Secure Control Design for Networked Control Systems With Nonlinear Dynamics Under Time-Delay-Switch Attacks

Arman Sargolzaei, *Senior Member, IEEE*, Federico M. Zegers, Alireza Abbaspour, *Member, IEEE*, Carl D. Crane, and Warren E. Dixon, *Fellow, IEEE*

***Abstract*—A continuous controller is developed for a centralized network control system (NCS), which is composed of agents with nonlinear dynamics subject to a time-delay-switch (TDS) attack and additive disturbances. Since the state tracking error is unmeasurable during TDS attacks, controllers cannot use the state tracking error to coordinate the NCS. Therefore, a novel error signal is designed to address this unique challenge and enable the NCS to achieve a formation control objective. Furthermore, a TDS attack mitigation strategy is developed, which uses both learning- and model-based approaches to estimate an agent's state for TDS attack detection and compensation. Lyapunov–Krasovskii functionals are used in the stability analysis to prove that the tracking errors converge to a steady-state residual, which is a function of the system uncertainty and TDS attack properties. The leader–follower formation control problem for unmanned aerial vehicles based on a pure pursuit guidance law is selected for a simulation study to validate the performance of the proposed method.**

***Index Terms*—Lyapunov–Krasovskii (LK), nonlinear systems, security of networked control systems (NCSs), time-delay-switch (TDS) attack.**

I. Introduction

CENTRALIZED network control systems (NCSs) are widely employed in small-scale industrial applications, such as formation flight, reconnaissance, power grid automation, and search and rescue [1], [2], where it is paramount that NCSs provide these services even in the presence of cyberattacks. In a centralized NCS, every follower agent has a direct line of communication with the leader agent, which is a highly capable asset that can compute control commands for all agents in the NCS using the information provided by the followers. The use of a communication network between the leader and followers gives NCSs a distinct advantage in terms of scalability and design cost when compared with single-agent control systems. However, these benefits come at the expense of increased vulnerability to a range of cyber-physical attacks as any agent or communication link can be targeted. Past results have focused on securing NCSs against two major categories of cyber-physical attacks, namely, false-data-injection (FDI) attacks [3]–[5] and denial-of-service (DoS) attacks [6], [7].

Along with prevention strategies, cyberattack countermeasure algorithms have explored a variety of techniques to manage the operation of control systems under attack. A series of studies [4], [5], [7], [8] analyzed a set of different FDI mitigation techniques. Similarly, Zegers *et al.* [9] used redundant state information to detect and mitigate against Byzantine adversaries, which are the agents capable of launching FDI attacks or ceasing communication with neighboring agents. The results in [10]–[13] investigated DoS attacks and, their more effective counterpart, distributed DoS attacks. Despite these results, NCSs are vulnerable to additional emerging threats, such as the time-delay-switch (TDS) attack [14]. A TDS attack occurs when an adversary injects unknown time-varying delays into any signal used by an NCS, e.g., reference, control, and feedback signals.

Several research efforts have investigated the impact of natural time delays on control systems [15]–[22] and their effects on stability [23], [24]. Pajic *et al.* [23] presented a method for state estimation in control systems in the presence of time delays, noise, and modeling errors. However, the developed algorithm solely relies on state estimation. In [24], a delay-dependent robust method was developed for linear systems under measurement delay. Assuming knowledge of the delays, Zhang *et al.* [24] designed a method, which is robust to the largest delay in the communication channel, leading to a worst-case design approach that may not be as energy efficient when compared to adaptive methods that use less conservative time-varying estimates of the delay. Moreover, such results focus on linear dynamic systems, where the linearity can be exploited to facilitate prediction of the state trajectory despite the delay.

Manuscript received 6 April 2021; revised 3 November 2021; accepted 14 January 2022. Date of publication 24 February 2022; date of current version 30 January 2023. This work was supported by the Air Force Office of Scientific Research under Grant FA9550-19-1-0169. Recommended by Associate Editor S.-J. Chung. *(Corresponding author: Arman Sargolzaei.)*

Arman Sargolzaei is with the Department of Mechanical Engineering, Tennessee Technological University, Cookeville, TN 38501 USA (e-mail: a.sargolzaei@gmail.com).

Federico M. Zegers, Carl D. Crane, and Warren E. Dixon are with the Department of Mechanical and Aerospace Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: fredzeg@ufl.edu; ccrane@ufl.edu; wdixon@ufl.edu).

Alireza Abbaspour is with the Autonomous Driving Division, TuSimple, California, CA 92126 USA (e-mail: alireza.abaspour@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2022.3154354.

Digital Object Identifier 10.1109/TAC.2022.3154354

Prediction and delay compensation for nonlinear systems is inherently more challenging, and while there are fewer results developed for such systems, there has been recent progress. The results in [25]–[33] focused on nonlinear systems with input delays. The proposed techniques only considered actuator delays and have not investigated delays in state measurements or nonlinear systems with state delays. Compensation for known nonlinear systems with state delays was investigated in [34] and [35], and compensation for uncertain nonlinear systems with state delays was explored in [36]–[39]. However, these techniques assume that the state is measurable, where such a strategy is not applicable when TDS attacks are applied to the state. Tan [40] proposed two different estimation methods that use a neural network (NN) for a class of nonlinear systems with time-varying time delays that are caused naturally. The method is more general and accurate than linear time-delay estimation procedures that focus on state measurement delays. However, the method in [40] considered an entirely offline data-driven technique that requires heavy computation and cannot be used to estimate TDS attacks in real-time.

There are only a few studies that investigated TDS-attack detection and compensation [14], [41], [42]. An emotional learning control strategy was developed in [41] to enable a nonlinear system to compensate for TDS attacks. While the design was effective in counteracting the TDS attack, responsiveness was limited to systems with recurrent dynamic behavior. In [14], real-time detection and management of TDS attacks via an adaptive control algorithm was studied. The suggested adaptive control algorithm was further extended by an adaptive channel allocation method in [42]. Moreover, the abovementioned TDS attack detection and compensation techniques are designed for a system with linear dynamics.

The main objective of this article is to design a centralized continuous controller for all agents in an NCS, such that the state of each agent tracks a virtual leader trajectory in the presence of exogenous disturbances and TDS attacks. To the best of our knowledge, previous published methods are not capable of generating robustness to TDS attacks for NCS composed of agents with nonlinear control-affine dynamics. In this work, the state tracking error is only measurable during the absence of TDS attacks, which is unknown *a priori*. Hence, it is not practical to design a controller that utilizes the state tracking error. The proposed controller uses alternative auxiliary error signals, which are always measurable, unaffected by TDS attacks, and facilitate the objective. The stability analysis employs Lyapunov–Krasovskii (LK) functionals to prove uniformly ultimately bounded (UUB) convergence of the tracking error despite the system being exposed to TDS attacks and disturbances [43, Def. 4.6].

In summary, we provide following multiple contributions.

1) Alternative signals capable of rendering safe and stable closed-loop control of an NCS, which is subjected to TDS attacks.
2) A control strategy for nonlinear control-affine dynamical systems that subsume linear time-invariant and linear time-varying systems.

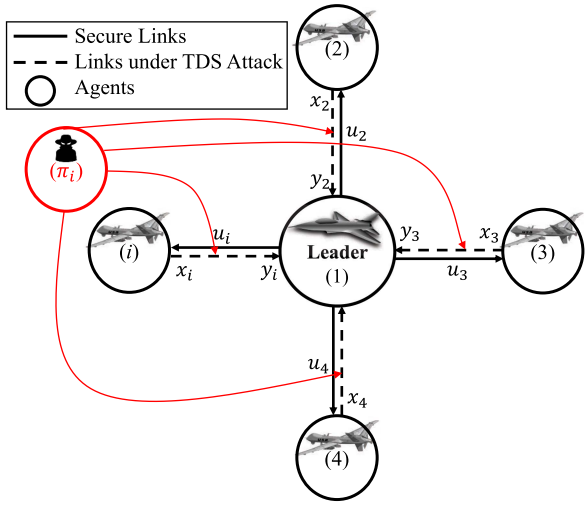

Fig. 1. Illustration of a centralized NCS subject to TDS attacks. In this article, a star graph communication topology is considered, where the leader is denoted by the central node and the followers are denoted by the external nodes. The vulnerable and secure communication/sensor links are shown with dashed and solid lines, respectively.

3) An observer for each agent that leverages model knowledge and an NN architecture to detect TDS attacks and facilitate both safe and stable closed-loop control.

II. Notation

Let $\mathbb{R}$ and $\mathbb{Z}$ denote the set of real numbers and integers, respectively. Let $\mathbb{R}^{m\times n}$ and $\mathbb{Z}^{m\times n}$ denote the the sets of real and integer matrices of dimension $m \times n$, respectively. We write $\mathbb{R}_{>x} \triangleq (x, \infty)$, $\mathbb{R}_{\geq x} \triangleq [x, \infty)$, and $\mathbb{Z}_{>x} \triangleq \mathbb{R}_{>x} \cap \mathbb{Z}$, and $\mathbb{Z}_{\geq x} \triangleq \mathbb{R}_{\geq x} \cap \mathbb{Z}$ given $x \in \mathbb{R}$. Let C^k denote the set of k-continuously differentiable functions for $k \in \mathbb{Z}_{>0}$. The Euclidean norm of a vector $r \in \mathbb{R}^p$ is denoted by $\|r\| \triangleq \sqrt{r^T r}$. The function composition operation is denoted by $\circ$, where given suitable functions f and g, $(f \circ g)(x) = f(g(x))$.

III. Problem Formulation

In this section, we discuss the agent dynamics and the TDS attack model. We then provide a detailed problem statement.

A. Agent Dynamics, Network Topology, and TDS Attack

As illustrated in Fig. 1, consider a centralized NCS composed of $N \in \mathbb{Z}_{>0}$ agents indexed by $\mathcal{V} \triangleq \{1, 2, \ldots, N\}$. The NCS consists of a single leader, indexed by 1, and $N-1$ follower agents. The communication topology of the centralized NCS is modeled by an undirected and static star graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ represents the node set and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ specifies the edge set. With respect to the star graph, the leader is modeled by the central node and the followers are modeled by the outer nodes. In the centralized NCS, each follower $i \in \mathcal{V}$ broadcasts their measurable output $y_i \in \mathbb{R}^{n_i}$ to a leader, which computes a corresponding control input, which is broadcast back to the

follower i. The motion model of agent i is

$$\dot{x}_i(t) = f_i(x_i(t)) + g_i(x_i(t))u_i(t) + d_i(x_i(t), t)$$
$$y_i(t) = \pi_i(x_i(t), \tau_i(t)) \tag{1}$$

where $t_0 \in \mathbb{R}_{\geq 0}$ denotes the initial time, n_i denotes the dimension of the state, $x_i \in \mathbb{R}^{n_i}$ denotes the state, $f_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i}$ denotes the known drift dynamics, $g_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times n_i}$ denotes the known control effectiveness matrix, $d_i : \mathbb{R}^{n_i} \times [t_0, \infty) \to \mathbb{R}^{n_i}$ denotes an unknown disturbance, $u_i \in \mathbb{R}^{n_i}$ denotes the control input, and $\pi_i : \mathbb{R}^{n_i+1} \to \mathbb{R}^{n_i}$ denotes the known output function of agent i.

A TDS attack is generated when an adversary injects a time-delay into a state feedback signal of the NCS. We model a TDS attack on the output of agent i through the use of the output function π_i, defined as

$$\pi_i(x_i(t), \tau_i(t)) \triangleq x_i(t - \tau_i(t)) \tag{2}$$

where $\tau_i : [t_0, \infty) \to \mathbb{R}_{\geq 0}$ denotes an unknown delay.

Assumption 1: For all $i \in \mathcal{V}$, f_i is C^1 and bounded given a bounded argument, i.e., if $\|x\| \leq \bar{x}$ for some $\bar{x} \in \mathbb{R}_{>0}$, then $\|f_i(x)\| \leq \bar{f}$ for some $\bar{f} \in \mathbb{R}_{>0}$ [36].

Assumption 2: For all $i \in \mathcal{V}$, g_i is C^1 and bounded given a bounded argument.

Assumption 3: For all $i \in \mathcal{V}$, the exogenous disturbance is bounded, i.e., $\|d_i(x_i(t), t)\| < \bar{d}_i \; \forall t \geq t_0$, where $\bar{d}_i \in \mathbb{R}_{>0}$.[1]

Assumption 4: For all $i \in \mathcal{V}$, the control effectiveness matrix g_i is invertible, where the inverse of g_i, i.e., g_i^{-1}, is bounded given a bounded argument.

Assumption 5: The graph $\mathcal{G}$ is connected $\forall t \geq t_0$ [44].[2]

Assumption 6: For all $i \in \mathcal{V}$, the delay is differentiable and bounded, i.e., $|\tau_i(t)| \leq \tau_{i,\max} \; \forall t \geq t_0$ for some $\tau_{i,\max} \in \mathbb{R}_{>0}$.[3] Moreover, the derivative of the delay is bounded such that $|\dot{\tau}_i(t)| \leq \dot{\tau}_{i,\max} < 1 \; \forall t \geq t_0$ for some $\dot{\tau}_{i,\max} \in (0, 1)$ [27], [45].

B. Objective

The main objective is to design a centralized-and-continuous controller for each agent in an NCS such that the state x_i described by (1) tracks a virtual leader trajectory $x_{d_i} : [t_0, \infty) \to \mathbb{R}^{n_i}$ for all time, even in the presence of TDS attacks. The tracking error $e_i \in \mathbb{R}^{n_i}$ of agent i is defined as

$$e_i(t) \triangleq x_{d_i}(t) - x_i(t). \tag{3}$$

Assumption 7: For all $i \in \mathcal{V}$, the virtual leader trajectory $x_{d_i} \in \mathbb{R}^{n_i}$ is C^1 where x_{d_i} and $\dot{x}_{d_i}$ are bounded.

Problem Statement: Given the motion model of agent i in (1), a centralized NCS modeled by $\mathcal{G}$, and Assumptions 1–7, design a continuous controller, observer, and TDS attack estimator that renders e_i in (3) UUB for each agent $i \in \mathcal{V}$.

While (3) is only measurable during normal operation, it is unmeasurable during a TDS attack. However, each agent can measure their output y_i, i.e., $x_i(t - \tau_i(t))$, which is a signal that the leader can use to compute the corresponding control for follower i. It should be noted that even though f_i and g_i are known, this article's main technical challenge lies in the fact that the state is not measurable under TDS attacks, which implies $f_i(x_i)$ and $g_i(x_i)$ are also unmeasurable under TDS attacks. Nevertheless, model knowledge can be leveraged to develop state and delay estimates to facilitate safe and stable control. To overcome the challenge of control with state delays, our second objective is to design an observer to estimate the states of the NCS in real-time. The state estimation error $\tilde{x}_i : [t_0, \infty) \to \mathbb{R}^{n_i}$ of agent i is defined as

$$\tilde{x}_i(t) \triangleq x_i(t) - \hat{x}_i(t) \tag{4}$$

where $\hat{x}_i \in \mathbb{R}^{n_i}$ is the state estimate of agent i. Observe that (4) is only measurable during normal operation and is unmeasurable during a TDS attack.

The estimation tracking error, defined as the error between the desired state trajectory and the estimated state of agent i, is denoted by $\hat{e}_i \in \mathbb{R}^{n_i}$ and is given by

$$\hat{e}_i(t) \triangleq x_{d_i}(t) - \hat{x}_i(t). \tag{5}$$

The estimated output of agent i is denoted by $\hat{y}_i \in \mathbb{R}^{n_i}$. The output error between the true output and estimated output of agent i is denoted by $\tilde{y}_i \in \mathbb{R}^{n_i}$ and is defined as

$$\tilde{y}_i(t) \triangleq y_i(t) - \hat{y}_i(t). \tag{6}$$

Let $\delta t \in \mathbb{R}_{>0}$ be a user-defined parameter that determines the time interval $[t - \delta t, t]$. The integral of the output error over $[t - \delta t, t]$ is denoted by $e_{y_i} \in \mathbb{R}^{n_i}$ and is defined as

$$e_{y_i}(t) \triangleq \int_{t-\delta t}^{t} \tilde{y}_i(s) ds. \tag{7}$$

While the signals needed for closed-loop system, i.e., x_i and e_i, are not measurable during TDS attacks, and the auxiliary error $r_i \in \mathbb{R}^{n_i}$ defined as

$$r_i(t) \triangleq \hat{e}_i(t) + e_{y_i}(t) \tag{8}$$

is always measurable and facilitates the objective. Using the measurable error signal in (8), we will develop a controller, observer, and TDS attack compensator that satisfies the problem statement for each follower $i \in \mathcal{V}$.

The rest of this article is organized as follows. The error signals, state observer, and the Lyapunov-based controller are presented in Section IV. The proposed TDS attack estimation algorithm is introduced in Section V. In Section VI, we provide the stability analysis for the control strategy. An application of a centralized NCS, namely, leader–follower formation control of unmanned aerial vehicles (UAVs), is described in Section VII. Finally, the performance of the proposed secure controller is evaluated in Section VIII.

IV. Controller and Observer Development

We now derive the pertinent closed-loop error systems and present both the controller and state observer of agent $i \in \mathcal{V}$. Let $\mathcal{D} \subset \mathbb{R}^{4n_i+5}$ be a user-defined compact and convex set. All subsequent bounds derived using the mean value theorem

[1] In practice, the upper bound on the exogenous disturbance can be estimated from experiments, simulations, prior history, or human expert knowledge [36].

[2] In this work, fixed communication radii are not considered.

[3] Tolerable amount of delay originates from the need to satisfy the inequality in (51).

(MVT) are computed with respect to $\mathcal{D}$. Substituting (1) into the time derivative of (3) yields[4]

$$\dot{e}_i = \dot{x}_{d_i} - f_i(x_i) - g_i(x_i)u_i - d_i. \tag{9}$$

Observe that $f_i(x_i)$ and $g_i(x_i)$ should be interpreted as $(f_i \circ x_i)(t) = f_i(x_i(t))$ and $(g_i \circ x_i)(t) = g_i(x_i(t))$, respectively. Based on the subsequent stability analysis,[5] the controller for agent i is designed as

$$u_i \triangleq (g_i(x_{d_i}))^{-1}\bar{u}_i \tag{10}$$

where $g_i(x_{d_i}) = (g_i \circ x_{d_i})(t)$, $\bar{u}_i \triangleq \dot{x}_{d_i} - f_i(x_{d_i}) + K_i r_i$, and $K_i \in \mathbb{R}_{>0}$ is a user-defined gain. Re-expressing the definition of $\bar{u}_i$ for $\dot{x}_{d_i}$, substituting the result into (9), multiplying both sides of (10) on the left-hand side by g_i, and substituting the result into (9) yields

$$\begin{aligned}\dot{e}_i = & -[f_i(x_i) - f_i(x_{d_i})] - K_i r_i \\ & -[g_i(x_i) - g_i(x_{d_i})]u_i - d_i.\end{aligned} \tag{11}$$

Let $\eta_i \in \mathbb{R}^{n_i \times n_i}$ be defined as

$$\eta_i \triangleq [g_i(x_i) - g_i(x_{d_i})]\,(g_i(x_{d_i}))^{-1} \tag{12}$$

where applying Assumptions 2, 4, and 7 along with the MVT to (12) implies

$$\|\eta_i\| \leq \bar{\eta}_i \|e_i\| \tag{13}$$

for some $\bar{\eta}_i \in \mathbb{R}_{>0}$. Substituting (8), (10), and (12) into (11), while adding and subtracting $K_i x_i$, yields the closed-loop tracking error as

$$\dot{e}_i = -K_i e_i - K_i e_{y_i} + \chi_{1_i} + N_{d_i} \tag{14}$$

where the auxiliary terms $\chi_{1_i} \in \mathbb{R}^{n_i}$ and $N_{d_i} \in \mathbb{R}^{n_i}$ are, respectively, defined as

$$\chi_{1_i} \triangleq -[f_i(x_i) - f_i(x_{d_i})] - K_i \eta_i r_i - K_i \tilde{x}_i \tag{15}$$

and

$$N_{d_i} \triangleq -\eta_i \dot{x}_{d_i} + \eta_i f_i(x_{d_i}) - d_i. \tag{16}$$

Using the MVT, (3), and (13), the auxiliary term in (15) can be upper bounded as

$$\|\chi_{1_i}\| \leq c_i \|e_i\| + K_i \bar{\eta}_i \|e_i\| \|r_i\| + K_i \|\tilde{x}_i\| \tag{17}$$

for some $c_i \in \mathbb{R}_{>0}$. By applying Assumptions 1, 3, and 7 and using (13), the auxiliary term in (16) can be upper bounded as

$$\|N_{d_i}\| \leq \dot{x}_{d_i,\max} \bar{\eta}_i \|e_i\| + f_{i,\max} \bar{\eta}_i \|e_i\| + \bar{d}_i \tag{18}$$

where $\|\dot{x}_{d_i}\| \leq \dot{x}_{d_i,\max}$ and $\|f_i(x_{d_i})\| \leq f_{i,\max}$ for some $\dot{x}_{d_i,\max}, f_{i,\max} \in \mathbb{R}_{>0}$. The state estimate of agent i is generated by the following observer:

$$\begin{aligned}\dot{\hat{x}}_i &\triangleq f_i(\hat{x}_i) + g_i(x_{d_i})u_i + L_i \hat{e}_i \\ \hat{y}_i &\triangleq \pi_i(\hat{x}_i, \hat{\tau}_i)\end{aligned} \tag{19}$$

where $L_i \in \mathbb{R}_{>0}$ is a user-defined gain. Substituting (1), (10), and (19) into the time derivative of (4) yields the closed-loop estimation error as

$$\dot{\tilde{x}}_i = -L_i \tilde{x}_i + \chi_{2_i} - N_{d_i} \tag{20}$$

where $\chi_{2_i} \triangleq f_i(x_i) - f_i(\hat{x}_i) + K_i \eta_i r_i - L_i e_i$. Using the MVT, (4), and (13), the auxiliary term χ_{2_i} can be upper bounded as

$$\|\chi_{2_i}\| \leq \tilde{c}_i \|\tilde{x}_i\| + K_i \bar{\eta}_i \|e_i\| \|r_i\| + L_i \|e_i\| \tag{21}$$

for some $\tilde{c}_i \in \mathbb{R}_{>0}$. Substituting (10) and (19) into the time derivative of (5) yields the closed-loop estimation tracking error as

$$\dot{\hat{e}}_i = -K_i \hat{e}_i - K_i e_{y_i} + \chi_{3_i} \tag{22}$$

where $\chi_{3_i} \triangleq -[f_i(\hat{x}_i) - f_i(x_{d_i})] - L_i \hat{e}_i \in \mathbb{R}^{n_i}$. Using the MVT and (5), the auxiliary term in χ_{3_i} can be upper bounded as

$$\|\chi_{3_i}\| \leq (\hat{c}_i + L_i)\|\hat{e}_i\| \tag{23}$$

for some $\hat{c}_i \in \mathbb{R}_{>0}$. Applying the Leibniz integral rule to (7) and substituting in the output definition in (1), (2), (6), and (19), while adding and subtracting $\hat{x}_i(t - \tau_i)$, yields

$$\dot{e}_{y_i} = \tilde{x}_i(t - \tau_i) + [\hat{x}_i(t - \tau_i) - \hat{x}_i(t - \hat{\tau}_i)] - \tilde{y}_i(t - \delta t). \tag{24}$$

Substituting (22) and (24) into the time derivative of (8) yields the closed-loop auxiliary error

$$\begin{aligned}\dot{r}_i = & -K_i r_i + \chi_{3_i} + \tilde{x}_i(t - \tau_i) + [\hat{x}_i(t - \tau_i) - \hat{x}_i(t - \hat{\tau}_i)] \\ & - \tilde{y}_i(t - \delta t).\end{aligned} \tag{25}$$

V. TDS Attack Compensation

This section presents a TDS attack detection and compensation strategy. Since the unknown delay function τ_i of agent i is defined over a noncompact domain, i.e., $[t_0, \infty)$, the following nonlinear mapping is defined to map $[t_0, \infty)$ into a compact spatial domain [46]. Let $k_{\tau_i} \in \mathbb{R}_{>0}$ be a user-defined saturation coefficient and $f_{\tau_i} : [t_0, \infty) \to [0, 1]$ be defined as

$$f_{\tau_i}(t) \triangleq \frac{k_{\tau_i}(t - t_0)}{k_{\tau_i}(t - t_0) + 1}.$$

Observe that $f_{\tau_i}^{-1} : [0, 1] \to [t_0, \infty)$ defined as

$$f_{\tau_i}^{-1}(\xi) = \frac{k_{\tau_i} t_0 (1 - \xi) + \xi}{k_{\tau_i}(1 - \xi)}$$

is the inverse of f_{τ_i}, where $f_{\tau_i}(t) = \xi$ and $f_{\tau_i}^{-1}(\xi) = t$. Hence, substituting $f_{\tau_i}^{-1}(\xi) = t$ into $\tau_i(t)$ yields

$$\tau_i(t) = \tau_i(f_{\tau_i}^{-1}(\xi)). \tag{26}$$

[4]For brevity, time dependencies are henceforth omitted and the disturbance $d_i(x_i(t), t)$ is expressed as d_i.

[5]Functions f and g are assumed to be bounded given a bounded argument as stated in Assumptions 1 and 2, respectively. By Assumption 7, x_{d_i} is a bounded trajectory, which is contained within a compact set $\mathcal{D}$. Since f and g are continuous functions, they admit a maximum over $\mathcal{D}$ by the extreme value theorem. In addition, by the proof of Theorem 1, we show that if $\Pi_i^*(t_0) \in \mathcal{S}_{\mathcal{D}_i}$, then the trajectories of $\hat{x}$ are bounded for all time $t > 0$. Similarly, the function f is restricted to a compact domain containing $\hat{x}$ is bounded by the extreme value theorem.

Since $(\tau_i \circ f_{\tau_i}^{-1}) : [0,1] \to \mathbb{R}_{\geq 0}$ is a continuous function defined over a compact domain, the Stone–Weierstrass Theorem in [47] is leveraged to express (26) as

$$\tau_i(f_{\tau_i}^{-1}(\xi)) = W_i^T \sigma\left(V_i^T \delta_i\right) + \varepsilon_i. \tag{27}$$

With respect to the right-hand side (RHS) of (27), $\varepsilon_i \in \mathbb{R}$ denotes the function reconstruction error corresponding to the NN representation of τ_i, $n_n \in \mathbb{Z}_{>0}$ denotes the number of neurons, $a \in \mathbb{Z}_{\geq 0}$ is a subsequently defined constant, $W_i \in \mathbb{R}^{(n_n+1)\times 1}$ and $V_i \in \mathbb{R}^{(a+2)\times n_n}$ denote the ideal and unknown weights for the outer and inner layer of the NN, respectively, $\delta_i : [0,1] \to \mathbb{R}^{a+2}$ denotes the subsequently defined input to the NN, and $\sigma : \mathbb{R}^{n_n} \to \mathbb{R}^{n_n+1}$ denotes the stacked vector of bounded and continuous activation functions, which are selected to be C^2 [48].

Let $\hat{\tau}_i : [t_0, \infty) \to \mathbb{R}_{\geq 0}$ denote the delay estimate of agent i induced by a TDS attack. The NN approximation for the time delay affecting agent i with respect to the spatial domain [0, 1] is denoted by $(\hat{\tau}_i \circ f_{\tau_i}^{-1}) : [0,1] \to \mathbb{R}_{\geq 0}$ and defined by

$$\hat{\tau}_i(f_{\tau_i}^{-1}(\xi)) \triangleq \hat{W}_i^T \sigma\left(\hat{V}_i^T \delta_i\right) \tag{28}$$

where $\hat{W}_i \in \mathbb{R}^{(n_n+1)\times 1}$ and $\hat{V}_i \in \mathbb{R}^{(a+2)\times n_n}$ denote the outer and inner NN weight estimates, respectively. Note that $\hat{W}_i$ and $\hat{V}_i$ are composed with $f_{\tau_i}^{-1}$ to ensure all arguments in the RHS of (28) originate from the common domain [0, 1]. Let $\Delta\xi > 0$ and $a \in \mathbb{Z}_{\geq 0}$ be the user-defined parameters that determine sampling points for the input of the NN corresponding to agent i, namely, δ_i. We then define the NN input as

$$\delta_i \triangleq \left[1, \hat{\tau}_i(f_{\tau_i}^{-1}(\xi)), \hat{\tau}_i(f_{\tau_i}^{-1}(\xi) - \Delta\xi), \hat{\tau}_i(f_{\tau_i}^{-1}(\xi) - 2\Delta\xi), \ldots, \hat{\tau}_i(f_{\tau_i}^{-1}(\xi) - a\Delta\xi)\right]^T. \tag{29}$$

Observe that by selecting $a \geq 1$, previous samples of the estimated delay are used as inputs for the NN, which can be shown to improve estimation performance.[6] Note that, for $a = 0$, $\delta_i = [1, \hat{\tau}_i(f_{\tau_i}^{-1}(\xi))]^T$ denotes the traditional NN input that only contains the estimated delay evaluated at the current time, which is expressed in terms of the corresponding spatial point. The delay estimation error $\tilde{\tau}_i \in \mathbb{R}_{\geq 0}$ is defined as

$$\tilde{\tau}_i(t) \triangleq \tau_i(t) - \hat{\tau}_i(t). \tag{30}$$

The outer NN weight error $\tilde{W}_i \in \mathbb{R}^{(n_n+1)\times 1}$ is defined as

$$\tilde{W}_i(t) \triangleq W_i - \hat{W}_i(t). \tag{31}$$

And, the inner NN weight error $\tilde{V}_i \in \mathbb{R}^{(a+2)\times n_n}$ is defined as

$$\tilde{V}_i(t) \triangleq V_i - \hat{V}_i(t). \tag{32}$$

Substituting (27) and (28) into (30) yields

$$\tilde{\tau}_i = W_i^T \sigma\left(V_i^T \delta_i\right) - \hat{W}_i^T \sigma\left(\hat{V}_i^T \delta_i\right) + \varepsilon_i. \tag{33}$$

[6]Future works will characterize the performance benefits produced by the construction of the NN input in (29).

Using a Taylor series approximation, (33) can be expressed as

$$\tilde{\tau}_i = \tilde{W}_i^T \sigma\left(\hat{V}_i^T \delta_i\right) + \hat{W}_i^T \sigma'\left(\hat{V}_i^T \delta_i\right) \tilde{V}_i^T \delta_i + \tilde{N}_i \tag{34}$$

where

$$\tilde{N}_i \triangleq \tilde{W}_i^T \sigma'\left(\hat{V}_i^T \delta_i\right) \tilde{V}_i^T \delta_i + W_i^T \mathcal{O}\left(\tilde{V}_i^T \delta_i\right) + \varepsilon_i$$

$$\sigma'\left(\hat{V}_i^T \delta_i\right) \triangleq \left.\frac{\partial \sigma\left(V_i^T \delta_i\right)}{\partial V_i^T \delta_i}\right|_{\hat{V}_i^T \delta_i}.$$

Observe that $\mathcal{O}$ denotes the higher order terms and that $\|\tilde{N}_i\| \leq \tilde{N}_{i,\max}$ for some $\tilde{N}_{i,\max} \in \mathbb{R}_{>0}$ [49]. Let $\Gamma_{1_i} \in \mathbb{R}^{(n_n+1)\times(n_n+1)}$ and $\Gamma_{2_i} \in \mathbb{R}^{(a+2)\times(a+2)}$ be the symmetric and positive-definite gain matrices. Based on the subsequent stability analysis, let $\hat{\mathbf{W}}_i \triangleq \text{vec}(\hat{W}_i)$ and $\hat{\mathbf{V}}_i \triangleq \text{vec}(\hat{V}_i)$, such that

$$\dot{\hat{\mathbf{W}}}_i \triangleq \text{proj}\left(\text{vec}\left(\Gamma_{1_i} \sigma\left(\hat{V}_i^T \delta_i\right) \omega_{4_i} \|\tilde{y}_i\|^2\right), \hat{\mathbf{W}}_i\right) \tag{35}$$

and

$$\dot{\hat{\mathbf{V}}}_i \triangleq \text{proj}\left(\text{vec}\left(\Gamma_{2_i} \delta_i \omega_{4_i} \|\tilde{y}_i\|^2 \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i)\right), \hat{\mathbf{V}}_i\right) \tag{36}$$

where $\omega_{4_i} \in \mathbb{R}_{>0}$ is a parameter defined in the following section. With respect to (35) and (36), the function $\text{proj}(\cdot,\cdot)$ denotes a Lipschitz continuous projection operator defined in [50, Equation 4], that is, used to bound $\hat{W}_i$ and $\hat{V}_i$ within user-defined compact sets.

Remark 1: Recall that τ_i is bounded by Assumption 6. Furthermore, observe that $\hat{W}_i$ and $\sigma(\hat{V}_i^T \delta_i)$ are bounded by construction. Hence, (28) implies that there exists a $\hat{\tau}_{i,\max} \in \mathbb{R}_{>0}$ such that $|\hat{\tau}_i(t)| \leq \hat{\tau}_{i,\max}$ $\forall t \geq t_0$, $i \in \mathcal{V}$. Moreover, (30) implies that there exists a $\tilde{\tau}_{i,\max} \in \mathbb{R}_{>0}$ such that $|\tilde{\tau}_i(t)| \leq \tilde{\tau}_{i,\max}$ $\forall t \geq t_0$, $i \in \mathcal{V}$ since τ_i and $\hat{\tau}_i$ are bounded.

VI. Stability Analysis

To facilitate the stability analysis and the use of LK-based functionals, let the stacked error system of agent i be denoted by $z_i \in \mathbb{R}^{4n_i}$ and defined as

$$z_i \triangleq [e_i^T,\ \tilde{x}_i^T,\ r_i^T,\ \hat{e}_i^T]^T.$$

Moreover, let $\Pi_i \in \mathbb{R}^{4n_i+4}$ be defined as

$$\Pi_i \triangleq [z_i^T,\ \sqrt{P_{\text{LK}_i}},\ \sqrt{Q_{\text{LK}_i}},\ \sqrt{R_{\text{LK}_i}},\ \sqrt{S_{\text{LK}_i}}]^T \tag{37}$$

where

$$P_{\text{LK}_i} \triangleq \omega_{1_i} \int_{t-\tau_i}^{t} \|\tilde{x}_i(s)\|^2 ds \tag{38}$$

$$Q_{\text{LK}_i} \triangleq \omega_{2_i} \int_{t-\tau_i}^{t} \left(\int_{\theta}^{t} \|\tilde{x}_i(s)\|^2 ds\right) d\theta \tag{39}$$

$$R_{\text{LK}_i} \triangleq \omega_{3_i} \int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds \tag{40}$$

$$S_{\text{LK}_i} \triangleq \omega_{4_i} \int_{t-\delta t}^{t} \left(\int_{\theta}^{t} \|\tilde{y}_i(s)\|^2 ds\right) d\theta \tag{41}$$

where $\omega_{1_i}, \omega_{2_i}, \omega_{3_i}, \omega_{4_i} \in \mathbb{R}_{>0}$ are user-defined constants. The following objects are presented to further facilitate the stability analysis. Let $H_i \in \mathbb{R}_{\geq 0}$ be defined as

$$H_i \triangleq \frac{1}{2}\text{tr}(\tilde{W}_i^T \Gamma_{1_i}^{-1} \tilde{W}_i) + \frac{1}{2}\text{tr}(\tilde{V}_i^T \Gamma_{2_i}^{-1} \tilde{V}_i). \tag{42}$$

And, observe that there exits an $H_{i,\max} \in \mathbb{R}_{>0}$ such that $|H_i(t)| \leq H_{i,\max} \ \ \forall t \geq t_0, i \in \mathcal{V}$ since (31) and (32) are bounded.[7] Furthermore, note that $H_{i,\max}$ can be made small through the selection of Γ_{1_i} and Γ_{2_i}. Using the Cauchy–Schwarz inequality, (6) and (7), one obtains the following useful inequality:

$$-\omega_{4_i}\int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds \leq -\frac{\omega_{4_i}}{2\delta t}\|e_{y_i}\|^2 - \frac{\omega_{4_i}}{2}\int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds. \tag{43}$$

Another pair of useful inequalities are [36]

$$-\omega_{2_i}\int_{t-\tau_i}^{t} \|\tilde{x}_i(s)\|^2 ds \leq -\frac{\omega_{2_i}}{2}\int_{t-\tau_i}^{t} \|\tilde{x}_i(s)\|^2 ds - \frac{\omega_{2_i}}{2\tau_{i,\max}}\int_{t-\tau_i}^{t}\int_{\theta}^{t} \|\tilde{x}_i(s)\|^2 ds d\theta \tag{44}$$

and

$$-\frac{\omega_{4_i}}{2}\int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds \leq -\frac{\omega_{4_i}}{4}\int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds - \frac{\omega_{4_i}}{4\delta t}\int_{t-\delta t}^{t}\int_{\theta}^{t} \|\tilde{y}_i(s)\|^2 ds d\theta. \tag{45}$$

Using the MVT over $\mathcal{D}$, Remark 1, and (30), it follows that

$$\|\hat{x}_i(t-\tau_i) - \hat{x}_i(t-\hat{\tau}_i)\| \leq \mathring{c}_i|\tilde{\tau}_i| \leq \mathring{c}_i\tilde{\tau}_{i,\max} \tag{46}$$

for some $\mathring{c}_i \in \mathbb{R}_{>0}$. The following parameter definitions and sufficient conditions are provided for convenience. Let $\epsilon > 0$ and $\kappa_{p_i} > 0$, for $p \in \{1, 2, \ldots, 12\}$, be user-defined parameters that are selected as

$$\kappa_{1_i}, \kappa_{2_i} \in (0,1), \qquad \kappa_{3_i}, \kappa_{7_i} > \frac{(\bar{d}_i)^2}{2\epsilon}, \quad \kappa_{4_i} > \frac{1}{2}$$
$$\kappa_{9_i} > \frac{\mathring{c}_i^2\tilde{\tau}_{i,\max}^2}{2\epsilon}, \qquad \kappa_{12_i} \in (0,2). \tag{47}$$

Let $\zeta_i \triangleq 1 - \dot{\tau}_i$, and note that $|\zeta_i| \geq \zeta_{i,\min}$, where $\zeta_{i,\min} \triangleq 1 - \dot{\tau}_{i,\max} > 0$ by Assumption 6. Once the parameters in (47) are fixed, we can then select the following parameters:

$$\delta t \leq \min\{\tilde{\tau}_{i,\max} : i \in \mathcal{V}\}$$

$$K_i > \max\left\{\frac{2}{2-(\kappa_{1_i}+\kappa_{2_i})}\left(c_i + \dot{x}_{d_i,\max}\bar{\eta}_i + f_{i,\max}\bar{\eta}_i + \frac{\kappa_{3_i}}{2} + \frac{\dot{x}_{d_i,\max}\bar{\eta}_i\kappa_{5_i}}{2} + \frac{f_{i,\max}\bar{\eta}_i\kappa_{6_i}}{2}\right), \frac{1}{2}\left(\hat{c}_i\kappa_{8_i} + \kappa_{9_i} + \kappa_{10_i} + \kappa_{11_i}\right), \frac{2\hat{c}_i}{2-\kappa_{12_i}}\left(\frac{1}{2\kappa_{8_i}} + 1\right)\right\}$$

$$\omega_{2_i} > 0, \qquad \omega_{3_i} > \frac{1}{2\kappa_{10_i}}, \qquad \omega_{4_i} > \delta t\left(\frac{K_i}{\kappa_{1_i}} + \frac{K_i}{\kappa_{12_i}}\right)$$

$$\omega_{1_i} > \max\left\{\frac{1}{\zeta_{i\min}\kappa_{11_i}}, \frac{4}{\zeta_{i\min}}\left(\omega_{3_i} + \delta t\omega_{4_i} + \omega_{4_i}\tilde{\tau}_{i,\max} + \omega_{4_i}\tilde{N}_{i,\max}\right)\right\}$$

$$L_i > \frac{2\kappa_{4_i}}{2\kappa_{4_i}-1}\left(\tilde{c}_i + \frac{\dot{x}_{d_i,\max}\bar{\eta}_i}{2\kappa_{5_i}} + \frac{f_{i,\max}\bar{\eta}_i}{2\kappa_{6_i}} + \frac{\kappa_{7_i}}{2} + \omega_{1_i} + \tau_{i,\max}\omega_{2_i}\right) \tag{48}$$

where δt is used in (7), K_i is used in (10), L_i is used in (19), and ω_{q_i}, for $q \in \{1, 2, \ldots, 4\}$, is used in (38)–(41), respectively. Based on the sufficient conditions presented in (47) and (48), define the following positive constants:

$$\phi_{1_i} \triangleq K_i\left(1 - \frac{\kappa_{1_i}}{2} - \frac{\kappa_{2_i}}{2}\right) - c_i - \dot{x}_{d_i,\max}\bar{\eta}_i - f_{i,\max}\bar{\eta}_i$$

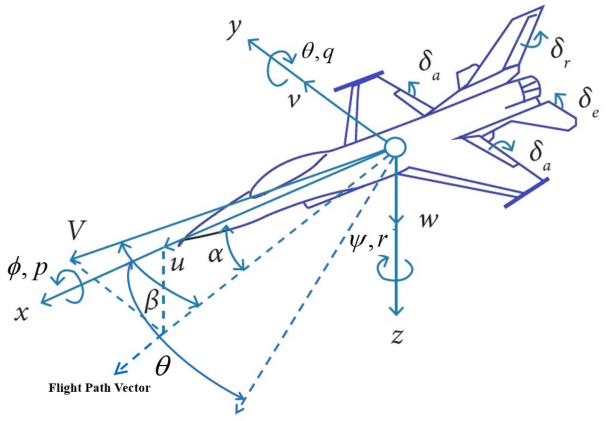

Fig. 2. Aircraft coordinate system [51]. The roll, pitch, and yaw rates about the body-fixed frame of the aircraft are shown by p, q, and r, respectively. The angle of attack (α), side slip angle (β), the Euler angle (ϕ), and pitch angle (θ) are illustrated. Note that the pitch angle will be controlled through the angle of attack.

[7] From the Stone–Weierstrass theorem and the construction of (27), one can show that W_i and V_i are fixed matrices of ideal weights. Moreover, the update laws for $\hat{W}_i(t)$ and $\hat{V}_i(t)$ are embedded within the projection operator, which ensures that $\hat{W}_i(t)$ and $\hat{V}_i(t)$ are bounded for all time-independent of the argument for the projection algorithm. Therefore, $\tilde{W}_i(t)$ and $\tilde{V}_i(t)$ are bounded *a priori*.

$$
\begin{aligned}
&- \frac{\kappa_{3_i}}{2} - \frac{\dot{x}_{d_i,\max}\bar{\eta}_i\kappa_{5_i}}{2} - \frac{f_{i,\max}\bar{\eta}_i\kappa_{6_i}}{2} \\
\phi_{2_i} &\triangleq \frac{\omega_{4_i}}{2\delta t} - \frac{K_i}{2\kappa_{1_i}} - \frac{K_i}{2\kappa_{12_i}} \\
\phi_{3_i} &\triangleq L_i\left(1 - \frac{1}{2\kappa_{4_i}}\right) - \tilde{c}_i - \frac{\dot{x}_{d_i,\max}\bar{\eta}_i}{2\kappa_{5_i}} - \frac{f_{i,\max}\bar{\eta}_i}{2\kappa_{6_i}} - \frac{\kappa_{7_i}}{2} \\
&- \omega_{1_i} - \tau_{i,\max}\omega_{2_i} \\
\phi_{4_i} &\triangleq K_i - \frac{\hat{c}_i\kappa_{8_i}}{2} - \frac{\kappa_{9_i}}{2} - \frac{\kappa_{10_i}}{2} - \frac{\kappa_{11_i}}{2} \\
\phi_{5_i} &\triangleq K_i\left(1 - \frac{\kappa_{12_i}}{2}\right) - \frac{\hat{c}_i}{2\kappa_{8_i}} - \hat{c}_i \qquad (49) \\
\phi_{6_i} &\triangleq \omega_{3_i} - \frac{1}{2\kappa_{10_i}}, \quad \phi_{7_i} \triangleq \frac{\zeta_{i\min}\omega_{1_i}}{2} - \frac{1}{2\kappa_{11_i}} \\
\phi_{8_i} &\triangleq \frac{\zeta_{i\min}\omega_{1_i}}{4} - \omega_{3_i} - \omega_{4_i}\tilde{N}_{i,\max} \\
\phi_{9_i} &\triangleq \frac{\bar{d}_i^2}{2\kappa_{3_i}} + \frac{\bar{d}_i^2}{2\kappa_{7_i}} + \frac{\mathring{c}_i^2\tilde{\tau}_{i,\max}^2}{2\kappa_{9_i}} + \frac{\zeta_{i\min}\omega_{1_i}\mathring{c}_i^2\tilde{\tau}_{i,\max}^2}{2} \\
\phi_{i,\min} &\triangleq \min\left\{\phi_{1_i}, \phi_{3_i}, \phi_{4_i}, \phi_{5_i}\right\} \\
\phi_{i,\min}^* &\triangleq \min\left\{\frac{\phi_{i,\min}}{2}, \frac{\zeta_{i,\min}\omega_{2_i}}{2\omega_{1_i}}, \frac{\zeta_{i,\min}}{2\tau_{i,\max}}, \frac{\omega_{4_i}}{4\omega_{3_i}}, \frac{1}{4\delta t}\right\}
\end{aligned}
$$

where $\phi_{1,i}$ through $\phi_{9,i}$ originate from (58). Let $\Pi_i^* \triangleq [\Pi_i^T, \sqrt{H_i}]^T \in \mathbb{R}^{4n_i+5}$, and define the bounding function $\rho_i : \mathbb{R} \to \mathbb{R}$ as

$$
\begin{aligned}
\rho_i\left(\|z_i\|\right) \triangleq\ & 2K_i\bar{\eta}_i\|z_i\| + \frac{L_i\kappa_{4_i}}{2} + \frac{K_i}{2\kappa_{2_i}} + \frac{L_i\kappa_{8_i}}{2} \\
&+ \frac{L_i}{2\kappa_{8_i}} + L_i. \qquad (50)
\end{aligned}
$$

Observe that ρ_i is a positive, nondecreasing, and radially unbounded function. The domain over which the Lyapunov analysis is performed is defined by

$$
\mathcal{D}_i \triangleq \left\{\Pi \in \mathbb{R}^{4n_i+5} : \|\Pi\| \leq \inf \rho_i^{-1}\left(\left[\phi_{i,\min}^*, \infty\right)\right)\right\}
$$

where $\mathcal{D}_i \subseteq \mathcal{D}$ and the preimage of $A \subset \mathbb{R}$ under ρ_i is defined as $\rho_i^{-1}(A) \triangleq \{a \in \mathbb{R} : \rho_i(a) \in A\}$. The set of admissible initial conditions is defined by

$$
\mathcal{S}_{\mathcal{D}_i} \triangleq \left\{\Pi \in \mathbb{R}^{4n_i+5} : \|\Pi\| \leq \frac{\sqrt{2}}{2}\inf \rho_i^{-1}\left(\left[\phi_{i,\min}^*, \infty\right)\right)\right\}.
$$

Given the abovementioned definitions, select Γ_{1_i}, Γ_{2_i}, and the parameters in (47) and (48) such that

$$
2\sqrt{2H_{i,\max} + \frac{2\phi_{9_i}}{\phi_{i,\min}^*}} < \inf \rho_i^{-1}\left(\left[\phi_{i,\min}^*, \infty\right)\right). \qquad (51)
$$

Note that the condition in (51) implies that $\tau_{i,\max}$ cannot be too large, otherwise the desired UUB result is unattainable. Recall that $H_{i,\max}$ can be made small through the appropriate selection of Γ_{1_i} and Γ_{2_i}. The term $\phi_{i,\min}^*$ can be made large through the selection of large K_i, L_i, and ω_{2_i} and small $\omega_{1_i}, \omega_{3_i}, \tau_{i,\max}$, and δt. Since ρ_i is a nondecreasing function, it follows that the RHS of (51) is nondecreasing with respect to $\phi_{i,\min}^*$. Hence, (51) can be satisfied for some selection of parameters, provided the delay is small enough. We now present the main result.

Theorem 1: The controller in (10), observer in (19), and TDS-attack estimator in (28) ensure the semiglobal UUB tracking, in the sense that

$$
\limsup_{t\to\infty} \|\Pi_i^*(t)\| \leq 2\sqrt{2H_{i,\max} + \frac{2\phi_{9_i}}{\phi_{i,\min}^*}} \qquad (52)
$$

provided Assumptions 1–7 are satisfied, the sufficient conditions listed in (47), (48), and (51) are satisfied, and the initial condition of the system is selected such that $\Pi_i^*(t_0) \in \mathcal{S}_{\mathcal{D}_i}$.

Proof: Let $V_{L_i} : \mathcal{D}_i \to \mathbb{R}_{\geq 0}$ be a common Lyapunov function candidate for agent $i \in \mathcal{V}$ defined as

$$
\begin{aligned}
V_{L_i} \triangleq\ & \frac{1}{2}e_i^T e_i + \frac{1}{2}\tilde{x}_i^T\tilde{x}_i + \frac{1}{2}r_i^T r_i + \frac{1}{2}\hat{e}_i^T\hat{e}_i + P_{\mathrm{LK}_i} \\
&+ Q_{\mathrm{LK}_i} + R_{\mathrm{LK}_i} + S_{\mathrm{LK}_i} + H_i. \qquad (53)
\end{aligned}
$$

Note that V_{L_i} characterizes the objective at the agent level. The Lyapunov function candidate can be bounded below and above as

$$
\frac{1}{2}\|\Pi_i^*\|^2 \leq V_{L_i} \leq \|\Pi_i\|^2 + H_{i,\max}. \qquad (54)
$$

Using (14), (20), (22), and (25), applying the Leibniz integral rule to (38)–(41), substituting the result into the time derivative of (53), and applying the Cauchy–Schwarz inequality, yields

$$
\begin{aligned}
\dot{V}_{L_i} \leq\ & -K_i\|e_i\|^2 + K_i\|e_i\|\|e_{y_i}\| + \|e_i\|\|\chi_{1_i}\| + \|e_i\|\|N_{d_i}\| \\
&- L_i\|\tilde{x}_i\|^2 + \|\chi_{2_i}\|\|\tilde{x}_i\| + \|N_{d_i}\|\|\tilde{x}_i\| - K_i\|r_i\|^2 \\
&+ \|r_i\|\|\chi_{3_i}\| + \|r_i\|\|\tilde{x}_i(t-\tau_i)\| + \|r_i\|\|\hat{x}_i(t-\tau_i) \\
&- \hat{x}_i(t-\hat{\tau}_i)\| + \|r_i\|\|\tilde{y}_i(t-\delta t)\| - K_i\|\hat{e}_i\|^2 \\
&+ K_i\|\hat{e}_i\|\|e_{y_i}\| + \|\hat{e}_i\|\|\chi_{3_i}\| + \omega_{1_i}\|\tilde{x}_i(t)\|^2 \\
&- \zeta_i\omega_{1_i}\|\tilde{x}_i(t-\tau_i)\|^2 + \tau_i\omega_{2_i}\|\tilde{x}_i(t)\|^2 + \omega_{3_i}\|\tilde{y}_i(t)\|^2 \\
&- \omega_{3_i}\|\tilde{y}_i(t-\delta t)\|^2 + \delta t\omega_{4_i}\|\tilde{y}_i(t)\|^2 \\
&- \zeta_i\omega_{2_i}\int_{t-\tau_i}^{t}\|\tilde{x}_i(s)\|^2 ds - \omega_{4_i}\int_{t-\delta t}^{t}\|\tilde{y}_i(s)\|^2 ds \\
&+ \mathrm{tr}\left(\tilde{W}_i^T\Gamma_{1_i}^{-1}\dot{\tilde{W}}_i\right) + \mathrm{tr}\left(\tilde{V}_i^T\Gamma_{2_i}^{-1}\dot{\tilde{V}}_i\right). \qquad (55)
\end{aligned}
$$

TABLE I
LEADER AND VIRTUAL LEADER TRAJECTORY SPECIFICATIONS

	Leader's Position	Virtual Leader's Position
Longitudinal Direction (X axis)	$X_l = 110 + 150t$	$X_{vl} = 100 + 150t$
Lateral Direction (Y axis)	$Y_l = 110 + 40\sin(0.1t) + 2t$	$Y_{vl} = 100 + 40\sin(0.1t) + 2t$
Horizontal Direction (Z axis)	$H_l = 1100 + 40\cos(0.1t) + 2t$	$H_{vl} = 1100 + 40\cos(0.1t) + 2t$

TABLE II
ROOT MEAN SQUARE ERROR OF FOLLOWER TRACKING DESIRED ROLL, PITCH, AND YAW RATES IN THE PRESENCE OF A TDS ATTACK FOR SCENARIO I

State	Traditional controller [51]	Proposed controller
Roll rate	4.24	3.86
Pitch rate	1.81	1.78
Yaw rate	0.18	0.16

Using (17), (18), (21), (23), $\dot{\tilde{V}}_i = -\dot{\hat{V}}_i$, and $\dot{\tilde{W}}_i = -\dot{\hat{W}}_i$, (55) can be upper bounded by

$$\begin{aligned}\dot{V}_{L_i} \le & -K_i \|e_i\|^2 + K_i \|e_i\| \|e_{y_i}\| + \|e_i\| \left(c_i \|e_i\| + K_i \|\tilde{x}_i\| \right. \\ & \left. + K_i\bar{\eta}_i \|e_i\| \|r_i\|\right) + \|e_i\| \left(\dot{x}_{d_i,\max}\bar{\eta}_i \|e_i\| + f_{i,\max}\bar{\eta}_i \|e_i\| \right. \\ & \left. + \bar{d}_i\right) + \left(\tilde{c}_i \|\tilde{x}_i\| + K_i\bar{\eta}_i \|e_i\| \|r_i\| + L_i \|e_i\|\right) \|\tilde{x}_i\| \\ & - L_i \|\tilde{x}_i\|^2 + \left(\dot{x}_{d_i,\max}\bar{\eta}_i \|e_i\| + f_{i,\max}\bar{\eta}_i \|e_i\| + \bar{d}_i\right) \|\tilde{x}_i\| \\ & - K_i \|r_i\|^2 + \left(\hat{c}_i + L_i\right) \|r_i\| \|\hat{e}_i\| + \|r_i\| \|\hat{x}_i\left(t - \tau_i\right) \\ & - \hat{x}_i\left(t - \hat{\tau}_i\right)\| + \|r_i\| \|\tilde{y}_i\left(t - \delta t\right)\| + \|r_i\| \|\tilde{x}_i\left(t - \tau_i\right)\| \\ & - K_i \|\hat{e}_i\|^2 + K_i \|\hat{e}_i\| \|e_{y_i}\| + \left(\hat{c}_i + L_i\right) \|\hat{e}_i\|^2 \\ & + \omega_{1_i}\|\tilde{x}_i(t)\|^2 - \zeta_i\omega_{1_i}\|\tilde{x}_i(t - \tau_i)\|^2 + \tau_i\omega_{2_i}\|\tilde{x}_i(t)\|^2 \\ & + \delta t\omega_{4_i}\|\tilde{y}_i(t)\|^2 + \omega_{3_i}\|\tilde{y}_i(t)\|^2 - \omega_{3_i}\|\tilde{y}_i(t - \delta t)\|^2 \\ & - \zeta_i\omega_{2_i}\int_{t-\tau_i}^{t} \|\tilde{x}_i(s)\|^2 ds - \omega_{4_i}\int_{t-\delta t}^{t} \|\tilde{y}_i(s)\|^2 ds \\ & - \text{tr}\left(\tilde{W}_i^T\Gamma_{1_i}^{-1}\dot{\hat{W}}_i\right) - \text{tr}\left(\tilde{V}_i^T\Gamma_{2_i}^{-1}\dot{\hat{V}}_i\right).\end{aligned} \tag{56}$$

Using the MVT over $\mathcal{D}_i$, Remark 1, (1), (2), (6), (19), and (30) while adding and subtracting $\hat{x}_i(t - \tau_i)$, it follows that $\|\tilde{y}_i\| \le \|\tilde{x}_i(t - \tau_i)\| + \mathring{c}_i\tilde{\tau}_{i,\max}$, where the Young's inequality yields

$$\begin{aligned}\|\tilde{y}_i\|^2 \le & \ \|\tilde{x}_i(t - \tau_i)\|^2 + 2\mathring{c}_i\tilde{\tau}_{i,\max}\|\tilde{x}_i(t - \tau_i)\| + \mathring{c}_i^2\tilde{\tau}_{i,\max}^2 \\ \le & \ \|\tilde{x}_i(t - \tau_i)\|^2 + 2\left(\frac{1}{2}\mathring{c}_i^2\tilde{\tau}_{i,\max}^2 + \frac{1}{2}\|\tilde{x}_i(t - \tau_i)\|^2\right) \\ & + \mathring{c}_i^2\tilde{\tau}_{i,\max}^2 \\ \le & \ 2\|\tilde{x}_i(t - \tau_i)\|^2 + 2\mathring{c}_i^2\tilde{\tau}_{i,\max}^2.\end{aligned} \tag{57}$$

Using (35), (36), (43), (46), (57), and the Young's inequality, (56) can be upper bounded by

$$\begin{aligned}\dot{V}_{L_i} \le & \left(\frac{K_i\kappa_{1_i}}{2} + c_i + \frac{K_i\kappa_{2_i}}{2} + \dot{x}_{d_i,\max}\bar{\eta}_i + f_{i,\max}\bar{\eta}_i + \frac{\kappa_{3_i}}{2}\right. \\ & \left. + \frac{\dot{x}_{d_i,\max}\bar{\eta}_i\kappa_{5_i}}{2} + \frac{f_{i,\max}\bar{\eta}_i\kappa_{6_i}}{2} - K_i\right)\|e_i\|^2 + \left(\frac{K_i}{2\kappa_{1_i}}\right. \\ & \left. + \frac{K_i}{2\kappa_{12_i}} - \frac{\omega_{4_i}}{2\delta t}\right)\|e_{y_i}\|^2 + \left(2K_i\bar{\eta}_i\|z_i\| + \frac{L_i\kappa_{4_i}}{2} + \frac{K_i}{2\kappa_{2_i}}\right. \\ & \left. + \frac{L_i\kappa_{8_i}}{2} + \frac{L_i}{2\kappa_{8_i}} + L_i\right)\|z_i\|^2 + \left(\tilde{c}_i + \frac{L_i}{2\kappa_{4_i}} + \frac{\dot{x}_{d_i,\max}\bar{\eta}_i}{2\kappa_{5_i}}\right. \\ & \left. + \frac{f_{i,\max}\bar{\eta}_i}{2\kappa_{6_i}} + \frac{\kappa_{7_i}}{2} + \omega_{1_i} + \tau_{i,\max}\omega_{2_i} - L_i\right)\|\tilde{x}_i\|^2 \\ & + \left(\frac{\bar{d}_i^2}{2\kappa_{3_i}} + \frac{\bar{d}_i^2}{2\kappa_{7_i}} + \frac{\zeta_{i\min}\omega_{1_i}}{2}\mathring{c}_i^2\tilde{\tau}_{i,\max}^2 + \frac{1}{2\kappa_{9_i}}\mathring{c}_i^2\tilde{\tau}_{i,\max}^2\right) \\ & + \left(\frac{\hat{c}_i\kappa_{8_i}}{2} + \frac{\kappa_{9_i}}{2} + \frac{\kappa_{10_i}}{2} + \frac{\kappa_{11_i}}{2} - K_i\right)\|r_i\|^2 \\ & + \left(\frac{\hat{c}_i}{2\kappa_{8_i}} + \frac{K_i\kappa_{12_i}}{2} + \hat{c}_i - K_i\right)\|\hat{e}_i\|^2 + \left(\frac{1}{2\kappa_{10_i}} - \omega_{3_i}\right) \\ & \times \|\tilde{y}_i\left(t - \delta t\right)\|^2 + \left(\frac{1}{2\kappa_{11_i}} - \frac{\zeta_{i\min}\omega_{1_i}}{2}\right)\|\tilde{x}_i\left(t - \tau_i\right)\|^2 \\ & + \left(\omega_{3_i} + \omega_{4_i}\tilde{N}_{i,\max} - \frac{\zeta_{i\min}\omega_{1_i}}{4}\right)\|\tilde{y}_i\|^2 \\ & - \zeta_{i,\min}\omega_{2_i}\int_{t-\tau_i}^{t}\|\tilde{x}_i(s)\|^2 ds - \frac{\omega_{4_i}}{2}\int_{t-\delta t}^{t}\|\tilde{y}_i(s)\|^2 ds.\end{aligned} \tag{58}$$

Using (44), (45), the auxiliary parameters in (49), and the bounding function in (50), (58) can be further upper bounded by

$$\begin{aligned}\dot{V}_{L_i} \le & -\left(\frac{\phi_{i,\min}}{2} - \rho_i\left(\|z_i\|\right)\right)\|z_i\|^2 - \frac{\phi_{i,\min}}{2}\|z_i\|^2 + \phi_{9_i} \\ & - \frac{\zeta_{i,\min}\omega_{2_i}}{2\omega_{1_i}}P_{\text{LK}_i} - \frac{\zeta_{i,\min}}{2\tau_{i,\max}}Q_{\text{LK}_i} - \frac{\omega_{4_i}}{4\omega_{3_i}}R_{\text{LK}_i} - \frac{S_{\text{LK}_i}}{4\delta t} \\ \le & -\left(\phi_{i,\min}^* - \rho_i\left(\|z_i\|\right)\right)\|z_i\|^2 - \phi_{i,\min}^*\|\Pi_i\|^2 + \phi_{9_i}.\end{aligned} \tag{59}$$

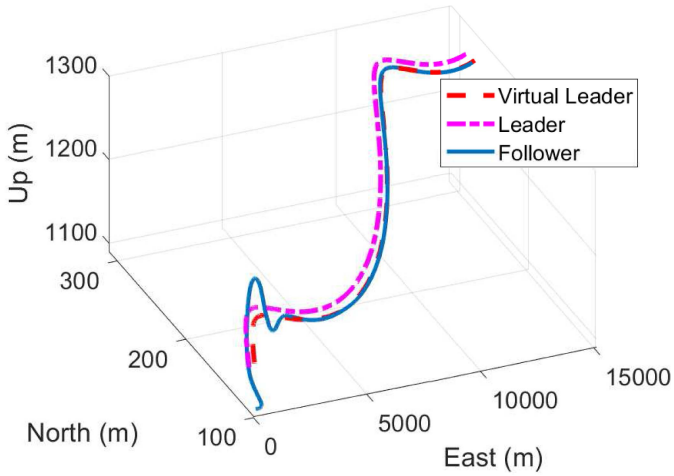

Fig. 3. Leader, virtual leader, and follower trajectories under the proposed strategy, where the follower is subjected to a TDS attack and an environmental disturbance for Scenario I. The simulation is 100-s long. A TDS attack is injected at the 1-s time point. The follower tracks the virtual leader under disturbances and TDS attacks.

Using (54) and recalling that $\Pi_i^* \in \mathcal{D}_i$, it follows that

$$\begin{aligned}\dot{V}_{L_i} \leq & -\left(\phi_{i,\min}^* - \rho_i\left(\|z_i\|\right)\right)\|z_i\|^2 - \frac{\phi_{i,\min}^*}{4}\|\Pi_i^*\|^2 + \phi_{9_i} \\ & + \phi_{i,\min}^* H_{i,\max} - \frac{\phi_{i,\min}^*}{4}\|\Pi_i^*\|^2 \\ \leq & -\frac{\phi_{i,\min}^*}{4}\|\Pi_i^*\|^2 \qquad \forall \|\Pi_i^*\| \geq 2\sqrt{H_{i,\max} + \frac{\phi_{9_i}}{\phi_{i,\min}^*}}.\end{aligned} \tag{60}$$

Invoking [43, Th. 4.18], we conclude the semiglobal UUB tracking, where (52) holds, provided $\Pi_i^*(t_0) \in \mathcal{S}_{\mathcal{D}_i}$. Last, observe that $\Pi_i^* \in \mathcal{L}_\infty$, which implies $e_i,\ \tilde{x}_i,\ r_i,\ \hat{e}_i \in \mathcal{L}_\infty$. Hence, (10), $r_i \in \mathcal{L}_\infty$, and Assumptions 1, 4, and 7 can be used to conclude that $u_i \in \mathcal{L}_\infty$. Moreover, $\hat{x}_i \in \mathcal{L}_\infty$ since $\hat{e}_i,\ x_{d_i} \in \mathcal{L}_\infty$. Last, $e_{y_i} \in \mathcal{L}_\infty$ since $r_i,\ \hat{e}_i \in \mathcal{L}_\infty$. ■

VII. Simulation Study: Leader–Follower Formation Control of UAVs

The proposed algorithm is implemented and evaluated on a centralized leader–follower NCS, where each agent is modeled as a WVU YF-22 unmanned aircraft. This model was chosen to exemplify the capability of the proposed result in which a six-degrees-of-freedom (DoFs) nonlinear system is controlled to achieve leader–follower formation flight. The objective is to perform the formation control while tracking a virtual leader trajectory in the presence of TDS attacks and environmental disturbances.

A. Nonlinear Dynamic Model of UAV

The nonlinear dynamic model of the aircraft is described by the six-DoFs equations of motion in [52]. As illustrated in the Fig. 2, $p_i \in \mathbb{R}$, $q_i \in \mathbb{R}$, and $r_{y_i} \in \mathbb{R}$ are the roll, pitch, and yaw rates, respectively, about the body-fixed frame of the aircraft, which are described by

$$\begin{aligned}\dot{p}_i = & \frac{1}{I_{x_i}I_{z_i} - I_{xz_i}^2}\left[(I_{z_i}I_{a_i} + I_{xz_i}n_{a_i})r_{y_i}\right. \\ & + I_{xz_i}(I_{x_i} - I_{y_i} + I_{z_i})p_i q_i \\ & \left. + \left(I_{z_i}(I_{y_i} - I_{z_i}) - I_{xz_i}^2\right)q_i r_{y_i}\right]\end{aligned} \tag{61}$$

$$\dot{q}_i = \frac{1}{I_{y_i}}[p_i r_{y_i}(I_{z_i} - I_{x_i}) + m_{a_i} + I_{xz_i}(r_{y_i}^2 - p_i^2)] \tag{62}$$

$$\begin{aligned}\dot{r}_{y_i} = & \frac{1}{I_{x_i}I_{z_i} - I_{xz_i}^2}\left[((I_{x_i} - I_{y_i} + I_{z_i})I_{xz_i})\,q_i r_{y_i}\right. \\ & \left. + \left(I_{x_i}(I_{x_i} - I_{y_i}) + I_{xz_i}^2\right)p_i q_i + (I_{xz_i}I_{a_i} + I_{x_i}n_{a_i})\right]\end{aligned} \tag{63}$$

where the moments of inertia about the x-, y-, and z-axis are $I_{x_i} \in \mathbb{R}$, $I_{y_i} \in \mathbb{R}$, and $I_{z_i} \in \mathbb{R}$, respectively. Note that $n_{a_i} \in \mathbb{R}$, $l_{a_i} \in \mathbb{R}$, and $m_{a_i} \in \mathbb{R}$ are aerodynamic yawing, rolling, and pitching moments, respectively, and the inertia moment about the x–z-plane is defined by $I_{xz_i} \in \mathbb{R}$.

The angle of attack $\alpha_i \in \mathbb{R}$, the side slip angle $\beta_i \in \mathbb{R}$, the Euler angle $\phi_i \in \mathbb{R}$, and the pitch angle $\theta_i \in \mathbb{R}$ for agent i are described by

$$\begin{aligned}\dot{\beta}_i = & \frac{1}{m_i v_i}\left[m_i g_{a_i}\sin(\theta_i - \alpha_i)\sin\phi_i - T_i\sin\beta_i\cos\alpha_i\right. \\ & \left. + F_{Y_i}\cos\beta_i\right] - r_i\cos\alpha_i + p_i\sin\alpha_i\end{aligned} \tag{64}$$

$$\begin{aligned}\dot{\alpha}_i = & \frac{1}{m_i v_i\cos\beta}\left[-L_i^* + m_i g_{a_i}\cos(\theta_i - \alpha_i)\cos\phi_i\right. \\ & \left. - T_i\sin\alpha_i\right] + q_i - (r_{y_i}\sin\alpha_i + p_i\cos\alpha_i)\tan\beta_i\end{aligned} \tag{65}$$

$$\dot{\phi}_i = p_i + (q_i\sin\phi_i + r_{y_i}\cos\phi_i)\tan\theta_i \tag{66}$$

$$\dot{\theta}_i = -r_{y_i}\sin\phi_i + q_i\cos\phi_i \tag{67}$$

where $m_i \in \mathbb{R}_{\geq 0}$ is the mass of UAV and $g_{a_i} \in \mathbb{R}_{\geq 0}$ is the magnitude of the acceleration due to gravity. The indicated air speed $v_i \in \mathbb{R}$ is described as

$$\begin{aligned}\dot{v}_i = & \frac{1}{m_i}\left[F_{Y_i}\sin\beta_i - m_i g_{a_i}\sin(\theta_i - \alpha_i) - D_i\right. \\ & \left. + T_i\cos\beta_i\cos\alpha_i\right]\end{aligned} \tag{68}$$

where $T_i \in \mathbb{R}$ is the thrust, $L_i^* \in \mathbb{R}$ is the lift, $D_i \in \mathbb{R}$ is the drag force, and $F_{Y_i} \in \mathbb{R}$ is the aerodynamic side force.

B. Dynamic Model of NCS

For simplicity, we assume that all agents have the same nonlinear dynamic model. Moreover, this article uses a 3-D pure pursuit (PP) guidance law for the guidance system design. The guidance system's task in a formation flight is to ensure the follower UAVs track the leader UAV while preserving a desired relative spacing. This is achieved by maintaining the line of sight between the follower and leader aircrafts. More details about the PP algorithm can be found in [51]. Due to the fact that the PP algorithm is not designed to control velocity, we designed a velocity controller based on the developed dynamic inversion technique. The velocity controller has two loops. The inner-loop controls the velocity

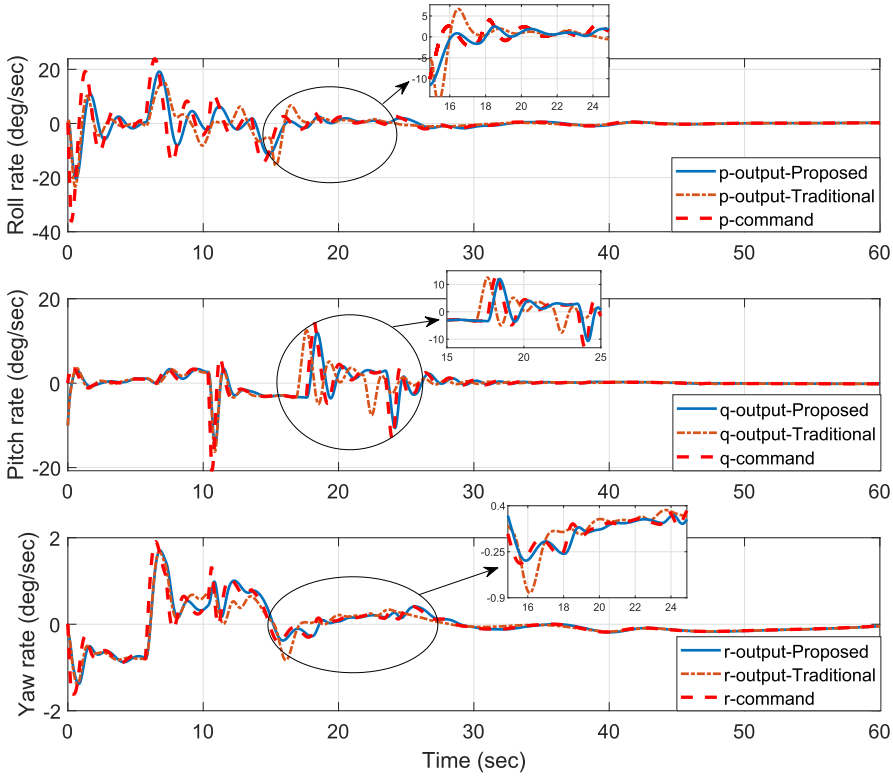

Fig. 4. Plot of the p, q, and r states in the presence of a TDS attack and disturbance for Scenario I. The proposed controller is able to track the command with more accuracy than the traditional control technique in [51]. Both controllers perform well at steady-state (almost after 30 s of simulation), where the deviation between the delayed and actual signals is small.

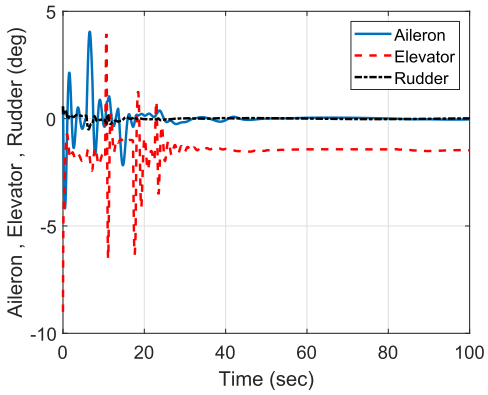

Fig. 5. Aileron, elevator, and rudder signal of the follower under a TDS attack and disturbance for Scenario I. The control signals approach steady-state values after almost 24 s.

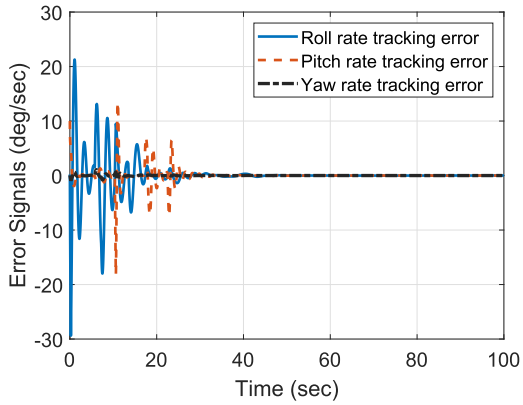

Fig. 6. Tracking error signals of roll, pitch, and yaw rates for the follower under a TDS attack and disturbance for Scenario I. Tracking errors approach zero after 25 s.

using throttle, and the outer-loop controls the relative distance by feeding the desired velocity to the inner loop (see [51]).

1) Inner Control Loop: The fast states of the aircraft are the attitude rates that are controlled with actuator inputs $\delta_{a_i} \in \mathbb{R}$, $\delta_{e_i} \in \mathbb{R}$, and $\delta_{r_i} \in \mathbb{R}$, which are shown in Fig. 2. The desired reference values of the attitude rates come from the outer control loop. Considering the dynamic system described in (1) and the aircraft model in (61)–(63), the inner dynamic model of the ith agent can be written as

$$\dot{x}_i^{\text{in}} = f_i^{\text{in}}(x_i^{\text{in}}) + g_i^{\text{in}}(x_i^{\text{in}})u_i^{\text{in}}\left(\pi_i(x_i^{\text{in}}, \tau_i^{\text{in}}), t\right) + d_i \tag{69}$$

where $x_i^{\text{in}} \triangleq [p_i\, q_i\, r_{y_i}]^T \in \mathbb{R}^3$ and $u_i^{\text{in}} \triangleq [\delta_{a_i}\, \delta_{e_i}\, \delta_{r_i}]^T \in \mathbb{R}^3$ are the inner control loop state and input, respectively, for the ith agent. Let $\tau_i^{\text{in}} \in \mathbb{R}^3$ denote the time-delay injected into the inner control loop state of the system. The nonlinear function f_i^{in} can be derived from (61)–(63). The matrix g_i^{in} is

$$g_i^{\text{in}}(x_i^{\text{in}}) = \begin{bmatrix} L_{\delta_i^a} & 0 & L_{\delta_i^r} \\ 0 & M_{\delta_i^e} & 0 \\ N_{\delta_i^a} & 0 & N_{\delta_i^r} \end{bmatrix} \tag{70}$$

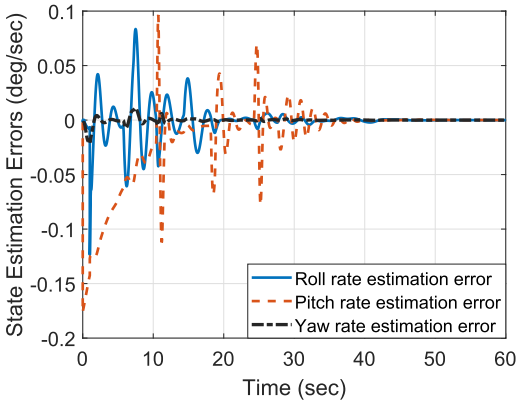

Fig. 7. State estimation errors for roll, pitch, and yaw rates of the follower under a TDS attack and disturbance for Scenario I. The proposed nonlinear state estimator can accurately estimate the yaw, roll, and pitch signals after almost 10, 30, and 35 s, respectively.

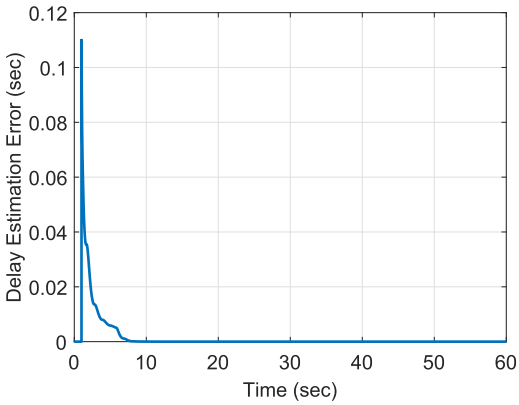

Fig. 8. TDS attack estimation error for Scenario I. The delay estimation error, defined in (30), approaches zero after 8 s, illustrating the performance of the delay estimation algorithm.

where $L_{\delta_i^a}, L_{\delta_i^r}, M_{\delta_i^e}, N_{\delta_i^a}, N_{\delta_i^r} \in \mathbb{R}$ are rolling, pitching, and yawing moments about deflections of the control input axis.

2) Controller Design of Outer Control Loop: The slow states $\alpha_i \in \mathbb{R}$, $\beta_i \in \mathbb{R}$, and $\phi_i \in \mathbb{R}$ are used for the outer control loop design. Based on this literature, the assumption of the time-scale separation between the outer control loop and the inner control loop is implemented to ensure that the deflections of the control surfaces have no interaction with the states of the outer control loop. Considering the dynamic system described in (1) and the airplane dynamic model in (64)–(66), the outer control loop dynamic model of the ith agent is defined as

$$\dot{x}_i^{\text{out}} = f_i^{\text{out}}(x_i^{\text{out}}) + g_i^{\text{out}}(x_i^{\text{in}})x_i^{\text{in}} \tag{71}$$

where $x_i^{\text{out}} \triangleq [\beta_i\ \alpha_i\ \phi_i]^T \in \mathbb{R}^3$, $f_i^{\text{out}} \in \mathbb{R}^3$, and $g_i^{\text{out}} \in \mathbb{R}^{3\times 3}$ can be obtained from (64)–(66). Since we are controlling the flight path, by controlling the angle of attack (α), the pitch angle (θ) will be controlled as well. Thus, the dynamic inversion controller for aircraft attitude is designed based on the angle of attack instead of the pitch angle [51].

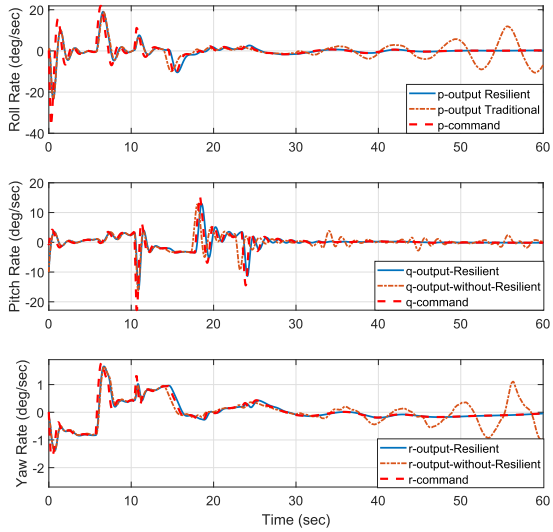

Fig. 9. Plot of the p, q, and r states in the presence of a TDS attack, disturbance, and measurement noise for Scenario II. While the traditional control technique in [51] has better tracking performance than the proposed strategy during the first 25 s of the simulation (i.e., prior to the TDS attack), only the proposed strategy is robust to the TDS attack, which attains a maximum delay of 10.1 s. The traditional controller causes the system to go unstable as a result of the TDS attack, leading to safety concerns.

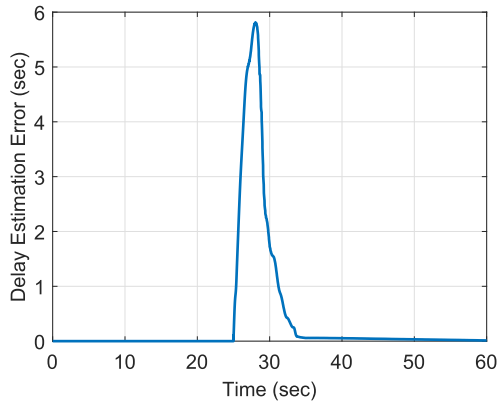

Fig. 10. TDS attack estimation error for Scenario II. The delay estimation error approaches zero as time progresses.

VIII. Simulation Results and Discussion

A six-DoFs model of an aircraft with all actuator and sensor limitations is used to demonstrate the proposed strategy through a MATLAB Simulink simulation. The details of the parameters can be found in [51]. The virtual leader's and leader's direction, distance, and relative velocity are presented in Table I. The virtual leader trajectory is selected to enable validation with the results presented in [51].

A. Scenario I

In this scenario, a TDS attack modeled by $\tau_1 = 0.04\tanh((1/30)t) + 0.08$ has been injected at the 1-s time point

to the rolling rate (p_1), pitching rate (q_1), and yawing rate (r_1) sensors of the follower. The injection of a TDS attack during the transmission of these states can directly affect the controller performance. A disturbance defined by $d_1 = 0.01\sin(t/8) + 0.02\sin(t/9)$ is applied in the simulation. Fig. 3 shows the trajectories of the virtual leader, the leader, and the follower using the virtual trajectory defined in Table I. Fig. 3 shows that the follower can follow the virtual leader despite the injection of a TDS attack. In Fig. 4, the inner-loop controller performance of the proposed controller with TDS attacks compensation and a traditional controller (dynamic inversion) without the TDS attack compensation are compared. The inner-loop is responsible for controlling the rolling, pitching, and yawing rates of the aircraft. And, as can be seen in the breakout windows of Fig. 4, the proposed controller significantly outperforms the dynamic inversion controller provided in [51]. Table II gives the follower's tracking error for the roll, pitch, and yaw rates in the presence of a TDS attack on the system's sensors for the proposed controller and the controller in [51]. The actuator inputs for the follower are illustrated in Fig. 6. The estimation error signals for roll, pitch, and yaw rates are shown in Fig. 7. Finally, the error between injected and estimated TDS attack is shown in Fig. 8.

B. Scenario II

This scenario illustrates the proposed controller's performance under a TDS attack with a large delay. We also added Gaussian noise to the sensor measurement signals. A TDS attack modeled by $\tau_1 = 10\tanh(0.4t) + 0.1$ has been injected at the 25-s time point to the rolling rate, pitching rate, and yawing rate sensors of the follower. The performance comparison of proposed and traditional controller is shown in Fig. 9. It can be seen that our strategy achieves robustness to a TDS attack with a delay magnitude of 10.1 s. Fig. 10 illustrates the delay estimation error indicating the TDS attack compensator's ability to estimate a maximum delay of approximately 10 s.

IX. Conclusion

For a centralized NCS subjected to disturbances and TDS attacks, a continuous secure controller, observer, and TDS-attack compensator were developed to enable an NCS consisting of agents with nonlinear control-affine dynamics to track a desired trajectory. A Lyapunov stability analysis along with LK functionals were used to prove that the trajectory tracking error is UUB. The NN-based design of the TDS-attack estimator was derived from the presented Lyapunov analysis. Simulation results showed that the tracking errors converge to a neighborhood of the origin, where the objective of having the NCS track, a virtual trajectory in the presence of TDS attacks and environmental disturbances was achieved. Future works may investigate the identification of TDS attacks and extend the development to systems with unknown dynamics. One may also extend the development to systems that utilize intermittent state or output feedback as dictated by a timer or event trigger mechanism. This result is focused on a particular class of bounded TDS attacks, and future works can consider how to generate robustness to more general classes of TDS attacks.

Acknowledgment

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

References

[1] H. Shayeghi, H. Shayanfar, and A. Jalili, "Load frequency control strategies: A state-of-the-art survey for the researcher," *Energy Convers. Manage.*, vol. 50, no. 2, pp. 344–353, 2009.
[2] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, "Security challenges of networked control systems," in *Sustainable Interdependent Networks*. Berlin, Germany: Springer, 2018, pp. 77–95.
[3] S. Mokhtari, A. Abbaspour, K. K. Yen, and A. Sargolzaei, "A machine learning approach for anomaly detection in industrial control systems based on measurement data," *Electronics*, vol. 10, no. 4, 2021, Art. no. 407.
[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, 2011, Art. no. 13.
[5] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4281–4292, Jun. 2020.
[6] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures π," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2011, pp. 232–237.
[7] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 220–225.
[9] F. M. Zegers, M. T. Hale, J. M. Shea, and W. E. Dixon, "Event-triggered formation control and leader tracking with resilience to Byzantine adversaries: A reputation-based approach," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 3, pp. 1417–1429, Sep. 2021.
[10] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, R. Majumdar and P. Tabuada, Eds. Berlin, Germany: Springer, 2009, pp. 31–45.
[11] R. Biswas and J. Wu, "Optimal filter assignment policy against distributed denial-of-service attack," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 339–352, Jan./Feb. 2022.
[12] C. Peng and H. Sun, "Switching-like event-triggered control for networked control systems under malicious denial of service attacks," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3943–3949, Sep. 2020.
[13] C. Deng, "Distributed resilient control for cyber-physical systems under denial-of-service attacks," in *Proc. IEEE Int. Conf. Mechatronics Technol.*, 2019, pp. 1–5.
[14] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, Mar. 2016.
[15] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-area measurement-based stabilizing control of power system considering signal transmission delay," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1971–1979, Nov. 2004.
[16] J. Quanyuan, Z. Zhenyu, and C. Yijia, "Wide-area TCSC controller design in consideration of feedback signals' time delays," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, 2005, pp. 1676–1680.
[17] Y. Zhu and M. Krstic, *Delay-Adaptive Linear Control*, vol. 70. Princeton, NJ, USA: Princeton Univ. Press, 2020.
[18] Y. Zhu, M. Krstic, and H. Su, "Predictor feedback for uncertain linear systems with distributed input delays," *IEEE Trans. Autom. Control*, vol. 65, no. 12, pp. 5344–5351, Dec. 2020.
[19] Y. Zhu, M. Krstic, and H. Su, "Delay-adaptive control for linear systems with distributed input delays," *Automatica*, vol. 116, 2020, Art. no. 108902.
[20] F. Mazenc, M. Malisoff, and S.-I. Niculescu, "Reduction model approach for linear time-varying systems with delays," *IEEE Trans. Autom. Control*, vol. 59, no. 8, pp. 2068–2082, Aug. 2014.

[21] F. Mazenc and M. Malisoff, "Continuous discrete sequential observers for time-varying systems under sampling and input delays," *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1704–1709, Apr. 2020.
[22] V. B. Kolmanovskii and J.-P. Richard, "Stability of some linear systems with delays," *IEEE Trans. Autom. Control*, vol. 44, no. 5, pp. 984–989, May 1999.
[23] M. Pajic *et al.*, "Robustness of attack-resilient state estimators," in *Proc. ACM/IEEE 5th Int. Conf. Cyber-Phys. Syst.*, 2014, pp. 163–174.
[24] C.-K. Zhang, L. Jiang, Q. Wu, Y. He, and M. Wu, "Delay-dependent robust load frequency control for time delay power systems," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2192–2201, Aug. 2013.
[25] N. Sharma, S. Bhasin, Q. Wang, and W. E. Dixon, "Predictor-based control for an uncertain euler-lagrange system with input delay," *Automatica*, vol. 47, no. 11, pp. 2332–2342, 2011.
[26] M.-S. Koo and H.-L. Choi, "Non-predictor controller for feedforward and non-feedforward nonlinear systems with an unknown time-varying delay in the input," *Automatica*, vol. 65, pp. 27–35, 2016.
[27] S. Obuz, J. R. Klotz, R. Kamalapurkar, and W. Dixon, "Unknown time-varying input delay compensation for uncertain nonlinear systems," *Automatica*, vol. 76, pp. 222–229, 2017.
[28] N. Fischer, A. Dani, N. Sharma, and W. E. Dixon, "Saturated control of an uncertain nonlinear system with input delay," *Automatica*, vol. 49, no. 6, pp. 1741–1747, 2013.
[29] H. Min, S. Xu, B. Zhang, and Q. Ma, "Output-feedback control for stochastic nonlinear systems subject to input saturation and time-varying delay," *IEEE Trans. Autom. Control*, vol. 64, no. 1, pp. 359–364, Jan. 2019.
[30] S. Obuz, A. Parikh, I. Chakraborty, and W. Dixon, "Lyapunov-based control of an uncertain Euler–Lagrange system with uncertain time-varying input delays without delay rate constraints," *IFAC PapersOnLine*, vol. 49, no. 10, pp. 141–146, 2016.
[31] M. Bagheri, P. Naseradinmousavi, and M. Krstić, "Feedback linearization based predictor for time delay control of a high-DOF robot manipulator," *Automatica*, vol. 108, 2019, Art. no. 108485.
[32] F. Mazenc, M. Malisoff, and T. N. Dinh, "Robustness of nonlinear systems with respect to delay and sampling of the controls," *Automatica*, vol. 49, no. 6, pp. 1925–1931, 2013.
[33] A. Polyakov, D. Efimov, W. Perruquetti, and J.-P. Richard, "Implicit Lyapunov–Krasovski functionals for stability analysis and control design of time-delay systems," *IEEE Trans. Autom. Control*, vol. 60, no. 12, pp. 3344–3349, Dec. 2015.
[34] X. Zhang, W. Lin, and Y. Lin, "Nonsmooth feedback control of time-delay nonlinear systems: A dynamic gain based approach," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 438–444, Jan. 2017.
[35] X. Li and X. Yang, "Lyapunov stability analysis for nonlinear systems with state-dependent state delay," *Automatica*, vol. 112, 2020, Art. no. 108674.
[36] R. Kamalapurkar, N. Fischer, S. Obuz, and W. E. Dixon, "Time-varying input and state delay compensation for uncertain nonlinear systems," *IEEE Trans. Autom. Control*, vol. 61, no. 3, pp. 834–839, Mar. 2016.
[37] Y. Liu, H. Wang, and L. Guo, "Composite robust H_∞ control for uncertain stochastic nonlinear systems with state delay via a disturbance observer," *IEEE Trans. Autom. Control*, vol. 63, no. 12, pp. 4345–4352, Dec. 2018.
[38] N. Sharma, S. Bhasin, Q. Wang, and W. E. Dixon, "RISE-based adaptive control of a control affine uncertain nonlinear system with unknown state delays," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 255–259, Jan. 2012.
[39] F. Mazenc, M. Malisoff, and Z. Lin, "Further results on input-to-state stability for nonlinear systems with delayed feedbacks," *Automatica*, vol. 44, no. 9, pp. 2415–2421, 2008.
[40] Y. Tan, "Time-varying time-delay estimation for nonlinear systems using neural networks," *Int. J. Appl. Math. Comput. Sci.*, vol. 14, pp. 63–68, 2004.
[41] A. Sargolzaei, K. K. Yen, and M. Abdelghani, "Control of nonlinear heartbeat models under time-delay-switched feedback using emotional learning control," *Int. J. Recent Trends Eng. Technol.*, vol. 10, no. 2, pp. 85–91, 2014.
[42] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901–15912, 2017.
[43] H. K. Khalil and J. W. Grizzle, *Nonlinear Systems*, vol. 3. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.
[44] Z. Ding, "Distributed adaptive consensus output regulation of network-connected heterogeneous unknown linear systems on directed graphs," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4683–4690, Sep. 2017.
[45] N. Bekiaris-Liberis and M. Krstic, "Compensation of time-varying input and state delays for nonlinear systems," *J. Dyn. Syst., Meas., Control*, vol. 134, no. 1, 2012, Art. no. 011009.
[46] I. Chakraborty, S. S. Mehta, E. Doucette, and W. E. Dixon, "Control of an input delayed uncertain nonlinear system with adaptive delay estimation," in *Proc. Amer. Control Conf.*, 2017, pp. 1779–1784.
[47] N. E. Cotter, "The Stone–Weierstrass theorem and its application to neural networks," *IEEE Trans. Neural Netw.*, vol. 1, no. 4, pp. 290–295, Dec. 1990.
[48] R. R. Selmic and F. L. Lewis, "Neural-network approximation of piecewise continuous functions: Application to friction compensation," *IEEE Trans. Neural Netw.*, vol. 13, no. 3, pp. 745–751, May 2002.
[49] F. L. Lewis, J. Campos, and R. Selmic, *Neuro-Fuzzy Control of Industrial Systems With Actuator Nonlinearities*, vol. 24. Philadelphia, PA, USA: SIAM, 2002.
[50] Z. Cai, M. S. de Queiroz, and D. M. Dawson, "A sufficiently smooth projection operator," *IEEE Trans. Autom. Control*, vol. 51, no. 1, pp. 135–139, Jan. 2006.
[51] M. Sadeghi, A. Abaspour, and S. H. Sadati, "A novel integrated guidance and control system design in formation flight," *J. Aerosp. Technol. Manage.*, vol. 7, no. 4, pp. 432–442, 2015.
[52] A. Abbaspour, A. Sargolzaei, and K. K. Yen, "A neural network based resilient control design for distributed power systems under faults and attacks," in *Proc. IEEE Int. Conf. Environ. Elect. Eng., IEEE Ind. Commercial Power Syst. Eur.*, 2018, pp. 1–6.

Arman Sargolzaei (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2012 and 2015, respectively, the master's degree in aerospace engineering and the Ph.D. degree in mechanical engineering, under the supervision of Dr. Crane and Dr. Dixon, from the University of Florida, Gainesville, FL, USA, in 2019 and 2020, respectively.

He is currently an Assistant Professor with the Department of Mechanical Engineering, Tennessee Technological University, Cookeville, TN, USA. Prior to joining Tennessee Tech, he was an Assistant Professor of electrical engineering and the Director of Advanced Mobility Institute, Florida Polytechnic University. His mission is to enhance the quality of life for people, with assuring security and privacy concerns through extensive collaboration among multidisciplinary fields.

Dr. Sargolzaei was the recipient of the "2017 Faculty Research Excellence" and the "2018 Faculty Research Excellence" awards.

Federico M. Zegers received B.S. degree in mechanical engineering and mathematics, and the M.S. and Ph.D. degrees in mechanical engineering from the Department of Mechanical and Aerospace Engineering, University of Florida, Gainesville, FL, USA, in 2016, 2019, and 2021, respectively.

He is currently a Research Aerospace Engineer with Air Force Research Laboratory, Eglin Air Force Base, FL, USA. His research focuses on robotics, Lyapunov-based nonlinear and adaptive control, switched and hybrid systems, and multi-agent systems. In 2017 Dr. Zegers joined the Nonlinear Controls and Robotics group under the guidance of Dr. Warren Dixon, where he was awarded the 2020 Graduate Student Research Award in Dynamics, Systems, and Control.

Alireza Abbaspour (Member, IEEE) was born in Mashhad, Iran, in 1988. He received the B.Sc. degree in control engineering from the Sadjad University of Technology, Mashhad, Iran, in 2010, and the M.Sc. degree in guidance and control engineering from the Malek Ashtar University of Technology, Tehran, Iran, in 2013, and the Ph.D. degree in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2018.

He has an extensive background within academia and industry in designing autopilot systems for unmanned vehicles (aircraft and self-driving cars). He is currently a Senior System Safety Engineer of autonomous driving with Tusimple, San Diego, CA, USA. He has authored or coauthored 43 journals, book chapters, patents, and conference papers. His research interests include fault detection and isolation, failure effect analysis, fault-tolerant control systems, flight control system, autonomous driving, system safety, and security of control systems.

Carl D. Crane received the B.S. and M.E. degrees in mechanical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1978 and 1979, respectively, and the Ph.D. degree in mechanical engineering from the University of Florida, Gainesville, FL, USA, in 1987.

He is currently a Professor with the Department of Mechanical and Aerospace Engineering and the Director of the Center for Intelligent Machines and Robotics, University of Florida. For five years, he was an Officer with the Army Corps of Engineers. His research interests include spatial mechanisms, tensegrity systems, robotics, and autonomous navigation for more than 25 years. He has authored one book and more than 40 papers in the area of spatial geometry and robotic systems. His research interests include the development and implementation of system architectures for autonomous ground vehicle navigation and the design and implementation of passive parallel mechanisms to be used for force control applications.

Dr. Crane was the Team Leader of the University of Florida's 2004 and 2005 DARPA Grand Challenge autonomous vehicle development efforts and for the University of Florida's 2007 DARPA Urban Challenge project team. In 2003, he was named as a Fellow of the ASME. He has supervised 110 master's graduates and 33 Ph.D. graduates during his career with the University of Florida.

Warren E. Dixon (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA, in 2000.

Until 2004, he was a Research Staff Member and Eugene P. Wigner Fellow with Oak Ridge National Laboratory. He joined the Mechanical and Aerospace Engineering Department, University of Florida, where he is currently an Ebaugh Professor and Department Chair. His research focuses on the development and application of Lyapunov-based control techniques for uncertain nonlinear systems.

Dr. Dixon was the recipient of the 2015 and 2009 American Automatic Control Council (AACC) O. Hugo Schuck (Best Paper) Award, the 2013 Fred Ellersick Award for Best Overall MILCOM Paper, the 2011 American Society of Mechanical Engineers (ASME) Dynamics Systems and Control Division Outstanding Young Investigator Award, the 2006 IEEE Robotics and Automation Society (RAS) Early Academic Career Award, and the Air Force Commander's Public Service Award (2016) for his contributions to the U.S. Air Force Science Advisory Board. He is an ASME Fellow. He is/was an Associate Editor for the *Journal of Dynamic Systems, Measurement and Control*, *Automatica*, IEEE CONTROL SYSTEMS, IEEE TRANSACTIONS ON SYSTEMS MAN AND CYBERNETICS: PART B CYBERNETICS, and *International Journal of Robust and Nonlinear Control*.