AIAA AVIATION Forum
June 15-19, 2020, VIRTUAL EVENT
AIAA AVIATION 2020 FORUM

10.2514/6.2020-2621

Safety Constrained Multi-UAV Time Coordination: A Bi-level Control Framework in GPS Denied Environment [*]

Wenbin Wan[†], Hunmin Kim[‡], Yikun Cheng[§], Naira Hovakimyan[¶]
University of Illinois at Urbana-Champaign, Urbana, IL 61801

Petros G. Voulgaris[‖]
University of Nevada, Reno, NV 89557

Lui Sha[**]
University of Illinois at Urbana-Champaign, Urbana, IL 61801

Unmanned aerial vehicles (UAVs) suffer from sensor drifts in GPS denied environments, which can cause safety issues. To avoid intolerable sensor drifts while completing the time-critical coordination task for multi-UAV systems, we propose a safety constrained bi-level control framework. The first level is the *time-critical coordination level* that achieves a consensus of coordination states and provides a virtual target which is a function of the coordination state. The second level is the *safety-critical control level* that is designed to follow the virtual target while adapting the attacked UAV(s) at a path re-planning level to support resilient state estimation. In particular, the *time-critical coordination level* framework generates the desired speed and position profile of the virtual target based on the multi-UAV cooperative mission by the proposed consensus protocol algorithm. The *safety-critical control level* is able to make each UAV follow its assigned path while detecting the attacks, estimating the state resiliently, and driving the UAV(s) outside the effective range of the spoofing device within the escape time. The numerical simulations of a three-UAV system demonstrate the effectiveness of the proposed safety constrained bi-level control framework.

I. Introduction

In recent years, there has been an increasing interest in multi-UAV systems due to the wide range of applications, including civilian transportation [1], aerial photography for agriculture [2], searching and rescuing [3], and other cooperative tasks. In order to get accurate and reliable state measurements for completing various cooperative tasks safely, the global positioning system (GPS) is the most widely used senor for multi-UAV systems. However, GPS receivers are potentially vulnerable to various types of attacks, such as blocking, jamming, and spoofing [4]. 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 [5]. Furthermore, GPS is more vulnerable when its signal strength is weak. In particular, due to various applications of multi-UAV systems, 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 [6]. A multi-antenna receiver system was used to detect GPS spoofing attacks by monitoring the angle-of-arrival of the spoofing attempts in [7]. 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 [8–10]. However, those solutions require modifications of the hardware or the low-level computing modules and assume that an attacker

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

[†] Graduate student, Department of Mechanical Science and Engineering, *wenbinw2@illinois.edu*.

[‡] Postdoctoral Research Associate, Department of Mechanical Science and Engineering, *hunmin@illinois.edu*

[§] Graduate student, Department of Mechanical Science and Engineering, *yikun2@illinois.edu*.

[¶] Professor, Department of Mechanical Science and Engineering, *nhovakim@illinois.edu*, AIAA Fellow.

[‖] Professor, Department of Mechanical Engineering, *pvoulgaris@unr.edu*.

[**] Professor, Department of Computer Science, *lrs@illinois.edu*.

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 [11].

In Cyber-physical system (CPS) security literature, GPS spoofing attacks have been described as a malicious signal injection to the genuine sensor output [12]. 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 [13, 14]. The fundamental limitations of structural detectability, as well as graph-theoretical detectability for linear time-invariant systems, have been studied in [15], 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 [16]. A switching mode resilient detection and estimation framework for GPS spoofing attacks has been studied in [17]. Attack detection using multiple GPS signals by checking cross-correlation was introduced in [18]. In [19], the maximum deviations of the state were identified due to the sensor attacks while remaining stealthy due to the detection. Resilience to cyber-attacks for multi-agent systems becomes more challenging than for single-agent systems. There has been much effort in investigating resilient strategies for multi-agent systems in the presence of cyber-attack. A method of switching the network topologies is utilized to secure consensus tracking performance in the presence of the cyber-attack on communication channels in [20]. In [21], an event-triggered mechanism and a distributed observer-based controller are designed to ensure the overall consensus of multi-agent systems is achieved. The coordinated path following design based on an adaptive control method and a synchronization scheme is presented in [22], where coordinated path following goal is achieved. These architectures can efficiently handle a class of attacks for multi-agent systems, but do not consider fundamental problems indirectly induced by attacks and cannot address the significant 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 while completing the time-critical coordination task for a Multi-UAV system. We model the sensor drift problem in the presence of GPS spoofing attacks 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. We propose a safety constrained bi-level control framework for multi-UAV systems that adapts the UAV(s) at a path re-planning level to support resilient state estimation against GPS spoofing attacks. The proposed framework achieves a consensus of coordination state at the *time-critical coordination level* and is equipped with an escape controller (ESC) that drives the UAV(s) away from the effective range of the spoofing device within the escape time to avoid intolerable sensor drift at *safety-critical control level*.

The remainder of this paper is organized as follows: In Section II, we introduce the notation convention, definition of the *escape time* and the dynamic system models for multi-UAV systems. In the same section, we formulate the problem. In Section III, we propose a resilient safety constrained bi-level control framework. In Section IV, the numerical simulations of the multi-UAV system for a time-critical mission under the GPS spoofing attack is presented. Section V draws the conclusion.

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; $A^\top$, $tr(A)$ and A^{-1} denote the transpose, trace and inverse of matrix A, respectively; I denotes the identity matrix with an appropriate dimension; $\|\cdot\|$ denotes the standard Euclidean norm for a vector or an induced matrix norm; $\times$ is used to denote Cartesian product; $\mathbb{E}[\,\cdot\,]$ denotes the expectation operator. For a matrix S, $S > 0$ and $S \geq 0$ indicate that S is positive definite and positive semi-definite, respectively.

B. Escape time

In the presence of the GPS spoofing attack, the state estimation algorithm relies on the relative measurement sensors because the GPS signals do not contain legitimate information. In this case, the variance of the state estimation errors is strictly increasing and unbounded in time (Theorem 4.2 in [17]). Regarding the sensor drift problem, we utilize a new resilience measure, escape time, which is defined as follows:

Definition II.1 *[17] The escape time $k^{esc} \geq 0$ is the time difference between the attack time k^a and the first time instance when the estimation error $\|x_k - \hat{x}_k\|$ is not within the tolerable error distance $\zeta \in \mathbb{R}^n_+$ with the significance α,* *i.e.*

$$k^{esc} = \arg\min_{k \geq k^a} k - k^a$$
$$s.t.\ \zeta^\top P_k^{-1} \zeta < \chi^2_{df}(\alpha),$$

where P_k is the error covariance of $x_k - \hat{x}_k$, and χ^2 is the chi-squared test value with degree of freedom df.

The escape time provides a new safety criterion for optimal control with increasing uncertainties. It is worth to notice that the escape time k^{esc} can be calculated by Algorithm 1 in [17].

C. System model

In what follows, we describe the multi-UAV system in detail.

1. Agent model

Consider the discrete-time dynamic system model of the *single agent*:

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{1a}$$
$$y_k^G = C^G x_k + d_k + v_k^G \tag{1b}$$
$$y_k^I = C^I (x_k - x_{k-1}) + v_k^I \tag{1c}$$

where $x_k \in \mathbb{R}^n$ is the state, $u_k \in \mathbb{R}^m$ is the control input and A, B, C^G and C^I are the system matrix, input matrix, and output matrix with proper sizes. The sensor measurement $y_k^G \in \mathbb{R}^{m_G}$ is the GPS measurement which may be corrupted by unknown GPS spoofing signal $d_k \in \mathbb{R}^{m_G}$. We assume that the attacker can inject any signal d_k into y_k^G. The sensor measurement $y_k^I \in \mathbb{R}^{m_I}$ is the inertial measurement unit (IMU) measurement which returns a noisy measurement of the state difference. The output y_k^I can represent any *relative* sensor measurement, such as velocity measurement by a camera. In this paper, we use IMU for the illustration.

The noise signals w_k, v_k^G and v_k^I are assumed to be independent and identically distributed (i.i.d.) Gaussian random variables with zero means and covariances $\mathbb{E}[w_k w_k^\top] = \Sigma_w \geq 0$, $\mathbb{E}[v_k^G (v_k^G)^\top] = \Sigma_G > 0$, and $\mathbb{E}[v_k^I (v_k^I)^\top] = \Sigma_I > 0$, respectively.

2. Multi-agent network

Let $x_{i,k} \in \mathbb{R}^n$, $i = 1, \cdots, N$ be the state of the i^{th} agent associated with dynamic system model (1) where N is the total number of the agents. Graph theory can provide the natural abstractions for how information is shared between agents in a network [23]. An undirected graph $\mathcal{G} = (V, E)$ consists of a set of nodes $V = \{1, 2, \cdots, N\}$, which corresponds to the different agents, and a set of edges $E \subset V \times V$, which relates to a set of unordered pairs of agents. In particular, $(i, j), (j, i) \in E$ if and only if there exists a communication channel between agents i and j. The neighborhood $\mathcal{N}(i) \subseteq V$ of the agent i will be understood as the set $\{j \in V \mid (i, j) \in E\}$.

3. Path following consensus

Each agent $i \in V$ has a desired trajectory $g_i : s_{i,k} \rightarrow \mathbb{R}^{n_s}$ that is parameterized by coordination state variable $s_{i,k} \in [0, 1]$ as shown in Fig. 1. Dimension n_s is usually 2 (2−D mission) or 3 (3−D mission). At time k, $g_i(s_{i,k})$ is the virtual target that the agent i follows at that time, i.e., agent i pursues to minimize the error $\|g_i(s_{i,k}) - x_{i,k}\|$ which is marked in red in Fig. 1. The state $s_{i,k}$ can be seen as a normalized length of trajectory. The agents also desire to achieve the consensus of the coordination state variable

$$s_{i,k} - s_{j,k} \xrightarrow{k \to \infty} 0 \quad \forall i, j \in V,$$

so that the virtual targets of the agents arrive at the destination at the same time.

The agent i knows coordination state $s_{i,k}$ as well as the coordination states $s_{j,k}$ for neighboring agents $j \in \mathcal{N}(i)$.

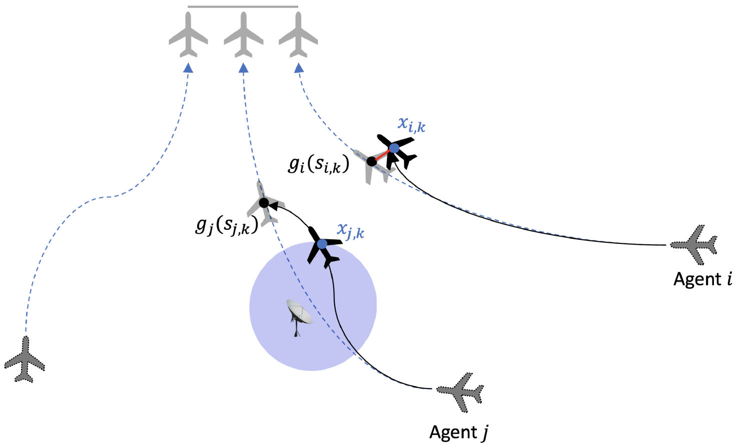


Fig. 1 Illustration of the path following consensus. The goal of the multi-agent system is for all agents to reach the desired goal state simultaneously. For the agent i at time k, the virtual target/predetermined desired state is $g_i(s_{i,k})$ and the true state is $x_{i,k}$. The error between the virtual target $g_i(s_{i,k})$ and the true state $x_{i,k}$ (marked in red) is to be minimized. The attacker is on the path of the agent j and the effective spoofing area is displayed as the light blue circle. When the attack is detected, the agent j will be re-planning the trajectory so that the state estimation errors remain in the tolerable region, while the other agents will adjust their coordination states accordingly to achieve time-coordination.

D. Problem Statement

Given a multi-agent network described in Section II.C.2 consisting of number of N agents described in (1), the agent i, where $i = 1, \cdots, N$, aims to follow its desired trajectory $g_i(\cdot)$ with a reference rate ρ, i.e.,

$$g_i(s_{i,k}) - x_{i,k} \xrightarrow{k\to\infty} 0 \tag{2a}$$

$$s_{i,k+1} - s_{i,k} \xrightarrow{k\to\infty} \rho, \tag{2b}$$

and to achieve time coordination, i.e.,

$$s_{i,k} - s_{j,k} \xrightarrow{k\to\infty} 0 \tag{3}$$

for all $i, j \in V$, and for all $k \geq 0$. Meanwhile, each agent aims to detect the GPS spoofing attack; obtain the attack-resilient state estimation when considering the limited sensor availability; complete the path following mission securely.

III. Safety Constrained Bi-level Control Framework

To address the problem described in Section II.D for a multi-agent system, we propose a safety constrained bi-level control framework shown in Fig. 2. The first level, *time-critical coordination level*, is designed to achieve time coordination with the assigned trajectories. The second level is at *safety-critical control level* that supports resilient estimation and path following control. The safety constrained bi-level control framework consists of a time-critical coordinator at the *time-critical coordination level*; an attack detector, a resilient state estimator, a robust controller, and an escape controller (ESC) at the *safety-critical control level*.

The following explains each module in the proposed framework as shown in Fig. 2.

Time-critical coordinator. The time coordination algorithm guarantees that each agent reaches an agreement on some distributed variables of interest; i.e., the coordination state variables. With the coordination state variables, the assigned trajectories generate the virtual targets for UAVs to follow.

Safety-critical controller. The robust controller is a complex controller that operates the UAV to follow the virtual targets in the presence of noise, but without the presence of attacks. The robust controller can be implemented as any effective control technique such as optimal control, model predictive control, PID, etc. The escape controller (ESC) is a model predictive controller (MPC)-based structure that adapts the UAV at a path re-planning level for safe operation. ESC drives the UAV out of the effective range of the spoofing device *within the escape time*.

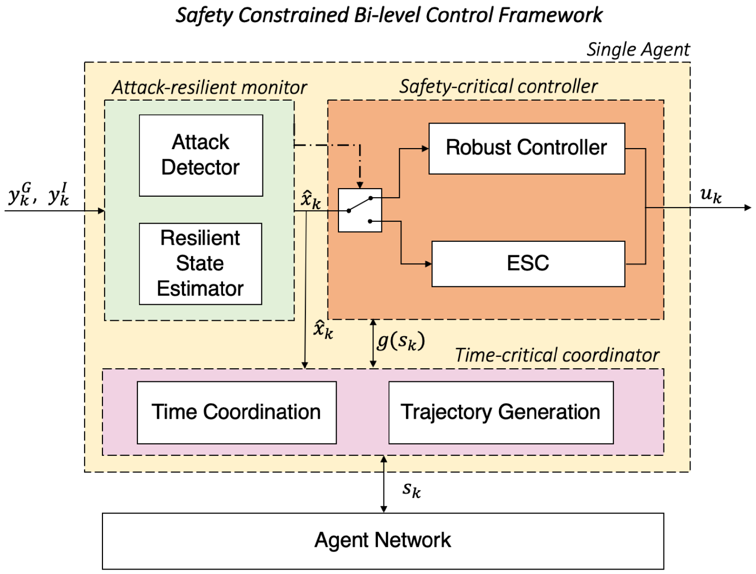


Fig. 2 A safety constrained bi-level control framework consisting of an attack-resilient monitor, a safety-critical controller and a time critical coordinator.

Attack-resilient monitor. 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 (the dot-dashed line in Fig. 2) of the attack detector determines i) whether the GPS measurement should be used for the state estimation and ii) the switching rule between the two controllers: the robust controller and the escape controller (ESC).

In what follows, each subsection describes the details of the corresponding component.

A. Time coordination (Consensus Protocol)

Consider the coordinate state of the consensus network model

$$s_{i,k+1} = s_{i,k} + z_{i,k}, \tag{4}$$

where $z_{i,k} \geq 0$ is the control input for the coordination state of the agent i at time index k. To solve the path following consensus problem in (2) and (3), we propose the design of the control input $z_{i,k}$. The control input $z_{i,k}$ is designed by

$$z_{i,k} = \max\left\{ -k_e \|g_i(s_{i,k}) - x_{i,k}\| - k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k}) + \rho + \mathbb{1}_{\text{attacked}} \hat{z}_{i,k}, 0 \right\}, \tag{5}$$

where $k_e > 0$ and $k_s > 0$ are coordination control gains, and the reference rate ρ is the desired rate of progress that is a constant. The first term $-k_e \|g_i(s_{i,k}) - x_{i,k}\|$ indicates that the agent reduces the coordination speed when there is a tracking error. The second term $-k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k})$ is the consensus term which reduces errors between the local coordination state with those of the neighbors. The third term ρ is the desired rate if there is no tracking error and no coordination error. The last term $\hat{z}_{i,k} = k_e \|g_i(s_{i,k}) - x_{i,k}\|$ drives the virtual target away from the spoofing device even when the UAV detours the planned trajectory. Function $\mathbb{1}_{i,\text{attacked}}$ is an indicator function and $\mathbb{1}_{i,\text{attacked}} = 1$ if an attack is detected, otherwise $\mathbb{1}_{i,\text{attacked}} = 0$. Moreover, if $-k_e \|g_i(s_{i,k}) - x_{i,k}\| - k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k}) + \rho + \mathbb{1}_{i,\text{attacked}} \hat{z}_{i,k}$ is less than zero, then the virtual target chooses to stay at current state rather than go backwards.

B. 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:

$$\begin{aligned} \hat{x}_k &= A\hat{x}_{k-1} + Bu_{k-1} + K_k^G(y_k^G - C^G(A\hat{x}_{k-1} + Bu_{k-1})) + K_k^I(y_k^I - C^I(A\hat{x}_{k-1} + Bu_{k-1} - \hat{x}_{k-1})) && (6)\\ P_k &= (A - K_kCA + K_kDC)P_{k-1}(A - K_kCA + K_kDC)^\top + (I - K_kC)\Sigma_w(I - K_kC)^\top + K_k\Sigma_yK_k^\top, && (7)\end{aligned}$$

where $\hat{x}_k$ is the state estimate and P_k is the state estimation error covariance at time k. We define

$$K_k := \begin{bmatrix} K_k^G & K_k^I \end{bmatrix}, \quad C := \begin{bmatrix} C^G \\ C^I \end{bmatrix}, \quad \Sigma_y := \begin{bmatrix} \Sigma_G & 0 \\ 0 & \Sigma_I \end{bmatrix}, \quad \text{and} \quad D := \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix}.$$

The optimal gain K_k, given by

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

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

In [17], it has been shown that the covariance in (7) 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 is unbounded in time. That is, the sensor drift problem can be formulated as instability of the covariance matrix.

C. Attack Detector

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

$$H_0 : d_k = 0; \quad H_1 : d_k \neq 0, \tag{8}$$

using CUSUM (CUmulative SUM) algorithm, which is widely used in attack detection research [24–26].

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

$$\hat{d}_k = y_k^G - C^G(A\hat{x}_{k-1} + Bu_{k-1}). \tag{9}$$

Note that the current estimate $\hat{x}_k$ should not be used for the prediction, because it is correlated with the current output; i.e., $\mathbb{E}[\hat{x}_k(y_k^G)^\top] \neq 0$. 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 (8) 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 $\chi^2_{df}(\alpha)$:

$$\begin{aligned} &\text{Accept } H_0, \text{ if } \hat{d}_k^\top(P_k^d)^{-1}\hat{d}_k \leq \chi^2_{df}(\alpha) \\ &\text{Accept } H_1, \text{ if } \hat{d}_k^\top(P_k^d)^{-1}\hat{d}_k > \chi^2_{df}(\alpha), \end{aligned} \tag{10}$$

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 false positive/negative due to noise, we use the test (10) in a cumulative form. The proposed χ^2 CUSUM detector is characterized by the detector state $S_k \in \mathbb{R}_+$:

$$S_k = \delta S_{k-1} + (\hat{d}_k)^\top(P_k^d)^{-1}\hat{d}_k, \quad S_0 = 0, \tag{11}$$

where $0 < \delta < 1$ is the pre-determined forgetting factor. At each time k, the CUSUM detector (11) 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 (7) with $K_k^G = 0$ and ii) switch the controller to ESC, if

$$S_k > \sum_{i=0}^{\infty} \delta^i \chi^2_{df}(\alpha) = \frac{\chi^2_{df}(\alpha)}{1 - \delta}. \tag{12}$$

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

Remark III.1 *As shown in Fig. 3, the resilient state estimation uses the GPS measurement and the IMU measurement to estimate the state by (6) for the detection purpose as in (9). When the GPS attack is detected, only the IMU measurement is used to estimate the state for the control purpose as in (6) and (7) with $K^G_k = 0$.*

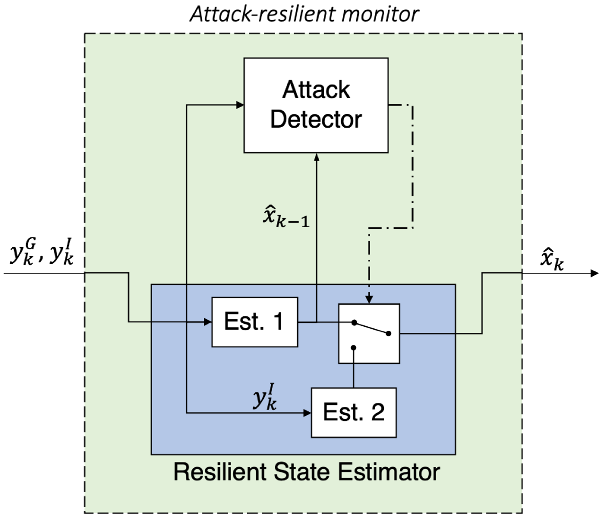


Fig. 3 Resilient state estimator. GPS and IMU measurements are used in the Estimator 1 (Est. 1). Estimator 2 (Est. 2) only uses the IMU measurement. Est. 1 is used to estimate the state by (6) for the detection as in (9). When GPS is free of attacks, Est. 1 is also used to estimate the state for the control since the GPS measurement is trustful. In the presence of the GPS attack, Est. 2 is used for the control.

D. Escape Controller (ESC)

In the presence of the GPS spoofing attack, the variance P_k in (7) of the state estimation errors is strictly increasing and unbounded in time (Thm. 4.2 [17]), and the escape time provides a new criterion for optimal trajectory regeneration with increasing uncertainties. The goal of ESC is to drive the UAV outside of the effective range of the spoofing device within the escape time so that the state estimation error remains within the tolerable region with a predetermined probability. In particular, the *safety constraint* can be formulated as

$$d(x^a_{k^a+k^{esc}}, x_{k^a+k^{esc}}) - r_{effect} > 0, \tag{13}$$

where x^a_k denotes the location of the attacker at time k, k^a and k^{esc} are the attack time and the escape time, and the function $d(a, b)$ measures the distance between a and b. The value r_{effect} is the upper bound of the effective range of the spoofing device. The *safety constraint* (13) implies that ESC should drive the UAV outside of the effective range of the spoofing device within the escape time.

Remark III.2 *We assume that the upper bound of the effective range r_{effect} and the location of the attacker x^a_k are known. Due to hardware constraints, the output power/nominal strength of the spoofing device is bounded where the output power determines the effective range of the spoofing device. The distance between the attacker and UAV can be obtained by monitoring the injected GPS signal strength using Friis transmission equation [27]. The location of the attacker can be estimated similar to locating the epicenter of an earthquake, which can be done with at least three measurements from different seismic stations by measuring a series of GPS signal strengths from different locations of the UAV.*

There are two key challenges for considering the *safety constraint* (13). First, the states and the attacker location are unknown, and their estimates $\hat{x}_i$ and $\hat{x}^a_i$ are subject to stochastic noise. Moreover, we cannot guarantee that the *safety constraint* (13) is always feasible. Addressing the above two challenges, we replace the *safety constraint* (13) by the repulsive potential function [28] 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, $D := d(x^a_{k^a+k^{esc}}, \hat{x}_{k^a+k^{esc}})$. The scaling parameter β is a large constant, which represents a penalty when the constraint has not been fulfilled. Utilizing the soft constraint, we reformulate the MPC problem as follows:

Program III.1

$$\begin{aligned} \min_{u} \; & \sum_{i=k^a}^{k^a+N} \hat{\hat{x}}_{i+1}^{\top} Q_i \hat{\hat{x}}_{i+1} + u_i^{\top} R_i u_i + \sum_{i=k^a+k^{esc}}^{k^a+N} U_{rep}(D_i) \\ s.t. \; & \hat{x}_{i+1} = A\hat{x}_i + Bu_i \\ & h(\hat{x}_i, u_i) \leq 0 \\ & for \;\; i = k^a, k^a+1, \cdots, k^a+N, \end{aligned} \tag{14}$$

where $N \geq k^{esc}$ is the prediction horizon, $\hat{\hat{x}}_i$ is defined as the difference between the state estimation and the goal state at time index i, i.e., $\hat{\hat{x}}_i := \hat{x}_i - x_i^{goal}$, Q_i and R_i are symmetric positive definite weight matrices, and $\hat{x}_i^a$ is the estimate of the attacker location. Value r_{effect} is the upper bound of the effective range of the spoofing device. Inequality (14) is any nonlinear constraint on the state estimation $\hat{x}_i$ (e.g., velocity) and the control input u_i (e.g., acceleration).

Remark III.3 *Each agent obtains the attacker's information and switches to ESC when it is under attack. In the cases that a large portion of the planned trajectory is inside the effective range of the spoofing device, following the virtual target may cause the agent to re-enter the effective range when the agent switches back to the robust controller. Once the agent obtains the attacker information, it will share with the robust controller to avoid re-entering.*

Remark III.4 *Comparing to the use of the repulsive potential function U_{rep} in the collision avoidance literature [29–31], the proposed application of the repulsive potential function in Program III.1 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 happens, 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 III.1 after the escape time.*

IV. Simulation

The scenario in Fig. 1 is used to demonstrate the efficacy of the proposed framework. In the simulation, three UAVs are moving to the desired goal positions simultaneously from different initial locations by using feedback control[*] based on the state estimate from (6). When one of the UAVs is in the effective range of the spoofing device, its state estimate will be no longer trustful. After the GPS measurement is turned off, the only available relative state measurement causes the sensor drift problem [17]. The UAV will switch the controller from the robust controller to ESC when the attack is detected, using ESC to escape away from the attacker within the escape time, while all UAVs will adjust their coordination states if necessary to achieve time-coordination. The online computation of ESC is described in Program III.1 done using `Julia`, and ESC is implemented by using `JuMP` [32] package with `Ipopt` solver.

A. Single UAV Model

We use a double integrator UAV dynamics under the GPS spoofing attack as in [33]. The discrete time state vector x_k considers planar position and velocity at time step k, i.e.

$$x_k = [r_k^x, r_k^y, v_k^x, v_k^y]^{\top},$$

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

where r_k^x, r_k^y denote x, y position coordinates, and v_k^x, v_k^y denote velocity coordinates. We consider the acceleration of UAV as the control input $u_k = [u_k^x, u_k^y]^\top$. We assume that the state constraint and control input constraint are given as

$$\sqrt{(v_k^x)^2 + (v_k^y)^2} \leq 5, \quad \sqrt{(u_k^x)^2 + (u_k^y)^2} \leq 2.$$

With sampling time at 0.1 seconds, the double integrator model is discretized into the following matrices:

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

and the outputs y_k^G and y_k^I are the position measurements from GPS and the velocity measurements from IMU, with the output matrices:

$$C^G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad C^I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The covariance matrices of the sensing and disturbance noises are chosen as $\Sigma_w = 0.1I$, $\Sigma_G = I$ and $\Sigma_I = 0.01I$.

B. Trajectory generation and time coordination for multi-UAV systems

The nominal trajectories of a three-UAV system $g_i(s_{i,k})$, where $i \in \{1, 2, 3\}$, are generated by the cubic Bézier curves [34]

$$g_i(s_{i,k}) \triangleq (1 - s_{i,k})^3 \mathbf{P}_i^{(0)} + 3(1 - s_{i,k})^2 s_{i,k} \mathbf{P}_i^{(1)} + 3(1 - s_{i,k}) s_{i,k}^2 \mathbf{P}_i^{(2)} + s_{i,k}^3 \mathbf{P}_i^{(3)}, \tag{15}$$

where $s_{i,k} \in [0, 1]$ is the coordination state and $\mathbf{P}_i^{(j)}$, where $j \in \{0, 1, 2, 3\}$, are the control points for the agent i. The control points we used are listed in Table 1.

(j) i	(0)	(1)	(2)	(3)
1	$[0,\ 0]^\top$	$[100,\ 100]^\top$	$[10,\ 300]^\top$	$[190,\ 400]^\top$
2	$[200,\ 0]^\top$	$[100,\ 100]^\top$	$[250,\ 200]^\top$	$[200,\ 400]^\top$
3	$[400,\ 0]^\top$	$[450,\ 150]^\top$	$[300,\ 300]^\top$	$[210,\ 400]^\top$

Table 1 Bézier curve control points $\mathbf{P}_i^{(j)}$

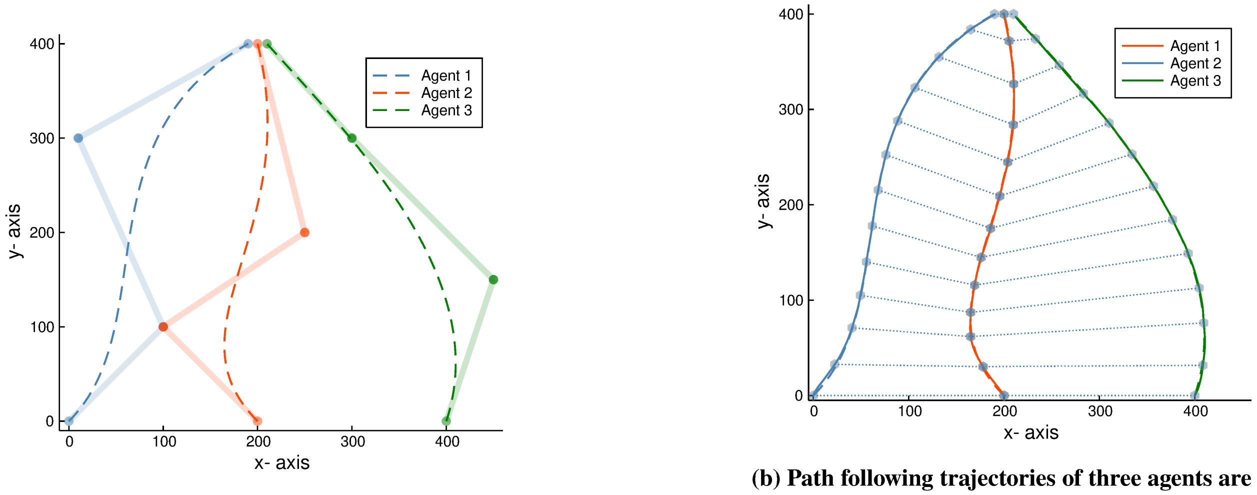
Fig. 4a shows the trajectories generated by (15), and the Bézier curve control points for each agent are marked with colored dots. Agent i aims to follow the trajectory starting from point $\mathbf{P}_i^{(0)}$ and plans to arrive at the destination point $\mathbf{P}_i^{(3)}$ simultaneously. To achieve these goals, the time coordination controller proposed in (5) is used to update the consensus network in (4); then a proportional-derivative (PD) tracking controller is used to track the virtual target generated by the coordination state in (4).

The parameters used in (5) and the PD controller were set to the following values:

$$\rho = \frac{1}{1200}, \quad k_e = 0.005, \quad k_s = 0.005, \quad k_p = 0.05 \quad \text{and} \quad k_i = 0.315,$$

where k_p and k_i are the proportional gain and the derivative gain.

Fig. 4b shows the path following and time coordination results. A series of locations of the three agents are plotted by the hex points. Their connections by the dotted lines indicates that they have the same coordination states. We can see that the time coordination and PD control are both well designed, and all of the agents arrived at goal destination simultaneously.



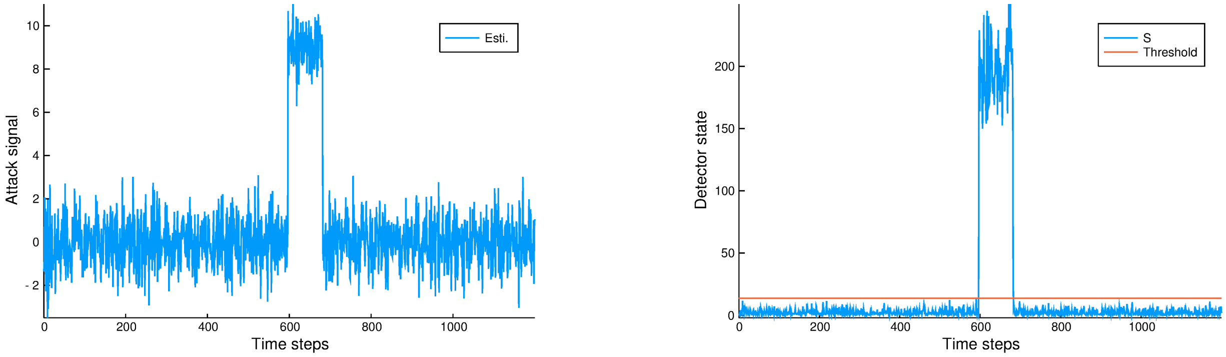
(a) Trajectories of the three agents in dashed lines generated by Bézier curves (15) using the control points summarized in Table 1.

(b) Path following trajectories of three agents are plotted in solid lines. Every three hex points connected by two dotted lines indicate the locations of three agents at the same coordination state.

Fig. 4 Trajectory generation

C. In the presence of GPS spoofing attack

The GPS attack happens when the UAV is in the effective range of the spoofing device. In this attack scenario, the attack signal is $d_k = [10, 10]^\top$ and the effective range of the spoofing device $r_{effect} = 30$. The location of the attacker is $x_k^a = [200, 200]^\top$, which is unknown to the UAV until it is inside the effective range of the spoofing device. The estimation obtained by (9) is shown in Fig. 5a. The detector state S_k can be obtained by using the estimated attack signal as in (11). The abnormal high detector state values shown in Fig. 5b implies that there is an attack. Statistical significance of the attack is tested using the CUSUM detector described in (12) with the significance α at 1%. The threshold is calculated by $\frac{\chi^2_{df}(\alpha)}{1-\delta}$ with $\alpha = 0.01$ and $\delta = 0.15$.



(a) Attack signal estimation.

(b) Attack detection.

Fig. 5 Attack estimation and detection.

ESC in Program III.1 with the prediction horizon $N = k^{esc} + 50$ and the scaling parameter $\beta = 10000$ is used to generate the new trajectory for safety operation. Fig. 6 shows the trajectory of the simulated attack scenario. ESC drives the attacked UAV away from the effective range of the spoofing device; time coordination is achieved and all of the agents arrive at the destination points simultaneously.

Fig. 7 presents how the proposed control framework performs in different cases where $r_{effect} \in \{15, 50, 60, 70\}$. Regardless of the size of r_{effect}, the UAV will escape the effective range within the escape time and achieve time coordination. In Fig. 7a, the attacked UAV can pass the attacker without changing the direction or even its speed, since

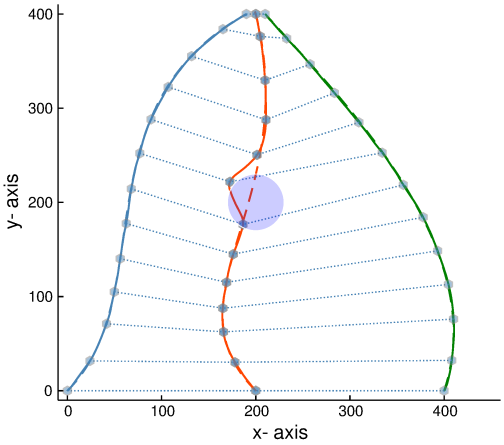
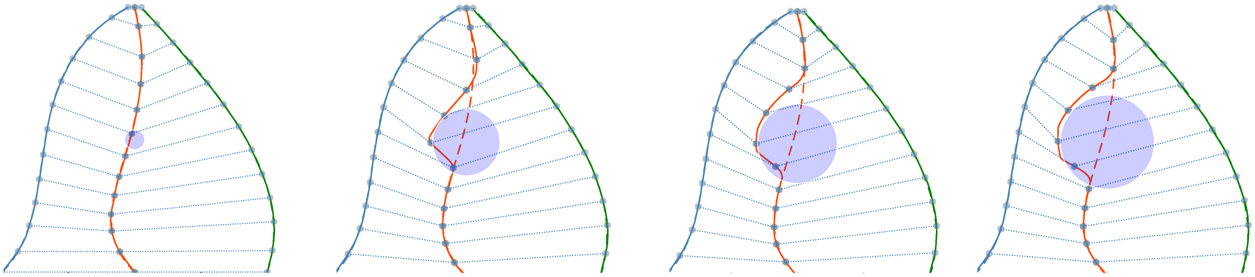


Fig. 6 Trajectory in the presence of the attack. The attacker is located at $[200, 200]^\top$ with $r_{effect} = 30$, which is displayed as the light blue circle.

r_{effect} is small enough. From Fig. 7b to Fig. 7d, the UAV drives away from the effective range within the escape time and tries to get back to the assigned trajectory.



(a) $r_{effect} = 15$ **(b)** $r_{effect} = 50$ **(c)** $r_{effect} = 60$ **(d)** $r_{effect} = 70$

Fig. 7 Trajectories when attacker is located at $[200, 200]^\top$ with different effective ranges.

V. Conclusion

We presented a safety-constrained bi-level control framework for multi-UAV systems that achieves a consensus of coordination states at the *time-critical coordination level* and adapts the UAV(s) to support resilient state estimation and path re-planning at the *safety-critical control level*. In particular, the time coordination and the trajectory generation guaranteed the consensus of coordination states and provide the virtual targets for UAV(s) to follow at the first level. A resilient state estimator was designed and the χ^2 CUSUM algorithm was used for attack detection. The state estimation suffers from the increasing variance due to the limited senor availability in the presence of the GPS spoofing attack. In this case, the robust controller cannot drive the attacked UAV(s) outside the effective range of the spoofing device with the tolerable estimation errors. The large estimation errors will cause safety problems and will fail the global path following mission. To solve these problems, the escape controller (ESC) was designed to escape away from the effective range of the spoofing device within the escape time and complete the global path following mission safely. The simulations of a three-UAV system were given to demonstrate the results.

References

[1] Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, N. S., Khreishah, A., and Guizani, M., “Unmanned Aerial Vehicles (UAVs): A survey on civil applications and key research challenges,” *IEEE Access*, Vol. 7, 2019, pp. 48572–48634.

[2] Chiu, M. T., Xu, X., Wang, K., Hobbs, J., Hovakimyan, N., Huang, T. S., Shi, H., Wei, Y., Huang, Z., Schwing, A., et al., "The 1st Agriculture-Vision Challenge: Methods and Results," *arXiv preprint arXiv:2004.09754*, 2020.

[3] Scherer, J., Yahyanejad, S., Hayat, S., Yanmaz, E., Andre, T., Khan, A., Vukadinovic, V., Bettstetter, C., Hellwagner, H., and Rinner, B., "An autonomous multi-UAV system for search and rescue," *Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, Association for Computing Machinery, New York, NY, USA, 2015, p. 33–38.

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

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

[6] McMilin, E., De Lorenzo, D. S., Walter, T., Lee, T. H., and Enge, P., "Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," *Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, FL*, Citeseer, 2014, pp. 2233–2242.

[7] Montgomery, P. Y., "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," *Radionavigation Laboratory Conference Proceedings*, 2011, pp. 124–130.

[8] Magiera, J., and Katulski, R., "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of Applied Research and Technology*, Vol. 13, No. 1, 2015, pp. 45–57.

[9] Chen, Y.-H., "A study of geometry and commercial off-the-shelf (COTS) antennas for controlled reception pattern antenna (CRPA) arrays," *Proceedings of ION GNSS*, 2012, pp. 907–914.

[10] Chen, Y.-H., Lo, S., Akos, D. M., De Lorenzo, D. S., and Enge, P., "Validation of a controlled reception pattern antenna (CRPA) receiver built from inexpensive general-purpose elements during several live-jamming test campaigns," *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, San Diego, California*, 2013, pp. 154–163.

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

[12] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., "False data injection attacks against state estimation in wireless sensor networks," *49th Conference on Decision and Control (CDC)*, IEEE, 2010, pp. 5967–5972.

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

[14] Pajic, M., Weimer, J., Bezzo, N., Tabuada, P., Sokolsky, O., Lee, I., and Pappas, G. J., "Robustness of attack-resilient state estimators," *ACM/IEEE International Conference on Cyber-Physical Systems*, 2014, pp. 163–174.

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

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

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

[18] Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., and Humphreys, T. E., "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 49, No. 4, 2013, pp. 2250–2267.

[19] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., "False data injection attacks against state estimation in wireless sensor networks," *49th Conference on Decision and Control (CDC)*, IEEE, 2010, pp. 5967–5972.

[20] Feng, Z., Hu, G., and Wen, G., "Distributed consensus tracking for multi-agent systems under two types of attacks," *International Journal of Robust and Nonlinear Control*, Vol. 26, No. 5, 2016, pp. 896–918.

[21] Ding, D., Wang, Z., Ho, D. W., and Wei, G., "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Transactions on Cybernetics*, Vol. 47, No. 8, 2016, pp. 1936–1947.

[22] Gu, N., Wang, D., Peng, Z., and Liu, L., "Adaptive bounded neural network control for coordinated path-following of networked underactuated autonomous surface vehicles under time-varying state-dependent cyber-attack," *ISA Transactions*, 2019.

[23] Mesbahi, M., and Egerstedt, M., *Graph Theoretic Methods in Multiagent Networks*, Vol. 33, Princeton University Press, 2010.

[24] Page, E. S., "Continuous inspection schemes," *Biometrika*, Vol. 41, No. 1/2, 1954, pp. 100–115.

[25] Barnard, G. A., "Control charts and stochastic processes," *Journal of the Royal Statistical Society. Series B (Methodological)*, 1959, pp. 239–271.

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

[27] Friis, H. T., "A Note on a Simple Transmission Formula," *Proceedings of the IRE*, Vol. 34, No. 5, 1946, pp. 254–256.

[28] Ge, S. S., and Cui, Y. J., "New potential functions for mobile robot path planning," *IEEE Transactions on robotics and automation*, Vol. 16, No. 5, 2000, pp. 615–620.

[29] Olfati-Saber, R., "Flocking for multi-agent dynamic systems: algorithms and theory," *IEEE Transactions on Automatic Control*, Vol. 51, No. 3, 2006, pp. 401–420.

[30] Choset, H. M., Hutchinson, S., Lynch, K. M., Kantor, G., Burgard, W., Kavraki, L. E., and Thrun, S., *Principles of Robot Motion: Theory, Algorithms, and Implementation*, MIT press, 2005.

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

[32] Dunning, I., Huchette, J., and Lubin, M., "JuMP: A Modeling Language for Mathematical Optimization," *SIAM Review*, Vol. 59, No. 2, 2017, pp. 295–320.

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

[34] Bartels, R. H., Beatty, J. C., and Barsky, B. A., *An Introduction to Splines for Use in Computer Graphics and Geometric Modelling*, Morgan Kaufmann, 1998.