International Journal Of
Industrial Electronics Control and Optimization
Print ISSN: 3517-2645
Online ISSN: 3568-2645
Homepage: https://ieco.usb.ac.ir/

Adaptive Resilient Control of Uncertain Nonlinear Cyber-physical Systems under Deception Attack

Maryam Shahriari-kahkeshi | Seyed Hojat Nourian

Department of Electrical Engineering, Faculty of Engineering, Shahrekord University, Shahrekord, Iran.
Corresponding Author's email: m.shahriyarikahkeshi@alumni.iut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: **********
Received in revised form: **********
Accepted: **********
Published online: **********

Keywords: Deception attack, False data injection attack, Nonlinear cyber-physical systems, Resilient control.

ABSTRACT

This work proposes an adaptive resilient control for uncertain nonlinear cyber-physical systems (CPSs) under deception attacks. It is assumed that attacker injects false data into the commands exchanged between the controller and actuator over the communication channels. The injected false data affects the control input in both additive and multiplicative forms. To deal with the uncertain dynamics of the system and additive term of cyber-attacks, the radial basis function-neural networks (RBF-NNs) are invoked. Also, to handle adverse effects of multiplicative term of cyber-attack, the Nussbaum-type gain function is employed. Then, by integrating the RBF-NN model and Nussbaum function into the command filtered backstepping (CFB) approach, the proposed resilient control scheme is designed. Compared with the existing works, the proposed control eliminates the "explosion of complexity" problem in the conventional backstepping approach, removes the trial and error in choosing time constant of the first order filters in the dynamics surface control (DSC) approach, compensates the filtering error and deals with both additive and multiplicative cyber-attacks in "controller to actuator" channel, simultaneously. Also, it mitigates the effects of the cyber-attack without requiring separate attack estimation unit, controller reconfiguration or readjustment algorithm. Simulation results on the robotic arm under different cyber-attacks verify effective resilient performance of the proposed control scheme.

I. Introduction

Cyber-physical systems integrate physical systems into the cyber space via network of communication channels [1, 2]. Such systems which typically include processing and computing units are able to monitor and control physical systems through communication networks and have found wide applications in different science and engineering fields like aerospace, smart grids, power systems, industrial processes, and etc. [3-6]. Most of the CPSs use open communication and computation platform and they are often vulnerable to various cyber-attacks.

Daniel of service (DoS) attack and deception attack are common types of cyber-attacks that affect the CPSs and deteriorate the system performance [7, 8]. The DoS attack is a cyber-attack in which adversaries block the communication channels between different system layers and prevent signal transmission. Depending on the place of DoS attack occurrence, control layer may not receive sensor measurements or actuator may not receive control inputs. Therefore, control system fails due to the lack of real-time data. A typical form of the deception attack is a false data injection (FDI) attack in which attackers penetrate the communication network and directly, inject false signals to manipulate the actual control inputs or sensor measurements. Generally, FDI attacks may occur at the communication channels transmitting "sensor measurements to the control unit" or transmitting "control commands to the actuators". As a result of FDI attack, control units or physical layers receive false data instead of the true one. Hence, to preserve the desired performance of the control system, it is necessary to deal with cyber-attacks carefully.

Mostly, existing researches on security of the CPSs in the presence of cyber-attacks focus on two subjects: (1) attack detection, and (2) resilient control design [9-11].

The first subject models cyber-attack as a conflict signal injecting to the network, then studies attack effects and concentrates on developing attack detection and identification schemes to detect system anomalies. Generally speaking, attack detection schemes can be divided into model-based and data-based approaches. The model-based schemes use analytical model of the system for attack detection while the other ones infer system model by using historical data of the system and detect attack occurrence by analyzing the available data [12-14].

The second subject tries to develop resilient control schemes to mitigate attack effects. Generally, there are two perspectives to design resilient control schemes named as active and passive. The active approach extracts attack information by detecting, estimating or identifying it via separate attack identification unit, and then mitigates attack effects based on the attack characteristics [15-20]. In contrast, the passive approach assumes that adversary attack is a bounded signal and tries to compensate its adverse effects without identifying and readjusting or reconfiguring controller after attack occurrence [21-27]. In passive approach, controller is designed to be resilient against predefined attacks. As it is inferred from above discussion, designing active attack mitigation scheme is more complicated than the passive one because it requires attack detection, and estimation unit as well as controller readjustment algorithm.

In [15], an active attack mitigation strategy based on the attack detection and reconstruction scheme was proposed for nonlinear CPSs under deception attack. It designs diagnostic observer for detecting and estimating occurred attack online and then mitigates attack effects by using the output of the attack diagnostic unit. In [16] attack mitigation scheme was proposed for nonlinear CPSs in the companion form under actuator deception attack based on the neural estimation of the occurred attack and sliding mode approach. In [17] resilient consensus scheme based on the attack detection and isolation approach was proposed for nonlinear second order multi-agent systems under FDI attack in communication channels between the follower agents. It first, detects the agent that receives false data, then by scanning all links ended to the detected agents, it identifies the under attack link. Finally, by eliminating the under attack link from the consensus algorithm, the attack mitigation is done. In [18] linear networked control systems under FDI attack and process noise were considered and then an active attack mitigation scheme was proposed. An attack mitigation scheme based on the adaptive sliding mode approach and attack estimation was proposed for linear CPSs in the presence of FDI actuator attack in [20].

In [6] consensus of cyber-physical power systems in presence of model uncertainties, disturbances and cyber-attacks has been considered. The considered system in [20] is a fractional order linear time-invariant one, and the considered cyber-attack is a time-dependent bounded function. The passive resilient scheme proposed in [6] designs an adaptive chattering-free fractional order sliding mode controller to achieve consensus in presence of uncertainties, disturbances and cyber-attacks. An adaptive neural network-based DSC scheme was proposed for uncertain nonlinear time-delay CPSs under sensor and actuator deception attack in [21]. In [22] passive resilient control of nonlinear CPSs in the canonical form under actuator attack and input saturation was investigated. The proposed scheme in [22] is based on the Nussbaum function, barrier Lyapunov function and extended state observer and it assumes that system model is exactly known. Adaptive backstepping-based resilient control of nonlinear CPSs in the presence of deception and injection attack was studied in [23, 24]. The considered CPSs in [23, 24] has special form known as linearly parameterized strict-feedback form with bounded control gains, also it assumes that attack signal satisfies special inequalities which limit applicability of the proposed schemes for handling general form of attacks. Two other passive resilient control schemes for nonlinear CPSs under FDI attack were proposed in [25, 26]. In [27], a fixed-time adaptive resilient control framework based on the reinforcement learning, disturbance observer and nonsingular fast terminal sliding mode was proposed for nonlinear CPSs under FDI attack. In [28], a reinforcement learning-based optimal resilient control was proposed for large scale interconnected nonlinear systems in the presence of sensor attack and actuator hysteresis. Also, some model free resilient control schemes were proposed for nonlinear CPSs in [29-31]. In [32], a leader-follower formation control based on the neural networks, projection algorithm and DSC approach was proposed for an uncertain unmanned surface vehicle under stochastic disturbance. In [33], an adaptive backstepping sliding mode control was proposed to stabilize nonlinear multi-input multi-output epidemic systems under input saturation, modeling uncertainties and external disturbances.

Inspired by the above discussion, this paper solves the control problem in nonlinear uncertain CPSs under FDI attack in “controller to actuator” communication channel. An adaptive resilient control scheme based on the RBF-NN, Nussbaum function and CFB approach is proposed to deal with the modeling uncertainty, and to mitigate the attack effects as well as unknown control direction problem arisen because of actuator multiplicative attack. The suggested scheme does not require any prior information about attack time, severity and characteristic. Also, it does not require attack detection and identification unit, and

controller reconfiguration mechanism for mitigating attack effects online. In addition it is able to mitigate different kind of additive and multiplicative attacks as well as constant, time-varying and stochastic ones. Stability analysis shows that the proposed resilient scheme ensures stability of the CPSs under input attack and guarantees that by proper selection of the design parameters, tracking error can be made small.

Thorough comparison among the prior reviewed works and the proposed scheme has been provided in Table 1. In this Table, the reviewed references on passive resilient control of nonlinear CPSs and the proposed work were compared with each other, from four different aspects including: (1) considered nonlinear CPS form, (2) attack location, (3) control approach, and (4) limitations of the schemes.

Main contributions of the proposed work are: (1) Compared with the existing works [22-25], the proposed work considers a more general class of nonlinear CPSs, therefore, it is applicable to wide variety of practical systems like those described later in remark 2. (2) The proposed resilient control scheme-based on the CFB approach eliminates the "explosion of complexity" problem which is conventional in the backstepping-based approaches suggested in [23, 24, 26, 27, 33]. (3) The proposed scheme uses a compensation mechanism to eliminate the filtering error. Also, it uses a command filter to obtain derivatives of the virtual input and therefore, it eliminates sensitivity to the time-constant of the first order filters in the DSC-based approaches, unlike [21, 32]. (4) Compared with [21, 22, and 25], the proposed scheme not only deals with additive attacks, but also can handle the multiplicative attacks that multiply the control gain by an unknown term, alter the magnitude and effectiveness of the control input and cause more significant changes than the additive attacks. However the proposed approach provides a simple controller with considerable advantages, it only deals with actuator attack and it is not applicable for CPSs with unsafe "sensor to controller" communication channel.

Note: Throughout the paper, scalars are represented in italics; while the vectors are denoted in bold and italics.

II. Problem Statement and Preliminaries

This section first presents problem statement and then describes some preliminaries.

A. Problem Statement

The following class of uncertain nonlinear CPSs under deception attack represented in Fig. 1 is considered:

$$\begin{aligned} \dot{x}_i &= x_{i+1} + f_i(\boldsymbol{x}_i), \quad 1 \le i \le n-1 \\ \dot{x}_n &= f_n(\boldsymbol{x}) + u, \\ y &= x_1, \end{aligned} \tag{1}$$

where $x_i \in \Re$ is the state variable, $\boldsymbol{x} = [x_1 \ \ldots \ x_n] \in \Re^n$ and $\boldsymbol{x}_i = [x_1 \ \ldots \ x_i] \in \Re^i$ represent the state vectors, $u \in \Re$ is the control input and $y \in \Re$ is the output variable. Also, $f_i(\boldsymbol{x}_i)$ for $i = 1, 2, ..., n$ represents the uncertain smooth functions in the system model. The model of deception attack affecting the control signal is described by

$$u = b v_n + a(\boldsymbol{x}), \tag{2}$$

where v_n is the controller output, b describes multiplicative attack signal which is unknown constant,

TABALE I COMPARISON BETWEEN THE PROPOSED SCHEME AND RELATED PASSIVE RESILIENT METHODS

Ref. No.	Considered CPS	Attack location	Control approach	Limitations
[21]	Time-delay nonlinear CPS	Sensor and actuator deception attack	Dynamic surface control approach	(1) Existence of filtering error, and (2) sensitivity to time constant of the first order filters
[22]	*n*th order affine nonlinear CPS	Actuator attack	Adaptive control	(1) Applicable to simple form of nonlinear CPSs, and (2) ability to deal with simple additive actuator attack
[23, 24]	linearly parameterized nonlinear CPS	Sensor and actuator attack	Backstepping approach	(1) Explosion of complexity problem, and (2) applicable to linearly parameterized form of CPSs.
[25]	*n*th order affine nonlinear CPS	Sensor and actuator attack	Feedback linearization approach	(1) Applicable to simple form of nonlinear CPSs, and (2) only deals with additive attack.
[26]	Nonlinear strict-feedback CPS	Sensor attack	Backstepping approach	(1) Explosion of complexity problem, and (2) dealing with sensor attack.
[27]	Large scale nonlinear systems	Sensor attack	Reinforcement-based adaptive backstepping control	(1) Explosion of complexity problem, and (2) dealing with sensor attack.
Proposed Scheme	Nonlinear CPS in the strict-feedback form	Actuator attack	Command filtered backstepping approach	(1) Dealing with actuator attack.

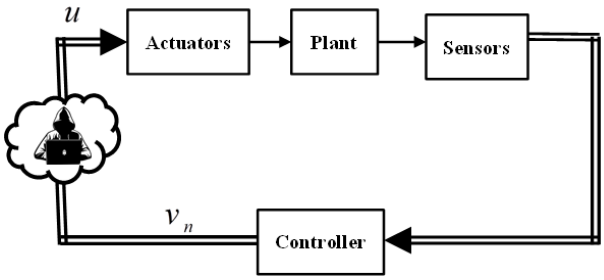

Fig. 1. Schematic of the under attack CPS.

$a(\boldsymbol{x})$ represents the injected attack signal which is unknown bounded state-dependent function, and u denotes the under-attack signal that is send to the actuator through the network.

Substituting the attack signal (2) in (1), results in

$$\begin{aligned} \dot{x}_i &= x_{i+1} + f_i(\boldsymbol{x}_i), \quad 1 \le i \le n-1 \\ \dot{x}_n &= f_n(\boldsymbol{x}_n) + bv_n + a(\boldsymbol{x}), \\ y &= x_1. \end{aligned} \tag{3}$$

Remark 1. It is worth to note that the occurrence time, severity, and characteristic of the attack signal is unknown for controller design.

Remark 2. Wide variety of practical systems such as the jet engine compression system [34], the twin otter aircraft [35], the robot manipulator [36], and the piezoelectric-positioning mechanism [37] can be described by the nonlinear system in the strict-feedback form. Therefore, it is of both theoretical and practical importance to study the control problem for strict-feedback nonlinear systems.

Assumption 1. The desired signal y_d and its first derivative, i.e., $\dot{y}_d$ are known, smooth and bounded.

Remark 3. In assumption 1, y_d is the desired input to the closed-loop system. Therefore, it is reasonable to assume that it is available and known. The backstepping approach requires the knowledge of $y_d^{(i)}$ where $i = 0,1,\ldots,n-1$, or conventional DSC approach requires the knowledge of y_d, $\dot{y}_d$ and $\ddot{y}_d$. However, assumption 1 just needs the knowledge of y_d and its first derivative which is less restrictive. It signifies that the proposed scheme is more suitable for some important applications where higher order derivatives are unavailable.

Before presenting the proposed resilient control approach, some preliminaries are reviewed briefly.

B. Preliminary Concepts

Because of using RBF-NN for modeling uncertain dynamics of the system and unknown additive FDI attack, at first, RBF-NN is described briefly. Figure (2) shows the RBF-NN structure.

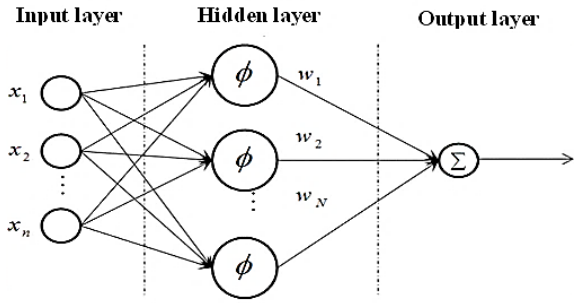

Fig. 2. Structure of the RBF-NN.

As it is obtained from Fig. 2, RBF-NN consists of three layers: input layer, hidden layer and output layer. Activation function in the hidden layer of the RBF-NN has a radial basis function form as follows:

$$\phi_i(x) = exp\left(-\frac{\|\boldsymbol{x} - \chi_i\|}{2\eta_i^2}\right), \tag{4}$$

where $\boldsymbol{x}$ is the input vector, χ_i and η_i denote the center and width of the activation functions, respectively. The center parameter can be placed on a random subset or all of the training examples, or chosen by using the clustering algorithms or determined by invoking heuristic algorithms or learning procedure. Also, the basis function widths can be either chosen to be the same for all of the units or can be chosen differently for each unit, depending on the part of the input space they represent. It is worth to note that the training process may adapt the width parameter for each of the basis functions, also.

As it is obtained from Fig. 2, output of the RBF-NN can be written as

$$f(\boldsymbol{x}) = \sum_{i=1}^{N} w_i \phi(x_i), \tag{5}$$

where w_i is the weight coefficient between the *i*th neuron and output, N is the number of the network neurons, and x_i is the input of the *i*th neuron. For simplicity, network output in (5) is rewritten in the following linear regression form

$$f(\boldsymbol{x}) = \boldsymbol{w}^T \boldsymbol{\varphi}(\boldsymbol{x}), \tag{6}$$

where $\boldsymbol{w} = [w_1 \quad w_2 \quad \ldots \quad w_N]^T$ is the weight vector and $\boldsymbol{\varphi}(\boldsymbol{x}) = [\phi_1(\boldsymbol{x}_1) \quad \phi_2(\boldsymbol{x}_2) \quad \ldots \quad \phi_N(\boldsymbol{x}_N)]^T$ is the activation function vector.

According to the universal approximation property of the RBF-NN [38, 39], the RBF-NN with sufficiently large number of neurons (N_i) can approximate any continuous

real valued function $f_i(x_i): \Re^i \to \Re$ over a compact set $\Omega \subset \Re^i$ to any desired accuracy as:

$$f_i(\boldsymbol{x}_i) = \boldsymbol{w}_i^{*T} \boldsymbol{\varphi}_i(\boldsymbol{x}_i) + \varepsilon_i(\boldsymbol{x}_i), \tag{7}$$

where $\boldsymbol{w}_i^* \in R^N$ represents an ideal weight vector satisfying (8), and $\varepsilon_i(\boldsymbol{x}_i)$ is the approximation error with an assumption of $|\varepsilon_i(\boldsymbol{x}_i)| \le \bar{\varepsilon}_i$, where the unknown constant $\bar{\varepsilon}_i > 0$ for all $x_i \in \Omega$,

$$\boldsymbol{w}^* = arg \min_{w \in R^N} \left\{ \sup_{x_i \in \Omega} \left| f_i(\boldsymbol{x}_i) - \boldsymbol{w}_i^T \boldsymbol{\varphi}_i(\boldsymbol{x}_i) \right| \right\}. \tag{8}$$

Since $\boldsymbol{w}_i^*$ is ideal weight vector, it is unknown and it is necessary to estimate it online. In the following, $\boldsymbol{w}_i$ denotes the estimation of $\boldsymbol{w}_i^*$.

Now, some required lemmas for controller design are explained.

Lemma 1 [40]. Consider the following command filter

$$\begin{aligned} \dot{z}_1 &= \omega_n z_2, \\ \dot{z}_2 &= -2\xi\omega_n z_2 - \omega_n (z_1 - v), \end{aligned} \tag{9}$$

where v is the input signal. If the first and second derivatives of the input signal v for all $t \ge 0$ are bounded, i.e., $|\dot{v}| \le \bar{v}$ and $|\ddot{v}| \le \bar{v}_1$, also $z_1(0) = v(0)$, $z_2(0) = 0$, then for any $v^* > 0$, there exists filter design parameters $\omega_n > 0$ and $\xi \in (0,1]$ such that $|z_1 - v| \le v^*$, $|\dot{z}_1|$, $|\dot{z}_1|$, and $|\ddot{z}_1|$ is bounded.

Definition 1 [41]. Function $N(\kappa): \Re \to \Re$ is called Nussbaum function if it satisfies the following properties:

$$\begin{aligned} &\lim_{p \to \infty} \sup \frac{1}{p} \int_0^p N(\kappa) d\kappa = +\infty, \\ &\lim_{p \to -\infty} \sup \frac{1}{p} \int_0^p N(\kappa) d\kappa = -\infty. \end{aligned} \tag{10}$$

Lemma 2 [42]. Consider smooth functions $V(.)$ and $\kappa(.)$ defined on interval $(0, t_f)$, in which $V(t) \ge 0$ for $\forall t \in (0, t_f)$ and $N(\kappa)$ is a Nussbaum function, if the following inequality holds then κ, V, and $\int_0^t \left(bN(\kappa) + 1\right) \dot{\kappa} e^{a_1 \tau} d\tau$ on the defined interval $(0, t_f)$ will be bounded:

$$0 \le V(t) \le a_0 + e^{-a_1 t} \int_0^t \left(bN(\kappa) + 1\right) \dot{\kappa} e^{a_1 \tau} d\tau, \tag{11}$$

In the above inequality, $a_0, a_1 > 0$ are proper constant values and b satisfies $b: R \to \left[l^- \quad l^+ \right]$ where $l^- l^+ > 0$.

III. Proposed Scheme

In this section the proposed CFB-based resilient control scheme is explained for considered CPS (3) under FDI attack. In the proposed scheme to decrease number of learning parameters, and consequently to reduce the online computational burden, the minimal learning parameters (MLP) algorithm [43] has been used. In this algorithm, norm of the weight vector of the RBF-NN is considered as one adaptive parameter and it is updated online. This algorithm aims to achieve universal approximation property with fewest possible adjustable parameters and helps to improve computational efficiency. For having this, let us define adaptive parameter θ_i as $\theta_i := \|\boldsymbol{w}_i\|$ for $i = 1, 2, ..., n$ and update it online based on the adaptive laws which will be derived later. By using this strategy, number of adaptive parameters is decreased from N_i (number of RBF-NN neurons for modeling $f_i(\boldsymbol{x}_i)$) to *1*.

Let us define the proposed error surfaces as

$$\begin{aligned} s_1 &= x_1 - y_d, \\ s_i &= x_i - x_{i,c}, \quad for \ i = 2, ..., n \end{aligned} \tag{12}$$

where $x_{i,c}$ is obtained from the following command filter

$$\begin{aligned} \dot{z}_{i,1} &= \omega_n z_{i,2}, \\ \dot{z}_{i,2} &= -2\xi\omega_n z_{i,2} - \omega_n (z_{i,1} - v_i). \end{aligned} \tag{13}$$

In (13), v_i is the filter input, $z_{i,1}$ and $z_{i,2}$ are the filter outputs. Also, ξ and ω_n are design parameters of the filter. In order to eliminate the filtering error, the compensated tracking error signal e_i is defined as:

$$e_i = s_i - \zeta_i \quad for \quad i = 1, ..., n, \tag{14}$$

where ξ_i is defined as:

$$\begin{aligned} \dot{\zeta}_i &= -c_i \zeta_i + x_{i+1,c} - \alpha_i + \zeta_{i+1}, \quad i = 1, ..., n-1 \\ \dot{\zeta}_n &= 0, \end{aligned} \tag{15}$$

and $\zeta(0) = 0$. In (15), c_i, $i = 1, ..., n-1$ are positive constants chosen by the designer. As it was proved in detail in [44, Lemma 3, 45], ζ_i is bounded and $\lim_{t \to \infty} |\zeta_i| \le \frac{v^*}{2c_0}$ where $c_0 = (1/2) min(c_i)$.

By considering RBF-NN model in (7), and adjusting norm of the weight coefficients as an adaptive parameter, the following inequality is obtained:

$$e_i f_i \le \frac{1}{2}e_i^2\theta_i\boldsymbol{\varphi}_i^T\boldsymbol{\varphi}_i + \frac{1}{2} + \frac{1}{2}e_i^2 + \frac{1}{2}\varepsilon_i^2. \tag{16}$$

Also, the following inequalities hold:

$$\begin{aligned} e_i e_{i+1} &\le \frac{1}{2}e_i^2 + \frac{1}{2}e_{i+1}^2, \\ \tilde{\theta}_i\theta_i &\le \frac{1}{2}\tilde{\theta}_i^2 + \frac{1}{2}\theta_i^2. \end{aligned} \tag{17}$$

Now, design steps of the proposed scheme are presented.

Step 1: At first, by considering the first error surface and differentiating it with respect to time, and substituting the first equation of (3) for $i=1$ in the result, dynamics of the first error surface is obtained as:

$$\dot{s}_1 = x_2 + f_1 - \dot{y}_d. \tag{18}$$

Now the following virtual input for stabilizing (18) is proposed:

$$\alpha_1 = -c_1 s_1 + \dot{y}_d - \frac{1}{2}\hat{\theta}_1 e_1\boldsymbol{\varphi}_1^T\boldsymbol{\varphi}_1, \tag{19}$$

where c_1 is a design parameter and $\hat{\theta}_1$ is an adaptive parameter updated based on the following adaptive law:

$$\dot{\hat{\theta}}_1 = \frac{\gamma_1}{2}e_1^2\boldsymbol{\varphi}_1^T\boldsymbol{\varphi}_1 - \gamma_1\sigma_1\hat{\theta}_1, \tag{20}$$

where σ_1 is a design parameter and positive constant γ_1 represents a learning rate. Considering (14) for $i=1$, differentiating it with respect to time and substituting (15), (18), and (19) in the result, gives:

$$\dot{e}_1 = e_2 - c_1 e_1 + \left(f_1 - \frac{1}{2}\hat{\theta}_1 e_1\boldsymbol{\varphi}_1^T\boldsymbol{\varphi}_1\right). \tag{21}$$

Consider the following Lyapunov function for stability analysis

$$V_1 = \frac{1}{2}e_1^2 + \frac{1}{2\gamma_1}\tilde{\theta}_1^2, \tag{22}$$

where $\tilde{\theta}_1 = \theta_1 - \hat{\theta}_1$ is the parameter estimation error. Differentiating (22) with respect to time and substituting (21) in the result gives

$$\dot{V}_1 = e_1 e_2 - c_1 e_1^2 + e_1 f_1 - \left(\frac{1}{2}\hat{\theta}_1 e_1^2\boldsymbol{\varphi}_1^T\boldsymbol{\varphi}_1\right) - \frac{1}{\gamma_1}\tilde{\theta}_1\dot{\hat{\theta}}_1. \tag{23}$$

By applying inequalities (16) and (17) to (23) and considering (20), equation (23) can be expressed as

$$\dot{V}_1 \le (1-c_1)e_1^2 + \frac{1}{2}e_2^2 + \sigma_1\tilde{\theta}_1\hat{\theta}_1 + \frac{1}{2} + \frac{1}{2}\varepsilon_1^2. \tag{24}$$

Substituting $\hat{\theta}_1 = \theta_1 - \tilde{\theta}_1$ in (24), gives

$$\dot{V}_1 \le (1-c_1)e_1^2 + \frac{1}{2}e_2^2 + \sigma_1\left(\tilde{\theta}_1\theta_1 - \tilde{\theta}_1^2\right) + \frac{1}{2} + \frac{1}{2}\varepsilon_1^2. \tag{25}$$

Applying inequality (17) to (25) results in:

$$\dot{V}_1 \le (1-c_1)e_1^2 + \frac{1}{2}e_2^2 + \frac{\sigma_1}{2}\theta_1^2 - \frac{\sigma_1}{2}\tilde{\theta}_1^2 + \frac{1}{2} + \frac{1}{2}\bar{\varepsilon}_1^2. \tag{26}$$

Step i (i=2, …, n-1): Consider the *i*th error surface. By taking the time derivative of s_i and substituting (3) in the results, we will have

$$\dot{s}_i = x_{i+1} + f_i - \dot{x}_{i+1,c}. \tag{27}$$

To stabilize (27), the following virtual control input is proposed:

$$\alpha_i = -c_i s_i + \dot{x}_{i,c} - \frac{1}{2}\hat{\theta}_i e_i\boldsymbol{\varphi}_i^T\boldsymbol{\varphi}_i - e_{i-1}, \tag{28}$$

where c_i is a design parameter, and $\hat{\theta}_i$ is an adaptive parameter adjusted based on the following adaptive law

$$\dot{\hat{\theta}}_i = \frac{\gamma_i}{2}e_i^2\boldsymbol{\varphi}_i^T\boldsymbol{\varphi}_i - \gamma_i\sigma_i\hat{\theta}_i, \tag{29}$$

where σ_i is a design parameter and positive constant γ_i is the learning rate. Again, by doing the same procedures as those described in step 1, we will have

$$\dot{e}_i = e_{i+1} - c_i e_i + f_i - \frac{1}{2}\hat{\theta}_i e_i\varphi_i^T\varphi_i - e_{i-1}. \tag{30}$$

Again, the following Lyapunov function is considered for stability analysis

$$V_i = \frac{1}{2}e_i^2 + \frac{1}{2\gamma_i}\tilde{\theta}_i^2, \tag{31}$$

where $\tilde{\theta}_i = \theta_i - \hat{\theta}_i$. Differentiating (31) with respect to time and substituting (30) in the result, gives

$$\begin{aligned} \dot{V}_i = {} & e_i e_{i+1} - c_i e_i^2 + e_i f_i - \frac{1}{2}\hat{\theta}_i e_i^2\boldsymbol{\varphi}_i^T\boldsymbol{\varphi}_i - e_i e_{i-1} \\ & - \frac{1}{\gamma_i}\tilde{\theta}_i\dot{\hat{\theta}}_i. \end{aligned} \tag{32}$$

Applying inequalities (16) and (17) to (32), gives:

$$\dot{V}_i \le \left(\frac{3}{2}-c_i\right)e_i^2+\frac{1}{2}e_{i+1}^2+\frac{1}{2}e_i^2\tilde{\theta}_i\boldsymbol{\varphi}_i^T\boldsymbol{\varphi}_i-\frac{1}{\gamma_i}\tilde{\theta}_i\dot{\hat{\theta}}_i + \frac{1}{2}+\frac{1}{2}\varepsilon_i^2+\frac{1}{2}e^2{}_{i-1}. \tag{33}$$

Substituting (29) in (33), and substituting $\tilde{\theta}_i=\theta_i-\hat{\theta}_i$ in the result, gives

$$\dot{V}_i \le \left(\frac{3}{2}-c_i\right)e_i^2+\frac{1}{2}e_{i+1}^2+\frac{\sigma_i}{2}\theta_i^2-\frac{\sigma_i}{2}\tilde{\theta}_i^2 + \frac{1}{2}+\frac{1}{2}\bar{\varepsilon}_i^2+\frac{1}{2}e^2{}_{i-1}. \tag{34}$$

Step n: Consider the *n*th error surface in (12). Taking the time derivative of (12) and substituting the last equation of (3) in $\dot{s}_n$, results in

$$\dot{s}_n=f_n+bv_n+a(\mathbf{x}_n)-\dot{x}_{n,c}. \tag{35}$$

To stabilize (35), the control input is proposed as

$$\begin{aligned} v_n &= N(\kappa)\nu, \\ \dot{\kappa} &= e_n\nu, \end{aligned} \tag{36}$$

where ν has the following form

$$\nu=c_ne_n-\dot{x}_{n,c}+\frac{1}{2}\hat{\theta}_ne_n\boldsymbol{\varphi}_n^T\boldsymbol{\varphi}_n+e_{n-1}. \tag{37}$$

In (37), c_n is a design parameter and $\hat{\theta}_n$ is adjusted based on the following adaptive law:

$$\dot{\hat{\theta}}_n=\frac{\gamma_n}{2}e_n^2\boldsymbol{\varphi}_n^T\boldsymbol{\varphi}_n-\gamma_n\sigma_n\hat{\theta}_n, \tag{38}$$

where $\gamma_n>0$ is the learning rate and $\sigma_n>0$ is a design parameter. Considering (35) and $\zeta_n=0$, the following tracking error is obtained

$$\dot{e}_n=f_n+a-\frac{1}{2}\hat{\theta}_ne_n\boldsymbol{\varphi}_n^T\boldsymbol{\varphi}_n+(bN(\kappa)+1)\nu - c_ne_n-e_{n-1}. \tag{39}$$

Now for stability analysis, the following Lyapunov function is considered:

$$V_n=\frac{1}{2}e_n^2+\frac{1}{2\gamma_n}\tilde{\theta}_n^2. \tag{40}$$

Taking time derivative of (40) and using (39) results in

$$\dot{V}_n=e_n(f_n+a)-\frac{1}{2}\hat{\theta}_ne_n^2\boldsymbol{\varphi}_n^T\boldsymbol{\varphi}_n+e_n(bN(\kappa)+1)\nu - c_ne_n^2-e_ne_{n-1}-\frac{1}{\gamma_n}\tilde{\theta}_n\dot{\hat{\theta}}_n. \tag{41}$$

Applying inequalities (16) and (17) to (41) and substituting (38) in the result, gives

$$\dot{V}_n \le (1-c_n)e_n^2+\frac{1}{2}+\frac{1}{2}\bar{\varepsilon}_n^2+e_n(bN(\kappa)+1)\nu + \frac{1}{2}e_{n-1}^2+\sigma_n\tilde{\theta}_n\hat{\theta}_n \tag{42}$$

Substituting $\hat{\theta}_n=\theta_n-\tilde{\theta}_n$ in (42) and applying inequality (17) to (42), results in

$$\dot{V}_n \le (1-c_n)e_n^2+e_n(bN(\kappa)+1)\nu+\frac{\sigma_n}{2}\theta_n^2 - \frac{\sigma_n}{2}\tilde{\theta}_n^2+\frac{1}{2}+\frac{1}{2}\varepsilon_n^2+\frac{1}{2}e_{n-1}^2 \tag{43}$$

IV. Main Results

This section presents main results and provides stability analysis of the closed-loop system.

Theorem 1. Consider the nonlinear system (1) under FDI attack in "controller to actuator" channel which affects the CPS in the additive and multiplicative forms. It can be shown that the proposed RBF-NN-based CFB approach guarantees that the closed loop system is stable and all signals of the closed-loop system are uniformly ultimately bounded.

Proof. Consider the following Lyapunov candidate function

$$V_T=\sum_{i=1}^{n}V_i. \tag{44}$$

Taking the time derivative of (44) and substituting (26), (34), and (43) in the result, gives

$$\dot{V}_T \le \left(\frac{3}{2}-c_1\right)e_1^2+\left(\frac{5}{2}-c_2\right)e_2^2+\left(\frac{5}{2}-c_3\right)e_3^2+\ldots + \left(\frac{3}{2}-c_n\right)e_n^2+e_n(bN(\kappa)+1)\nu + \sum_{i=1}^{n}\left(\frac{1}{2}+\frac{1}{2}\varepsilon_i^2+\frac{\sigma_i}{2}\theta_i^2-\frac{\sigma_i}{2}\tilde{\theta}_i^2\right), \tag{45}$$

Comparing (45) with (44), it makes possible to rewrite (45) as

$$\dot{V}_T \le -\mu V_T+\beta+(bN(\kappa)+1)\dot{\kappa} \tag{46}$$

where μ and β are obtained from substituting (44) and (45) in (46) as follows:

$$\mu \triangleq \min\left\{\begin{matrix} 2c_1-3 \\ 2c_i-5, \quad 2\le i\le n-1 \\ 2c_n-3 \\ \gamma_i\sigma_i \end{matrix}\right\}, \qquad \beta=\sum_{i=1}^{n}\left(\frac{1}{2}+\frac{1}{2}\varepsilon_i^2+\frac{\sigma_i}{2}\theta_i^2\right). \tag{47}$$

Solving (47) with respect to time gives

$$V_T \le e^{-\mu t}V(0)+\frac{\beta}{\mu}\left(1-e^{-\mu t}\right) +e^{-\mu t}\int_0^t\left(bN(\kappa)+1\right)\dot{\kappa}e^{\mu\tau}d\tau. \tag{48}$$

Applying Lemma 2 to (48) reveals that κ, V, and $\int_0^t\left(bN(\kappa)+1\right)\dot{\kappa}e^{\mu\tau}d\tau$ are bounded on interval $(0,t)$. Therefore, e_i and $\tilde{\theta}_i$ for $i=1,2,...,n$ are bounded. Because $s_i=e_i+\zeta_i$ and according to [44: Lemma 3, 45] $|\zeta_i|$ is bounded, therefore signal s_i is bounded. Let us denote the bound of $\int_0^t\left(bN(\kappa)+1\right)\dot{\kappa}e^{\mu\tau}d\tau$ by $\bar{\Delta}$, so the ultimate bound of the tracking error will be $\lim_{t\to\infty}|s_1|\le\sqrt{\frac{2\beta}{\mu}}+2\bar{\Delta}+\frac{\nu^*}{2c_0}$. ■

Remark 4. It can be seen from Lemma 1, and the definition of β, μ, and c_0 that the tracking error bound depends on the design parameters c_i, σ_i, and γ_i for $i=1,...,n$. Also, it depends on the command filter parameters (ω_n, ξ) and width and center of the basis functions in the RBF-NN. Increasing c_i can lead to smaller tracking error and faster convergence, but it might induce undesirable oscillations or require larger control effort, potentially leading to input saturation. Also, appropriately tuning of the adaptation parameters γ_i and σ_i ensures accurate estimation and effective compensation of uncertainties, thus minimizing tracking error. Also, a command filter with high natural frequency (ω_n) generally leads to smaller filtering errors and thus, potentially improves the tracking accuracy, as the filter can more closely track the desired signals. However, increasing the bandwidth too much can lead to increase the sensitivity to noise and oscillations. Also, the damping ratio of the command filter (ξ) influences the transient response of the filtered signals. An appropriate damping ratio helps preventing from oscillations and overshoots in the filtered commands, which can in turn, reduce fluctuations in the tracking error. Also, width and center of the basis functions in the RBF-NN structure are two other important design parameters. A basis function with narrow (small) width results in a more precise approximation of the unknown system dynamics in specific regions of the state space. In such case, if the system moves into regions that are not covered by the RBF centers well, or if the width is excessively small, the network's generalization capability might be compromised, leading to increased tracking error and larger control signal. While basis functions with large width cover a wider area of the input space and consequently, improve the network's generalization ability across a larger operating range, they potentially reduce the tracking error, control effort and chattering. A well-distributed set of centers, particularly in regions where the system dynamics exhibit significant variations, enhances the approximation capability, thereby reducing the tracking error.

In summary, there are inherent trade-offs in the selection of these parameters. For instance, achieving a very small tracking error often requires higher controller gains, which can lead to increased control input amplitude and potential saturation issues.

TABLE II PHYSICAL PARAMETERS

Physical Parameters	Definition	Numerical Value
L (m)	Distance between center and end of the joint	1
M (kg)	Mass of the joint	1
g (m/S^2)	Acceleration of gravity	9.8
l (kg m^2)	Moment of inertia	4/3

V. Simulation Results

To investigate the performance of the proposed scheme, the following robotic arm described by (49) is considered [22]

$$\ddot{\theta}=-l^{-1}(2\dot{\theta}+mgLcos\theta)+l^{-1}\tau. \tag{49}$$

In (49), θ, $\dot{\theta}$, and $\ddot{\theta}$ denote the position, velocity and acceleration, and τ represents the applied control input to the joint. Other physical parameters and their numerical values for simulation have been given in Table II.

The control objective is to design a control input such that the system output tracks the desired signal y_d in the presence of FDI attack in "controller to actuator" channel. For simulation, initial conditions were set to $\boldsymbol{x}_0=\begin{bmatrix}0.2\pi & 0\end{bmatrix}^T$, $\zeta_0=0$, and $\hat{\boldsymbol{\theta}}_0=\begin{bmatrix}0 & 0\end{bmatrix}^T$, and design parameters were chosen as $c_1=2$, $c_2=0.5$, $\omega_n=40$, $\xi=0.6$, $\gamma_1=\gamma_2=0.5$, and $\sigma_1=\sigma_2=0.03$. Also,

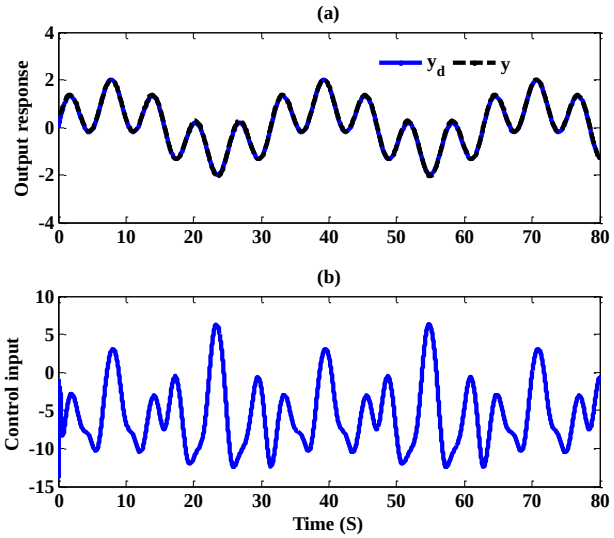

Fig. 3. (a) Output response, and (b) Control input under no FDI attack.

Nussbaum-type function was chosen as $N(\kappa)=exp(\kappa^2)cos((\kappa/2)\pi)$. The RBF-NN contains 25 nodes with centers χ_i, $i=1,...,25$ evenly spaced in the range $[-2,2]\times[-2,2]$, and the width of the basis function is set to $\eta_i=2$ for $i=1,...,25$. Figure (3) shows the output response of the proposed controller for

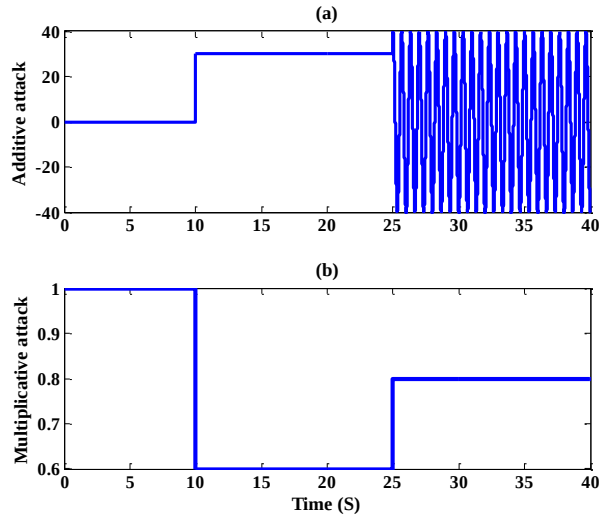

Fig. 4. Attack signal, (a) Additive term, and (b) Multiplicative term (case 1).

tracking $y_d=sin\,t+sin\,0.2t$ under no FDI attack. As it is obtained from the figure, the output variable tracks the desire output accurately and the control input is bounded.

Now, performance of the proposed scheme against three different FDI attacks is simulated and discussed.

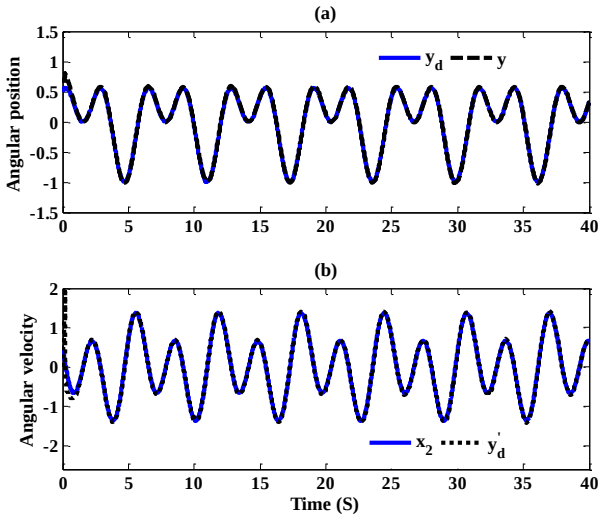

Fig. 5. (a) Angular position, and (b) Angular velocity of the robotic arm under FDI attack (case 1).

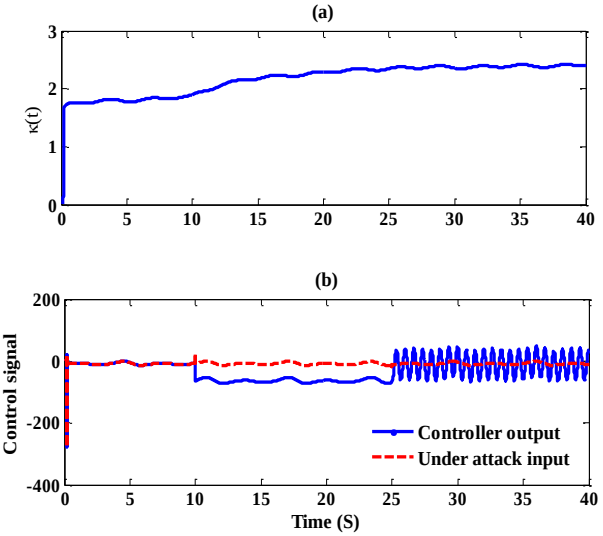

Fig. 6. (a) κ, (b) Controller output and under attack input. (case 1).

Case 1: In this case, a simple attack defined in (50) is applied to the system. Figure 4 shows the considered unlimited duration attack in (50):

$$u=\begin{cases} v_n & t<10 \\ 0.6v_n+30 & 10\le t\le 25 \\ 0.8v_n-40cos\,0.3\pi t & t\ge 25 \end{cases} \quad (50)$$

Figures 5-7 show the simulation results of the proposed scheme for tracking $y_d=0.5(sin\,t+cos\,2t)$ in the presence of considered attack in (50).

Figure 5 displays the angular position and velocity of the robotic arm under FDI attack in (50). Figure 6 shows the actual and under attack control inputs, and Fig. (7) depicts adaptive parameters. As it is obvious from the results, proposed resilient control scheme tolerates the cyber-attack and preserves tracking ability of the closed-loop system

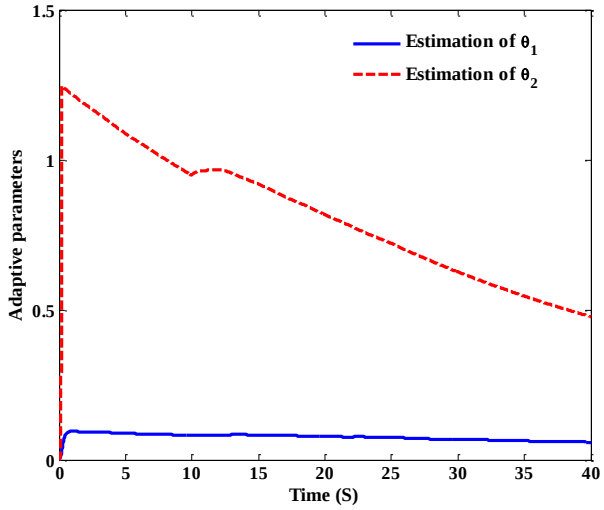

Fig. 7. Adaptive parameters (case 1).

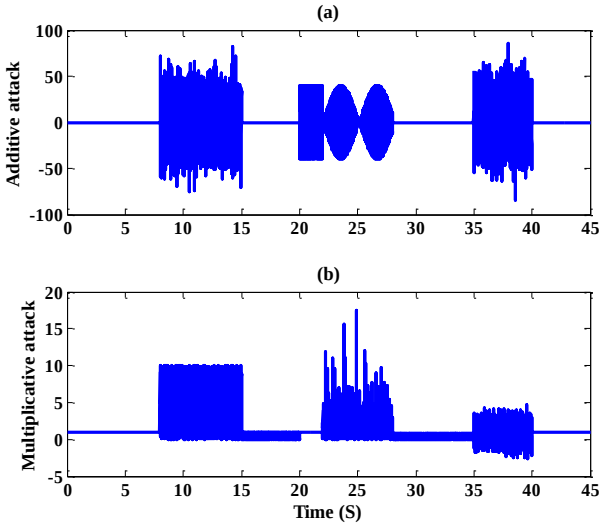

Fig. 8. Stochastic attack, (a) Additive term, and (b) Multiplicative term (case 2).

under FDI attack, properly. As it is seen from the results, all of the closed-loop signals are bounded.

Case 2: In this case, a random stochastic attack with high switching frequency defined in (51) is injected into the "controller to actuator" communication channel. Figure 8 represents the considered attack. As it is seen form Fig. 8, at time interval $(20 \quad 22]$ only additive term is non-zero, at intervals $(15 \quad 20]$ and $(28 \quad 35]$, only multiplicative attack is nonzero and in other intervals, both of additive and multiplicative terms are non-zero. Figure 9 represents the output response and the tracking error in presence of stochastic attack given in (51). It is clear from Fig. 9(a) that the output results can track the desired trajectory in presence of random attack. Also, results in Fig. 9(b) indicate that the norm of the tracking error is bounded.

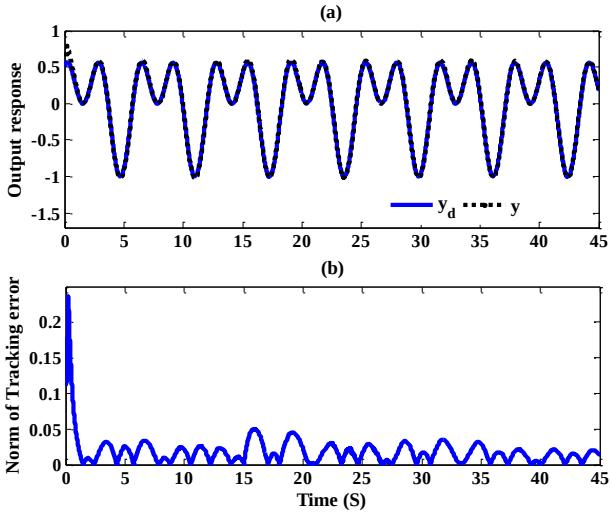

Fig. 9. (a) Output response, and (b) Norm of the tracking error (case 2)

Obtained results verify that the proposed method is able to mitigate simultaneous additive and multiplicative attacks and it is not dependent on the attack function. This ability helps the system to defend against the total intrusion of an attacker regardless of the attack variations. The other advantage of the proposed approach is elimination of the need for attack reconstruction and control reconfiguration in presence of attacks. Therefore, the complexity and cost of control design will be decreased.

$$u=\begin{cases} v_n & t\le 8 \\ 10\,\mathrm{rand}(.)v_n+20\mathrm{randn}(.) & 8<t\le 15 \\ \mathrm{rand}(.)v_n & 15<t\le 20 \\ v_n+40\cos\left(30\pi\,\mathrm{randn}(.)\right) & 20<t\le 22 \\ 0.5\exp(\text{-randn}(.))v_n & \\ \quad +40\cos(30\pi\mathrm{t})\sin\left(t\right) & 22<t\le 28 \\ 0.8\mathrm{rand}(.)v_n & 28<t\le 35 \\ (1+\mathrm{randn}(.))v_n & \\ \quad +20\,\mathrm{randn}(.) & 35<t\le 40 \\ v_n & 40<t \end{cases} \tag{51}$$

Case 3: In this case the following time-dependent attack is considered. Figures 10 and 11 illustrate the considered attack, output response and norm of the tracking error.

As it is seen from Fig. 11, the output signal tracks the desired trajectory and norm of the tracking error is bounded. Therefore, the proposed scheme is resilient against time-varying attack.

Simulation results in Figs. 4-11 verify that boundedness of the output variable and the tracking error is achieved regardless of the FDI attack type at "controller to actuator" channel.

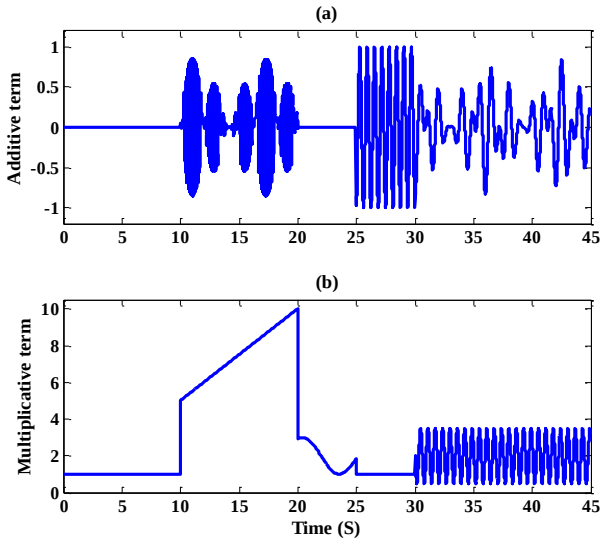

Fig. 10. Time-varying attack, (a) additive term, and (b) multiplicative term (case 3).

Obtained results show that the proposed approach could mitigate different kind of FDI attacks without using attack reconstruction or controller reconfiguration units.

$$u = \begin{cases} v_n & t \le 10 \\ \sin(t)\cos(30x_2) + 0.5tv_n & 10 < t \le 20 \\ (2+\sin t)v_n & 20 < t \le 25 \\ v_n + \sin(10t) & 25 < t \le 30 \\ (2-1.5\cos(10t))v_n + \sin(x_1)\cos(2\pi t) & t > 30 \end{cases} \quad (52)$$

VI. Conclusion

This paper proposes an adaptive resilient control scheme for uncertain *n*th order nonlinear CPSs under injection attack. The main findings are: (1) an adaptive command filtered backstepping-based control scheme is able to handle the injection attack, and also it guarantees that the tracking error can be made small by adjusting the design parameters; (2) the proposed scheme eliminates the "explosion of complexity" problem, removes challenges in choosing time-constant of filters and compensates the filtering error, simultaneously, (3) the proposed scheme is resilient against both additive and multiplicative forms of cyber-attacks without any prior knowledge about the attack time, severity and characteristics, (4) it does not require attack detection and estimation units separately, as well as

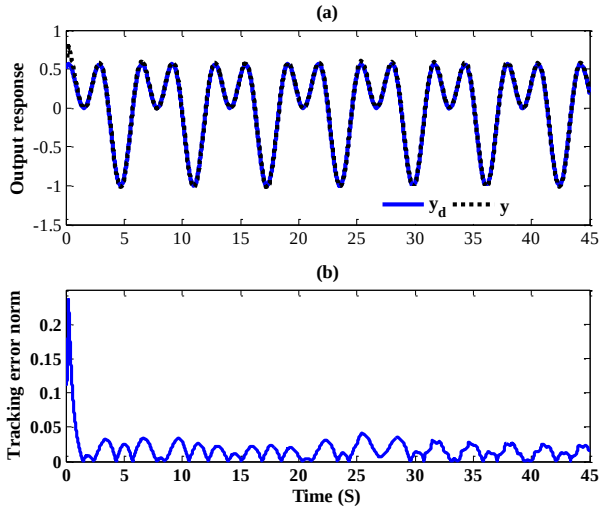

Fig. 11. (a) Output response, and (b) norm of the tracking error (case 3).

controller readjustment or reconfiguration algorithm, and (5) it decreases the number of adjustable parameters and online computational burden by using MLP algorithm. Therefore, the proposed approach maintains system stability and performance despite deceptive attack without noticeably increasing the complexity or imposing computational burden to design and implementation of the control system. However, the proposed passive resilient control offers a simpler and potentially more robust approach to mitigate attacks, but it may have limitations in terms of performance, adaptability in the face of some unforeseen disturbances or changes in the operating condition of the systems. Obtained simulation results verify the effectiveness and appropriate performance of the proposed resilient control scheme.

Extending the proposed scheme to deal with nonlinear CPSs in the presence of sensor attack can be considered as a future work.

References

[1] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security- A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[2] Z. Lian, P. Shi, and M. Chen, "A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense, and Design," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 1471-1483, Jan. 2025, doi: 10.1109/JIOT.2024.3495046.

[3] S. Chase Hassler, U. Ahmad Mughal, and M. Ismail, "Cyber-Physical Intrusion Detection System for Unmanned Aerial Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, pp. 6106-6117, June 2024, doi: 10.1109/TITS.2023.3339728.

[4] M.K. Hasan, A.A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M.A. Razzaque, "Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations," *Journal of Network and*

Computer Applications, vol. 209, p. 103540, Jan. 2023, doi: 10.1016/j.jnca.2022.103540.
[5] M. Javaid, A. Haleem, R.P. Singh, and R. Suman, "An Integrated Outlook of Cyber–Physical Systems for Industry 4.0: Topical Practices, Architecture, and Applications," *Green Technologies and Sustainability*, vol. 1, no. 1, p. 100001, Jan. 2023, doi: 10.1016/j.grets.2022.100001.
[6] M. Nazifi, and M. Pourgholi, "Adaptive Fractional-Order Consensus Control of Cyber-Physical Power Systems in the Presence of Unbounded Perturbations," *International Journal of Industrial Electronics Control and Optimization*, vol. 8, no. 2, pp. 105-116, June 2025, doi: 10.22111/ieco.2024.48807.1571.
[7] W. Duo, M. Zhou, and A. Abusorrah, "A Survey of Cyber-Attacks on Cyber-Physical Systems: Recent Advances and Challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5, pp. 784-800, May 2022, doi: 10.1109/JAS.2022.105548.
[8] Z. Yu, H. Gao, X. Cong, N. Wu, and H.H. Song, "A Survey on Cyber–Physical Systems Security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21670-21686, Dec. 2023, doi: 10.1109/JIOT.2023.3289625.
[9] L. Hu, Z.D. Wang, Q.L. Han, and X.H. Liu, "State Estimation under False Data Injection Attacks: Security Analysis and System Protection," *Automatica*, vol. 87, no. 2, pp. 176–183, Jan. 2018, doi: 10.1016/j.automatica.2017.09.028.
[10] D. Zhang, Q.G. Wang, G. Feng, Y. Shi, and A.V. Vasilakos, "A Survey on Attack Detection, Estimation and Control of Industrial Cyber–Physical Systems," *ISA Transactions*, vol. 116, pp. 1-16, Oct. 2021, doi: 10.1016/j.isatra.2021.01.036.
[11] D. Zhang G. Feng,Y. Shi, and D. Srinivasan, "Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances," *IEEE/CAA Journal of Automatics Sinica*, vol. 8, no. 2, pp. 319-333, Feb. 2021, doi: 10.1109/JAS.2021.1003820.
[12] S. Tan, J.M. Guerrero, P. Xie, R. Han, and J.C. Vasquez, "Brief Survey on Attack Detection Method for Cyber-Physical Systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329-5339, Dec. 2020, doi: 10.1109/JSYST.2020.2991258.
[13] D. Ding, Q-L. Han, Y. Xiang, X. Ge, and X-M. Zhang, "A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems," *Neurocomputing*, vol. 275, pp. 1674-1683, Jan. 2018, doi: 10.1016/j.neucom.2017.10.009.
[14] M. Kordestani, and M. Saif, "Observer-Based Attack Detection and Mitigation for Cyber-Physical Systems–A Review," *IEEE Systems, Man, and Cybernetics Magazine*, vol. 7, no. 2, pp. 35-60, Apr. 2021, doi: 10.1109/MSMC.2020.3049092.
[15] M. Shahriari-kahkeshi, S.A. Alem, and P. Shi, "Detection, Reconstruction and Mitigation of Deception Attacks in Nonlinear Cyber-Physical Systems," *International Journal of Adaptive Control and Signal Processing*, vol. 38, no. 9, pp. 2972-2995, Sep. 2024, doi: 10.1002/acs.3854.
[16] F. Farivar, M. Sayad Haghighi, A. Jolfaei, and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber Physical Systems and Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2716-2725, 2020, doi: 10.1109/TII.2019.2956474.
[17] M. Jahangiri-Heidari, M. Shahriari-kahkeshi, and P. Shi, "Resilient Consensus of Nonlinear Multiagent Systems under False Data Injection Attack on Communication Channels: An Attack Detection and Isolation-based Approach," *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 8219-8230, Apr. 2025, doi: 10.1109/JIOT.2024.3500587.
[18] A. Sargolzaei, K. Yazdani, A. Abbaspour, C.D. Crane, and W.E. Dixon, "Detection and Mitigation of False Data Injection Attacks in Networked Control Systems," *IEEE Transactions on Industrial Information*, vol. 16, no. 6, pp. 4281-4292, June 2020, doi: 10.1109/TII.2019.2952067.
[19] R. Huang, and Y. Li, "Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2367 – 2376, May 2023, doi: 10.1109/TSG.2022.3217060.
[20] S. Lü, X. Jin, L. Ding, and Q. Tan, "Adaptive Sliding-Mode Control of a Class of Disturbed Cyber–Physical Systems Against Actuator Attacks," *Computers and Electrical Engineering*, vol. 96, p. 107492, Dec. 2021, doi: 10.1016/j.compeleceng.2021.107492.
[21] S.J. Yoo, "Neural-Network-Based Adaptive Resilient Dynamic Surface Control Against Unknown Deception Attacks of Uncertain Nonlinear Time-delay Cyber-Physical Systems," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 10, pp. 4341-4353, Oct. 2020, doi: 10.1109/TNNLS.2019.2955132.
[22] Y. Zhao, C. Zhou, and Y.C. Tian, "Anti-Saturation Resilient Control of Cyber-Physical Systems under Actuator Attacks," *Information Sciences*, vol. 608, pp. 1245-1260, Aug. 2022, doi: 10.1016/j.ins.2022.07.010.
[23] Y. Yang, J. Huang, X. Su, and B. Deng, "Adaptive Control of Cyber-Physical Systems under Deception and Injection Attacks," *Journal of the Franklin Institute*, vol. 358, no. 12, pp. 6174-6194, Aug. 2021, doi: 10.1016/j.jfranklin.2021.06.008.
[24] Y. Yang, J. Huang, X. Su, K. Wang, and G. Li, "Adaptive Control of Second-Order Nonlinear Systems with Injection and Deception Attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 1, pp. 574-581, Jan. 2022, doi: 10.1109/TSMC.2020.3003801.
[25] Y. Zhao, X. Du, C. Zhou, Y.C. Tian, X. Hu, and D.E. Quevedo, "Adaptive Resilient Control of Cyber-Physical Systems under Actuator and Sensor Attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3203 – 3212, May 2022, doi: 10.1109/TII.2021.3108876.
[26] S. Liu, X. Wang, B. Niu, X. Song, H. Wang, and X. Zhao, "Adaptive Resilient Output Feedback Control Against Unknown Deception Attacks for Nonlinear Cyber-Physical Systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 8, pp. 3855 – 3859, Aug. 2024, doi: 10.1109/TCSII.2024.3372413.
[27] M. Mazare, "Reinforcement Learning-based Fixed-time Resilient Control of Nonlinear Cyber Physical Systems Under False Data Injection Attacks and Mismatch Disturbances," *Journal of the Franklin Institute*, vol. 360, no. 18, Dec. 2023, pp. 14926 – 14938, doi: 10.1016/j.jfranklin.2023.10.026.
[28] J. Zhao, and G-H. Yang, "Reinforcement-Learning-Based Fuzzy Adaptive Finite-Time Optimal Resilient Control for Large-Scale Nonlinear Systems Under False Data Injection Attacks," *IEEE Transactions on Fuzzy Systems*, vol. 32, no. 4, Apr. 2024, pp. 2483-2495, doi:10.1109/TFUZZ.2023.3343722.
[29] Y-S. Ma, W-W. Che, C. Deng, and Z-G. Wu, "Model-Free Adaptive Resilient Control for Nonlinear CPSs With Aperiodic Jamming Attacks," *IEEE Transactions on Cybernetics*, vol. 53, no. 9, Sep. 2023, pp. 5949-5956, doi: 10.1109/TCYB.2022.3219987.
[30] S. Gao, L. Liu, H. Wang, and A. Wang, "Data-Driven Model-Free Resilient Speed Control of an Autonomous

Surface Vehicle in the Presence of Actuator Anomalies," *ISA Transactions*, vol. 127, Aug. 2022, pp. 251-258, doi: 10.1016/j.isatra.2022.04.050.
[31] S-S. Sun, and Y-X. Li, "Data-Driven Adaptive Resilient Funnel Consensus Tracking of Multi-Agent Systems Under Jamming Attacks," *International Journal of Robust and Nonlinear Control*, Aug. 2024, doi: 10.1002/rnc.7593.
[32] A. Azarbahram, N. Pariz, M-B. Naghibi-Sistani, and R. Kardehi Moghaddam, "Leader-Follower Formation Control of Uncertain USV Networks Under Stochastic Disturbances," *International Journal of Industrial Electronics Control and Optimization*, vol. 5, no. 2, pp. 133-142, Apr. 2022, doi: 10.22111/ieco.2022.37987.1346.
[33] F. Nobakht, H. Eliasi, "Adaptive Backstepping Control of Two-Group SEIAR Epidemic Model in the Presence of Input Saturation and External Disturbances," *International Journal of Industrial Electronics Control and Optimization*, In Press, April 2025, doi: 10.22111/ieco.2025.50181.1632.
[34] M. Krstic, I. Kanellakopoulos, and P.V. Kokotovic, Nonlinear and Adaptive Control Design, Wiley, New York, NY, USA, 1995.
[35] X.D. Tang, G. Tao, and S.M. Joshi, "Adaptive Actuator Failure Compensation for Nonlinear MIMO Systems with an Aircraft Control Application," *Automatica*, vol. 43, no. 11, pp. 1869-1883, 2007, doi: 10.1016/j.automatica.2007.03.019.
[36] Y.M. Li, S.C. Tong, and T.S. Li, "Adaptive Fuzzy Output Feedback Control for a Single-Link Flexible Robot Manipulator Driven DC Motor via Backstepping", *Nonlinear Analysis: Real World Applications*, vol. 14, no. 1, pp. 483-494, 2013, doi: 10.1016/j.nonrwa.2012.07.010.
[37] F.J. Lin, H.J. Shieh, and P.K. Huang, "Adaptive Wavelet Neural Network Control with Hysteresis Estimation for Piezo–Positioning Mechanism," *IEEE Transactions on Neural Networks*, vol. 17, no. 2, pp. 432-444, 2006, doi: 10.1109/TNN.2005.863473.
[38] M.M. Polycarpou, and J. Mears, "Stable Adaptive Tracking of Uncertainty Systems Using Nonlinearly Parameterized On-line Approximators," *International Journal of Control*, vol. 70, no. 3, pp. 363–384, Jan. 1998, doi: 10.1080/002071798222280.

[39] R.M. Sanner, and J.E. Slotine, "Gaussian Networks for Direct Adaptive Control," *IEEE Transactions on Neural Networks*, vol. 3, no. 6, pp. 837–863, Nov. 1992, doi: 10.1109/72.165588.
[40] J.A. Farrell, M. Polycarpou, M. Sharma, and W. Dong, "Command Filtered backstepping," 2008 American Control Conference, Washington, USA, June 11-13, 2008.
[41] R.D. Nussbaum, "Some Remarks on the Conjecture in Parameter Adaptive Control," *Systems & Control Letter*, vol. 3, no. 5, pp. 243–246, Nov. 1982. doi: 10.1016/0167-6911.
[42] X.D. Ye, and J.P. Jiang, "Adaptive Nonlinear Design without a Prior Knowledge of Control Directions," *IEEE Transactions on Automatic Control*, vol. 43, no. 11, pp. 1617–1621, Nov. 1998, doi: 10.1109/9.728882.
[43] Y. Yang, and J. Ren, "Adaptive fuzzy robust tracking controller design via small gain approach and its application," *IEEE Transactions on Fuzzy Systems*, vol. 11, no. 6, pp. 783-795, Dec. 2003, doi: 10.1109/TFUZZ.2003.819837.
[44] W. J. Dong, J. A. Farrell, M. Polycarpou, V. Djapic, and M. Sharma,"Command Fitered Adaptive Backstepping," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 3, pp. 566-580, May. 2012, doi: 10.1109/TCST.2011.2121907.
[45] J. Yu, P. Shi, C. Lin, and H. Yu, "Adaptive Neural Command Filtering Control for Nonlinear MIMO Systems With Saturation Input and Unknown Control Direction," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2536-2545, June 2020, doi: 10.1109/TCYB.2019.2901250.

Maryam Shahriari-kahkeshi received her M.Sc. and Ph.D degrees in control engineering from Isfahan University of Technology, Isfahan, Iran in 2010 and 2014, respectively. She is currently an Associate Professor with the Faculty of Engineering, Shahrekord University, Shahrekord, Iran. Her research interests include artificial intelligence, nonlinear control systems, cyber-physical systems, fault tolerant control systems, and resilient control systems design.

Seyed Hojat Nourian received his BSc. in Electrical Engineering from Water and Electricity Industry Training Complex, Isfahan, Iran in 2013, and MSc. in Control Engineering from Shahrekord University, Shahrekord, Iran in 2025. His research interests are cyber-physical systems, cyber-attacks and resilient control systems under cyber-attacks.