2021 60th IEEE Conference on Decision and Control (CDC)
December 13-15, 2021. Austin, Texas

# Adaptive Backstepping based Secure Control for P-normal Form of Second-Order Nonlinear Systems Against Deception Attacks

Mengze Yu, Wei Wang, Jing Zhou and Yongxin Tong

2021 60th IEEE Conference on Decision and Control (CDC) | 978-1-6654-3659-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDC45484.2021.9683733

*Abstract*— **In this paper, the adaptive secure control problem for a class of second-order nonlinear systems with p-normal form and uncertain time-varying parameters against sensor and actuator deception attacks is investigated. Multiplicative type of attacks are considered. A novel adaptive backstepping based resilient control scheme is constructed by employing the power integrator Lyapunov function technique and a special Nussbaum function. It is shown that all the closed-loop signals remain uniformly bounded despite the occurrence of the attacks. Simulation results on an illustrative example are provided to illustrate the effectiveness of the proposed control scheme.**

## I. INTRODUCTION

In recent years, networked control systems (NCSs), which realized the integration of the cyber space with the physical space, are ubiquitous for the potential engineering application in various fields. In such systems, communication network is usually set up to achieve information transmission between different components. Since it is usually public, the exchanged data may be influenced by malicious intruders, which can be regard as cyber attacks and may pose a great threat to normal operation of NCSs. Therefore, the safety issue of NCSs has gained much attention in control field.

In general, there are two kinds of cyber attacks which have been mainly recognized and concerned, i.e. deception attacks [1]–[9] and denial-of-service (DoS) attacks [10]–[12]. In the absence of control system information, the attackers often attempt to launch DoS attacks to block information exchange among different control components. By contrast, when the attackers are smart enough to illegally access the transmitted data, they are more likely to launch deception attacks to inject the modified data to that received by the controller and actuators, which may cause devastating damage to the entire system. Thus, it is necessary to develop secure control approaches to assure an accepted level of the system performance under deception attacks. Considering that these attacks often bring about uncertainties and the fact that adaptive control [1]–[6], [8], [9], [13], [14] is an effective way to ensure the desired performance of systems with various uncertainties, some seminal results have been reported on adaptive control to resist deception attacks. In [1], the sensor deception attack in linear cyber systems are treated by developing an adaptive secure control scheme. In [2], an adaptive controller with the learning framework is proposed for linear networked vehicles suffering from both sensor and actuator attacks. By introducing Nussbaum function technique, the problem with unknown sign of control coefficient caused by the deception attacks is treated by an adaptive resilient control method for a class of NCSs in [3]. Note that these methods are merely proposed for linear systems, hence they cannot be directly applied to nonlinear NCSs. In fact, most of actual physical systems inevitably contain some nonlinear components. Therefore, it is more imperative and meaningful to study the adaptive secure control of nonlinear NCSs under deception attacks. In [4] and [5], the stability of nonlinear strict-feedback system is guaranteed under data injection attacks by introducing novel coordinate transformations and Lyapunov functions in backstepping protocol establishing procedure, respectively. In [6], neural network is adopted in adaptive backstepping control to compensate for the attack-induced uncertainties for switched systems. In [9], the adaptive consensus control for a class of uncertain multi-agents systems under deception attacks are developed.

Note that the system models considered in all of the results mentioned above are standard strict-feedback nonlinear systems of triangular form. It means that the orders of the $(i+1)$th state ($x_{i+1}$) or the control input involved in the time derivative of the $i$th state ($\dot{x}_i$) are limit to one. However, in practice, many controlled plants can be modeled as uncertain nonlinear systems with p-normal form in which the mentioned orders may be arbitrary, such as complicated mechanical systems connected by high order nonlinear springs [15], [16]. The aforementioned control schemes are not applicable to such systems. Over the past decades, a series of results on adaptive control of uncertain p-normal systems have been published [15]–[18]. However, there are rare results available to solve the security problem of deception attacks.

Motivated by these observations, we study the problem of adaptive secure control for a class of second-order NCSs with p-normal form and uncertain time-varying parameters under both sensor and actuator attacks. A novel adaptive resilient control scheme is proposed by utilizing the backstepping technique. The main challenges and the contributions of this paper can be summarized as follows.

- As far as we are aware, this is the first work to manage the secure control of nonlinear systems with p-normal form against deception attacks. Compared with the existing results [4]–[6], [9], the aforementioned orders of the $(i+1)$th state and the control input in the system model considered in this paper are allowed to be any positive odd rational number rather than one. For these systems, the quadratic Lyapunov function cannot be used in the second step of the backstepping design. To overcome this difficulty, the power integrator

Mengze Yu and W. Wang are with School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China. yumengze0214@126.com, w.wang@buaa.edu.cn

J. Zhou is with The Department of Engineering Sciences, University of Agder, Grimstad, Norway 4898, Norway. jing.zhou@uia.no

Yongxin Tong is with School of Computer Science and Engineering, Beihang University, Beijing 100191, China. yxtong@buaa.edu.cn

Lyapunov function [15], [16] is introduced such that the backstepping controller design can be established.

- The main difficulty in this paper is that the actual control direction of the virtual control signal designed in each recursive step of backstepping design may become unknown and distinct under the deception attacks. Similar issues are treated in [3], [9] by introducing the Nussbaum function technique. However, both the general Nussbaum functions developed for single system as in [3], [7], [14] or most of the existing multiple Nussbaum function techniques as in [9], [19], [20] cannot be adopted to stabilize the the considered system, which will be discussed in detail later. To settle this problem, a special type of Nussbaum functions are introduced in this paper such that the closed-loop stability of the entire system can be guaranteed.

The remainder of this paper is organized as follows. In Section II, the models of the considered system and deception attacks and the control objective are introduced. In Section III, the purposed secure control scheme are provided and the stability analysis are given. Simulation results and conclusion are given in Section IV and Section V, respectively.

## II. Preliminaries and Problem Formulation

### A. System Model

In this paper, a class of second-order NCSs with p-normal form are considered as follows.

$$\begin{aligned}\dot{x}_1 &= \theta_1(t)^T\varphi_1(x_1) + b_1(x_1)x_2^{p_1} + d_1(t)\\ \dot{x}_2 &= \theta_2(t)^T\varphi_2(\bar{x}_2) + b_2(\bar{x}_2)\tilde{u}^{p_2} + d_2(t)\end{aligned} \tag{1}$$

where $\bar{x}_2 = [x_1, x_2]^T \in R^2$, $\tilde{u} \in R$ are the measurable states and the input signal received from actuators, respectively. $\theta_i(t) \in R^{q_i}, i = 1, 2$ denotes a vector of the uncertain time-varying system parameters. $\varphi_i(\cdot)$ denotes a vector of known smooth functions. $d_i(t), i = 1, 2$ denotes the external disturbance. $b_i(\cdot) \in R, i = 1, 2$ denotes a smooth nonlinear function and $b_2(\cdot)$ represents the control coefficient. The order $p_i \geq 1$ is a positive odd rational number whose numerators and denominators are all positive odd integers. In this paper, $y = x^p$ is identical with $y = \text{sign}(x)|x|^p$.

### B. Deception attacks model

In the considered NCSs, both sensor-to-controller and controller-to-actuator communication channels are subjected to the adversaries, as depicted in Fig. 1.

The considered deception attacks are modeled as

$$\tilde{x}_i(t) = \lambda_{is}(t)x_i(t), \ i = 1, 2 \tag{2}$$

$$\tilde{u}(t) = \lambda_a(t)u(t) \tag{3}$$

where $\tilde{x}_i(t)$ is the compromised state which can be applied for feedback, $u(t)$ is the actual control signal to be designed. $\lambda_{is}(t)$ and $\lambda_a(t)$ are unknown time-varying attack weights. It implies that under the cyber-attacks injected to both communication channels, $\tilde{x}_i(t)$ and $\tilde{u}(t)$ received by controller and actuator may be modified and different from the actual measured state $x_i(t)$ and input $u(t)$. It is clear that if neither communication channel suffers from these attacks, $\lambda_{is}(t) = 1$ and $\lambda_a(t) = 1$.

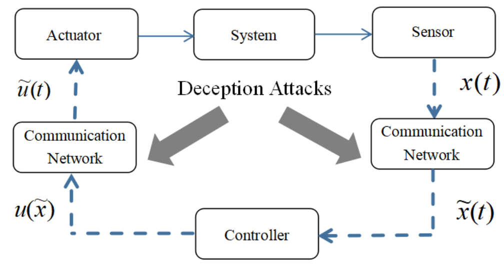


Fig. 1. Closed-loop framework of the system under attacks.

Consequently, defining $\bar{\tilde{x}}_2 = [\tilde{x}_1, \tilde{x}_2]^T$, system (1) under deception attacks can be rewritten as follows

$$\begin{aligned}\dot{x}_1 &= \theta_1(t)^T\varphi_1(x_1) + b_1(x_1)\lambda_{2s}^{-p_1}(t)\tilde{x}_2^{p_1} + d_1(t)\\ \dot{x}_2 &= \theta_2(t)^T\varphi_2(\bar{x}_2) + b_2(\bar{x}_2)\lambda_a^{p_2}(t)u(\bar{\tilde{x}}_2)^{p_2} + d_2(t)\end{aligned} \tag{4}$$

where $u(\bar{\tilde{x}}_2)$ indicates that only the compromised states signals are available for control design.

*Remark 1:* Compared with the existing results [4]–[6], [9], the weights $\lambda_{is}(t)$ multiplied by different states may be distinct in this paper. The actuator attack model (3) is a multiplicative manner instead of an additive one with injected state information ($i.e.$ $\tilde{u} = u + w^T(t)\psi(x)$) as in [2]–[6]. It is reasonable because the adversaries may directly use the stolen control information as the deception data. Besides, the sign of each $b_i(\cdot)$ is allowed to be unknown in this paper. In fact, from (4), the actual coefficients of $\tilde{x}_2$ and $u$ under attacks are $b_1\lambda_{2s}^{-p_1}$ and $b_2\lambda_a^{p_2}$. Since the signs of all the attack weights are unknown, the signs of $b_1\lambda_{2s}^{-p_1}$ and $b_2\lambda_a^{p_2}$ are uncertain which may be different from that of $b_1$ and $b_2$, respectively. In this case, the predesigned negative feedback control signal may become positive feedback, which may cause devastating damage to most of the closed-loop control systems. Such an issue constitutes as the major difference between secure control and fault-tolerant control problems, as seen from [21], [22] and references therein, where the loss-of-effectiveness type of faults $\bar{u}(t) = \rho(t)u(t)$ with $0 < \rho(t) < 1$ are concerned.

### C. Control Objective

The *control objective* in this paper is to design an adaptive controller such that all the signals in the closed-loop system are uniformly bounded despite the occurrence of deception attacks.

To achieve the control objective, the following assumptions are firstly imposed.

*Assumption 1:* The uncertain parameters $\theta_i(t)$ and the disturbance $d_i(t)$ lie on two compact sets, respectively, $i.e.$ $\theta_i(t) \in \Omega_{\theta_i} = \{||\theta_i(t)|| \leq M_i\}$ and $d_i(t) \in \Omega_{d_i} = \{|d_i(t)| \leq \varepsilon_i\}$, where $M_i$ and $\varepsilon_i$ are unknown positive constant.

*Assumption 2:* There exist two constants $b_m$ and $b_M$ such that $0 < b_m \leq |b_i| \leq b_M$.

*Assumption 3:* The continuous attack weights satisfy $\lambda_{is}(t) \neq 0$ and $\lambda_a(t) \neq 0$. Furthermore, there exist some unknown positive constants $\bar{\lambda}_{is}, \underline{\lambda}_{is}, \mu_{is}, \bar{\lambda}_a, \underline{\lambda}_a$ such that the following inequalities hold

$$\underline{\lambda}_{is} \leq |\lambda_{is}(t)| \leq \bar{\lambda}_{is}, \ |\dot{\lambda}_{is}(t)| \leq \mu_{is}, \ \underline{\lambda}_a \leq |\lambda_a(t)| \leq \bar{\lambda}_a$$

*Remark 2:* If $\lambda_{is}(t) = 0$ and $\lambda_a(t) = 0$, the states are totally canceled and any input signals cannot be received by actuators. Then the system may become uncontrollable. Assumption 3 is included to exclude this case. Moreover, since the energy provided for launching the attacks is usually limited, the boundedness of $|\lambda_{is}(t)|$, $|\dot{\lambda}_{is}(t)|$ and $|\lambda_a(t)|$ is reasonable. It follows that $|\lambda_{is}^{-1}(t)| \leq \underline{\lambda}_{is}^{-1} \triangleq \epsilon_{is}$,

The following lemmas are introduced as preliminary results for convenience of the control design.

*Lemma 1:* [16] If $f(x, y)$ is a continuous real-value function for $x \in R^m$ and $y \in R^n$, there exist two smooth functions $A(x) \geq 0$ and $B(y) \geq 0$ such that

$$|f(x,y)| \leq A(x)B(y)$$

*Lemma 2:* [15] If $0 < \eta = \frac{\eta_1}{\eta_2} < 1$, where $\eta_1$ and $\eta_2$ are positive odd integers, then the following inequation holds

$$|x^\eta - y^\eta| \leq 2^{1-\eta}|x-y|^\eta, \forall x, y \in R$$

To handle the issue of unknown control coefficients as discussed in Remark 1, a special type of Nussbaum functions are introduced as follows.

*Definition 1:* [4] If $\mathcal{N}(s)$: $R \longmapsto R$ is a continue function satisfying the following equalities:

$$\liminf_{k\to\infty} \frac{k - \int_0^k \mathcal{N}^-(s)ds}{\int_0^k \mathcal{N}^+(s)ds} = 0$$

$$\liminf_{k\to\infty} \frac{k + \int_0^k \mathcal{N}^+(s)ds}{-\int_0^k \mathcal{N}^-(s)ds} = 0$$

with the positive and negative truncated functions $\mathcal{N}^+(s) = \max\{0, \mathcal{N}(s)\}$, $\mathcal{N}^-(s) = \min\{0, \mathcal{N}(s)\}$, then it is called as $\mathcal{N}$ function which can be expressed as $\mathcal{N}(s) \in \mathcal{N}$.

Then Lemma 3 is given as follows.

*Lemma 3:* [4] Define two smooth functions $V(t)$ and $\chi_i(t)$ on $[0, +\infty)$ $(i = 1, \ldots, N)$ with $V(t) \geq 0$. Let the time-varying functions $g_i(t) \in [g_i^-, g_i^+]$ for two constants $g_i^-$ and $g_i^+$ satisfying $g_i^- g_i^+ > 0$ $(0 \notin [g_i^-, g_i^+])$. If there exist two positive constant $\beta$ and $C$ satisfy

$$\dot{V}(t) \leq -\beta V(t) + C + \sum_{i=1}^{N} \left[g_i(t)\mathcal{N}(\chi_i(t)) + 1\right] \dot{\chi}_i(t) \quad (5)$$

$$\dot{\chi}_i(t) \geq 0 \quad (6)$$

then $V(t)$ and $\chi_i(t)$ are bounded over $[0, +\infty)$.

## III. Design of Adaptive Resilient Controllers

In this section, an adaptive backstepping resilient control scheme will be presented. Firstly, we define the following error variables.

$$\begin{aligned} z_1 &= \tilde{x}_1 \\ z_2 &= \tilde{x}_2^{p_1} - \alpha_1^{p_1} \end{aligned} \quad (7)$$

$\alpha_1$ is the first virtual control signal, which will be determined later.

*Step 1:* From (4) and (7), we can compute the time derivative of $z_1$ as

$$\begin{aligned} \dot{z}_1 &= \lambda_{1s}\dot{x}_1 + \dot{\lambda}_{1s}x_1 \\ &= \lambda_{1s}\theta_1^T(t)\varphi_1(x_1) + \lambda_{1s}b_1\lambda_{2s}^{-p_1}\tilde{x}_2^{p_1} \\ &\quad + \lambda_{1s}d_1(t) + \dot{\lambda}_{1s}x_1 \end{aligned} \quad (8)$$

Then we choose the following Lyapunov function candidate $V_1^0$

$$V_1^0 = \frac{1}{2}z_1^2 \quad (9)$$

From (8) and (9), the time derivative of $V_1^0$ can be obtained as

$$\begin{aligned} \dot{V}_1^0 &= z_1\Big(\lambda_{1s}\theta_1^T\varphi_1(x_1) + \lambda_{1s}b_1\lambda_{2s}^{-p_1}\tilde{x}_2^{p_1} + \lambda_{1s}d_1 + \dot{\lambda}_{1s}x_1\Big) \\ &= z_1\big(\lambda_{1s}\theta_1^T\varphi_1 + \lambda_{1s}b_1\lambda_{2s}^{-p_1}z_2 + \lambda_{1s}b_1\lambda_{2s}^{-p_1}\alpha_1^{p_1} \\ &\quad + \lambda_{1s}d_1 + \dot{\lambda}_{1s}x_1\big) \end{aligned} \quad (10)$$

We shall analyze the upper bound of each terms involved in the second equation of (10). According to Assumption 3 and Lemma 1, there exists a smooth function $A_1(\cdot)$, an unknown positive constant $\bar{\varsigma}_1$ and a known positive smooth function $\phi_1(\tilde{x}_1)$ such that

$$\begin{aligned} ||\varphi_1(x_1)||^2 &= ||\varphi_1(\lambda_{1s}^{-1}\tilde{x}_1)||^2 \\ &\leq A_1(\lambda_{1s}^{-1})\phi_1(\tilde{x}_1) \leq \bar{\varsigma}_1\phi_1(\tilde{x}_1) \end{aligned} \quad (11)$$

According to Assumptions 1-3, (11) and Young's inequality $|ab| \leq a^2 + \frac{1}{4}b^2$, we have

$$z_1\lambda_{1s}\theta_1^T\varphi_1 \leq \bar{\lambda}_{1s}^2 M_1^2\bar{\varsigma}_1 z_1^2\phi_1(\tilde{x}_1) + \frac{1}{4} \quad (12)$$

$$z_1\lambda_{1s}b_1\lambda_{2s}^{-p_1}z_2 \leq \bar{\lambda}_{1s}^2 b_M^2\epsilon_{2s}^{p_1}z_1^2 + \frac{1}{4}z_2^2 \quad (13)$$

$$z_1\lambda_{1s}d_1 \leq \bar{\lambda}_{1s}^2\varepsilon_1^2 z_1^2 + \frac{1}{4} \quad (14)$$

$$z_1\dot{\lambda}_{1s}x_1 \leq \mu_{1s}\epsilon_{1s}z_1^2 \quad (15)$$

Combining (10) and (12)-(15), there is

$$\dot{V}_1^0 \leq z_1\left(\Theta_1 z_1 F_1(\tilde{x}_1) + \lambda_{1s}b_1\lambda_{2s}^{-p_1}\alpha_1^{p_1}\right) + \frac{1}{4}z_2^2 + \frac{1}{2} \quad (16)$$

where $\Theta_1$ is an unknown positive constant and $F_1(\tilde{x}_1)$ is a smooth function, which are defined as follows.

$$\Theta_1 = \max(\bar{\lambda}_{1s}^2 M_1^2\bar{\varsigma}_1, \bar{\lambda}_{1s}^2 b_M^2\epsilon_{2s}^{p_1} + \bar{\lambda}_{1s}^2\varepsilon_1^2 + \mu_{1s}\epsilon_{1s}) \quad (17)$$

$$F_1(\tilde{x}_1) = \phi_1(x_1) + 1 \quad (18)$$

By adopting the $\mathcal{N}$ function $\mathcal{N}(s)$ in Lemma 3, the virtual control $\alpha_1^{p_1}$ is designed as

$$\alpha_1^{p_1} = \mathcal{N}(\chi_1)\left(c_1 + \hat{\Theta}_1 F_1(\tilde{x}_1)\right)z_1 \quad (19)$$

$$\dot{\chi}_1 = \left(c_1 + \hat{\Theta}_1 F_1(\tilde{x}_1)\right)z_1^2 \quad (20)$$

where $\chi_1$ is an auxiliary variable, $c_1 > 0$ is a design parameter, $\hat{\Theta}_1$ is the estimate of $\Theta_1$. Defining $\tilde{\Theta}_1$ as the parameter estimation error, i.e. $\tilde{\Theta}_1 = \Theta_1 - \hat{\Theta}_1$, the Lyapunov function (9) can be augmented as

$$V_1 = V_1^0 + \frac{1}{2\gamma_1}\tilde{\Theta}_1^2 \quad (21)$$

where $\gamma_1$ is a positive constant. Then it is shown that

$$\dot{V}_1 \leq -c_1 z_1^2 + \lambda_{1s}b_1\lambda_{2s}^{-p_1}\mathcal{N}(\chi_1)\dot{\chi}_1 + \dot{\chi}_1$$

$$+\frac{1}{\gamma_1}\tilde{\Theta}_1(\gamma_1 z_1^2 F_1-\dot{\hat{\Theta}}_1)+\frac{1}{4}z_2^2+\frac{1}{2} \tag{22}$$

Design the adaptive law $\dot{\hat{\Theta}}_1$ as

$$\dot{\hat{\Theta}}_1=\gamma_1 z_1^2 F_1-\sigma_1\hat{\Theta}_1,\ \hat{\Theta}_1(0)\geq 0 \tag{23}$$

where $\sigma_1$ is a positive constant. Define $b_1'=\lambda_{1s}b_1\lambda_{2s}^{-p_1}$, then it is shown that

$$\begin{aligned}\dot{V}_1\leq &-c_1z_1^2-\frac{\sigma_1}{2\gamma_1}\tilde{\Theta}_1^2+(b_1'\mathcal{N}(\chi_1)+1)\dot{\chi}_1\\ &+\frac{1}{4}z_2^2+\frac{1}{2}+\frac{\sigma_1}{2\gamma_1}\Theta_1^2\end{aligned} \tag{24}$$

*Step 2:* It can be observed from (18)-(20) that $\alpha_1^{p_1}$ is a smooth function of $\tilde{x}_1$, $\hat{\Theta}_1$ and $\chi_1$. Then as inspired by [15], [16], we introduce the following power integrator as the Lyapunov function candidate

$$W(\tilde{x}_2,\alpha_1)=\int_{\alpha_1}^{\tilde{x}_2}(s^{p_1}-\alpha_1^{p_1})^{2-\frac{1}{p_1}}ds \tag{25}$$

From Lemma 2, $W(\tilde{x}_2,\alpha_1)$ satisfies that

$$\begin{aligned}W&\leq|\tilde{x}_2-\alpha_1||\tilde{x}_2^{p_1}-\alpha_1^{p_1}|^{2-\frac{1}{p_1}}\\ &\leq 2^{1-\frac{1}{p_1}}|z_2|^{2-\frac{1}{p_1}}|\tilde{x}_2^{p_1}-\alpha_1^{p_1}|^{\frac{1}{p_1}}\leq 2z_2^2\end{aligned} \tag{26}$$

$$\begin{aligned}W&\geq 2^{(1-p_1)(2-\frac{1}{p_1})}\int_{\alpha_1}^{\tilde{x}_2}(s-\alpha_1)^{2p_1-1}ds\\ &=a(\tilde{x}_2-\alpha_1)^{2p_1}\end{aligned} \tag{27}$$

where $a=\frac{2^{(1-p_1)(2-\frac{1}{p_1})}}{2p_1}$. Thus, $W$ is positive definite with respect to $z_2$. According to [15], from (4), the time derivative of $W$ is derived as

$$\begin{aligned}\dot{W}=&z_2^{2-\frac{1}{p_1}}\left(\lambda_{2s}\theta_2^T\varphi_2+\lambda_{2s}b_2\lambda_a^{p_2}u^{p_2}+\lambda_{2s}d_2+\dot{\lambda}_{2s}x_2\right)\\ &+L\left(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1}\left(\lambda_{1s}\theta_1^T\varphi_1+\lambda_{1s}b_1\lambda_{2s}^{-p_1}\tilde{x}_2^{p_1}+\lambda_{1s}d_1+\dot{\lambda}_{1s}x_1\right)\right.\\ &\left.+\frac{\partial\alpha_1^{p_1}}{\partial\hat{\Theta}_1}\dot{\hat{\Theta}}_1+\frac{\partial\alpha_1^{p_1}}{\partial\chi_1}\dot{\chi}_1\right)\end{aligned} \tag{28}$$

where

$$L=-(2-\frac{1}{p_1})\int_{\alpha_1}^{\tilde{x}_2}(s^{p_1}-\alpha_1^{p_1})^{1-\frac{1}{p_1}}ds \tag{29}$$

Similar to (26), it is shown that $|L|\leq 4|z_2|$. Then similar to (11), there exists an unknown positive constant $\bar{\varsigma}_2$ and a known smooth function $\phi_2(\bar{\tilde{x}}_2)$ such that

$$||\varphi_2(\bar{x}_2)||^2\leq\bar{\varsigma}_2\phi_2(\bar{\tilde{x}}_2) \tag{30}$$

Then a generic notation $Q(v)$ is introduced to denote a $C^\infty$ upper bound of $|v|$. For example, $Q(v)$ can be defined as $Q(v)=\sqrt{\Delta+v^2}$, where $\Delta$ is a positive constant. According to Assumptions 1-3, (28), (30) and Young's inequality, we can obtain that

$$\begin{aligned}z_2^{2-\frac{1}{p_1}}\lambda_{2s}\theta_2^T\varphi_2&\leq\bar{\lambda}_{2s}M_2|z_2|Q(z_2)^{1-\frac{1}{p_1}}||\varphi_2||\\ &\leq\bar{\lambda}_{2s}^2M_2^2\bar{\varsigma}_2z_2^2Q(z_2)^{2-\frac{2}{p_1}}\phi_2+\frac{1}{4}\end{aligned} \tag{31}$$

$$z_2^{2-\frac{1}{p_1}}\lambda_{2s}d_2\leq\bar{\lambda}_{2s}^2\varepsilon_2^2z_2^2Q(z_2)^{2-\frac{2}{p_1}}+\frac{1}{4} \tag{32}$$

$$z_2^{2-\frac{1}{p_1}}\dot{\lambda}_{2s}x_2\leq\mu_{2s}^2\epsilon_{2s}^2z_2^2Q(z_2)^{2-\frac{2}{p_1}}\tilde{x}_2^2+\frac{1}{4} \tag{33}$$

$$L\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1}\lambda_{1s}\theta_1^T\varphi_1\leq 16\bar{\lambda}_{1s}^2M_1^2\bar{\varsigma}_1z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1})^2\phi_1+\frac{1}{4} \tag{34}$$

$$L\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1}\lambda_{1s}d_1\leq 16\bar{\lambda}_{1s}^2\varepsilon_1^2z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1})^2+\frac{1}{4} \tag{35}$$

$$L\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1}\dot{\lambda}_{1s}x_1\leq 16\mu_{1s}^2\epsilon_{1s}^2z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1})^2\tilde{x}_1^2+\frac{1}{4} \tag{36}$$

$$L\frac{\partial\alpha_1^{p_1}}{\partial\hat{\Theta}_1}\dot{\hat{\Theta}}_1\leq 16z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\hat{\Theta}_1})^2(\dot{\hat{\Theta}}_1)^2+\frac{1}{4} \tag{37}$$

$$L\frac{\partial\alpha_1^{p_1}}{\partial\chi_1}\dot{\chi}_1\leq 16z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\chi_1})^2(\dot{\chi}_1)^2+\frac{1}{4} \tag{38}$$

$$\begin{aligned}L\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1}\lambda_{1s}b_1\lambda_{2s}^{-p_1}\tilde{x}_2^{p_1}\leq&16\bar{\lambda}_{1s}^2b_M^2\epsilon_{2s}^{2p_1}z_2^2(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1})^2Q(\tilde{x}_2)^{2p_1}\\ &+\frac{1}{4}\end{aligned} \tag{39}$$

Combining (28) and (31)-(39), there is

$$\dot{W}\leq z_2^{2-\frac{1}{p_1}}(\Theta_2z_2^{\frac{1}{p_1}}F_2+\lambda_{2s}b_2\lambda_a^{p_2}u^{p_2})+\frac{9}{4} \tag{40}$$

where $\Theta_2$ is an unknown positive constant and $F_2(\bar{\tilde{x}}_2,\hat{\Theta}_1,\chi_1)$ is a smooth function, which are defined as follows.

$$\begin{aligned}\Theta_2=&\max(\bar{\lambda}_{2s}^2M_2^2\bar{\varsigma}_2,\bar{\lambda}_{2s}^2\varepsilon_2^2,\mu_{2s}^2\epsilon_{2s}^2,16\bar{\lambda}_{1s}^2M_1^2\bar{\varsigma}_1,\\ &16\bar{\lambda}_{1s}^2b_M^2\epsilon_{2s}^{2p_1},16\bar{\lambda}_{1s}^2\varepsilon_1^2,16\mu_{1s}^2\epsilon_{1s}^2,16)\end{aligned} \tag{41}$$

$$\begin{aligned}F_2=&Q(z_2)^{2-\frac{2}{p_1}}(\phi_2+\tilde{x}_2^2+1)+(\frac{\partial\alpha_1^{p_1}}{\partial\tilde{x}_1})^2\left(\phi_1+1+\tilde{x}_1^2\right.\\ &\left.+Q(\tilde{x}_2)^{2p_1}\right)+(\frac{\partial\alpha_1^{p_1}}{\partial\hat{\Theta}_1})^2(\dot{\hat{\Theta}}_1)^2+(\frac{\partial\alpha_1^{p_1}}{\partial\chi_1})^2(\dot{\chi}_1)^2\end{aligned} \tag{42}$$

By adopting the $\mathcal{N}$ function $\mathcal{N}(s)$ in Lemma 3, the control signal $u$ is designed as

$$u^{p_2}=\mathcal{N}(\chi_2)\left(c_2+\frac{1}{4}+\hat{\Theta}_2F_2\right)z_2^{\frac{1}{p_1}} \tag{43}$$

$$\dot{\chi}_2=\left(c_2+\frac{1}{4}+\hat{\Theta}_2F_2\right)z_2^2 \tag{44}$$

where $\chi_2$ is an designed auxiliary variable, $c_2>0$ is a design parameter, $\hat{\Theta}_2$ is the estimate of $\Theta_2$. Defining $\tilde{\Theta}_2$ as the parameter estimation error, i.e. $\tilde{\Theta}_2=\Theta_2-\hat{\Theta}_2$, the Lyapunov function (25) can be augmented as

$$V_2=W+\frac{1}{2\gamma_2}\tilde{\Theta}_2^2 \tag{45}$$

where $\gamma_2>0$. Taking the derivative of $V_2$, yields that

$$\begin{aligned}\dot{V}_2\leq&-c_2z_2^2-\frac{1}{4}z_2^2+\lambda_{2s}b_2\lambda_a^{p_2}\mathcal{N}(\chi_2)\dot{\chi}_2+\dot{\chi}_2\\ &+\frac{1}{\gamma_2}\tilde{\Theta}_2(\gamma_2z_2^2F_2-\dot{\hat{\Theta}}_2)+\frac{9}{4}\end{aligned} \tag{46}$$

Design the adaptive law $\dot{\hat{\Theta}}_2$ as

$$\dot{\hat{\Theta}}_2=\gamma_2z_2^2F_2-\sigma_2\hat{\Theta}_2,\ \hat{\Theta}_2(0)\geq 0 \tag{47}$$

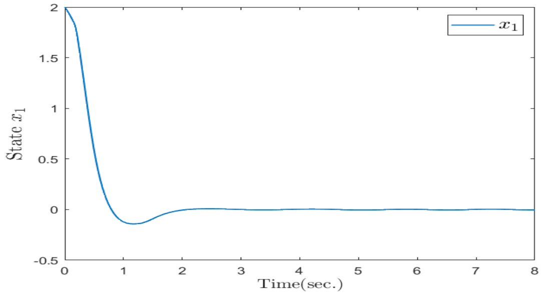


Fig. 2. Trajectory of $x_1$

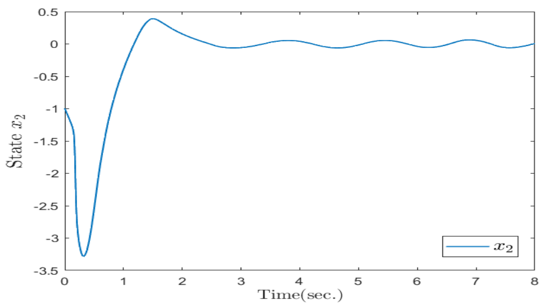


Fig. 3. Trajectory of $x_2$

where $\sigma_2 > 0$. Define $b_2' = \lambda_{2s} b_2 \lambda_a^{p_2}$, then it is shown that

$$\dot{V}_2 \leq - c_2 z_2^2 - \frac{1}{4} z_2^2 - \frac{\sigma_2}{2\gamma_2} \tilde{\Theta}_2^2 + (b_2' \mathcal{N}(\chi_2) + 1) \dot{\chi}_2 + \frac{9}{4} + \frac{\sigma_2}{2\gamma_2} \Theta_2^2 \quad (48)$$

### A. Stability Analysis

Now, we formally state the stability analysis results with the designed backstepping based adaptive secure control scheme in the following theorem.

*Theorem 1:* Consider the uncertain nonlinear time-varying systems (1) with p-normal form suffering from deception attacks (2), (3) under the constraints of Assumptions 1-3. Then, the designed adaptive secure controller (43) with parameter estimators (23), (47) can guarantee the closed-loop system signals uniformly bounded.

*Proof:* Define the Lyapunov function for the entire closed-loop system as

$$V = V_1 + V_2 = \frac{1}{2} z_1^2 + W + \frac{1}{2\gamma_1} \tilde{\Theta}_1^2 + \frac{1}{2\gamma_2} \tilde{\Theta}_2^2 \quad (49)$$

Combining (24),(26) and (48), we can obtain that

$$\dot{V} \leq -\omega V + R + \sum_{i=1}^{2} (b_i' \mathcal{N}(\chi_i) + 1) \dot{\chi}_i \quad (50)$$

where $\omega = \min(2c_1, \frac{c_2}{2}, \sigma_1, \sigma_2)$, $R = \frac{11}{4} + \frac{\sigma_1}{2\gamma_1} \Theta_1^2 + \frac{\sigma_2}{2\gamma_2} \Theta_2^2$. Then from (18), (23), (42) and (47), it follows that

$$\hat{\Theta}_i(t) = e^{-\sigma_i t} \hat{\Theta}_i(0) + \int_0^t \gamma_i e^{-\sigma_i (t-s)} z_i^2(s) F_i(s) ds \geq 0 \quad (51)$$

Then from (20) and (44), it is clear that $\dot{\chi}_i \geq 0$. From (50) and Lemma 3, it can be concluded that $V(t)$ and $\chi_i(t) (i = 1, 2)$ are bounded, which implies that $z_1$, $W$, $\hat{\Theta}_1$ and $\hat{\Theta}_2$ are

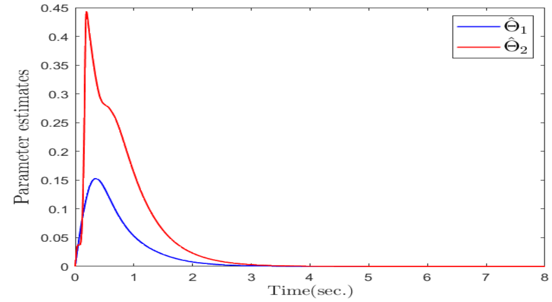


Fig. 4. Trajectories of $\hat{\Theta}_1$ and $\hat{\Theta}_2$

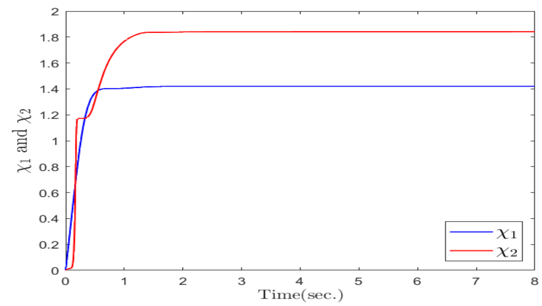


Fig. 5. Trajectories of $\chi_1$ and $\chi_2$

bounded. From (19), $\alpha_1$ is bounded. From (27), it is shown that $\tilde{x}_2 - \alpha_1$ is bounded, hence $\tilde{x}_2$ and $z_2$ are also bounded. Since $x_i = \lambda_{is}^{-1} \tilde{x}_i (i = 1, 2)$, it indicates that real state signal $x_i$ is bounded. From (42) and (43), it is clear that the control signal $u$ is bounded. Thus, all the closed-loop signals remain uniformly bounded. ■

*Remark 3:* From (16) and (40), under the deception attacks (2), (3), the actual control coefficients of $\alpha_1$ and $u$ are $b_1' = \lambda_{1s} b_1 \lambda_{2s}^{-p_1}$ and $b_2' = \lambda_{2s} b_2 \lambda_a^{p_2}$, respectively, which are non-identically unknown, so the Nussbaum function is necessary for the control design. However, consider the case that the sum of multiple Nussbaum functions including different control direction may appear on the right side of the single inequality (50), traditional Nussbaum functions such as $N(\chi) = \chi^2 cos(\chi)$ in [3] and [14] cannot be adopted to guarantee the boundedness of $V$ because they may cancel one another, as pointed out in [19]. On the other hands, although the multiple Nussbaum function technique is effective to deal with this case, most of the current multiple Nussbaum functions such as $N_i(\chi_i) = \cosh(\alpha \chi_i) \sin(\frac{\chi_i}{\beta^i})$ [19] and $N_i'(\chi_i) = 2^{N-i} \chi_i e^{\chi_i^2} sin(2^{i-1} \chi_i)$ [20] cannot be adopted, either. The reason is that the inequalities (12)-(14) and (31)-(39) inevitably lead to an constant $R$ on the right side of (50). If these multiple Nussbaum functions are adopted, the unbounded term $Rt$ will appear in the upper bound of $V(t)$ by integrating both sides of (50), the boundedness of the closed-loop system cannot be assured. To handle this problem, a special class of $\mathcal{N}$ functions are adopted in this paper. By introducing the Lemma 3, the boundedness of $V(t)$ can be shown under the designed controller.

*Remark 4:* There are two points that can be further studied for the problem concerned in this paper. First, if we integrate both sides of (50), it can be obtained that $V(t) \leq e^{-\omega t} V(0) + \frac{R}{\omega} +$

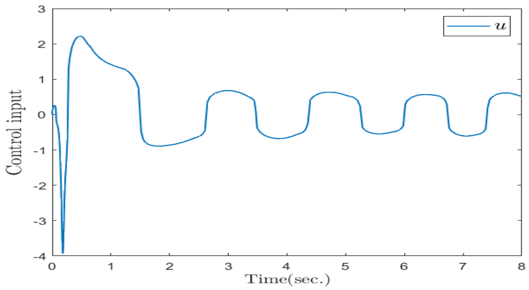


Fig. 6. Trajectory of control input $u$

$\sum_{i=1}^{2}\int_0^t e^{-\omega(t-s)}\left(b_i'\mathcal{N}(\chi_i(s))+1\right)\dot{\chi}_i(s)ds$. The upper bound of the term $\sum_{i=1}^{2}\int_0^t e^{-\omega(t-s)}(b_i'\mathcal{N}(\chi_i(s))+1)\dot{\chi}_i(s)$ $ds$ is unknown. Thus the proposed adaptive control scheme can only guarantee that the closed-loop system signals are uniformly bounded, whereas the upper bound of $V(t)$ is unknown. It is worthy of further investigation to limit the upper bound of the states. Second, It will be interesting to extend current results to more general high-order uncertain nonlinear systems.

## IV. Simulation Example

In this section, a numerical example is chosen to verify the effectiveness of the proposed control scheme. The system model is given as follows:

$$\begin{aligned}\dot{x}_1 &= \theta_1(t)^T x_1 \sin(x_1) + b_1 x_2^{\frac{7}{5}}\\ \dot{x}_2 &= \theta_2(t)^T x_1 x_2 + b_2\tilde{u}^3 + d(t)\end{aligned} \tag{52}$$

where the parameters are set as $\theta_1(t) = 0.1\sin(t)$, $\theta_2(t) = \cos(t)$, $b_1 = 1 - 0.2\sin(x_1)$, $b_2 = 1$ and $d(t) = 0.2\sin(4t)$. The attack weights are set as $\lambda_{1s}(t) = 1 + 0.2\sin(t)$, $\lambda_{2s}(t) = -1 + 0.4\cos(t)$ and $\lambda_a(t) = 0.8 + 0.2\sin(t)$. The $\mathcal{N}$ function is chosen as $\mathcal{N}(s) = e^{0.4s^2}\sin(s)$ as in [4]. The control parameters are given as $c_1 = 1$, $c_2 = 0.75$, $\gamma_1 = 0.2$, $\gamma_2 = 0.1$, $\sigma_1 = \sigma_2 = 2$. The initial value of states are set as $[x_1(0), x_2(0), \hat{\Theta}_1(0), \hat{\Theta}_2(0), \chi_1(0), \chi_2(0)]$=$[2, -1, 0, 0, 0, 0]$.

The performance of state signals under deception attacks are shown in Fig. 2 and Fig. 3. The trajectory of parameter estimates $\hat{\Theta}_i(i = 1, 2)$ is given in Fig. 4. Then the performance of designed auxiliary variables $\chi_i(i = 1, 2)$ is shown in Fig. 5. The control input $u$ is plot in Fig. 6. It is clear that all the closed-loop signals are bounded despite the occurrence of deception attacks.

## V. Conclusion

In this paper, a novel adaptive secure control method is proposed for a class of uncertain nonlinear second-order networked control systems with p-normal form under sensor and actuator deception attacks. A special class of Nussbaum function is intruduced to settle the issue that the actual sign of control coefficient of the virtual control signals designed in each recursive step may become non-identically unknown under the considered attacks. Based on the adaptive backstepping technique and the power integrator Lyapunov function theory, the closed-loop stability of the entire system can be established despite the possible occurrence of the deception attacks.

## Acknowledgment

This work was supported in part by the National Key Research and Development Program of China under Grant 2018AAA0101100 and in part by the National Natural Science Foundation of China under Grant 62022008, Grant 61973017.

## References

[1] T. Yucelen, W. M. Haddad, and E. M. Feron, “Adaptive control architectures for mitigating sensor attacks in cyber-physical systems”, *Cyber-Physical Systems*, 2: 24–52, 2016.
[2] X. Jin, W. M. Haddad, Z. Jiang, A. Kanellopoulos, and K. Vamvoudakis, “An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons”, *International Journal of Adaptive Control and Signal Processing*, 33: 1788–1802, 2019.
[3] L. An, G. Yang, “Improved adaptive resilient control against sensor and actuator attacks”, *Information Science*, 423: 145–156, 2018.
[4] X. Ren, G. Yang, “Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks”, *International Journal of Robust Nonlinear Control*, 30: 65–79, 2020.
[5] Y. Yang, J. Huang, X. Su, K. Wang, and L. Guo, “Adaptive control of second-order nonlinear systems with injection and deception attacks”, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, to be published, doi: 10.1109/TSMC.2020.3003801.
[6] Z. Jie, J. Zhao, “Resilient adaptive control of switched nonlinear cyber-physical systems under uncertain deception attacks,” *Information Science*, 543: 398–409, 2021.
[7] H. Song, P. Shi, W. Zhang, C. C. Lim, and L. Yu, “Distributed $H_\infty$ estimation in sensor networks with two-channel stochastic attacks,” *IEEE Transactions on Cybernetics*, 50(2): 465–475, 2020.
[8] D. Ding, Z. Wang, Q. Han, and G. Wei, “Security control for discretetime stochastic nonlinear systems subject to deception attacks”, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(5): 779–789, 2018.
[9] R. Gao, J. Huang and L. Wang, “Leaderless consensus control of uncertain multi-agents systems with sensor and actuator attacks”, *Information Science*, 505: 144–156, 2019.
[10] C. D. Persis, P. Tesi, “Input-to-state stabilizing control under denial-of-service”, *IEEE Transactions on Automatic Control*, 60(11): 2930–2944, 2015.
[11] L. An, G. Yang, “Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks”, *IEEE Transactions on Cybernetics*, 49(3): 827–838, 2018.
[12] R. Majumdar, P. Tabuada, *Safe and Secure Networked Control Systems under Denial-of-Service Attacks*. Berlin: Springer, 2009.
[13] M. Krstic, I. Kanellakopoulos, and P. V. Kokotovic, *Nonlinear and Adaptive Control Design*. New York: Wiley, 1995.
[14] J. Zhou, C. Wen, *Adaptive Backstepping Control of Uncertain Systems*. Berlin: Springer, 2008.
[15] W. Lin, C. Qian, “A continuous feedback approach to global strong stabilization of nonlinear systems”, *IEEE Transactions on Automatic Control*, 46(7): 1061–1079, 2001.
[16] W. Lin, C. Qian, “Adaptive control of nonlinearly parameterized systems: a nonsmooth feedback framework”, *IEEE Transactions on Automatic Control*, 47(5): 757–774, 2002.
[17] N. Duan, H. Min, “Decentralized adaptive NN state-feedback control for large-scale stochastic high-order nonlinear systems”, *Neurocomputing*, 173(3): 1412–1421, 2016.
[18] L. Hu, X. Li, “Decentralised adaptive neural connectively finite-time control for a class of p-normal form large-scale nonlinear systems”, *International Journal of Systems Science*, 50(16): 3003–3021, 2019.
[19] J. Huang, Y. Song, W. Wang, C. Wen, and G. Li, “Fully distributed adaptive consensus control of a class of high-order nonlinear systems with a directed topology and unknown control directions,” *IEEE Transactions on Cybernetics*, 48(8): 2349–2356, 2018.
[20] C. Wang, C. Wen, and L. Guo, “Multivariable adaptive control with unknown signs of the high-frequency gain matrix using novel Nussbaum functions,” *Automatica*, 111: 1–10, 2019.
[21] L. Zhang, G. Yang, “Observer-based adaptive decentralized fault-tolerant control of nonlinear large-Scale systems with sensor and actuator faults”, *IEEE Transactions on Industrial Electronics*, 62(11): 6058–6064, 2017.
[22] S. Tong, B. Huo, and Y. Li, “Observer-based adaptive decentralized fuzzy fault-tolerant control of nonlinear large-scale systems with actuator failures”, *IEEE Transactions on Fuzzy Systems*, 22(1): 1–15, 2014.