IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE SYSTEMS, MAN AND CYBERNETICS SOCIETY SECTION

Received March 3, 2022, accepted March 19, 2022, date of publication March 23, 2022, date of current version March 30, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3161672

Adaptive Neural Security Control for Networked Singular Systems Under Deception Attacks

WENGANG AO[1], (Member, IEEE), HUIYAN ZHANG[1], (Member, IEEE), NING ZHAO[2], AND LUIS I. MINCHALA[3], (Senior Member, IEEE)

[1]National Research Base of Intelligent Manufacturing Service, Chongqing Technology and Business University, Chongqing 400067, China
[2]College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin, Heilongjiang 150001, China
[3]Department of Electrical Electronics and Telecommunications Engineering, University of Cuenca, Cuenca 010105, Ecuador

Corresponding author: Huiyan Zhang (huiyanzhang@ctbu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62003062; in part by the Science and Technology Research Project of Chongqing Municipal Education Commission under Grant KJZD-M201900801 and Grant KJQN201900831; in part by the Chongqing Natural Science Foundation under Grant cstc2020jcyj-msxmX0077; in part by the High-Level Talents Research Project of Chongqing Technology and Business University (CTBU) under Grant 1953013, Grant 1956030, and Grant ZDPTTD201918; in part by the Science and Technology Partnership Program of the Ministry of Science and Technology (MOST) under Grant KY201802006; and in part by the Open Fund Project of Chongqing Key Laboratory of Manufacturing Equipment Mechanism Design and Control under Grant 1556031.

ABSTRACT This paper studies the issue of the adaptive neural security controller design for uncertain networked singular systems in the presence of deception attacks. Considering that the attack signal is unknown, the neural networks technique is exploited to approximate the attack signal, which eliminates the assumption that the attack signal has a known upper bound. By combining the state feedback with the estimated information of the attack, the impact of the attack is effectively compensated. Furthermore, a novel Lyapunov function, including the decomposed state vector and the weight matrix estimation error, is established to evaluate the bounded area of the system state. Finally, a numerical example substantiates the validity of the theoretical results.

INDEX TERMS Networked singular systems, neural networks, security control, deception attacks.

I. INTRODUCTION

Singular systems, also widely called descriptor systems, can be transformed into a differential equation and an algebraic equation through matrix transformation to describe the dynamic and static characteristics of the system respectively [1]. Normal system equations only contain dynamic characteristics and do not involve static responses between variables. Therefore, from a certain perspective, the singular system model can describe the working process of the practical physical system more concretely and vividly than the normal system model. When considering and analyzing singular systems, this also makes the problems faced more complicated than normal systems [2], [3]. With the development of wireless communication technology, the transmission of signal commands between system components has gradually tended to communicate through network channels. Combining it with the field of control, networked singular systems have been widely used in industrial processes [4], electric power grids [5] and other fields [6]–[10]. However, the introduction of wireless networks also brings new challenges to the analysis and synthesis of networked systems [11]. In particular, the detection and defense of networked attacks in networked systems have attracted extensive research interest from scholars in recent years.

Generally speaking, cyber-attacks will adversely affect the stability of networked systems. From the perspective of attackers, network channels are most prone to two attack modes: denial of service (DoS) attacks [12], [13] and deception attacks [14], [15]. The impact of DoS attacks is mainly reflected in the blocking of the communication channel and suspending signal transmission, which will cause the system to be in an out-of-control scenario for a long time, and even seriously affect people's normal life and cause significant economic losses [16]–[18]. For deception attacks, its main purpose is to tamper with the real signal while injecting false signals. Affected by it, the system will deviate from the stable state and eventually lead to the paralysis of the entire system or server. Usually, deception attacks have more subtle characteristics to destroy the performance of the system [19].

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su.

As a result, security control has become an important defense method to resist the impact of attacks on networked systems. The reference [20] considered the guaranteed cost security control of discrete-time stochastic nonlinear systems under deception attacks. The reference [21] proposed an adaptive control method to defend against the impact of attacks, which is different from the above-mentioned method of dealing with attacks in [20]. In the network-induced problems, there are not only security threats, but also network bandwidth limitations [22]–[24]. For this reason, the problem of event-triggered path tracking control for autonomous vehicles under deception attacks was studied in [24]. A learning-based event-triggered control strategy was proposed to improve resource utilization efficiency and achieve tracking performance under deception attacks.

All the references discussed above assume that deception attacks are bounded or known, which limits the scope of application of the proposed method [25], [26]. According to the characteristics of deception attack, it can be regarded as an unknown nonlinear function related to the state. A mature technique-neural networks [27], [28] can be used to approximate an unknown nonlinear function and the adaptive technique is utilized to estimate unknown parameters. Some remarkable results have been reported in [29]–[34]. In [29], for an uncertain networked nonlinear systems, the model-based adaptive event-triggered controller was designed to solve the stabilization problem and save communication resources. For uncertain switched nonstrict-feedback nonlinear systems, the authors in [30] addressed the adaptive asymptotic tracking control problem by using backstepping approach and common Lyapunov function strategy. In practice, the state of the system is not completely measurable. To this end, taking switched systems under quantized measurements into consideration, [31] focused on the adaptive neural network unknown input observer design problem. By adaptively adjusting the controller parameters, the tracking error of the second-order strictly nonlinear system can reach an arbitrarily small range [32]–[34]. Based on these existing results, a natural idea is to use these techniques to deal with deception attacks. Specially, in the controller design, the approximated signal can be used as an input to compensate for the impact of the attack. Some previous results have used neural networks technique to deal with deception attack signals. The reference [35] has studied the neural networks-based security control problem for stochastic system under mixed attacks. The reference [36] has developed neural networks distributed security filters for networked switching systems in the presence of deception attacks. As we can see, neural networks-based security control issues have paid little attention to discrete-time networked singular systems under deception attacks, which inspires our interest.

In this paper, we provide a design strategy of the neural networks-based security controller for uncertain networked singular systems under deception attacks. The main contribution of this paper is concluded as follows:

a. The state decomposition approach is used to construct a novel Lyapunov function with fewer decision variables.
b. Different from the existing works for resisting deception attacks [37], [38], neural networks method is applied to approximate unknown attack signals, which will deal with the impact of attacks more intelligently.
c. Some feasible matrix inequality conditions are proposed to ensure that networked singular systems are regular, impulse-free and bounded.

The reminder of this paper is given as follows: The problem formulation including system description and the framework of the considered control strategy is given in Section II. The main results on how to design the adaptive neural security controller are presented in Section III and the effectiveness of the designed control strategy is estimated using simulation studies in Section IV. Finally, authors conclude this paper in Section V.

Notations: The notations $\mathbb{R}^{n\times m}$ and $\mathbb{R}^n$ denote the space of all $n \times m$-dimensional real matrices and n-dimensional Euclidean space, respectively. I_n and $0_{n\times m}$ stand for the $n \times n$-dimensional identity matrix and the $n \times m$-dimensional zero matrix, respectively. $\mathcal{P} > 0$ (< 0) means that $\mathcal{P}$ is a real positive (negative)-definite matrix. The symbols $\|\cdot\|$ and $\|\cdot\|_F$ represent the Euclidean vector norm and Frobenius norm, respectively.

II. PROBLEM FORMULATION

A. SYSTEM DESCRIPTION

Consider the following networked singular system:

$$Ex(k+1) = (A + \Delta A(k))x(k) + (B + \Delta B(k))u(k), \quad (1)$$

where $x(k) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^m$ are the system state vector and the control input, respectively. System matrices A and B are known. Singular matrix $E \in \mathbb{R}^{n\times n}$ satisfies $\text{rank}(E) = r < n$. $\Delta A(k)$ and $\Delta B(k)$ are unknown matrices and satisfy

$$[\Delta A(k)\ \Delta B(k)] = J_1 G(k) [J_2\ J_3], \quad (2)$$

where $J_1 \in \mathbb{R}^{n\times p}$, $J_2 \in \mathbb{R}^{q\times n}$, $J_3 \in \mathbb{R}^{q\times m}$ are known matrices, and the time-varying matrix $G(k)$ is assumed as $G^T(k)G(k) \le I$. In the following analysis, in order to simplify the notation, we use ΔA and ΔB instead of $\Delta A(k)$ and $\Delta B(k)$, respectively.

Due to $\text{rank}(E) = r < n$, there are nonsingular matrices $\mathcal{M}$ and $\mathcal{N}$ such that

$$\mathcal{M}(E, A, \Delta A, B, \Delta B)\mathcal{N} = \left(\begin{bmatrix} I_r & 0 \\ * & 0 \end{bmatrix}, \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}, \begin{bmatrix} \Delta A_1 \\ \Delta A_2 \end{bmatrix}, \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}, \begin{bmatrix} \Delta B_1 \\ \Delta B_2 \end{bmatrix} \right),$$

where

$$\begin{aligned} A_1 &= [A_{11} \quad A_{12}], \quad [\Delta A_i \quad \Delta B_i] = J_1^i G(k)[J_2 \quad J_3], \\ A_2 &= [A_{21} \quad A_{22}], \quad i = 1, 2, \\ \Delta A_1 &= [\Delta A_{11} \quad \Delta A_{12}], \quad J_1^1 \in \mathbb{R}^{r\times p}, \\ \Delta A_2 &= [\Delta A_{21} \quad \Delta A_{22}], \quad J_1^2 \in \mathbb{R}^{(n-r)\times p}. \end{aligned}$$

Let $\mathcal{N}^{-1}x(k) = [\eta_1^T(k)\ \eta_2^T(k)]^T$, we rewrite system (1) as

$$\begin{cases} \eta_1(k+1) &= (A_1+\Delta A_1)\eta(k)+(B_1+\Delta B_1)u(k) \\ 0 &= (A_2+\Delta A_2)\eta(k)+(B_2+\Delta B_2)u(k). \end{cases} \tag{3}$$

B. CONTROLLER UNDER DECEPTION ATTACKS

In this paper, the information transmission channel between the controller and the actuator relies on the network medium, which is susceptible to the influence of deception attacks, specifically manifested as tampering with data and destroying the authenticity of data. The framework of the control strategy under deception attacks is shown in Fig. 1. Under deception attacks, the actuator input can be described as

$$u(k) = \bar{u}(k) + f(\eta(k)),$$

where $f(\eta(k))$ denotes the malicious signal injected by the adversary and is the unknown nonlinear function, and $\bar{u}(k)$ stands for the control signal.

In order to effectively resist the impact of attacks on the system, the key issue is how to identify unknown deception attacks. Here, we use the neural networks method to approximate the unknown nonlinear function, and then use the approximate information to effectively compensate for the impact of the attack. Then, a controller is constructed as

$$\bar{u}(k) = K\eta(k) - \hat{f}(\eta(k)), \tag{4}$$

where $K = [K_1\ K_2]$ is the controller gain to be designed and $\hat{f}(\eta(k))$ is the estimation of $f(\eta(k))$. The known nonlinear function $f(\eta(k))$ is approximately as follows:

$$f(k) = W^T S(\eta(k)) + \delta(\eta(k)),\ \ \eta(k) \in \Omega \subset \mathbb{R}^n, \tag{5}$$

where Ω is a compact set, $W \in \mathbb{R}^{l\times m}$ is the ideal weights of the hidden-to-output layer, $Z \in \mathbb{R}^{n\times l}$ is the ideal weights of input-to-hidden layer, and l is the number of neural networks nodes. And

$$S(\eta(k)) = [S_1(\eta(k)), \ldots, S_l(\eta(k))]^T \in \mathbb{R}^l$$

is the basis function satisfying $||S(\cdot)|| \le S_{\max}$, where $S_{\max}$ is a positive constant, and the form of $S_i(\theta)$ is given as follows:

$$S_i(\eta(k)) = \exp\left(-\frac{\|\eta(k)-v_i\|^2}{\varsigma}\right),$$

where ς is width of function $S_i(\eta(k))$ and $v_i = [v_{i1}, \ldots, v_{in}]^T \in \mathbb{R}^n$ is the center of function $S_i(\eta(k))$. $\delta(\eta(k))$ represents the approximation error with $||\delta(\eta(k))|| \le \bar{\delta}$.

Based on the above description, the neural networks estimation of the unknown function $f(x(k))$ is designed as

$$\hat{f}(k) = \hat{W}^T(k)S(\eta(k)), \tag{6}$$

where $\hat{W}(k) \in \mathbb{R}^{l\times m}$ is the estimation of W. For the needs of subsequent analysis, we design the dynamic response of $\hat{W}(k)$ as follows:

$$\hat{W}(k+1) = -\alpha\hat{W}(k) + \hat{W}(k) - \sigma\rho(k)\eta^T(k)R^T, \tag{7}$$

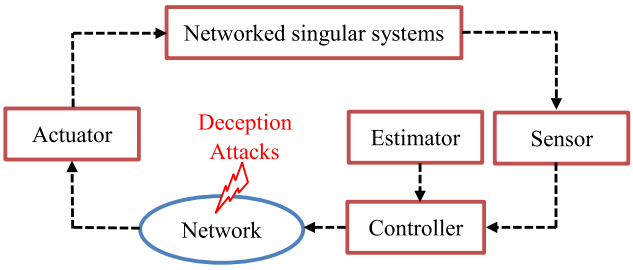

FIGURE 1. The framework of a networked singular system under deception attacks.

where $\sigma > 0$ and $\alpha > 0$ are two scalar parameters, the matrix $R \in \mathbb{R}^{n\times m}$ is an adjustment parameter and

$$\rho(k) = S(\eta(k))/(1 + ||S(\eta(k))||^2||R\eta(k)||^2).$$

Let the estimated error be $\tilde{W}(k) = \hat{W}(k) - W$. Then the dynamic equation of the error can be obtained

$$\tilde{W}(k+1) = -\alpha\hat{W}(k) + \tilde{W}(k) - \sigma\rho(k)\eta^T(k)R^T. \tag{8}$$

Remark 1: Different form the existing works on deception attacks [37], [38], a neural networks method is employed to estimate the unknown attack signal rather than restricting it to be bounded. With the powerful approximation capabilities of neural networks, the estimated information of the attack signal can be effectively used to resist the impact of the attack.

Under deception attacks, the augmented system consisting of system (3), controller (4) and neural networks (5) and (6) is formed as follows:

$$\begin{cases} \eta_1(k+1) = \bar{A}_1\eta(k) + \bar{B}_1\tilde{W}^T(k)S(\eta(k)) + \bar{B}_1\delta(\eta(k)) \\ 0 = \bar{A}_2\eta(k) + \bar{B}_2\tilde{W}^T(k)S(\eta(k)) + \bar{B}_2\delta(\eta(k)) \end{cases} \tag{9}$$

where

$$\begin{aligned} \bar{A}_1 &= A_1 + \Delta A_1 + \bar{B}_1K, \quad \bar{B}_1 = B_1 + \Delta B_1, \\ \bar{A}_2 &= A_2 + \Delta A_2 + \bar{B}_2K, \quad \bar{B}_2 = B_2 + \Delta B_2. \end{aligned}$$

Before proceeding, a lemma and a definition are needed to obtain the main results.

Lemma 1 [39]: Given matrices $U = U^T, \bar{J}_1, \bar{J}_2$ and $G(k)$ satisfying (2). The inequality

$$U + \mathrm{He}\{\bar{J}_1G(k)\bar{J}_2\} < 0$$

holds if and only if there exists a matrix $\Lambda > 0$ such that

$$U + \bar{J}_1\Lambda\bar{J}_1^T + \bar{J}_2^T\Lambda^{-1}\bar{J}_2 < 0.$$

Definition 1 [40]: If $\det(sE - A)$ is not identically 0, and

$$\deg(\det(sE - A)) = \mathrm{rank}(E)$$

holds, then pair (E, A) is said to be regular and causal.

III. MAIN RESULTS

In this section, two theorems will give sufficient conditions for the system (9) to be uniform and ultimately bounded under the presence of deception attacks. Based on the results of Theorem 1, Theorem 2 gives a design scheme for the control gain.

Theorem 1: For given a constant $\alpha > 0$, if there exist constants $\varepsilon > 0$, $\lambda > 0$, $\upsilon > 0$, and matrices $P > 0$, $H_1, H_2 \in \mathbb{R}^{r\times r}$, $H_3, H_4 \in \mathbb{R}^{r\times(n-r)}$, $H_5 \in \mathbb{R}^{(n-r)\times(n-r)}$, the following inequalities satisfy

$$-\lambda\alpha + \frac{\lambda}{4\varepsilon} + \upsilon S_{\max}^2 < 0, \tag{10}$$

$$\begin{bmatrix} \Phi_1 & \Phi_2 \\ * & -I_{p+m} \end{bmatrix} < 0, \tag{11}$$

where

$$\begin{aligned}
\Phi_1 &= -e_1^T P e_1 + e_2^T P e_2 - \upsilon e_4^T e_4 + F_1^T F_1 \\
&\quad + \mathrm{He}\Big\{\big[e_1^T H_1 + e_2^T H_2\big]\big[(A_1 + B_1K)E_1 + B_1 e_4 - e_2\big] \\
&\quad + \big[e_1^T H_3 + e_2^T H_4 + e_3^T H_5\big]\big[(A_2 + B_2K)E_1 + B_2 e_4\big]\Big\}, \\
E_1 &= \begin{bmatrix} e_1^T & e_3^T \end{bmatrix}^T, \quad F_1 = (J_2 + J_3K)\,E_1 + J_3 e_4, \\
M &= \Big(e_1^T H_1 + e_2^T H_2\Big) J_1^1 + \Big(e_1^T H_3 + e_2^T H_4 + e_3^T H_5\Big) J_1^2, \\
N &= \Big(e_1^T H_1 + e_2^T H_2\Big) B_1 + \Big(e_1^T H_3 + e_2^T H_4 + e_3^T H_5\Big) B_2, \\
e_1 &= \begin{bmatrix} I_r & 0_{r\times r} & 0_{r\times(n-r)} & 0_{r\times m} \end{bmatrix}, \ \Phi_2 = [\sqrt{2}M \quad N], \\
e_2 &= \begin{bmatrix} 0_{r\times r} & I_r & 0_{r\times(n-r)} & 0_{r\times m} \end{bmatrix}, \\
e_3 &= \begin{bmatrix} 0_{(n-r)\times r} & 0_{(n-r)\times r} & I_{n-r} & 0_{(n-r)\times m} \end{bmatrix}, \\
e_4 &= \begin{bmatrix} 0_{m\times r} & 0_{m\times r} & 0_{m\times(n-r)} & I_m \end{bmatrix},
\end{aligned}$$

then the system in (9) under deception attacks is bounded.

Proof: It can be verified that system (9) are regular and impulse-free. Based on $\Phi_1 < 0$ in (10), we have

$$\mathrm{He}\{H_5(A_{22} + B_2K_2)\} < 0,$$

which implies that $(A_{22} + B_2K_2)$ is nonsingular. As a result, system (9) is regular and impulse-free.

Now, we analyze that system (9) under deception attacks is bounded. Construct the Lyapunov function as

$$V(k) = V_1(k) + \lambda V_2(k), \tag{12}$$

with

$$V_1(k) = \eta_1^T(k) P \eta_1(k), \quad V_2(k) = \mathrm{Tr}\{\tilde{W}^T(k)\tilde{W}(k)\}.$$

The difference of $V_1(k)$ along (9) can be derived as

$$\begin{aligned}
\Delta V_1(k) &= V_1(k+1) - V_1(k) \\
&= \eta_1^T(k+1) P \eta_1(k+1) - \eta_1^T(k) P \eta_1(k).
\end{aligned} \tag{13}$$

Calculating the difference of $V_2(k)$ along (8), it follows that

$$\begin{aligned}
&\Delta V_2(k) \\
&= V_2(k+1) - V_2(k) \\
&= \mathrm{Tr}\left\{\tilde{W}^T(k+1)\tilde{W}(k+1)\right\} - \mathrm{Tr}\left\{\tilde{W}^T(k)\tilde{W}(k)\right\} \\
&= \mathrm{Tr}\Big\{\alpha^2 \hat{W}^T(k)\hat{W}(k) - 2\alpha \hat{W}^T(k)\tilde{W}(k) \\
&\quad + 2\alpha\sigma \hat{W}^T(k)\rho(k)R\eta(k) - 2\sigma \tilde{W}^T(k)\rho(k)R\eta(k)\Big\} \\
&\quad + \sigma^2 ||\rho(k)||^2 ||R\eta(k)||^2,
\end{aligned} \tag{14}$$

where $\rho(k)$ is defined in (7). Note that

$$||\rho(k)||^2 ||R\eta(k)||^2 \le \frac{1}{4}.$$

With this, we have

$$\begin{aligned}
\mathrm{Tr}\Big\{2\alpha\sigma \hat{W}^T(k)\rho(k)R\eta(k)\Big\} &\le \alpha \mathrm{Tr}\Big\{\hat{W}^T(k)\hat{W}(k)\Big\} + \frac{\alpha\sigma^2}{4}, \\
-\mathrm{Tr}\Big\{2\sigma \tilde{W}^T(k)\rho(k)R\eta(k)\Big\} &\le \frac{\mathrm{Tr}\Big\{\tilde{W}^T(k)\tilde{W}(k)\Big\}}{4\varepsilon} + \varepsilon\sigma^2.
\end{aligned} \tag{15}$$

Rewrite the term $\mathrm{Tr}\{-2\alpha \hat{W}^T(k)\tilde{W}(k)\}$ as

$$\begin{aligned}
&\mathrm{Tr}\left\{-2\alpha \hat{W}^T(k)\tilde{W}(k)\right\} \\
&\quad = \mathrm{Tr}\left\{\alpha W^T W - \alpha \tilde{W}^T(k)\tilde{W}(k) - \alpha \hat{W}^T(k)\hat{W}(k)\right\}.
\end{aligned} \tag{16}$$

With the help of (14)–(16), the difference of $V_2(k)$ can be continued as

$$\Delta V_2(k) \le -(\alpha - \frac{1}{4\varepsilon})||\tilde{W}(k)||_F^2 + \mu, \tag{17}$$

where $\mu = \alpha||W||_F^2 + (\frac{\alpha+1}{4} + \varepsilon)\sigma^2$.

For any matrices H_j, $j = 1, 2, \ldots, 5$, with appropriate dimensions, we have

$$\begin{aligned}
0 &= 2\Big[\eta_1^T(k)H_1 + \eta_1^T(k+1)H_2\Big]\Big[-\eta_1(k+1) + \bar{A}_1\eta(k) \\
&\quad + \bar{B}_1\tilde{W}^T(k)S(\eta(k)) + \bar{B}_1\delta(\eta(k))\Big] \\
&= 2\zeta^T(k)\Big[e_1^T H_1 + e_2^T H_2\Big]\Big[-e_2 + \bar{A}_1E_1 + \bar{B}_1 e_4\Big]\zeta(k) \\
&\quad + 2\zeta^T(k)\Big[e_1^T H_1 + e_2^T H_2\Big]\bar{B}_1\delta(\eta(k)),
\end{aligned} \tag{18}$$

$$\begin{aligned}
0 &= 2\Big[\eta_1^T(k)H_3 + \eta_1^T(k+1)H_4 + \eta_2^T(k)H_5\Big] \\
&\quad \times\Big[\bar{A}_2\eta(k) + \bar{B}_2\tilde{W}^T(k)S(\eta(k)) + \bar{B}_2\delta(\eta(k))\Big] \\
&= 2\zeta^T(k)\Big[e_1^T H_3 + e_2^T H_4 + e_3^T H_5\Big]\Big[\bar{A}_2E_1 + \bar{B}_2 e_4\Big]\zeta(k) \\
&\quad + 2\zeta^T(k)\Big[e_1^T H_3 + e_2^T H_4 + e_3^T H_5\Big]\bar{B}_2\delta(\eta(k)),
\end{aligned} \tag{19}$$

where

$$\zeta^T(k) = \Big[\eta_1^T(k) \quad \eta_1^T(k+1) \quad \eta_2^T(k) \quad S^T(\eta(k))\tilde{W}(k)\Big]^T.$$

By virtue of (2), it is obtained from (18) and (19) that

$$\begin{aligned}
0 &= \zeta^T(k)\mathrm{He}\Big\{\big[e_1^T H_1 + e_2^T H_2\big]\big[-e_2 + (A_1 + B_1K)E_1 \\
&\quad + B_1 e_4 + J_1^1 G(k) F_1\big]\Big\}\zeta(k) + 2\zeta^T(k) \\
&\quad \times\big[e_1^T H_1 + e_2^T H_2\big]\big[B_1 + J_1^1 G(t) J_3\big]\delta(\eta(k)),
\end{aligned} \tag{20}$$

$$\begin{aligned}
0 &= 2\zeta^T(k)\mathrm{He}\Big\{\big[e_1^T H_3 + e_2^T H_4 + e_3^T H_5\big]\big[(A_2 + B_2K)E_1 \\
&\quad + B_2 e_4 + J_1^2 G(k) F_1\big]\Big\}\zeta(k) + 2\zeta^T(k)\big[e_1^T H_3 \\
&\quad + e_2^T H_4 + e_3^T H_5\big]\big[B_2 + J_1^2 G(t) J_3\big]\delta(\eta(k)).
\end{aligned} \tag{21}$$

Notice that for any a constant $\upsilon > 0$, it is clear that

$$-\upsilon S^T(\eta(k))\tilde{W}(k)\tilde{W}^T(k)S(\eta(k)) + \upsilon S_{\max}^2 \mathrm{Tr}\left\{\tilde{W}^T(k)\tilde{W}(k)\right\} I_n \geq 0. \quad (22)$$

Applying Lemma 1 and combining (12), (13), (17) and (20)–(22), we derive

$$\Delta V(k) \leq \zeta^T(k)[\Phi + M^T M + N^T N + \mathrm{He}\{MG(t)F_1\}]\zeta(k) + \bar{\mu}, \quad (23)$$

where $\bar{\mu} = \lambda\mu + (1 + \lambda_{\max}(J_3^T J_3))\bar{\delta}$. According to the condition of the theorem and using Schur complement, there exists a small scalar $\nu > 0$, such that

$$\Delta V(k) \leq -\nu V(k) + \bar{\mu},$$

which means that system (9) is bounded. The proof is completed. ■

By Theorem 1, the following result is given to design the controller.

Theorem 2: For given constants $\alpha > 0$, $\beta > 0$ and $\chi > 0$, if there exist constants $\varepsilon > 0$, $\lambda > 0$, $\upsilon > 0$, and matrices $\bar{P} > 0$, $Y = [Y_1\ Y_2]$, $Z = \mathrm{diag}\{Z_1, Z_2\} \in \mathbb{R}^{n\times n}$, $L_1, L_2 \in \mathbb{R}^{r\times(n-r)}$, such that (10) and the following inequality hold:

$$\begin{bmatrix} \bar{\Phi}_1 & \bar{\Phi}_2 \\ * & -I_{\bar{n}} \end{bmatrix} < 0 \quad (24)$$

where

$$\begin{aligned}
\bar{\Phi}_1 &= -e_1^T\bar{P}e_1 + e_2^T\bar{P}e_2 + \mathrm{He}\Big\{\big[e_1^T + \beta e_2^T\big]\big[-Z_1e_2 \\
&\quad +(A_1ZE_1 + B_1YE_1) + B_1e_4\big] + e_3^T\bar{F}_3\Big\} - \upsilon e_4^T e_4, \\
\bar{\Phi}_2 &= [\sqrt{2}\bar{M} \quad \bar{N} \quad \bar{F}_1^T \quad \bar{F}_2 \quad \bar{F}_3], \\
\bar{F}_1 &= (J_2Z + J_3Y)E_1 + J_3e_4,\ \bar{F}_2 = \chi(e_1^TL_1 + e_2^TL_2), \\
\bar{F}_3^T &= \chi^{-1}\big[(A_2Z + B_2Y)E_1 + B_2e_4\big], \\
\bar{M} &= (e_1^T + \beta e_2^T)J_1^1 + e_3^TJ_1^2 + (e_1^TL_1 + e_2^TL_2)J_1^2, \\
\bar{N} &= (e_1^T + \beta e_2^T)B_1 + e_3^TB_2 + (e_1^TL_1 + e_2^TL_2)B_2, \\
\bar{n} &= 2(n-r) + p + m + q,
\end{aligned}$$

then the system in (9) under deception attacks is bounded and the controller gain can be obtained by

$$K = YZ^{-1}.$$

Proof: Let

$$\begin{cases} Z = \mathrm{diag}\{Z_1, Z_2\} = \mathrm{diag}\left\{H_1^{-T}, H_5^{-T}\right\}, \\ L = \begin{bmatrix} L_1^T & L_2^T \end{bmatrix}^T = Z_1^T\begin{bmatrix} H_3^T & H_4^T \end{bmatrix}^T, \\ \bar{P} = Z_1^TPZ_1, \quad H_2 = \beta H_1, \end{cases}$$

pre- and post-multiplying (11) with $\Psi^T = \mathrm{diag}\{Z_1^T, Z_1^T, Z_2^T, I_{2m+p}\}$ and Ψ, respectively, yields

$$\begin{bmatrix} \tilde{\Phi}_1 & \tilde{\Phi}_2 \\ * & -I_{p+m} \end{bmatrix} < 0, \quad (25)$$

where

$$\begin{aligned}
\tilde{\Phi}_1 &= -e_1^T\bar{P}e_1 + e_2^T\bar{P}e_2 - \upsilon e_4^Te_4 + \tilde{F}_1^T\tilde{F}_1 \\
&\quad +\mathrm{He}\Big\{\big[e_1^T + \beta e_2^T\big]\big[(A_1 + B_1K)ZE_1 - Z_1e_2 + B_1e_4\big] \\
&\quad +\big[e_1^TZ_1^TH_3 + e_2^TZ_1^TH_4 + e_3^T\big]\big[(A_2 + B_2K)ZE_1 \\
&\quad +B_2e_4\big]\Big\}, \\
\tilde{F}_1 &= (J_2 + J_3K)ZE_1 + J_3e_4, \quad \tilde{\Phi}_2 = [\sqrt{2}\bar{M} \quad \bar{N}].
\end{aligned}$$

Denote $K = YZ^{-1}$. Substituting it to (25) and using Schur complement, (24) can ensure that (11) holds. The proof is completed. ■

Remark 2: In contrast to state feedback, the dual-channel feedback, i.e. state feedback and the estimator-based state feedback, is more helpful to compensate the impact of attacks on system performance, which will be shown in the numerical simulation.

Remark 3: This paper is different from the existing results [35], [36] in the following two aspects:

1. The system models considered are different. Specifically, networked Markov jump systems were studied in [35] and networked switched systems were investigated in [36]. However, in this paper, networked singular system is considered.

2. The issues considered are different. The event-triggered controller and distributed security filtering design issues were discussed in [35], [36], respectively, however in the current work, the robust controller design problem is addressed.

IV. SIMULATION STUDIES

In this section, a numerical example is provided to illustrate the effectiveness of the adaptive neural security controller for networked singular system under deception attacks.

Consider singular system (1) with

$$E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ A = \begin{bmatrix} -1 & 1 & 0 \\ 0.3 & -2.5 & -4 \\ -0.1 & 0.3 & -3.8 \end{bmatrix},$$
$$B = \begin{bmatrix} 1.5 & 1 & 1 \end{bmatrix}^T,$$

and the uncertain parameters described as

$$J_1 = \begin{bmatrix} -0.1 & 0.1 & 0.1 \end{bmatrix}^T,\ J_2 = 0.01\begin{bmatrix} 0.5 & 1 & 1 \end{bmatrix},$$
$$J_3 = 0.02,\ G(k) = \sin(0.1k\pi).$$

Based that the above information, we can obtain $\mathcal{M} = \mathcal{N} = I_3$, which means that $x(k) = \eta(k)$. Other parameters are taken as $\beta = 1.8$, $\upsilon = 80$, and $\chi = 10$. By using Theorem 2, the controller gain is obtained

$$K = \begin{bmatrix} -0.5790 & 3.2069 & 5.8619 \end{bmatrix}.$$

Let the initial condition of system (1) is $x(0) = [0.5\ 0.4\ 0.2]^T$. We assume the malicious attack signal as

$$f(x(k)) = 0.8\sqrt{x_1^2(k) + x_2^2(k)} + \sin(x_1(k)).$$

The neural networks for approximating $f(x(k))$ includes 81 nodes with the centers v_1 and v_2 evenly spaced in

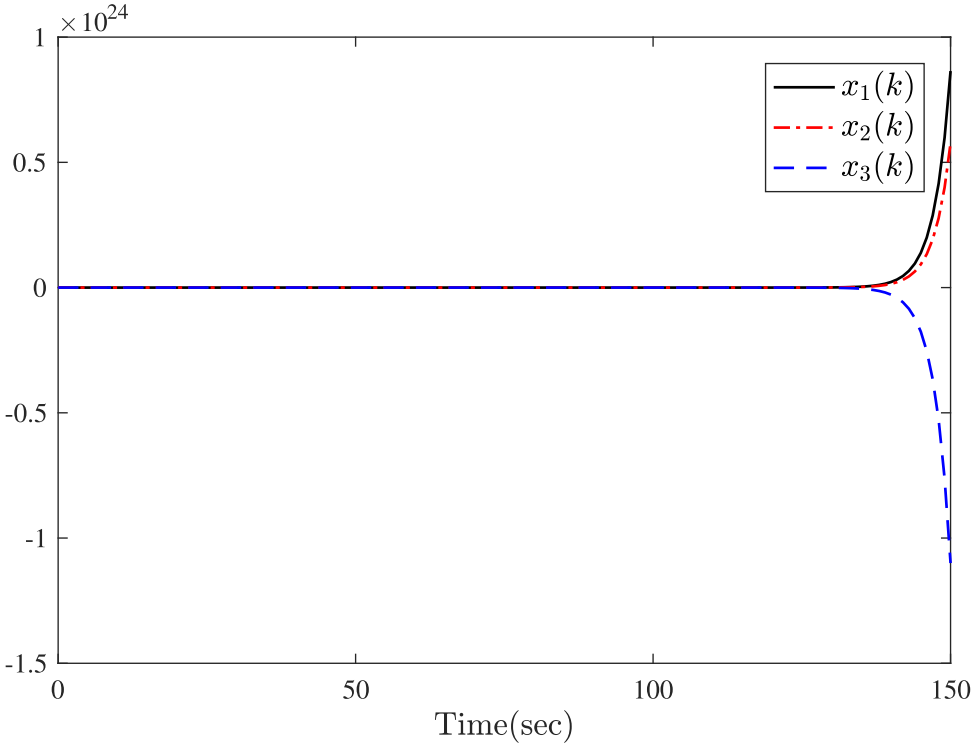

FIGURE 2. The states of the system with state feedback and deception attack.

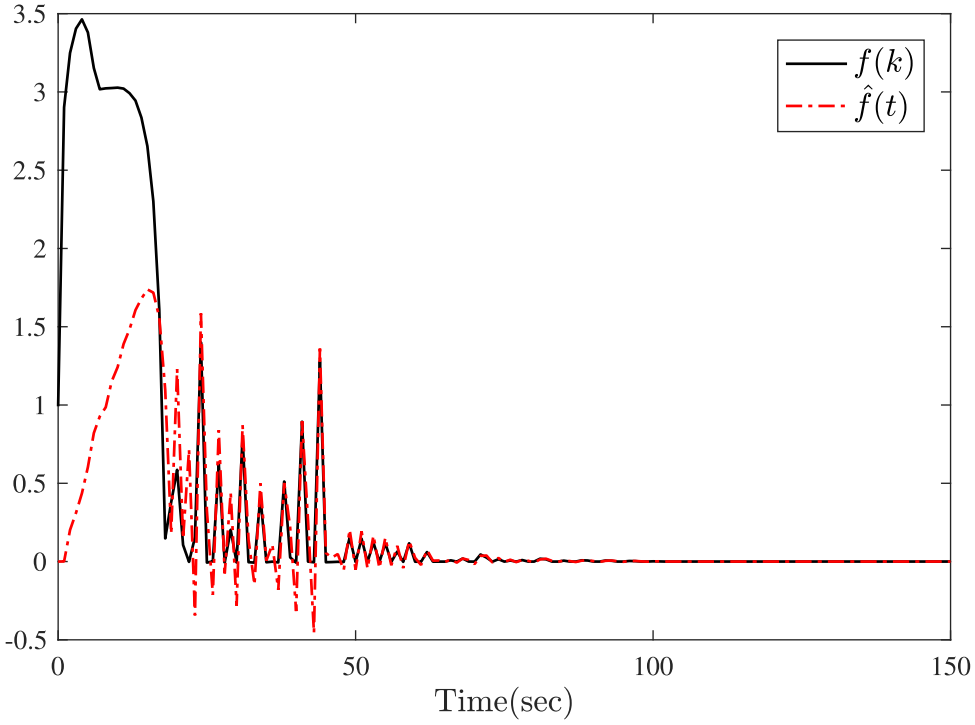

FIGURE 3. The attack signal and its estimated signal.

$[-5.5, 5.5] \times [-5.5, 5.5]$ and width $\varsigma = 2$. The initial weight is set as $\hat{W}(0) = 0_{81\times 1}$. The design parameters are taken as $\alpha = 0.01$, $\sigma = 0.25$ and $R = [-1\ 1]$. Under deception attack, the state of the system with a state feedback $Kx(k)$ is given in Fig. 2. We can see that the feedback control fails and the attack is severely causing the system to destabilize. In order to resist the impact of the attack on the system, neural networks method is used to approximate the attack signal. Meanwhile, the approximate information is used to compensate the impact of the attack on the system performance in

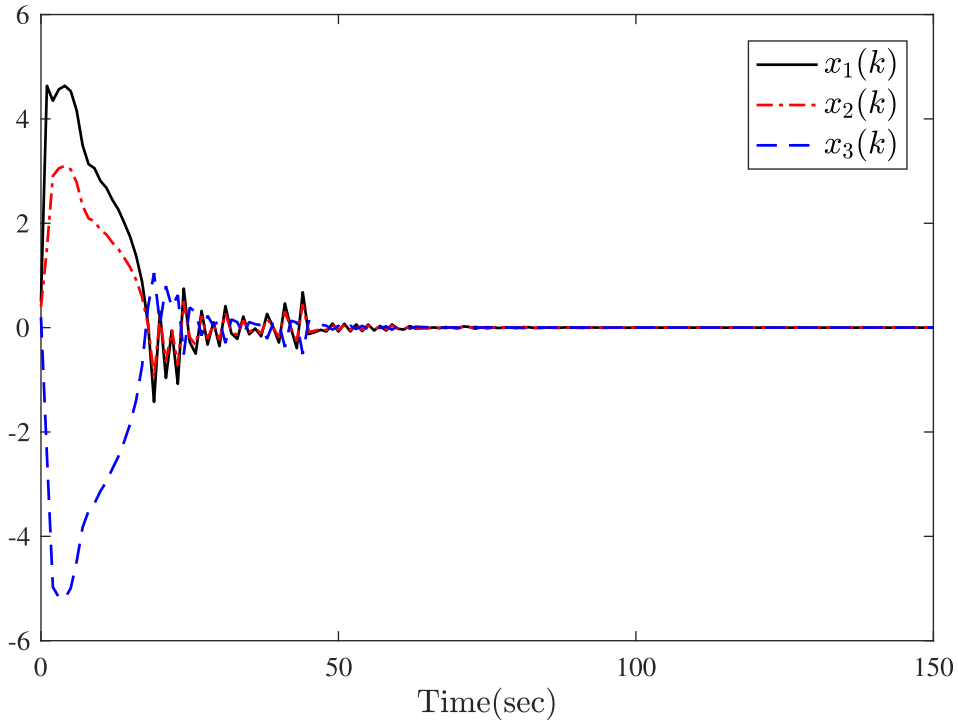

FIGURE 4. The states of the system with controller (4) and deception attack.

the process of designing the controller. The attack signal and its estimated signal are plotted in Fig. 3, from which we can clearly see that after 50 seconds, the neural network can better approximate the attack signal. This facilitates effective resistance to the attack signal. The state of the system with the controller (4) and deception attack are recorded in Fig. 4, from which we can observe that that the state $x(t)$ still remain bounded.

V. CONCLUSION

This paper has studied the problem of adaptive neural security control for networked singular systems with structure uncertainties and deception attacks. For the sake of estimating the deception attack signal, the neural networks technique has been used to approximate the unknown nonlinear function. With the help of the state decomposition method, the underlying system is decomposed into fast and slow subsystems to construct an appropriate Lyapunov function. Then, sufficient conditions have been provided to guarantee the closed-loop system is regular, impulse free and bounded in the presence of deception attacks. Furthermore, the control gain has been designed by solving the linear matrix inequalities. Finally, the effectiveness of the proposed method has been demonstrated by simulation analysis. One possible future topic is to investigate the adaptive event-triggered-based neural security control problem for networked singular systems under multiple cyber-attacks.

REFERENCES

[1] L. Dai, Ed., *Singular Control Systems*. Berlin, Germany: Springer, 1989.

[2] S. Xu, P. Van Dooren, R. Stefan, and J. Lam, "Robust stability and stabilization for singular systems with state delay and parameter uncertainty," *IEEE Trans. Autom. Control*, vol. 47, no. 7, pp. 1122–1128, Jul. 2012.

[3] Z. Gao and D. W. C. Ho, "State/noise estimator for descriptor systems with application to sensor fault diagnosis," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1316–1326, Apr. 2006.

[4] Z. Du, D. Yue, and S. Hu, "H_∞ stabilization for singular networked cascade control systems with state delay and disturbance," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 882–894, May 2014.

[5] F. D. Freitas, N. Martins, S. L. Varricchio, J. Rommes, and F. C. Véliz, "Reduced-order transfer matrices from RLC network descriptor models of electric power grids," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 1905–1916, Nov. 2011.

[6] M. Sathishkumar and Y.-C. Liu, "Resilient annular finite-time bounded and adaptive event-triggered control for networked switched systems with deception attacks," *IEEE Access*, vol. 9, pp. 92288–92299, 2021.

[7] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 158–167, Mar. 2021.

[8] R. Yang, L. Li, and P. Shi, "Dissipativity-based two-dimensional control and filtering for a class of switched systems," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 5, pp. 2737–2750, May 2021.

[9] L. Zhang, Y. Zhu, and W. X. Zheng, "Synchronization and state estimation of a class of hierarchical hybrid neural networks with time-varying delays," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 2, pp. 459–470, Feb. 2016.

[10] Y. Zhu, W. X. Zheng, and D. Zhou, "Quasi-synchronization of discrete-time Lur'e-type switched systems with parameter mismatches and relaxed PDT constraints," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 2026–2037, May 2020.

[11] L. Zhang, M. Chen, and B. Wu, "Observer-based controller design for networked control systems with induced delays and data packet dropouts," *ICIC Exp. Lett., B, Appl.*, vol. 12, no. 3, pp. 243–253, 2021.

[12] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[13] H. S. Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated DoS signals," *SIAM J. Control Optim.*, vol. 54, no. 6, pp. 3084–3105, Jan. 2016.

[14] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.
[15] E. Tian and C. Peng, "Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, Nov. 2020.
[16] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.
[17] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.
[18] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy," *IEEE Trans. Autom. Control*, vol. 65, no. 8, pp. 3714–3721, Aug. 2020.
[19] H. Song, P. Shi, W. Zhang, C. Lim, and L. Yu, "Distributed H_∞ estimation in sensor networks with two-channel stochastic attacks," *IEEE Trans. Cybern.*, vol. 50, no. 2, pp. 465–475, Feb. 2020.
[20] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, May 2016.
[21] Y. Yang, J. Huang, X. Su, K. Wang, and G. Li, "Adaptive control of second-order nonlinear systems with injection and deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 1, pp. 574–581, Jan. 2022.
[22] Y. Zhu, Z. Zhong, X. Z. Wei, and D. Zhou, "HMM-based $\mathcal{H}_\infty$ filtering for discrete-time Markov jump LPV systems over unreliable communication channels," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2035–2046, Dec. 2018.
[23] R. Yang and W. X. Zheng, "Output-based event-triggered predictive control for networked control systems," *IEEE Trans. Ind. Electron.*, vol. 67, no. 12, pp. 10631–10640, Dec. 2020.
[24] Z. Gu, T. Yin, and Z. Ding, "Path tracking control of autonomous vehicles subject to deception attacks via a learning-based event-triggered mechanism," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 12, pp. 5644–5653, Dec. 2021.
[25] L. Celentano, M. V. Basin, and P. Shi, "Majorant-based control methodology for mechatronic and transportation processes," *IEEE Access*, vol. 9, pp. 157916–157939, 2021.
[26] J. Pongfai, W. Assawinchaichote, P. Shi, and X. Su, "Novel D-SLP controller design for nonlinear feedback control," *IEEE Access*, vol. 8, pp. 128796–128808, 2020.
[27] H. Dyoniputri and Afiahayati, "A hybrid convolutional neural network and support vector machine for dysarthria speech classification," *Int. J. Innov. Comput., Inf. Control*, vol. 17, no. 1, pp. 111–123, 2021.
[28] L. Yao, Z. Gu, and H. Wang, "Integrated fault diagnosis and fault-tolerant control of nonlinear network control systems," *Int. J. Innov. Comput., Inf. Control*, vol. 16, no. 4, pp. 1385–1398, 2020.
[29] Z. Chen, B. Niu, X. Zhao, L. Zhang, and N. Xu, "Model-based adaptive event-triggered control of nonlinear continuous-time systems," *Appl. Math. Comput.*, vol. 408, Nov. 2021, Art. no. 126330.
[30] N. Xu, X. Zhao, G. Zong, and Y. Wang, "Adaptive control design for uncertain switched nonstrict-feedback nonlinear systems to achieve asymptotic tracking performance," *Appl. Math. Comput.*, vol. 408, Nov. 2021, Art. no. 126344.
[31] L. Chen, Y. Zhu, and C. K. Ahn, "Adaptive neural network-based observer design for switched systems with quantized measurements," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Dec. 10, 2021, doi: 10.1109/TNNLS.2021.3131412.
[32] N. Lu, X. Sun, X. Zheng, and Q. Shen, "Command filtered adaptive fuzzy backstepping fault-tolerant control against actuator fault," *ICIC Exp. Lett.*, vol. 15, no. 4, pp. 357–365, 2021.
[33] X. Zheng, Q. Shen, X. Sun, and Q. Fu, "Adaptive fault tolerant control for a class of high-order nonlinear systems," *ICIC Exp. Lett.*, vol. 14, no. 9, pp. 861–866, 2020.
[34] S. Oucheriah, "Robust adaptive output feedback controller for a quadratic boost converter," *ICIC Express Lett., Appl.*, vol. 10, no. 9, pp. 789–795, Sep. 2019.
[35] X. Gao, F. Deng, P. Zeng, and H. Zhang, "Adaptive neural event-triggered control of networked Markov jump systems under hybrid cyberattacks," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Aug. 24, 2021, doi: 10.1109/TNNLS.2021.3105532.
[36] H. Shang, G. Zong, and K. Shi, "Neural-network-based distributed security filtering for networked switched systems," *Int. J. Robust Nonlinear Control*, vol. 32, no. 5, pp. 2791–2804, Mar. 2022, doi: 10.1002/rnc.5554.
[37] J. Liu, Y. Gu, J. Cao, and S. Fei, "Distributed event-triggered H_∞ filtering over sensor networks with sensor saturations and cyber-attacks," *ISA Trans.*, vol. 81, pp. 63–75, Oct. 2018.
[38] K. Liu, H. Guo, Q. Zhang, and Y. Xia, "Distributed secure filtering for discrete-time systems under round-robin protocol and deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3571–3580, Aug. 2020.
[39] L. Xie, M. Fu, and C. E. de Souza, "H_∞ control and quadratic stabilization of systems with parameter uncertainty via output feedback," *IEEE Trans. Autom. Control*, vol. 37, no. 8, pp. 1253–1256, Aug. 1992.
[40] S. Xu and C. Yang, "Stabilization of discrete-time singular systems: A matrix inequalities approach," *Automatica*, vol. 35, no. 9, pp. 1613–1617, Sep. 1999.

WENGANG AO (Member, IEEE) received the B.S. degree in engineering mechanics from Sichuan University, Chengdu, in June 2000, and the M.E. degree in solid mechanics from Chongqing University, Chongqing, in June 2007. He is currently an Associate Professor with Chongqing Technology and Business University. His research interests include strength theory, kinematics and dynamics, robust control, and intelligent robots.

HUIYAN ZHANG (Member, IEEE) received the M.Sc. degree in control engineering and the Ph.D. degree in control theory and control engineering from the Harbin Institute of Technology, Harbin, in September 2014 and April 2019, respectively. From September 2015 to September 2017, she was a joint training Ph.D. student with the School of Electrical and Electronic Engineering, The University of Adelaide. She is currently an Associate Professor with Chongqing Technology and Business University. Her research interests include stochastic switched systems, event-triggered scheme, model reduction, balanced truncation, robust control, and filtering design.

NING ZHAO received the B.S. degree in mathematics and applied mathematics from Hulunbuir University, Hulunbuir, in June 2015, and the M.E. degree in mathematics from Heilongjiang University, Harbin, China, in June 2018. He is currently pursuing the Ph.D. degree in control science and engineering with the College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin. His current research interests include networked control systems, event-triggered control, and security control.

LUIS I. MINCHALA (Senior Member, IEEE) received the B.S.E.E. degree in electronics from the Salesian Polytechnic University, Cuenca, Ecuador, in 2006, and the M.S. and Ph.D. degrees in control engineering from the Tecnológico de Monterrey, Monterrey, Mexico, in 2011 and 2014, respectively. From 2012 to 2013, he was a Visiting Scholar at Concordia University, Montreal, QC, Canada. Between 2017 and 2018, he was a Postdoctoral Fellow with the Climate Change Research Group, Tecnológico de Monterrey. Currently, he is a full-time Researcher with the Department of Electrical, Electronic and Telecommunications Engineering, Universidad de Cuenca, Ecuador. He has authored and coauthored more than 40 indexed publications, including journal articles, conference proceedings, book chapters, and a book.