ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

Data-driven Tracking Control of Nonlinear Systems under Deception Attacks and Packet Loss

Yipeng Liu*

College of Information Engineering, Nanjing University of Finance & Economics, Nanjing, 210023, China
liuyipengyouxiang@163.com
**Corresponding author*

Abstract: *In this paper, the tracking control problem of nonlinear systems subject to deception attacks and random packet loss is investigated. Firstly, the system with an unknown model is dynamically linearized by using the pseudo partial derivative (PPD). Secondly, based on the model-free adaptive control (MFAC) approach, a data-driven controller model is designed which is solely dependent on the input/output (I/O) data, and the influence of deception attacks and packet loss is considered. Thirdly, the effectiveness of the data-driven tracking control method is demonstrated by stability analysis, the validity is confirmed by a simulation example.*

Keywords: *Data-Driven, Model-Free Adaptive Control (MFAC), Pseudo Partial Derivative (PPD), Deception Attacks, Packet Loss*

1. Introduction

In recent years, the advent of Networked Control Systems (NCSs) has revolutionized the field of control engineering by enabling the exchange of information through shared communication networks. NCS are now integral to a myriad of applications, including remote diagnostics [1], autonomous vehicles [2], and unmanned marine vessels [3]. These systems offer significant advantages such as reduced installation costs, simplified maintenance, and improved reliability.

For NCSs, obtaining accurate models of the dynamics is often challenging due to their inherent complexity. Consequently, data-driven control methods have emerged as promising solutions, where the input/output (I/O) data is used to update and adjust control signals, eliminating the need for the specific system model. As a novel data-driven method, model-free adaptive control (MFAC) offers an effective strategy for managing nonlinear systems. It possesses the capability to linearize complex, unknown dynamics through the application of pseudo partial derivatives (PPD), thereby enhancing control precision and adaptability [4]. Extensive research has been conducted on MFAC method. For example, by integrating the MFAC method with model predictive control, Hou and Lei proposed a constrained model-free adaptive predictive control approach to address the issue of urban traffic congestion [5]. Jiang and others designed an algorithm with variable output constraints based on the MFAC method, which enhanced the stability of the navigation system for unmanned surface vehicles [6].

Among the various types of cyber-attacks, deception attacks pose a unique challenge to NCSs. When deception attacks occur, the data packets exchanged between sensors and controllers are manipulated, the integrity of system information is also altered [7]. Deception attacks are not only covert but also highly destructive, which can lead to significant deviations from the desired system performance and, in severe cases, system failure. Recently, the security control problem for NCSs under deception attacks has attracted intensive research. For instance, Asadi and others introduced a data-driven control technique considering the impact of deception attacks. They conducted research on the issue of secure automatic generation control in interconnected power grids [8]. Yu and others investigated the security data-driven control problem for a class of nonlinear systems under deception attacks and false data injection attacks. They designed a controller based on the MFAC approach and analysed the system's stability [9].

In addition to cyber-attacks, packet loss is also a serious problem for NCSs, which is a common occurrence that is attributed to congestion, interference, or hardware limitations in networked

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

environments. Packet loss can disrupt the flow of information, leading to erratic system behaviour and reduced control effectiveness [10]. The design of controllers that are robust against both deception attacks and packet loss is therefore of paramount importance to ensure the safety and reliability of NCS.

In this paper, a comprehensive study on the tracking control of nonlinear systems under the dual challenges of deception attacks and packet loss is presented. By employing the MFAC strategy which dynamically linearizes the system using PPD, a controller is designed which is resilient to the adverse effects of cyber-attacks and network-induced perturbations. Furthermore, an example is simulated to prove the overall stability of the system is enhanced.

2. Problem Formulation

2.1. System Modeling

Consider a class of single input single output discrete-time nonlinear systems, which is presented as follows:

$$y(k+1) = f(y(k),\cdots,y(k-n_y),u(k),\cdots,u(k-n_u)), \tag{1}$$

where $y(k) \in \mathbb{R}$ is the system output, $u(k) \in \mathbb{R}$ is the system input, n_y and n_u are the unknown orders, $f(\cdots) \in \mathbb{R}^{n_y+n_u+2}$ is an unknown nonlinear function.

Then, the following assumptions are given:

Assumption 1: The partial derivative of $f(\cdots)$ with respect to $u(k)$ is continuous.

Assumption 2: System (1) is generalized Lipschitz, in other words, if $\Delta u(k) \neq 0$, then $|\Delta y(k+1)| \leq b|\Delta y(k)|$ holds, where $\Delta y(k+1) = y(k+1) - y(k)$, $\Delta u(k+1) = u(k+1) - u(k)$ and b is a positive constant.

Remark 1. Assumption 1 represents a standard constraint condition for general nonlinear systems in the design of control systems. Assumption 2 imposes an upper limit on the rate of change of the system's output. From the perspective of energy conservation, bounded variations in input signal will lead to bounded variations in the output signal within the system. These two assumptions are also widely applied to industrial systems, such as temperature control systems, pressure control systems, and level control systems.

Based on Assumption 1 and Assumption 2, system (1) can be dynamically linearized as below:

$$\Delta y(k+1) = \phi(k)\Delta u(k), \tag{2}$$

where $\phi(k)$ is bounded and $|\phi(k)| \leq b$.

Assumption 3: The PPD $\phi(k)$ satisfies $\phi(k) \geq b_1 > 0$ or $\phi(k) \leq -b_1 < 0$, b_1 is a constant and $b_1 > 0$. Without loss of generality, in this paper, let $\phi(k)$ satisfies $\phi(k) \geq b_1 > 0$.

In this paper, the structure of system (1) is presented in Figure 1. The network channel between the sensor and the controller is subject to deception attacks and random packet loss.

The main objective of this paper is to design a data-driven control strategy for system (1) such that the system output follows the desired output signal under deception attacks and packet loss.

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

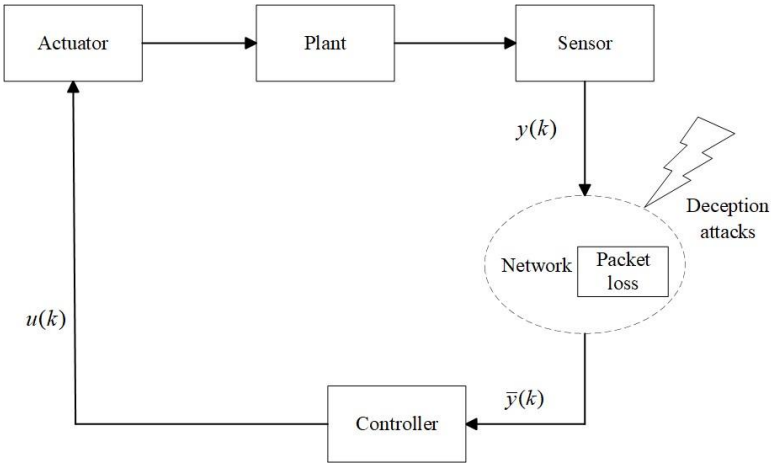

Figure 1: The framework of networked systems under deception attacks and packet loss

2.2. Deception Attacks Model

Due to the openness of communication networks, sensors may be subject to malicious cyber-attacks when transmitting data packets over networks. In this paper, consider that deception attacks occur in the channel between the sensor and the controller, then the system output $\bar{y}(k)$ under deception attacks is given as follows:

$$\bar{y}(k) = \sigma(k)\xi(k) + (1-\sigma(k))y(k), \tag{3}$$

and

$$\xi(k) = g(k)(y(k) + \omega(k)), \tag{4}$$

where $\xi(k)$ is the deception signal, $g(k)$ is the multiplicative attack coefficient and $\omega(k)$ is the additive attack coefficient. The mathematical expectations of the two coefficients satisfy $E\{g(k)\} = \bar{g}$ and $E\{\omega(k)\} = \bar{\omega}$, $\bar{g} \in (0,1)$, $\bar{\omega} \in (0,1)$. $\sigma(k)$ is a function used to describe whether deception attacks have occurred, and it follows a Bernoulli distribution:

$$\begin{cases} P\{\sigma(k) = 1\} = \bar{\sigma}, \\ P\{\sigma(k) = 0\} = 1 - \bar{\sigma}, \end{cases} \tag{5}$$

specially, $\bar{\sigma}$ represents the probability of deception attacks occurring, $\bar{\sigma} \in [0,1]$.

2.3. Design of the Controller under Deception Attacks and Packet Loss

In this paper, the dynamic linearization approach can be used on the basis of the PPD parameter $\phi(k)$. However, it is difficult to get the exact value of $\phi(k)$ since all nonlinear factors about system (1) are concentrated to the PPD parameter. Therefore, $\hat{\phi}(k)$ is employed to estimate the value of $\phi(k)$, the following formula is obtained:

$$\hat{\phi}(k) = \hat{\phi}(k-1) + \frac{\eta \Delta u(k-1)}{\mu + \Delta u(k-1)^2}(\Delta y(k) - \hat{\phi}(k-1)\Delta u(k-1)), \tag{6}$$

where η represents the step size factor, $\mu > 0$ is a weighting factor, $\eta \in (0,1)$.

In order to design the controller for system (1) which is only influenced by I/O data, the following formula is obtained:

$$u(k) = u(k-1) + \frac{\rho\phi(k)}{\lambda + \phi(k)^2}(y^*(k+1) - y(k)), \tag{7}$$

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

where $y^*(k+1)$ is the desired output signal at time $(k+1)$, $\lambda > 0$ is a weighting factor, ρ represents the step size factor, $\rho \in (0,1)$.

Moreover, $\beta(k)$ is defined as the packet loss signal with a value of 0 or 1, that is, $\beta(k) \in \{0,1\}$. If $\beta(k) = 1$, then the system is not influenced by packet loss at time k; if $\beta(k) = 0$,then packet loss occurs on the channel between the sensor and the controller at time k, the signal of the controller cannot be updated normally.

The mathematical expectation of $\beta(k)$ is $E\{\beta(k)\} = \bar{\beta}$, where $\bar{\beta} \in [0,1]$ is the probability that no packet loss has occurred.

Therefore, under the influence of deception attacks and packet loss, the data-driven controller model is represented as follows:

$$\hat{\phi}(k) = \hat{\phi}(k-1) + \frac{\eta\beta(k)\Delta u(k-1)}{\mu + \Delta u(k-1)^2}(\Delta\bar{y}(k) - \hat{\phi}(k-1)\Delta u(k-1)), \tag{8}$$

$$\hat{\phi}(k) = \hat{\phi}(1),\ \left|\hat{\phi}(k)\right| \le \varepsilon \text{ or } \left|\Delta u(k-1)\right| \le \varepsilon, \tag{9}$$

$$u(k) = u(k-1) + \frac{\rho\hat{\phi}(k)}{\lambda + \hat{\phi}(k)^2}(y^*(k+1) - y(k)), \tag{10}$$

where the reset mechanism (9) for $\hat{\phi}(k)$ is established to enable the expression of the estimated PPD value in equation (8). Then the tracking ability of the parameter estimation method is strengthened.

3. Main Results

In this section, the main results of the research in this paper is presented, the boundedness of PPD estimation and tracking error is demonstrated.

Define $e(k)$ as the tracking error at time k, the expression is given as follows:

$$e(k) = y^*(k) - y(k). \tag{11}$$

Theorem 1: Based on Assumptions 1-3, for system (1) under deception attacks and packet loss, the PPD estimation $\hat{\phi}(k)$ is bounded.

Proof: According to equation (9), if $\left|\hat{\phi}(k)\right| \le \varepsilon$ or $\left|\Delta u(k-1)\right| \le \varepsilon$, then $\hat{\phi}(k) = \hat{\phi}(1)$, it is obvious that $\hat{\phi}(k)$ is bounded.

In other cases, define $\tilde{\phi}(k) = \hat{\phi}(k) - \phi(k)$ as the estimation error of the PPD parameter.

Calculate the mathematical expectation for the output $\bar{y}(k)$ after being attacked. Since the attack coefficients $g(k)$, $\omega(k)$, and the deception attack signal $\xi(k)$ are independent of $y(k)$, it can be obtained that

$$\begin{aligned} E\{\bar{y}(k)\} &= E\{\sigma(k)\xi(k) + (1-\sigma(k))y(k)\} \\ &= E\{\sigma(k)g(k)(y(k) + \omega(k)) + (1-\sigma(k))y(k)\} \\ &= E\{(\sigma(k)g(k) + 1 - \sigma(k))y(k) + \sigma(k)g(k)\omega(k)\} \\ &= (\bar{\sigma}(\bar{g} - 1) + 1)E\{y(k)\} + \bar{\sigma}\bar{g}\bar{\omega}, \end{aligned} \tag{12}$$

define $\Delta\bar{y}(k) = \bar{y}(k) - \bar{y}(k-1)$, combine equation (12) and calculate the mathematical

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

expectation for $\Delta\bar{y}(k)$, one has

$$\begin{aligned} E\{\Delta\bar{y}(k)\} &= E\{\sigma(k)\xi(k)+(1-\sigma(k))y(k) \\ &\quad -\sigma(k-1)\xi(k-1)-(1-\sigma(k-1))y(k-1)\} \\ &= (\bar{\sigma}(\bar{g}-1)+1)E\{y(k)\}-(\bar{\sigma}(\bar{g}-1)+1)E\{y(k-1)\} \\ &= (\bar{\sigma}(\bar{g}-1)+1)E\{\Delta y(k)\}. \end{aligned} \tag{13}$$

Subtract $\phi(k)$ from both sides of the equal sign in equation (8), one obtains

$$\begin{aligned} \bar{\phi}(k) &= \hat{\phi}(k-1)+\frac{\eta\beta(k)\Delta u(k-1)}{\mu+\Delta u(k-1)^2}(\Delta\bar{y}(k)-\hat{\phi}(k-1)\Delta u(k-1))-\phi(k) \\ &= \bar{\phi}(k-1)-\Delta\phi(k)+\frac{\eta\beta(k)\Delta u(k-1)}{\mu+\Delta u(k-1)^2}(\Delta\bar{y}(k)-\hat{\phi}(k-1)\Delta u(k-1)), \end{aligned} \tag{14}$$

calculate the mathematical expectation of $\bar{\phi}(k)$, it can be derived that

$$\begin{aligned} E\{\bar{\phi}(k)\} &= E\{\bar{\phi}(k-1)\}-E\{\Delta\phi(k)\}+E\{\frac{\eta\beta(k)\Delta u(k-1)}{\mu+\Delta u(k-1)^2}(\Delta\bar{y}(k) \\ &\quad -(\bar{\phi}(k-1)+\phi(k-1))\Delta u(k-1))\} \\ &= E\{\bar{\phi}(k-1)\}-E\{\Delta\phi(k)\}-E\{\frac{\eta\beta(k)\bar{\phi}(k-1)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\} \\ &\quad +E\{\frac{\eta\beta(k)\Delta u(k-1)}{\mu+\Delta u(k-1)^2}(\Delta\bar{y}(k)-\phi(k-1)\Delta u(k-1))\} \\ &= E\{\bar{\phi}(k-1)\}-E\{\Delta\phi(k)\}-E\{\frac{\eta\beta(k)\bar{\phi}(k-1)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\} \\ &\quad +E\{\frac{\eta\beta(k)\Delta u(k-1)}{\mu+\Delta u(k-1)^2}\}((\bar{\sigma}(\bar{g}-1)+1)E\{\Delta y(k)\}-E\{\Delta y(k)\}) \\ &= E\{\bar{\phi}(k-1)\}-E\{\Delta\phi(k)\}-E\{\frac{\eta\beta(k)\bar{\phi}(k-1)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\} \\ &\quad +\bar{\sigma}(\bar{g}-1)E\{\frac{\eta\beta(k)\phi(k-1)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\} \\ &= E\{(1-\frac{\eta\beta(k)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2})\}E\{\bar{\phi}(k-1)\} \\ &\quad +\bar{\sigma}(\bar{g}-1)E\{\frac{\eta\beta(k)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\}E\{\phi(k-1)\}-E\{\Delta\phi(k)\}, \end{aligned} \tag{15}$$

for $\mu>0$, $\eta\in(0,1)$, one has

$$\eta\Delta u(k-1)^2<\Delta u(k-1)^2<\mu+\Delta u(k-1)^2,$$

then there exists $a_1\in(0,1)$, $a_2\in(0,1)$, so that the following inequality holds:

$$0<a_1\le\frac{\eta\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\le a_2<1. \tag{16}$$

Combine equation (15) and (16), it can be obtained that

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

$$\begin{aligned}E\{|\bar{\phi}(k)|\} &\le E\{\left|1-\frac{\eta\beta(k)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\right|\}E\{|\bar{\phi}(k-1)|\}+|\bar{\sigma}(\bar{g}-1)| \\ &\times E\{\left|\frac{\eta\beta(k)\Delta u(k-1)^2}{\mu+\Delta u(k-1)^2}\right|\}E\{|\phi(k-1)|\}+E\{|\Delta\phi(k)|\} \\ &\le E\{|1-a_1\beta(k)|\}E\{|\bar{\phi}(k-1)|\}+|\bar{\sigma}(\bar{g}-1)| \\ &\times E\{|a_2\beta(k)|\}E\{|\phi(k-1)|\}+E\{|\Delta\phi(k)|\} \\ &\le |1-a_1\bar{\beta}|E\{|\bar{\phi}(k-1)|\}+|a_2\bar{\beta}\bar{\sigma}(\bar{g}-1)|E\{|\phi(k-1)|\} \\ &+E\{|\Delta\phi(k)|\} \\ &\le |1-a_1\bar{\beta}|E\{|\bar{\phi}(k-1)|\}+|a_2b\bar{\beta}\bar{\sigma}(\bar{g}-1)|+|2b|,\end{aligned} \tag{17}$$

define $d_1=1-a_1\bar{\beta}$, $d_2=a_2b\bar{\beta}\bar{\sigma}(\bar{g}-1)+2b=b(2+a_2\bar{\beta}\bar{\sigma}(\bar{g}-1))$, $d_1\in(0,1)$, $d_2>0$, then inequality (17) can be transformed as

$$\begin{aligned}E\{|\bar{\phi}(k)|\} &\le d_1E\{|\bar{\phi}(k-1)|\}+d_2 \\ &\le d_1{}^2E\{|\bar{\phi}(k-2)|\}+d_1d_2+d_2 \\ &\le \cdots \\ &\le d_1{}^{k-1}E\{\bar{\phi}(1)\}+\frac{d_2}{1-d_1},\end{aligned} \tag{18}$$

from inequality (18), $E\{\bar{\phi}(k)\}$ is bounded, then $\bar{\phi}(k)$ is bounded.

Since $\bar{\phi}(k)=\hat{\phi}(k)-\phi(k)$ and $\phi(k)$ is bounded, then $\hat{\phi}(k)$ is bounded, the proof of Theorem 1 is completed.

Theorem 2: For system (1) under deception attacks and packet loss, if Theorem 1 is satisfied, if $y^*(k+1)=y^*$, y^* is a constant, $\bar{\beta}\neq 0$, $\lambda>\frac{b^2}{4}$, then the tracking error $e(k)$ is bounded.

Proof: First, define $h(x)=\frac{x}{\lambda+x^2}$, $x>0$. Since $\lambda>0$, if $x\ge\sqrt{\lambda}$, $h(x)$ is monotonically decreasing, if $0<x<\sqrt{\lambda}$, $h(k)$ is monotonically increasing. From Theorem 1, $\hat{\phi}(k)$ is bounded, assume $0<\varepsilon\le\hat{\phi}(k)\le\hat{b}$, then $h(\hat{\phi}(k))_{\min}=\min\left\{h(\varepsilon),h(\hat{b})\right\}$.

Define $\Phi(k)=\phi(k)h(\hat{\phi}(k))=\frac{\phi(k)\hat{\phi}(k)}{\lambda+\hat{\phi}(k)^2}$, from Assumption 3, $0<b_1\le\phi(k)\le b$, then one has

$$0<b_1\min\left\{h(\varepsilon),h(\hat{b})\right\}\le\Phi(k)\le\frac{b\hat{\phi}(k)}{2\sqrt{\lambda}\hat{\phi}(k)}=\frac{b}{2\sqrt{\lambda}}.$$

Define $\Phi_1=b_1\min\left\{h(\varepsilon),h(\hat{b})\right\}$, $\Phi_2=\frac{b}{2\sqrt{\lambda}}$, it can be derived that

$$0<\Phi_1\le\Phi(k)\le\Phi_2, \tag{19}$$

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

if $\lambda > \frac{b^2}{4}$, $\Phi_2 = \frac{b}{2\sqrt{\lambda}} < 1$, the inequality (19) can be transformed as

$$0 < \Phi_1 \le \Phi(k) \le \Phi_2 < 1. \tag{20}$$

Then, define $\bar{e}(k) = y^*(k) - \bar{y}(k)$ as the error between the expected output signal at time k and the system output after being attacked. Since $y^*(k+1) = y^*$, it can be obtained that

$$\begin{aligned}
\bar{e}(k) &= y^* - \bar{y}(k) \\
&= y^* - (\sigma(k)\xi(k) + (1-\sigma(k))y(k)) \\
&= y^* - \sigma(k)g(k)(y(k) + \omega(k)) - (1-\sigma(k))y(k) \\
&= y^* - (1+\sigma(k)(g(k)-1))y(k) - \sigma(k)g(k)\omega(k) \\
&= (1+\sigma(k)(g(k)-1))y^* - (1+\sigma(k)(g(k)-1))y(k) \\
&\quad -\sigma(k)(g(k)-1)y^* - \sigma(k)g(k)\omega(k) \\
&= (1+\sigma(k)(g(k)-1))e(k) - \sigma(k)(g(k)-1)y^* \\
&\quad -\sigma(k)g(k)\omega(k),
\end{aligned} \tag{21}$$

combine equation (11) and (21), the tracking error at time $(k+1)$ can be obtained as below:

$$\begin{aligned}
e(k+1) &= y^* - y(k+1) \\
&= y^* - y(k) - \Delta y(k+1) \\
&= e(k) - \phi(k)\Delta u(k) \\
&= e(k) - \frac{\rho\beta(k)\phi(k)\hat{\phi}(k)}{\lambda + \hat{\phi}(k)^2}(y^* - \bar{y}(k)) \\
&= e(k) - \rho\beta(k)\Phi(k)((1+\sigma(k)(g(k)-1))e(k) \\
&\quad -\sigma(k)(g(k)-1)y^* - \sigma(k)g(k)\omega(k)) \\
&= (1-\rho\beta(k)\Phi(k)((1+\sigma(k)(g(k)-1)))e(k) \\
&\quad +\rho\beta(k)\Phi(k)\sigma(k)(g(k)-1)y^* + \rho\beta(k)\Phi(k)\sigma(k)g(k)\omega(k),
\end{aligned} \tag{22}$$

Consider $0 < \Phi(k) < 1$, take the absolute value of $e(k+1)$:

$$\begin{aligned}
|e(k+1)| &\le |1-\rho\beta(k)\Phi(k)((1+\sigma(k)(g(k)-1))||e(k)| \\
&\quad +|\rho\beta(k)\Phi(k)\sigma(k)(g(k)-1)y^*| + |\rho\beta(k)\Phi(k)\sigma(k)g(k)\omega(k)| \\
&\le |1-\rho\beta(k)((1+\sigma(k)(g(k)-1))||e(k)| \\
&\quad +|\rho\beta(k)\sigma(k)(g(k)-1)y^*| + |\rho\beta(k)\sigma(k)g(k)\omega(k)|,
\end{aligned} \tag{23}$$

then, one has

$$\begin{aligned}
E\{|e(k+1)|\} &\le |1-\rho\bar{\beta}((1+\bar{\sigma}(\bar{g}-1))|\, E\{|e(k)|\} \\
&\quad +|\rho\bar{\beta}\bar{\sigma}(\bar{g}-1)y^*| + |\rho\bar{\beta}\bar{\sigma}\bar{g}\bar{\omega}|.
\end{aligned} \tag{24}$$

Since $\bar{\sigma} \in [0,1]$, $\bar{g} \in (0,1)$, then $0 < 1+\bar{\sigma}(\bar{g}-1) < 1$. According to $\rho \in (0,1)$, $\bar{\beta} \in (0,1]$, it can be derived that $|1-\rho\bar{\beta}(1+\bar{\sigma}(\bar{g}-1))| \le 1-\rho\bar{\beta}(1+\bar{\sigma}(\bar{g}-1)) < 1$.

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

Define $m_1 = 1-\rho\bar{\beta}(1+\bar{\sigma}(\bar{g}-1))$, $m_1 \in (0,1)$, $m_2 = \left|\rho\bar{\beta}\bar{\sigma}(\bar{g}-1)y^*\right| + \left|\rho\bar{\beta}\bar{\sigma}\bar{g}\bar{\omega}\right|$, from inequality (24) one obtains

$$\begin{aligned} E\{|e(k+1)|\} &\le m_1 E\{|e(k)|\} + m_2 \\ &\le m_1^2 E\{|e(k-1)|\} + m_1 m_2 + m_2 \\ &\le \cdots \\ &\le m_1^k E\{|e(1)|\} + \frac{m_2}{1-m_1}, \end{aligned} \tag{25}$$

therefore, $E\{e(k)\}$ is bounded, then $e(k)$ is bounded. This completes the proof of Theorem 2.

4. Simulation Example

This section verifies the effectiveness of the control strategy through a simulation example. Consider a class of nonlinear discrete systems:

$$y(k+1) = \frac{(y(k)+0.1)u(k)}{(1+y(k)^2)+0.5u(k)^3}$$

In this simulation example, the dynamic above is only utilized to generate the I/O data rather than the specific model in the MFAC approach.

The desired output is presented as:

$$y^*(k) = \begin{cases} 1 & 0<k\le 200 \\ -1 & 200<k\le 400 \\ 1 & 400<k\le 600 \\ -1 & 600<k\le 800 \end{cases}$$

The initial values of the system are set as: $u(1)=0$, $y(1)=-1$, $\hat{\phi}(1)=2$. The system parameters selected as: $\varepsilon=0.05$, $\eta=0.5$, $\mu=1$, $\rho=0.5$, $\lambda=3$, $\bar{\sigma}=0.5$. $g(k)=1+0.1*(rand(1)-0.5)$, $\omega(k)=0.1*(rand(1)-0.5)$. Then the simulation results are shown in the following figures.

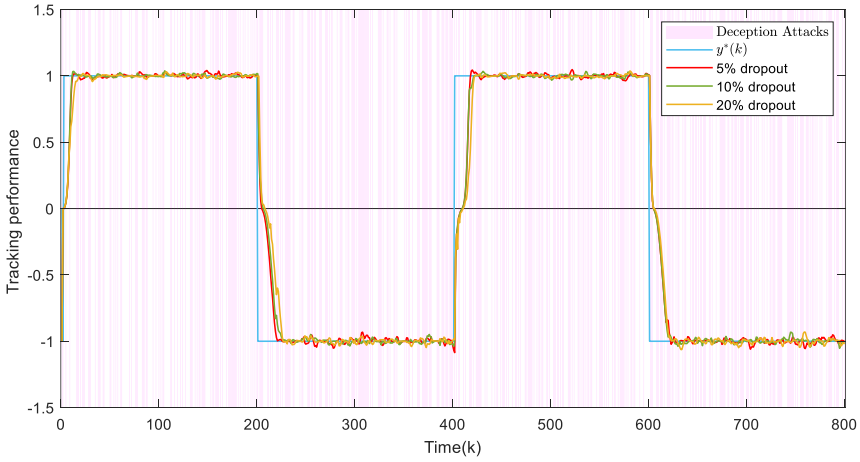

Figure 2: Tracking performance at different packet loss rates

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

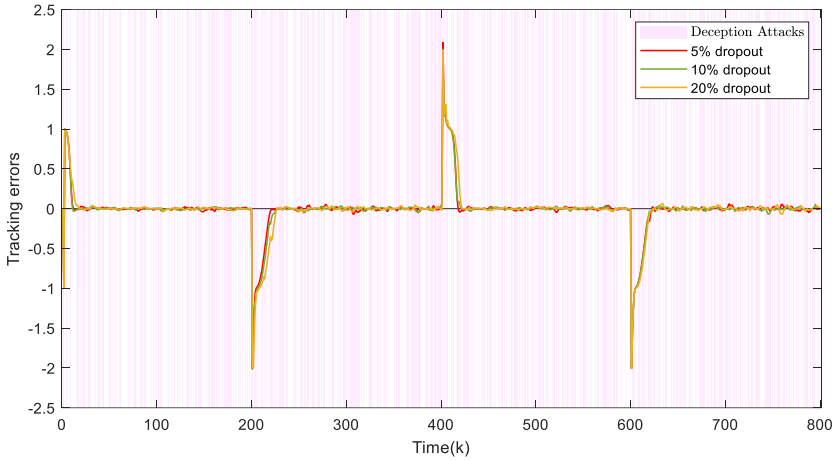

Figure 3: Tracking errors at different packet loss rates

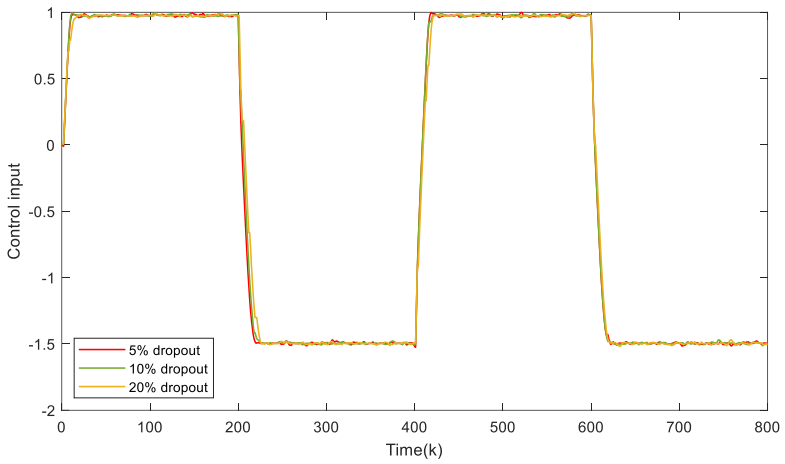

Figure 4: Input signals at different packet loss rates

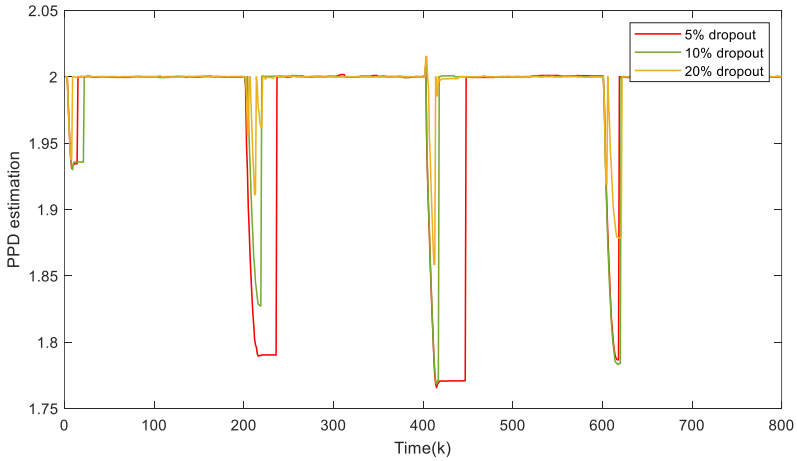

Figure 5: PPD estimations at different packet loss rates

Figure 2 shows the comparison between the system output and the desired output when the packet loss rate is 5%, 15%, and 30%, respectively. Figure 3 shows the tracking errors at different packet loss rates. The pink rectangles indicate that deception attack have occurred. It can be observed that deception attacks and packet loss lead to fluctuations and deviations in the system output curve, by using the MFAC method, the output trajectory gradually coincides with the desired trajectory. In addition, with different packet loss probabilities, the larger the packet loss probability is, the slower the system output reaches the desired tracking trajectory, and the slower the tracking error converges to 0. However, regardless of the value of the packet loss rate, the system can be stabilized gradually under the influence of deception attacks and packet loss.

ISSN 2616-5775 Vol. 7, Issue 5: 180-189, DOI: 10.25236/AJCIS.2024.070524

As presented in Figure 4, in the case that the desired output is stable, the control inputs of the system converge gradually with the advance of time. Moreover, the larger the packet loss rate is, the slower the convergence speed is. Figure 5 shows the curves of the PPD estimations under different packet loss rates, which reflects the boundedness of the PPD parameter estimation values.

The above simulation example demonstrates the effectiveness of the MFAC tracking control strategy, which ultimately enables the system to achieve the desired tracking performance under deception attacks and packet loss.

5. Conclusions

In this paper, the tracking control problem for nonlinear systems is investigated by utilizing the MFAC approach. Firstly, the system with unknown model is dynamically linearized by using PPD parameters. Secondly, a data-driven controller model is designed under the influence of deception attacks and packet loss, which is only related to I/O data. Then, the effectiveness of the data-driven tracking control method is demonstrated by stability analysis. Finally, a simulation example is provided to testify the validity of the MFAC approach.

References

[1] Z.-H. Pang, C. -D. Bai, S. Liu, Q. -L. Han and X. -M. Zang. A novel networked predictive control method for systems with random communication constraints [J]. Journal of Systems Science and Complexity, 2021, 34: 1364-1378.

[2] S. Liu, Z. -S. Hou, T. Tian, Z. Deng and Z. Li. A novel dual successive projection-based model-free adaptive control method and application to an autonomous Car [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 30(11):3444-3457.

[3] Y. Liao, Q. Jiang, T. Du and W. Jiang. Redefined output model-free adaptive control method and unmanned surface vehicle heading control [J]. IEEE Journal of Oceanic Engineering, 2020, 45(3):714-723.

[4] X. Liu, L. Qiu, Y. Fang and J. Rodríguez. Predictor-based data-driven model-free adaptive predictive control of power converters using machine learning [J]. IEEE Transactions on Industrial Electronics, 2023, 70(8):7591-7603.

[5] Z. -S. Hou and T. Lei. Constrained model free adaptive predictive perimeter control and route guidance for multi-region urban traffic systems [J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(2): 912-924.

[6] Q. Jiang, Y. Liao, Y. Li, J. Fan and Y. Miao. Heading control of unmanned surface vehicle with variable output constraint model-free adaptive control algorithm [J]. IEEE Access, 2019, 7: 131008-131018.

[7] N. Yang, R. Gao, Y. Feng and H. Su. Event-triggered impulsive control for complex networks under stochastic deception attacks [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 1525-1534.

[8] Y. Asadi, M. M. Farsangi, A. M. Amani, E. Bijami and H. H. Alhelou. Data-driven automatic generation control of interconnected power grids subject to deception attacks [J]. IEEE Internet of Things Journal, 2023, 10(9): 7591-7600.

[9] W. Yu, X. Bu and Z. -S. Hou. Security data-driven control for nonlinear systems subject to deception and false data injection attacks [J]. IEEE Transactions on Network Science and Engineering, 2022, 9(4): 2910-2921.

[10] J. Chen, C. Hua and X. Guan. Iterative learning model-free control for networked systems with dual-direction data dropouts and actuator faults [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(11): 5232-5240.