2020 59th IEEE Conference on Decision and Control (CDC)
Jeju Island, Republic of Korea, December 14-18, 2020

A Safety Constrained Control Framework for UAVs in GPS Denied Environment

Wenbin Wan[†], Hunmin Kim[†], Naira Hovakimyan[†], Lui Sha[*] and Petros G. Voulgaris[‡]

***Abstract*— Unmanned aerial vehicles (UAVs) suffer from sensor drifts in GPS denied environments, which can lead to potentially dangerous situations. To avoid intolerable sensor drifts in the presence of GPS spoofing attacks, we propose a safety constrained control framework that adapts the UAV at a path re-planning level to support resilient state estimation against GPS spoofing attacks. The attack detector is used to detect GPS spoofing attacks and provides a switching criterion between the robust control mode and emergency control mode. An attacker location tracker (ALT) is developed to track the attacker's location and estimate the spoofing device's output power by the unscented Kalman filter (UKF) with sliding window outputs. Using the estimates from ALT, we design an escape controller (ESC) based on the model predictive controller (MPC) such that the UAV escapes from the effective range of the spoofing device within the escape time.**

I. Introduction

UAVs have been used across the world for commercial, civilian, as well as educational applications over the decades. The mechanical simplicity and agile maneuverability appeal to many applications, such as cargo transportation, aerial photography, and agricultural farming. The most widely used sensor for UAVs is the global positioning system (GPS), which offers accurate and reliable state measurements. However, GPS receivers are vulnerable to various types of attacks, such as blocking, jamming, and spoofing [1]. The Vulnerability Assessment Team at Los Alamos National Laboratory has demonstrated that the civilian GPS spoofing attacks can be easily implemented by using GPS simulator [2]. Furthermore, GPS is more vulnerable when its signal strength is weak. Due to various applications of UAVs, the operating environment becomes diverse as well, where GPS signals are weak or even denied due to other structures such as skyscrapers, elevated highways, bridges, and mountains.

Literature review. One of the GPS spoofing attack detection techniques is to analyze raw antenna signals or utilize multi-antenna receiver systems. The GPS spoofing attack can be detected by checking whether the default radiation pattern is changed in [3]. A multi-antenna receiver system was used to detect GPS spoofing attacks by monitoring the angle-of-arrival of the spoofing attempts in [4]. As an extension of this work, the GPS spoofing mitigation has also been investigated where an array of antennas is utilized to obtain genuine GPS signals by spatial filtering [5]. However, those solutions require modifications of the hardware or the low-level computing modules and assume that an attacker can only use single-antenna spoofing systems. Furthermore, the attacker can spoof the GPS receivers without being detected if multi-antenna spoofing devices are available [6].

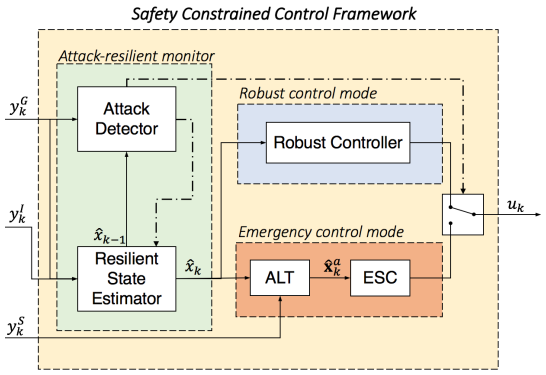


Fig. 1: A safety constrained control framework.

In the cyber-physical systems (CPS) security literature, GPS spoofing attacks have been described as a malicious signal injection to the genuine sensor output [7]. Attack detection against malicious signal injection has been widely studied over the last few years. The attack detection problem has been formulated as an ℓ_0/ℓ_∞ optimization problem, which is NP-hard in [8]. The fundamental limitations of structural detectability, as well as graph-theoretical detectability for linear time-invariant systems, have been studied in [9], where distributed attack detection has also been studied. The attack detection problem has been formulated as an attack-resilient estimation problem of constrained state and unknown input in [10]. A switching mode resilient detection and estimation framework for GPS spoofing attacks has been studied in [11]. We notice that existing emergency control architectures focus on switching control from a high-performance controller to a robust high-assurance controller in the presence of attacks [12]. These architectures can efficiently handle a class of attacks, but cannot address the fundamental problem due to limited sensor availability in the presence of cyber-attacks.

Contribution. The current paper addresses safety problems induced by limited sensor availability due to GPS spoofing attacks. We formulate the sensor drift problem as an increasing variance of state estimation to quantify the sensor drift and introduce escape time under which the state estimation error remains within a tolerable error with high confidence.

This work has been supported by the National Science Foundation (ECCS-1739732, and CMMI-1663460).

[†]Wenbin Wan, Hunmin Kim, and Naira Hovakimyan are with the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, USA. {wenbinw2, hunmin, nhovakim}@illinois.edu

[*]Lui Sha is with the Department of Computer Science, University of Illinois at Urbana-Champaign, USA. lrs@illinois.edu

[‡]Petros G. Voulgaris is with the Department of Mechanical Engineering, University of Nevada, Reno, USA. pvoulgaris@unr.edu

We develop a novel safety constrained control framework that adapts the UAV at a path re-planning level to support resilient state estimation against GPS spoofing attacks. In the presence of the GPS spoofing attack, the attacker location tracker (ALT) tracks the attacker's location and estimates the output power of the spoofing device by the unscented Kalman filter (UKF) with sliding window outputs. The estimates are then used in the escape controller (ESC) that drives the UAV away from the effective range of the spoofing device within the escape time to avoid intolerable sensor drift.

II. Preliminaries

A. Notation

We use the subscript k of x_k to denote the time index. $\mathbb{R}^n_+$ denotes the set of positive elements in the n-dimensional Euclidean space. $\mathbb{R}^{n\times m}$ denotes the set of all $n\times m$ real matrices. $A^\top$ A^{-1} and $tr(A)$ denote the transpose, inverse and trace of matrix A, respectively. I denotes the identity matrix with an appropriate dimension. $\|\cdot\|$ denotes the standard Euclidean norm. $\times$ is used to denote matrix multiplication when the multiplied terms are in different lines. $\mathbb{E}[\cdot]$ and $\mathbb{P}[\cdot]$ denote the expectation operator and the probability operator. For a matrix S, $S>0$ and $S\geq 0$ indicate that S is positive definite and positive semi-definite, respectively.

B. System Model

Consider the discrete-time dynamic system model:

$$x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1} \tag{1a}$$
$$y^G_k = C^G x_k + d_k + v^G_k \tag{1b}$$
$$y^I_k = C^I(x_k - x_{k-1}) + v^I_k \tag{1c}$$
$$y^S_k = \begin{cases} C^S \frac{\eta_k}{\mathbf{d}(x^a_k, x_k)^2} + v^S_k, & \textit{under the attack} \\ \eta^S + v^S_k, & \textit{otherwise}\ , \end{cases} \tag{1d}$$

where $x_k \in \mathbb{R}^n$ is the state, and A, B, C^G, C^I and C^S are given matrices with appropriate dimensions. Output $y^G_k \in \mathbb{R}^{m_G}$ is the GPS measurement which may be corrupted by unknown GPS spoofing signal $d_k \in \mathbb{R}^{m_G}$. The signal d_k is injected by the attacker when the UAV is in the effective range of the spoofing device. Output $y^I_k \in \mathbb{R}^{m_I}$ is the IMU measurement, which returns a noisy measurement of the state difference. Output $y^S_k \in \mathbb{R}^{m_S}$ represents the GPS signal strength. The defender is unaware of x^a_k and η_k, where $x^a_k \in \mathbb{R}^n$ is the attacker location, and $\eta_k \in \mathbb{R}^{m_S}$ is the nominal power of the spoofing device. If GPS is under the attack, y^S_k is a function of the distance between the attacker and UAV. The function $\mathbf{d}(a,b)$ measures the distance between a and b. If the UAV receives genuine GPS signals, this output represents the genuine GPS signal strength η^S. We assume that the attacker can inject any signal d_k into y^G_k. The noise w_k, v^G_k, v^I_k, and v^S_k are assumed to be i.i.d. Gaussian random variables with zero means and covariances $\mathbb{E}[w_k w_k^\top] = \Sigma_w \geq 0$, $\mathbb{E}[v^G_k (v^G_k)^\top] = \Sigma_G > 0$, $\mathbb{E}[v^I_k (v^I_k)^\top] = \Sigma_I > 0$, and $\mathbb{E}[v^S_k (v^S_k)^\top] = \Sigma_S > 0$, respectively.

Remark 2.1: y^I_k can represent any *relative* sensor measurement. In this paper, we use IMU for the illustration.

Remark 2.2: The signal strength output y^S_k in (1d) is derived by the GPS signal attenuation due to free-space path loss. Friis transmission equation is given by: $P_r = P_t G_t G_r \frac{\lambda^2}{(4\pi r)^2}$, where P_t and P_r are the transmit power and the receive power; G_t and G_r are the transmit and receive antenna gains; r is the distance between two antennas; λ is the wavelength [13]. We write $G_r(\frac{\lambda}{4\pi})^2$ as the output matrix C_S ; $G_t P_t$ as the nominal power of the spoofing device η_k; and r as the distance $\mathbf{d}(x^a_k, x_k)$.

C. Problem Statement

Given the system (1) with sensor measurements (1b)-(1d), the defender aims to detect the GPS spoofing attack, achieve resilient state estimation when considering the limited sensor availability, and complete the global mission securely.

III. Safety Constrained Control Framework

To address the problem described in Section II-C, we propose a safety constrained control framework, which consists of an attack detector, a resilient state estimator, a robust controller, an attacker location tracker (ALT), and an escape controller (ESC). The proposed safety constrained control framework drives the UAV outside the effective range of the spoofing device. The following explains each module in the proposed framework as shown in Fig. 1.

Robust Control Mode. The robust controller is a complex controller that operates the UAV to the destination in the presence of noise, but without the presence of attacks. Any robust control technique can be implemented in this module.

Emergency Control Mode. ALT is designed to track the location of the attacker and estimate the spoofing device's output power by applying UKF with sliding window outputs. ESC is an MPC-based controller that drives the UAV out of the effective range of the spoofing device based on the estimation of the attacker location obtained by ALT.

Attack-resilient Monitor & Decision Logic. The resilient state estimator is developed based on the Kalman-filter like state estimator. The attack detector is designed by the χ^2-based anomaly detection algorithm. Based on the previous estimation from the resilient state estimator, the Boolean output (dotted-dashed line in Fig. 1) of the attack detector determines (i) whether the GPS measurement should be used for the state estimation; and (ii) the switching rule between the robust control mode and the emergency control mode.

ALT and ESC adapt the UAV at a path re-planning level for safe operation. In what follows, each subsection describes the details of the corresponding component.

A. Resilient State Estimator

The defender implements an estimator and χ^2 detector to estimate the state and detect the GPS spoofing attack. The following Kalman-filter like state estimator is used to estimate the current state:

$$\begin{aligned}\hat{x}_k = {} & A\hat{x}_{k-1} + Bu_{k-1} + K^G_k(y^G_k - C^G(A\hat{x}_{k-1} + Bu_{k-1})) \\ & + K^I_k(y^I_k - C^I(A\hat{x}_{k-1} + Bu_{k-1} - \hat{x}_{k-1}))\end{aligned} \tag{2}$$

$$\begin{aligned}P_k = {} & (A - K_kCA + K_kDC)P_{k-1}(A - K_kCA + K_kDC)^\top \\ & + (I - K_kC)\Sigma_w(I - K_kC)^\top + K_k\Sigma_y K_k^\top,\end{aligned} \tag{3}$$

where $\hat{x}_k$ is the state estimate and P_k is the state estimation error covariance at time k, and $K_k := \begin{bmatrix} K_k^G & K_k^I \end{bmatrix}$, $C := \begin{bmatrix} C^G \\ C^I \end{bmatrix}$, $\Sigma_y := \begin{bmatrix} \Sigma_G & 0 \\ 0 & \Sigma_I \end{bmatrix}$ and $D := \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix}$. The optimal gain K_k, given by

$$K_k = (AP_{k-1}(CA - DC)^\top + \Sigma_w C^\top) \times \left((CA - DC)P_{k-1}(CA - DC)^\top + C\Sigma_w C^\top + \Sigma_y\right)^{-1}, \quad (4)$$

is the solution of the optimization problem $\min_{K_k} tr\,(P_k)$.

In [11], it has been shown that the covariance in (3) is bounded when the GPS signal is available. If the GPS is denied, and only the relative sensor y_k^I is available, the covariance is strictly increasing and unbounded in time. That is, the sensor drift problem can be formulated as the instability of the covariance matrix.

B. Attack Detector

We conduct the χ^2 test to detect the GPS spoofing attacks:

$$H_0 : d_k = 0; \quad H_1 : d_k \neq 0, \quad (5)$$

using CUSUM (CUmulative SUM) algorithm, which is widely used in attack detection research [14].

Since $d_k = y_k^G - C^G x_k - v_k^G$, given the previous state estimate $\hat{x}_{k-1}$, we estimate the attack vector by comparing the sensor output and the output prediction:

$$\hat{d}_k = y_k^G - C^G(A\hat{x}_{k-1} + Bu_{k-1}). \quad (6)$$

Due to the Gaussian noises w_k and v_k injected to the linear system in (1), the states follow Gaussian distribution since any finite linear combination of Gaussian distributions is also Gaussian. Similarly, $\hat{d}_k$ is Gaussian as well, and thus the use of χ^2 test (5) is justified. In particular, the χ^2 test compares the normalized attack vector estimate $\hat{d}_k^\top (P_k^d)^{-1}\hat{d}_k$ with $\chi^2_{df}(\alpha)$:

$$\begin{aligned} &\text{Accept } H_0, \text{ if } \hat{d}_k^\top (P_k^d)^{-1}\hat{d}_k \leq \chi^2_{df}(\alpha) \\ &\text{Accept } H_1, \text{ if } \hat{d}_k^\top (P_k^d)^{-1}\hat{d}_k > \chi^2_{df}(\alpha), \end{aligned} \quad (7)$$

where $P_k^d := \mathbb{E}[(d_k - \hat{d}_k)(d_k - \hat{d}_k)^\top] = C^G(AP_{k-1}A^\top + \Sigma_w)(C^G)^\top + \Sigma_G$, and $\chi^2_{df}(\alpha)$ is the threshold found in the Chi-square table. In $\chi^2_{df}(\alpha)$, df denotes the degree of freedom, and α denotes the statistical significance level.

To reduce the effect of noise, we use the test (7) in a cumulative form. The proposed χ^2 CUSUM detector is characterized by the detector state $S_k \in \mathbb{R}_+$:

$$S_k = \delta S_{k-1} + (\hat{d}_k)^\top (P_k^d)^{-1}\hat{d}_k, \quad S_0 = 0, \quad (8)$$

where $0 < \delta < 1$ is the pre-determined forgetting factor. At each time k, the CUSUM detector (8) is used to update the detector state S_k and detect the attack.

The attack detector will i) update the estimated state $\hat{x}_k$ and the error covariance P_k in (3) with $K_k^G = 0$ and ii) switch the control mode to emergency control mode, if

$$S_k > \sum_{i=0}^{\infty} \delta^i \chi^2_{df}(\alpha) = \frac{\chi^2_{df}(\alpha)}{1-\delta}. \quad (9)$$

If $S_k < \frac{\chi^2_{df}(\alpha)}{1-\delta}$, then it returns to the robust control mode.

C. Attacker Location Estimation (ALT)

We formulate the simultaneous estimation of the attacker location x_k^a and unknown parameter η_k as a target tracking problem of the attacker state $\mathbf{x}_k^a := [(x_k^a)^\top, \eta_k]^\top$.

Estimating the attacker state $\mathbf{x}_k^a$ encounters two significant problems: i) the output equation y_k^S in (1d) is highly nonlinear, and ii) a single measurement of the signal strength suffers from the infinite number of solutions.

To address the first issue, we use the unscented Kalman filter (UKF) [15], which has been developed to deal with highly nonlinear systems and provides a better estimation than the extended Kalman filter. Motivated by the fact that locating the epicenter of an earthquake can be done with at least three measurements from different seismic stations, we resolve the second issue using sliding window outputs. To be specific, we estimate $\mathbf{x}_{k+1}^a$ using UKF with M-sized sliding window outputs:

$$\mathbf{x}_{k+1}^a = \mathbf{x}_k^a + \mathbf{w}_k^a; \quad \boldsymbol{y}_k^S = [y_k^S, y_{k-1}^S, \cdots, y_{k-M+1}^S]^\top.$$

The signal strength measurements from (1d) can be written as $y_k^S = f(\mathbf{x}_k^a) + v_k^S$, where $f(\mathbf{x}_k^a) := C^S\eta_k / \mathbf{d}(x_k^a, x_k)^2$.

The state estimation by using UKF with sliding window outputs can track the moving attacker's location, while nonlinear regression algorithms may fail to track it. The algorithm is summarized in Algorithm 1 in the Appendix. Due to the page limit, the algorithm's derivation is omitted and can be found in this paper's *arXiv* version [16].

D. Escape Controller (ESC)

In the presence of the GPS spoofing attack, the variance P_k in (3) of the state estimation errors is strictly increasing and unbounded in time (Thm. 4.2 [11]). The escape time is defined in [11], providing a new criterion for optimal trajectory regeneration with increasing uncertainties. In particular, ESC is designed to drive the UAV outside of the spoofing device's effective range within the escape time. Given the estimates of UAV state $\hat{x}_k$ and attacker state $\hat{\mathbf{x}}_k^a$ with their covariances, the safety problem due to the increasing and unbounded errors can be formulated as the safety-critical constraint:

$$\mathbf{d}(\hat{x}^a_{k^a+k^{esc}}, \hat{x}_{k^a+k^{esc}}) - r_{effect} > 0, \quad (10)$$

where k^a is the time of the attack, k^{esc} is the escape time, and r_{effect} is the upper bound of the effective range. This constraint implies that ESC should drive the UAV outside of the spoofing device's effective range within the escape time.

Remark 3.1: r_{effect} can be assumed to be known. Due to hardware constraints, the output power of the spoofing device η_k is bounded, and η_k also can be estimated by ALT in Section III-C. The output power determines the effective range of the spoofing device, and r_{effect} can be found by $r_{effect} = \text{argmax}_r\, g(r)$, where $g(r) := C^S \frac{\eta_k}{r^2} > \eta^S$.

There are two significant challenges in considering the safety-critical constraint in (10). First, the states and the attacker location are unknown, and their estimates $\hat{x}_i$ and $\hat{x}_i^a$ are subject to stochastic noise. Moreover, we cannot

guarantee that constraint (10) is always feasible. Addressing the above two challenges, we introduce two programs for ESC in Section III-D.1 and III-D.2.

1) ESC with Tube: Since the constraint (10) is the safety-critical constraint, we can reformulate it as a conservative constraint such that ESC should drive the UAV outside of the effective range of the spoofing device with probability γ by the single individual chance constraint (ICC):

$$\mathbb{P}[\mathbf{d}(x^a_{k^a+k^{esc}}), x_{k^a+k^{esc}}] - r_{effect} > 0) > \gamma. \quad (11)$$

Now we formally introduce the stochastic MPC problem as:

Program 3.1:

$$\min_{u} \sum_{i=k^a}^{k^a+N} \hat{\tilde{x}}_{i+1}^\top Q_i \hat{\tilde{x}}_{i+1} + u_i^\top R_i u_i$$

$$\text{s.t. } \hat{x}_{i+1} = A\hat{x}_i + Bu_i$$

$$\mathbf{d}(\hat{x}^a_{k^a+k^{esc}}, \hat{x}_{k^a+k^{esc}}) - r_{effect} > s(P_{k^a+k^{esc}}, P^a_k, \gamma) \quad (12)$$

$$h(\hat{x}_i, u_i) \leq 0 \quad (13)$$

$$\text{for } \; i = k^a, k^a+1, \cdots, k^a+N,$$

where $N \geq k^{esc}$ is the prediction horizon, $\hat{\tilde{x}}_i$ is defined as the difference between the state estimation and the goal state at time index i, i.e., $\hat{\tilde{x}}_i := \hat{x}_i - x_i^{goal}$, Q_i and R_i are symmetric positive definite weight matrices, and $\hat{x}^a_i$ is the estimate of the attacker location. Value r_{effect} is the upper bound of the effective range of the spoofing device. $P_{k^a+k^{esc}}$ is the UAV state covariance at escape time, and P^a_k is the attacker state covariance. Function $s(\cdot)$ is the probabilistic tube size that can be seen as a margin to fulfill the safety-critical ICC in (11). Inequality (13) is any nonlinear constraint on the state estimation $\hat{x}_i$ and the control input u_i.

To provide the theoretical guarantees on the capability of Program 3.1 and the equivalence between the stochastic MPC problem with ICC in (11) and Program 3.1, we use the results from [17], [18]. Since the MPC problem with ICC in (11) is the standard nonlinear stochastic MPC problem, Assumptions in [18] can be verified.

Theorem 3.1: Under the Assumptions 1-4, 6 and 9 in [18], if Program 3.1 is feasible at $t = k^a$, then it is recursively feasible; the constraints (13) and (11) are satisfied and the origin is practically asymptotically stable for the resulting closed loop system. The impact of the hard constraint (12) is equivalent to the nonlinear ICC (11).

Proof: See proofs of Thm. 1 in [17] and Thm. 8 & 10 in [18]. □

From Theorem 3.1, we can conclude that as long as Program 3.1 is feasible at the time of attack k^a, we can guarantee that the UAV can escape within the escape time in probability. However, Program 3.1 may not be feasible in some cases. To address this issue, we introduce a program with a soft constraint in the subsequent section.

2) ESC with Potential Function: The hard constraint (12) can be replaced by the repulsive potential function as a high penalty in the cost function, which is active only after the escape time $k^a + k^{esc}$. The repulsive potential function $U_{rep}(D)$ is defined as the following:

$$U_{rep}(D) := \begin{cases} \frac{1}{2}\beta\left(\frac{1}{D} - \frac{1}{r_{effect}}\right)^2 & \text{if } D \leq r_{effect} \\ 0 & \text{if } D > r_{effect} \end{cases},$$

which can be constructed based on the distance between the location of the attacker and the location of UAV, $D := \mathbf{d}(\hat{x}^a_{k^a+k^{esc}}, \hat{x}_{k^a+k^{esc}})$. The scaling parameter β is a large constant, representing a penalty when the constraint has not been fulfilled. Utilizing the soft constraint, we reformulate the MPC problem as follows:

Program 3.2:

$$\min_{u} \sum_{i=k^a}^{k^a+N} \hat{\tilde{x}}_{i+1}^\top Q_i \hat{\tilde{x}}_{i+1} + u_i^\top R_i u_i + \sum_{i=k^a+k^{esc}}^{k^a+N} U_{rep}(D_i)$$

$$\text{s.t. } \hat{x}_{i+1} = A\hat{x}_i + Bu_i$$

$$h(\hat{x}_i, u_i) \leq 0 \quad \text{for } \; i = k^a, k^a+1, \cdots, k^a+N.$$

Remark 3.2: Comparing to the use of the repulsive potential function U_{rep} in the collision avoidance literature [19], the proposed application of the repulsive potential function in Program 3.2 has two differences. First of all, the repulsive potential function is known before the collision happens in collision avoidance literature, while we can only get the repulsive potential function U_{rep} after the collision occurs, i.e., only after the UAV has entered the effective range of the spoofing device. Second, the repulsive potential function U_{rep} is only counted in the cost function in Program 3.2 after the escape time.

IV. Simulation

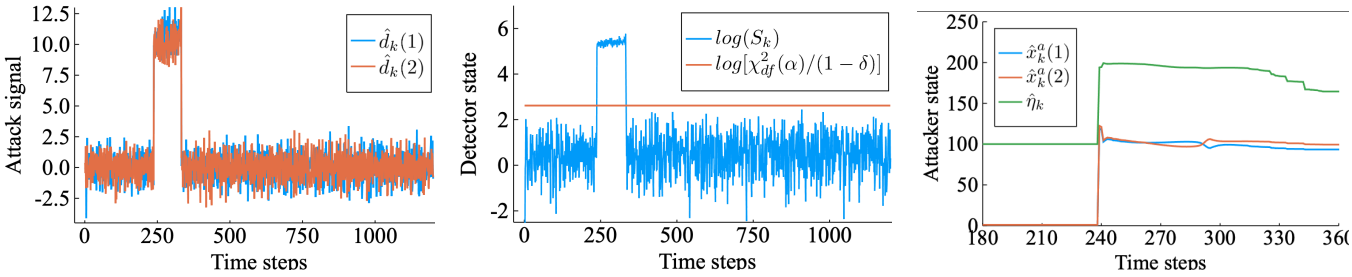
In the simulations, the UAV is moving from the start position with the coordinates at $(0, 0)$ to the target position $(300, 300)$ by using feedback control[1], based on the estimate from (2). The UAV will switch the control mode from the robust control mode to the emergency control mode when the attack is detected. We solve the problem with Program 3.2. The online computation is done using `Julia`, and ESC is implemented using `JuMP` [20] with `Ipopt` solver.

A. UAV Model

We use a double integrator UAV dynamics under the GPS spoofing attack as in [21]. The discrete time state vector x_k considers planar position and velocity at time step k, i.e. $x_k = [r^x_k, r^y_k, v^x_k, v^y_k]^\top$, where r^x_k, r^y_k denote x, y position coordinates, and v^x_k, v^y_k denote velocity coordinates. We consider the acceleration of UAV as the control input $u_k = [u^x_k, u^y_k]^\top$. We assume that the state constraint and control input constraint are given as $\sqrt{(v^x_k)^2 + (v^y_k)^2} \leq 5$ and $\sqrt{(u^x_k)^2 + (u^y_k)^2} \leq 2$. With sampling time at 0.1 seconds, the double integrator model is discretized into the following matrices:

$$A = \begin{bmatrix} 1 & 0 & 0.1 & 0 \\ 0 & 1 & 0 & 0.1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.1 & 0 \\ 0 & 0.1 \end{bmatrix},$$

[1]We implemented a proportional-derivative (PD) like tracking controller, which is widely used for double integrator systems.



(a) Attack signal estimation. (b) Attack detection. (c) Attacker state estimation.

Fig. 2: Attack estimation, attack detection and attacker state estimation.

and the outputs y_k^G, y_k^I and y_k^S are the position measurements from GPS, the velocity measurements from IMU, and GPS signal strength measurements respectively, with the output matrices: $C^G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$, $C^I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and $C^S = \begin{bmatrix} 1 \end{bmatrix}$. The covariance matrices are $\Sigma_w = 0.1I$, $\Sigma_G = I$, $\Sigma_I = 0.01I$ and $\Sigma_S = I$.

B. GPS Spoofing Attack and Attack Signal Estimation

The GPS attack happens when the UAV is in the effective range of the spoofing device. In this attack scenario, the attack signal is $d = [10, 10]^\top$. The attacker's location and the nominal power of the spoofing device are $x_k^a = [100, 100]^\top$ and $\eta_k = 200$, which are both unknown to the UAV. The estimation obtained by (6) is shown in Fig. 2a.

C. Attack Detection

Using the estimated attack signal to calculate the detector state S_k by (8), the attack detector is able to detect the attack using the normalized attack vector as shown in Fig. 2b in $log-$scale. Statistic significance of the attack is tested using the CUSUM detector described in (9). The threshold is calculated by $\frac{\chi^2_{df}(\alpha)}{1-\delta}$ with the significance $\alpha = 0.01$ and the forgetting factor $\delta = 0.15$.

D. Attacker State Estimation

When the GPS attack is detected, the UAV first estimates the attacker state $\mathbf{x}_k^a$ by using Algorithm 1 with window size $M = 5$. The estimation result is shown in Fig. 2c. The estimated location and the estimated nominal power quickly converge to the true values. The estimates are drifting when the UAV remains in GPS denied environment. After obtaining an estimate of the attacker state, ESC is used to escape away from the effective range of the spoofing device.

E. Trajectory Generation

Program 3.2 with the prediction horizon $N = k^{esc} + 40$ and the scaling parameter $\beta = 50000$ is used to generate the estimated and true trajectories of the simulated scenario shown in Fig. 3. As shown in Fig. 4, the state estimation error $\|x_k - \hat{x}_k\|$ is increasing when the UAV is in the effective range of the spoofing device, and the error is bounded by the tolerable error distance $\zeta = 3$ corresponding to $k^{esc} = 125$.

Fig. 5 presents how the proposed control framework performs in different cases where $r_{effect} \in \{10, 30, 50, 70\}$. Regardless of the size of r_{effect}, the UAV will escape away from the effective range within the escape time. Note that in Fig 5a the UAV can pass the attacker without changing the direction or even its speed since r_{effect} is small enough.

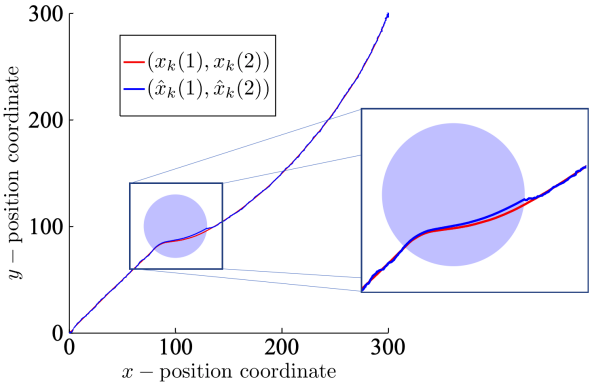


Fig. 3: Estimated and true trajectories of the simulated scenario. The attacker is located at $(100, 100)$ with $r_{effect} = 30$, which is displayed as the light blue circle.

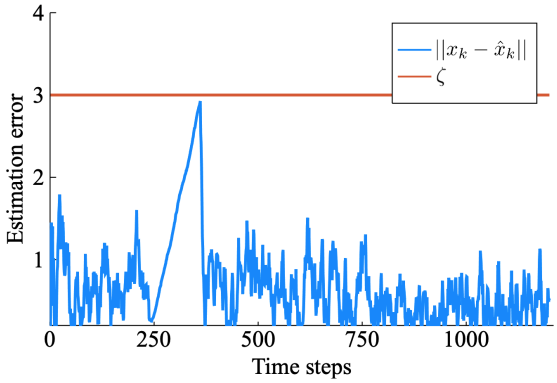
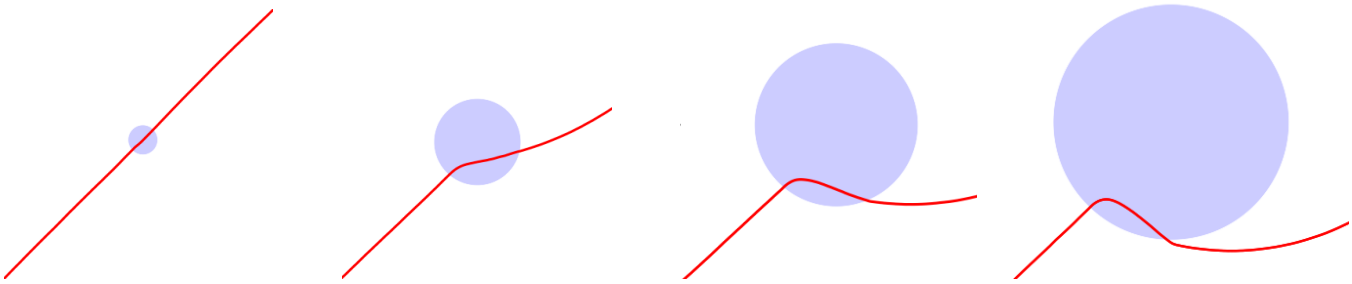


Fig. 4: Bounded estimation error $\|x_k - \hat{x}_k\|$.

V. Conclusion

We present a secure safety constrained control framework that adapts the UAV at a path re-planning level to support resilient state estimation against GPS spoofing attacks. In the presence of the GPS spoofing attack, using the robust controller may still keep the UAV within the effective range of the spoofing device after the estimation errors may not be in the tolerable region. To solve the safety problem raised by the large estimation error, ALT is developed to track the attacker location and estimate the effective range of the spoofing device by using UKF with sliding window outputs. Then, ESC is used to escape away from the effective range



(a) $r_{effect} = 10$ (b) $r_{effect} = 30$ (c) $r_{effect} = 50$ (d) $r_{effect} = 70$

Fig. 5: Trajectories with different effective ranges.

of the spoofing device within the escape time. A numerical simulation is given to demonstrate the results.

REFERENCES

[1] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[2] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[3] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation, Tampa, FL*, pp. 2233–2242, Citeseer, 2014.

[4] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the International Technical Meeting of The Institute of Navigation*, pp. 124–130, 2009.

[5] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of applied research and technology*, vol. 13, no. 1, pp. 45–57, 2015.

[6] K. Jansen and C. Pöpper, "Advancing attacker models of satellite-based localization systems: the case of multi-device attackers," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 156–159, ACM, 2017.

[7] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *IEEE Conference on Decision and Control (CDC)*, pp. 5967–5972, 2010.

[8] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[9] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[10] W. Wan, H. Kim, N. Hovakimyan, and P. G. Voulgaris, "Attack-resilient estimation for linear discrete-time stochastic systems with input and state constraints," *IEEE 58th Conference on Decision and Control (CDC)*, pp. 5107–5112, 2019.

[11] H.-J. Yoon, W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. G. Voulgaris, "Towards resilient UAV: Escape time in GPS denied environment with sensor drift," *IFAC-PapersOnLine*, vol. 52, no. 12, pp. 423–428, 2019.

[12] X. Wang, N. Hovakimyan, and L. Sha, "RSimplex: A robust control architecture for cyber and physical failures," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 4, p. 27, 2018.

[13] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, pp. 254–256, May 1946.

[14] T. L. Lai, "Sequential changepoint detection in quality control and dynamical systems," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 613–658, 1995.

[15] S. J. Julier and J. K. Uhlmann, "New extension of the Kalman filter to nonlinear systems," in *Signal processing, sensor fusion, and target recognition VI*, vol. 3068, pp. 182–193, International Society for Optics and Photonics, 1997.

[16] W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. G. Voulgaris, "A safety constrained control framework for UAVs in GPS denied environment," *arXiv preprint arXiv:1910.10826*, 2019.

[17] J. Köhler, R. Soloperto, M. A. Müller, and F. Allgöwer, "A computationally efficient robust model predictive control framework for uncertain nonlinear systems," *arXiv preprint arXiv:1910.12081*, 2019.

[18] H. Schlüter and F. Allgöwer, "A constraint-tightening approach to nonlinear stochastic model predictive control for systems under general disturbances," *arXiv preprint arXiv:1912.01946*, 2019.

[19] M. T. Wolf and J. W. Burdick, "Artificial potential functions for highway driving with collision avoidance," in *IEEE International Conference on Robotics and Automation*, pp. 3731–3736, 2008.

[20] I. Dunning, J. Huchette, and M. Lubin, "Jump: A modeling language for mathematical optimization," *SIAM Review*, vol. 59, no. 2, pp. 295–320, 2017.

[21] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

APPENDIX

We present the UKF with sliding window outputs, and its derivation can be found in [16]. Consider the following partially nonlinear system:

$$\begin{aligned} x_{k+1} &= A_k x_k + w_k \\ y_k &= f(x_k) + v_k, \end{aligned}$$

where $x_k \in \mathbb{R}^n$ is the state, $y_k \in \mathbb{R}^m$ is the output. The noise signals w_k and v_k are assumed to be i.i.d. Gaussian with zero means and covariances $\mathbb{E}[w_k w_k^\top] = \Sigma_{w'} \geq 0$ and $\mathbb{E}[v_k v_k^\top] = \Sigma_v > 0$.

Algorithm 1 UKF with sliding window outputs

▷ Prediction

$\hat{x}_{k|k-1} = A_{k-1}\hat{x}_{k-1}$;

$P_{k|k-1} = A_{k-1}P_{k-1}A_{k-1}^\top + \Sigma_{w'}$;

▷ Sigma points generation

$\mathcal{X}_k = \{\hat{x}_{k|k-1} \pm (\sqrt{nP_{k|k-1}})_i^\top\}$, $i \in \{1, \cdots, n\}$;

▷ Measurement Update

for $i = 1 : 2n$ **do**

$\hat{\boldsymbol{y}}_k^i := [\hat{y}_k^i, \hat{y}_{k-1}^i, \cdots, \hat{y}_{k-M+1}^i]^\top$

$= [f(\mathcal{X}_k^i), (A_{k-1}^{-1}\mathcal{X}_k^i), \cdots, f(A_{k-1}^{-M+1}\mathcal{X}_k^i)]^\top$;

end for

$\bar{\boldsymbol{y}}_k = \sum_{i=0}^{2n} W_k^i \hat{\boldsymbol{y}}_k^i$;

$\boldsymbol{P}_k^y = \sum_{i=0}^{2n} W_k^i (\hat{\boldsymbol{y}}_k^i - \bar{\boldsymbol{y}}_k)(\hat{\boldsymbol{y}}_k^i - \bar{\boldsymbol{y}}_k)^\top + \boldsymbol{\Sigma}_v$;

$\boldsymbol{P}_k^{xy} = \sum_{i=0}^{2n} W_k^i (\mathcal{X}_k^i - \hat{x}_{k|k-1})(\hat{\boldsymbol{y}}_k^i - \bar{\boldsymbol{y}}_k)^\top$;

$K_k = \boldsymbol{P}_k^{xy}(\boldsymbol{P}_k^y)^{-1}$

$\hat{x}_k = \hat{x}_{k|k-1} + K_k(\boldsymbol{y}_k - \bar{\boldsymbol{y}}_k)$;

$P_k = P_{k|k-1} - K_k \boldsymbol{P}_k^y K_k^\top$