer is pictured in Fig. 7 in Section 5. The second category contains those jammers which are both powered by an internal rechargeable battery and have an external antenna

connected via an SMA connector; these jammers are referred to as SMA-Battery Jammers, or Group 2. A typical Group 2 jammer is pictured in Fig. 10. The jammers in the last group also have batteries, but do not have external antennas; these are called NonSMA-Battery Jammers, or Group 3. A typical Group 3 jammer is pictured in Fig. 14.

2.3 Affected Frequencies

All 18 jammers broadcast power at or near the L1 frequency, 6 broadcast power at or near the L2 frequency, and none broadcast power at or near the L5 frequency. Some of the jammers also broadcast power at frequencies outside of the GPS bands, typically cell-phone or wi-fi bands, but those frequencies are outside the scope of this paper. The power levels at the non-GPS frequencies were significantly greater than the power levels at the GPS frequencies. The logical reason for the increase in power outside of the GPS frequencies is that the other systems are ground-based instead of space-based systems, and would therefore require more power to sustain effective jamming. Theoretically, the jammers that broadcast power outside of L1 or L2 frequencies could be made significantly more powerful with a slight design modifiication such that the full power were applied solely at the GPS frequencies.

2.4 Jammer Antennas

The jammer antennas have been removed in most of the testing for this paper, but they will modify the behavior in a real-world scenario. The antennas used by Group 1 and Group 2 jammers are loaded monopole antennas, Fig. 1, while those used by the Group 3 jammers are electrically short helical antennas that have approximately the same gain pattern as the loaded monopoles, Fig. 2. The result is that the antennas on the jammers broadcast linearly polarized radiation, as opposed to the GPS satellites which broadcast right-hand circularly polarized radiation. The polarization mismatch will cause some loss in received power at GPS receivers, which typically use right hand circularly polarized antennas.

3 JAMMER SIGNAL CHARACTERISTICS TEST EQUIPMENT

This section illustrates and describes the equipment used during the digitization and recording of signals

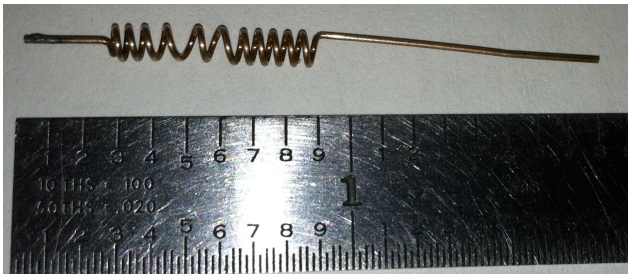

Figure 1 Slightly stretched loaded monopole antenna with cover removed. Used on Group 1 and Group 2 jammers.

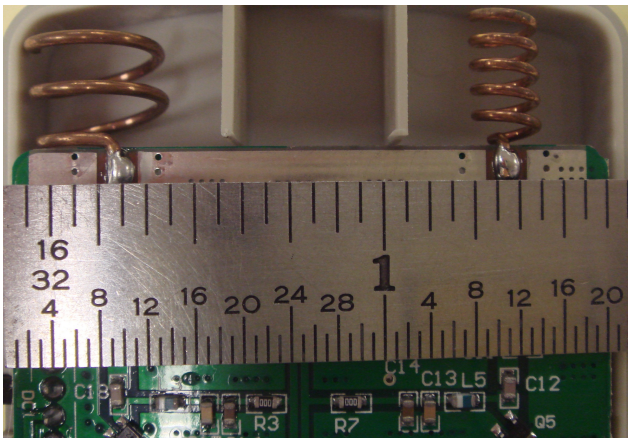

Figure 2 Electrically short helical antenna, with outside shell of the jammer removed. Used on Group 3 jammers.

Figure 3 Ramesy RF enclosure. Photograph reproduced with permission from Ramsey Electronics.

from all 18 GPS jammers. Four main pieces of equipment were used: a radio frequency enclosure, a spectrum analyzer, a data acquisition system, and a set of pickup antennas.

3.1 Radio Frequency Enclosure

Broadcasting malicious interference is illegal in the United States. During all the tests presented in this paper, the jammers were placed inside of a RF enclosure in order to prevent their signals from propagating through the environment. The signals were contained using a Ramsey RF enclosure, model STE3000B, Fig. 3. This box contains power connections, a shielded viewing port, a set of integrated metal-lined gloves, and a set of pass-throughs for the signal of interest.

The RF enclosure was tested for effectiveness by placing a jammer with antenna attached inside. A GPS receiver was then placed in the same room with a passive antenna pickup attached to a combiner with a rooftop GPS antenna signal. The jammer was activated, with no detectable change in behavior or C/N0 ratio of the GPS receiver.

3.2 Spectrum Analyzer

A spectrum analyzer was used to provide power spectra in order to determine the frequencies at which the jammers broadcast signals. The spectrum analyzer used in this testing was the Agilent CSA Spectrum Analyzer model N1996A, Fig. 4. This analyzer provides a power spectrum from 100 kHz–3GHz.

Figure 4 Agilent CSA Spectrum Analyzer model N1996A. Photograph reproduced with permission from Agilent Technologies.

3.3 Data Acquisition System

This study used the National Instruments data acquisition equipment NI PXI-5663, which is composed of the NI PXI-5601 downconverter, the local oscillator module NI PXI-5652, and the IF digitizer NI PXI-5622, Fig. 5. The system was hooked up to a HP GPS Timing and Reference Receiver for improved reference time. The system records 16-bit samples of in-phase and quadrature (I/Q) signals at 62.5 MHz and stores the data on a 12-drive RAID array. The system uses a finite impulse response (FIR) filter with a cutoff at 50MHz, creating an effective bandwidth of 50 MHz. The 50MHz filter is applied after downconverting, without an image-reject filter. The lack of the image-reject filter allows images from other frequencies to enter the spectrum of interest. The images have been removed in all power measurements with a post-processing digital FIR filter, in addition to the bandwidth-limiting filters presented in Subsection 5.6. The images have not been removed in any of the plots included in this paper.

Figure 5 National Instruments RF hardware. Photograph reproduced with permission from National Instruments.

3.4 Pickup Antennas

Group 3 jammers do not have external antenna connections. Measuring their signals necessitated the use of antennas. Two antennas were used. The first was an active L1/L2 GPS antenna, Antcom model 53G1215A-XT-1, and the second was a passive 1–2 GHz 4" spiral patch antenna made by Applied EM, model SAC0401.

4 JAMMER SIGNAL CHARACTERISTICS TEST PROCEDURE

The ultimate goal of this test was to record I/Q samples of the jamming signals and derive the jammer characteristics from the recorded data. A picture of the test 1 setup, without the spectrum analyzer or

pickup antennas, is shown in Fig. 6. The procedure is first described for the Group 1 and Group 2 jammers, and then the changes are described for the Group 3 jammers.

The test procedure is as follows. For the first two groups, the jammers were placed one at a time inside of the RF enclosure to prevent any signal leakage, and connected to the signal feed-through with a shielded coaxial cable. Another cable connected the external feed-through port to the spectrum analyzer. Once the signal analyzer was ready for a test run, the jammer under test was plugged in and activated. On the spectrum analyzer display, frequencies at which the jammers transmitted signals were identified. Once the signal bands of interest had been determined, the jammer output cable was attached to the data acquisition equipment where the signal was downconverted and I/Q sampled at 62.5 MHz for 1 minute at the appropriate frequencies.

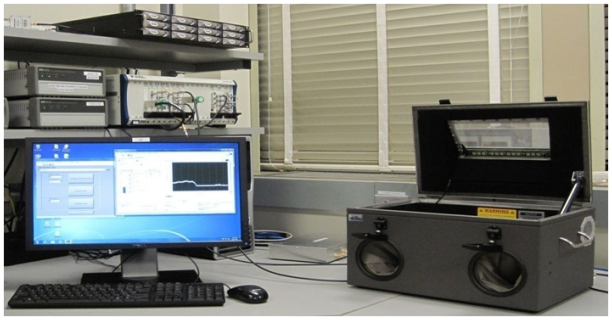

Figure 6 Test 1 setup, without the spectrum analyzer or pickup antennas shown.

None of the Group 3 jammers had external antennas. In order to capture the signal an antenna was placed in the RF enclosure oriented directly head-on to the jammers, and the antenna was connected to the feed-through. The active L1/L2 antenna was used to capture the signals at the L1 and L2 frequencies, but the passive antenna was used to locate power at all frequencies and to record data at non-GPS frequencies. No internal dimension of the RF enclosure is more than 18 inches, causing near-field effects to distort the recorded signals.

5 JAMMER SIGNAL CHARACTERISTICS TEST RESULTS

Although 18 jammers were tested, only a representative subset are presented. The signals were analyzed using DFTs and power plots, derived from the I/Q data and the NI system impedance. Each vertical slice of the upcoming DFT plots is a single DFT of 64 Hamming-windowed samples, in order to create about a 1-MHz resolution. The set of samples used is shifted by one index from one vertical slice to next. Unless otherwise noted, the horizontal axis of each plot spans 5000 such DFTs, that is 5063 I/Q samples, or about 80 microseconds. The plots will show that the jamming method used was a swept tone, *i.e.* linear frequency modulation. Some plots of the longer-term power behavior (80 ms instead of 80 microseconds) are also included for one of the interesting cases.

5.1 Group 1—Cigarette Lighter Jammers

Group 1 contained four jammers. One of the devices with its antenna removed is shown in Fig. 7. This group only interfered with the L1 frequency.

Figure 7 Cigarette Lighter Jammer, Group 1, with antenna removed.

Three of the Group 1 jammers appeared to be of the same model and one, Jammer 2, was slightly different. Despite their similarities in external appearance, the three jammers of the same model exhibited markedly different signal properties. Two of the signatures are shown in Fig. 8 and Fig. 9 for two physically similar devices, Jammer 1 and Jammer 4. The time and frequency scales are the same on both plots, but the power scales are not. They both exhibit linear frequency modulation, but over different frequency ranges and sweep rates. The first one actually sweeps outside of the sampled bandwidth causing an apparent power drop, but the second one stays within a 14MHz band centered around the L1 frequency.

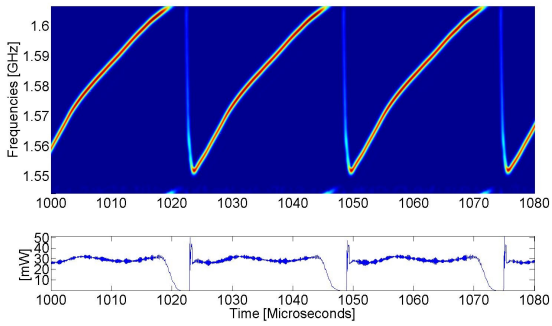

Figure 8 Jammer 1. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

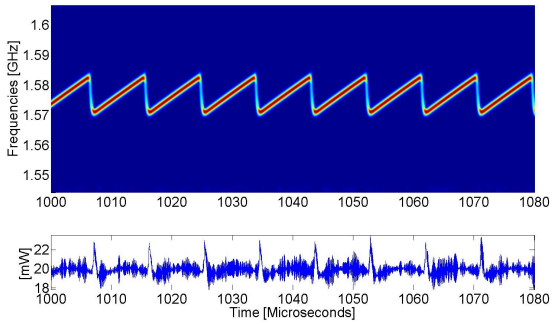

Figure 9 Jammer 4. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

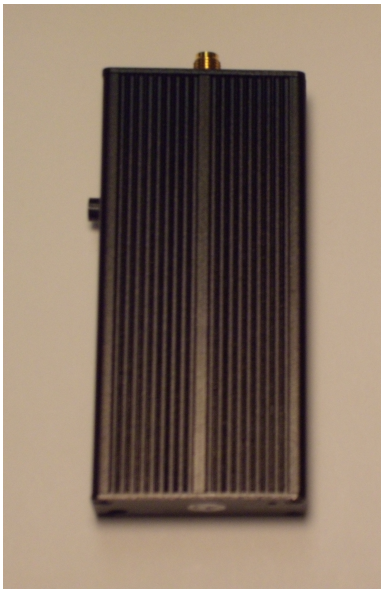

Figure 10 SMA-Battery Jammer, Group 2, with antenna removed.

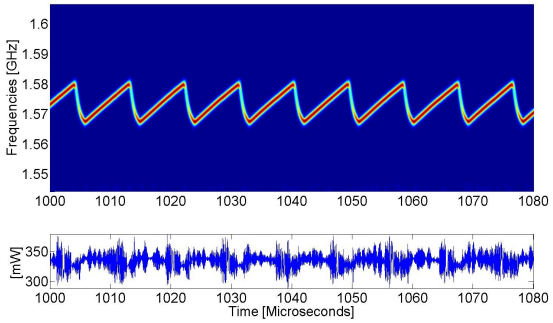

Figure 11 Jammer 8. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

5.2 Group 2—SMA-Battery Jammers

Ten of the 18 jammers were battery-powered and had external antennas, and were thus placed into Group 2. One of the devices, with the antenna removed, is shown in Fig. 10. There were only a few repeated models in this group, and the jammers had between one and four antennas. All broadcast power at L1, two broadcast power at L2 in addition to L1, and five of the jammers broadcast power at other frequencies in addition to the GPS frequencies.

Most of the jammers in this group produce signals that look very similar to that shown in Fig. 11. These jammers used, almost exclusively, linear frequency modulation, similar to Group 1. Despite the same type of jamming behavior, they still had some jammer-to-jammer variation in sweep rate and significantly different behavior in sweep range.

Three jammers in this group deserves additional attention, Jammers 10, 12 and 13. In Jammers 12 and 13 the signal that seemed intended to jam L1 does not sweep through L1, 1575.42 MHz. This type of behavior is explained more in Section 5.5. Jammer 10 produced a triangular waveform of tone frequency versus time and at a much shorter sweep period than the other jammers. The pattern at the L2 frequency is shown in Fig. 12 and Fig. 13. Where Fig. 13 is a more detailed view and contains only 8 microseconds of data instead of 80.

5.3 Group 3—NonSMA-Battery Jammers

Four of the jammers were placed in Group 3, the NonSMA-Battery Group. One of the devices is shown in Fig. 14. All four jammers in this group broadcast power at other frequencies in addition to L1 and

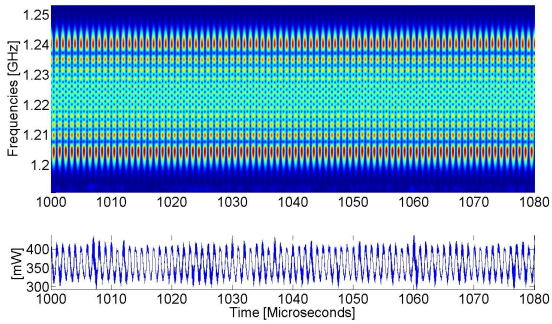

Figure 12 Jammer 10. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

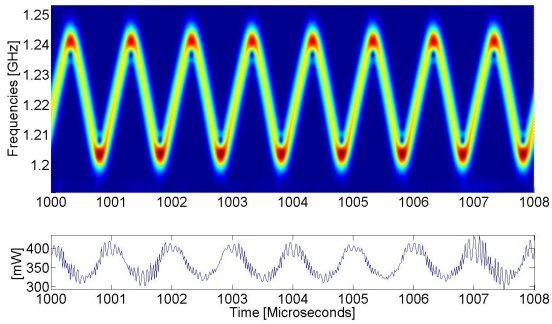

Figure 13 Jammer 10. The top plot displays vertical slices of 20-point Hamming-windowed DFTs, and the bottom plot is of power. Note the shorter time period and reduced number of points in the DFT.

Figure 14 NonSMA-Battery Jammer, Group 3. It is meant to be disguised as a cellphone.

L2. Three of the jammers appeared to be of the same model, while a fourth was different.

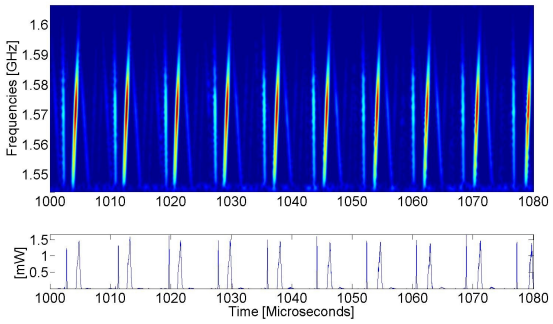

Figure 15 Jammer 16. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

The two figures in this section show data recorded using the L1/L2 active GPS antenna. Fig. 15 and Fig. 16 show the L1 signals from Jammers 16 and 18. The lower-power reflected image seen in Fig. 16 may be due to the lack of an image reject filter on the NI data acquisition system. Although not as severe, variations in sweep range between jammer of the same apparent models was similar to that seen in Group 1.

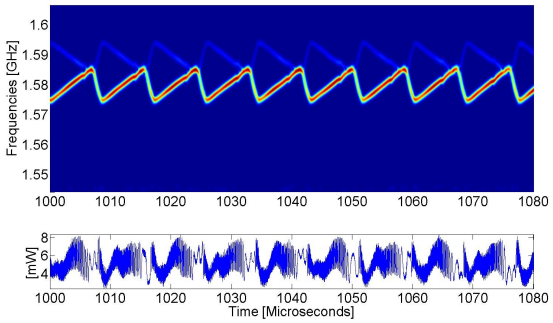

Figure 16 Jammer 18. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power.

The only jammer in this group that deserves additional attention is Jammer 17, because the signal that seemed intended to jam L1 does not sweep through L1, 1575.42 MHz. This type of behavior is explained more in Section 5.5.

5.4 Sweep Periods

The sweep behavior is presented in Table 1 for all 18 jammers. The first column sorts the jammers into their

groups and the second column numbers them for reference. The third column presents the sweep periods and the fourth column presents the sweep ranges about the L1 frequency, with the first number being the range above the L1 frequency and the second being the range below the L1 frequency. The fifth and sixth columns are the analog of columns three and four but for the L2 frequency.

The sweep rates were calculated twice, starting at 1 second into the data sets and then again 30 seconds later. The values of the sweep periods did not change significantly between these two measurements. The values of the sweep ranges were calculated twice and the extremes were taken. The sweep ranges changed as much as 2.5 MHz between measurements. Any entries of "over" indicate that the jammer exceeded the 62.5 MHz range of the data acquisition equipment.

5.5 Variations in Behavior

Eleven of the 18 jammers had consistent and effective behavior over the one-minute data sets, but seven of them had variations in behavior for at least part of their data sets. Four types of aberrant behavior with respect to standard chirp signals were identified. The first types of deviant behavior does *not* diminish the jammer's effectiveness. The second and third type of behavior could diminish the jammer effectiveness, and the fourth type *does* diminish the jammer effectiveness.

The first aberrant behavior, exhibited by three jammers, was small variations, or ripples, in the linear frequency modulation, such as that shown in Fig. 17 for Jammer 6.

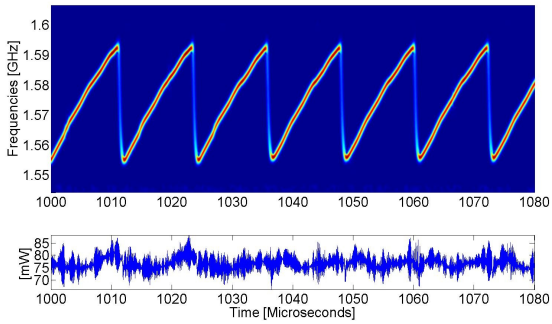

Figure 17 Jammer 6. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power. Notice the slight ripples in the sweep pattern.

The second type of aberrant behavior is gross irregularities in the tone sweep, where the ripples from the first type of behavior now become distinct jumps in frequency. Two jammers showed this behavior. An example from Jammer 15 is shown in Fig. 18.

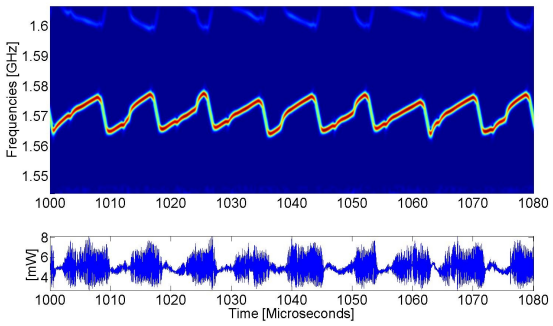

Figure 18 Jammer 15. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power. Notice the significant changes in the sweep pattern.

The third type of interesting behavior was variations in the peaks and troughs of the tone sweep—that is, the tone was swept from a variable low frequency to a variable high frequency. Jammer 5 exhibited this behavior (along with type 2 behavior), shifting the center frequency by at least 2.5 MHz over 41 microseconds in what appears to be an additional sawtooth pattern on top of the chirp signal. An example is plotted in Fig. 19 for a longer time period of about 190 microseconds.

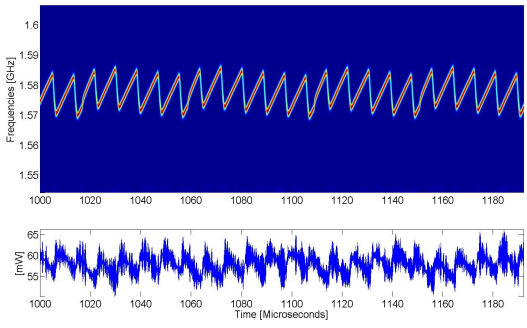

Figure 19 Jammer 5. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power. Notice the variation of the center frequency and the longer time span.

The fourth type of interesting behavior was the jammer's center frequency being too far from the L1 or L2 frequency to be an effective GPS jammer. A total of 3 jammers exhibited this type of behavior (12, 13, and 17), although many of the jammers did not have their center frequencies directly on the L1 or L2 frequencies. An example is plotted in Fig. 20 for Jammer

Table 1 Sweep behavior of the GPS jammers.

Group Number	Jammer Number	L1 Sweep Period microseconds	L1 Sweep Range (L1+/-) MHz	L2 Sweep Period microseconds	L2 Sweep Range (L2+/-) MHz
1	1	26	31.3 / 25.4	-	-
	2	27	31.3 / 31.3	-	-
	3	9	8.6 / 5.4	-	-
	4	9	9.6 / 4.4	-	-
2	5	9	11.6 / 7.4	-	-
	6	12	19.6 / 21.4	-	-
	7	9	7.6 / 6.4	-	-
	8	9	6.6 / 9.4	-	-
	9	9	5.6 / 8.4	-	-
	10	1	over / over	1	19.4 / 29.6
	11	9	5.6 / 6.4	9	3.4 / 7.6
	12	8	17.6 / -5.6	-	-
	13	9	18.6 / -4.6	-	-
	14	9	7.6 / 6.4	-	-
3	15	9	3.6 / 13.4	9	2.4 / 16.6
	16	8	over / over	8	16.4 / 26.6
	17	9	-5.4 / 16.4	9	-7.6 / 20.6
	18	9	10.6 / 8.4	9	0.4 / 15.6

13, with a line placed across the L1 frequency for reference. Jammer 17 also exhibited this type of behavior, and was offset a similar amount on both the L1 and L2 frequencies.

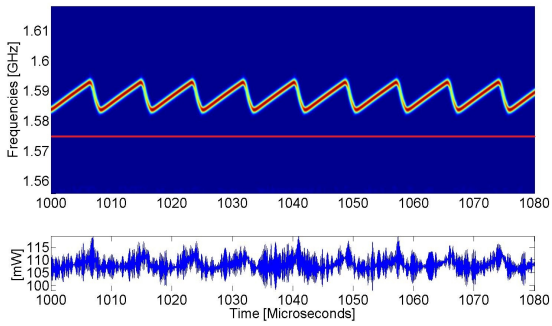

Figure 20 Jammer 13. The top plot displays vertical slices of 64-point Hamming-windowed DFTs, and the bottom plot is of power. Notice the offset in the center frequency from L1.

5.6 Radio Frequency Power In Bands

The GPS signal is spread over several megahertz by the PRN codes that modulate the L1 or L2 carrier waves. Different GPS receivers exploit this spreading by using more or less of the bandwidth. As a result, the RF power of the GPS jamming signal within different bands centered at L1 is an important concern. In order to determine the power in bands of different sizes, the raw data were filtered to pass only the bandwidths of interest. The images were removed from Jammers 15 and 18 before the application of the bandwidth filters. The images could be removed because there was no overlap with the data of interest.

The data were digitally filtered using an FIR equiripple bandpass filter from the Filter Design toolbox in MATLAB, providing 60 dB attenuation at 2MHz past the cutoff frequency. It may be important to note that a real GPS receiver will probably not have frequency cutoffs as sharp as those used in this paper. The power results are presented in Table 2 for the averages and peak of the three groups, for the three different bandwidths: 2, 20 and 50 MHz. The table also indicates whether each jammer broadcasts power at frequencies other than the GPS frequencies. No power data is given for the non-GPS frequencies because they are not the focus of this paper, and no jammers broadcast any power at the L5 frequency.

It should be emphasized that the power values for two of the groups, Group 1 and Group 2, were derived using direct cable connections and that in real applications there will be additional losses due to the antennas of the jammers. The Group 3 values should be considered even less reliable, because of near-field effects and because they were measured using an active L1/L2 GPS antenna.

Table 2 Mean jammer power for different bandwidths about L1 and L2, and indicators of power at other frequencies.

Group Number	Jammer Number	L1 Bandwidth, MHz			L2 Bandwidth, MHz			Non-GPS Frequencies
		2	20	50	2	20	50	
		Power in band, mW			Power in band, mW			Yes/No
1	1	1.7	9.5	22	-	-	-	No
	2	0.1	0.7	1.8	-	-	-	No
	3	5.8	20	20	-	-	-	No
	4	7.0	23	23	-	-	-	No
2	5	15	58	58	-	-	-	No
	6	6.3	40	77	-	-	-	Yes
	7	150	520	520	-	-	-	Yes
	8	87	334	334	-	-	-	Yes
	9	159	499	499	-	-	-	Yes
	10	1.2	6.5	19	27	146	351	No
	11	244	642	642	221	482	482	No
	12	0.00	58	109	-	-	-	No
	13	0.00	43	107	-	-	-	No
	14	18	42	42	-	-	-	Yes
3	15	1.18	4.76	4.95	0.60	5.44	7.70	Yes
	16	0.01	0.04	0.07	0.04	0.20	0.26	Yes
	17	0.00	1.46	3.44	0.00	0.37	7.74	Yes
	18	1.39	4.61	4.69	0.61	4.66	5.64	Yes

There were three jammers (12, 13, and 14) that all showed similar interesting long-term power behavior. An example of the long-term power plots is shown in Fig. 21 with an 80 ms (not microsecond) range. The power appears to behave in a saw-tooth pattern with a period of approximately 15 ms.

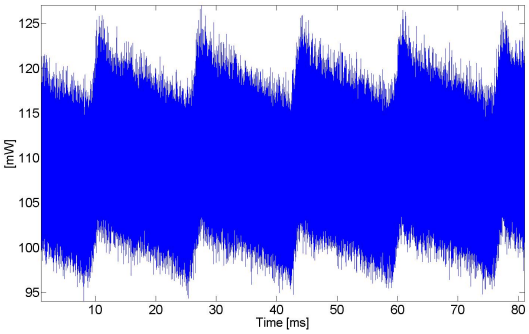

Figure 21 Jammer 12, over a long time span of 80 ms, with a 15 ms period.

6 MAXIMUM EFFECTIVE RANGE TEST EQUIPMENT

In addition to the tests described above, four jammers were subjected to tests designed to estimate their maximum effective ranges. This section presents the four main pieces of equipment in the second test: the RF enclosure, a set of attenuators, a GPS simulator, and a GPS receiver. The RF enclosure is the same Ramsey enclosure mentioned in Section 3. The attenuators are just standard RF attenuators with SMA couplings and are not shown in this paper.

6.1 GPS Simulator

The GPS simulator used in this test is the Spirent GSS7700 GPS/SBAS Simulator, Fig. 22, along with a Spirent GSS8000 GNSS Simulator and Spirent GSS8368 Multi-Box Combiner Unit, Fig. 23. The simulator is a commercially available, high-fidelity system.

6.2 GPS Receiver

The GPS receiver used in this test is the Novatel ProPakII-RT2. This is an L1 and semicodeless L2 receiver.

7 MAXIMUM EFFECTIVE RANGE TEST PROCEDURE

The ultimate goal of this test was to determine the effective range of these GPS jammers without broad-

Figure 22 Spirent GSS7700 GPS SBAS Simulator. Photograph reproduced with permission from Spirent Federal Systems.

Figure 23 Spirent GSS8000 GNSS Simulator and Combiner. Photograph reproduced with permission from Spirent Federal Systems.

Figure 24 Jammer effective ranges test setup.

casting harmful radiation in an outdoor test. Ideally, the jammers and a receiver would be taken outside and tested with all antennas attached. This type of test would possibly interfere with other equipment and is illegal. A close approximation to this scenario can be constructed using a GPS simulator, GPS receiver, GPS jammer, RF enclosure, and a set of attenuators.

The setup for the second test is shown in Fig. 24. The procedure was as follows. A GPS jamming signal was passed through the RF enclosure and combined with a GPS simulator signal. The combined signal was then fed into a GPS receiver. Attenuators were inserted into the line of the GPS jammer before it arrived at the combiner.

The attenuation was increased with a 1 dB resolution until tracking was sustained after jammer activation, and then again until acquisition was possible within 5 minutes from a cold start. The attenuation values that allowed acquisition and tracking were recorded and are shown in Table 3. As will be shown in Section 8, the attenuation values can be converted into effective ranges of the jammers with a number of reasonable assumptions about transmitting and receiving antenna gains and path losses.

The power level on the GPS simulator was set to a value of -130 dBm, the required minimum power level of the GPS constellation at ground level [9], and then another 10 dB was added. The 10 dB was added in order to overcome the losses due to the signal combiner and cable line losses, along with the fact that the GPS constellation transmits at a power level greater than the minimum required level. As a sanity check against the results, the C/N0 ratio for all the visible satellites was calculated using a patch antenna attached to the same receiver on top of one of the academic buildings on Cornell University's Ithaca campus. The resulting C/N0s were similar to within approximately 1 or 2 dB-Hz.

8 MAXIMUM EFFECTIVE RANGE TEST RESULTS

The jammer attenuations that allowed the receiver to acquire and start tracking are presented in Table 3, for one jammer from Group 1 and three jammers from Group 2. No jammers from Group 3 were included due to the uncertainties introduced by the near-field effects.

The attenuation values by themselves are not very useful, but they can be converted into distance measurements if we make a number of assumptions and use

Table 3 Effective attenuation.

Group Number	Jammer Number	Tracking dB	Acquisition dB
1	1	82	92
2	10	82	88
	11	108	111
	13	77	89

Equation 1 from reference [10]. In Equation 1 the term P_r is the received power, P_t is the transmitted power, G_t is the transmitting antenna gain, G_r is the receiving antenna gain and the other terms are due to the isotropic radiation path loss. Equation 1 can be rearranged to solve for the range, as in Equation 2. The total attenuation experienced along the path of the jammer to the receiver is equal to the term γ in Equation 3, or $G_t G_r \left(\frac{P_t}{P_r}\right)$.

$$\frac{P_r}{P_t} = \frac{G_t G_r \lambda^2}{(4\pi r)^2} \tag{1}$$

$$r = \left(\frac{\lambda}{4\pi}\right) \sqrt{G_t G_r \left(\frac{P_t}{P_r}\right)} \tag{2}$$

$$r = \left(\frac{\lambda}{4\pi}\right) \sqrt{\gamma} \tag{3}$$

If we assume that the transmitting and receiving antennas are perfect, lossless, isotropic radiators, then the gain terms G_r and G_t become unity. The above assumption is revisited in the next paragraph. The result is that the measured attenuations are now equal to $\left(\frac{P_t}{P_r}\right)$. The next step is to convert from dB to unitless gain and plug the result into Equation 3. Solving for the result at the L1 frequency we arrive at the results listed in Table 4.

Table 4 Effective distance, with lossless isotropic antennas.

Group Number	Jammer Number	Tracking m	Acquisition m
1	1	308	973
2	10	308	614
	11	6140	8670
	13	173	689

Distinct scenarios with different antennas can be approximately tested using Table 3 and Equations 1–3. For example, a patch antenna that is oriented perfectly skyward might have 10 dB of attenuation at very low elevations, and the jammer might have around an additional 3 dB loss due to the jammer broadcasting linearly polarized signals. Another set of losses might come from emissions passing through a car door or any imperfections in the system. These effects could be incorporated into Equation 2 to determine a revised effective range, instead of the idealized lossless isotropic antenna case presented in Table 4.

Due to the ignored losses in the real system, it would likely be safe to assume that the effective range of the GPS jammers would be no greater than those listed in Table 4. The ranges could potentially be greater if a high gain antenna was aimed directly at the jamming source, or if the jamming source used a high gain transmitting antenna, though none of the jammers tested employed such an antenna.

9 SUMMARY AND CONCLUSION

This paper surveyed the signal properties of 18 commercially available GPS jammers based on experimental data, and was divided into two distinct tests. The first test of the 18 jammers provided information on the characteristics of current civil GPS jammer signals, and the second test provided an estimate of four of the jammers' effective ranges.

The first test showed that the jammers used, without exception, the swept tone method. The majority of the jammers used chirp signals, all jammed L1, only six jammed L2 and none jammed L5. The sweep rate of the jammers is on average about 9 microseconds, and they tend to cover a range of less than 20 MHz. Not all jammers were centered on the L1 or L2 frequency, and at least one jammer's center frequency moved more than 2.5 MHz during 41 microseconds of operation. Seven of the 18 jammers exhibited some sort of what can be classified as aberrant behavior. Depending on which jammer is being used and the type of filter on the GPS receiver, three of the 18 jammers would likely not be effective at almost any range.

The second test on a subset of four of the devices provided information on the effective range of the GPS jammers. Using the setup from Section 6 and the procedure in Section 7 an upper bound on the effective distances were calculated for idealized lossless isotropic radiating and receiving antennas with matched polarizations. The Group 1 Cigarette-Lighter Jammer (J1) disrupted tracking at an effective range of 300 m and acquisition at about 1 km. The most powerful L1 and L2 Group 2 SMA-Battery Jammer (J11) disrupted

tracking at an effective range of 6.1 km and acquisition at an effective range of about 8.7 km.

ACKNOWLEDGEMENTS

The authors thank the U.S. Department of Homeland Security for providing interference devices for testing.

REFERENCES

[1] Misra, P. and Enge, P., *Global Positioning System: Signals, Measurements, and Performance*, Ganga-Jamuna Press, Lincoln, Massachusetts, 2nd ed., 2006.

[2] Spilker, J. Jr. and Van Dierendonck, A. J., *Global Positioning System: Theory and Applications Volume 2*, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1st ed., 1996, pp. 117-142.

[3] Michael, K., McNamee, A., Michael, M.G., "The Emerging Ethics of Humancentric GPS Tracking and Monitoring," *Proceedings of the International Conference on Mobile Business*, IEEE Computer Society, 2006.

[4] Poisel, R., *Modern Communications Jamming Principles and Techniques*, Artech House, Boston, Massachusetts, 1st ed., 2004.

[5] Spilker, J. Jr. and Natali, F., *Global Positioning System: Theory and Applications Volume 1*, chap. Interference Effects and Mitigation Techniques, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1st ed., 1996, pp. 717-771.

[6] Moeness, A., Zhao, L., Lindsey, A., "Subspace Array Processing for the Suppression of FM Jamming in GPS Receivers," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 40, No. 1, 2004.

[7] Adamy, D., *EW 102 : A Second Course In Electronic Warfare*, Artech House, Boston, Massachusetts, 2004, Books24x7. <http://common.books24x7.com/toc.aspx?bookid=10256>(accessed September 16, 2011).

[8] Poisel, R., *Electronic Warfare Target Location Methods*, Artech House, Boston, Massachusetts, 1st ed., 2005.

[9] Anon., *Global Positioning System Wing (GPSW) System Engineering and Integration*, Global Positioning Systems Wing, June 2010, IS-GPS-200E.

[10] Couch, L. II, *Digital And Analog Communication Systems*, Macmillan Publishing Company, New York, NY, 4th ed., 1993.