Characterization of Receiver Response to Spoofing Attacks

by

Daniel Shepard

THESIS

Presented to the Faculty of the Undergraduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

BACHELOR OF SCIENCE

IN

AEROSPACE ENGINEERING

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2011

Characterization of Receiver Response to Spoofing Attacks

APPROVED BY

SUPERVISING COMMITTEE:

Todd Humphreys, Supervisor

Mack Grady, Supervisor

Acknowledgments

I would like to thank Dr. Humphreys and Dr. Grady for advising me on this thesis. It has been a wonderful experience that I could not have completed without you. I would also like to thank Jahshan Bhatti for helping me with the spoofer code.

Characterization of Receiver Response to Spoofing Attacks

Daniel Shepard, B.S. ASE
The University of Texas at Austin, 2011

Supervisors: Todd Humphreys
Mack Grady

Test procedures are developed for characterizing the response of civil GPS receivers to spoofing attacks. Two response characteristics are analyzed in detail for four representative GPS receivers: (1) the agressiveness with which a spoofer can manipulate the victim receiver's time and position solution, and (2) the spoofer power advantage over the authentic signals required for successful receiver capture. Two of the tested receivers are commonly used in critical infrastructure applications, one in "smart" power grid regulation and one in telecommunications networks. The implications of the test results for these critical infrastructure applications are discussed.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In 2001, the U.S. Department of Transportation (USDOT) evaluated the transportation infrastructure's vulnerability to GPS and raised concern over the threat of GPS spoofers [3]. Spoofers generate counterfeit GPS signals that commandeer a victim receiver's tracking loops and induce spoofer-controlled time or position offsets. The USDOT report noted the absence of any "off the shelf" defense against civilian spoofing and recommended a study to characterize spoofing effects and observables. In 2008, researchers demonstrated that an inexpensive portable software-defined GPS spoofer could be built from off-the-shelf components, again highlighting the threat of spoofing [1].

Studying the response of various civil GPS receivers to spoofing attacks allows one to better determine the effects that such an attack could have on various critical infrastructures which rely on civil GPS for positioning, timing, or both. The specific questions that this research seeks to answer through experimentation are:

1. How aggressively can a civil GPS receiver's navigation and timing solution be manipulated by a spoofing attack?

2. Would a jamming-power-to-noise-power (J/N)-type detector, commonly used in military GPS receivers to detect jamming attacks, trigger on a spoofing attack?

The four receivers tested are meant to be a representative cross-section of civil user equipment. The receivers are (1) a science-grade receiver, (2) a time reference receiver with a highly stable internal clock used in telecommunications networks, (3)

a time reference receiver with a less stable internal clock used on the power grid, and (4) a consumer-grade handheld receiver.

While much promising research is currently being conducted on methods for detecting and mitigating spoofing, these methods are still years away from wide-scale implementation. Meanwhile, it is important to understand what risks a spoofing attack poses on existing equipment. One option for reducing these risks is to simply purchase receivers that have proven to be more difficult to spoof.

Cell phone networks are one segment of critical infrastructure that is vulnerable to civil spoofing attacks. CDMA cell phone towers rely on GPS timing for tower-to-tower synchronization. This prevents the towers from interfering with one another and enables call handoff from one tower to the next. If a particular tower deviates more than $10\mu s$ from GPS time, handoff to and from that tower is disrupted and overall network throughput is reduced [4].

The power grid also possesses a unique vulnerability to spoofing attacks. More efficient distribution of power across the grid will require real-time measurements of the voltage and current phasors [5]. Synchrophasor Measurement Units (SMUs) have been proposed as a smart grid technology for precisely this purpose. SMUs rely on GPS to time stamp their measurements, which are sent back to a central monitoring station for processing. Manipulation of a SMU's time stamp results in spurious variations in the measured phase angles. These variations could distort power flow or stability estimates in such a way that grid operators would take incorrect or unnecessary control actions including powering up or shutting down generators. This could cause blackouts or damage to power grid equipment.

Chapter 2

The Spoofer

The Civil GPS Spoofer used for these tests, shown in Figure 2.1, was designed by Dr. Todd Humphreys and Dr. Brent Ledvina and is the only spoofer reported in open literature to date that is capable of precisely aligning its counterfeit signals with the authentic GPS signals [1]. Such alignment capability allows the spoofer to carry out a sophisticated spoofing attack in which no obvious clues remain to suggest that an attack is underway. This spoofer is implemented on a portable software-defined radio platform with a Digital Signal Processor (DSP) at its core. This platform is composed of:

- A Radio Frequency (RF) front-end that down-mixes and digitizes GPS L1 and L2 frequencies
- A DSP board that performs acquisition and tracking of GPS L1 C/A and L2C signals, calculates a navigation solution, and produces a consistent set of spoofed GPS L1 C/A signals with a fictitious implied navigation and timing solution.
- A RF back-end with a digital attenuator that converts the digital samples of the spoofed signals from the DSP to analog output at the GPS L1 frequency and at a user-specified broadcast power.
- A Single Board Computer (SBC) that handles communication between the spoofer and a host computer over the Internet.

The spoofer works by first acquiring and tracking GPS L1 C/A and L2C signals to obtain a navigation solution. Once a navigation solution has been obtained, the

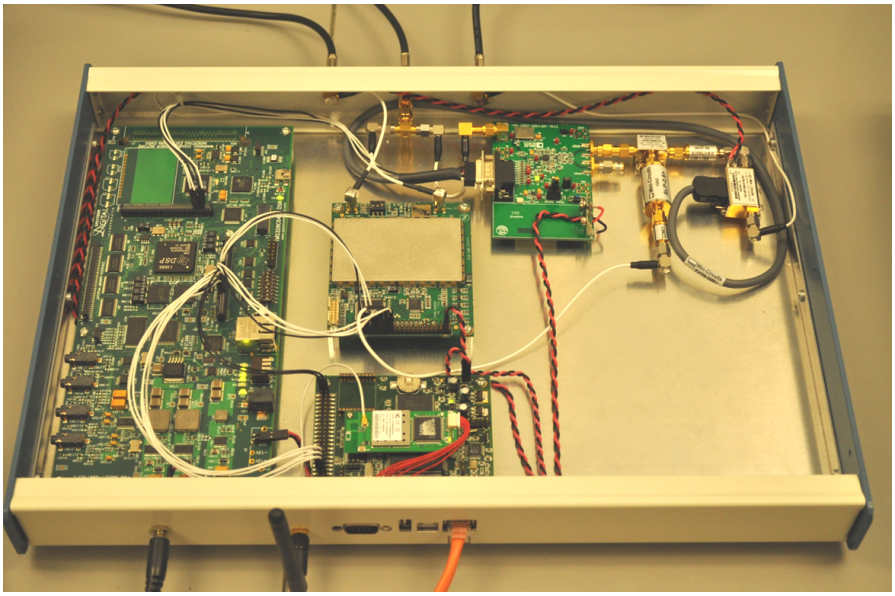

Figure 2.1: The Civil GPS Spoofer

spoofer enters its "feedback" mode. In this mode, the spoofer produces a counterfeit, data-free feedback GPS signal that is summed with its own antenna input. The feedback signal is tracked by the spoofer and used to calibrate the delay between production of the digitized spoofed signal and output of the analog spoofed signal This is necessary because the delay is non-deterministic on startup of the receiver, although it stays constant thereafter.

After feedback calibration is complete, the spoofer is ready to begin an attack. It produces signals that are initially nearly perfectly aligned with the authentic signals at a low power to remain below the noise floor. The spoofer then raises the power of the spoofed signals slightly above the that of the authentic signals. At this point, the spoofer has taken control of the victim receiver's tracking loops and slowly leads the spoofed signals away from the authentic signals, carrying the receiver's tracking solution with it. Once the spoofed signals have moved more than $600m$ in position or $2\mu s$ in time away from the authentic signals, the receiver has been completely captured.

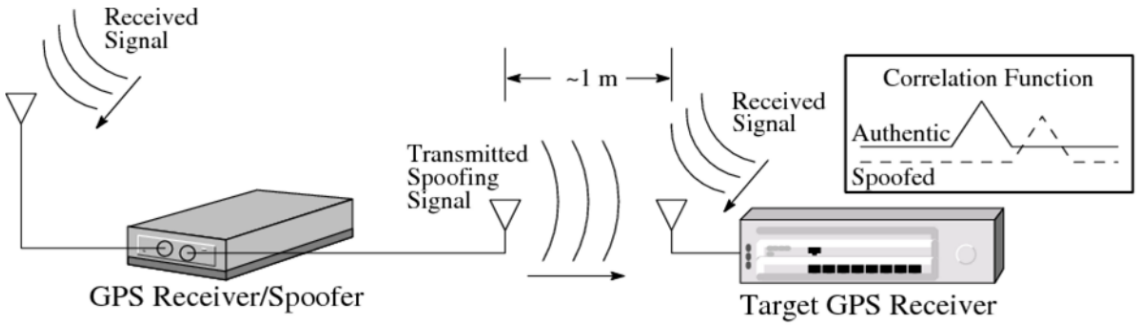

Figure 2.2: A proximity spoofing attack [1]

For the experiments reported in this paper, the spoofed signals were not broadcast over the air, but were routed via coaxial cable to the antenna input of the target receiver, where they were summed with the authentic signals. This configuration is representative of a proximity spoofing attack, where the spoofer is within a meter or so of the target receiver, as shown in Figure 2.2. In this case, the spoofer does not need to account for the distance between its antenna and the target receiver's antenna.

Some modifications to the spoofer were required for these tests. First, the spoofer had to be modified to predict the incoming $50Hz$ GPS navigation data bits so that its $5ms$ internal processing delay would not be reflected in the spoofer's output signals. Such a delay would be an obvious indicator of a spoofing attack. Second, a spoofer control scheme had to be developed to support repeated controlled tests. The following sections describe the modifications in more detail.

2.1 Data Bit Prediction

The data bit structure on the civil GPS L1 C/A signal is well-defined by the GPS Interface Control Document (ICD). These data bits have a bit rate of $50Hz$ and act as a secondary modulation of the signal over the spreading code that has a bit rate of $1.023MHz$. A full set of databits consists of a $37,500$-bit superframe, lasting 12.5 minutes, that is divided into 25 frames with $1,500$ bits each. Each frame is then

further divided into five 300-bit subframes each with ten 30-bit long words.

The first two subframes of each frame contain the satellite ephemerides (orbital parameters) and clock parameters which repeat every frame. These two subframes may be updated by the control segment at the start of every even hour as defined by Coordinated Universal Time (UTC). The last three subframes are referred to as the almanac and contain health status information and less precise ephemerides for each GPS satellite. The almanac is updated much less frequently than the ephemerides (usually about once a week), but the timing of its update is not specified. Each subframe also begins with the same two words called the telemetry (TLM) word, which marks the beginning of the subframe, and the Hand-Over word (HOW), which gives the time of transmission and the subframe number [6].

Using the data bit format described by the GPS ICD, a C++ class called the Data Bit Manager (DBM) was developed that would store the received data bits, keep track of the status of the local data bit database, and return predictions of the data bits when requested. The DBM was incorporated into the spoofer to allow it to immediately predict the current data bit once the database has been filled. It is obviously not possible to completely predict the data bits while an update to the ephemerides or almanac is occurring. This means that the spoofer should not begin an attack during a time when the ephemerides or almanac data are changing, since this might result in erroneous data bits in the spoofed signals. These erroneous bits would cause havoc in the tracking loops of the target receiver during the initial phase of a spoofing attack when the spoofed and authentic signals are nearly aligned. The DBM was designed to handle an update to the data bits once the target receiver has been captured by holding over the old bits until the new ones have been received. This results in a delay to the update of the data bits seen by the target receiver, but no receiver would view this suspiciously since the control segment does not always update the ephemerides perfectly on time.

2.2 Spoofer Control

In order to operate the spoofer during an attack, it is necessary to have real-time control of the spoofer's counterfeit navigation and timing solution and of the output power of the spoofed signals. At the beginning of this thesis work, the spoofer was already capable of communicating with a host computer over the Internet through its Single Board Computer (SBC) using a client/server type relationship. This communication consisted primarily of data packets sent from the spoofer to the host computer reporting tracking information, the spoofer's navigation solution, and the position and velocity offset from the spoofer's navigation solution suggested by the spoofed signals. The only commands that the SBC was able to receive were power cycle commands, receiver status requests, a command to re-flash the DSP with a new image, and configuration file transfers.

The original SBC client and server code was overhauled to include a wide variety of commands that allow the spoofer to be precisely controlled. These commands are input through a command line interface with a second window displaying the current receiver status. Figure 2.3 shows the command line and display windows on the host computer. The control commands incorporated into the spoofer include:

zero Zero out the spoofer's target position and velocity offset.

att (LEVEL) Set the attenuation of the spoofer's digital attenuator in dB.

reset (soft/hard) Perform a soft/hard reset of the DSP.

dbm (on/off) Turn the databit manager on/off.

plock (on/off) Turn the frequency lock to the authentic signal on/off (required to better mask the spoofer during the initial phases of a spoofing attack).

feedback (on/off) Turn feedback mode on/off.

upload (OPTION) Upload data to the SBC/DSP with the following options:

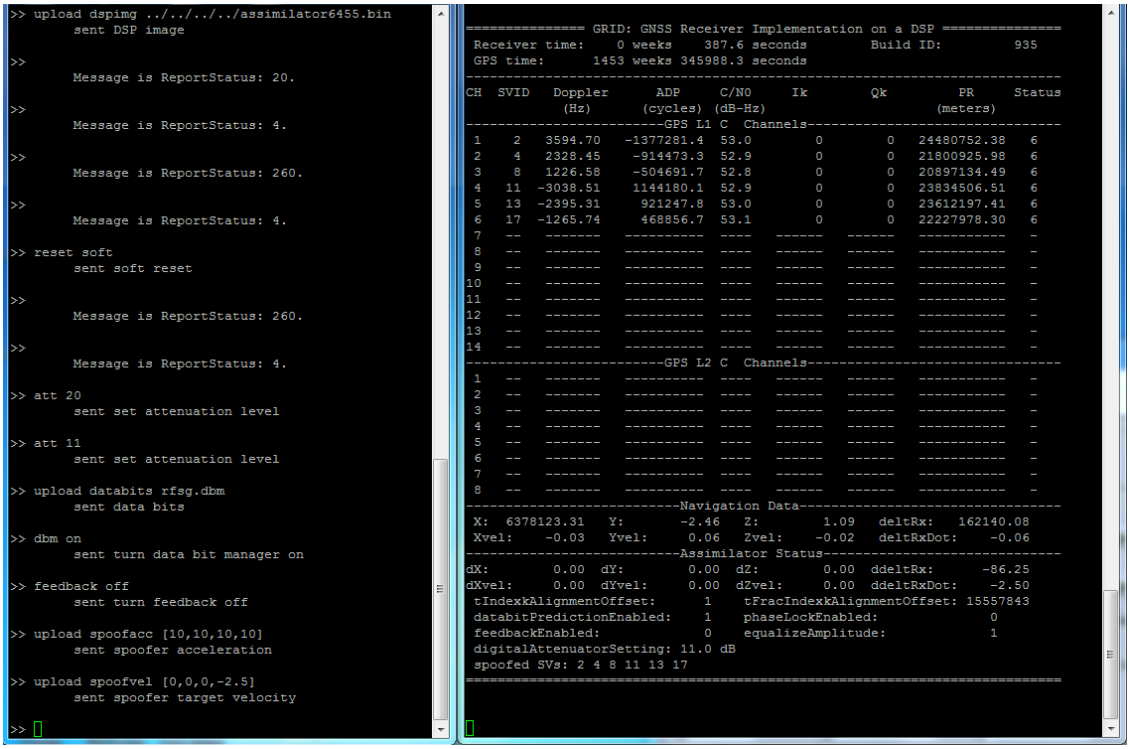

Figure 2.3: The command line (left) and display (right) windows for the SBC client

dspimg (FILENAME) Flash a new image to the DSP.

dspconfig (FILENAME) Send a new dspconfig file to the SBC.

sbcconfig (FILENAME) Send a new sbcconfig file to the SBC.

databits (FILENAME) Send a data bit database to the DBM.

spoofvel [VX,VY,VZ,DTDOT] Update target velocity the spoofer is trying to match.

spoofacc [AX,AY,AZ,DTDOTDOT] Update the acceleration of the spoofer (used to smoothly transition between target velocities).

download (OPTION) Download data from the SBC/DSP with the following options:

databits (FILENAME) Retrieve the data bit database from the DBM.

script (FILENAME) Run a set of commands consecutively from an input file.

sleep (TIME) Wait for a number of seconds to elapse before continuing execution.

Chapter 3

Approach

Two questions were posed in Section 1 that this work seeks to answer. Those questions were

1. How aggressively can a civil GPS receiver's navigation and timing solution be manipulated by a spoofing attack?
2. Would a jamming-power-to-noise-power (J/N)-type detector, commonly used in military GPS receivers to detect jamming attacks, trigger on a spoofing attack?

In order to answer these questions, they first need to be broken down into a more manageable form that can be answered directly from testing.

3.1 Aggressive Receiver Manipulation

It is important to understand the types of dynamics that a spoofer could induce in a target receiver, since the critical infrastructure that is reliant on GPS often requires certain accuracy in position/timing. This is the reason for using GPS in the first place. The potential for spoofer induced oscillations in position and timing is also important for certain applications including the smart grid.

This suggests three questions that need to be answered:

1. How quickly could a timing or position bias be introduced?
2. What kinds of oscillations could a spoofer cause in a receiver's position and timing?

3. How different are receiver responses to spoofing?

The approach taken to answer these questions was to determine the maximum velocities that can be induced in a target receiver over a range of accelerations. The curve in the acceleration-velocity plane created by connecting these points defines the upper bound of a region in which the spoofer can safely manipulate the target receiver without raising any alarms or causing the target receiver to have difficulty tracking. Figure 3.1 shows four conceivable shapes for this curve (a vertical line, a horizontal line, a line with a negative slope, and an exponential curve) with the green area representing the safe region for a spoofer to operate and the red area representing the region where a spoofer will likely be caught. Once these curves have been obtained, they can be used to determine the kinds of dynamics a spoofer could induce on that receiver and compared to curves of other receivers to find which receivers provide the most "resistance" to a spoofing attack.

3.2 Jamming Detector

A J/N-type jamming detector works by comparing the in-band absolute power with a measure of the in-band noise power under quiescent conditions. Account is taken of natural variations in in-band power due to satellite geometry and solar activity. Once it is determined what spoofing power ratio (the ratio of spoofing signal power to authentic signal power) is required to reliably capture a receiver's tracking loops, the increase in absolute in-band power during a spoofing attack can be estimated. To avoid frequent false alarms, a J/N-type jamming detector triggers only if the measured J/N ratio exceeds a threshold above which natural variations only rarely push the J/N measurement. In [7] it is estimated that such a trigger would be insensitive to civil GPS spoofing attacks up to a spoofing power ratio of 3, where the spoofing power ratio is defined as

$$\eta = \frac{P_{spoof}}{P_{auth}} \tag{3.1}$$

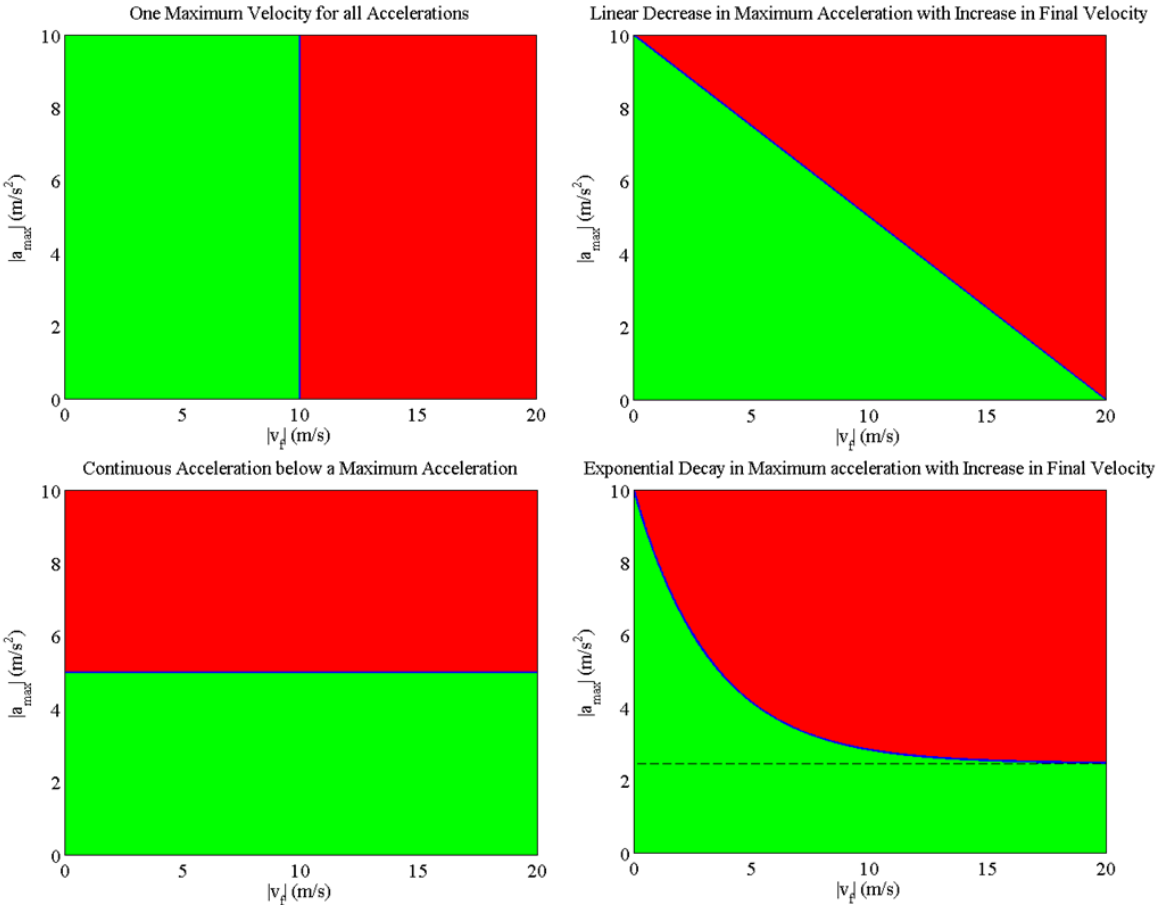

Figure 3.1: These are plots of four potential shapes of maximum acceleration-velocity curves for the dynamics that can be induced by a spoofer. The green area represents the region where a spoofer can safely operate, and the red area represents the region where a spoofer will likely be caught.

with P_{spoof} being the power of each spoofing signal and P_{auth} being the power of the authentic signal. The question that needs to be answered through testing is then: What power ratio is required for reliable spoofing?

Chapter 4

Procedure

The four receivers tested in these experiments were:

science receiver: The CASES receiver developed by the UT Radionavigation Lab in collaboration with Cornell University and ASTRA.

telecommunications network time reference receiver: The HP 58503B, which is commonly used in cell phone base stations. It has a highly stable Ovenized Crystal Oscillator (OCXO) steered by the GPS time solution.

power grid time reference receiver: This receiver provides the time signal for most power grid Synchrophasor Measurement Units (SMUs). It has a low stability oscillator (most likely a Temperature Controlled Crystal Oscillator (TCXO) or simple Crystal Oscillator (XO)) slaved to the GPS time solution.

name brand receiver: The Trimble Juno SB.

Pictures of three of these these receivers are shown in Figure 4.1. These receivers are meant to be a representative cross-section of civil GPS receivers.

These tests were performed in a controlled signal environment with a set of six GPS L1 C/A signals generated by a National Instruments Radio Frequency Signal Generator (RFSG) at a constant power level. Limiting the signals to a set of six GPS L1 C/A signals at constant power greatly simplified the tests without any sacrifice to the results. These signals were tracked by the spoofer, which produced a set of six corresponding spoofed signals. The spoofed signals were then summed with the RFSG signals. This combination of spoofed and RFSG signals was fed into both the

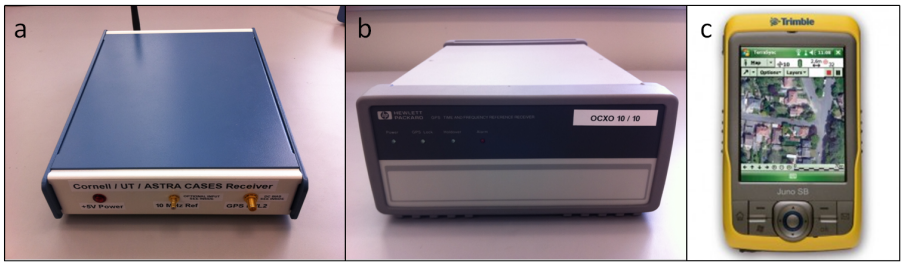

Figure 4.1: Three of the tested receivers a) CASES receiver, b) HP 58503B, and c) Trimble Juno SB

target receiver and a National Instruments Radio Frequency Signal Analyzer (RFSA). The RFSA was used for visualization of the spoofing attack and measurement of the signal power. Figure 4.2 shows the described test setup.

4.1 Power Ratio Test

The power ratio test was performed by first setting the digital attenuator on the spoofer's RF back-end so that the spoofed signals are slightly stronger than the authentic signals with the signals still aligned. Then, the spoofer attempted to capture the target receiver by moving the spoofed signals forward in time at a rate of $1m/s$. This rate corresponds to $\frac{10}{3}ns/s$ in units of time via the following equation

$$v_{m/s} = cv_{s/s} \tag{4.1}$$

where c is the speed of light (about $3E8m/s$). Once the spoofed signal's correlation peak had completely separated from the authentic signal's correlation peak ($2\mu s$ off), the authentic signals were removed. The target receiver's output was then observed to see if any signals were lost. If no signals were lost, then the spoofing attack was successful in capturing the receiver. The authentic signals were then reinserted and the power of each signal was measured using the RFSA. After recording the results, this process was repeated a number of times. The attenuator setting was modified as needed to find a power ratio limit above which a spoofer could

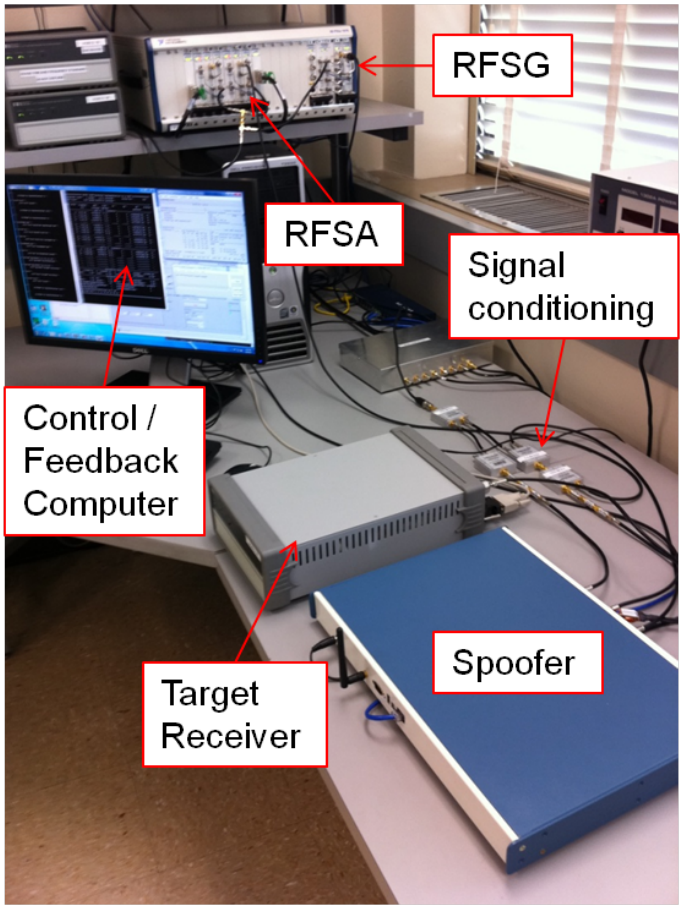

Figure 4.2: The experimental setup

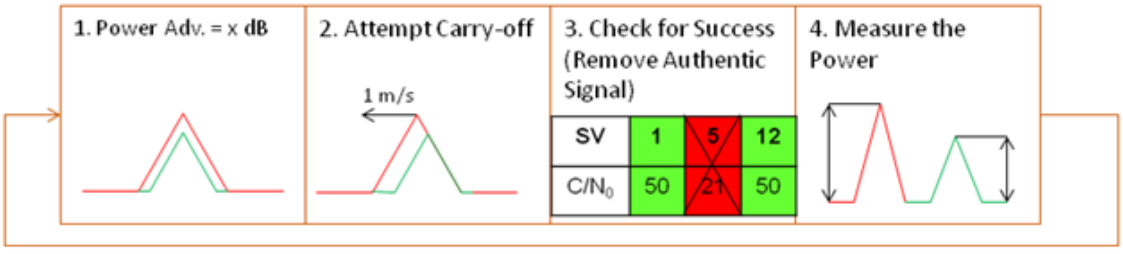

Figure 4.3: Graphical representation of the procedure for the power ratio test

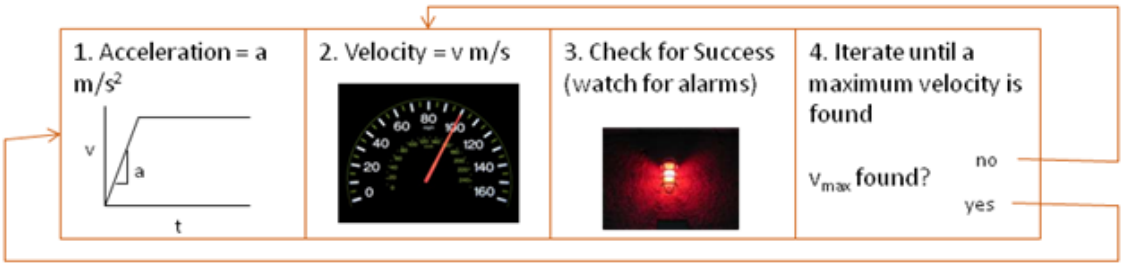

Figure 4.4: Graphical representation of the procedure for the spoofed velocity and acceleration test

consistently capture the target receiver. This procedure is summarized in a graphical format in Figure 4.3.

4.2 Spoofed Acceleration and Velocity Test

The spoofed acceleration and velocity test was performed with only the spoofing signals as input to the target receiver to simulate the behavior of the receiver after it has been captured. This way there was no need to worry about interference with the authentic signals during these tests. First, an acceleration was set for the spoofer. Next, a final velocity was chosen for the spoofer to reach. The output from the target receiver was observed for any alarms or loss of lock on any satellites until the receiver stabilized at the final velocity. If any evidence of the spoofing attack was evident, then the spoofing attack was deemed unsuccessful. This process was repeated while modifying the final spoofed velocity until a maximum spoofed velocity was determined for that acceleration. Once this maximum velocity was found, the spoofed acceleration was modified and the process repeated until 5 or 6 data points were collected. This procedure is summarized in a graphical format in Figure 4.4.

Chapter 5

Results and Implications

5.1 Spoofing Power Ratio Test

The power ratio test results are summarized with the histogram shown in Figure 5.1. This histogram shows the number of successful and failed spoofing attacks for the range of power ratios tested.

As can be seen from Figure 5.1, it is definitely possible to successfully spoof a target receiver at a power ratio below 3. In fact, a power ratio of around 1.1 is all that is required to spoof with a high probability of success, which keeps the absolute in band power well below the natural variations due to solar activity. This means that a J/N-type jamming detector would not typically detect a spoofing attack.

However, a J/N-type jamming detector is still an important component in spoofing detection schemes. One such scheme, coined the Vestigial Signal Defense (VSD) [1], involves detecting the vestige of the authentic signal and distinguishing it from a multipath signal, which can only be done if the authentic signal has not been drowned out or nulled by the spoofer. Nulling the authentic signal is inherently difficult since it requires precise anti-alignment of the phase of a spoofed replica signal with the authentic signal. This makes drowning out the authentic signal the more likely attack scenario. A J/N type jamming detector would corner the spoofer to operating below a power ratio of 3, effectively eliminating the possibility of the spoofer suppressing the authentic signal with excessive spoofing power.

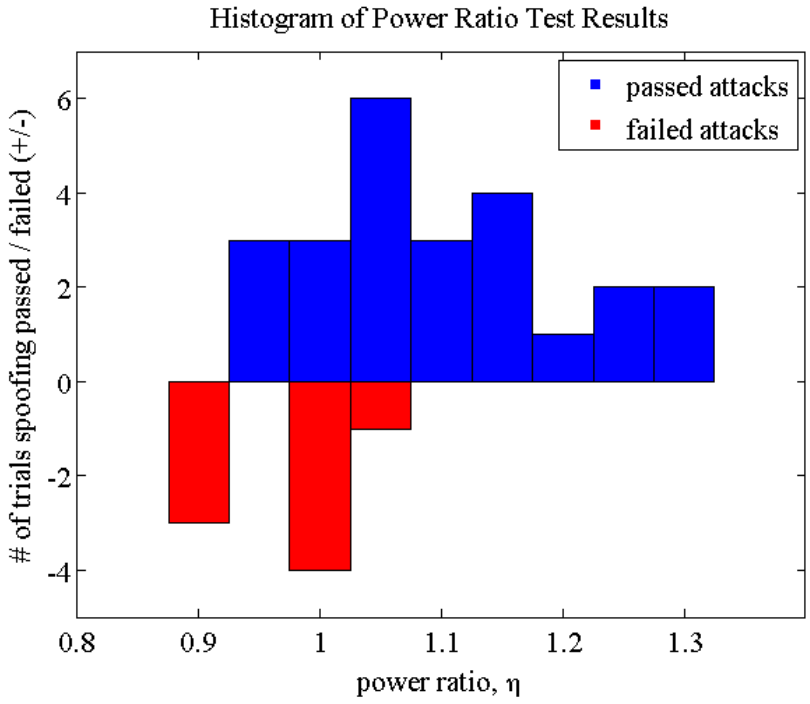

Figure 5.1: Histogram of the spoofing power ratio test results

5.2 Spoofed Velocity and Acceleration Test

The velocity and acceleration data points collected for each of the four tested receivers were fit to a single curve for each receiver of the form

$$|a_{max}| = f(v_f) = \beta_1 e^{\beta_2 |v_f|} + \beta_3 \tag{5.1}$$

where v_f is the final velocity of the spoofer, a_{max} is the maximum acceleration the spoofer can use to reach the final velocity without being caught, and β_1, β_2, and β_3 are fit parameters. An exponential model was chosen for this data based on intuition and the testing results themselves. This model is meant to represent the capability of the receiver's discrete tracking loops to remain locked to the GPS signal under the spoofer imposed dynamics. It defines the upper bound of a region of the acceleration-velocity plane in which the spoofer can safely operate. Knowledge of this curve for a particular receiver allows one to assess the security implications of a

Table 5.1: Raw data for the science receiver

acceleration m/s^2	velocity m/s
8.8	2.2
7	4.6
6	6.4
5.5	8
5	1300

Table 5.2: Fit parameters for the science receiver

β_1	β_2	β_3
7.55	0.3	4.94

spoofing attack on a system that incorporates that receiver.

5.2.1 Science Receiver (CASES)

The raw velocity and acceleration data points for the science receiver are given in Table 5.1. This data was fit to Equation 5.1 and plotted along with the curve fit in Figure 5.2. The resulting values for the fit parameters are also listed in Table 5.2.

The first interesting feature to note in Figure 5.2 is that there is a horizontal asymptote at an acceleration of about $5m/s^2$. This suggests that the science receiver can be accelerated continuously at accelerations below $5m/s^2$. The only limit to the velocity that can be induced in the science receiver is due to the doppler range of the correlators. Outside this range, the correlators are unable to produce local replicas at the appropriate frequency resulting in a loss of satellite lock. This doppler range is set to $\pm 10,000Hz$ because the receiver is meant to be stationary. The maximum attainable velocity is thus dependent on the exact satellite geometry, but is generally around $1,300m/s$. At around this speed, the receiver starts being unable to track some satellites due to the large doppler.

Another interesting note about this receiver's response to induced dynamics

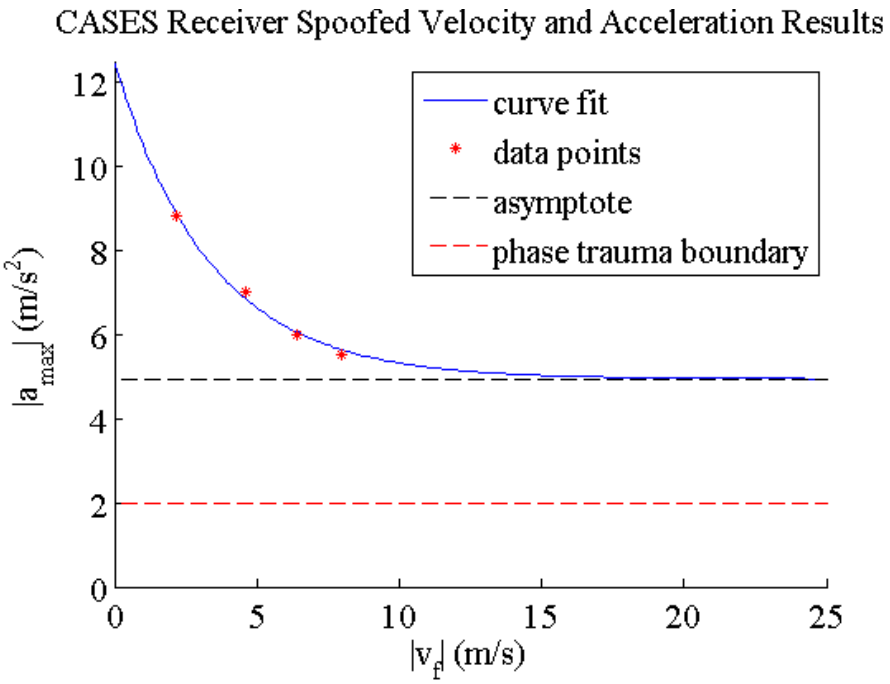

Figure 5.2: Spoofed velocity and acceleration curve fit for the science receiver

is that above accelerations of about $2m/s^2$ the receiver indicates a constant state of phase trauma during acceleration. Phase trauma indicates that the receiver's Phase Lock Loop (PLL) may be experiencing cycle slips. This is a special feature of the science receiver that would normally indicate Ionospheric scintillation [8]. However, scintillation does not manifest itself in this way over long periods of time. Indications of constant phase trauma over any more than a second or two could be considered as an alarm that something is wrong with the receiver. This effectively limits a spoofer that is trying to influence the navigation solution of the science receiver to accelerations below $2m/s^2$. Although in this sense it adds an extra layer of protection to the science receiver, it also creates vulnerability in another sense. If a spoofer wished to reek havoc on the science data from the receiver, then it could capture the receiver and force phase trauma indications on command by imparting small instantaneous velocity changes.

Table 5.3: Raw data for the telecommunications network time reference receiver

acceleration m/s^2	velocity m/s
5.8	1.45
5	1.7
4.5	1.8
4	1.9
2	2
1	2

Table 5.4: Fit parameters for the telecommunications network time reference receiver

β_1	β_2	β_3
38.02	1.33e-1	-25.53

5.2.2 Telecommunications Network Time Reference Receiver (HP)

The raw velocity and acceleration data points for the telecommunications network time reference receiver are given in Table 5.3. This data was fit to Equation 5.1 and plotted along with the curve fit in Figure 5.3. The resulting values for the fit parameters are also listed in Table 5.4.

As can be seen from a comparison of Figure 5.2 and Figure 5.3, the HP receiver is much more resistant to dynamics than the science receiver. The maximum velocity that could be successfully induced in the telecommunications network time reference receiver was $2m/s$. This resistance to spoofer induced dynamics is due to the trust that the HP receiver places in its highly stable oscillator. The receiver was designed such that its oscillator's time output is only loosely coupled to the GPS time solution. The oscillator is slowly steered into alignment with the GPS time solution. The receiver is also capable of entering a "holdover" mode. It enters this mode if the difference between the GPS time solution and the receiver's oscillator is greater than $1\mu s$. This feature acts as an alarm to indicate that GPS should no longer be trusted. It is this feature that causes the deviation from the curve fit in Figure 5.3. There is simply no spoofer acceleration that will allow the HP receiver to stabilize at a speed

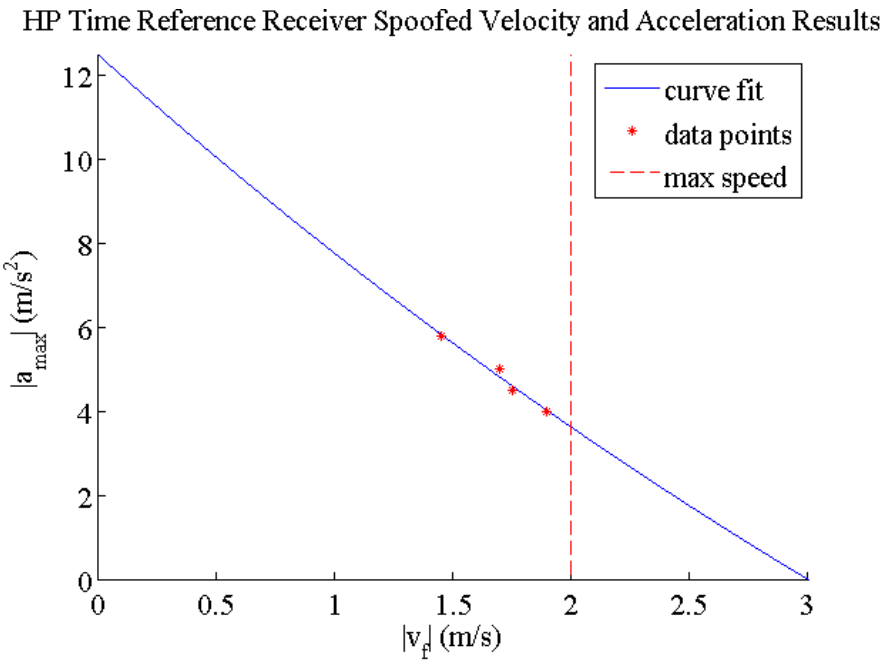

Figure 5.3: Spoofed velocity and acceleration curve fit for the telecommunications network time reference receiver

greater than $2m/s$ before entering holdover mode.

5.2.2.1 Implications for Cellular CDMA Communications Networks

Although the HP receiver provides a high resistance to imposed dynamics, it can still be led off far enough in time to cause some harmful effects on CDMA cell phone networks that typically use this receiver. A $10\mu s$ time offset can still be imparted in around 35 minutes, including time for receiver capture. At this time offset the dependent cell phone tower becomes an "island tower", unable to transfer calls to and from adjacent towers [4]. At larger time offsets, approaching $60\mu s$, the tower's signal could begin to jam signals from neighboring towers, causing a significant disruption in the network.

Time offsets might also wreak havoc on other uses of the cell phone network, such as E911-style localization [9]. E911 or Enhanced 911 is a system that uses Time Difference Of Arrival (TDOA) techniques to locate cell phone users who dial 911 in

Table 5.5: Raw data for the power grid time reference receiver

acceleration m/s^2	velocity m/s
10	2.5
8	75
7	120
5	190
3	360
2	400
1	400

Table 5.6: Fit parameters for the power grid time reference receiver

β_1	β_2	β_3
10.48	3.3e-3	-0.31

emergency situations.

5.2.3 Power Grid Time Reference Receiver

The raw velocity and acceleration data points for the power grid time reference receiver are given in Table 5.5. This data was fit to Equation 5.1 and plotted along with the curve fit in Figure 5.4. The resulting values for the fit parameters are also listed in Table 5.6.

As can be seen in Figure 5.4, the power grid time reference receiver can be manipulated fairly well by a spoofer. A secondary x-axis was added to the figure to represent the corresponding phase angle rate that could be induced in a $60Hz$ phasor being measured using the receiver's time output. This conversion was performed using the following equation

$$\frac{d\theta}{dt} = 360f\frac{v_{m/s}}{c} \tag{5.2}$$

where $\frac{d\theta}{dt}$ is the phase angle rate and f is the frequency of the measured phasor

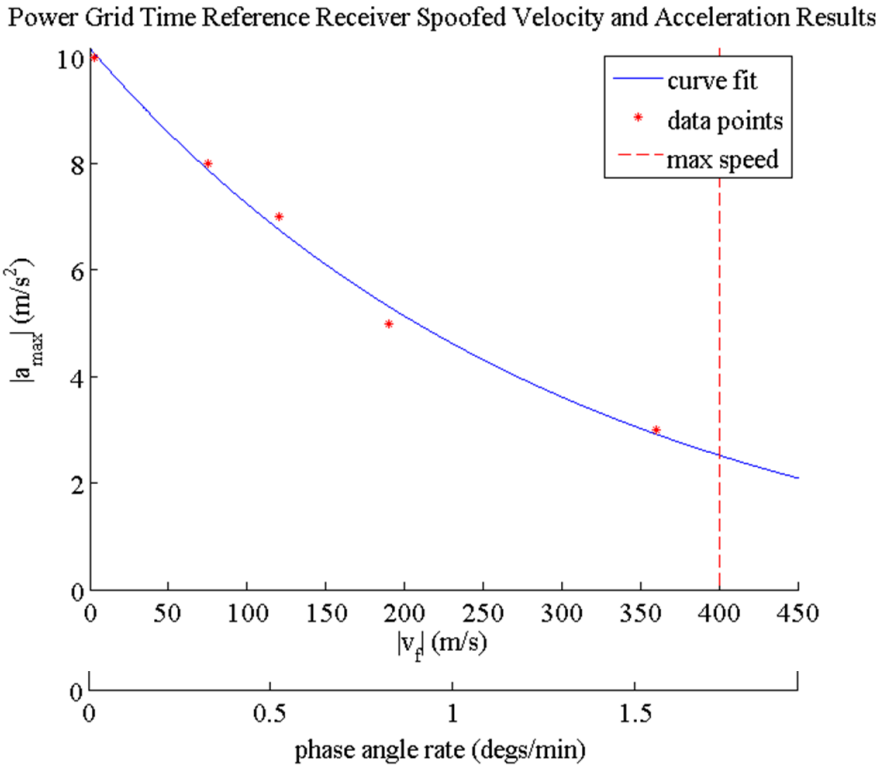

Figure 5.4: Spoofed velocity and acceleration curve fit for the power grid time reference receiver with secondary x-axis corresponding to the induced phase angle rate for a $60Hz$ phasor (such as the voltage phasor for the power grid)

($60Hz$). This receiver is commonly used to time stamp measurements from Synchrophasor Measurement Units (SMUs). SMUs are a proposed smart grid technology to make real time measurements of the voltage phasor (a $60Hz$ phasor) for stability analysis and power flow estimation of the power grid for control purposes. These results show that the power grid time reference receiver can reach a maximum speed of $400m/s$, which corresponds to a $1.73^o/min$ phase angle rate for a voltage phasor on the power grid. It is not entirely clear why the test results deviate from the curve fit at low accelerations.

5.2.3.1 Implications for Power Grid Monitoring and Control

One of the most important uses of SMUs for the smart grid is real time state estimation. It has been suggested that SMUs are necessary to provide accurate, real-time estimates of the state of the power grid so that power margins can be reduced to make the grid more efficient [5]. Spoofing poses a risk to state estimation because a change in the voltage phase angle difference between two locations in the grid directly relates to a change in the estimated power flow between those locations. Alteration of the voltage phase angle at a particular location by even 10^o could suggest to an operator or automatic control logic that an incorrect or unnecessary control action needs to be taken. A spurious 10^o phase deviation can be imposed by the spoofer in a matter of minutes.

One might think that such an alteration of the phase angle would always be viewed as abnormal by an operator, but as it turns out wind power leaves behind a similar signature over the same time scale. This can be seen clearly thanks to a proof of concept network set up by Dr. Mack Grady on the Texas power grid [2]. Figure 5.5 shows the variation of wind power generation in west Texas on March 10, 2009. There is a large spike and a subsequent drop in wind power generation during the 11:00pm to midnight hour. The SMU data, shown in Figure 5.6, reveals a corresponding rise in the phase angle difference between Austin and west Texas. The grid operator looking at SMU measurements would not be able to tell the difference between a spike in

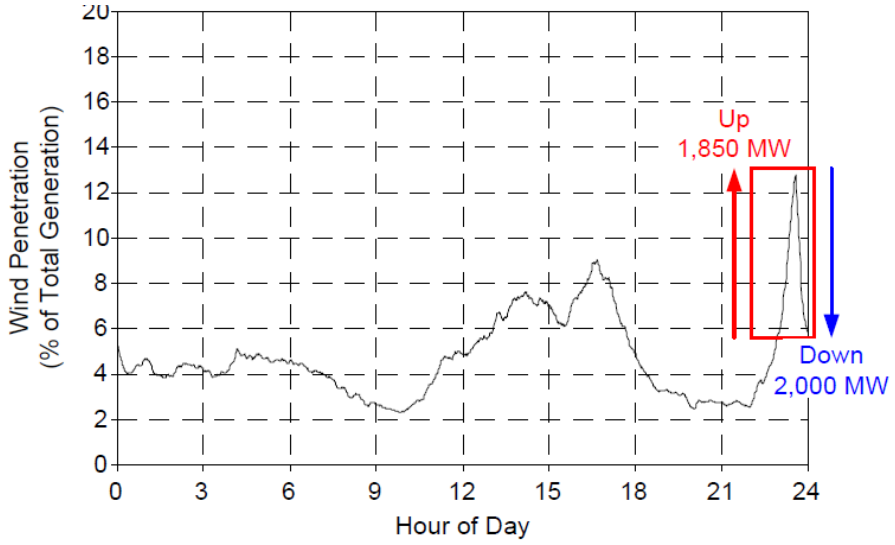

Figure 5.5: Texas wind generation on March 10, 2009 [2]

wind generation and a spoofing attack without the benefit of direct measurements of the wind power production. This suggests that current power flow meters, if retained and monitored, could provide a cross-check for SMU power flow estimates that could not be affected by a spoofer.

Another important application of SMUs is to determine the stability of the power grid. Unstable, low frequency oscillations in the measured phase angles can damage power generators if no corrective action is taken. These low frequency oscillations occur due to increases and decreases of the load on the power grid with the amplitude of the oscillations scaling with the magnitude of the load. Most often these oscillations are damped by the power system stabilizers on the generators, but larger disturbances can be difficult for these stabilizers to handle on their own and the damping could become negative. The oscillations of concern are of magnitudes greater than several tenths of a degree and frequencies between $0.1Hz$ and $0.8Hz$ [2].

Oscillations on the power grid are modeled as the superposition of multiple second order systems. The frequencies and damping coefficients of these oscillations are estimated using a modified version of the Prony Method [10]. The Prony Method

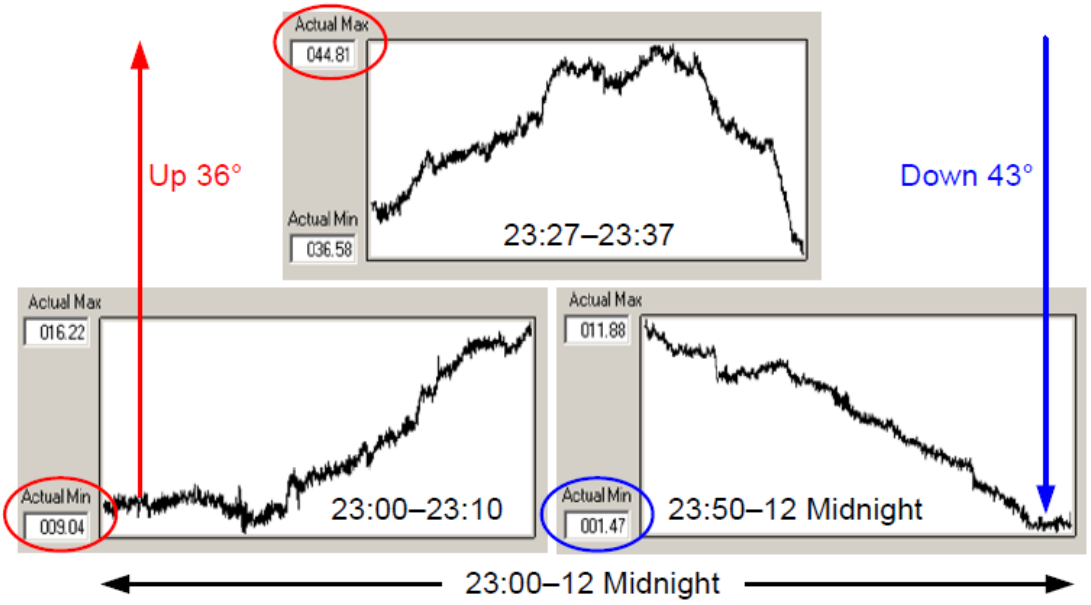

Figure 5.6: SMU measured voltage phase angle difference between Austin and west Texas during wind generation spike on March 10, 2009 [2]

is a close cousin of the Fourier Transform that works on discrete data points taken from a moving window; the data points are modeled as a linear combination of damped sinusoids and fit to a function of the form

$$f[mt_s + t_0] = \sum_{i=1}^{n} \frac{1}{2} A_i e^{(\sigma_i \pm j(\lambda_i(mt_s+t_0)+\phi_i))} \tag{5.3}$$

where m is the sample number, t_s is the sampling interval, t_0 is the start of the window, $f[mt_s + t_0]$ is the sample, n is the number of damped sinusoids used for the fit, and A_i, σ_i, λ_i, and ϕ_i are the amplitude, damping coefficient, frequency, and phase angle of the ith damped sinusoid.

Figure 5.7 shows a plot of the observed damping ratios on the Texas power grid calculated using this method over an hour-long period. There is a large cluster of points, indicating a persistent mode of the system, at $0.7Hz$ and a $2Hz$ cluster that appears due to high wind power generation [2]. There are also a number of high amplitude oscillations, indicated by red dots, that appear occasionally during this

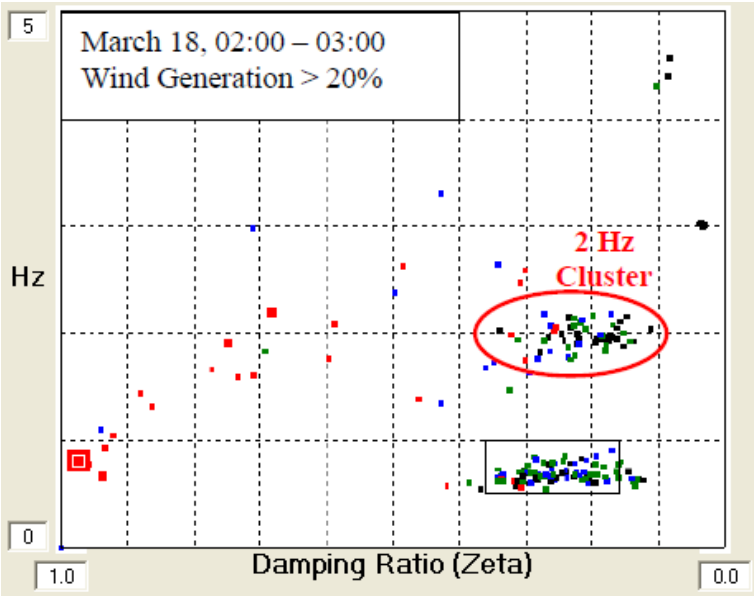

Figure 5.7: Example of SMU calculated damping ratios and frequencies over an hour long period. The color of the dots indicate the magnitude of the oscillation with the largest 25% marked red, the second 25% marked blue, the third 25% marked green, and the lowest 25% marked black. In this case, the red are several degrees in magnitude and all others are less than a degree [2].

time frame. These points have a large damping ratio, likely due to the power system stabilizers, and quickly die off.

Based on these tests, it seems impossible for a spoofer to cause oscillations in the PMU measurements of sufficient magnitude at an appropriate frequency to affect power grid stability estimates. This is largely due to the low acceleration capability of the spoofer. An oscillation at $0.1Hz$ with an amplitude of 0.1^o would require a maximum acceleration of about $550m/s^2$ and a maximum velocity of about $900m/s$. These values are far beyond the admissible dynamics indicated in Figure 5.4.

5.2.4 Name Brand Receiver (Trimble)

The raw velocity and acceleration data points for the name brand receiver are given in Table 5.7. This data was fit to Equation 5.1 and plotted along with the

Table 5.7: Raw data for the name brand receiver

acceleration m/s^2	velocity m/s
49.2	12.3
35	15.7
30	19.5
27	23
25	190
24.5	1300

Table 5.8: Fit parameters for the name brand receiver

β_1	β_2	β_3
444.16	0.24	24.92

curve fit in Figure 5.8. The resulting values for the fit parameters are also listed in Table 5.8.

From comparisons of Figure 5.8 with the plots for the other receivers, the Trimble is by far the most easily manipulated receiver of those tested. There is a horizontal asymptote at around $25m/s^2$, which suggests that the Trimble can be accelerated continuously at accelerations below $25m/s^2$. As with the science receiver, the only limit to the velocity that can be induced is due to the doppler range of the correlators. This doppler range appears to be about $\pm 10,000Hz$, which is the same as the science receiver. This doppler range limits the maximum attainable velocity to somewhere around $1,300m/s$, since after this speed some satellites will begin to exceed this doppler range. These results suggest that many name brand receivers, especially any Trimble receiver, could be wildly manipulated by a spoofer.

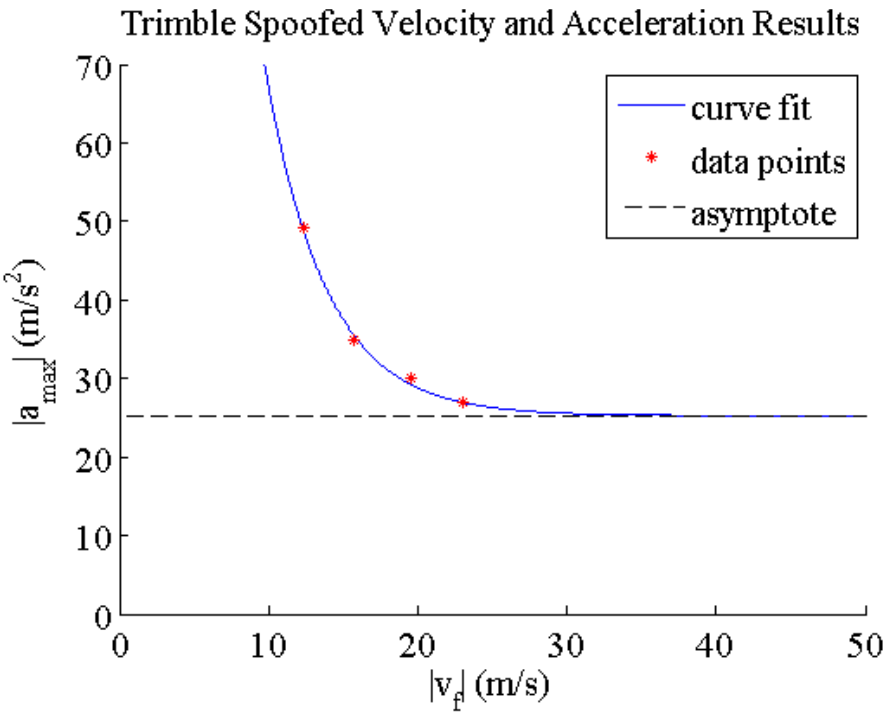

Figure 5.8: Spoofed velocity and acceleration curve fit for the name brand receiver

Chapter 6

Conclusions

Results of tests designed to characterize the response of a civil GPS receiver to a spoofing attack indicate that a J/N-type jamming detector is insufficient to catch a spoofer. The ratio of spoofed signal power to authentic signal power required to consistently capture a target receiver is only about 1.1. This increase in J/N would typically be ignored by a jamming detector because it is within the natural variation in J/N caused by changing satellite geometry and by solar activity [7]. However, J/N type jamming detectors are essential components in many potential spoofing defenses, including the Vestigial Signal Defense (VSD), since they limit the amount of power a spoofer can safely transmit.

Investigations into the dynamics that a spoofer can induce in a target receiver yielded results that varied drastically between the four tested receivers. An empirical curve fit of maximum attainable velocity for different accelerations based on an exponential model was produced for each receiver. These curves define the upper bound of a region of the acceleration-velocity plane in which the spoofer can operate without triggering alarms in the target receiver. These empirical formulas can be used to assess the vulnerability of critical infrastructures utilizing these receivers.

The science receiver results showed that there is no limit to the velocity a spoofer can induce in the receiver until the Doppler range of the correlators is exceeded at around $1,300 m/s$. However, the acceleration was severely limited due to the science receiver's constant indication of phase trauma during accelerations above $2 m/s^2$. This type of visibility into the receiver's tracking loops provides a huge advantage towards limiting a spoofer's capability of dynamically manipulating a receiver.

The telecommunications network time reference receiver was by far the most difficult receiver to manipulate, with a maximum attainable velocity for any acceleration being only $2m/s$. This receiver's inherent resistance to spoofing is due to the receiver placing trust in its oscillator and only slowly steering it towards the GPS time solution. However, the receiver can still be slowly steered away from GPS time: a $10\mu s$ departure can be forced in around $35min$, including time for capturing the receiver. This time offset is enough to degrade the throughput of a CDMA cell phone network. Furthermore, it appears possible to use a network of spoofers to cause multiple neighboring towers to interfere with one another, since CDMA cell phone towers all use the same spreading code and distinguish themselves only by the phasing (i.e., time offset) of their spreading codes.

The power grid time reference receiver was fairly easily manipulated, with a maximum attainable velocity of $400m/s$, but it could only track single-digit accelerations. This receiver is typically used as the time reference for Synchrophasor Measurement Units (SMUs), which measure voltage phasors on the power grid. SMUs are a proposed smart grid technology that will provide real-time stability analysis and power flow state estimation. A spoofer could easily cause large variations in the power flow estimates from SMU data by altering the receiver's time stamp, which in turn changes the voltage phase angle suggesting a change in the power flow. The maximum attainable phase angle rate from these tests was $1.73^o/min$. These changes in power flow measurements could cause a grid operator or automatic control logic to take corrective actions based on falsified data potentially resulting in damage to the power grid. Current power flow meters could provide a valuable cross-check against the SMU derived power flow estimates that is not susceptible to a spoofing attack. In order to affect the stability measures, a spoofer would be required to falsify unstable, low-frequency oscillations in the phase measurements. Based on the test results, it appears that a spoofer is incapable of producing such oscillations at the appropriate frequencies with sufficient magnitudes.

The name-brand receiver was by far the easiest receiver to manipulate, with

continuous acceleration possible at accelerations as high as $25m/s^2$ up until the Doppler range of the correlators is exceeded. This occurs at around the same speed as the science receiver, $1,300m/s$. This suggests that the navigation and timing solution of portable GPS receivers meant to operate under a wide variety of platform dynamics could be wildly manipulated by a spoofer.

Bibliography

[1] T. Humphreys, B. Ledvina, and M. Psiaki, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS Conference*, (Portland, Oregon), Institute of Navigation, sep 2008.

[2] W. M. Grady and D. Castello, "Implementation and application of an independent texas synchrophasor network," tech. rep., Schweitzer Eng. Laboratories, jan 2010.

[3] "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," tech. rep., John A. Volpe National Transportation Systems Center, 2001.

[4] "Recommended minimum performance standards for cdma2000 spread spectrum base stations," tech. rep., 3GPP2, feb 2004.

[5] J. Giri, D. Sun, and R. Avila-Rosales, "Wanted: A more intelligent grid," *IEEE Power & Energy*, pp. pp. 34–40, apr 2009.

[6] Anon., "Icd-gps-200c: Navstar GPS space segment/navigation user interfaces," tech. rep., ARINC Research Corporation, 2003. http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=9364.

[7] T. Humphreys and K. Wesson, "Detection strategy for cryptographic civil GNSS anti-spoofing," 2011. to appear.

[8] T. E. Humphreys, M. L. Psiaki, P. M. Kitner, and B. M. Ledvina, "GPS carrier tracking loop performance in the presence of ionospheric scintillations," in *Proceedings of the ION GNSS Conference*, (Long Beach, California), Institute of Navigation, sep 2005.

[9] P. Kuykendall and P. V. W. Loomis, "In sync with GPS: GPS clocks for the wireless infrastructure," tech. rep., Trimble Navigation.

[10] E. Schweitzer, D. Whitehead, and A. Guzman, "Advanced real-time synchrophasor applications," tech. rep., Schweitzer Eng. Laboratories, sep 2008.

[11] G. Benmouyal, E. Schweitzer, and A. Guzman, "Synchronized phasor measurement in protective relays for protection, control, and analysis of electric power systems," tech. rep., Schweitzer Eng. Laboratories, sep 2002.

[12] A. G. Phadke, B. Pickett, and M. Adamiak, "Synchronized sampling and phasor measurements for relaying and control," *IEEE Trans. Power Delivery*, vol. 9, pp. pp. 442–452, jan 1994.