Civilian GPS Jammer Signal Tracking and Geolocation

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

Jahshan A. Bhatti
University of Texas, Austin, TX

BIOGRAPHIES

Ryan H. Mitch is pursuing a Ph.D. 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, nonlinear estimation and filtering, and GNSS integrity.

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, applications, and integrity, spacecraft attitude and orbit determination, and general estimation, filtering, and detection.

Brady W. O'Hanlon is a Ph.D. candidate in the School of Electrical and Computer Engineering at Cornell University. He received both his M.S. and 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.

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.

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

ABSTRACT

This paper investigates the simulation, Kalman Filter tracking, and Kalman Filter geolocation of a chirp–type civilian Global Positioning System (GPS) jammer. The paper is divided into four parts. The first two parts present information on the current generation of GPS jammers and propose a simple method of jammer signal simulation. The third part outlines a method by which a Kalman Filter can track the state of the simulated signal at the output of a simulated radio frequency (RF) front end. The method uses in-phase and quadrature accumulations, accumulation models, and noise models. The paper also considers the computational speed and numerical issues of the proposed system. Results are presented for the Kalman Filter signal tracker on data from a truth-model simulation. The fourth part outlines a particular implementation of a Time Difference of Arrival (TDOA) jammer geolocation system and its associated state and measurements. A method of Time–of–Arrival measurement formulation which reduces the required communication bandwidth between different TDOA stations is also presented. A jammer TDOA data collection campaign at White Sands Missile Range in June of 2012 is detailed. Results of the proposed TDOA jammer geolocation system on two sets of real data are compared to Inertial Navigation

Preprint from ION GNSS 2012

System (INS) position estimates.

INTRODUCTION

The Global Positioning System and other Global Navigation Satellite Systems (GNSS) have found a wide variety of uses in civilian life. They are heavily used in trucking and shipping [1], aircraft and maritime navigation [2], and for high precision timing applications [3, 4].

Ubiquitous positioning capabilities are sometimes considered a threat to some individuals operating outside of the boundaries of the law. The threat of undesired GPS geolocation can be avoided through the use of a civilian GPS jammer, also referred to as a personal privacy device (PPD). A straightforward application of one of these devices would be a car thief preventing recovery of a stolen vehicle by jamming the GPS–enabled theft recovery device. Another potential example would be that of an employee of a trucking company attempting to hide his position from his superiors by jamming the corporation–owned GPS tracker, and then proceeding to do as he wishes while being paid to make deliveries. The case with the most benign intent would be someone who simply wishes to enforce their privacy with a personal privacy device, and prevent themselves from being tracked while in their own vehicle [5].

All of the above scenarios involve jamming or interfering with the GPS or another GNSS. Therefore, GPS jammers have become available for purchase at certain locations around the world and at certain sites on the internet. This has led to a number of incidents. In the so called Newark incident a piece of equipment at Newark airport was periodically jammed by a commuter [2]. There was also an incident in Great Britain where a group of car thieves used GPS jammers [1].

Enforcement of the laws protecting the GPS and GNSS bands requires that the jammers be located and taken away from their operators. This has led to an increased focus by the GNSS community on GPS jammers in general [6, 7, 8] and on their geolocation in specific [9]. This paper will focus on various related aspects of GPS jammer signal processing with the long–term goal of enabling further law enforcement actions by means of jammer geolocation.

The remainder of the paper is divided into five sections. The first section discusses the background of GPS jammers. The second section is on GPS jammer signal simulation. The third is on tracking of the simulated GPS jamming signal using a Kalman Filter. The fourth section focuses on GPS jammer geolocation, specifically using a Kalman Filter and the Time Difference of Arrival geolocation method. The fifth section presents the summary and conclusions.

GPS JAMMER BACKGROUND

Civilian GPS jammers can be found in a variety of form factors, but are on average approximately the size of a hand-held cell phone [7]. Three different civilian GPS jammers are shown in Fig 1. The jammer on the far left in the picture is the lowest power jammer and is powered from an automobile accessory power outlet. The middle one is slightly more powerful, contains a battery, and can be carried around and activated at almost any location and time. The one on the far right is slightly less powerful than the middle one, but it also contains a battery and is disguised to look like a cellular telephone.

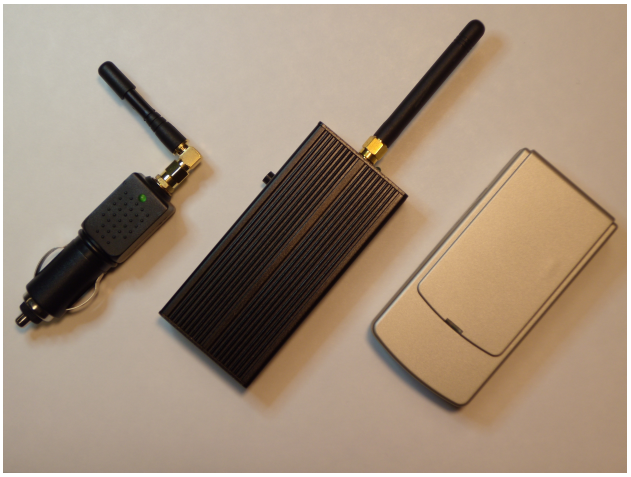

Figure 1 Three different form factors of civilian GPS jammers.

Processing of signals from GPS jammers can benefit from an understanding of the RF output of the jammers. A typical output of a civil GPS jammer is shown in Fig 2. The horizontal axis is time and the top plot's vertical axis is frequency. Each vertical slice of the top plot in the figure is a Fast Fourier Transform (FFT) of the RF sampled signal, centered at the L1 frequency. The bottom plot's vertical axis is power. The figure shows a classic example of a chirp signal, or a tone whose frequency repeatedly ramps linearly upwards and then resets back to the starting frequency.

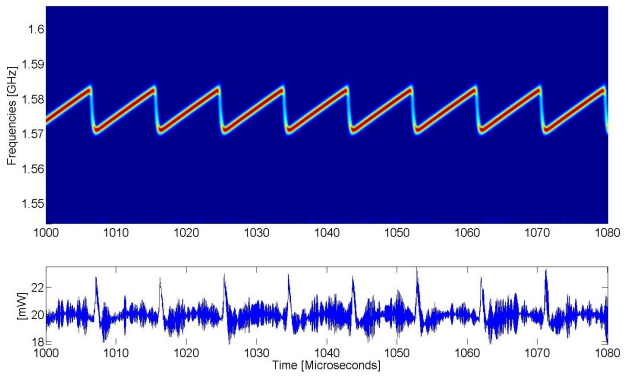

Figure 2 Typical civilian GPS jammer output. The top plot is a surface color contour FFT power spectra, in batches of 64 data points. The bottom plot is of power into the system that digitized the RF signal.

GPS JAMMER SIMULATION

To enable algorithm development and testing, the civilian GPS jamming signal was simulated in software. There are many ways that the GPS jamming signal could be simulated, particularly for jammer signals that differ slightly from that in Fig 2, but only one method is presented. In this method, an idealized chirp signal is assumed, and some parts of its parameterization are shown graphically in Fig 3.

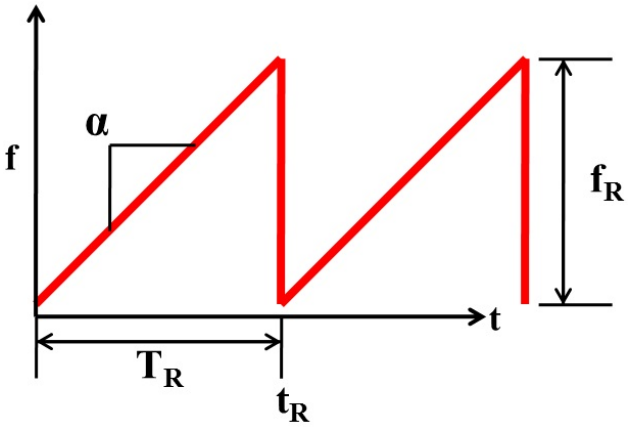

Figure 3 Candidate parameterization of an idealized chirp–type jammer, with important features labeled.

The parameterization assumes that the signal starts at one frequency and linearly ramps upward in time with a slope denoted by α. Once the ramp has progressed at rate α for a time T_R, the jammer reset period, the jammer frequency resets by an amount f_R, the jammer reset frequency amount. This occurs at time t_R, which is incremented by T_R to define each new reset.

The parameterization in Fig 3 leads to the following state vector in Eq 1.

$$\underline{x} = \begin{bmatrix} \phi \\ f \\ \alpha \\ A \\ f_R \\ t_R \\ T_R \end{bmatrix} \tag{1}$$

where the first four states (ϕ, f, α, A) evolve continuously over time. They are the phase, frequency, frequency rate of change, and the amplitude. Their respective units are cycles, Hertz, Hertz/sec, and Volts. The last three states (f_R, t_R, T_R) act on the system at discrete times (t_R), and have units of Hertz, seconds, and seconds, respectively. The combination of these continuous and discrete states creates a hybrid system formulation of a GPS jammer signal.

The previously described signal state can be used to generate a signal history. The state can be initialized to a starting value and then propagated forward in time by using its dynamics:

$$x_{k+1} = \Phi^J\left(t_{k+1}, t_k; x_k\right) x_k \tag{2}$$

where the term $\Phi^J\left(t_{k+1}, t_k; x_k\right)$ is the general state transition matrix that takes the state from time t_k and propagates it forward to time t_{k+1}. $\Phi^J\left(t_{k+1}, t_k; x_k\right)$ is a product of two types of terms:

$$\Phi_1^J\left(t_b, t_a\right) = \begin{bmatrix} 1 & \Delta t & 0.5\Delta t^2 & 0 & 0 & 0 & 0 \\ 0 & 1 & \Delta t & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{3}$$

$$\Phi_2^J = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4}$$

where Δt is the defined as $t_b - t_a$.

$\Phi_1^J\left(t_b, t_a\right)$ is the state transition matrix for the linear portion of the frequency ramp from time t_a to t_b assuming that there is no reset over that time period, and Φ_2^J is the state transition matrix for the instantaneous time of reset.

As an example, if a single reset were to occur during the interval from t_k to t_{k+1} then the propagation of the

state would take the form in the first line; otherwise it takes the form in the second line:

$$\begin{aligned} x_{k+1} &= \Phi_1^J\left(t_{k+1}, t_R\right)\Phi_2^J\Phi_1^J\left(t_R, t_k\right)\underline{x}_k \\ x_{k+1} &= \Phi_1^J\left(t_{k+1}, t_k\right)\underline{x}_k \end{aligned} \tag{5}$$

Process noise has also been added in an attempt to improve the fidelity of the simulation. The process noise influence matrix Γ_k is shown below:

$$\Gamma_k = \begin{bmatrix} \frac{\Delta t^3}{6} & 0 & 0 & 0 \\ \frac{\Delta t^2}{2} & 0 & 0 & 0 \\ \Delta t & 0 & 0 & 0 \\ 0 & \Delta t & 0 & 0 \\ 0 & 0 & \Delta t & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \Delta t \end{bmatrix} \tag{6}$$

where continuous-time phase noise is allowed to enter only through the α and f_R states, and additional noise has been added to the A and T_R states.

The full state dynamics are shown below:

$$\underline{x}_{k+1} = \Phi^J\left(t_{k+1}, t_k; x_k\right)\underline{x}_k + \Gamma_k\underline{w}_k \tag{7}$$

where the vector $\underline{w}_k$ is the process noise vector. In this study's simulation, the process noise vector is zero–mean, white, Gaussian noise that has been scaled by the user–specified standard deviations. In an actual system, this vector may have different statistical behavior.

The jammer state is used to generate a simulated RF signal. This RF signal is assumed to be the output of the GPS jammer, immediately upon leaving the jammer antenna. The signal simulation is accomplished by passing the phase state history through a cosine function and then multiplying the result by the jammer amplitude state A:

$$y_k = A_k cos(2\pi\phi_k) \tag{8}$$

White, Gaussian, measurement noise v_k with a user–specified standard deviation has been added to create a more realistic simulation of a jammer's output signal:

$$y_k = A_k cos(2\pi\phi_k) + v_k \tag{9}$$

The simulated signal y_k can be used as the input to tracking and localization algorithms.

KALMAN FILTER TRACKING OF A GPS JAMMER

Accurate tracking of a civil GPS jammer is useful for a number of purposes, specifically for developing measurements for geolocation algorithms. This study recommends the use of a Kalman Filter for signal tracking for three reasons. The filter has the ability to track signals through significant noise, it can be programmed to run with a low computational burden, and the resulting estimated states have a high degree of accuracy and would be optimal if the true system corresponded to the filter stochastic model.

The reader is assumed to have moderate knowledge of Kalman Filtering techniques, and the derivation of the Kalman Filter is not required here. Readers interested in gaining a further understanding of Kalman Filters are referred to the extensive body of literature on the subject, with a number of references provided by way of example, [10, 11, 12]. Furthermore, the reader is assumed to have an understanding of how Kalman Filters can be used to track RF signals, specifically GPS signals as in references [13, 14].

This section will present its Kalman Filter formulation in seven subsections. The first subsection will discuss the Kalman Filter state and its dynamics. The second subsection will present the derivation of the measurements provided to the Kalman Filter, the in-phase and quadrature accumulations. The third subsection will derive an accumulation measurement model for the Kalman Filter. The fourth subsection will cover the way in which measurement noise enters the system. The fifth subsection will discuss Kalman Filter architecture selection and numerical considerations. The sixth subsection will detail a simple Kalman Filter state initialization procedure. The final subsection will present results of the Kalman Filter using data from a jammer truth-model simulation.

Kalman Filter State and Dynamics

The Kalman Filter state and dynamics are the same as that used in the jammer simulation presented in the previous section. Explicitly, the state is given in Eq 1, and the state transition matrices are given in Eqs 3 and 4, and the process noise is given in Eq 6. The full state dynamics are shown in Eq 7.

Kalman Filter Measurements: Accumulations

The Kalman Filter measurements must be synthesized in a causal manner from raw digitized data fed in from

the RF front end. The Kalman Filter derivation presented in this paper uses a model of the signal after it has passed through the ADC. It is assumed that signal amplitude has been halved due to the IF mixing.

The jamming signal input to the RF front end after digitization at the ADC is the following:

$$y_i^J = \frac{A_k}{2} cos\left(2\pi\left[\phi_k^J + f_k^J \Delta t_i + \alpha_k^J \frac{\Delta t_i^2}{2} - f_{mix} t_i\right]\right) + v_i \tag{10}$$

where ϕ_k^J, f_k^J, α_k^J, and A_k are the first four entries of the jammer state at time t_k. The term f_{mix} is the mixing frequency that brings the signal to IF, and is in units of Hertz. v_i is zero–mean, white, Gaussian noise, and is in units of volts. The output time t_i is assumed to lie between time t_k and t_{k+1}, but before a reset occurs. It can be expressed in equations as follows:

$$t_i \in [t_k, t_{k+1}], \ < t_{R,k} \tag{11}$$

$$\Delta t_i = (t_i - t_k) \tag{12}$$

Technically, Eq 10 should also contain a term that considers the process noise shown in Eq 7, but this effect is beyond the scope of the current study.

If a reset does occur in the interval of $[t_k, t_{k+1}]$, violating the assumption of Eq 11, then a consistent form of y_i^J from Eq 10 can be maintained by redefining two states to account for the reset:

$$f_k^J = \begin{cases} f_k^J, & \text{if } t_i \in [t_k, t_{R,k}) \\ f_k^J + f_{R,k}^J, & \text{if } t_i \in [t_{R,k}, t_{k+1}] \end{cases}$$
$$\phi_k^J = \begin{cases} \phi_k^J, & \text{if } t_i \in [t_k, t_{R,k}) \\ \phi_k^J - f_{R,k}^J (t_{R,k} - t_k), & \text{if } t_i \in [t_{R,k}, t_{k+1}] \end{cases} \tag{13}$$

The jammer signal at the RF front end output, y_i^J, is used to form in-phase (I) and quadrature (Q) accumulations according to the following recipes:

$$I_k = \sum_{i=1}^{N} y_i^J cos\left(\phi_i^N\right) \tag{14}$$

$$Q_k = \sum_{i=1}^{N} y_i^J sin\left(\phi_i^N\right) \tag{15}$$

where the term ϕ_i^N is the phase at time t_i that is generated by the numerically controlled oscillator (NCO). The superscript N denotes that this is the NCO phase. These accumulations constitute the measurements that are used by the Kalman Filter.

Accumulations will contain significant power if the NCO frequency time history is close to that of the actual jamming signal frequency. A good selection of NCO phase history is the one that would be generated by the Kalman Filter's estimate of the jamming signals state.

It should be emphasized that a causal system will require that the NCO be fed the (k-2)th state to compute the kth accumulation. This requirement exists because the system must accumulate I and Q values over one accumulation period (T_{accum}) and then perform the Kalman Filter calculations over the next accumulation period, before the new state can be fed back to the NCO. Fortunately, the state at time t_{k-2} can be propagated with the dynamics model up to time t_k, to maximize accumulation power. If the state estimate is poor, then the forward propagation could potentially make the accumulation results worse. This forward propagation step is not required when tracking the GPS signal because the GPS signal dynamics are slow and benign in most applications.

The accumulations in Eqs 14 and 15 are the sums of the products of two trigonometric terms over an accumulation period, and are therefore nonlinear equations. As a result of this nonlinearity, there is only a small region of states whose corresponding phase histories will generate any power in the accumulations. If the state estimate is too far away from the true states then the accumulations will have insufficient power for tracking purposes, and will appear to be random noise. This nonlinear effect is known as the measurement's pull-in range.

One solution to the pull-in problem that still preserves the traditional RF signal tracking architecture of the Kalman Filter is to generate multiple accumulations by feeding a variety of states to the NCOs. There is no theoretical limit to this approach, but there are practical limits such as computation time and complexity.

The multiple accumulation approach is used to improve the filter's pull-in range with respect to errors in the estimate of the jammer's t_R state, which can be difficult to estimate. Therefore, this paper recommends that two pairs of accumulations be calculated at each Kalman Filter measurement update. The first (I,Q) pair will be referred to as Type A, and the second will be referred to as Type B. These two accumulations will create a larger pull-in region for the estimation of the t_R state.

The central concepts of accumulation Types A and B

are shown graphically in Fig 4 for a full accumulation period, where one accumulation period T_{accum} is assumed to be much less than one reset period T_R.

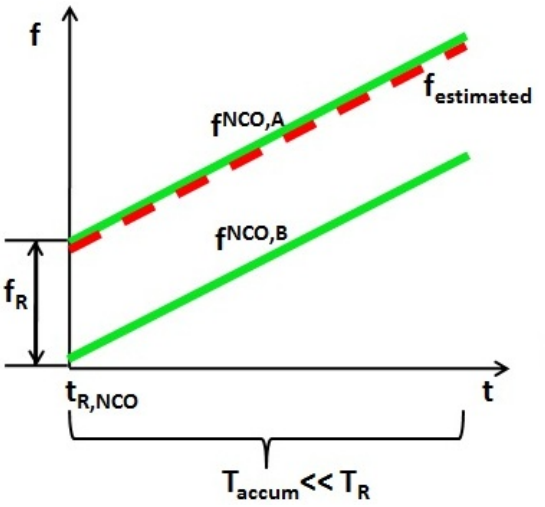

Figure 4 Frequencies generated by the NCOs for accumulation Types A and B. The Kalman Filter's estimate of the jammer frequency is the red dashed line and the NCO frequencies are the solid green lines.

Accumulation Type A would be considered the classical implementation of a Kalman Filter tracking an RF signal. The NCO generates exactly the phase history predicted by the current state estimate, with no modifications to the jammer frequency state. Accumulation Type A will have significant power if the state estimate, in particular the reset time t_R and reset amount f_R, are close to the real jammer states. The primary feature of accumulation Type B is that the frequency state fed into the NCO is assumed to reset by an amount f_R at the very beginning of the accumulation interval, denoted time $t_{R,NCO}$ in Fig 4. Accumulation Type B will have significant power if the jammer frequency state resets at the beginning of the accumulation interval.

The two accumulation types were designed so that Type A will have all of the power and Type B will have none of the power if the reset time is correctly predicted. If the reset time is erroneously predicted to occur outside of the accumulation interval when it actually occurs near the beginning then Type A will have no power and Type B will have significant power, assuming that the remainder of the jammer state estimate is within the pull-in range of the actual jammer state. If the reset time occurs in the middle of an accumulation interval then both types will have power, where the amount of power in each will be a function of the time duration for which they have the correct frequency.

The resulting Kalman Filter measurements for accumulation period k are:

$$z_k = \begin{bmatrix} I_A \\ Q_A \\ I_B \\ Q_B \end{bmatrix}_k = \begin{bmatrix} \sum_{i=1}^{N} y_i^J cos\left(\phi_i^N\right) \\ \sum_{i=1}^{N} y_i^J sin\left(\phi_i^N\right) \\ \sum_{i=1}^{N} y_i^J cos\left(\phi_i^N + f_R^N \Delta t_i\right) \\ \sum_{i=1}^{N} y_i^J sin\left(\phi_i^N + f_R^N \Delta t_i\right) \end{bmatrix}_k \tag{16}$$

Kalman Filter Measurement Model

Kalman Filter tracking requires a model of how the states affect the measurements provided to the filter. The current system uses accumulations as its measurements, and will therefore require a model of how the accumulations depend on the state. This section will only consider accumulation Type A, but calculation of Type B is straightforward and simply requires another frequency term. Manipulation of the accumulation's recipes of Eqs 14 and 15 will be required to reach the final accumulation measurement models.

The first step is to rewrite Eqs 14 and 15 to include the time per sample T_s:

$$I_k = \frac{1}{T_s} \sum_{i=1}^{N} y_i^J cos\left(\phi_i^N\right) T_s \tag{17}$$

$$Q_k = \frac{1}{T_s} \sum_{i=1}^{N} y_i^J sin\left(\phi_i^N\right) T_s \tag{18}$$

The above equations can be viewed as discrete approximations to continuous integrals. Conversion to continuous integration yields the following two equations:

$$I_k \quad \cong \quad \frac{1}{T_s} \int_{t_k}^{t_k + NTs} y^J(t_i) cos\left(\phi^N(t_i)\right) dt_i \tag{19}$$

$$Q_k \quad \cong \quad \frac{1}{T_s} \int_{t_k}^{t_k + NTs} y^J(t_i) sin\left(\phi^N(t_i)\right) dt_i \tag{20}$$

The next step is to substitute the modeled state and known NCO phase time history into Eqs 19 and 20, by replacing $y^J(t_i)$ and $\phi^N(t_i)$ with the following formulas:

$$y^J(t_i) = \frac{A_k}{2} cos\left(2\pi \left[\phi_k^J + f_k^J \Delta t_i + \alpha_k^J \frac{\Delta t_i^2}{2} - f_{mix} t_i\right]\right) \tag{21}$$

$$\phi^N(t_i) = \left(2\pi \left[\phi_k^N + f_k^N \Delta t_i + \alpha_k^N \frac{\Delta t_i^2}{2} - f_{mix} t_i\right]\right) \tag{22}$$

where Eq 21 is the noiseless input at the RF front end, similar to Eq 10, and Eq 22 is the NCO phase history over the accumulation interval.

The Kalman Filter accumulation measurement models are the following:

$$I_k \cong \frac{A_k}{2T_s}\int_0^{NT_s} cos\left(2\pi\left[\phi_k^J + f_k^J t + \alpha_k^J\frac{t^2}{2} - f_{mix}(t+t_k)\right]\right) cos\left(2\pi\left[\phi_k^N + f_k^N t + \alpha_k^N\frac{t^2}{2} - f_{mix}(t+t_k)\right]\right)dt \tag{23}$$

$$Q_k \cong \frac{A_k}{2T_s}\int_0^{NT_s} cos\left(2\pi\left[\phi_k^J + f_k^J t + \alpha_k^J\frac{t^2}{2} - f_{mix}(t+t_k)\right]\right) sin\left(2\pi\left[\phi_k^N + f_k^N t + \alpha_k^N\frac{t^2}{2} - f_{mix}(t+t_k)\right]\right)dt \tag{24}$$

where a change of dummy integration variables has been performed to switch from t_i to t. The change of variables results in the Δt terms changing to t and the bounds of integration changing from $[t_k, t_{k+1}]$ to $[0, NTs]$.

Typically, in GPS tracking the above equations are further modified with the following trigonometric identities:

$$\begin{aligned} cos(a)*cos(b) &= \frac{1}{2}\left[cos(a-b)+cos(a+b)\right] \\ cos(a)*sin(b) &= \frac{1}{2}\left[-sin(a-b)+sin(a+b)\right] \end{aligned} \tag{25}$$

and result in the following equations:

$$I_k \cong \frac{A_k}{4T_s}\int_0^{NT_s}\left[cos\left(2\pi\left[\Delta\phi + \Delta f t + \Delta\alpha\frac{t^2}{2}\right]\right) + cos\left(2\pi\left[\sum\phi + \sum f t + \sum\alpha\frac{t^2}{2} - 2f_{mix}(t+t_k)\right]\right)\right]dt \tag{26}$$

$$Q_k \cong \frac{A_k}{4T_s}\int_0^{NT_s}\left[-sin\left(2\pi\left[\Delta\phi + \Delta f t + \Delta\alpha\frac{t^2}{2}\right]\right) + sin\left(2\pi\left[\sum\phi + \sum f t + \sum\alpha\frac{t^2}{2} - 2f_{mix}(t+t_k)\right]\right)\right]dt \tag{27}$$

where the terms with Δ and Σ are defined as:

$$\begin{aligned} \Delta* &= *_k^J - *_k^N \\ \Sigma* &= *_k^J + *_k^N \end{aligned} \tag{28}$$

The trigonometric functions containing the Σ terms in Eqs 26 and 27 are then typically ignored. They are ignored because they have a large effective frequency when compared to integration time, which causes the integration of that term to be effectively zero. That is *not* always the case in the current system. GPS integration times tend to be the length of one Coarse/Acquisition code, or 1 ms, but this system will use accumulations that are approximately three orders of magnitude shorter, or 1 μs. In addition to the lower accumulation times, the frequency resets could cause issues if the IF is not chosen correctly.

Ideally, the models in Eqs 26 and 27 could be reduced to a more compact version, such as the sinc function used in GPS, but that is not possible in the current system. The difficulty arises from the t^2 entries in the trigonometric identities. The integration of a trigonometric term that contains a quadratic variable results in a Fresnel integral, which has no closed form solution and must be approximated numerically or with a series expansion. As a result, Eqs 26 and 27 are considered to be the final form of the accumulation measurement models.

Measurement Model Speed Considerations

The measurement models presented in Eqs 26 and 27 can be manipulated to save computational effort by avoiding numerical integration and instead using a Taylor Series expansion. Equations 26 and 27 will be further expanded using another trigonometric identity to isolate the t^2 terms.

$$\begin{aligned} cos(u \pm v) &= cos(u)cos(v) \mp sin(u)sin(v) \\ sin(u \pm v) &= sin(u)cos(v) \pm cos(u)sin(v) \end{aligned} \tag{29}$$

To simplify notation the following substitutions are made:

$$\begin{aligned} a_d &= 2\pi\Delta\phi \\ b_d &= 2\pi\Delta f \\ c_d &= \pi\Delta\alpha \\ a_s &= 2\pi\left(\sum\phi - 2f_{mix}t_k\right) \\ b_s &= 2\pi\left(\sum f - 2f_{mix}\right) \\ c_s &= \pi\sum\alpha \end{aligned} \tag{30}$$

Application of Eqs 29 and 30 to Eqs 26 and 27 result in the following equations:

$$\begin{aligned} I_k \cong \frac{A_k}{4T_s}\int_0^{NT_s} &\left[cos\left(a_d + b_d t\right) cos\left(c_d t^2\right) - \right. \\ &sin\left(a_d + b_d t\right) sin\left(c_d t^2\right) + \\ &cos\left(a_s + b_s t\right) cos\left(c_s t^2\right) - \\ &\left. sin\left(a_s + b_s t\right) sin\left(c_s t^2\right)\right] dt \end{aligned} \tag{31}$$

$$\begin{aligned} Q_k \cong \frac{A_k}{4T_s}\int_0^{NT_s} &\left[-sin\left(a_d + b_d t\right) cos\left(c_d t^2\right) - \right. \\ &cos\left(a_d + b_d t\right) sin\left(c_d t^2\right) + \\ &sin\left(a_s + b_s t\right) cos\left(c_s t^2\right) + \\ &\left. cos\left(a_s + b_s t\right) sin\left(c_s t^2\right)\right] dt \end{aligned} \tag{32}$$

The trigonometric functions containing t^2 terms can now be replaced with their Taylor Series expansions. The results avoid evaluation of the Fresnel integral, and can be integrated in a term–by–term manner:

$$\begin{aligned} I_k \cong \frac{A_k}{4T_s}\int_0^{NT_s} &\left[cos\left(a_d + b_d t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\left(c_d t^2\right)^{2n} - \right. \\ &sin\left(a_d + b_d t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left(c_d t^2\right)^{2n+1} + \\ &cos\left(a_s + b_s t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\left(c_s t^2\right)^{2n} - \\ &\left. sin\left(a_s + b_s t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left(c_s t^2\right)^{2n+1}\right] dt \end{aligned} \tag{33}$$

$$\begin{aligned} Q_k \cong \frac{A_k}{4T_s}\int_0^{NT_s} &\left[-sin\left(a_d + b_d t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\left(c_d t^2\right)^{2n} - \right. \\ &cos\left(a_d + b_d t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left(c_d t^2\right)^{2n+1} + \\ &sin\left(a_s + b_s t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\left(c_s t^2\right)^{2n} + \\ &\left. cos\left(a_s + b_s t\right)\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}\left(c_s t^2\right)^{2n+1}\right] dt \end{aligned} \tag{34}$$

Evaluation of Eqs 33 and 34 preserves the numerical accuracy of all of the components in Eqs 23 and 24 except for those contained in c_d and c_s. Theoretically, the Taylor Series can be evaluated with as many terms as required. Practically, there are numerical limitations to the number of terms that could be used in the series.

The final speed increase of the above series expansion is significant. A three term expansion running in MATLAB on an i7 processor was able to realize greater than one order of magnitude time reduction in the execution speed of the measurement model, when compared to a tightly toleranced Gaussian quadrature integration method.

Measurement Noise

A measurement noise model is required for Kalman Filter signal tracking. Actual measurement noise is assumed to enter the system only through the v_k term in Eq 9. There will be additional significant error due to the small number of samples used in each accumulation measurement, which are only approximations of the continuous integrals in Eqs 23 and 24, and the process noise term that was ignored in Eq 10.

The accumulations of Eqs 14 and 15 are rewritten below to specifically include the effects of noise:

$$I_k = \sum_{i=1}^{N}\left(\frac{A_i}{2}cos(2\pi\phi_i) + v_i\right) cos\left(\phi_i^N\right) \tag{35}$$

$$Q_k = \sum_{i=1}^{N}\left(\frac{A_i}{2}cos(2\pi\phi_i) + v_i\right) sin\left(\phi_i^N\right) \tag{36}$$

Equations 35 and 36 can be rewritten to separate the signal part accumulations (I_{sig}, Q_{sig}) and the noise part accumulations:

$$\begin{aligned} I_k &= \sum_{i=1}^{N}\frac{A_i}{2}cos(2\pi\phi_i)cos\left(\phi_i^N\right) + \sum_{i=1}^{N}v_i cos\left(\phi_i^N\right) \\ &= I_{sig} + v_I \end{aligned} \tag{37}$$

$$Q_k = \sum_{i=1}^{N} \frac{A_i}{2} i cos(2\pi\phi_i) sin\left(\phi_i^N\right) + \sum_{i=1}^{N} v_i sin\left(\phi_i^N\right) = Q_{sig} + v_Q \tag{38}$$

The noise accumulation terms are rewritten in vector forms:

$$v_I = \sum_{i=1}^{N} v_i cos\left(\phi_i^N\right) = \underline{v}^T * cos\left(\underline{\phi}^N\right) \tag{39}$$

$$v_Q = \sum_{i=1}^{N} v_i sin\left(\phi_i^N\right) = \underline{v}^T * sin\left(\underline{\phi}^N\right) \tag{40}$$

where $\underline{v}$ is an N-by-1 column vector of noise values over an accumulation and $\underline{\phi}^N$ is an N-by-1 column vector of the complete NCO phase history over an accumulation period.

The Kalman Filter in this study uses four measurements from two different accumulation types, Type A and Type B. The measurement noise vectors for both accumulation types are stacked into one vector below:

$$\underline{v}_h = \begin{pmatrix} v_{I,A} \\ v_{Q,A} \\ v_{I,B} \\ v_{Q,B} \end{pmatrix} = \begin{pmatrix} \underline{v}^T * cos\left(\underline{\phi}_A^N\right) \\ \underline{v}^T * sin\left(\underline{\phi}_A^N\right) \\ \underline{v}^T * cos\left(\underline{\phi}_B^N\right) \\ \underline{v}^T * sin\left(\underline{\phi}_B^N\right) \end{pmatrix} = \begin{pmatrix} C_A^T \\ S_A^T \\ C_B^T \\ S_B^T \end{pmatrix} \underline{v} \tag{41}$$

where $\underline{v}_h$ is a 4-by-1 column vector of accumulation noises. C_A and C_B are N-by-1 column vectors of the cosine of the NCO phase histories for accumulation types A and B, respectively. Similarly, the S_A and S_B terms are the sine values of the NCO phase histories for accumulation types A and B. The superscript ^{T} indicates a matrix or vector transpose.

The accumulation measurement noise covariance matrix is defined using $\underline{v}_h$ as follows:

$$\begin{aligned} R &= E\left[\underline{v}_h \underline{v}_h^T\right] \\ &= E\left[\begin{pmatrix} C_A^T \\ S_A^T \\ C_B^T \\ S_B^T \end{pmatrix} \underline{v}\underline{v}^T \begin{pmatrix} C_A & S_A & C_B & S_B \end{pmatrix}\right] \\ &= \sigma_v^2 \left[\begin{pmatrix} C_A^T \\ S_A^T \\ C_B^T \\ S_B^T \end{pmatrix} \begin{pmatrix} C_A & S_A & C_B & S_B \end{pmatrix}\right] \\ &= \sigma_v^2 \begin{bmatrix} C_A^T C_A & C_A^T S_A & C_A^T C_B & C_A^T S_B \\ & S_A^T S_A & S_A^T C_B & S_A^T S_B \\ & & C_B^T C_B & C_B^T S_B \\ & & & S_B^T S_B \end{bmatrix} \end{aligned} \tag{42}$$

where $E[*]$ indicates the expected value of the quantity enclosed in the square brackets, and σ_v is the standard deviation of v_i, the zero–mean, white, Gaussian noise.

Kalman Filter Architecture and Numerical Considerations

In nonlinear systems appropriate selection of the type of Kalman Filter to be implemented is important. The classical filter is the linear Kalman Filter, but there are a wide variety of filters and filter modifications that have been created to handle issues that can arise in real systems. For instance, an Unscented Kalman Filter is appropriate for systems where it is difficult to calculate the partial derivatives, and a particle filter is useful for systems that are extremely nonlinear. This study started with a simple linear Kalman Filter and added modifications as necessary.

The first modification enables handling of the nonlinearities that arise in the measurement model. The linear Kalman Filter was changed to an Extended Kalman Filter (EKF), which effectively linearizes the dynamics and measurement equations about the estimated state using a Taylor Series Expansion.

The second modification is meant to improve handling of the nonlinearities in the measurement model. The entries in the system's measurement sensitivity matrix, the partial derivatives of each measurement with respect to the state, are highly dependent on the current state estimate. That dependence causes significant changes in the measurement sensitivity matrix over even small state changes, and can cause issues in a standard EKF. This study added an iteration routine to the standard EKF, creating an Iterated Extended Kalman Filters (IEKF). The iteration routine allows multiple relinearizations of the partial derivatives at each measurement update step, and enforces a nonlinear residuals cost improvement in the overall update. A reader interested in IEKFs is encouraged to read reference [15].

The third and final modification is meant to handle the severe numerical issues present in this system. The numerical issues arise from the drastically different numerical scales of the states involved. The α state might have units with order of magnitude equal to 10^{12} [Hz/s], while the T_R state might have units on the order of 10^{-6} [sec]. These two states can cover a numerical magnitude range equal to 10^{18}. In simulations running in MATLAB, the greatest condition number that can be supported, with any significant

digits remaining after matrix inversion, is 10^{16}. Because 10^{18} is two orders of magnitude above 10^{16} there will be no significant numbers left over after matrix inversion, and the algorithm will not produce meaningful results. A modification that can fix this is the use of Matrix Square Root Techniques. The current modification uses a combination of normalization and Cholesky factorization to keep track of smaller numbers. The result after applying the square root information modification is an Iterated Extended Square Root Information Filter (IESRIF). A reader interested in Square Root Information techniques, such as that used in the IESRIF, is encouraged to read [12].

Kalman Filter State Initialization

Convergence of a nonlinear Kalman Filter can only be accomplished if the initial state estimate is within the pull-in range of the system. Because a real system will have no *a priori* knowledge of the jammer state, initialization is accomplished through close examination of a small batch of data containing at least one full reset period. The data is Hamming windowed in a point–by–point manner, and then FFTs are computed. The simulated result for a jamming signal mixed to a 5 MHz IF and with significant measurement noise added is shown in Fig 5.

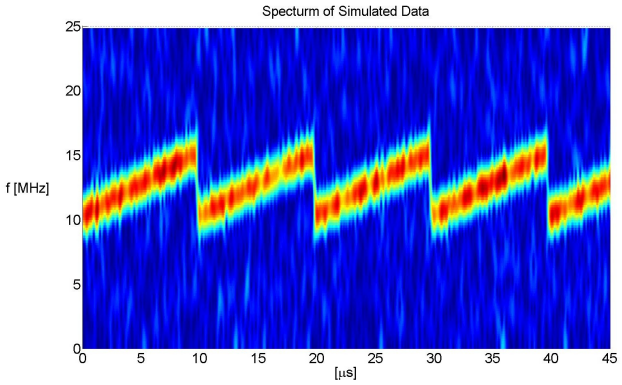

Figure 5 Spectrum of a simulated jamming signal with significant noise at the output of an RF front end.

A coarse initialization procedure that can start the Kalman Filter state within the pull-in range of the system is outlined below.

At the start of the initialization, the phase state ϕ is set to zero. The frequency state f is taken as the maximum powered frequency in an FFT at a given time. The α, T_R, and f_R states are computed using the minimum and maximum frequencies (f_{min}, f_{max}), and the time of the minimum and maximum frequencies (t_{min}, t_{max}), as shown graphically in Fig 6.

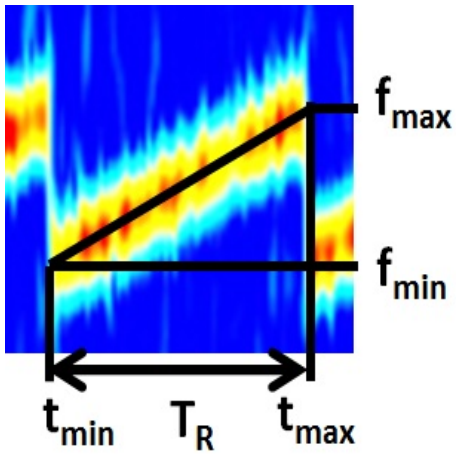

Figure 6 A magnified and brightened portion of Fig 5, marked with important values for Kalman Filter initialization.

The intial values of α, T_R, and f_R are determined from the following simple set of equations:

$$\begin{aligned} f_R &= f_{max} - f_{min} \\ T_R &= t_{max} - t_{min} \\ \alpha &= \frac{f_R}{T_R} \end{aligned} \tag{43}$$

The amplitude state is estimated, and the previously mentioned states refined, using multiple accumulations similar to Eq 14 and 15, but with many different initial state hypotheses. The reset time t_R for the next reset period is determined from further examination of the FFTs surface plot.

Kalman Filter Results On Simulated Data

This section presents results of the proposed Kalman Filter using simulated data.

The performance of the Kalman Filter is dependent on the parameters used in the civil GPS jammer simulation. The parameters used to generate the results in this study are listed in the following paragraph and in Tables 1 and 2. The initial covariance estimates were tuned based on the expected accuracy of the initialization scheme.

The parameterization in this paper causes the process noise on α to move the state only slightly, because in many real jammers the slope does not change much. The amplitude state is allowed to vary only slightly, as

Table 1 States used in the civil GPS jammer simulation. The σ column is the standard deviation of the process noise ($\underline{w}_k$) for each state, in appropriate units.

State	units	Nominal Value	σ
α	Hz/sec	5*10^{11}	5*10^{14}
A	Volts	1	100
f_R	Hz	5*10^{6}	1*10^{11}
T_R	sec	10*10^{-6}	0.1

Table 2 Parameters used in the civil GPS jammer simulation. The σ column is the standard deviation of the measurement noise (v_k), in appropriate units.

Parameter	units	Nominal Value	σ
v_i	Volts	0	0.1
N	N/A	10	N/A
1/Ts	Hz	50*10^{6}	N/A

the whole simulation spans only 200 μs of real time, and the amplitude would likely stay relatively constant over this time in a real jammer. The process noise standard deviation on state f_R is increased above what is typically seen in GPS jammers. The rationale for the noise intensity increase on the f_R state is to test the performance of the Kalman Filter tracker with a more difficult simulation than that which is expected to be encountered in a real system.

There is a trade-off between the noise intensities on the α and f_R states and the ability of the Kalman Filter to track the signal. It appears to be more difficult to track a noisy f_R state than a noisy α state. The reason is that both the noise and the state of f_R act on the measurements in a discrete (instantaneous) manner, as opposed to α which has both the noise and the state act on the measurements in a continuous manner.

The results of a simulation and the Kalman Filter tracking of its outputs are shown for the most interesting 4 states in Figs 7, 8, 9, and 10. The first three figures are for the first three states, ϕ, f, and α, and the fourth figure is for the fifth state, f_R.

The phase tracks accurately, although it contains a bias that is not observable or important. Although not shown, if the phase in Fig 7 is linearly detrended and replotted, the result would be a series of parabolas whose slopes change at the frequency resets.

The states frequency f and frequency rate α are strongly observable. There is a trade-off between the number of samples used in an accumulation and the pull-in of the f and α states. The more samples used in an accumulation the more power the accumulation

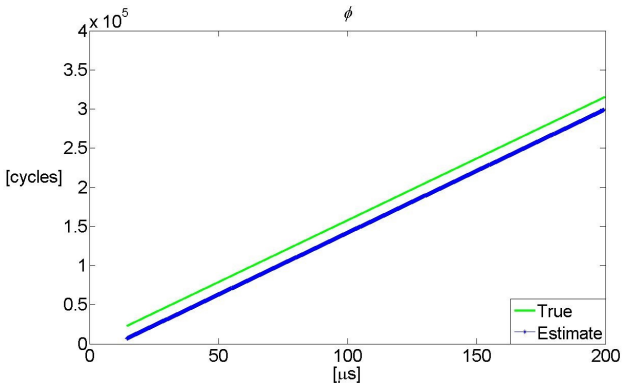

Figure 7 Kalman Filter phase estimate time history ϕ (blue stars) and true simulator phase (green line).

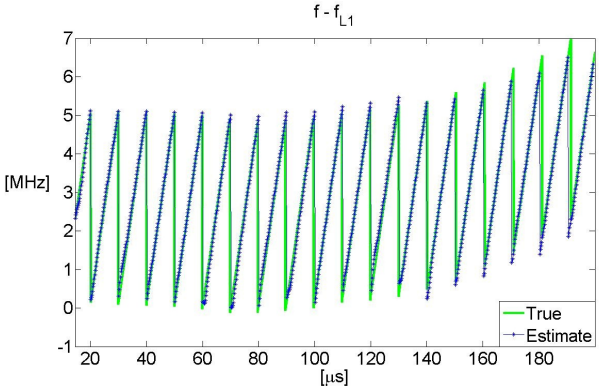

Figure 8 Kalman Filter frequency estimate time history f (blue stars) and true simulator frequency (green line).

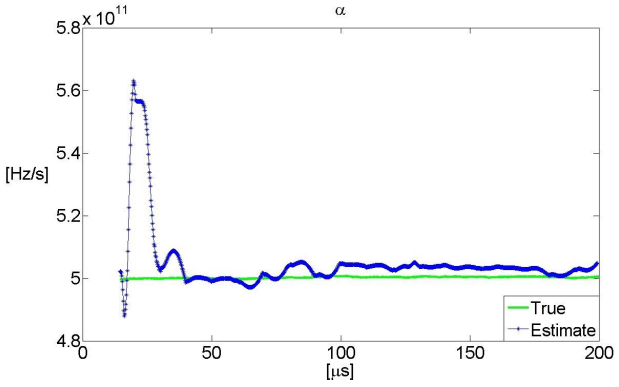

Figure 9 Kalman Filter frequency rate estimate time history α (blue stars) and true simulator frequency rate (green line).

can have. The accumulation loses power if the f, α, and f_R states fed to the NCOs are not close to the jammer states. Therefore, in a system with intense process noise only a few samples should be used in each accumulation. The trade-offs will manifest as an increase in the SNR required to track the noisy jammer, and a decreased Kalman Filter execution speed.

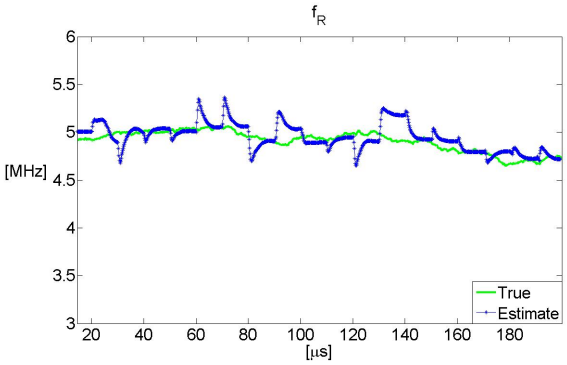

Figure 10 Kalman Filter frequency reset estimate time history f_R (blue stars) and true simulator frequency reset (green line).

The frequency reset state f_R is observable. The current implementation of the filter sometimes has difficulty estimating the state at the reset time, but the filter is able to continue to gain information about that state even after a few accumulations have passed. The likely reason for the added information is that the expected noise intensity on α cannot account for the changes seen in the accumulation measurements, so the effects must be attributed to the f_R state.

Although the simulation results are encouraging, the current GPS jammer simulation and Kalman Filter tracker make a number of assumptions that might be violated in the real world. One of the primary assumptions made in this study is that the frequency state reset is instantaneous, or over no more than one sample. In actual systems, the reset will occupy a finite amount of time, and must be handled accordingly. A second assumption is that the entire spectrum of the jammer is contained in the sampled data, whereas in the real world the jamming frequency may move outside of the Nyquist range of the system. A third assumption is that the process noise is zero–mean, white, Gaussian noise, and that the state behavior is a random walk. Actual GPS jammers would be more accurately modeled by a Gauss-Markov sequence with appropriate reference and standard deviation values. A fourth assumption is that the RF front end has a very precise clock, and its effects can be ignored. A fifth assumption is that there are no environmental effects such as multipath, additional signals, or correlated measurement noise. At least some of the above effects should be addressed before attempts are made to use the proposed Kalman Filter on real data.

KALMAN FILTER JAMMER GEOLOCATION

Accurate geolocation of a civil GPS jammer is useful for numerous reasons, but this study's primary motivation is the further enablement of law enforcement actions. This study uses a Kalman Filter and TDOA measurement model for jammer geolocation.

This section will present its Kalman Filter implementation in seven subsections. The first subsection discusses reasons for selecting the TDOA geolocation method, and the jamming scenarios that this study is concerned with. The second subsection presents the Kalman Filter's state and dynamics, and the third subsection presents the Kalman Filter's measurements. The fourth subsection presents the Kalman Filter's measurement model, and the fifth section discusses the chosen filter architecture and numerical considerations. The sixth and seventh subsections cover data collection and results obtained using that data.

TDOA Geolocation Method

There are numerous methods of geolocating a radiation source, but this study will only use the time difference of arrival method. The existing literature on time difference of arrival techniques is extensive, and a small sampling includes the following references: [16, 17, 18, 19, 20].

The time difference of arrival geolocation method was used instead of numerous other possible techniques, such as direction of arrival (DOA) or power difference of arrival, for three reasons. Firstly, TDOA can be a very accurate technique. Secondly, TDOA can be implemented on general purpose RF equipment. Finally, TDOA can also be implemented efficiently in real time, particularly if the technique is modified so that the method's computational load can be spread among multiple stations and the needed inter-station communication bandwidth kept reasonably low.

Traditional TDOA systems start their measurement formulation by communicating measurement RF data streams from multiple stations to one central station. Then the central station computes cross-correlations on the data streams. The peak of each cross correlation function corresponds to a time difference of arrival measurement between the cross correlated stations. The correlations are typically used in lieu of

other methods because very little *a priori* information about the signal of interest is required. This study leverages significant *a priori* information about civil GPS jammers to reduce the communication demands on the receiver array, as well as distribute the computational load among multiple stations.

The type of scenario that this study is primarily concerned with is the geolocation of jammers used in cars or other road–based vehicles. These vehicle–bound jammers are naturally constrained to be on the surface of the earth. This constraint is realized in the form of a fixed altitude on the earth-shaped ellipsoid from the World Geodetic Survey (WGS84). In the current study, the altitude will be assumed to be the average altitude of all of the receivers in the array. In a theoretical situation where a road crossed through the array at a slightly different altitude, that altitude could be used instead of the average altitude of the receivers in the array. If the altitude varies too much over the road, then a topographic map could be used to constrain the solution. In the current study the altitude constraint is enforced in the form of an altitude measurement, with a user–selected measurement noise standard deviation. The standard deviation used in this study was 10 m.

Kalman Filter State and Dynamics

The position of the GPS jammers is estimated using a Kalman Filter–type approach. Note that the new Kalman Filter will be almost completely unrelated to the Kalman Filter presented earlier in this paper. In this study, the following state is estimated at every sample time t_k:

$$\underline{x}_k = \begin{bmatrix} t^B \\ x^J \\ y^J \\ z^J \end{bmatrix}_k \tag{44}$$

where t^B is the time that a particular signal feature is broadcast from the jammer, and the elements x^J, y^J, and z^J are the x, y, and z positions of the jammer in the Earth Centered Earth Fixed (ECEF) coordinate frame at time t_k. The current study used the above state because the batches of measurements covered a small enough amount of time (0.01 sec) that the velocities did not contribute much to the position evolution over a measurement batch. Similar to GPS, the current system is measurement rich and can compute position solutions without the aid of a dynamics model using individual batches of measurements.

If the velocities of the jammer are required, as might be the case in some scenarios when tracking a jammer in a moving car, the state would be the following:

$$\underline{x}_k = \begin{bmatrix} t^B \\ x^J \\ y^J \\ z^J \\ \dot{x}^J \\ \dot{y}^J \\ \dot{z}^J \end{bmatrix}_k \tag{45}$$

where $\dot{x}^J$, $\dot{y}^J$, and $\dot{z}^J$ are the velocities of the jammer in the ECEF coordinate frame.

The state transition matrix for the case without velocity states is:

$$\underline{x}_{k+1} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \underline{x}_k \tag{46}$$

and the state transition matrix with velocity states is:

$$\underline{x}_{k+1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \Delta t & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \Delta t \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \underline{x}_k \tag{47}$$

The top row of the state transition matrix is set to zero because the broadcast time state t^B, and all information associated with it, are dropped and then re-estimated at every measurement update step of the Kalman Filter. This dropping and re-estimating is suboptimal because the jammers have a regular reset period, but it helps maintain the independence of each measurement set.

In the current study, no noise was considered to enter into the state dynamics. This is a valid assumption for two reasons. Firstly, the batches of data used in the position estimation span a small enough time that the effects are negligible. Secondly, the broadcast time t^B is estimated from zero *a priori* information at each measurement interval. A scenario that used velocity states would require a process noise term. Further consideration of the type of process noise that could be used is beyond the scope of this study.

Theoretically, the jammer reset period and reset time can be added as fourth and fifth states. If these states are added, then an estimated broadcast time that is significantly outside of the standard deviations predicted by those states' estimates can be flagged as a measurement error. The measurement would then be ignored by the filter.

Kalman Filter Measurements

The measurements used in this study's Kalman Filter are the following:

$$\underline{z}_k = \begin{bmatrix} t_1 \\ \vdots \\ t_n \\ h_{Avg,receivers} \end{bmatrix} \tag{48}$$

where t_1 through t_n are the time of the jammer signal feature arrival at each of the n stations used in the array, and $h_{Avg,receivers}$ is the average height of the receivers.

The signal feature time of arrival is the time when the jamming signal ramps past a chosen frequency, specifically the L1 frequency, or another frequency close to L1 if the jamming signal does not pass through that frequency. Computation of this crossing time is straightforward and could be accomplished in real time, but it has been accomplished in an after-the-fact manner in this study.

At every station, FFTs are computed sequentially on batches of RF data expected to contain the jamming signal. Figure 11 contains a color-contour plot of 50μs of FFTed data from a chirp–type jammer. Each vertical slice in the plot is a single FFT of 12 Hamming windowed data points. Each slice has been advanced by one point from the preceding slice.

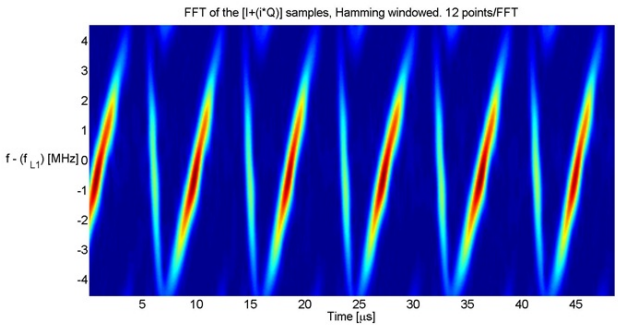

Figure 11 FFT'd data from a GPS jammer with color-contoured signal power plotted versus frequency on the vertical axis and time on the horizontal axis.

In each FFT, only the point with the maximum power is considered further. Additionally, the maximum powered point in every FFT below a certain power threshold is ignored. The power threshold can be determined on the fly. One possibility would be to calculate the maximum power in a batch of FFTs and then set the threshold to some fixed fraction of that peak power. Figure 12 is a plot of the same data used in Fig 11, but now the maximum powered point in each FFT above a threshold has a black dot placed on it.

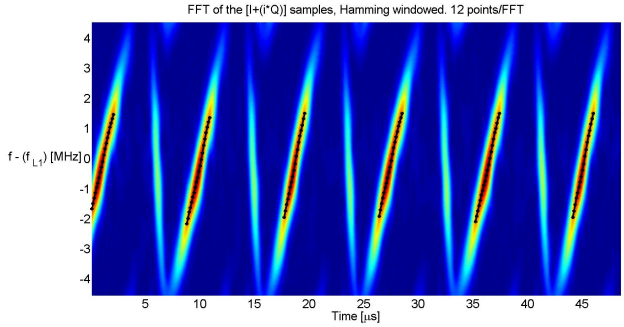

Figure 12 Maximum powered points in each FFT (black dotted line) above a selected power threshold on real jamming data. The points are overlaid on top of the FFTs used in their calculation.

The same points, but without the FFTs underlaid, are shown in Fig 13. The resulting data can be used to solve for the time at which the jamming signal sweeps through L1, the f_{L1} crossing, also shown in Fig 13.

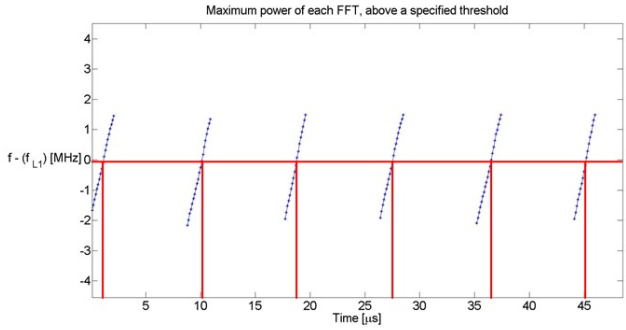

Figure 13 Frequency of maximum power points above a selected power threshold in each FFT (dotted line) versus time. The red horizontal line indicates the L1 frequency, and the red vertical lines are the signal feature times of arrival for the current station.

Two possible methods for calculating the f_{L1} crossing are interpolation or polynomial curve fitting and evaluation at the L1 frequency. One advantage of the polynomial fit is that it can reduce the effects of measurement noise. A method that would provide more optimal noise reduction would be to track the frequency directly, in the sense of the Kalman Filter presented in the third section of this paper.

The time series of f_{L1} crossings that result from the above procedure are the measurements provided to the Kalman Filter.

The measurement series from each of the n stations must be time–aligned for meaningful results. One method would be to use GPS at each station to discipline each receiver's clock and its definition of f_{L1} when the GPS signal is not completely jammed, as is the case when the jammer is at a significant distance from the station of interest. Once the jammer moves close enough to completely prevent GPS signal tracking, the system would then transition to an open–loop synchronization method, assuming that there are no unjammed GNSS bands and no user–specified network timing signal.

Open–loop synchronization would use the clock's current time estimate as a time stamp for every measurement, but it would no longer have time measurement updates from the GPS satellites. During this open–loop synchronization the accuracy of the time stamps and the f_{L1} frequency crossing at each station are functions primarily of two factors, the quality of the clocks at each station and the time that has elapsed since the complete loss of GPS signals. A full analysis of clock affects on TDOA measurements is beyond the scope of this study.

Kalman Filter Measurement Model

The Kalman Filter measurement model for TDOA techniques is simple. The relation between the time of arrival (TOA) measurements and the jammers states is:

$$\rho_i + ct^B = ct_i^R \tag{49}$$

where c is the speed of light in a vacuum, or in this case it could be the speed of light in the atmosphere. The variable ρ_i is the distance between the jammer and receiver i, and is formally defined as:

$$\rho_i = \sqrt{(x_i - x_J)^2 + (y_i - y_J)^2 + (z_i - z_J)^2} \tag{50}$$

Equation 49 is easily understood as a form very close to the classical GPS pseudorange equation. The only difference is that the pseudorange, which equals $c(t_i^R - t^B)$ is not explicitly computed because t^B must be kept separate because it is unknown. This TOA equation will become a TDOA calculation during the Kalman Filter measurement update, which will in effect difference all the equations to isolate the effect of the unknown ct^B term from the unknown ρ_i terms.

Kalman Filter Architecture and Numerical Considerations

The filter used in this study is an IEKF. The iteration routine is required to converge to the correct states because the state t^B must estimated at every time step and the measurement model is nonlinear. This TDOA filter is similar to a batch filter, as it considers no process noise and its dynamics are stationary states, but the system is a Kalman Filter because it updates its state information in sequential measurement updates for each signal feature broadcast time.

To improve the rate of convergence of the iteration routine, the state t^B is initialized to the earliest measurement reception time at each Kalman Filter measurement update step. The resulting speed improvement was not significant when compared to the total execution time of the Kalman Filter.

Data Collection for Kalman Filter Geolocation

Data for jammer geolocation was collected at a GPS jamming event sponsored by the Department of Homeland Security (DHS) at White Sands Missile Range in New Mexico. The event spanned multiple days and included participants from both industry and academia. The jamming was performed only at night to minimize interference with GPS users near the range. The jamming scenarios included, but were not limited to, static civilian jammers and jammers mounted in cars driving on prespecified routes. The results presented in this study are for a subset of the mobile cases only, as some of the vehicles with jammers contained sophisticated INSs, and were therefore able to provide position solutions in a GPS–denied environment.

Four stations were used to collect data in this study. Each station is denoted by a red square on the Google Maps image shown in Fig 14. The stations at the top and bottom of the image are separated by approximately one kilometer, while the other two stations are separated by approximately 500 meters.

All of the stations used general purpose RF equipment and stored the data for processing in an after-the-fact manner. The important pieces of RF equipment are shown in Figs 15, 16, and 17.

Figure 15 contains three important pieces of equipment. The first two boxes on the left are Ettus Research Equipment USRP N200s with two daughter boards (DBSRX2 800-2350 MHz Rx). They are general purpose RF-front ends which can filter RF signals, mix the signals to baseband, digitize the data and then

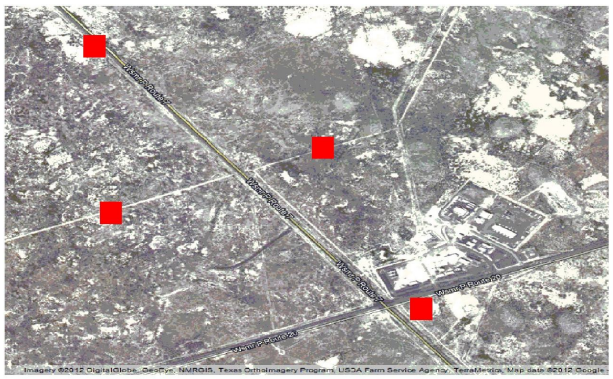

Figure 14 A Google Maps image overlaid with red square to indicate receiver station locations. (Imagery ©2012 DigitalGlobe, GeoEye, NMRGIS, Texas Orthoimagery Program, USDA Farm Service Agency, Map data ©2012 Google)

Figure 15 General purpose RF recording equipment. The two boxes on the left are Ettus Research USRP N200s, the box in the middle is an ovenized crystal oscillator and the box on the right is a power inverter.

stream it over an ethernet cable to a laptop. The two USRPs' relative digitization times are synchronized using an Ettus Research Equipment MIMO cable (shown plugged into the front of both boxes). The box in the middle is an ovenized crystal oscillator, and is used to drive the RF-front end mixing chain and sample times in the two Ettus USRPs. The box on the right is a Belkin car cigarette lighter socket DC power inverter. It powered all of the other equipment in the figure.

Figures 16, and 17 show two different antennas that receive signals at the GPS frequency. Figure 16 shows an antenna mounted on a ground plane and on a tripod. This setup allows the antenna to be aimed towards the location where a GPS jammer is expected, so that its emissions may be received. The second antenna, shown in Fig 17, is a simple GPS patch antenna. The second antenna is meant to enable time synchronization between different stations by means of GPS. Time synchronization requires tracking at least 4 GPS satellites if the platform is mobile, and only one if the platform is stationary. To ensure tracking of the minimum number of GPS satellites, the second antenna was placed on a ground plane (sheet of metal) which was pointed away from the expected jammer locations and further shielded from the jammers using the car or a raised piece of ground near each station. The ground plane and shielding severely attenuate the received power of the GPS jammer and allows tracking of the GPS satellites.

Figure 16 Jammer pickup antenna on ground plane, mounted on a tripod for easier aiming.

A picture from one of the setups on a typical night

Figure 17 GPS pickup patch antenna. Mounted on a large ground plane and shielded with a car when used in the field.

is shown in Fig 18. The jammer pickup antenna was placed on top of the car and was aimed towards the road where the suspected jammer was assumed to travel. The second antenna was mounted on a ground plane and placed against the driver's side tire. The shielding and placement selection of the second antenna effectively attenuated power emitted from the GPS jammer at that antenna. The rest of the equipment was located inside the car and was powered by the power inverter as the car idled.

Figure 18 Picture of the bottom right station in Fig 14, on a typical night of testing.

The other three stations were set up with similar equipment and in a similar manner. The data was collected from both antennas at approximately 9 MHz, with 14- bit digitization, and with the L1 frequency set as the baseband frequency of the Ettus USRPs. Each USRP used a different fixed gain for each antenna and for each of the two tests considered in this study. The first test was of a higher power jammer and typically used gains of 25dB for the jammer pickup antenna and 35 dB for the GPS pickup antenna. The second test was of a lower power jammer and typically used gains of 30dB for the jammer pickup antenna and 40 dB for the GPS pickup antenna. The total amount of recorded data was approximately 10 TB, but a much smaller amount is considered in this study.

Results of Kalman Filter Geolocation Using Real Data

There were numerous jamming events throughout the multiple nights of testing at White Sands Missile Range, but the results of only two scenarios are shown in the present study. The two studies use data from jammers mounted on top of vehicles with inertial navigation systems. These vehicle–mounted jammers were driven through the receiver array.

The first set of results is for a more powerful GPS jammer. This first jammer was able to completely disable a hand-held road navigation unit placed inside of the car at the top left station in Fig 14, which was very near the road. The jammer shown in the middle of Fig 1 has a similar form factor to the jammer used in the first test, although the tested jammer was slightly larger. More detailed information on this type of jammer can be found in reference [7], where it is listed as that paper's second classification of jammer type.

The second set of results is for a weaker GPS jammer. In addition to radiating less power than the first jammer, this particular jammer swept a much larger frequency range. The larger sweep range results in less time spent inside of a narrow band at the L1 frequency, reducing the time–averaged received power. The jammer shown at the far left of Fig 1 has a nearly identical form factor to that used in the second test. More detailed information on this type of jammer can be found in reference [7], where it is listed as that paper's first classification of jammer type.

The TDOA position solutions are compared to the INS position solutions for the first and second tests, with results plotted on top of a Google Maps image in Figs 19 and 20, respectively. In both figures the receiver station positions are denoted with red squares,

the INS position solutions with blue dots, and the TDOA position solutions with green dots. The results use only small batches of data in short Kalman Filter runs every 5 seconds, with no shared *a priori* information passed between batches. The amount of measurements used comprise only 0.16% of the data that could have been used. Using all of the data would improve results, but may be difficult to accomplish in a real–time system.

The average difference magnitude between the TDOA and INS positions for the first scenario is approximately 15 meters in the local east-north plane, while the average position difference magnitude for the second scenario is approximately 8.5 meters. The listed differences are with respect to an INS, which may contain a minor bias. The vertical, or altitude, position difference is negligible because of the altitude constraint measurement.

SUMMARY AND CONCLUSIONS

This paper has covered four related topics of civilian GPS jammers.

The first topic has been a brief background review on civil GPS jamming, and it has been shown that the output of a typical jammer is a chirp signal.

The second topic has been a particular parameterization of the jammer's linear chirp signal. The chirp signal dynamics were described with standard linear systems–type techniques, and the state has been related to a theoretical RF output at the jammer antenna.

The third topic has been a method of tracking the simulated signal through the use of accumulations, accumulation models, noise models, and Kalman Filter–type estimation techniques. Two different types of accumulations have been used to improve the pull-in of the filter, one that uses the estimated jammer frequency in the NCO and one that used the jammer frequency plus its reset. Results of the jammer simulator and Kalman Filter signal tracker have been presented for a signal with a given parameterization. The Kalman Filter is able to track a weak jamming signal with significant process noise.

The final topic has been a TDOA geolocation method using a Kalman Filter. The measurements used in this study's TDOA model are not simple cross–correlation peaks, but instead are a signal feature, the L1 frequency crossing of the chirp signal. The real data used in geolocation were collected at a DHS–sponsored jamming event at White Sands Missile Range in June of 2012. The presented TDOA algorithm has been tested on the collected data for two types of jammers in moving vehicles. The resulting position differences between the INSs on the vehicles containing the jammers and the TDOA position estimates are approximately 15 and 8.5 meters, for the first and second test, respectively.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to the Department of Homeland Security for their arrangement and sponsorship of the jamming event at White Sands Missile Range and to the 746th Test Squadron for their part in the jamming event and for their processing of the vehicular INS data.

The authors would also like to express their thanks to the following members of the UT/Austin Radionavigation Laboratory for helping to staff the receiver stations at White Sands Missile Range: Todd Humphreys, Daniel Shepard, and Reese Shetrone.

REFERENCES

[1] Arthur, C., "Car thieves using GPS 'jammers'," Monday 22 February 2010, http://www.guardian.co.uk/technology/2010/feb/22/car-thieves-using-gps-jammers.

[2] Anon., "National PNT Advisory Board comments on Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures," November 2010.

[3] Misra, P. and Enge, P., *Global Positioning System: Signals, Measurements, and Performance*, Ganga-Jamuna Press, Lincoln, Massachusetts, 2nd ed., 2006, pp. 53–58.

[4] Spilker, J. and Natali, F., *Global Positioning System: Theory and Applications Volume 1*, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1st ed., 1996.

[5] Pullen, S. and Gao, G., "GNSS Jamming in the Name of Privacy," *Inside GNSS*, Vol. 7, Mar./Apr. 2012.

[6] Mitch, R. H., Dougherty, R. C., Psiaki, M. L., Powell, S. P., O'Hanlon, B. W., Bhatti, J. A., and Humphreys, T. E., "Innovation Column: Know Your Enemy," *GPS World*, January 2012.

[7] Mitch, R. H., Dougherty, R. C., Psiaki, M. L., Powell, S. P., O'Hanlon, B. W., Bhatti, J. A.,

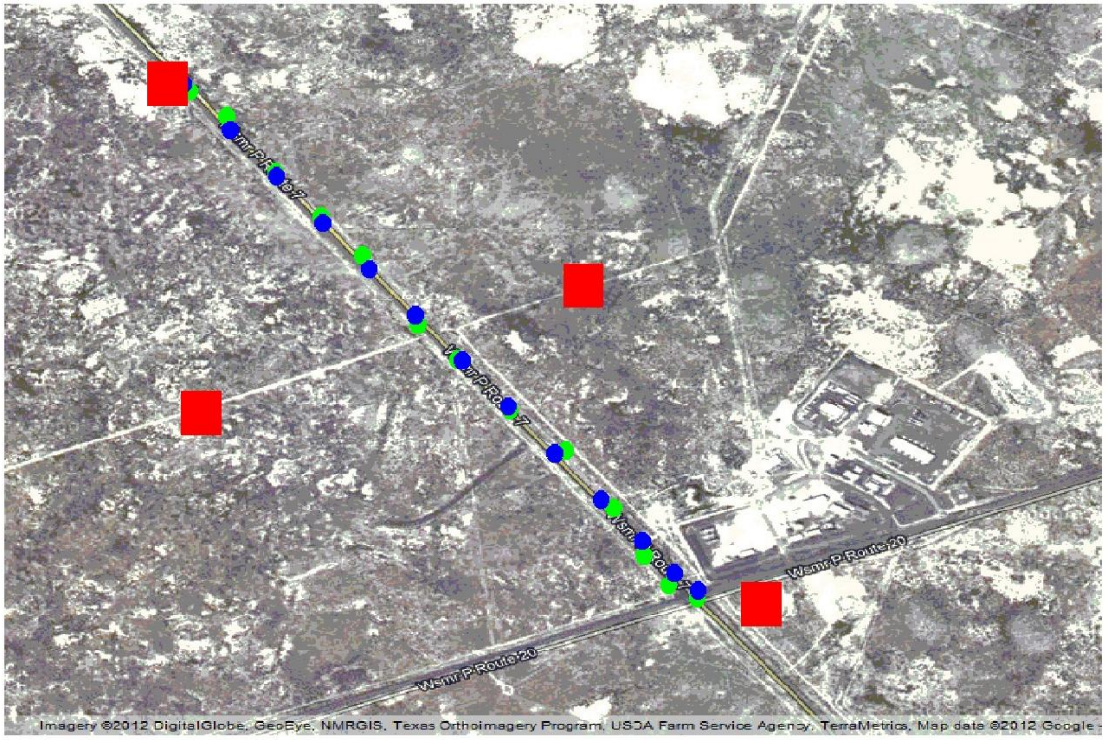

Figure 19 Results of the scenario using the higher power jammer, with plots in five second intervals. The receiver stations are red squares, INS position solutions are blue dots, and TDOA positions solutions are green dots.

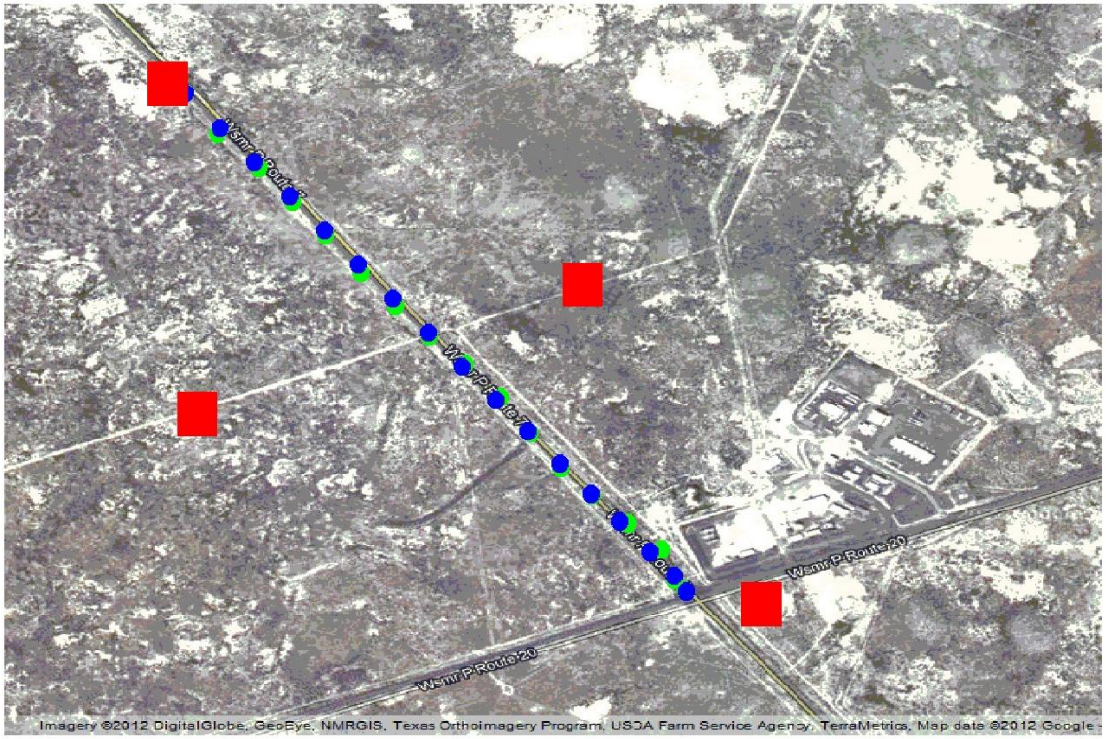

Figure 20 Results of the scenario using the lower power jammer, with plots in five second intervals. The receiver stations are red squares, INS position solutions are blue dots, and TDOA positions solutions are green dots.

and Humphreys, T. E., "Signal Characteristics of Civil GPS Jammers," *Proceedings of the ION GNSS 2011*, Sept. 20-23, 2011, pp. 1907–1919, Portland, OR.

[8] Kraus, T., Bauernfeind, R., and Eissfeller, B., "Survey of In-Car Jammers - Analysis and Modeling of the RF signals and IF samples (suitable for active signal cancellation)," *Proceedings of the ION GNSS 2011*, Sept. 20-23, 2011, pp. 430–435, Portland, OR.

[9] Bhatti, J., Humphreys, T. E., and Ledvina, B. M., "Development and Demonstration of a TDOA-Based GNSS Interference Signal Localization System," *Proceedings of the IEEE/ION PLANS Conference*, Myrtle Beach, SC, April 2012.

[10] Bar-Shalom, Y., Li, R. X., and Kirubarajan, T., *Estimation with Applications to Tracking and Navigation*, John Wiley & Sons, 605 Third Avenue, New York, NY, 1st ed., 2001.

[11] Brown, R. and Hwang, P. Y. C., *Introduction to Random Signals and Applied Kalman Filtering*, John Wiley & Sons, 111 River Street, Hoboken, NJ, 3rd ed., 1997.

[12] Bierman, G. J., *Factorization Methods for Discrete Sequential Estimation*, Dover Publications, 31 East 2nd Street, Mineola, NY, 1st ed., 1977.

[13] Psiaki, M. L. and Jung, H., "Extended Kalman Filter Methods for Tracking Weak GPS Signals," *Proceedings of the ION GPS 2002*, Portland, OR, Sept. 24-27 2002, pp. 2539–2553.

[14] Chiang, Q. Z. and Psiaki, M. L., "GNSS Signal Tracking Using a Bank of Correlators," *Proceedings of the ION GNSS 2010*, Portland, OR, Sept. 21-24 2010, pp. 3258–3267.

[15] Bell, B. M. and Cathey, F. W., "The Iterated Kalman Filter Update as a Gauss-Newton Method," *IEEE Transactions on Automatic Control*, Vol. 38, No. 2, February 1993.

[16] Poisel, R., *Electronic Warfare Target Location Methods*, Artech House, Boston, Massachusetts, 1st ed., 2005, pp. 140–168.

[17] Isoz, O., Balaei, A. T., and Akos, D., "Interference detection and localization in the GPS L1 band," *Proceedings of the ION ITM*, Jan. 2010, pp. 925–929, San Diego, CA.

[18] Lindstrom, J., Akos, D. M., Isoz, O., and Junered, M., "GNSS interference detection and localization using a network of low-cost front-end modules," *Proceedings of the ION GNSS Meeting*, Sept., 25-28 2007, pp. 1165–1172, Fort Worth, TX.

[19] Gromov, K. G., *GIDL: Generalized Interference Detection and Localization System*, Ph.D. thesis, Standford University, March 2002.

[20] Montminy, M. B., *Passive Geolocation of Low-Power Emitters in Urban Environments Using TDOA*, Master's thesis, Air Force Institute of Technology, March 2007.