Unmanned Aircraft Capture and Control via GPS Spoofing

Andrew J. Kerns
Department of Electrical and Computer Engineering
The University of Texas at Austin
Austin, TX 78712
akerns@utexas.edu

Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys
Department of Aerospace Engineering
The University of Texas at Austin
Austin, TX 78712
dshepard@utexas.edu, jahshan@utexas.edu, todd.humphreys@mail.utexas.edu

Abstract

The theory and practice of unmanned aerial vehicle (UAV) capture and control via Global Positioning System (GPS) signal spoofing are analyzed and demonstrated. The goal of this work is to explore UAV vulnerability to deceptive GPS signals. Specifically, this paper (1) establishes the necessary conditions for UAV capture via GPS spoofing, and (2) explores the spoofer's range of possible post-capture control over the UAV. A UAV is considered captured when a spoofer gains the ability to eventually specify the UAV's position and velocity estimates. During post-capture control, the spoofer manipulates the true state of the UAV, potentially resulting in the UAV flying far from its flight plan without raising alarms. Both overt and covert spoofing strategies are considered, as distinguished by the spoofer's attempts to evade detection by the target GPS receiver and by the target navigation system's state estimator, which is presumed to have access to non-GPS navigation sensor data. GPS receiver tracking loops are analyzed and tested to assess the spoofer's capability for covert capture of a mobile target. The coupled dynamics of a UAV and spoofer are analyzed and simulated to explore practical post-capture control scenarios. A field test demonstrates capture and rudimentary control of a rotorcraft UAV, which results in unrecoverable navigation errors that cause the UAV to crash.

Keywords: Unmanned vehicle security, GPS spoofing, Counter-UAV.

1 Introduction

For autonomous or semi-autonomous operation, unmanned aerial vehicles (UAVs) demand reliable navigation. By far the most common historical approach to ensuring reliable UAV navigation has been to build a state estimator around a sensor core consisting of an inertial measurement unit (IMU) and a Global Positioning System (GPS) receiver (Kendoul, 2012). But given the fragility of GPS and other Global Navigation Satellite System (GNSS) signals under conditions of signal blockage or jamming, there is currently

great interest in developing UAV navigation and control systems that can operate in GNSS-denied environments (Kendoul, 2012, Bachrach et al., 2011, Weiss et al., 2011, Garratt and Chahl, 2008). Promising recent results demonstrate that vision-aided navigation is a practical alternative to GNSS for closed-loop UAV control in an unmapped environment (Chowdhary et al., 2013). Nonetheless, as opposed to GNSS-aided navigation, vision-aided techniques inevitably drift during long-range exploration unless an *a priori* feature map is available, and they are only appropriate in benign weather and lighting conditions. Consequently, one can expect most UAV navigation systems to rely on GNSS receivers for years to come, with vision and other non-GNSS sensors serving to fill gaps in GNSS signal availability.

GNSS vulnerability extends beyond signal blockage and jamming. Spoofing attacks, in which counterfeit GNSS signals are generated for the purpose of manipulating a target receiver's reported position, velocity, and time, have been demonstrated with low-cost equipment against a wide variety of GPS receivers (Humphreys et al., 2008, Shepard and Humphreys, 2011, Shepard et al., 2012a, Shepard et al., 2012b). Whereas the military GPS waveform is by design unpredictable and therefore resistant to spoofing (Spilker, 1996), civil GPS waveforms—and those of other civil GNSS—are unencrypted, unauthenticated, and openly specified in publicly-available documents (Global Positioning System Directorate, 2012, European Union, 2010). Also, although not entirely constrained by the signal specifications, the navigation data messages modulating these civil waveforms are highly predictable. The combination of known signal structure and data bit predictability makes civil GNSS signals an easy target for spoofing attacks.

A number of promising methods are currently being developed to defend against civil GNSS spoofing attacks. These can be categorized as (1) receiver-autonomous signal-processing-oriented techniques, which require no antenna motion or specialized antenna hardware (Ledvina et al., 2010, Wesson et al., 2011, Dehghanian et al., 2012, Wesson et al., 2013); (2) receiver-autonomous antenna-oriented techniques, which require antenna motion or specialized antenna hardware (De Lorenzo et al., 2005, Montgomery et al., 2009, Broumandan et al., 2012); (3) cryptographic techniques that require signal specification modifications to overlay unpredictable but verifiable modulations on existing or future civil GNSS signals (Wesson et al., 2012, Humphreys, 2013); and (4) techniques that exploit the existing encrypted military signals to offer civil GPS signal authentication for networked GPS receivers (Lo et al., 2009, Psiaki et al., 2011, Psiaki et al., 2013, O'Hanlon et al., 2012). Unfortunately, it will take years before these technologies mature and are implemented on a wide scale. Meanwhile, there are no off-the-shelf defenses against GNSS spoofing.

This paper explores the extent of unmanned aerial vehicle (UAV) vulnerability to deceptive GNSS signals by (1) establishing the necessary conditions for UAV capture via GPS spoofing, (2) investigating a spoofer's range of possible post-capture control over the UAV, and (3) demonstrating in field tests the capture and rudimentary control of a UAV via GPS spoofing. These contributions are novel within the open literature, and may well be novel in the classified domain.

This paper's focus is on civil GPS signal spoofing, and only civil GPS signals will be considered hereafter. Nonetheless, the claims made regarding civil GPS signal vulnerability apply broadly to current and planned civil GNSS signals whose specifications have been made public, including the modernized GPS L2C and L5 signals and the Galileo open service signals.

For both capture and post-capture control, two broad spoofing strategies are considered: overt (the spoofer makes no attempt to conceal the attack), and covert (the spoofer seeks to evade detection by the target GPS receiver and by the target UAV navigation system as a whole). As one might expect, covert capture requirements are much more stringent, and covert control authority is much more limited, than their overt counterparts.

The next section gives an overview of the components involved in a spoofing attack and explains how a spoofer compensates for the signal propagation and processing delays. Navigation system capture via GPS spoofing is then defined and necessary conditions are presented for both overt and covert capture. This is followed by a detailed theoretical analysis of overt and covert post-capture control, accompanied by illustrative simulations. This paper concludes with the results of a field test in which a GPS spoofer captures

a rotorcraft UAV and causes it to crash.

2 System Components, Geometry, and Delays

By contrast to the so-called proximity spoofing attacks treated in (Humphreys et al., 2008) and (Shepard et al., 2012b), where the spoofer is effectively co-located with the target receiver, the current paper considers spoofing from a distance, as illustrated in Fig. 1. Through its receive antenna, marked RX, the spoofer receives authentic signals from all visible GPS satellites. The vectors $\Delta\boldsymbol{r}_{\mathrm{TX}}$ and $\Delta\boldsymbol{r}_t$ represent, respectively, the 3-dimensional coordinates of the spoofer's transmit antenna, marked TX, and the target aircraft's GPS antenna, both relative to the spoofer's receive antenna. The spoofer and target antennas are assumed to be located at respective distances r_{si} and r_{ti} from the ith GPS satellite.

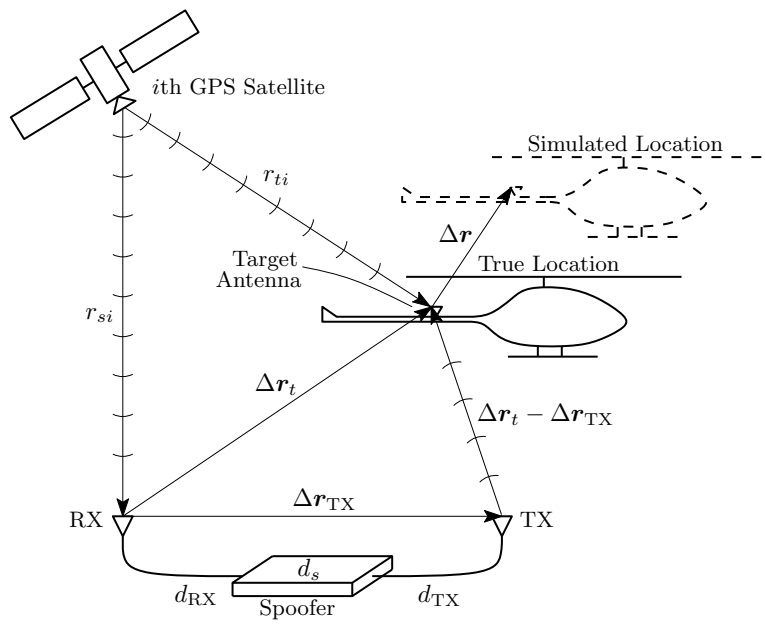

Figure 1: Illustration of the components, geometry, and delays involved in a GPS spoofing attack targeting a GPS-guided aircraft.

The spoofer generates a counterfeit signal for each authentic signal received. In the case of an initially-aligned attack, the spoofer's counterfeit signal ensemble arrives at the target antenna in such a way that each signal is approximately spreading-code-phase aligned (within a few meters) with its authentic counterpart. After capture of the target receiver's carrier- and code-phase tracking loops, the spoofer adjusts the relative code phases of its spoofing signals to induce the target receiver to report the simulated (false) location $\Delta\boldsymbol{r}$ relative to its true location; the target receiver's apparent time offset from true time can also be adjusted by a common displacement of the counterfeit code phases.

An aligned attack is only possible if the spoofer (1) measures all relevant system delays to within a few nanoseconds, and (2) compensates for these delays by generating a slightly advanced (predicted) version of the signals it receives. For civil GPS signals, reliable prediction is trivial because the spreading codes are unencrypted and openly documented, the satellites follow regular orbits, and the modulating navigation data follow regular patterns. Military GPS signals, by contrast, enjoy strong encryption of the spreading code; indeed, spreading code unpredictability is the very basis of their security.

For the ith GPS satellite, the total distance-equivalent system delay that must be compensated is given by

$$cd_i = r_{si} - r_{ti} + c(d_{\mathrm{RX}} + d_{\mathrm{TX}} + d_s) + ||\Delta\boldsymbol{r}_t - \Delta\boldsymbol{r}_{\mathrm{TX}}||$$

where d_{RX} and d_{TX} are, respectively, the receive and transmit cable delays, d_s is the spoofer signal processing delay, and c is the speed of light. The ranges r_{si} and r_{ti} are readily calculated from the broadcast satellite ephemerides so long as the spoofer knows its own receive antenna location and the relative coordinates $\Delta \boldsymbol{r}_t$ of the target. Delays d_{RX} and d_{TX} are easily calculated to nanosecond-accuracy for cables of known lengths and standard type. For the spoofer discussed here (the only one capable of all-in-view aligned GPS spoofing that has been reported in the open literature), measuring d_s is somewhat more challenging as there arises a non-deterministic buffering delay at turn-on. To overcome this, a one-time calibration is performed at turn-on whereby a reference spoofing signal is fed back internally from the spoofer's radio frequency (RF) output to its RF input and is subsequently tracked by the spoofer's GPS tracking engine. By comparing the code phase of the transmitted and received versions of the reference signal, the spoofer can measure its end-to-end delay d_s, which amounts to approximately 5 ms, to within a few nanoseconds.

To generate an aligned counterfeit version of the ith satellite's signals, the spoofer forecasts, for each signal, three quantities to an instant d_i seconds into the future: the modulated navigation data symbol value, the Doppler frequency offset, and the code phase offset. Forecasts are based on the predicted satellite position and velocity and on measured trends in the spoofer's internal clock. Note that typical target aircraft velocities and accelerations are small enough that there is no need to forecast target motion by d_i; a current estimate of $\Delta \boldsymbol{r}$ and its time derivative will suffice to enable meter- and deci-Hertz-accurate signal alignment at the target antenna.

3 Navigation System Capture

A target aircraft's navigation system is said to be captured by a GPS spoofer when the spoofer can exert control over the system's top-level 6-dimensional position and velocity (PV) estimate $\hat{\boldsymbol{x}} = [\hat{\boldsymbol{r}}^T, \hat{\boldsymbol{v}}^T]^T$. Control of the system's receiver clock offset estimate δt is implicit in navigation system capture, but focus here will rest only on control of $\hat{\boldsymbol{r}}$ and $\hat{\boldsymbol{v}}$. In the current context, "exert control" means that the spoofer can eventually force $\hat{\boldsymbol{x}}$ to match a spoofer-prescribed value $\boldsymbol{x}^\star$ to within the precision of the GPS standard positioning service (SPS), which is currently better than 3 m in position and 10 cm/s in velocity when a receiver has access to corrections from a satellite augmentation system, such as the Wide Area Augmentation System (WAAS) (Misra and Enge, 2012).

One can think of the capture condition as analogous to nonlinear controllability of the PV estimator in steady-state (Hermann and Krener, 1977): from an initial estimate $\hat{\boldsymbol{x}}(t_0)$ at the onset of spoofing, there exists $t_1 \geq t_0$ such that $\hat{\boldsymbol{x}}(t_1) \approx \boldsymbol{x}^\star$. The value of t_1 is lower bounded by the dynamics of the PV estimator, which performs a weighted fusion of the GPS-provided PV measurements and measurements from non-GPS navigation sensors. Navigation system capture implies that the spoofer has obtained control over a sufficient number of the target GPS receiver's active code and carrier tracking loops so that, within the constraints imposed by each loop's update interval and finite bandwidth, the spoofer can dictate the receiver's reported PV solution via adjustments to the simulated code phase and carrier phase rate values.

A limited variant of full capture, called manifold capture, occurs when the spoofer can only control $\hat{\boldsymbol{x}}$ within an $m < 6$-dimensional submanifold of the PV state space. For example, a particular UAV's navigation system may ignore GPS position and velocity measurements in the vertical direction, relying solely on an altimeter. Manifold capture is analogous to controllability of a subsystem of a larger uncontrollable system.

Full or manifold capture requires that at least a submanifold of the target aircraft's state estimate $\hat{\boldsymbol{x}}$ be controllable from the GPS receiver's PV output. This condition holds for most unmanned aircraft equipped with a GPS receiver when operated in the active GPS mode because the navigation state estimator typically models non-GPS navigation sensors as subject to disturbances or drifts that get corrected using GPS measurements. Such models are appropriate for inertial sensors (Flenniken IV et al., 2005), magnetometers (Wendel et al., 2006), barometric altimeters (Kim and Sukkarieh, 2003), and electro-optical navigation systems based on exploratory simultaneous localization and mapping (SLAM) (Durrant-Whyte and Bailey,

2006, Nuetzi et al., 2011, Chowdhary et al., 2013). Only SLAM-type navigational systems that strictly limit exploration, or systems that perform map-matching with a high-resolution *a priori* map, have been shown to deliver position and velocity estimates with similar accuracy and long-term stability to those of a GPS receiver (Castle et al., 2011). Thus, it is reasonable to expect that most UAV systems will remain at least manifold capturable for some years hence.

3.1 Overt Capture

In overt capture, the spoofer makes no attempt to conceal its attempt to subjugate the target system. Hence, the spoofer need not align its simulated signals with their authentic counterparts at the target receiver's antenna at the beginning of the attack; it may instead simply jam the target GPS frequency bands, causing the target receiver to lose lock and attempt re-acquisition of all signals. Following such a jamming prelude, the spoofer will successfully gain control of the target GPS receiver's tracking loops if its simulated signals arrive with sufficient power that (1) they comfortably exceed the target receiver's acquisition detection threshold, and (2) the authentic signals are forced below the detection threshold by action of the RF front-end's automatic gain controller. Let $\eta = P_s/P_a$ be the spoofer power advantage, or the ratio of received spoofing signal power P_s to authentic signal power P_a, for a particular authentic signal. Experiments with various receiver types indicate that $\eta = 10$ dB is adequate to satisfy these conditions.

Nor is the spoofer strictly required to align its simulated PV state $\boldsymbol{x}^\star$ with the true state $\boldsymbol{x}$ or with the PV state estimate $\hat{\boldsymbol{x}}^s \approx \boldsymbol{x}$ for overt capture. The spoofer may wish to ensure a smooth transition to post-capture control by setting $\boldsymbol{x}^\star \approx \boldsymbol{x}$, but an abrupt transition may be acceptable—or even desirable—for an overt spoofer's purposes.

3.2 Covert Capture

In covert capture, the target aircraft's navigation system is assumed to be equipped with spoofing detection measures that the spoofer must avoid triggering. As noted in the introduction, ongoing development of several sophisticated spoofing detection methods has been reported in the literature. However, these techniques are all years away from widespread implementation, and some are too costly or heavy for practical use on small UAVs. Therefore, this paper will define covert capture in terms of avoidance of simpler near-term-implementable spoofing detection techniques. Navigation system capture will be considered covert if the spoofer (1) satisfies all the conditions for overt capture, and (2) evades the following detection techniques: (a) jamming-to-noise (J/N) monitoring within the GPS receiver, (b) frequency unlock monitoring within the GPS receiver, and (c) innovations testing within the navigation system's state estimator. These techniques are briefly described below. Avoidance of even simpler spoofing detection strategies such as data bit latency monitoring (Humphreys et al., 2008), carrier-to-noise ratio monitoring (Warner and Johnston, 2003), and standard receiver autonomous integrity monitoring (RAIM) (Brown, 1996) will also be assumed for covert capture, but these are only mentioned in passing given that they do not pose a challenge for a sophisticated spoofer (Shepard et al., 2012b, Psiaki et al., 2013).

J/N Monitoring A GPS J/N monitor triggers an alarm when the power received in a given bandwidth significantly exceeds the power in that bandwidth under quiescent conditions (Ward, 1994). A few commercial receivers, including the ublox Lea-6N, are now being offered with J/N monitoring. A J/N monitor can serve as a spoofing detector if (1) the power received from a spoofer exceeds the triggering threshold, and (2) the receiver continues to track GPS signals at high carrier-to-noise ratios despite the apparent jamming (Akos, 2012). Thus, from a spoofer's point of view, avoidance of a J/N monitor entails limiting the spoofer power advantage η. For the ublox Lea-6N in its default configuration, laboratory tests have shown that maintaining $\eta \leq 12$ dB on all spoofed signals is sufficient to avoid triggering the J/N monitor.

Use of a J/N monitor also prevents the jam-then-spoof style attack mentioned in the previous section. Without this option, a spoofer must resort to the more difficult signal-aligned attack to wrest control of the

target receiver's tracking loops.

Frequency Unlock Monitoring Frequency unlock monitoring within a GPS receiver can be an effective spoofing detection strategy because (1) under non-spoofed conditions, frequency unlock is unusual except in cases of signal blockage or severe ionospheric scintillation (Humphreys et al., 2010), and (2) it is challenging for a spoofer to prevent frequency unlock in initial tracking loop capture because this requires precise knowledge of the target aircraft's velocity, as will be described in following sections. Phase unlock, a more sensitive tracking anomaly, is also an effective indicator of spoofing (Humphreys et al., 2012) but is ignored here because it occurs far too commonly in unspoofed conditions.

Innovations Testing Innovations testing within the target aircraft's navigation state estimator is a readily-implementable defense against spoofing. Spoofing is declared upon capture if the PV output from the spoofed GPS receiver is inconsistent with the navigation state estimator's PV estimate. This technique's spoofing detection sensitivity depends on the quality of the non-GPS sensors feeding data to the state estimator. A more stable IMU, for example, leads to improved sensitivity.

In following subsections, covert capture of the target GPS receiver's tracking loops—which entails avoiding both J/N and frequency unlock monitors—and covert capture of the navigation state estimator—which entails avoiding innovations test violations—are described in further detail.

3.2.1 GPS Receiver Tracking Loop Architecture

From a signal tracking perspective, an aligned GPS spoofing attack presents a unique problem that has not been previously addressed. Extensive prior literature explores signal pull-in ranges for phase-lock loops (PLLs) and delay-lock loops (DLLs) under the typical code-division multiple-access scenario where the input consists of an admixture of signals each having a unique spreading code with negligible cross-correlation (Zhuang, 1996, Lee and Un, 1982, Gupta, 1975, Lindsey and Chie, 1981). These results apply directly to signal tracking within a GPS receiver under normal circumstances. During a spoofing attack, however, each spoofing signal competes against its counterpart authentic signal for control of the tracking loops, and both signals have identical spreading codes. This is similar to the case of severe multipath except that the spoofing signal can be made more powerful than the authentic signal and can present itself as either a delayed or advanced version of the authentic signal.

For the analysis of GPS tracking loop capture presented in this paper, it is assumed that each signal is tracked by a phase-rate feedback PLL and a carrier-aided early-late DLL. This is a standard configuration for commercial and military GPS receivers (Van Dierendonck, 1996, Misra and Enge, 2012, Braasch and Van Dierendonck, 1999, Stephens and Thomas, 1995). Let the portion of the received signal corresponding to a unique spreading code (a single signal from a particular satellite) under a spoofing attack be represented by a complex baseband model as

$$\begin{aligned} s(t) =& C\left[t-\tau_a(t)\right]\exp\left(j\phi_a(t)\right) \\ &+ \sqrt{\eta}C[t-\tau_s(t)]\exp\left(j\phi_s(t)\right) + n(t) \end{aligned}$$

where $C(t)$ is the spreading code, $\tau_a(t)$ is the authentic signal's code phase, $\phi_a(t)$ is the authentic signal's carrier phase, η is the spoofer power advantage, $\tau_s(t)$ is the spoofing signal's code phase, $\phi_s(t)$ is spoofing signal's carrier phase, and $n(t)$ is a zero-mean complex white Gaussian noise process that models the combined target receiver thermal noise and noise embedded in the received spoofing signal (e.g., due to output amplitude quantization within the spoofer). This model neglects the low-rate GPS binary navigation data modulation because it does not affect loop dynamics and is assumed to be perfectly replicated by the spoofer.

The received signal $s(t)$ is first multiplied by three local spreading code replicas separated in code phase by $T_{EML}/2$ to produce the early, prompt, and late code-correlated signals based on the DLL's estimate of $\tau(t)$. Next, the code-correlated signals are multiplied by the local carrier replica, which is based on the PLL's

estimate of $\phi(t)$. The resulting signals are then integrated over the accumulation interval T_a to produce discrete accumulations modeled as

$$\begin{aligned} S_X(k) =& R\left(\Delta\tau_{X,a}(k)\right) \operatorname{sinc}\left(\frac{\Delta f_{D,a}(k)}{2\pi}\frac{T_a}{2}\right) \exp(j\Delta\bar{\phi}_a(k)) \\ &+ \sqrt{\eta} R\left(\Delta\tau_{X,s}(k)\right) \operatorname{sinc}\left(\frac{\Delta f_{D,s}(k)}{2\pi}\frac{T_a}{2}\right) \exp(j\Delta\bar{\phi}_s(k)) + N(k) \end{aligned}$$

where $S_X(k)$ is the accumulation at lag $X \in \{E, P, L\}$ (for early, prompt, and late); $\Delta\tau_{X,a}(k)$ and $\Delta\tau_{X,s}(k)$ are the code phase differences between the local replica at lag X and the authentic and spoofed signals, respectively; $R(\Delta\tau(k))$ is the autocorrelation function of the spreading code; $\Delta f_{D,a}(k)$ and $\Delta f_{D,s}(k)$ are the differences between the Doppler frequency of the local replica and the Doppler frequency of the authentic and spoofed signals, respectively; $\Delta\bar{\phi}_a(k)$ and $\Delta\bar{\phi}_s(k)$ are the differences between the carrier phase of the local replica and the carrier-phase of the authentic and spoofed signals, respectively, at the midpoint of the accumulation interval; and $N(k)$ is the accumulated noise, modeled as an uncorrelated discrete-time zero-mean complex Gaussian noise sequence.

The DLL delay discriminator ingests the early and late accumulations $S_E(k)$ and $S_L(k)$ and produces the delay feedback signal $e_\tau(k)$; the PLL phase discriminator ingests the prompt accumulation $S_P(k)$ and produces the carrier-phase feedback signal $e_\phi(k)$. The delay discriminator is typically either coherent or non-coherent; the phase discriminator is typically either a two-quadrant or a four-quadrant inverse tangent function (Braasch and Van Dierendonck, 1999).

The feedback signals from the delay and phase discriminators are filtered before they are passed to the code generator and number-controlled oscillator (NCO), respectively. For carrier-aided DLLs, a first-order DLL filter is adequate, with filtered feedback given by

$$y_{\mathrm{DLL}}(k) = 4B_{\mathrm{DLL}} e_\tau(k)$$

where B_{DLL} is the DLL bandwidth. The PLL filter is typically of the form

$$y_{\mathrm{PLL}}(k) = \frac{G_1}{T_a} e_\phi(k) + \frac{G_2}{T_a}\sum_{i=0}^{k} e_\phi(i) + \frac{G_3}{T_a}\sum_{i=0}^{k}\sum_{j=0}^{i} e_\phi(j).$$

Assignment of coefficients G_i is based on the filter order and on the product of the PLL bandwidth B_{PLL} and the accumulation interval T_a (Stephens and Thomas, 1995).

3.2.2 Covert Capture of GPS Receiver Tracking Loops

Covert capture of GPS receiver tracking loops has been briefly addressed in a previous experimental study (Tippenhauer et al., 2011). However, the cited study only tested a single receiver type and did not consider Doppler frequency alignment errors, which must be small to enable covert receiver capture. The simulation, live spoofing tests, and analysis in this section form the first complete study on covert capture of mobile GPS receiver tracking loops. To covertly capture the target GPS receiver's tracking loops, the spoofer must not cause frequency unlock in any PLL. For this, the spoofer must ensure that, within the target receiver, all spoofing signals are closely aligned with their authentic counterparts in both code phase $\tau(t)$ and Doppler frequency $f_D(t)$. Once aligned, the spoofing signals can be raised above the power of the authentic signals to assume control of S_E, S_P and S_L. Alignment between spoofing and authentic signals requires that all systematic and geometric delays and their time rates of change are known and accounted for in the production of the spoofing signals, as detailed in Sec. 2. While a properly-designed spoofer is capable of almost perfectly accounting for cable delays and internal delays, accurately compensating for the geometric delays and rates requires precise knowledge of the position and velocity of the spoofer and target aircraft. If the spoofer's receive antenna is properly isolated from its transmit antenna, then the spoofer has continuous access to

uncontaminated authentic GPS signals and can thus continuously track the position and velocity of its own receive and transmit antennas to SPS precision, assuming the vector $\Delta \boldsymbol{r}_{\mathrm{TX}}$ in Fig. 1 is known. However, the spoofer may not know the target aircraft's position and velocity to such precision. The spoofer could obtain precise target position and velocity data by intercepting the target UAV's automatic dependent surveillance-broadcast (ADS-B) messages (provided the target is ADS-B equipped), but it should be noted that ADS-B data are only useful for covert capture, not for post-capture control, as they are themselves GPS-dependent and would thus be corrupted post-capture by the spoofer's signals. Thus, an alternative target tracking solution such as radar or visual tracking would be of more general utility to the spoofer.

Errors in the spoofer's estimate of the target aircraft's position get mapped into the length-equivalent differential code phase $\Delta\rho \triangleq c(\tau_a - \tau_s)$; likewise, errors in estimated target velocity get mapped into differential Doppler $\Delta f_D \triangleq (\dot{\phi}_a - \dot{\phi}_s)/2\pi$. Let $P_p, P_v \in \mathbb{R}^{3\times 3}$ represent the position and velocity error covariance matrices of the spoofer's target tracking estimator. For practical values of P_p and P_v, the dominant causes of signal alignment errors $\Delta\rho$ and Δf_D are uncertainty in target position and velocity, respectively. The spoofer's estimate $\hat{\boldsymbol{r}}^s$ of target position $\boldsymbol{r}$ results in a linearized differential code phase $\Delta\rho \approx H\left(\boldsymbol{r} - \hat{\boldsymbol{r}}^s\right)$ where

$$H = \left[\frac{\partial}{\partial \boldsymbol{r}}\Delta\rho\right]_{\boldsymbol{r}=\hat{\boldsymbol{r}}^s} = \frac{\hat{\boldsymbol{r}}^s - \boldsymbol{r}_{\mathrm{TX}}}{||\hat{\boldsymbol{r}}^s - \boldsymbol{r}_{\mathrm{TX}}||} - \frac{\hat{\boldsymbol{r}}^s - \boldsymbol{r}_{\mathrm{SV}}}{||\hat{\boldsymbol{r}}^s - \boldsymbol{r}_{\mathrm{SV}}||},$$

and $\boldsymbol{r}_{\mathrm{TX}}$ and $\boldsymbol{r}_{\mathrm{SV}}$ are the spoofer and satellite transmitter positions, respectively. Worst-case errors in $\Delta\rho$ for a specific signal occur when H is aligned with the eigenvector of P_p corresponding to the largest eigenvalue; the same relationship holds for Δf_D and P_v when considering velocity tracking errors.

If $\Delta\rho$ or Δf_D is too large, then the spoofer will be unable to assume control of S_E, S_P and S_L, or will cause frequency unlock in the attempt. Capture, if successful, is overt. Determining the acceptable range of $\Delta\rho$, Δf_D, and η for covert capture begins with the general observation that covert capture is only possible for $\eta > 0$ dB and within a small neighborhood about $\Delta\rho = 0$, $\Delta f_D = 0$. Further study reveals that as η increases, the neighborhood about $\Delta\rho = 0$, $\Delta f_D = 0$ expands somewhat, but in no case is the admissible $\Delta\rho$ greater than twice the distance-equivalent spreading code chip interval (600 m for GPS L1 C/A). In fact, GPS tracking loops are fairly forgiving as regards $\Delta\rho$: simulations have shown that for $|\Delta\rho| \leq 50$ m identical acceptable ranges for Δf_D are obtained provided $\eta \geq 6$ dB. As $|\Delta\rho| \leq 50$ m is easily achieved in practice, subsequent analysis will assume as much and will focus on Δf_D, acceptable values of which are much harder for the spoofer to achieve.

Whether the target PLL loses lock for a given Δf_D depends on its frequency pull-in range under a spoofing attack scenario for different values of η. Analytical study of frequency pull-in is complicated by the stochastic, discrete-time, and nonlinear nature of the PLL. Indeed, even analysis of frequency pull-in for discrete-time PLLs in the absence of competing spoofing signals is challenging (Lee and Un, 1982, Bernstein et al., 1989), as manifest by the latest research in (Sarkar and Chattopadhyay, 1994), which resorts to numerical simulation. Likewise, the analysis presented here is based on numerical simulation of the foregoing tracking loop models. In all cases, it was assumed that the PLL and DLL are initially perfectly locked to the authentic signal and that the spoofer injects noise into its output to maintain a constant nominal carrier-to-noise ratio throughout the attack. The simulation also assumed that Δf_D is constant during the capture attempt.

Three PLL parameters affect the frequency pull-in range, with the most significant being the type of phase discriminator (PD) used. Due to its wider linear range, the four-quadrant discriminator is more forgiving of nonzero Δf_D than the two-quadrant discriminator. Therefore, the simulation analysis made the conservative assumption that the target receiver employs a two-quadrant discriminator. The next most important parameter is $T_a B_{\mathrm{PLL}}$, with higher values leading to a wider pull-in range. The analysis assumed a typical T_a of 10 ms and considered values of B_{PLL} of 5, 10, and 20 Hz. A B_{PLL} of 5 Hz is lower than is recommended for a mobile platform and is expected to perform poorly during normal operation, but was included for completeness. Dynamic platforms may apply even lower PLL bandwidths (and thus achieve better resistance against spoofing) if IMU aiding information is provided directly to the PLLs (deep coupling), but this practice is still uncommon among commercial GPS receivers. The final parameter of consequence is the order of the closed-loop PLL. Table 1 summarizes the PLL configuration test grid that was explored by simulation

Table 1: PLL pull-in simulation analysis test grid

Config.	PD	T_a (ms)	B_{PLL} [Hz]	Order
1	atan	10	10	3
2	atan	10	10	2
3	atan	10	20	3
4	atan	10	20	2
5	atan	10	5	3
6	atan	10	5	2

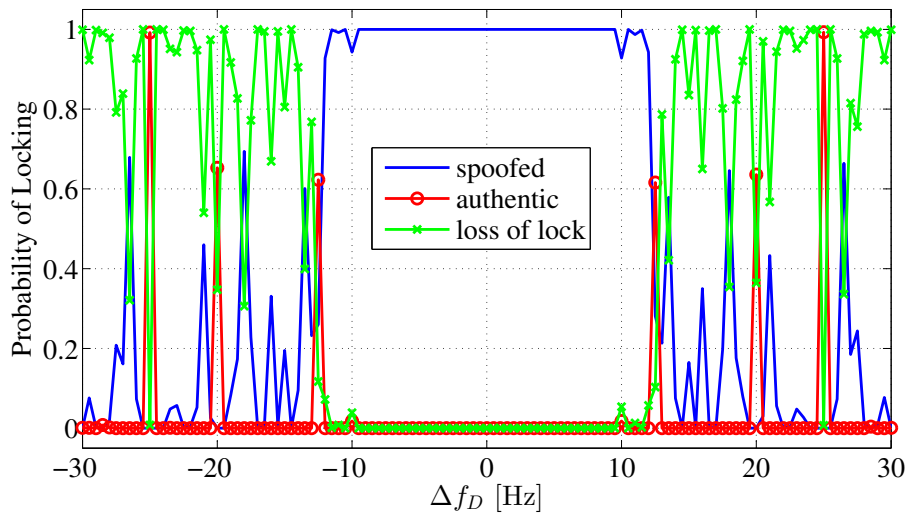

Figure 2: Probability of locking to the spoofed signal (blue) or authentic signal (red) or losing frequency lock (green) for simulation configuration 1 and a spoofer power advantage of $\eta = 5$ dB.

analysis.

Figure 2 shows example simulation results for configuration 1 with a spoofer power advantage $\eta = 5$ dB. For the results presented, 1000 Monte-Carlo simulations were run at each value of Δf_D with randomized spoofing signal carrier phase. The results show that in this scenario the spoofing signal reliably captures the PLL for $|\Delta f_D| \leq 11$ Hz. For $|\Delta f_D| > 11$ Hz, the capture probability falls off drastically: the target PLL tends to lose frequency lock instead of settling on the spoofing or authentic signals.

Table 2 summarizes the results of many tests like the one reported in Fig. 2. The table shows the maximum $|\Delta f_D|$ for high reliability capture, defined as the highest $|\Delta f_D|$ that yields $> 90\%$ probability of locking to the spoofing signal, over a range of spoofer power advantages η. The optimal spoofer power advantage for these configurations is approximately 8 dB. For $\eta = 8$ dB, all configurations except 6 (which suffers from a low B_{PLL}) have a maximum $|\Delta f_D| \geq 9.75$ Hz. These Doppler frequency error ranges can be converted to velocity estimate errors in the direction of the corresponding GPS satellite by scaling them by the GPS carrier wavelength (≈ 0.1903 m for GPS L1). This suggests that target velocity estimates are required to be accurate to about 2 m/s for covert tracking loop capture.

It is interesting to note that the maximum $|\Delta f_D|$ does not increase monotonically with η, as one might expect. This counter-intuitive result is due to the non-linear transient response of the PLL and occurs because the presence of the authentic signals aids the PLL in smoothly transitioning to tracking the spoofing signal. Higher values of η cause the authentic signal to become buried in the noise and, thus, prevents the authentic signal from aiding in this transition.

Table 2: Maximum $|\Delta f_D|$ for reliable capture [Hz]

Config.	Spoofer power advantage η						
	2 dB	3 dB	5 dB	8 dB	10 dB	12 dB	$\lim_{\eta\to\infty}$
1	2.25	5.25	11.00	11.00	9.75	9.25	7.25
2	2.25	4.75	6.75	9.75	10.25	9.75	7.75
3	3.75	6.25	12.25	12.25	10.75	10.5	7.75
4	4.75	6.75	11.25	12.75	11.25	10.5	8.75
5	1.75	3.25	7.75	10.25	9.75	8.25	6.75
6	1.75	2.75	3.75	6.25	7.25	8.25	6.75

Table 3: PLL capture probability from live spoofing tests against the CASES receiver under configuration 1. In parentheses, the maximum Doppler offset $|\Delta f_{D\max}|$ corresponding to each velocity offset is provided. For each signal, the maximum Doppler offset is achieved when the velocity offset is along the line-of-sight vector between the target receiver and the corresponding GPS satellite.

η (dB)	Velocity offset (corresponding $|\Delta f_{D\max}|$)			
	1 m/s (5.3 Hz)	2 m/s (10.5 Hz)	3 m/s (15.8 Hz)	5 m/s (26.3 Hz)
2	0	1	0.7	0
3	1	1	0.6	0
5	1	1	0.8	0
10	1	1	0.9	0.5

To further explore pull-in behavior under spoofing, the CASES receiver, a real-time software-defined GPS receiver developed jointly by the University of Texas at Austin and Cornell University (O'Hanlon et al., 2011), was tested in live spoofing attacks under configurations nearly identical to those tested in simulation, with the only difference being that the CASES receiver uses a PLL design with both phase and phase rate feedback. CASES testing revealed slightly wider pull-in ranges compared to simulation. The results for the first configuration from Table 1 are shown in Table 3. These results give the percent of all active PLLs that were captured by the spoofer at various η values and at various velocity offsets from the true velocity. Note that the 0 entry under a 1 m/s velocity offset indicates that for small η frequency unlock can be declared even at a low velocity offset as a result of the sustained interaction between nearly-equal phasors. Also note that, as a conservatively-designed science-grade receiver, CASES tends to declare frequency unlock far sooner than commercial receivers. Overall, the CASES results agree well with the simulations.

Three commercial receivers representative of those used in UAVs were also tested in their default configuration: the Javad Delta, the Trimble Juno SB, and the ublox Lea-6N. Results for these receivers, given in Table 4, indicate that commercial receivers are much more forgiving of large Δf_D values than the numerical simulations or CASES receiver. Indeed, all three receivers are capable of locking to spoofing signals with $|\Delta f_D| = 53$ Hz (velocity errors of 10 m/s) at spoofer power advantages as low as 1 dB. This robust behavior is explained by the fact that commercial receivers typically implement various layers of carrier tracking (e.g., frequency-lock loop fallback for a failing PLL) to withstand the rigors of carrier tracking on dynamic platforms. Ironically, the commercial receivers' robust tracking makes them more vulnerable to spoofing.

3.2.3 Covert Capture of the Navigation State Estimator

Covert capture of the target GPS receiver's tracking loops is only a necessary condition of overall covert capture—the spoofer must also evade detection by innovations testing within the navigation state estimator,

Table 4: Results from live spoofing tests against various commercial GPS receivers. Note that a velocity offset of 10 m/s corresponds to a maximum Doppler offset $|\Delta f_{D\max}| = 53$ Hz and that an offset of 15 m/s corresponds to $|\Delta f_{D\max}| = 79$ Hz. For each signal, the maximum Doppler offset is achieved when the velocity offset is along the line-of-sight vector between the receiver and satellite.

η (dB)	Maximum velocity offset [m/s]		
	Javad Delta	Trimble Juno SB	ublox Lea-6N
1	10	10	10
2	10	10	15
3	15	10	15

which presumably has access to several non-GPS navigation sensors, including an IMU, barometric altimeter, magnetometer, etc. Capture is covert if innovations testing during and immediately following capture of the GPS receiver tracking loops does not trigger alarms. A focus on this narrow time interval avoids any feedback effects of spoofer outputs on the captured UAV. Feedback effects will be considered in the discussion of post-capture innovations testing in Sec. 4.1.5. This section simply establishes requirements on the accuracy of the spoofer's estimate of UAV position and velocity for covert capture.

Let the normalized innovation squared (NIS) be defined as NIS $= \boldsymbol{\nu}^T S^{-1} \boldsymbol{\nu}$, where $\boldsymbol{\nu} \in \mathbb{R}^{n_z}$ is the measurement innovation and $S \in \mathbb{R}^{n_z \times n_z}$ is the innovation covariance matrix (Bar-Shalom et al., 2001). Under spoof-free conditions, the NIS at each measurement update of the navigation system state estimator will have a chi-squared distribution with n_z degrees of freedom. Avoiding detection by innovations testing requires much higher accuracy in the spoofer's estimate of the position and velocity of the target aircraft than was required for capturing the GPS receiver. Consider a target UAV with a state estimator that only employs GPS measurements (no non-GPS navigation sensors). The estimator's position and velocity measurement covariance will be within GPS SPS precision, which is currently better than 3 m in position and 10 cm/s in velocity (Misra and Enge, 2012). Assume that the state estimator experiences no filtering benefit so that its state estimate covariance is equal to the GPS measurement covariance. Even under such favorable conditions, the spoofer will find it difficult to estimate a UAV's position and velocity with sufficient accuracy to generate simulated signals consistent with SPS precision: for 2-σ covert capture reliability with a UAV that performs 8-σ innovations testing on uncorrelated Gaussian innovations, the covariance of the spoofer's estimate of UAV position and velocity required for covert navigation state estimator capture is smaller than that required for covert GPS receiver tracking loop capture by a factor of at least seven.

Clearly, innovations testing within the navigation state estimator offers a powerful near-term solution for spoofing detection because it forces the spoofer to perform precise (costly) tracking of the target UAV. Even if the threshold values are inflated to limit false alarms due to multipath and poor visible satellite geometry, the detection test will trigger unless a spoofer is capable of high-accuracy tracking of the mobile target. Conventional tracking systems, such as ground-based radar, are unlikely to meet these thresholds for covert capture. However, it should be noted that by intercepting the target UAV's ADS-B broadcasts, which contain accurate position and velocity data, the spoofer could substantially improve its chances of covert capture.

4 Post-Capture Control

This section explores post-capture control under both covert and overt scenarios. To simplify the analysis, the target UAV is assumed to be a rotorcraft and the target navigation system is assumed to be based on a conventional GPS-aided IMU configuration.

4.1 Theoretical Analysis of Post-Capture Control

This subsection constructs a continuous-time linear system model to explore the dynamics of post-capture control. The model consists of an interconnection of plants, estimators, and controllers for the UAV and spoofer.

Rotorcraft UAVs (RUAVs) typically employ a nonlinear estimator such as an extended Kalman filter to estimate their position, velocity, attitude, and IMU biases from high-rate IMU and low-rate GPS measurements (Kendoul, 2012, Christophersen et al., 2006). The state estimate is fed to a controller whose function is typically divided between an outer and inner loop, with some time-scale separation between the two (Kendoul, 2012). The outer loop generates attitude and thrust commands using a proportional-derivative (PD) controller to track a reference position and velocity trajectory. The inner loop generates control surface commands to track the attitude commanded by the outer loop. Given the loose coupling between GPS position and velocity measurements and RUAV attitude, one would not expect GPS spoofing to affect the performance of the inner loop, and this has been confirmed in field testing. Therefore, the abstract UAV model introduced in the following analysis represents only the UAV's translational dynamics, which are assumed to be uncoupled from the attitude dynamics. It is further assumed that the RUAV can directly and perfectly command translational accelerations. Unmodeled disturbances are addressed by integrator or adaptive elements (Christophersen et al., 2006), but the control action from these elements is assumed to be small. Without loss of generality, only one of the three mutually-uncoupled translational dimensions is considered. Despite its simplicity, the model captures the essential elements of RUAV control via GPS spoofing.

4.1.1 UAV Model

A one-dimensional linear model for the UAV's plant, estimator, and controller is developed as follows. The UAV's position r, velocity v, and acceleration a are governed by double-integrator dynamics so that given matrices

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and state vector $\boldsymbol{x} = [r, v]^T$, the plant dynamics model is $\dot{\boldsymbol{x}} = A\boldsymbol{x} + Ba$. The UAV makes biased acceleration measurements $a_m = a - b$, with b the measurement bias, and potentially-spoofed GPS position and velocity measurements $\boldsymbol{x}^\star = [r^\star, v^\star]^T$. The UAV's state estimator is modeled as a steady-state linear quadratic estimator

$$\frac{d}{dt}\begin{bmatrix} \hat{\boldsymbol{x}} \\ \hat{b} \end{bmatrix} = A_e \begin{bmatrix} \hat{\boldsymbol{x}} \\ \hat{b} \end{bmatrix} + L\left(\boldsymbol{x}^\star - \hat{\boldsymbol{x}}\right) + \begin{bmatrix} B \\ 0 \end{bmatrix} a_m$$

with Kalman gain matrix $L = [L_x^T, L_b^T]^T$ and

$$A_e = \begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}.$$

Let the estimation error be

$$\begin{bmatrix} \tilde{\boldsymbol{x}} \\ \tilde{b} \end{bmatrix} = \begin{bmatrix} \hat{\boldsymbol{x}} - \boldsymbol{x} \\ \hat{b} - b \end{bmatrix}$$

and let $C = \begin{bmatrix} I & 0 \end{bmatrix}$. Then the UAV estimation error dynamics are described by

$$\frac{d}{dt}\begin{bmatrix} \tilde{\boldsymbol{x}} \\ \tilde{b} \end{bmatrix} = \left(A_e - LC\right)\begin{bmatrix} \tilde{\boldsymbol{x}} \\ \tilde{b} \end{bmatrix} + L\left(\boldsymbol{x}^\star - \boldsymbol{x}\right).$$

Since (A_e, C) is an observable pair, the eigenvalues of $A_e - LC$ can be placed anywhere in the left half-plane. Let σ_x^2 and σ_v^2 be the GPS position and velocity measurement noise variance, respectively, and let

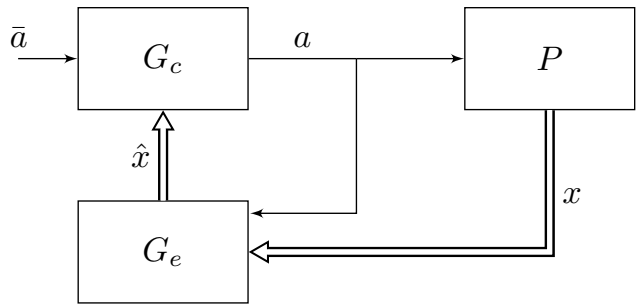

Figure 3: Block diagram of the closed-loop UAV system showing the interconnections between the UAV controller G_c, plant P, and estimator G_e. Thick lines represent vector data paths.

σ_{xv}^2 be the GPS position and velocity measurement noise covariance. Let σ_a^2 and σ_b^2 be the IMU acceleration measurement noise and bias process noise variances, respectively. The measurement and process noise matrices for the UAV estimator are then given respectively by

$$R = \begin{bmatrix} \sigma_x^2 & \sigma_{xv}^2 \\ \sigma_{xv}^2 & \sigma_v^2 \end{bmatrix} \quad Q = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \sigma_a^2 & 0 \\ 0 & 0 & \sigma_b^2 \end{bmatrix}.$$

The steady-state estimation error covariance P is the solution to the continuous algebraic Riccati equation (CARE)

$$A_e P + P A_e^T + Q - P C^T R^{-1} C P = 0$$

and the steady-state Kalman gain is $L = P C^T R^{-1}$.

The UAV's control objective is to track a prescribed reference position $\bar{r}$ and velocity $\bar{v}$ trajectory having double-integrator dynamics $\dot{\bar{\boldsymbol{x}}} = A\bar{\boldsymbol{x}} + B\bar{a}$ and state $\bar{\boldsymbol{x}} = [\bar{r}, \bar{v}]^T$, driven by a reference acceleration $\bar{a}$. The UAV's controller can be reasonably modeled as a PD compensator $a = -K(\hat{\boldsymbol{x}} - \bar{\boldsymbol{x}})$. The gain matrix $K = \begin{bmatrix} K_p & K_d \end{bmatrix} > 0$ is designed so that the closed-loop system is stable and the effect of actuator saturation is negligible. Since (A, B) is a controllable pair, the eigenvalues of $A - BK$ can be placed anywhere in the left-half plane.

The complete dynamics of the UAV system are then

$$\frac{d}{dt}\begin{bmatrix} \boldsymbol{x} \\ \hat{\boldsymbol{x}} \\ \tilde{b} \\ \bar{\boldsymbol{x}} \end{bmatrix} = \begin{bmatrix} A & -BK & 0 & BK \\ 0 & A - L_x - BK & B & BK \\ 0 & -L_b & 0 & 0 \\ 0 & 0 & 0 & A \end{bmatrix} \begin{bmatrix} \boldsymbol{x} \\ \hat{\boldsymbol{x}} \\ \tilde{b} \\ \bar{\boldsymbol{x}} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ L_x & 0 \\ L_b & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} \boldsymbol{x}^\star \\ \bar{a} \end{bmatrix}.$$

The UAV controller, plant, and estimator interconnections are represented as a block diagram in Fig. 3.

4.1.2 Spoofer Controller Design

The spoofer's control objective is to force the UAV to track some reference position $\bar{r}^s$ and velocity $\bar{v}^s$ trajectory having double-integrator dynamics $\dot{\bar{\boldsymbol{x}}}^s = A\bar{\boldsymbol{x}}^s + B\bar{a}^s$, where $\bar{\boldsymbol{x}}^s = [\bar{r}^s, \bar{v}^s]^T$, driven by a reference acceleration $\bar{a}^s$. If the UAV states could be estimated, then the spoofer could implement a full-state feedback controller. However, with typical parameters for Q and R, the state $\tilde{b}$ is nearly unobservable. Therefore, a reduced-order estimator and controller based only on estimates of the UAV's position, velocity, and acceleration is implemented to achieve the spoofer's control objective. In a later section, an estimate of $\bar{a}$ will also be incorporated into the spoofing strategy. Alternative designs to accomplish the spoofer's objectives are possible, but, to facilitate analysis, a single spoofer design is considered in this paper.

The spoofer estimates the UAV's position, velocity, and acceleration from low-rate noisy position and velocity measurements. The estimator uses a third-order model to track UAV maneuvers without bias and provide acceleration feedback. The spoofer's estimator is modeled as a steady-state linear quadratic estimator

$$\frac{d}{dt}\begin{bmatrix}\hat{\boldsymbol{x}}^s\\ \hat{a}^s\end{bmatrix} = A_e\begin{bmatrix}\hat{\boldsymbol{x}}^s\\ \hat{a}^s\end{bmatrix} + L^s\left(\boldsymbol{x}-\hat{\boldsymbol{x}}^s\right),$$

where the spoofer Kalman gain matrix $L^s = [(L_x^s)^T, (L_b^s)^T]^T$ is the solution to a CARE with appropriate process and measurement noise matrices as in the UAV model. Let $\bar{\sigma}_x^2$ and $\bar{\sigma}_v^2$ be the position and velocity measurement noise variance, respectively, and let $\bar{\sigma}_{xv}^2$ be the position and velocity measurement noise covariance. Let $\bar{\sigma}_a^2$ be the acceleration process noise variance. The measurement and process noise matrices for the spoofer estimator are then given by

$$\bar{R} = \begin{bmatrix}\bar{\sigma}_x^2 & \bar{\sigma}_{xv}^2\\ \bar{\sigma}_{xv}^2 & \bar{\sigma}_v^2\end{bmatrix}, \quad \bar{Q} = \begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & \bar{\sigma}_a^2\end{bmatrix}.$$

The steady-state spoofer estimation error covariance P^s is the solution to the CARE

$$A_e P^s + P^s A_e^T + \bar{Q} - P^s C^T \bar{R}^{-1} C P^s = 0$$

and the steady-state Kalman gain is $L^s = P^s C^T \bar{R}^{-1}$.

To constrain the dynamics of the spoofer, it is assumed that the spoofer generates physically-realizable GPS position and velocity trajectories $r^\star$ and $v^\star$ governed by double-integrator dynamics $\dot{\boldsymbol{x}}^\star = A\boldsymbol{x}^\star + Ba^\star$. The spoofer's controller can be designed as a modified PD compensator

$$a^\star = \hat{a}^s + K^s\left(\hat{\boldsymbol{x}}^s - \bar{\boldsymbol{x}}^s\right)$$

where $K^s = \begin{bmatrix}K_p^s & K_d^s\end{bmatrix}$. Although not the most general control architecture, a PD compensator is adequate and allows for a straightforward stability analysis. Unlike with the UAV controller, arbitrary choices for $K^s > 0$ will not yield a stable UAV-spoofer system. To increase the stability of the UAV-spoofer system, the measured acceleration $\hat{a}^s$ is added to $a^\star$ within the spoofer's controller, making the spoofer-simulated accelerations better match the dynamics assumed by the UAV estimator.

The complete dynamics of the spoofer system are

$$\frac{d}{dt}\begin{bmatrix}\boldsymbol{x}^\star\\ \hat{\boldsymbol{x}}^s\\ \hat{a}^s\\ \bar{\boldsymbol{x}}^s\end{bmatrix} = \begin{bmatrix}A & BK^s & B & -BK^s\\ 0 & A-L_x^s & B & 0\\ 0 & -L_b^s & 0 & 0\\ 0 & 0 & 0 & A\end{bmatrix}\begin{bmatrix}\boldsymbol{x}^\star\\ \hat{\boldsymbol{x}}^s\\ \hat{a}^s\\ \bar{\boldsymbol{x}}^s\end{bmatrix} + \begin{bmatrix}0 & 0\\ L_x^s & 0\\ L_b^s & 0\\ 0 & B\end{bmatrix}\begin{bmatrix}\boldsymbol{x}\\ \bar{a}^s\end{bmatrix}.$$

The foregoing spoofer system model assumes accurate knowledge of UAV parameters and implies a post-capture spoofing strategy that does not guarantee covertness. A more sophisticated strategy for post-capture control would be to perform online system identification to infer the parameters of the UAV's guidance, navigation, and control systems. However, for tractability, this paper only considers the aforementioned architecture, leaving more advanced attack models as an open problem.

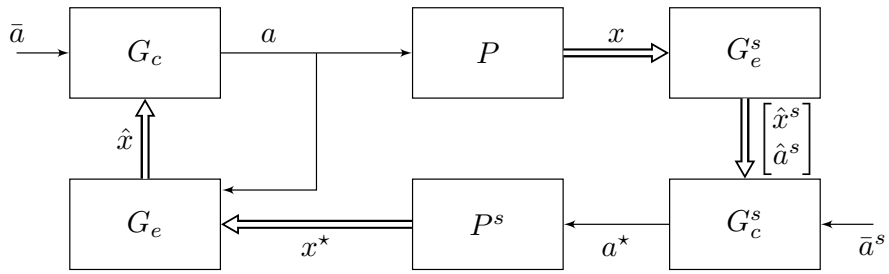

Figure 4: Block diagram of the closed-loop UAV-spoofer system showing the interconnections between the UAV controller G_c, plant P, and estimator G_e; and the spoofer controller G_c^s, plant P^s and estimator G_e^s. The spoofer plant P^s embodies the double integrator dynamics that generate $\boldsymbol{x}^\star$ from $a^\star$. Thick lines represent vector data paths.

4.1.3 Stability Analysis

The coupled dynamics of the UAV and spoofer systems are given by

$$\frac{d}{dt}\begin{bmatrix}\boldsymbol{x}\\ \hat{\boldsymbol{x}}\\ \tilde{b}\\ \bar{\boldsymbol{x}}\\ \boldsymbol{x}^\star\\ \hat{\boldsymbol{x}}^s\\ \hat{a}^s\\ \bar{\boldsymbol{x}}^s\end{bmatrix} = \begin{bmatrix} A & -BK & 0 & BK & 0 & 0 & 0 & 0\\ 0 & A-L_x-BK & B & BK & L_x & 0 & 0 & 0\\ 0 & -L_b & 0 & 0 & L_b & 0 & 0 & 0\\ 0 & 0 & 0 & A & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & A & BK^s & B & -BK^s\\ L_x^s & 0 & 0 & 0 & 0 & A-L_x^s & B & 0\\ L_b^s & 0 & 0 & 0 & 0 & -L_b^s & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & A \end{bmatrix}\begin{bmatrix}\boldsymbol{x}\\ \hat{\boldsymbol{x}}\\ \tilde{b}\\ \bar{\boldsymbol{x}}\\ \boldsymbol{x}^\star\\ \hat{\boldsymbol{x}}^s\\ \hat{a}^s\\ \bar{\boldsymbol{x}}^s\end{bmatrix} + \begin{bmatrix}0 & 0\\ 0 & 0\\ 0 & 0\\ B & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & B\end{bmatrix}\begin{bmatrix}\bar{a}\\ \bar{a}^s\end{bmatrix}$$

which can be written compactly as $\dot{\boldsymbol{z}} = M\boldsymbol{z} + N\boldsymbol{u}$. The interconnections between the UAV controller, plant, and estimator and the spoofer controller, plant, and estimator are represented as a block diagram in Fig. 4. Note that poles at the origin associated with states $\bar{\boldsymbol{x}}$ and $\bar{\boldsymbol{x}}^s$ do not affect the stability of the closed-loop system. To see this, consider a state transformation

$$\bar{\boldsymbol{z}} = \left[\begin{array}{c}\bar{\boldsymbol{x}}\\ \bar{\boldsymbol{x}}^s\\ \hline \bar{\boldsymbol{x}}-\hat{\boldsymbol{x}}\\ \hat{\boldsymbol{x}}-\boldsymbol{x}^\star\\ \tilde{b}\\ \bar{\boldsymbol{x}}^s-\hat{\boldsymbol{x}}^s\\ \hat{\boldsymbol{x}}^s-\boldsymbol{x}\\ \hat{a}^s\end{array}\right] = T\boldsymbol{z}$$

where

$$T = \left[\begin{array}{cccccccc} 0 & 0 & 0 & I & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I\\ \hline 0 & -I & 0 & I & 0 & 0 & 0 & 0\\ 0 & I & 0 & 0 & -I & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -I & 0 & I\\ -I & 0 & 0 & 0 & 0 & I & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right].$$

The dynamics of the transformed system are

$$\begin{aligned}\dot{\bar{\boldsymbol{z}}} &= TMT^{-1}\bar{\boldsymbol{z}} + TN\boldsymbol{u}\\ &= \bar{M}\bar{\boldsymbol{z}} + \bar{N}\boldsymbol{u}\end{aligned} \tag{1}$$

where

$$\bar{M} = \left[\begin{array}{cc|cccccc} A & 0 & & & & & & \\ 0 & A & & & & & & \\ \hline & & A-BK & L_x & -B & 0 & 0 & 0 \\ & & BK & A-L_x & B & BK^s & 0 & -B \\ & & 0 & -L_b & 0 & 0 & 0 & 0 \\ & & 0 & 0 & 0 & A & L_x^s & -B \\ & & -BK & 0 & 0 & 0 & A-L_x^s & B \\ & & 0 & 0 & 0 & 0 & -L_b^s & 0 \end{array}\right]$$

and

$$\bar{N} = \left[\begin{array}{cc} B & 0 \\ 0 & B \\ \hline B & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & B \\ 0 & 0 \\ 0 & 0 \end{array}\right].$$

As is evident in the structure of $\bar{M}$, the transformed system can be decoupled into dynamics governing the evolution of the reference trajectories and error states. The subsystem associated with the error states must be stable for effective UAV control. A brute-force grid search has been used to find spoofer gain matrices K^s that yield stable systems (system for which all poles of the error state subsystem are in the left-half plane). The stable region changes with different system parameters (L, K, L^s) as shown in Figs. 5 and 6. Increasing the IMU bias process noise variance σ_b generally decreases the dominant time constant of the system. For robust control, the spoofer gain should be chosen so that the system is stable over a range of expected parameter values.

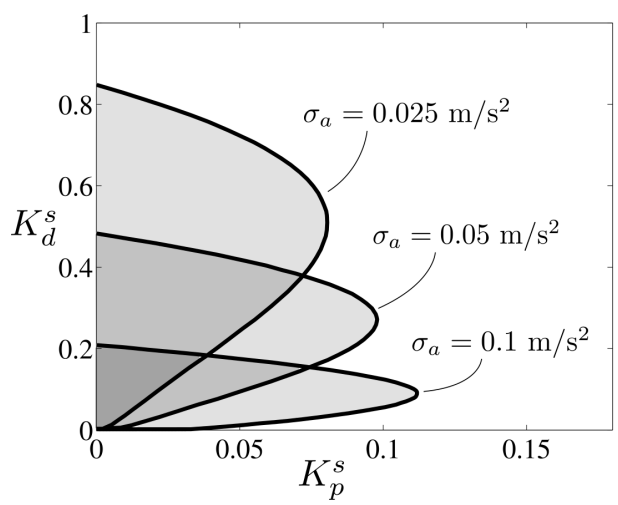

Figure 5: Decreasing the accelerometer measurement noise standard deviation σ_a increases the size of the stable region, represented in gray. Other parameters are fixed to $K_p = 1$ Hz^2, $K_d = 2$ Hz, $\sigma_x = 2$ m, $\sigma_v = 0.3$ m/s, $\sigma_{xv} = 0$, $\sigma_b = 1.24 \times 10^{-5}$ m/s^3, $\bar{\sigma}_x = 2$ m, $\bar{\sigma}_v = 0.3$ m/s, $\bar{\sigma}_{xv} = 0$, and $\bar{\sigma}_a = 0.5$ m/s^2.

4.1.4 Steady-State Performance

Using the previously-derived closed-loop dynamics, the steady-state behavior of the UAV-spoofer system can be summarized by the spoofer's position tracking error, defined as $e_r(t) = r(t) - \bar{r}^s(t)$. If $\bar{a}_L = \lim_{t\to\infty} \bar{a}(t)$

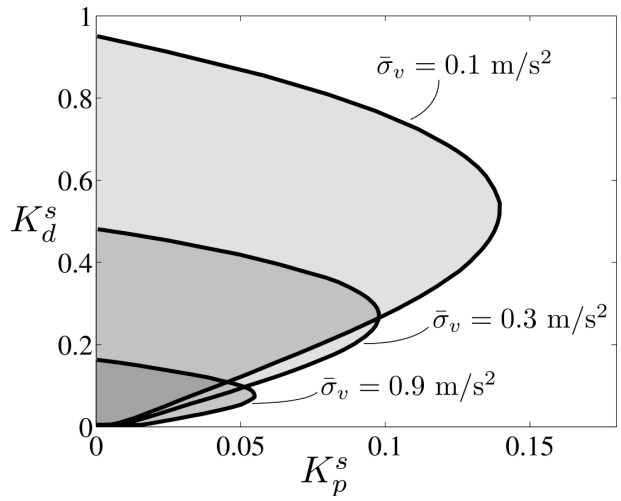

Figure 6: Increasing the spoofer velocity measurement noise standard deviation $\bar{\sigma}_v$ decreases the size of the stable region, represented in gray. Other parameters are fixed to $K_p = 1$ Hz^2, $K_d = 2$ Hz, $\sigma_x = 2$ m, $\sigma_v = 0.3$ m/s, $\sigma_{xv} = 0$, $\sigma_a = 0.05$ m/s^2, $\sigma_b = 1.24 \times 10^{-5}$ m/s^3, $\bar{\sigma}_x = 2$ m, $\bar{\sigma}_{xv} = 0$, and $\bar{\sigma}_a = 0.5$ m/s^2.

and $\bar{a}_L^s = \lim_{t\to\infty} \bar{a}^s(t)$, then the steady-state performance of the spoofer is

$$\lim_{t\to\infty} e_r(t) = \frac{1}{K_p^s}\left(\bar{a}_L^s - \bar{a}_L\right).$$

Thus, in steady-state, the tracking error is proportional to the relative acceleration of the spoofer and UAV reference trajectories. Furthermore, if $\bar{a}$ is predictable to the spoofer, $\bar{a}^s$ may be adjusted to minimize $\bar{a} - \bar{a}^s$ and thereby reduce the spoofer's tracking error. It is worth noting that, although this result only explicitly includes K_p^s, it assumes that other system parameters are known to the spoofer.

4.1.5 Covertness Test

It is assumed that, during post-capture control, the tracking loops of the target GPS receiver have been captured and have sufficient bandwidth to handle the dynamics imposed. In this case, the spoofer can covertly retain control over the tracking loops by introducing a common time offset in the simulated signals, which ensures there is negligible autocorrelation distortion due to interaction with the authentic signals. Thus, covertness during post-capture control is solely determined by innovations testing within the UAV's navigation state estimator.

As in Sec. 3.2.3, NIS is the metric used in innovations testing and is defined as NIS $\triangleq \boldsymbol{\nu}^T S^{-1}\boldsymbol{\nu}$, where $\boldsymbol{\nu} \in \mathbb{R}^{n_z}$ is the measurement innovation and $S \in \mathbb{R}^{n_z \times n_z}$ is the innovation covariance (Bar-Shalom et al., 2001). Under spoof-free conditions, the NIS at each filter iteration has a chi-squared distribution with n_z degrees of freedom.

The following section will perform innovations testing on the entire measurement vector. But to simplify analysis, this section will make claims using a simplified single-input, single-output (SISO) system. Consider NIS$_v$, the normalized innovation squared for a scalar velocity measurement only:

$$\text{NIS}_v \triangleq \nu_v^T S_v^{-1} \nu_v = \frac{\nu_v^2}{S_v},$$

where $\nu_v \in \mathbb{R}$ is the velocity measurement innovation and $S_v \in \mathbb{R}$ is the element of the innovation covariance matrix corresponding to the velocity innovation. For the nominal system parameters considered in this section, the UAV state estimator has low covariance on the velocity state, leading to innovations testing

that is more sensitive to velocity innovations than position innovations. Since in this case NIS $\approx$ NIS$_v$, velocity-only innovations testing provides a reasonable approximation of the full covertness test.

In this subsection, the attack is presumed covert if NIS$_v$ remains below the hypothesis testing threshold λ_v, that is, if $\text{NIS}_v^\star \triangleq \sup_t \text{NIS}_v(t) < \lambda_v$. Since the measurement innovation under test has only a single element, the threshold can be set as $\lambda_v = F^{-1}(1 - P_{fa})$, where $F(\cdot)$ is the cumulative distribution function (CDF) of a chi-squared distribution with one degree of freedom and P_{fa} is the desired false alarm probability. For a 5-σ hypothesis test, $\lambda_v \approx 26.3$.

To facilitate analysis, the transformed coupled dynamics of the UAV spoofer in Eq. 1 will be modified by ignoring various inputs and outputs in order to yield a tractable SISO version of the system. Two representative cases for the spoofer's control objective will be considered in order to define corresponding bounds on NIS$_v$, the output of the SISO system. A stable spoofer controller $K^s = [0.01 \;\; 0.1]$ is chosen and the remaining parameters are set to the same values used in Sec. 4.1.3: $K_p = 1$ Hz^2, $K_d = 2$ Hz, $\sigma_x = 2$ m, $\sigma_v = 0.3$ m/s, $\sigma_{xv} = 0$, $\sigma_b = 1.24 \times 10^{-5}$ m/s^3, $\sigma_a = 0.05$ m/s^2, $\bar{\sigma}_x = 2$ m, $\bar{\sigma}_v = 0.3$ m/s, $\bar{\sigma}_{xv} = 0$, and $\bar{\sigma}_a = 0.5$ m/s^2.

One input-output bound for a LTI system is (Fadali and Visioli, 2013)

$$||\boldsymbol{y}||_\infty \leq ||H||_\infty ||\boldsymbol{u}||_\infty$$

for input $\boldsymbol{u}$, output $\boldsymbol{y}$, and impulse response matrix H. Applying this input-output bound,

$$\text{NIS}_v^\star \leq \frac{1}{S_v} ||H||_\infty^2 ||\bar{a}||_\infty^2.$$

Case 1: Let $\bar{a}^s$ be zero, so that the spoofer's control objective is constant-velocity. Denote the resulting simplified SISO system as $H_{\nu,1}$. In order to guarantee covertness, the following condition must be satisfied: $\frac{1}{S_v}||H_{\nu,1}||_\infty^2 ||\bar{a}||_\infty^2 < \lambda_v$. For the nominal system parameters considered in this section, $\frac{1}{S_v}||H_{\nu,1}||_\infty^2 \approx 479$. Thus, $||\bar{a}||_\infty < 0.23$ m/s^2 implies covertness against a 5-σ hypothesis test.

Case 2: A so-called acceleration-matched (AM) control objective can be implemented such that the spoofer controller tracks only the constant-velocity portion of the original objective. To achieve an AM trajectory, let $\bar{a}^s = \bar{a}$, so that the spoofer's reference acceleration matches that of the UAV. Denote the resulting simplified SISO system as $H_{\nu,2}$. In order to guarantee covertness, the following condition must be satisfied: $\frac{1}{S_v}||H_{\nu,2}||_\infty^2 ||\bar{a}||_\infty^2 < \lambda_v$. For the nominal system parameters considered in this section, $\frac{1}{S_v}||H_{\nu,2}||_\infty^2 \approx 104$. Thus, $||\bar{a}||_\infty < 0.50$ m/s^2 implies covertness against a 5-σ hypothesis test.

The stated limits on $||\bar{a}||_\infty$ which guarantee covertness are quite low, but they follow from that strict policy that an attack in which NIS exceeds the 5-σ detection threshold very briefly is declared overt. Any parameter values, including the spoofer's controller gains, that are selected in this section can be modified and the resulting values of S_v, $||H_{\nu,1}||_\infty$, and $||H_{\nu,2}||_\infty$ used to determine new $||\bar{a}||_\infty$ limits.

4.2 Simulation of Post-Capture Control

Discrete-time simulation of post-capture UAV control has been performed at an update rate of 10 Hz to analyze the coupled dynamics of the UAV and spoofer in the presence of noise. Simple models are used with realistic noise variances for microelectromechanical (MEMS) accelerometers and modern commercial GPS receivers. Importantly, the spoofer is assumed to make position and velocity measurements of the UAV with the same position and velocity accuracy as the UAV's GPS receiver. The simulation assumes that the UAV operates in a horizontal plane and that the two horizontal directions have independent dynamics. The simulation closely follows the system model in Sec. 4.1 except that the simulated spoofer employs a more sophisticated UAV tracking filter. Parameter values are the same as those in Sec. 4.1 where applicable.

4.2.1 UAV Implementation

The simulated UAV state estimator is a Kalman filter that ingests GPS measurements and biased accelerometer measurements and estimates the state vector $\boldsymbol{x} = [\boldsymbol{r}^T, \boldsymbol{v}^T, \boldsymbol{b}^T]^T$, where $\boldsymbol{r}$ is the two-dimensional positions, $\boldsymbol{v}$ is the two-dimensional velocity, and $\boldsymbol{b}$ is the accelerometer bias state. The position, velocity, and acceleration measurements are each corrupted by zero-mean Gaussian noise with intensities $\sigma_x = 2$ m, $\sigma_v = 0.3$ m/s, and $\sigma_a = 0.05$ m/s^2, respectively. The simulated UAV controller is the PD compensator $K = [1 \;\; 2]$ in each dimension and tracks a reference trajectory by issuing acceleration commands $\boldsymbol{u}$. It is assumed that the UAV controller internally compensates for the actuator dynamics so that the acceleration commands are perfectly achieved. The UAV's position and velocity states evolve as a discrete-time double integrator on the acceleration input from the actuators. The accelerometer bias is simulated as a discrete-time Wiener process with independent increment intensity $\sigma_b = 1.24 \cdot 10^{-5}$ m/s^2.

4.2.2 Spoofer Implementation

The spoofer tracks the UAV position, velocity, and acceleration with a generalized pseudo-Bayesian estimator of the second order (GPB2), a multiple-model filter that is well-suited for tracking maneuvering targets (Bar-Shalom et al., 2001). The GPB2 estimator assumes two modes for the UAV: (1) non-maneuvering, wherein the UAV process model is driven by white acceleration noise, and (2) maneuvering, wherein the UAV process model is driven by Wiener acceleration noise. GPS spoofing causes the UAV's estimator to produce an erroneous estimate of accelerometer bias, an effect that can be approximately modeled as a Wiener process. The GPB2 estimator uses two models for the UAV motion that reflect the cumulative effect of maneuvering and erroneous bias estimates. These models are both driven by Wiener process accelerations, but with different intensities.

The spoofer controller that produces $\boldsymbol{a}^\star$ is implemented as a PD compensator with chosen gain $K^s = [0.01 \;\; 0.1]$, which is within the stability region found in Sec. 4.1.3. The spoofer plant is implemented as a discrete-time double integrator on the output of the spoofer controller. It is assumed that the spoofer can produce simulated signals that result in GPS measurements at the UAV equal to the output of the spoofer plant. The processing delay within the spoofer is presumed to be zero and the 10 Hz spoofer updates are synchronized with the 10 Hz controller updates in the UAV.

4.2.3 Post-Capture Control Simulation Results

Let the acceleration driving the UAV reference trajectory $\bar{\boldsymbol{a}}(t)$ be such that a square trajectory is formed with 100 m sides. On each side, the resulting reference trajectory velocity ramps from zero to a maximum velocity of 5 m/s, remains at a constant velocity, and then ramps down to zero. Let the acceleration driving the spoofer reference trajectory $\bar{\boldsymbol{a}}^s(t)$ be an impulse that causes the spoofer reference trajectory to move at a constant velocity of 2 m/s in the east-southeast direction. This trajectory will be referred to as the raw spoofer reference trajectory.

Figure 7 shows the two-dimensional position of the UAV, the estimate from the UAV's estimator, and the two reference trajectories. The spoofer is able to quickly move the UAV away from the UAV reference trajectory. Note that the output of the UAV's estimator remains near the UAV reference trajectory. The acceleration of the UAV reference trajectory appears to the spoofer as a disturbance which prevents the spoofer's controller from driving its tracking error to zero.

Figure 8 compares the NIS at each sample to the 2-σ and 5-σ thresholds. Since many samples are well above the 5-σ threshold, it is expected that a fault detection algorithm, even if very conservative, would trigger upon this type of attack. Thus, the dynamics of Fig. 7 lead to overt post-capture control.

In the foregoing simulation, the spoofer controller attempts to drive $\boldsymbol{x} - \bar{\boldsymbol{x}}^s$ to zero. However, the spoofer

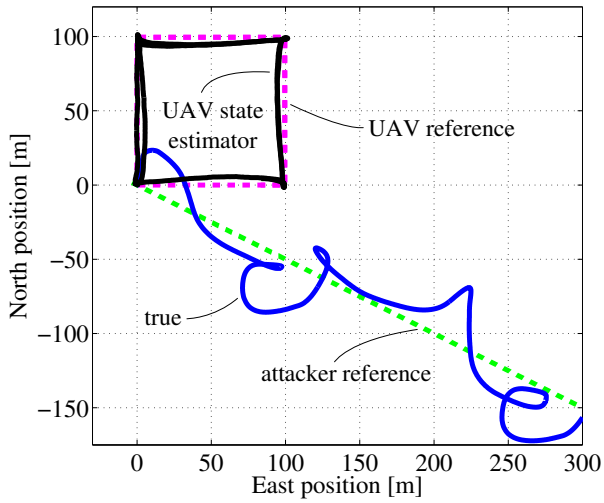

Figure 7: Position during post-capture control for square UAV reference trajectory and raw spoofer reference trajectory. The UAV tracks the spoofer reference trajectory, but position tracking errors are significant.

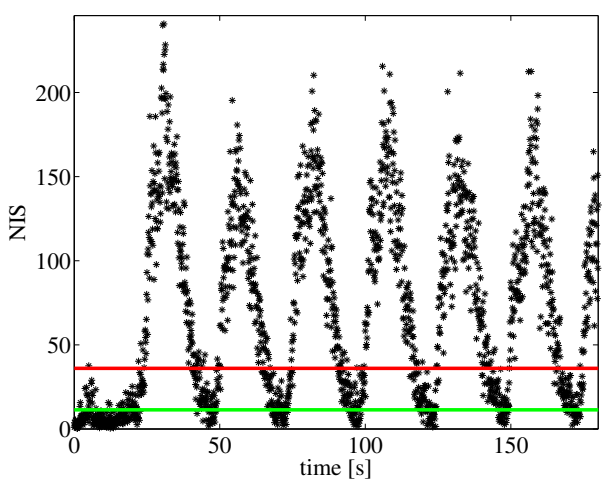

Figure 8: NIS reported by UAV state estimator for square UAV reference trajectory and raw spoofer reference trajectory. Thresholds for 2-sigma and 5-sigma hypothesis testing are drawn. Since the NIS exceeds the thresholds, the attack is declared overt.

may wish to relax this control objective to improve covertness. As introduced in Sec. 4.1.5, an acceleration-matched control objective can be implemented such that the spoofer controller tracks only the large-scale behavior of $\bar{\boldsymbol{x}}^s$ whereas on a smaller scale it mimics the UAV reference trajectory. Specifically, an AM reference trajectory is defined as $\bar{\boldsymbol{a}}^s_{\mathrm{AM}}(t) \triangleq \bar{\boldsymbol{a}}^s(t) + \bar{\boldsymbol{a}}_e(t)$ where $\bar{\boldsymbol{a}}_e(t)$ is the spoofer's estimate of the UAV reference trajectory by either (1) observing one or more cycles of a repeating trajectory, or (2) on-the-fly learning.

The same simulation reported in Figs. 7-8 has been repeated with the AM reference trajectory, assuming that the spoofer has a perfect estimate $\bar{\boldsymbol{a}}_e(t) = \bar{\boldsymbol{a}}(t)$ of the UAV reference trajectory. As seen in Fig. 9, the spoofer is able to force the UAV to closely track the AM reference trajectory. Importantly, this change in spoofer reference trajectory allows post-capture control to proceed covertly. In Fig. 10, none of the NIS samples exceed the 5-σ threshold.

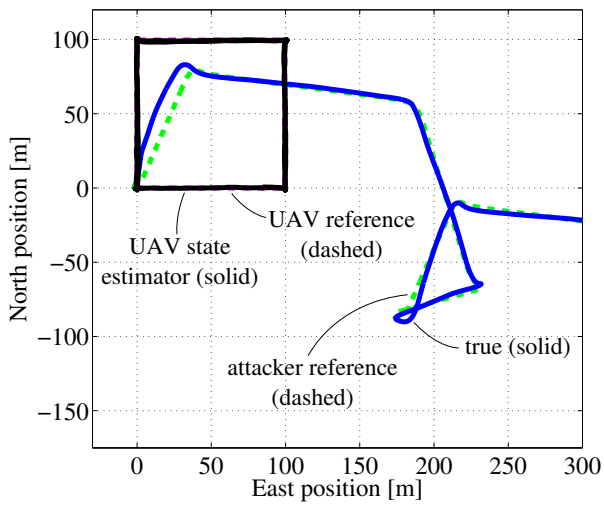

Figure 9: Position during post-capture control for square UAV reference trajectory and AM spoofer reference trajectory. The UAV tracks the AM spoofer reference trajectory with small position tracking errors.

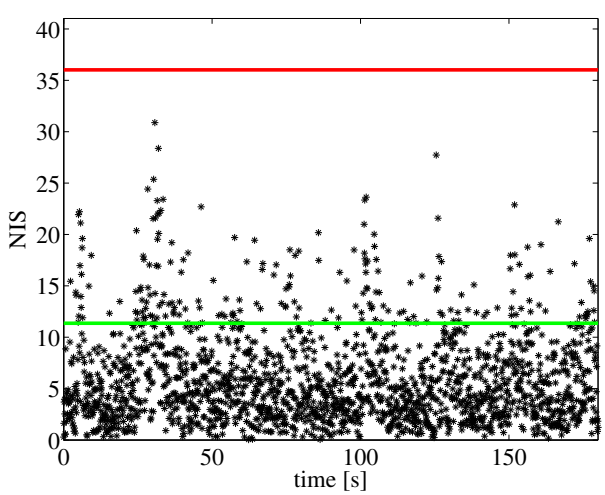

Figure 10: NIS reported by UAV state estimator for a square UAV reference trajectory and AM spoofer reference trajectory. Thresholds for 2-sigma and 5-sigma hypothesis testing are drawn. Since the NIS does not exceed the 5-sigma threshold, the attack is declared covert.

5 Field Demonstration

It would be challenging to perform an experiment validating all results in Sec. 4. Such an experiment would require real-time UAV PV tracking, a heavy burden for researchers and potential attackers alike. Further, the hypothetical experiment would require over-the-air transmission in protected frequency bands and thus would violate the regulations pertaining to those frequency bands unless government permission was granted. Due to these limitations, the field demonstration reported herein does not validate all of the modeling and analysis in this paper; rather, this section reports an overt spoofing attack against a UAV in which the spoofer briefly exerted control authority over the target using an open-loop control strategy, without any feedback on the true position and velocity of the UAV. The demonstration is a simple special case of the capture scenarios that were investigated analytically and via simulation in the foregoing sections. Importantly, the demonstration proves that navigation system capture and control sufficient to cause a UAV to crash is in fact possible in the field.

The GPS spoofing experiment reported briefly in (Shepard et al., 2012a), which used the same spoofer and target UAV as this paper's experiment, demonstrated an effective over-the-air spoofing attack. The trial occurred in June 2012 at White Sands Missile Range during an exercise overseen by the U.S. Department of Homeland Security. In that test, simulated GPS signals were transmitted over the air from a distance of approximately 620 m. The target aircraft was hovering approximately 12 m above ground level when the spoofer captured its navigation system. The spoofer then induced the captured GPS receiver to produce position and velocity solutions that falsely indicated the UAV was moving upward. As a result, the UAV moved downward to correct for its apparent deviation from the commanded hover position. Since the spoofer was performing open-loop control of the captured UAV, the UAV's downward motion was only arrested when a safety pilot took over manual control of the aircraft. A video of the over-the-air test is available at `http://radionavlab.ae.utexas.edu/spoofing/drone-capture-testimony-video`.

Although it offered a valuable and unprecedented demonstration, the over-the-air spoofing experiment at White Sands failed to capture any other than video data. Thus, to experimentally validate portions of this paper's modeling and analysis, a new experiment was conducted in June 2013 near Austin, Texas. In the new experiment, data were continuously recorded from the target UAV's GPS receiver and state estimator during the spoofing attack. To avoid unauthorized radio transmission in the protected GPS band, the spoofing signals were directly injected via a lightweight coaxial cable into the UAV's GPS antenna, where they combined with authentic GPS signals from overhead satellites. In both the former over-the-air trial and in this paper's cabled experiment, the UAV behaved as the foregoing analysis would predict for capture and open-loop control.

5.1 Setup

The target aircraft, a Hornet Mini UAV from Adaptive Flight Incorporated, is a 4.5-kg helicopter with an advanced avionics system. The Hornet Mini's navigation sensor suite comprises an IMU, magnetometer, baro-altimeter, and ublox GPS receiver. Its navigation state estimator is implemented as an extended Kalman filter (EKF). The EKF ignores direct GPS altitude measurements, relying instead on the baro-altimeter, but the GPS receiver still influences the altitude estimate through its vertical velocity measurements.

The portable software-defined GPS spoofer used for the experiment was reported originally in (Humphreys et al., 2008). Further development has been reported in (Shepard et al., 2012b, Shepard et al., 2012a) and (Humphreys et al., 2012). In the limit of a perfectly-known $\Delta \boldsymbol{r}_t$ (cf. Fig. 1) the spoofer is capable of generating simulated GPS signals that align to meter and deci-Hz levels with the authentic signals at the antenna of the target receiver. The spoofer hardware and target RUAV are shown in Fig. 11.

During normal operation, the Hornet Mini accepts high-level input from a human operator in the form of velocity commands that modify the reference trajectory on-the-fly. The Hornet Mini has a special operating mode in which a human operator assists the UAV so that prolonged operation is possible without GPS

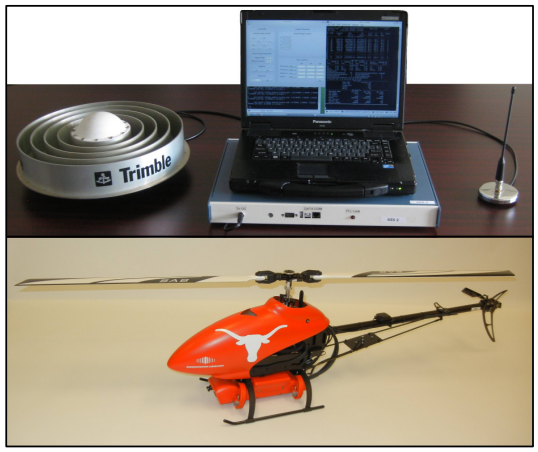

Figure 11: Spoofer hardware and target RUAV.

measurements (e.g., during GPS signal blockage). In this mode, referred to as GPS-denied mode, two significant changes occur with respect to the normal operating mode. First, the Hornet Mini's EKF entirely ignores GPS measurements for estimating the vehicle's state. Second, the Hornet Mini changes how it accepts high-level control input from the human operator so that the operator can counteract the drift that occurs in the navigation system during GPS-denied operation: whereas the UAV accepts velocity commands during GPS-based navigation, it accepts acceleration commands while in GPS-denied mode.

In the field demonstration, a human operator overseeing the Hornet Mini via video feed and visual line-of-sight instructed the UAV to maintain hover at a specified waypoint and then waited until the spoofing attack began. Once the operator witnessed the spoofer-induced maneuver, he swiftly took the corrective action of placing the Hornet Mini in GPS-denied mode. Thus, this experiment tested GPS-denied mode as a spoofing defense against an overt attacker.

5.2 Results

The attack began with the target aircraft hovering at a waypoint 8.8 m above ground level. The spoofer then began transmitting simulated GPS signals with a power level chosen such that $\eta = 10$ dB. The spoofer's initial induced position coincided with the UAV's hover position, which was known to the spoofer. Upon transmitting these signals, the spoofer captured the target GPS receiver, gaining control of its reported position and velocity measurements, but did not immediately attempt to alter these measurements from the nominal hovering position. Therefore, the condition $\boldsymbol{x}^\star \approx \boldsymbol{x}$ held during, and immediately after, receiver capture.

Post-capture, the spoofer controlled the UAV by inducing the captured GPS receiver to produce position and velocity solutions that indicated the UAV was moving southward. The UAV responded rapidly by moving northward. The effect of the attack is summarized in Fig. 12, which shows the north position from four sources: the spoofer's output, the GPS receiver on the UAV, the EKF on the UAV, and the truth trajectory, as reconstructed from pre- and post-attack onboard GPS measurements and observed movement during the experiment.

At $t = 0$, the spoofer begins transmission of simulated GPS signals to induce $\boldsymbol{x}^\star \approx \boldsymbol{x}$. The spoofer output is expressed in a north-east-down coordinate frame with origin at the UAV hover point $\boldsymbol{x}(0)$, with non-zero output only in the north direction. The spoofer's open-loop control law was $\boldsymbol{x}^\star(t) = [r_N^\star(t) \;\; 0 \;\; 0 \;\; v_N^\star(t) \;\; 0 \;\; 0]^T$

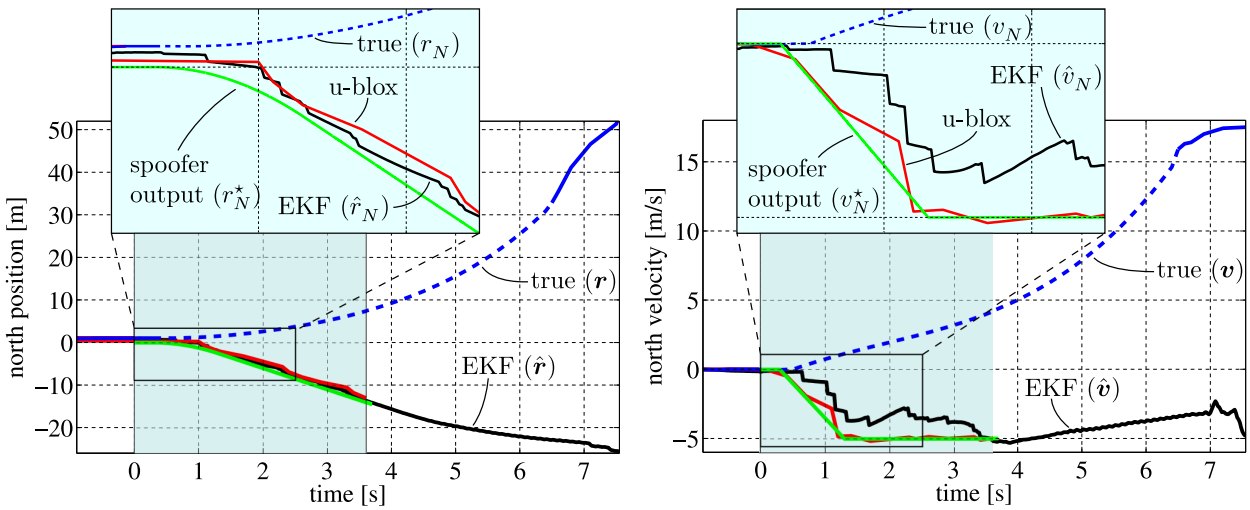

Figure 12: North position and velocity during the cabled test of UAV capture and open-loop control; where pre- and post-attack GPS data are unavailable, dotted lines indicate an interpolation based on measurement boundary constraints and observed movement during the experiment. The shaded region, $0 \leq t \leq 3.6$, indicates when the spoofer was transmitting simulated signals and the UAV was using GPS measurements for navigation.

for $0 \leq t \leq 3.8$, where

$$v_N^\star(t) = \begin{cases} 0 & 0 \leq t \leq 0.3 \\ -5(t-0.2) & 0.3 < t \leq 1.3 \\ -5 & 1.3 < t \leq 3.8 \end{cases}$$

$$r_N^\star(t) = \int_0^t v_N^\star(\tau) d\tau.$$

At $t = 0.3$ seconds, the spoofer begins to modulate $\boldsymbol{x}^\star$, moving it due south within an acceleration limit of 5 m/s^2 and a velocity limit of 5 m/s. As seen in Fig. 12, the EKF output follows the GPS measurements from the captured receiver and begins to move south at 5 m/s. Due to the apparent deviation of the UAV's position and velocity from the desired flight plan, the UAV controller commands a powerful northward movement. The spoofer's capture and control actions were overt according to the definitions in Secs. 3.2 and 4.1.5. Nonetheless, the the attack went undetected because the UAV's GPS receiver and navigation system were not designed with even rudimentary checks against spoofing.

At $t = 3.6$ seconds, action to wrest control from the spoofer is taken: the UAV is commanded by the human operator to enter GPS-denied mode, where GPS measurements are ignored by the UAV's EKF. After this point, the spoofer no longer has any control authority over the UAV; however, the effects of previous false measurements persist because the existing, erroneous UAV state estimate continues to propagate in the EKF according to its dynamics model. In an approximate sense, the dynamics model assumes constant-velocity motion. Thus, the velocity estimate injected by the spoofer persists, as clearly observed in the EKF output continuing south at nearly 5 m/s. Since at this point the UAV is moving north rapidly while the velocity estimate remains approximately constant, the absolute error of the velocity estimate exceeds 5 m/s and is quickly increasing.

Upon entering GPS-denied mode, the operator immediately commands the Hornet Mini to accelerate southward. However, since GPS-denied mode was only designed to counteract natural drift in the navigation system, the operator does not have sufficient control authority to halt the lingering effects of the spoofing

attack, which are far more severe than natural drift. At the moment GPS-denied mode is entered, the absolute error in the UAV's north velocity estimate is $|\hat{v}_N - v| \approx 8$ m/s and growing rapidly. Given enough unobstructed airspace, the operator could have brought even this large velocity error to zero by commanding a counteracting acceleration, but the close experimental conditions required by the cabled attack did not afford sufficient airspace.

At $t = 3.8$ seconds, the UAV's true northward motion causes the cable to separate from the UAV. From $t = 3.8$ to $t = 6.5$ seconds, the UAV's GPS receiver undergoes trauma owing to the sudden switch from tracking spoofer-generated GPS signals to authentic GPS signals. The position reported during this transient period is omitted in Fig. 12. After $t = 6.5$ seconds, the UAV's GPS receiver begins accurately reporting the UAV's true position. But at this point, the UAV is moving rapidly northward and losing altitude because the lack of proper velocity feedback gives rise to an extreme true velocity—approximately 17 m/s—that violates the assumptions of the UAV's attitude control loop. Shortly thereafter, the UAV crashes.

As a result of the state estimation errors forced by the spoofer, the UAV's accelerometer bias estimates change significantly during the experiment, commensurate with the UAV model in Sec. 4.1.1. However, the erroneous estimate of accelerometer drift is not large enough to explain the surprisingly attenuated evolution of the UAV's velocity estimate $\hat{v}_N$ between $t = 4$ seconds and $t = 6$ seconds, which, in the absence of accelerometer bias errors, would assume the shape of the actual velocity trajectory. The answer to this puzzle may lie in the UAV's attitude estimation errors, which misdirect a large fraction of the true northward acceleration to the UAV's vertical coordinate, which is strongly constrained by the baro-altimeter.

6 Discussion

The preceding analysis and demonstration show that overt methods for UAV capture and control are practical to implement today while covert methods are significantly more challenging for a potential attacker. It is worth noting that for the vast majority of currently-available commercial GPS receivers and UAV navigation systems, covert capture is synonymous with overt capture. For example, the post-capture control of the UAV in the field demonstration of Sec. 5 was overt by the standards of this paper; however, the attack was not detected by the victim GPS receiver or UAV.

One additional challenge of covert capture was ignored in Sec. 3, where it was presumed that the spoofer can control the received simulated signal power at the target by setting its own transmit power. In practice, the effect of body shadowing on the signal power received by an aircraft-mounted GPS antenna is significant for large aircraft (Rao et al., 2006). For small aircraft and certain antenna mounting positions, body shadowing becomes negligible, but the effect of the antenna gain pattern remains significant. If the spoofer is operated from a low elevation angle as seen by the target platform, typical GPS antennas will attenuate the simulated signals. A low-elevation spoofer can increase its transmit power to compensate for this attenuation, but without *a priori* knowledge of the antenna gain pattern, which is specific to the antenna model and mounting location, the spoofer must accept a large uncertainty in the low-elevation attenuation. And even with such knowledge, the attenuation is highly sensitive to changes in elevation angle, resulting in significant residual uncertainty. These effects ensure that a ground-based spoofer will find it difficult to precisely specify the power advantage η of the received spoofing signals.

To the knowledge of the authors, all modern commercial civil GPS receivers, even those which provide high-integrity measurements, are vulnerable to civil GPS spoofing. Thus, the techniques presented in this paper are broadly applicable to unmanned aircraft that are operating autonomously or semi-autonomously and are dependent on civil GPS signals for navigation. Aircraft navigation systems may employ high-performance inertial sensors, but for flights of significant duration, GPS measurements are necessary to avoid drift in a navigation solution dependent on strictly non-GPS measurements. Thus, low-but-nonzero drift sensors weaken the control authority possible with a GPS spoofing attack, but do not prevent such an attack.

7 Conclusions

An attacker who controls critical sensor measurements made by an autonomous system has great authority over that system. In this paper, the capability of an attacker transmitting falsified GPS signals to influence the behavior of an autonomous UAV was explored.

The requirements for overt and covert capture of a UAV's navigation system have been presented together with results from live tests of spoofing attacks against several commercial GPS receivers. By subjecting these commercial receivers to repeated spoofing attacks at various spoofing power advantage factors η, it was concluded that if the spoofer's estimation errors of the UAV position and velocity are below 50 m and 10 m/s, respectively, the spoofer is capable of reliable and covert capture of the target receiver's tracking loops.

A spoofer's post-capture control authority over a target UAV was explored using simplistic models for the UAV state estimator, plant, and controller dynamics. By analysis of the coupled dynamics of the UAV and spoofer, it was shown that a GPS spoofing attack can force a UAV to unknowingly follow a trajectory imposed by the spoofer. A strict upper bound on the magnitude of the UAV's reference acceleration trajectory was shown to result in the example spoofer design passing a covertness test based on innovations testing.

Finally, a field test showed that a destructive GPS spoofing attack against a rotorcraft UAV is both technically and operationally feasible. The demonstration is a proof-of-concept for a simple special case within the broad class of GPS spoofing attacks against mobile targets.

References

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION, Journal of the Institute of Navigation*, 59(4):281–290.

Bachrach, A., Prentice, S., He, R., and Roy, N. (2011). RANGE–robust autonomous navigation in GPS-denied environments. *Journal of Field Robotics*, 28(5):644–666.

Bar-Shalom, Y., Li, X. R., and Kirubarajan, T. (2001). *Estimation with Applications to Tracking and Navigation*. John Wiley and Sons, New York.

Bernstein, G. M., Liberman, M., and Lichtenberg, A. J. (1989). Nonlinear dynamics of a digital phase locked loop. *IEEE Transactions on Communications*, 37(10):1062–1070.

Braasch, M. S. and Van Dierendonck, A. (1999). GPS receiver architectures and measurements. *Proceedings of the IEEE*, 87(1):48–87.

Broumandan, A., Jafarnia-Jahromi, A., Dehgahanian, V., Nielsen, J., and Lachapelle, G. (2012). GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the IEEE/ION PLANS Meeting*, Myrtle Beach, SC. Institute of Navigation.

Brown, R. G. (1996). *Global Positioning System: Theory and Applications*, volume 2, chapter 5: Receiver Autonomous Integrity Monitoring, pages 143–168. American Institute of Aeronautics and Astronautics, Washington, D.C.

Castle, R. O., Klein, G., and Murray, D. W. (2011). Wide-area augmented reality using camera tracking and mapping in multiple regions. *Computer Vision and Image Understanding*, 115(6):854–867.

Chowdhary, G., Johnson, E. N., Magree, D., Wu, A., and Shein, A. (2013). GPS-denied indoor and outdoor monocular vision aided navigation and control of unmanned aircraft. *Journal of Field Robotics*, 30(3):415–437.

Christophersen, H. B., Pickell, R. W., Neidhoefer, J. C., Koller, A. A., Kannan, S. K., and Johnson, E. N. (2006). A compact guidance, navigation, and control system for unmanned aerial vehicles. *Journal of Aerospace Computing, Information, and Communication*, 3(5):187–213.

De Lorenzo, D. S., Gautier, J., Rife, J., Enge, P., and Akos, D. (2005). Adaptive array processing for GPS interference rejection. In *Proceedings of the ION GNSS Meeting*, Long Beach, CA. Institute of Navigation.

Dehghanian, V., Nielsen, J., and Lachapelle, G. (2012). GNSS spoofing detection based on receiver C/No estimates. In *Proceedings of the ION GNSS Meeting*, Nashville, TN. Institute of Navigation.

Durrant-Whyte, H. and Bailey, T. (2006). Simultaneous localization and mapping: part I. *IEEE Robotics & Automation Magazine*, 13(2):99–110.

European Union (2010). European GNSS (Galileo) open service signal in space interface control document. Technical report, European Union. `http://ec.europa.eu/enterprise/policies/satnav/galileo/open-service/`.

Fadali, M. S. and Visioli, A. (2013). *Digital control engineering: analysis and design*. Academic Press.

Flenniken IV, W. S., Wall, J. H., and Bevly, D. M. (2005). Characterization of various IMU error sources and the effect on navigation performance. In *Proceedings of the ION ITM*, Long Beach, CA. Institute of Navigation.

Garratt, M. A. and Chahl, J. S. (2008). Vision-based terrain following for an unmanned rotorcraft. *Journal of Field Robotics*, 25(4-5):284–301.

Global Positioning System Directorate (2012). Systems engineering and integration Interface Specification IS-GPS-200G. Technical report, Global Positioning System Directorate. `http://www.gps.gov/technical/icwg/`.

Gupta, S. (1975). Phase-locked loops. *Proceedings of the IEEE*, 63(2):291–306.

Hermann, R. and Krener, A. (1977). Nonlinear controllability and observability. *IEEE Transactions on Automatic Control*, 22(5):728–740.

Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2):1073–1090.

Humphreys, T. E., Bhatti, J. A., Shepard, D. P., and Wesson, K. D. (2012). The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques. In *Proceedings of the ION GNSS Meeting*.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M. (2008). Assessing the spoofing threat: development of a portable GPS civilian spoofer. In *Proceedings of the ION GNSS Meeting*, Savannah, GA. Institute of Navigation.

Humphreys, T. E., Psiaki, M. L., and Kintner, Jr., P. M. (2010). Modeling the effects of ionospheric scintillation on GPS carrier phase tracking. *IEEE Transactions on Aerospace and Electronic Systems*, 46(4):1624–1637.

Kendoul, F. (2012). Survey of advances in guidance, navigation, and control of unmanned rotorcraft systems. *Journal of Field Robotics*, 29(2):315–378.

Kim, J. and Sukkarieh, S. (2003). A baro-altimeter augmented INS/GPS navigation system for an uninhabited aerial vehicle. In *International Symposium on Satellite Navigation Technology*, Melbourne, Australia. Australian Global Positioning Systems Society.

Ledvina, B. M., Bencze, W. J., Galusha, B., and Miller, I. (2010). An in-line anti-spoofing module for legacy civil GPS receivers. In *Proceedings of the ION ITM*, San Diego, CA. Institute of Navigation.

Lee, J. and Un, C. (1982). Performance analysis of digital tanlock loop. *IEEE Transactions on Communications*, 30(10):2398–2411.

Lindsey, W. and Chie, C. M. (1981). A survey of digital phase-locked loops. *Proceedings of the IEEE*, 69(4):410–431.

Lo, S., De Lorenzo, D. S., Enge, P., Akos, D., and Bradley, P. (2009). Signal authentication. *Inside GNSS*, 0(0):30–39.

Misra, P. and Enge, P. (2012). *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jumana Press, Lincoln, MA, revised second edition.

Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M. (2009). A multi-antenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS*, 4(2):40–46.

Nuetzi, G., Weiss, S., Scaramuzza, D., and Siegwart, R. (2011). Fusion of IMU and vision for absolute scale estimation in monocular SLAM. *Journal of Intelligent & Robotic Systems*, 61(1):287–299.

O'Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., and Humphreys, T. E. (2012). Real-time spoofing detection using correlation between two civil GPS receiver. In *Proceedings of the ION GNSS Meeting*, Nashville, TN. Institute of Navigation.

O'Hanlon, B. W., Psiaki, M. L., Powell, S. P., Bhatti, J. A., Humphreys, T. E., Crowley, G., and Bust, G. S. (2011). CASES: A smart, compact GPS software receiver for space weather monitoring. In *Proceedings of the ION GNSS Meeting*, Portland, OR. Institute of Navigation.

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., and Humphreys, T. E. (2011). Civilian GPS spoofing detection based on dual-receiver correlation of military signals. In *Proceedings of the ION GNSS Meeting*, Portland, OR. Institute of Navigation.

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., and Humphreys, T. E. (2013). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, 49(4):2250–2267.

Rao, B. R., Rosario, E. N., and Davis, R. J. (2006). Radiation pattern analysis of aircraft mounted GPS antennas and verification through scale model testing. In *Proceedings of the IEEE/ION PLANS Meeting*. Insitute of Navigation.

Sarkar, B. and Chattopadhyay, S. (1994). A new look into the acquisition properties of a second-order digital phase locked loop. *IEEE Transactions on Communications*, 42(5):2087–2091.

Shepard, D. P., Bhatti, J. A., Humphreys, T. E., and Fansler, A. A. (2012a). Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In *Proceedings of the ION GNSS Meeting*, Nashville, TN. Institute of Navigation.

Shepard, D. P. and Humphreys, T. E. (2011). Characterization of receiver response to a spoofing attack. In *Proceedings of the ION GNSS Meeting*, Portland, OR. Institute of Navigation.

Shepard, D. P., Humphreys, T. E., and Fansler, A. A. (2012b). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4):146–153.

Spilker, Jr., J. J. (1996). *Global Positioning System: Theory and Applications*, chapter 3: GPS Signal Structure and Theoretical Performance, pages 57–119. American Institute of Aeronautics and Astronautics, Washington, D.C.

Stephens, S. A. and Thomas, J. B. (1995). Controlled-root formulation for digital phase-locked loops. *IEEE Transactions on Aerospace and Electronic Systems*, 31(1):78–95.

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 75–86, Chicago, IL. Association for Computing Machinery.

Van Dierendonck, A. J. (1996). *Global Positioning System: Theory and Applications*, chapter 8: GPS Receivers, pages 329–407. American Institute of Aeronautics and Astronautics, Washington, D.C.

Ward, P. W. (1994). GPS receiver RF interference monitoring, mitigation, and analysis techniques. *NAVIGATION, Journal of the Institute of Navigation*, 41(4):367–391.

Warner, J. S. and Johnston, R. G. (2003). A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing. *Journal of Security Administration*.

Weiss, S., Scaramuzza, D., and Siegwart, R. (2011). Monocular-SLAM–based navigation for autonomous micro helicopters in GPS-denied environments. *Journal of Field Robotics*, 28(6):854–874.

Wendel, J., Meister, O., Schlaile, C., and Trommer, G. F. (2006). An integrated GPS/MEMS-IMU navigation system for an autonomous helicopter. *Aerospace Science and Technology*, 10(6):527–533.

Wesson, K. D., Evans, B. L., and Humphreys, T. (2013). A combined symmetric difference and power monitoring GNSS anti-spoong technique. In *Proceedings of the IEEE Global Conference on Signal and Information Processing*, Austin, TX. Institute of Electrical and Electronics Engineers.

Wesson, K. D., Rothlisberger, M., and Humphreys, T. E. (2012). Practical cryptographic civil GPS signal authentication. *NAVIGATION, Journal of the Institute of Navigation*, 59(3):177–193.

Wesson, K. D., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E. (2011). An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *Proceedings of the ION GNSS Meeting*, Portland, OR. Institute of Navigation.

Zhuang, W. (1996). Performance analysis of GPS carrier phase observable. *IEEE Transactions on Aerospace and Electronic Systems*, 32(2):754–767.