SCIENCE CHINA
Information Sciences

September 2023, Vol. 66 190204:1–190204:14
https://doi.org/10.1007/s11432-022-3817-5

• RESEARCH PAPER •
Special Topic: Control, Optimization, and Learning for Networked Systems

Predictive sliding-mode control of networked high-order fully actuated systems under random deception attacks

Da-Wei ZHANG[1] & Guo-Ping LIU[1,2*]

[1]*Center for Control Theory and Guidance Technology, Harbin Institute of Technology, Harbin* 150001*, China;*
[2]*Center for Control Science and Technology, Southern University of Science and Technology, Shenzhen* 518055*, China*

Received 22 November 2022/Revised 21 April 2023/Accepted 8 June 2023/Published online 28 August 2023

Abstract This research addresses the output tracking of networked high-order fully actuated (NHOFA) systems under random deception attacks in the sensor to networked controller (SNC) and networked controller to actuator (NCA) communication channels, where a Bernoulli process represents the launching success rate of random deception attacks. A successful attack involves the output and control signals being tampered with by the injection of false data. Herein, a predictive sliding-mode control scheme is proposed to achieve the security tracking. In this scheme, a sliding-mode variable is introduced to defend the random deception attacks by enhancing the robustness of closed-loop systems. An incremental HOFA (IHOFA) prediction model is developed using a Diophantine equation as an alternative to the traditional reduced-order prediction model. Through this IHOFA prediction model, the multistep ahead predictions of the sliding-mode variable are constructed to optimize the tracking performance and defense of random deception attacks. By utilizing the Lyapunov function and linear matrix inequality (LMI) approach, a sufficient and necessary condition is proposed to ensure stability and high tracking performance of closed-loop NHOFA systems. Herein, an experiment on the tracking control of an air-bearing spacecraft (ABS) simulator is performed to demonstrate the effectiveness and practicability of the predictive sliding-mode control scheme.

Keywords NHOFA systems, random deception attacks, predictive sliding-mode control, stability and tracking performance, tracking control of ABS simulator

Citation Zhang D-W, Liu G-P. Predictive sliding-mode control of networked high-order fully actuated systems under random deception attacks. Sci China Inf Sci, 2023, 66(9): 190204, https://doi.org/10.1007/s11432-022-3817-5

1 Introduction

With the wide popularity and rapid development of the Internet of Things, networked control systems (NCSs) have attracted considerable attention and have been successfully employed in various fields, such as motor systems [1], unmanned aerial vehicles [2], power systems [3], and other applications [4–6]. In NCS analysis and control, hardware and software limitations resulting from varied and complicated operational scenarios, such as cyberattacks, network delays, and data losses and disorders, are yet to be investigated. Among them, deception attacks have been extensively studied because they can exploit the vulnerabilities within a system and maliciously tamper with data, which is a critical threat to security and reliability; therefore, numerous studies have focused on the defense of deception attacks in NCSs.

To realize the secure control of NCSs under deception attacks, a string of effective methods have been proposed thus far. For instance, Li et al. [7] designed an attack detector with a dynamical threshold to realize the distributed filtering under deception attacks with the aim of establishing a sufficient criterion for mean-square stability for estimation errors. Yoo [8] adopted an approximation based on neural networks and attack compensators to construct an adaptive memoryless resilient control, which ensured a robust closed-loop system with unknown deception attacks. Wu and Chang [9] utilized a dynamical quantizer and round-robin protocol to schedule the transmission of quantized data in communication

* Corresponding author (email: liugp@sustech.edu.cn)

channels. Further, they proposed a controller based on a mode-dependent observer to maintain the probability security of a closed-loop system under random deception attacks and quantization. Zhang et al. [10] established a detection condition of false data injection and a heuristic computing algorithm to present a novel moving target defense strategy so that the security of the system state and its estimations can be protected from deception attacks. Another group [11] provided a dynamical event-triggering protocol to relax data transmission pressure in the network channels and constructed a dynamical output feedback controller combined with a fault detection filter and the provided dynamical event-trigger to defend random deception attacks, such that the stochastic stability and security of closed-loop systems can be ensured. Meanwhile, Chattopadhyay and Mitra [12] provided a secure estimation method based on a novel learning filtering algorithm for developing a novel detector to identify and detect malicious adversary deception attacks on sensors. Li et al. [13] calculated a state estimation via a recursive algorithm to establish a cloud centralized controller and used the linear matrix inequality (LMI) method to obtain the controller gains for the mean-square consensus of closed-loop systems under deception attacks. Wu et al. [14] proposed a novel event-triggering method to transform NCSs under deception attacks into a switching system and established a Lyapunov function-based condition to ensure the exponential mean-square stability. High-order strict-feedback NCSs under deception attacks have also been explored by Yang et al. [15], who suggested a new adaptive control scheme introducing a novel S-type feedback function and a novel Lyapunov function to achieve the convergence of regulation errors to an arbitrary small interval. Gao and Huang [16] studied a stabilization problem of high-order strict-feedback NCSs under deception attacks and designed an adaptive control with time-variant scaled function to achieve the asymptotic stability of closed-loop systems under deception attacks. In addition, other researchers [17–19] have contributed extensively to the defense of other types of deception attacks for NCSs.

Among numerous methods for defending deception attacks, predictive control satisfies the desired control requirements and achieves the defense against deception attacks in the communication channels, which has been studied in the literature. For instance, a robust predictive control combined with a dynamical output feedback to deal with deception attacks has been proposed [20] to convert the stability of closed-loop systems into a solvable optimization problem by the LMI method. A research group [21] proposed an event-triggering multistep predictive control to improve the control performance and energy efficiency of communication, which realized stable and secure closed-loop systems. A combination of the resilient, robust predictive control strategy with the round-robin protocol was adopted to counter deception attacks [22], which reduced the communication pressures and let the closed-loop states considering deception attacks and round-robin protocol convergence to a given interval. Another group [23] proposed a predictive control with a dynamical event-triggering scheme to defend deception attacks, where some sufficient criteria were proposed to ensure mean-square asymptotic stability. Meanwhile, there are reports on predictive control against deception attacks (see [24–26] and references therein).

The high-order fully actuated (HOFA) system method [27], a new system model for control design, has become a commonly adopted model for physical systems because it maintains the full actuation characteristic of original systems and has a clear physical background. In fact, a number of physical theorems containing linear and angular momentum theorem, Lagrangian equation, Kirchhoff's law are originally second-order or high-order fully actuated, such that multiagent systems [28], combined spacecraft [29], circuit systems [30], and other applications can be represented through the HOFA system method. The networked high-order fully actuated (NHOFA) system is regarded as an NCS described by the HOFA system model. It is anticipated that its analysis and control will elicit new exciting topics, and numerous challenges related to NCSs will be re-established and resolved. Our team has obtained original results from the literature (see [31, 32]), which provides a better and solid foundation for our future, in-depth research.

In this work, a predictive sliding-mode control scheme is proposed to achieve the security tracking of NHOFA systems under random deception attacks, where one of the difficulties is to design a predictive sliding-mode control with the representation of the HOFA system form and the advantages of full actuation characteristic to overcome the negative impacts of random deception attacks, and the stability and secure tracking performance of closed-loop systems generated by the HOFA predictive sliding-mode control are analyzed. Major contributions to address these issues are summarized as follows: First, local HOFA feedback is designed to adjust the closed-loop system performance and regulate the prediction model. Second, a sliding-mode variable is exploited to cope with random deception attacks by improving the robustness of closed-loop systems. Then, an incremental HOFA (IHOFA) prediction model is established using a Diophantine equation. Through this model, the multistep sliding-mode predictions

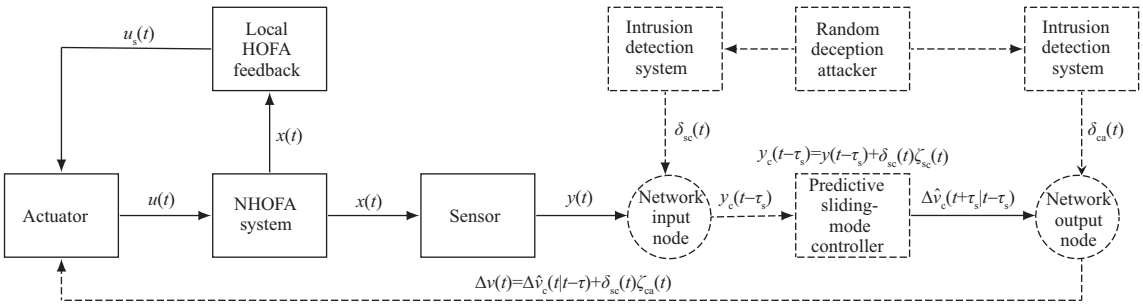

Figure 1 Predictive sliding-mode control of NHOFA systems under random deception attacks.

are constructed to realize the optimization of the tracking performance and defense against random deception attacks. Furthermore, through the proposed scheme, the stability and tracking performance of closed-loop NHOFA systems can be transformed into the asymptotic stability of the sliding-mode variable, which enables the establishment of a sufficient and necessary condition to analyze the asymptotic stability of the sliding-mode variable via the LMI method and the Lyapunov function. Additionally, an experiment on the tracking control of the air-bearing spacecraft (ABS) simulator is conducted to verify the effectiveness and practicability of the proposed scheme. The advantages of this research are as follows.

(1) An HOFA system model is presented to establish the dynamics of NCSs such that full actuation characteristics can be used to simplify the control design and avoid drawbacks of model reduction.

(2) An IHOFA prediction model is constructed using a Diophantine equation, which utilizes an HOFA form to design and represent the predictive control protocol for secure tracking.

(3) A sliding-mode variable is proposed to counter random deception attacks, which realizes the effective defense by improving the robustness of closed-loop systems.

There are differences between NHOFA systems and general networked high-order systems [15, 16, 33]. First, NHOFA systems can guarantee the physical meanings of the original systems due to the full actuation characteristic, whereas common networked high-order systems [15, 16, 33] use the traditional first-order state-space model to describe the NCS dynamics, which leads to loss of physical meanings. Second, NHOFA systems consider the high-dimension vector and high-order difference equation of the system model; however, general networked high-order systems [15,16,33] only consider the high-dimension vector but neglect the high-order difference equation. Last, the control design of NHOFA systems can directly apply full actuation characteristic of presenting a control law in HOFA form in a simple way, but that of general networked high-order systems [15, 16, 33] is hard in high-order form without considering model reduction.

Notation. $\|\cdot\|$ is the Euclidean norm. $N_y > N_u$ is the output and control prediction horizons. $\hat{\varpi}(t+i|t-j)$ indicates the i-th ahead prediction of $\varpi(t)$ based on $t-j$ time where $\varpi(t)$ represents the state, input, output, and other associated signals. q denotes a time operator satisfying $\varpi(t+i) = q^i\varpi(t)$, $i \in \mathbb{Z}$ (see [34]). $\Delta = 1 - q^{-1}$ is a difference operator so that $\Delta\varpi(t) = \varpi(t) - \varpi(t-1)$ is the increment.

2 Problem formulation

From [31, 32], NHOFA system is described by

$$x(t+n) = -\sum_{i=0}^{n-1} A_i x(t+i) + Bu(t),\ y(t) = Cx(t), \tag{1}$$

where x, $u \in \mathbb{R}^{\tilde{n}}$, $y \in \mathbb{R}^m$ indicate the state, input, and output vectors, $A_i \in \mathbb{R}^{\tilde{n}\times\tilde{n}}$, $i = 0, 1, \ldots, n-1$, $B \in \mathbb{R}^{\tilde{n}\times\tilde{n}}$, $C \in \mathbb{R}^{m\times\tilde{n}}$ are given coefficients, and $\det(B) \neq 0$.

Assumption 1 ([31])**.** The state vector of NHOFA system (1) is available.

Then predictive sliding-mode control of NHOFA systems under random deception attacks is shown in Figure 1, where $\tau_{\rm s}$ and $\tau_{\rm a}$ indicate the communication delays in the sensor to networked controller (SNC) and networked controller to actuator (NCA) channels, and $\tau = \tau_{\rm a} + \tau_{\rm s}$. $\delta_{\rm sc}(t)$ and $\delta_{\rm ca}(t)$ are regarded as random variables to represent the randomness of actually effective attacks in the SNC and NCA channels and also can be detected and converted as the values 0 and 1 via some feasible detection

strategies (e.g., [7]). $\delta_{\rm sc}(t)/\delta_{\rm ca}(t) = 1$ denotes that the random deception attack successfully attacks the SNC/NCA channel, and $\delta_{\rm sc}(t)/\delta_{\rm ca}(t) = 0$ indicates the random deception attack in the SNC/NCA channel is failed. Considering the complexities and uncertainties in the network, many kinds of cyber attacks are described by random processes to represent the randomness of attack patterns, where the Bernoulli process is one of the most common modes. Following the idea in [35], $\delta_{\rm sc}(t)$ and $\delta_{\rm ca}(t)$ are described by Bernoulli processes with the following probabilities:

$$\begin{aligned}&\mathrm{Prob}\{\delta_{\rm sc}(t)=1\}=\mu,\ \mathrm{Prob}\{\delta_{\rm sc}(t)=0\}=1-\mu,\\&\mathrm{Prob}\{\delta_{\rm ca}(t)=1\}=\nu,\ \mathrm{Prob}\{\delta_{\rm ca}(t)=0\}=1-\nu,\end{aligned}$$

where $\mu, \nu \in [0, 1]$ are known constants denoting the successful rate of initiated deception attacks. In this work, $\delta_{\rm sc}(t)$ and $\delta_{\rm ca}(t)$ result in the false data $\zeta_{\rm sc}(t)$ and $\zeta_{\rm ca}(t)$ injected in the SNC and NCA channels to tamper with the output and control signals; that is

$$y_{\rm c}(t) = y(t) + \delta_{\rm sc}(t)\zeta_{\rm sc}(t),\ \Delta v(t) = \Delta v_{\rm c}(t) + \delta_{\rm ca}(t)\zeta_{\rm ca}(t), \tag{2}$$

where $y(t)$ and $\Delta v(t)$ are the real signals sent by the local sensor and received by the local actuator, respectively, $y_{\rm c}(t)$ and $\Delta v_{\rm c}(t)$ denote the signals of output and predictive sliding-mode control increment received and generated by the networked controller, respectively.

Assumption 2 ([32])**.** (1) The clocks of all elements are synchronized; (2) there are timestamps in the process of data transmission; (3) $\tau_{\rm a}$ and $\tau_{\rm s}$ are given positive integers and also the multiples of the sampling period.

Assumption 3 ([12])**.** $\zeta_{\rm sc}(t)$ and $\zeta_{\rm ca}(t)$ are uniformly bounded in relation to time t.

To cope with random deception attacks, a predictive sliding-mode control scheme for NHOFA system (1) is provided as

$$u(t) = B^{-1}(u_{\rm s}(t) + v(t)),\ u_{\rm s}(t) = \sum_{i=0}^{n-1} K_{{\rm c},i}x(t+i), \tag{3}$$

where $u_{\rm s}(t) \in \mathbb{R}^{\tilde{n}}$ is a local HOFA feedback and $K_{{\rm c},i} \in \mathbb{R}^{\tilde{n}\times\tilde{n}}$, $i = 0, 1, \ldots, n-1$ denotes the associated HOFA feedback coefficient, and $v(t) \in \mathbb{R}^{\tilde{n}}$ is a security control item designed by predictive sliding-mode control. Then, a closed-loop NHOFA system is implemented as

$$x(t+n) = -\sum_{i=0}^{n-1} A_{i{\rm c}}x(t+i) + v_{\rm c}(t) + \delta_{\rm ca}(t)\zeta_{\rm ca}(t),\ y(t) = Cx(t),\ y_{\rm c}(t) = y(t) + \delta_{\rm sc}(t)\zeta_{\rm sc}(t), \tag{4}$$

where $A_{i{\rm c}} = A_i - K_{{\rm c},i}$, $i = 0, 1, \ldots, n-1$, and $v_{\rm c}(t) \in \mathbb{R}^{\tilde{n}}$ indicates the real tracking control item designed by the networked controller. Concretely, when $\delta_{\rm ca}(t) = 0$, the launch of a deception attack in the NCA channel is failed, and then $\Delta v(t) = \Delta v_{\rm c}(t)$ and $v(t) = v_{\rm c}(t)$. When $\delta_{\rm ca}(t) = 1$, the launch of deception attack in the NCA channel is successful, and then $\Delta v(t) = \Delta v_{\rm c}(t) + \delta_{\rm ca}(t)\zeta_{\rm ca}(t)$ and $v(t) = v(t-1) + \Delta v_{\rm c}(t) + \delta_{\rm ca}(t)\zeta_{\rm ca}(t) = v_{\rm c}(t) + \delta_{\rm ca}(t)\zeta_{\rm ca}(t)$.

Problem 1. Given NHOFA system (1) with Assumptions 1–3, a predictive sliding-mode control scheme (3) is provided to achieve the stability and tracking performance of closed-loop NHOFA system (4), such that the following Conditions (1) and (2) are satisfied:

(1) For a given reference $r(t)$, if $\|r(t)\| < \infty$, $\|y(t)\| < \infty$, $\forall t \geqslant 0$;

(2) $\lim_{t\to\infty}\|y(t) - r(t)\| = 0$.

3 Main results

3.1 Design of the sliding-mode variable

Sliding-mode control is an effective robust control approach to address the uncertainties, including parameter perturbations and external disturbances. When launching the deception attacks successfully, the false data injected in systems can be also equivalently regarded as the uncertainties. In this view, the sliding-mode control can be naturally introduced to the defense and control of deception attacks. In recent studies, there exist many representative cases on the sliding-mode control against deception attacks (see [36–38] and references therein).

Following this idea, the tracking error $e(t)$ is defined as $e(t) = y(t) - r(t)$, then Conditions (1) and (2) in Problem 1 are satisfied if $\lim_{t\to\infty}\|e(t)\| = 0$. Then, a linear sliding-mode variable $s(t) \in \mathbb{R}$ is designed as

$$s(t) = \Xi(q^{-1})e(t), \tag{5}$$

where $\Xi(q^{-1}) = \sum_{i=0}^{n_\xi} \xi_i q^{-i}$ is chosen as a Schur polynomial matrix, $\xi_i \in \mathbb{R}^{1\times m}$ represents the related coefficient matrix, n_ξ is a given positive integer. When $s(t) \equiv 0$, a corresponding linear difference equation is completely expressed as

$$s(t) = \Xi e(t) = \sum_{i=0}^{n_\xi} \xi_i q^{-i} e(t) = \xi_0 e(t) + \xi_1 e(t-1) + \cdots + \xi_{n_\xi} e(t-n_\xi) \equiv 0.$$

The unique solution of the above equation is $e(t) \equiv 0$, such that Problem 1 is solved if $\lim_{t\to\infty}\|s(t)\| = 0$.

3.2 Design of the predictive sliding-mode controller

When there exist no attacks in the SNC and NCA channels, the nominal form of closed-loop system (4) is given as

$$x(t+n) = -\sum_{i=0}^{n-1} A_{ic} x(t+i) + v_{\rm c}(t),\ y_{\rm c}(t) = y(t) = Cx(t) \tag{6}$$

by applying a q operator, and the nominal system (6) is equivalent to

$$A(q^{-1})x(t) = B(q^{-1})v_{\rm c}(t-1), \tag{7}$$

where $A(q^{-1}) = \sum_{i=0}^{n-1} A_{ic} q^{i-n} + I$, $B(q^{-1}) = q^{1-n}$. Then, a Diophantine equation is proposed as

$$E_l(q^{-1})A\Delta + q^{-l}F_l(q^{-1}) = I,$$

where $E_l(q^{-1})$ and $F_l(q^{-1})$ are polynomial matrices depended on prediction horizon l and system coefficient $A(q^{-1})$, given as $E_l(q^{-1}) = \sum_{k=0}^{l-1} e_{l,k} q^{-k}$, $F_l(q^{-1}) = \sum_{k=0}^{n} f_{l,k} q^{-k}$. Multiplying $E_l\Delta q^l$ at (7) obtains

$$E_l A\Delta x(t+l) = E_l B\Delta v_{\rm c}(t+l-1).$$

Combining it with the Diophantine equation, an IHOFA prediction model is constructed as

$$x(t+l) = F_l x(t) + G_l \Delta v_{\rm c}(t+l-1), \tag{8}$$

where $G_l(q^{-1}) = E_l(q^{-1})B(q^{-1}) = \sum_{k=0}^{l-1} g_{l,k} q^{1-n-k}$. Considering the communication delays in the SNC and NCA channels, $x(t)$ can be predicted as

$$\hat{x}(t-\tau_{\rm s}+l|t-\tau_{\rm s}) = F_l x(t-\tau_{\rm s}) + G_l\Delta\hat{v}_{\rm c}(t-\tau_{\rm s}+l-1|t-\tau_{\rm s}),$$

where $l = 1, 2, \ldots, \tau + N_y$. From $l = \tau+1$ to $l = \tau+N_y$,

$$\begin{aligned}
&\hat{x}(t+\tau_{\rm a}+1|t-\tau_{\rm s}) = F_{\tau+1}x(t-\tau_{\rm s}) + G_{\tau+1}\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}|t-\tau_{\rm s}),\\
&\vdots\\
&\hat{x}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s}) = F_{\tau+N_y}x(t-\tau_{\rm s}) + G_{\tau+N_y}\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}+N_y-1|t-\tau_{\rm s}),
\end{aligned}$$

so that the prediction of system output is given as

$$\hat{y}(t+\tau_{\rm a}+l|t-\tau_{\rm s}) = C\hat{x}(t+\tau_{\rm a}+l|t-\tau_{\rm s}), \tag{9}$$

with $l = 1, 2, \ldots, N_y$. When $l = N_u+1, \ldots, N_y$, $\hat{v}_{\rm c}(t+\tau_{\rm a}+l|t-\tau_{\rm s}) = \hat{v}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})$ such that $\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}+l|t-\tau_{\rm s}) = 0$. Combining (9) with (5), the sliding-mode variable $s(t)$ is predicted as

$$\begin{aligned}
&\hat{s}(t+\tau_{\rm a}+1|t-\tau_{\rm s}) = \Xi\hat{y}(t+\tau_{\rm a}+1|t-\tau_{\rm s}) - \Xi r(t+\tau_{\rm a}+1),\\
&\vdots
\end{aligned}$$

$$\hat{s}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})=\Xi\hat{y}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})-\Xi r(t+\tau_{\rm a}+N_y),$$

which can be compactly rewritten as

$$\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})=P_1\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})+P_2x(t-\tau_{\rm s})-\Xi_dR(t+\tau_{\rm a}+N_y),\tag{10}$$

with

$$\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})=\begin{bmatrix}\hat{s}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})\\ \vdots\\ \hat{s}(t+\tau_{\rm a}+1|t-\tau_{\rm s})\end{bmatrix},$$

$$\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})=\begin{bmatrix}\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})\\ \vdots\\ \Delta\hat{v}_{\rm c}(t+\tau_{\rm a}|t-\tau_{\rm s})\end{bmatrix},$$

$$R(t+\tau_{\rm a}+N_y)=\begin{bmatrix}r(t+\tau_{\rm a}+N_y)\\ \vdots\\ r(t+\tau_{\rm a}+1)\end{bmatrix},\ \Xi_d=\begin{bmatrix}\Xi & & \\ & \ddots & \\ & & \Xi\end{bmatrix},$$

and

$$P_1=\begin{bmatrix}L_{\tau+N_y} & 0 & \cdots & 0\\ \vdots & \vdots & \cdots & \vdots\\ L_{\tau+N_u+1} & 0 & \cdots & 0\\ 0 & L_{\tau+N_u} & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & L_{\tau+1}\end{bmatrix},\ P_2=\begin{bmatrix}D_{\tau+N_y}\\ \vdots\\ D_{\tau+N_u+1}\\ D_{\tau+N_u}\\ \vdots\\ D_{\tau+1}\end{bmatrix},$$

where $D_{\tau+l}=\Xi CF_{\tau+l}$, $L_{\tau+l}=\Xi CG_{\tau+l}$. Then, a cost function for secure tracking control performance is defined as

$$J(t)=\|\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})-S_{\rm ref}(t+\tau_{\rm a}+N_y)\|^2_{W_1}+\|\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})\|^2_{W_2},\tag{11}$$

with $S_{\rm ref}(t+\tau_{\rm a}+N_y)=[\,s^{\rm T}_{\rm ref}(t+\tau_{\rm a}+N_y)\ \cdots\ s^{\rm T}_{\rm ref}(t+\tau_{\rm a}+1)\,]^{\rm T}$, where $s_{\rm ref}(t)$ indicates the sliding-mode reference, W_1 and W_2 are the positive definite weighted coefficient matrices. In (11), the first item pays attention to the difference between sliding-mode prediction and sliding-mode reference, and the second one provides a limitation of predictive control increment such that it is realistic in practical applications. Additionally, an incremental constraint is given as

$$\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}+l|t-\tau_{\rm s})=\gamma_l\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}|t-\tau_{\rm s}),$$

where $\gamma_l>0$, $l=1,2,\ldots,N_u$, represents the weighting coefficient; hence P_1 can be degenerated by

$$P_3=P_1\Gamma,\ \Gamma=\text{Blockdiag}\{\gamma_{N_u}I,\ldots,\gamma_1I,I\}.$$

To obtain the optimal predictive sliding-mode control increment, let

$$\frac{\partial}{\partial\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})}J(t)=0.$$

By considering (10), the above is obtained that

$$P_3^{\rm T}W_1(P_3\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})+P_2x(t-\tau_{\rm s})-\Xi_dR(t+\tau_{\rm a}+N_y)$$

$$-S_{\rm ref}(t+\tau_{\rm a}+N_y))+W_2\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})=0,$$

such that

$$\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})=M_1^{-1}M_2x(t-\tau_{\rm s})+M_1^{-1}M_3S_{\rm ref}(t+\tau_{\rm a}+N_y)+M_1^{-1}M_4R(t+\tau_{\rm a}+N_y),\quad(12)$$

with $M_1=P_3^{\rm T}W_1P_3+W_2$, $M_2=-P_3^{\rm T}W_1P_2$, $M_3=P_3^{\rm T}W_1$, $M_4=M_3\Xi_d$. On the network node, the optimal predictive sliding-mode control increment is calculated as $\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}|t-\tau_{\rm s})=H\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})$ with $H=[\,0\ \cdots\ 0\ I\,]$, given as

$$\Delta\hat{v}_{\rm c}(t+\tau_{\rm a}|t-\tau_{\rm s})=HM_1^{-1}M_2x(t-\tau_{\rm s})+HM_1^{-1}M_3S_{\rm ref}(t+\tau_{\rm a}+N_y)+HM_1^{-1}M_4R(t+\tau_{\rm a}+N_y).$$

On the actuator node, $\Delta v_{\rm c}(t)$ is set to $\Delta v_{\rm c}(t)=\Delta\hat{v}_{\rm c}(t|t-\tau)$; that is

$$\Delta v_{\rm c}(t)=HM_1^{-1}M_2x(t-\tau)+HM_1^{-1}M_3S_{\rm ref}(t+N_y)+HM_1^{-1}M_4R(t+N_y).\quad(13)$$

From (12), the final form of predictive sliding-mode control depends on the sliding-mode reference $s_{\rm ref}(t)$. According to [39], a sliding-mode reference $s_{\rm ref}(t)$ is designed as

$$s_{\rm ref}(t+1)=(1-\lambda_1T)s(t)-\lambda_2Tf(s(t),\alpha,\beta),$$

where $\lambda_1,\lambda_2\in(0,1)$ are known constants, T is the sampling period, $f(s(t),\alpha,\beta)$ is a power function given as

$$f(s(t),\alpha,\beta)=\begin{cases}|s|^{\alpha}{\rm sgn}(s), & |s|\geqslant\beta,\\ \frac{s}{\beta^{1-\alpha}}, & |s|<\beta,\end{cases}$$

with $\beta>(\frac{\lambda_2T}{1-\lambda_1T})^{\frac{1}{1-\alpha}}$, $\frac{\lambda_2T}{1-\lambda_1T},\alpha,\beta\in(0,1)$, and ${\rm sgn}(s)$ is a symbolic function related to s and is generated by

$${\rm sgn}(s)=\begin{cases}1, & s>0,\\ 0, & s=0,\\ -1. & s<0.\end{cases}$$

Remark 1. In this paper, $u_{\rm s}(t)$ also plays an important role to adjust the secure tracking control performance of closed-loop system (4) by stabilizing the following system:

$$x(t+n)+\sum_{i=0}^{n-1}A_{ic}x(t+i)=0,$$

so that how to solve the solutions of $K_{{\rm c},i}$ is a key problem. According to our method in [31], a guidance is provided to obtain the completely analytical solutions of HOFA feedback coefficients $K_{{\rm c},i}$.

Step 1. Solve two polynomial matrices $\mathcal{D}_1(z)$ and $\mathcal{D}_2(z)$ satisfying

$$\mathcal{A}(z)\mathcal{D}_1(z)=\mathcal{D}_2(z),\ \mathcal{A}(z)=z^n+\sum_{i=0}^{n-1}A_iz^i.$$

Step 2. Let $\mathcal{D}_i(z)=[d_{ijl}(z)]_{\tilde{n}\times\tilde{n}}$, $i=1,2$, and $\epsilon_{\rm c}=\max\{\deg(d_{ijl}(z)),\ j,l=1,2,\ldots,\tilde{n}\}$ represents the highest degree of $d_{ijl}(z)$ with respect to z, such that $\mathcal{D}_i(z)=\sum_{j=0}^{\epsilon_{\rm c}}\mathcal{D}_{ij}z^j$.

Step 3. Choose a Schur matrix $\Lambda_{\rm c}$ and an arbitrary matrix $\mathcal{Z}_{\rm c}$ to compute two parameter matrices $\mathcal{W}_{\rm c}$ and $\mathcal{V}_{\rm c}$ as

$$\mathcal{V}=\sum_{i=0}^{\epsilon_{\rm c}}\mathcal{D}_{1i}\mathcal{Z}_{\rm c}\Lambda_{\rm c}^i,\ \mathcal{V}_c=\left[\,\mathcal{V}^{\rm T}\ \Lambda_{\rm c}^{\rm T}\mathcal{V}^{\rm T}\ \cdots\ (\Lambda_{\rm c}^{n-1})^{\rm T}\mathcal{V}^{\rm T}\,\right]^{\rm T},\ \mathcal{W}_{\rm c}=\sum_{i=0}^{\epsilon_{\rm c}}\mathcal{D}_{2i}\mathcal{Z}_{\rm c}\Lambda_{\rm c}^i.$$

Step 4. If $\det(\mathcal{V}_{\rm c})\neq0$, compute the coefficient matrix $K_{\rm c}=[\,K_{c,0}\ K_{c,1}\ \cdots\ K_{c,n-1}\,]$ via $K_{\rm c}=\mathcal{W}_{\rm c}\mathcal{V}_{\rm c}^{-1}$. Else, return to Step 3 to recompute the parameter matrices $\mathcal{W}_{\rm c}$ and $\mathcal{V}_{\rm c}$.

3.3 Analysis of stability and tracking performance

According to Subsection 3.1, the stability and tracking performance of closed-loop NHOFA system (4) can be transformed into the asymptotic stability of sliding-mode variable $s(t)$. Actually, $\Delta v_{\rm c}(t)$ in (13) is designed for nominal system (6). Combining (2) with (9), the prediction of $s(t)$ for closed-loop form (4) can be corrected as

$$\begin{aligned}\hat{s}(t+\tau_{\rm a}+l|t-\tau_{\rm s}) &= \Xi\hat{e}(t+\tau_{\rm a}+l|t-\tau_{\rm s})\\ &= \Xi C\hat{x}(t+\tau_{\rm a}+l|t-\tau_{\rm s})+\Xi\delta_{\rm sc}(t+\tau_{\rm a})\zeta_{\rm sc}(t+\tau_{\rm a})-\Xi r(t+\tau_{\rm a}+l)\\ &= \Xi CF_{\tau+l}x(t-\tau_{\rm s})+\Xi CG_{\tau+l}\Delta\hat{v}_c(t+\tau_{\rm a}+l-1|t-\tau_{\rm s})+\Xi CG_{\tau+l}\delta_{\rm ca}(t+\tau_{\rm a}-1)\zeta_{\rm ca}(t+\tau_{\rm a}-1)\\ &\quad+\Xi\delta_{\rm sc}(t+\tau_{\rm a})\zeta_{\rm sc}(t+\tau_{\rm a})-\Xi r(t+\tau_{\rm a}+l)\\ &= L_{\tau+l}\Delta\hat{v}_c(t+\tau_{\rm a}+l-1|t-\tau_{\rm s})+D_{\tau+l}x(t-\tau_{\rm s})+N_{\tau+l}w(t+\tau_{\rm a})-\Xi r(t+\tau_{\rm a}+l),\end{aligned}$$

with

$$w(t+\tau_{\rm a})=\begin{bmatrix}\delta_{\rm ca}(t+\tau_{\rm a}-1)\zeta_{\rm ca}(t+\tau_{\rm a}-1)\\ \delta_{\rm sc}(t+\tau_{\rm a})\zeta_{\rm sc}(t+\tau_{\rm a})\end{bmatrix},\ N_{\tau+l}=\begin{bmatrix}L_{\tau+l}&\Xi\end{bmatrix}.$$

Thus, $\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})$ in (10) is re-summarized as

$$\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})=P_1\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})+P_2x(t-\tau_{\rm s})+P_4w(t+\tau_{\rm a})-\Xi_dR(t+\tau_a+N_y),\ (14)$$

with $P_4=[\,N_{\tau+N_y}^{\rm T}\ \cdots\ N_{\tau+1}^{\rm T}\,]^{\rm T}$. Because W_2 cannot affect the closed-loop stability, let $W_2=0$ and $W_1=I$; then Eq. (12) can be degenerated as

$$P_3^{\rm T}P_3\Delta\hat{V}_{\rm c}(t+\tau_{\rm a}+N_u|t-\tau_{\rm s})=-P_3^{\rm T}P_2x(t-\tau_{\rm s})+P_3^{\rm T}\Xi_dR(t+\tau_{\rm a}+N_y)+P_3^{\rm T}S_{\rm ref}(t+\tau_{\rm a}+N_y).$$

Taking the above into (14) yields

$$\hat{S}(t+\tau_{\rm a}+N_y|t-\tau_{\rm s})=S_{\rm ref}(t+\tau_{\rm a}+N_y)+P_4w(t+\tau_{\rm a}),$$

which is equivalent to

$$\hat{S}_{\rm c}(t+N_y|t-\tau)=S_{\rm ref}(t+N_y)+P_4w(t);$$

the last row of the above is represented as

$$s(t+1)=s_{\rm ref}(t+1)+N_{\tau+1}w(t)=(1-\lambda_1T)s(t)-\lambda_2Tf(\cdot)+N_{\tau+1}w(t),\qquad(15)$$

where $f(\cdot)$ represents $f(s(t),\alpha,\beta)$.

Theorem 1. System (15) realizes the asymptotic stability if and only if $\Omega_{11}<0$ and $\Omega_{22}-\Omega_{12}^{\rm T}\Omega_{11}^{-1}\Omega_{12}<0$, where

$$\Omega_{11}=\lambda_1^2T^2-2\lambda_1T,\ \Omega_{12}=\begin{bmatrix}\lambda_1\lambda_2T^2-\lambda_2T&N_{\tau+1}-\lambda_1TN_{\tau+1}\end{bmatrix},\ \Omega_{22}=\begin{bmatrix}\lambda_2^2T^2&-\lambda_2TN_{\tau+1}\\ -\lambda_2TN_{\tau+1}^{\rm T}&N_{\tau+1}^{\rm T}N_{\tau+1}\end{bmatrix}.\qquad(16)$$

Proof. For system (15), a Lyapunov function is given as

$$\eta(t)=s^{\rm T}(t)s(t)>0.$$

Then system (15) realizes the asymptotic stability if and only if $\Delta\eta(t+1)=\eta(t+1)-\eta(t)<0$, which can be completely expressed as

$$\begin{aligned}\Delta\eta(t+1)=&s^{\rm T}(t)s(t)-s^{\rm T}(t)\lambda_1Ts(t)-s^{\rm T}(t)\lambda_2Tf(\cdot)+s^{\rm T}(t)N_{\tau+1}w(t)-s^{\rm T}(t)\lambda_1Ts(t)+s^{\rm T}(t)\lambda_1^2T^2s(t)\\ &+s^{\rm T}(t)\lambda_1\lambda_2T^2f(\cdot)-s^{\rm T}(t)\lambda_1TN_{\tau+1}w(t)-f^{\rm T}(\cdot)\lambda_2Ts(t)+f^{\rm T}(\cdot)\lambda_1\lambda_2T^2s(t)+f^{\rm T}(\cdot)\lambda_2^2T^2f(\cdot)\\ &-f^{\rm T}(\cdot)\lambda_2TN_{\tau+1}w(t)+w^{\rm T}(t)N_{\tau+1}^{\rm T}s(t)-w^{\rm T}(t)N_{\tau+1}^{\rm T}\lambda_1Ts(t)-w^{\rm T}(t)N_{\tau+1}^{\rm T}\lambda_2Tf(\cdot)\\ &+w^{\rm T}(t)N_{\tau+1}^{\rm T}N_{\tau+1}w(t)-s^{\rm T}(t)s(t)=\begin{bmatrix}s(t)\\ f(\cdot)\\ w(t)\end{bmatrix}^{\rm T}\begin{bmatrix}\Omega_{11}&\Omega_{12}\\ \Omega_{12}^{\rm T}&\Omega_{22}\end{bmatrix}\begin{bmatrix}s(t)\\ f(\cdot)\\ w(t)\end{bmatrix}<0,\end{aligned}$$

where Ω_{11}, Ω_{12} and Ω_{22} are provided in (16). According to Schur complement, $\left[\begin{smallmatrix}\Omega_{11}&\Omega_{12}\\ \Omega_{12}^{\rm T}&\Omega_{22}\end{smallmatrix}\right]<0$ can be equivalent to $\Omega_{11}<0$ and $\Omega_{22}-\Omega_{12}^{\rm T}\Omega_{11}^{-1}\Omega_{12}<0$.

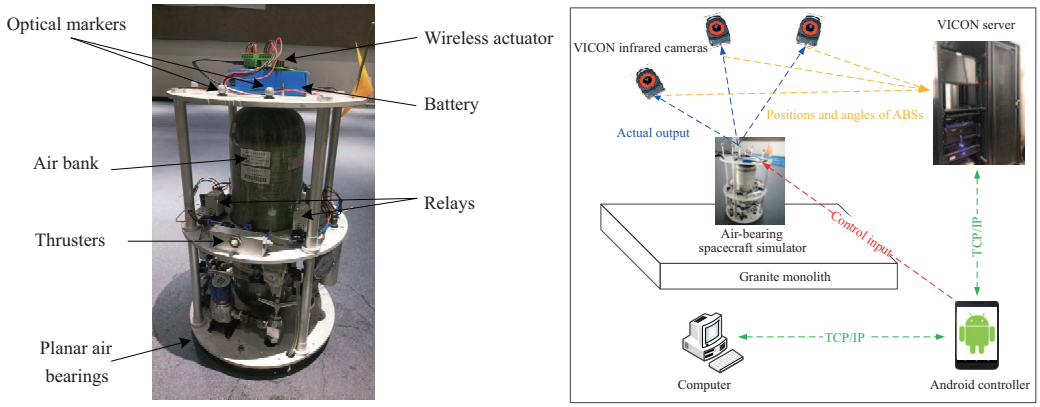

Figure 2 (Color online) (a) Hardware structure and (b) experiment platform of ABS simulator.

Table 1 Related parameters of ABS simulator

Parameter	Notation	Value
Mass	M	19.4 kg
Moment of inertia	J	0.239 kg $\cdot$ m^2
Radius	r	0.18 m

4 Application to air-bearing spacecraft simulator

4.1 Plant model

ABS simulator, given in Figure 2(a), is a common simulated device to realize the attitude joint orbit control of spacecraft at ground (see [40–42]). It has three freedom degrees to be controlled, containing x, y (positions in this plane), and ψ (angle rotating about z-axis). The related parameters of the ABS simulator are provided in Table 1.

An experimental platform of ABS simulator is established in Figure 2(b), where the information of x, y, and ψ is obtained by using VICON infrared cameras through optical markers of ABS simulator, and is sent to VICON server via local area network. Android controller uses the data to calculate the control inputs for the ABS simulator. A supervisory control software on computer is performed to achieve the monitoring and preservation of real-time information (more details are shown in [43, 44]). The origin is located at the center of the granite monolith. Based on the results in [31], a discrete-time second-order fully actuated system model of the ABS simulator is presented as

$$Mx(t+2) - 2Mx(t+1) + Mx(t) = T^2 F_x(t), \tag{17a}$$

$$My(t+2) - 2My(t+1) + My(t) = T^2 F_y(t), \tag{17b}$$

$$J\psi(t+2) - 2J\psi(t+1) + J\psi(t) = T^2 F_T(t), \tag{17c}$$

where T is the sampling period. The tests show that the Ping delay of our experimental platform is among 30–110 ms. In order to avoid the negative impacts of Ping delay and complicated computations, T is set to $T = 0.2$ s.

4.2 Comparative simulation

System (17a) is taken as an illustration to compare with an observer-based dynamic output feedback control (OBDOF) in [35] to illustrate the effectiveness. Following [35], choose $\mu = \nu = 0.05$, and the active times of random deception attacks are shown in Figure 3(a). When $\delta_{\rm sc}(t)/\delta_{\rm ca}(t) = 1$, the false data $\zeta_{\rm sc}(t)$ and $\zeta_{\rm ca}(t)$, shown in Figure 3(b), are injected in the SNC and NCA channels to tamper with the real signals. The communication delays in the SNC and NCA channels are given as $\tau_{\rm a} = 3$, $\tau_{\rm s} = 2$.

For the proposed work, a predictive sliding-mode control scheme for system (17a) is given as

$$F_x(t) = \frac{1}{T^2} K_{x0} x(t) + \frac{1}{T^2} K_{x1} x(t+1) + \frac{1}{T^2} v(t), \tag{18}$$

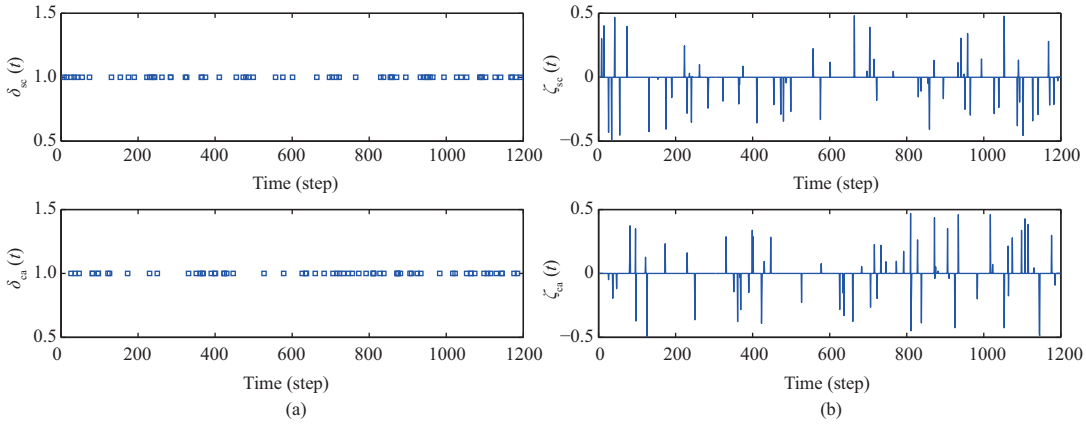

Figure 3 (Color online) Random deception attacks in the SNC and NCA channels. (a) Successful rate of random deception attacks; (b) random false data injected.

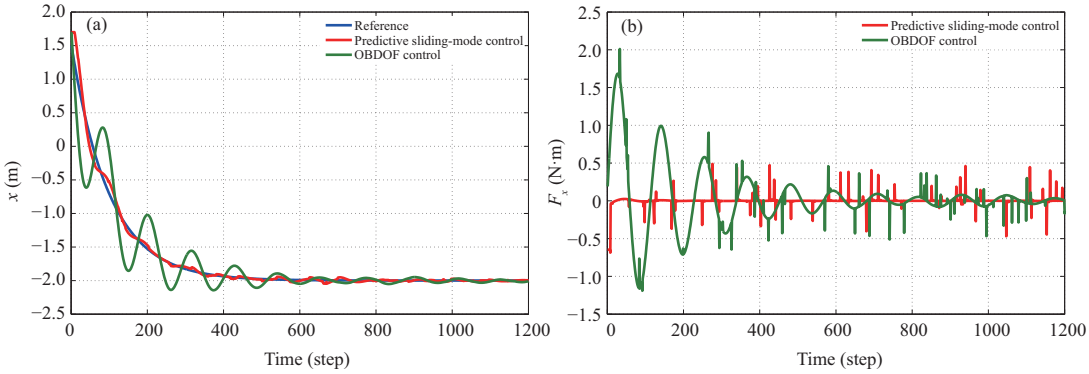

Figure 4 (Color online) Comparative results between predictive sliding-mode control (18) and OBDOF control in [35]. (a) Tracking performance; (b) control input.

where $K_{x0}=19.0159$, $K_{x1}=-19.2060$ are computed by using the guidance in Remark 1. For predictive control, let $N_y=5$, $N_u=3$, $W_1=I$, $W_2=10I$, $\Gamma=I$ and choose $s_x(t)=\Xi_x(q^{-1})e_x(t)$ with $\Xi_x=0.5-0.3q^{-1}-0.1q^{-2}$. For the sliding-mode reference, $\lambda_1=0.1$, $\lambda_2=0.05$, $\alpha=0.5$, $\beta=(\frac{\lambda_2 T}{1-\lambda_1 T})^{\frac{1}{1-\alpha}}+0.1$.

For OBDOF control in [35], system (17a) is firstly transformed into a first-order expression as

$$X(t+1)=A_xX(t)+B_xF_x(t)+B_x\delta_{\rm ca}(t)\zeta_{\rm ca}(t),\ \chi(t)=C_xX(t)+\delta_{\rm sc}(t)\zeta_{\rm sc}(t),$$

where

$$X(t)=\begin{bmatrix}x(t)\\x(t+1)\end{bmatrix},\ A_x=\begin{bmatrix}0&1\\-1&2\end{bmatrix},\ B_x=\begin{bmatrix}0\\0.0021\end{bmatrix},\ C_x=\begin{bmatrix}1\\0\end{bmatrix}^{\rm T}.$$

Then an OBDOF controller is established as

$$\Delta\hat{X}(t+1)=K_{\rm OBDOF,1}\Delta\hat{X}(t)+K_{\rm OBDOF,2}\Delta\chi(t),\ \Delta F_x(t)=K_{\rm OBDOF,3}\Delta\hat{X}(t)+K_{\rm OBDOF,4}(\chi(t)-r(t)).$$

The $K_{{\rm OBDOF},i}$, $i=1,\ldots,4$ is solved by an LMI as $A_{\rm OBDOF}^{\rm T}PA_{\rm OBDOF}-P<0$, where P is a symmetric and positive definite matrix and

$$A_{\rm OBDOF}=\begin{bmatrix}A_x&B_xK_{\rm OBDOF,3}&B_xK_{\rm OBDOF,4}\\K_{\rm OBDOF,2}C_x&K_{\rm OBDOF,1}&0\\-C_xA_x&-C_xB_xK_{\rm OBDOF,3}&I-C_xB_xK_{\rm OBDOF,4}\end{bmatrix}<0.$$

Then, the comparative results are shown in Figure 4.

Figure 4(a) illustrates the predictive sliding-mode control (18) can achieve the output tracking in steady and dynamical processes and overcome the negative effects caused by random deception attacks.

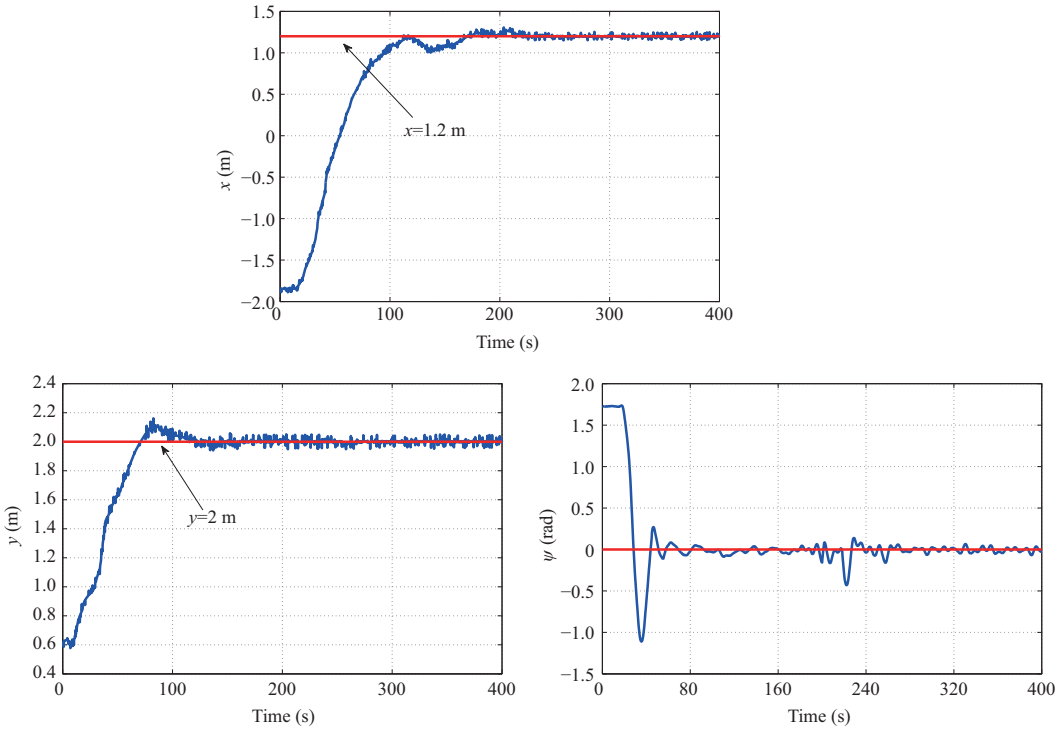

Figure 5 (Color online) Real responses of tracking experiment for ABS simulator under random deception attacks.

Meanwhile, OBDOF control in [35] also effectively copes with the same attacks to satisfy the tracking performance in a steady process, but it leads to unsatisfactory dynamical performance, containing overshoot and oscillation. The comparison of control input is given in Figure 4(b), which shows the total cost of control input for the predictive sliding-mode control (18) is less than that of OBDOF control in [35]. Figure 4 fully demonstrates the effectiveness and advantages of the proposed predictive sliding-mode control scheme.

4.3 Experimental verification

To further prove the practicability of a predictive sliding-mode control scheme, a tracking control experiment of the ABS simulator is taken to verify the theoretical results.

For systems (17a) and (17b), the prediction horizons, prediction and attack parameters, and communication delays are chosen as the same as in Subsection 4.2, the control protocol is selected as the same as (18). For system (17c), there is no information exchange. A local HOFA feedback is provided as

$$F_T(t) = \frac{1}{T^2}K_{\psi 0}\psi(t) + \frac{1}{T^2}K_{\psi 1}\psi(t+1),$$

where $K_{\psi 0} = 0.1673$, $K_{\psi 1} = -0.2151$ are computed by using the guidance in Remark 1. The experimental results are given in Figures 5–7 and the variation trends of sliding-mode variables are shown in Figure 8.

Figure 5 gives the real responses of the tracking control experiment for the ABS simulator under random deception attacks, where x and y responses can achieve the tracking performance under random deception attacks in the SNC and NCA channels with allowable errors, ψ is also be stabilized but still exists the vibration in the steady process because of the airflow in the experimental site and the reaction forces produced by thrusters. The control inputs of this experiment are plotted in Figure 6, which have some jitters because the linearized model (17) omits the uncertainties and nonlinearities but control inputs are still required to deal with them. Figure 7 provides the real motion trajectory of the ABS simulator, and shows the ABS simulator can reach and remain at the given location, so that the practicability of the proposed predictive sliding-mode control scheme is proved. Figure 8 shows the sliding-mode variables converge to 0. Note that the above drawbacks will be addressed along with our future and depth researches.

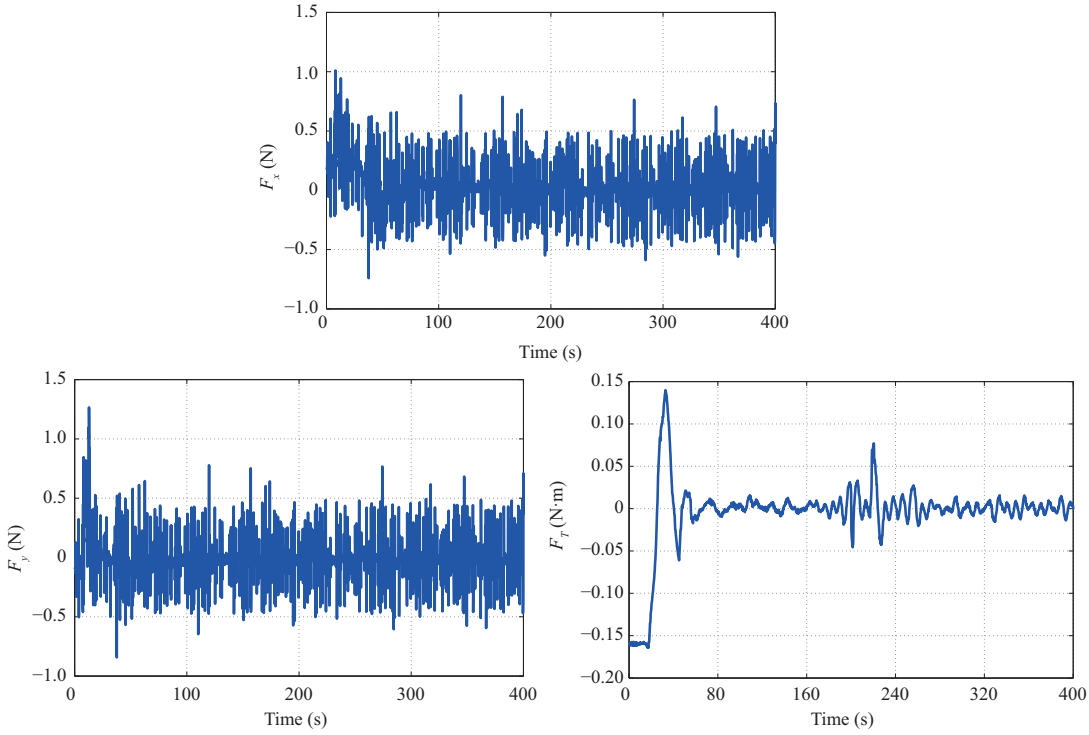

Figure 6 (Color online) Real control inputs of tracking experiment for ABS simulator under random deception attacks.

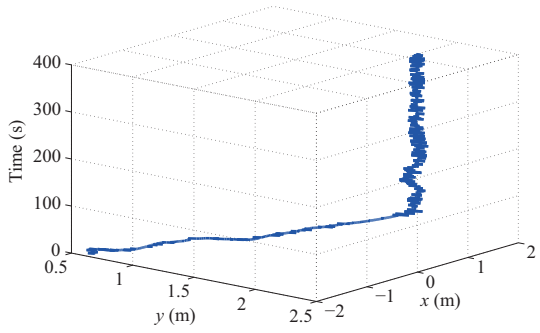

Figure 7 (Color online) Real trajectory of tracking experiment for ABS simulator under random deception attacks.

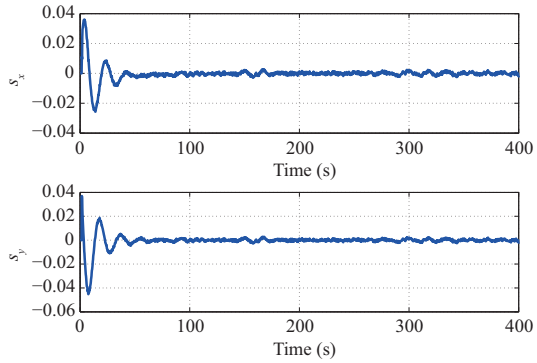

Figure 8 (Color online) Variation diagrams of sliding-mode variables s_x and s_y.

5 Conclusion

In this work, a predictive sliding-mode control scheme is proposed to address the security tracking of NHOFA systems under random deception attacks. A sliding-mode variable was adopted to counter random deception attacks by enhancing the robustness of closed-loop systems. Thereafter, an IHOFA prediction model was developed using a Diophantine equation. Through the model, multistep sliding-mode predictions were constructed to optimize the tracking performance and defense of random deception attacks. Consequently, a sufficient and necessary condition was put forward by using the Lyapunov function and the LMI method to ensure the stability and high tracking performance of closed-loop NHOFA systems. Future work will focus on the secure coordinated control of NHOFA multiagent systems under deception attacks and the secure tracking control of NHOFA systems under other types of cyberattacks.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 62173255, 62188101) and Shenzhen Key Laboratory of Control Theory and Intelligent Systems (Grant No. ZDSYS20220330161800001).

References

1 Qiu L, Dai L, Ahsan U, et al. Model predictive control for networked multiple linear motors system under DoS attack and time delay. IEEE Trans Ind Inf, 2023, 19: 790–799
2 Cuenca Á, Antunes D J, Castillo A, et al. Periodic event-triggered sampling and dual-rate control for a wireless networked control system with applications to UAVs. IEEE Trans Ind Electron, 2019, 66: 3157–3166
3 Bijami E, Farsangi M M, Lee K Y. Distributed control of networked wide-area systems: a power system application. IEEE Trans Smart Grid, 2020, 11: 3334–3345
4 Yu Y, Liu G P, Xiao H, et al. Design of networked secure and real-time control based on blockchain techniques. IEEE Trans Ind Electron, 2022, 69: 4096–4106
5 Yu Y, Liu G P, Zhou X, et al. Blockchain protocol-based predictive secure control for networked systems. IEEE Trans Ind Electron, 2023, 70: 783–792
6 Yu Y, Liu G P, Hu W. Learning-based secure control for multichannel networked systems under smart attacks. IEEE Trans Ind Electron, 2023, 70: 7183–7193
7 Li L, Yang H, Xia Y, et al. Attack detection and distributed filtering for state-saturated systems under deception attack. IEEE Trans Control Netw Syst, 2021, 8: 1918–1929
8 Yoo S J. Neural-network-based adaptive resilient dynamic surface control against unknown deception attacks of uncertain nonlinear time-delay cyberphysical systems. IEEE Trans Neural Netw Learn Syst, 2020, 31: 4341–4353
9 Wu B, Chang X H. Security control for nonlinear systems under quantization and Round-Robin protocol subject to deception attacks. ISA Trans, 2022, 130: 25–34
10 Zhang Z, Deng R, Cheng P, et al. Strategic protection against FDI attacks with moving target defense in power grids. IEEE Trans Control Netw Syst, 2022, 9: 245–256
11 Ning Z, Wang T, Zhang K. Dynamic event-triggered security control and fault detection for nonlinear systems with quantization and deception attack. Inf Sci, 2022, 594: 43–59
12 Chattopadhyay A, Mitra U. Security against false data-injection attack in cyber-physical systems. IEEE Trans Control Netw Syst, 2020, 7: 1015–1027
13 Li L, Zhang Y, Geng Q. Mean-square bounded consensus of nonlinear multi-agent systems under deception attack. ISA Trans, 2022, 129: 91–101
14 Wu Z, Xiong J, Xie M. Dynamic event-triggered L_∞ control for networked control systems under deception attacks: a switching method. Inf Sci, 2021, 561: 168–180
15 Yang Y, Huang J, Su X, et al. Adaptive control of cyber-physical systems under deception and injection attacks. J Franklin Institute, 2021, 358: 6174–6194
16 Gao R, Huang J. Adaptive control for high-order nonlinear systems subject to deception attacks with assignable stabilization performance. In: Proceedings of the 17th IEEE Conference on Industrial Electronics and Applications, Chengdu, 2022. 1194–1199
17 Yuan H, Guo Y, Xia Y. Event-based distributed filtering against deception attacks for sensor networks with quantization effect. ISA Trans, 2022, 126: 338–351
18 Zhang Q, Yin X, Hu S. A two-event-generator scheme for event-triggered control of uncertain NCSs under deception attacks. Inf Sci, 2022, 584: 148–169
19 Yang Y, Huang J, Su X, et al. Adaptive control of second-order nonlinear systems with injection and deception attacks. IEEE Trans Syst Man Cybern Syst, 2022, 52: 574–581
20 Wang J, Ding B, Hu J. Security control for LPV system with deception attacks via model predictive control: a dynamic output feedback approach. IEEE Trans Automat Contr, 2021, 66: 760–767
21 Tang X, Wu M, Li M, et al. On designing the event-triggered multistep model predictive control for nonlinear system over networks with packet dropouts and cyber attacks. IEEE Trans Cybern, 2022, 52: 11200–11212
22 Wang J, Song Y, Wei G. Security-based resilient robust model predictive control for polytopic uncertain systems subject to deception attacks and RR protocol. IEEE Trans Syst Man Cybern Syst, 2022, 52: 4772–4783
23 Wu Z, Wang Z, Wang Y, et al. Dynamic event-triggered networked predictive control for discrete-time NCSs under deception attacks. Intl J Robust Nonlinear, 2023, 33: 2682–2702
24 Liu Y, Chen Y, Li M. Event-based model predictive damping control for power systems with cyber-attacks. ISA Trans, 2023, 136: 687–700
25 Li B, Zhou X, Ning Z, et al. Dynamic event-triggered security control for networked control systems with cyber-attacks: a model predictive control approach. Inf Sci, 2022, 612: 384–398
26 Shi T, Guan Y, Zheng Y. Model predictive control of networked control systems with disturbances and deception attacks under communication constraints. Intl J Robust Nonlinear, 2022. doi: 10.1002/rnc.6363
27 Duan G R. High-order fully actuated system approaches: part I. Models and basic procedure. Int J Syst Sci, 2021, 52: 422–435
28 Zhang D W, Liu G P, Cao L. Proportional integral predictive control of high-order fully actuated networked multiagent systems with communication delays. IEEE Trans Syst Man Cybern Syst, 2023, 53: 801–812
29 Duan G Q, Liu G P. Attitude and orbit optimal control of combined spacecraft via a fully-actuated system approach. J Syst Sci Complex, 2022, 35: 623–640
30 Meng R, Hua C, Li K, et al. Adaptive event-triggered control for uncertain high-order fully actuated system. IEEE Trans Circuits Syst II, 2022, 69: 4438–4442
31 Zhang D W, Liu G P, Cao L. Predictive control of discrete-time high-order fully actuated systems with application to air-bearing spacecraft simulator. J Franklin Institute, 2023, 360: 5910–5927
32 Zhang D W, Liu G P. Predictive control for networked high-order fully actuated systems subject to communication delays and external disturbances. ISA Trans, 2023. doi: 10.1016/j.isatra.2023.03.041
33 Shao X, Ye D. Fuzzy adaptive event-triggered secure control for stochastic nonlinear high-order MASs subject to DoS attacks and actuator faults. IEEE Trans Fuzzy Syst, 2021, 29: 3812–3821
34 Duan G R. High-order fully actuated system approaches: Part X. Basics of discrete-time systems. Int J Syst Sci, 2022, 53: 810–832
35 Yu Y, Liu G P, Hu W. Security tracking control for discrete-time stochastic systems subject to cyber attacks. ISA Trans, 2022, 127: 133–145
36 Cao Z, Wang Z, Niu Y, et al. Sliding mode control for sampled-data systems subject to deception attacks: handling randomly perturbed sampling periods. IEEE Trans Cybern, 2022. doi: 10.1109/TCYB.2022.3202486
37 Qi W, Lv C, Park J H, et al. SMC for semi-Markov jump cyber-physical systems subject to randomly occurring deception

attacks. IEEE Trans Circuits Syst II, 2022, 69: 159–163
38 Xing M, Wu Y, Zhuang G, et al. Dynamic event-based sliding mode security control for singular semi-Markov jump LPV systems against deception attacks. ISA Trans, 2023, 133: 116–133
39 Sun B, Sun X. An algorithm of predictive sliding mode control based on power-function (in Chinese). Inform Control, 2011, 40: 39–43
40 Papakonstantinou C, Moraitis G, Lappas V, et al. Design of a low-cost air bearing testbed for nano CMG maneuvers. Aerospace, 2022, 9: 95
41 Rybus T, Wojtunik M, Basmadji F L. Optimal collision-free path planning of a free-floating space robot using spline-based trajectories. Acta Astronaut, 2022, 190: 395–408
42 Eun Y, Park S Y, Lee T, et al. Experimental validation of positive adaptive-control approach for spacecraft proximity maneuvers. J Aerosp Eng, 2021, 34: 04021096
43 Zhang D W, Liu G P, Cao L. Coordinated control of high-order fully actuated multiagent systems and its application: a predictive control strategy. IEEE ASME Trans Mechatron, 2022, 27: 4362–4372
44 Zhang D W, Liu G P, Cao L. Constrained cooperative control for high-order fully actuated multiagent systems with application to air-bearing spacecraft simulators. IEEE ASME Trans Mechatron, 2023, 28: 1570–1581