A Data-Driven Attack Detection Approach for DC Servo Motor Systems Based on Mixed Optimization Strategy

Xiao-Jian Li, *Member, IEEE*, and Xin-Yu Shen

***Abstract*—This article is concerned with the data-driven attack detection problem for cyber-physical systems with the actuator attacks and measurement noise. In most of existing data-driven detection methods, H_∞ index is used to characterize the sensitivity performance. It is well-known that compared with the H_∞ index, H_- index can significantly improve the diagnostic performance. However, the detection system design based on the H_-/H_∞ mixed optimization technique has not been solved within the data-driven framework. In this article, a residual generator is constructed from the available input–output (I/O) data. H_∞ and H_- indices are defined from the viewpoint of time-domain to characterize the robustness of residual generator against measurement noise and sensitivity to attack signals, respectively. In particular, a novel weighting system, which is expressed as an I/O model, is designed to transform the H_- performance into an H_∞ constraint, and the detection system design problem based on H_-/H_∞ mixed optimization technique is finally formulated into a constraint-type optimization one, which can be solved by the classical Lagrange multiplier method. Also, the proposed detection method is applied to a networked dc servo motor system to verify its advantages and effectiveness.**

***Index Terms*—Actuator attack, cyber-physical systems (CPSs), data-driven, mixed optimization.**

I. Introduction

DUE to innovations in computer technology, embedded technology, and network technology, recent years have witnessed a rapid development of cyber-physical systems (CPSs). CPSs integrate computation, communication, and control into one, and are widely used in power generation, energy development, chemical industry control, etc. However, with further progress of networked embedded control technology, cyber attacks have become one of the major threats to CPSs. Therefore, since the discovery of the Stuxnet malware [1], the issue of security in CPSs has become a hot topic of scientific inquiry [2]–[4].

The detection and secure control problems of CPSs with attacks have received increasing attention in the past years [5]–[15]. In [6], the detection problem of two Gaussian signals with uncertain mean and covariance has been studied. It has been proven that the design of a robust linear detector can be cast into a convex optimization problem. In [7], both hybrid-share real-time detector and mitigation mechanism have been proposed for CPSs. In [9], the attack detection problem for cyber-physical direct current (dc) microgrids with false-data injection attacks has been formalized as identifying a change in sets of inferred candidate invariants. In [11], a method has been proposed in order to detect stealthy false data injection attacks based on coding matrix. Besides, from the attackers' standpoint, the attack problem has been modeled as a constrained control problem and that the characterization of the maximum perturbation has been posed as reachable set computation in [12]. A variation of the receding-horizon control law to deal with the replay attacks has been proposed, and the resulting system performance degradation has been analyzed in [13]. Because attackers are constrained by execution resources, attacks tend to be sparse. Among the existing works, sparse attacks for CPSs have been widely studied. In [14], a low-complexity attacking strategy to construct sparse false data injection attack vectors has been designed, and strategic protection schemes have been also proposed based on greedy approaches.

However, the system dynamic matrices in the abovementioned results are all required to be known. As pointed out in [16], it may be strict to assume that all the system dynamic matrices are known in CPSs. Therefore, it is more reasonable to study the attack detection and secure control problems for CPSs with completely unknown system matrices. Up to now, such problems have not been investigated well, which is one of the main motivations of this article.

On the other hand, in the absence of accurate models of the controlled plants, full use of the online or offline data can be

Manuscript received July 25, 2019; revised September 27, 2019 and November 29, 2019; accepted December 15, 2019. Date of publication December 18, 2019; date of current version May 26, 2020. This work was supported in part by the Funds of the National Natural Science Foundation of China under Grant 61873050, in part by the Fundamental Research Funds for the Central Universities under Grant N180405022, and in part by the Research Fund of State Key Laboratory of Synthetical Automation for Process Industries under Grant 2018ZCX14. Paper no. TII-19-3315. *(Corresponding author: Xiao-Jian Li.)*

X.-J. Li is with the State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang 110819, China with the Key Laboratory of Vibration and Control of Aero-Propulsion System Ministry of Education, Northeastern University, Shenyang 110819, China, and also with the College of Information Science and Engineering, Northeastern University, Shenyang, Liaoning 110819, China (e-mail: lixiaojian@ise.neu.edu.cn).

X.-Y. Shen is with the College of Information Science and Engineering, Northeastern University, Shenyang, Liaoning 110819, China (e-mail: shenxinyu@stumail.neu.edu.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2960616

taken to reconfigure system states, diagnose failures, design controllers, or evaluate performance directly [17]–[24]. In view of the approximate dynamic programming approach, the data-driven fault-tolerant control (FTC) of a dc machine system with nonlinearity and load variations was achieved in [20]. Besides, a new recursive total principle component regression based design and implementation approach has been proposed for efficient data-driven fault detection in [21], which significantly increases the online efficiency and releases unnecessary memory occupation. In [22], when the information of the transmission control protocol/Internet protocol (TCP/IP)-based CPSs was eavesdropped, an approach to blocking network communications and injecting false sensor data into the CPSs was explored, and a closed-loop recursive identification strategy for the dynamic characteristic matrix of the CPSs was also designed. In [23], a novel closed-loop numerical algorithm for subspace state space system identification has been proposed, which can deliver effective unbiased pole estimation and show the superior through a practical dc motor system.

Although the detection schemes were given in [17] and [18] within the data-driven framework, the H_∞ index was used to characterize sensitivity. As is known to all, H_- index can improve the diagnostic performance significantly compared with the H_∞ index. In fact, the H_- index is defined as the lowest level of sensitivity of system outputs to system inputs, which is the worst-case sensitivity measure and fails to be a matrix norm. Moreover, the filter design problem caused by the introducing of H_- index is essentially nonconvex. Particularly, within the data-driven framework, how to solve the H_-/H_∞ mixed optimization problem to simultaneously satisfy the robustness of residual generator against measurement noise and sensitivity to attack signals still remains open, which also motivates the current research.

This article is concerned with the data-driven actuator attack detection problem of the networked dc servo motor systems with the completely unknown system matrices and measurement noise. The main contributions are summarized as follows.

1) A data-driven residual generator is designed to detect the actuator attacks. The H_∞ and the H_- indices are defined to characterize the robustness of residual generator against measurement noise and sensitivity to attack signals, respectively. Then, the attack detection problem is formulated as an H_-/H_∞ mixed optimization problem. Compared with the H_∞/H_∞ detection scheme in [17], the superiority of the proposed H_-/H_∞ attack detection method is verified in simulation section.
2) To solve the nonconvex problem encountered in addressing attack sensitivity performance characterized by H_- index, a weighting system in the form of I/O model is constructed to transform the attack sensitivity specification into an H_∞ constraint, which extends the model-based weighting system design approach in [29]. Finally, the H_-/H_∞ mixed optimization problem is formulated into a constraint-type optimization one, which can be solved directly by using the classical Lagrange multiplier method.

The rest of this article is organized as follows. In Section II, the attack model of CPSs and some basic assumptions are described. The design method of the data-driven residual generator based on the optimal parity vector via constructing a weighting system is proposed in Section III. In Section IV, the proposed design method is applied to the networked dc servo motor system to illustrate the effectiveness. Finally, Section V concludes this article.

Notation: Throughout this article, R^n denotes the n-dimensional Euclidean space; $\Gamma^\perp$ denotes the orthogonal complement of Γ; I denotes the identity matrix; $\|\cdot\|_2$ is used to represent the Euclidian norm of a vector or a matrix; and L_2 denotes the Hilbert space of the functions with the following norm: $\|\nu(k)\|_2 = \{\sum_{k=0}^{\infty} \nu^T(k)\nu(k)\}^{1/2}$.

II. System Modeling and Problem Statement

In this section, the model of a networked dc servo motor system is given, the concepts related to actuator attacks are also described, and the problem of data-driven attack detection is then provided.

A. Model Description

The networked dc servo motor system has been studied in [22], the state-space model of the dc motor system is established as described below

$$\begin{aligned}\begin{bmatrix}\Delta\dot{I}\\ \Delta\dot{\Omega}\end{bmatrix} &= \begin{bmatrix}-R_m/L_m & -C_{V/\Omega}/L_m\\ C_{T/I}/J & 0\end{bmatrix}\begin{bmatrix}\Delta I\\ \Delta\Omega\end{bmatrix}\\ &\quad + \begin{bmatrix}K_u/L_m & 0\\ 0 & -1/J\end{bmatrix}\begin{bmatrix}u\\ \Delta T\end{bmatrix}\\ y &= \begin{bmatrix}0 & K_y\end{bmatrix}\begin{bmatrix}\Delta I\\ \Delta\Omega\end{bmatrix}\end{aligned} \tag{1}$$

where R_m, L_m, $C_{V/\Omega}$, $C_{T/I}$, T, and J represent the armature resistance, armature inductance, motor constant, voltage constant, load torque, and total inertia, respectively. ΔI denotes the error between the steady-state current and the actual armature current, and $\Delta\Omega$ represents the error between the desired and actual speeds of the motor. Moreover, $K_u = U_T/u$, $K_y = y/\Omega$ where u, y, U_T, and Ω denote the control input, system output, terminal voltage, and rotating speed of the motor, respectively.

The Fig. 1 represents the block diagram structure of the networked dc servo motor system, which shows the connections among the components. More specifically, the client computer sends measurement data y to the server computer via the Ethernet hub, and after computing a control command by virtue of y, the server computer sends it back to the client computer through the Ethernet hub again.

It is pointed out in [22] that theTCP/IP-based networked dc servo system is a typical CPS. In addition, it is assumed that the adversary can break into the communication link from the server computer to the client computer, and an attack signal is then designed to devastate the system tracking performance. However, different from [22], this article investigates the attack detection problem of the system (1) from the viewpoint of defense. Due to most of the analytical model based attack detection approaches relying on the system parameters, the main challenge to be solved is how to design the detector only using the system input and output (I/O) data.

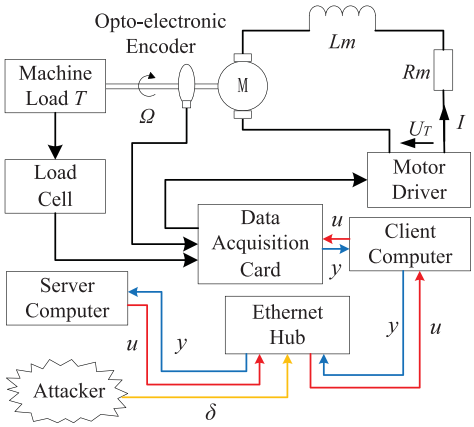

Fig. 1. Block diagram structure of the networked dc servo motor system.

To this end, the dynamics model of the networked dc servo motor system with the actuator attacks is established as

$$\begin{cases} x(k+1) = Ax(k) + B(u(k) + \delta(k)) \\ y(k) = Cx(k) + d(k) \end{cases} \tag{2}$$

where $x(k) \in R^n$ denotes the unmeasurable system state, $u(k) \in R^l$ and $y(k) \in R^m$ are control input and system output, respectively. $d(k)$ is the measurement noise. Similar to [25], $\delta(k) = [\delta_1(k), \delta_2(k), \ldots, \delta_l(k)]$ is a vector modeling how an attacker changes the control input at time k. If the qth, $q \in \{1, \ldots, l\}$ actuator is attacked, the qth element in the vector $\delta(k)$ is nonzero, otherwise it is not attacked. Moreover A, B, and C are unknown matrices with appropriate dimensions.

Remark 1: Just as mentioned in [5], both attack detection and fault detection aim to justify whether attacks/faults occurred or not, and for different types of attacks/faults, different detection approaches have been given in the literature. Analogous to the detection problem, the identification problem is to distinguish between distinct attacks/faults [5]. Especially, how to distinguish between actuator fault and actuator attack should also belong to the identification problem, and such an interesting problem will be further investigated in the future work.

B. Problem Statement

The objective of this article is to design a data-driven attack detector such that the residual signal is sensitive to actuator attacks and also with a certain robustness to system noise.

In order to construct such a residual generator, the system (2) is manipulated into the I/O model (3) in the normal case, i.e., $\delta(k) = 0$

$$\mathcal{Y}_f = \Gamma_s \mathcal{X}_k + \mathcal{H}_s^u \mathcal{U}_f + \mathcal{H}_s^d \mathcal{D}_f \tag{3}$$

where

$$\Gamma_s = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^s \end{bmatrix} \in \mathcal{R}^{m_s \times n} \tag{4}$$

is the extended observability matrix.

$$\mathcal{H}_s^u = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ CB & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ CA^{s-1}B & \cdots & CB & 0 \end{bmatrix} \in \mathcal{R}^{m_s \times l_s} \tag{5}$$

is a block Toeplitz matrix, and $\mathcal{H}_s^d$ is an identity matrix. Here, $m_s = (s+1)m$, $l_s = (s+1)l$, and $s \geq n$. Then, the state sequences and the block Hankel matrices for outputs are defined as follows:

$$\mathcal{X}_k = [x(k), x(k+1), \ldots, x(k+N)] \tag{6}$$

$$\mathcal{Y}_p = \begin{bmatrix} y(k-s) & y(k-s+1) & \cdots & y(k-s+N-1) \\ y(k-s+1) & y(k-s+2) & \cdots & y(k-s+N) \\ \vdots & \vdots & \vdots & \vdots \\ y(k) & y(k+1) & \cdots & y(k+N-1) \end{bmatrix} \tag{7}$$

$$\mathcal{Y}_f = \begin{bmatrix} y(k+1) & y(k+2) & \cdots & y(k+N) \\ y(k+2) & y(k+3) & \cdots & y(k+N+1) \\ \vdots & \vdots & \vdots & \vdots \\ y(k+s+1) & y(k+s+2) & \cdots & y(k+s+N) \end{bmatrix}. \tag{8}$$

Following the same lines, the matrices $\mathcal{U}_p, \mathcal{U}_f$, and $\mathcal{D}_f$ can be defined well, where f and p denote the dimensions of future and past windows, respectively, and N is chosen large enough which satisfies (11).

To investigate the attack detection problem, the underlying basic assumptions are introduced in this article.

Assumption 1: The order of the system n is known.

Assumption 2: (A, B) is controllable and (A, C) is observable.

Based on the Assumptions 1 and 2, the I/O data will be used to design the residual generator to detect attacks.

III. Data-Driven Mixed Optimization Attack Detection Approach

In this section, in order to realize the detection of actuator attacks, an observer-based residual generator is first designed by using the I/O data. Then, the H_∞ and H_- indices are defined to characterize the robustness of residual generator against system noise and sensitivity to attack signals, respectively. Finally, the observer design problem is transformed into an H_-/H_∞ mixed optimization problem, which is solved by the classical Lagrange multiplier method, and the parameters can be computed to construct the residual generator.

A. Data-Driven Observer-Based Residual Generator Design

Under the Assumption 2, the extended observability matrix Γ_s is full rank of column, and then there exists a left null space of Γ_s,

denoted by $\Gamma_s^{\perp}$. The construction of an observer-based residual generator can be achieved by identifying $\Gamma_s^{\perp}$ and $\Gamma_s^{\perp}\mathcal{H}_s^u$. To this end, let

$$\mathcal{Z}_p = \begin{bmatrix} \mathcal{Y}_p \\ \mathcal{U}_p \end{bmatrix}, \quad \mathcal{Z}_f = \begin{bmatrix} \mathcal{Y}_f \\ \mathcal{U}_f \end{bmatrix}.$$

According to [26], the identification process can be completed by performing singular value decomposition (SVD) on $\frac{1}{N}\mathcal{Z}_f\mathcal{Z}_p^T$

$$\frac{1}{N}\mathcal{Z}_f\mathcal{Z}_p^T = \begin{bmatrix} \mathcal{U}_{11} & \mathcal{U}_{12} \\ \mathcal{U}_{21} & \mathcal{U}_{22} \end{bmatrix} \begin{bmatrix} \Sigma & \\ & 0 \end{bmatrix} \begin{bmatrix} \mathcal{V}_1^T \\ \mathcal{V}_2^T \end{bmatrix} \tag{9}$$

where

$$\mathcal{U}_{12} \in \mathcal{R}^{m_s \times (m_s - n)}, \quad \mathcal{U}_{22} \in \mathcal{R}^{l_s \times (m_s - n)}.$$

From [27], it is known that

$$\Gamma_s^{\perp} = \mathcal{U}_{12}^T, \quad \Gamma_s^{\perp}\mathcal{H}_s^u = -\mathcal{U}_{22}^T. \tag{10}$$

In addition, to make sure $\Gamma_s^{\perp}$ and $\Gamma_s^{\perp}\mathcal{H}_s^u$ are available, the data employed in constructing $\frac{1}{N}\mathcal{Z}_f\mathcal{Z}_p^T$ should be collected under the input excitation condition, which satisfies

$$\text{rank}\left(\frac{1}{N}\begin{bmatrix} \mathcal{X}_k \\ \mathcal{U}_f \end{bmatrix}\mathcal{Z}_p^T\right) = n + sl. \tag{11}$$

According to [28], the observer-based residual generator is designed in the following:

$$z(k+1) = A_z z(k) + B_z u(k) + L_z y(k) \tag{12}$$

$$r(k) = g_z y(k) - C_z z(k) \tag{13}$$

where A_z, B_z, C_z, L_z, and g_z together with the transformation matrix T are able to be parameterized by the Luenberger equations

$$\begin{aligned} A_z T &= TA - L_z C \\ B_z &= TB \\ C_z T &= g_z C. \end{aligned} \tag{14}$$

Consider a vector $v_s = [v_s^0, v_s^1, \ldots, v_s^s] \in \mathcal{R}^{m \times s}$, where

$$v_s \in P_s, \quad P_s = \{v_s \mid v_s \Gamma_s = 0\}. \tag{15}$$

Here, v_s is the so-called parity vector. Then, the following equations hold:

$$A_z = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix}, \; B_z = \begin{bmatrix} v_s\mathcal{H}_{s,0}^u \\ v_s\mathcal{H}_{s,1}^u \\ \vdots \\ v_s\mathcal{H}_{s,s-1}^u \end{bmatrix}$$

$$C_z = \begin{bmatrix} 0 & 0 & \cdots & 1 \end{bmatrix}, \; L_z = -\begin{bmatrix} v_s^0 \\ v_s^1 \\ \vdots \\ v_s^{s-1} \end{bmatrix}$$

$$g_z = v_s^s \tag{16}$$

where

$$\mathcal{H}_s^u = \begin{bmatrix} \mathcal{H}_{s,0}^u & \mathcal{H}_{s,1}^u & \cdots & \mathcal{H}_{s,s-1}^u \end{bmatrix}$$

$$\mathcal{H}_{s,i}^u = \begin{bmatrix} 0 \\ \vdots \\ CB \\ \vdots \\ CA^{s-i-1}B \end{bmatrix}$$

for $i = 0, 1, \ldots, s-1$.

With $\Gamma_s^{\perp}$ and $\Gamma_s^{\perp}\mathcal{H}_s^u$ being identified by using the I/O data, v_s can be selected to construct the residual generator (12) and (13). In fact, there exists an optimal parity vector v_s such that the residual is robust against system noise and sensitive to attack signals simultaneously. The design criterion of the optimal parity vector v_s depends on the robustness and sensitivity indices defined in the next section.

Remark 2: It should be pointed out that the proposed observer design method is also applicable for the multi-input–multi-output (MIMO) systems. In fact, the I/O model (3) and the method of calculating the observer parameters (16) are still valid for the MIMO systems, and the detailed discussions can refer to [17] and [18].

B. Calculation of the Optimal Parity Vector

Similar to (3), by iterating the equations in (2), we can obtain the I/O model in the presence of an attack

$$y_s(k) = \Gamma_s x(k-s) + \mathcal{H}_s^u u_s(k) + \mathcal{H}_s^d d_s(k) + \mathcal{H}_s^{\delta}\delta_s(k) \tag{17}$$

where

$$y_s(k) = \begin{bmatrix} y(k-s) \\ y(k-s+1) \\ \vdots \\ y(k) \end{bmatrix}$$

Following the same lines, $u_s(k)$, $d_s(k)$, and $\delta_s(k)$ can be defined well, and $\mathcal{H}_s^{\delta}$ is the same as $\mathcal{H}_s^u$.

According to [28], the residual signal generated by (12) and (13) can be rewritten as

$$r(k) = v_s(y_s(k) - \mathcal{H}_s^u u_s(k)) = v_s(\mathcal{H}_s^d d_s(k) + \mathcal{H}_s^{\delta}\delta_s(k)) \tag{18}$$

Thus, on the basis of (18), we define the following robust performance index from a time-domain perspective:

$$R_d := \| v_s\mathcal{H}_s^d \|_{\infty} = \sup_{d \neq 0} \frac{\| v_s\mathcal{H}_s^d d \|_2}{\| d \|_2} \tag{19}$$

which is a measure of the worst-case influence of the disturbance $d(k)$ on the residual signal $r(k)$. In the existing work [17], [18],

an H_∞ index is used to characterize the sensitivity from the attack $\delta(k)$ to $r(k)$

$$S_{\delta,+} := \| v_s\mathcal{H}_s^\delta \| = \sup_{\delta\neq 0} \frac{\| v_s\mathcal{H}_s^\delta\delta \|_2}{\| \delta \|_2}. \tag{20}$$

According to (19) and (20), the H_∞/H_∞ optimization problem formulated as maximizing $J_{S/R} = \frac{S_{\delta,+}}{R_d}$ is solved to get the best performance of residual generator in [17].

It should be pointed out that (20) is not the worst-case attack sensitivity measure, while H_- index is a measure of evaluating the minimum sensitivity, which can significantly improve the diagnostic performance according to [10]. Therefore, in this article, we define the sensitivity index as

$$S_{\delta,-} := \| v_s\mathcal{H}_s^\delta \|_- = \inf_{\delta\neq 0} \frac{\| v_s\mathcal{H}_s^\delta\delta \|_2}{\| \delta \|_2}. \tag{21}$$

On the basis of (19) and (21), our problem is cast into an H_-/H_∞ mixed optimization one described as $\mathcal{P}_0$

$$\begin{aligned} &\mathcal{P}_0 : \text{maximize } \beta, \text{ subject to } S_{\delta,-} > \beta \\ &\text{with } R_d < \gamma_0, \text{ for a given } \gamma_0 \end{aligned} \tag{22}$$

where β denotes the sensitivity index to be optimized, and γ_0 is the prescribed robustness index.

Note that $S_{\delta,-}$ is an H_- index, which fails to be a norm. The filter design problem caused by the introducing of the H_- index is essentially nonconvex. To overcome this problem, we will refer to the method in [29] to transform the sensitivity specification into an H_∞ constraint.

Lemma 1: Consider the attack sensitivity specification $S_{\delta,-} = \| v_s\mathcal{H}_s^\delta \|_- > \beta$ in (22). Introduce a weighting matrix W_f such that

$$\| W_f \|_- > \eta > \beta \tag{23}$$

where η is a given positive scalar. If

$$\| v_s\mathcal{H}_s^\delta - W_f \|_\infty < \eta - \beta \tag{24}$$

holds, the specification $S_{\delta,-} = \| v_s\mathcal{H}_s^\delta \|_- > \beta$ can be ensured.

Proof: According to the definition similar to (21), we have

$$\begin{aligned} \| v_s\mathcal{H}_s^\delta \|_- &= \inf_{\delta\neq 0} \frac{\| v_s\mathcal{H}_s^\delta\delta \|_2}{\| \delta \|_2} \\ &\geq \inf_{\delta\neq 0} \left(| \frac{\| W_f\delta \|_2}{\| \delta \|_2} - \frac{\| (v_s\mathcal{H}_s^\delta - W_f)\delta \|_2}{\| \delta \|_2} | \right) \\ &\geq \inf_{\delta\neq 0} \left(\frac{\| W_f\delta \|_2}{\| \delta \|_2} \right) - \inf_{\delta\neq 0} \left(\frac{\| (v_s\mathcal{H}_s^\delta - W_f)\delta \|_2}{\| \delta \|_2} \right) \\ &> \inf_{\delta\neq 0} \left(\frac{\| W_f\delta \|_2}{\| \delta \|_2} \right) - \sup_{\delta\neq 0} \left(\frac{\| (v_s\mathcal{H}_s^\delta - W_f)\delta \|_2}{\| \delta \|_2} \right) \end{aligned} \tag{25}$$

Therefore, we can obtain that

$$\| v_s\mathcal{H}_s^\delta \|_- > \| W_f \|_- - \| v_s\mathcal{H}_s^\delta - W_f \|_\infty . \tag{26}$$

In view of (23), (26) and the sufficient condition (24), the attack sensitivity specification $S_{\delta,-} = \| v_s\mathcal{H}_s^\delta \|_- > \beta$ can be ensured, which completes the proof. ■

Assuming that the minimal state-space realization of W_f is

$$\begin{cases} x_w(k+1) = A_w x_w(k) + B_w\delta(k) \\ z_w(k) = C_w x_w(k) \end{cases} \tag{27}$$

where $x_w(k) \in \mathcal{R}^n$, A_w, B_w, and C_w are the constant matrices to be designed, and the detailed design processes are given in [29].

Within the data-driven framework, we first rewrite the state-space realization (27) into the I/O model

$$z_s^w(k) = \Gamma_s^w x_w(k-s) + \mathcal{H}_{\delta,s}^w\delta_s(k) \tag{28}$$

where Γ_s^w has the same structure as Γ_s in (4) by replacing A and C with A_w and C_w, and $\mathcal{H}_{\delta,s}^w$ has the same block Toeplitz structure as $\mathcal{H}_s^\delta$ in (17), which is derived by replacing A, B, and C with A_w, B_w, and C_w. Moreover, the parity vector α_s similar to v_s in (15) is also introduced to eliminate the states $x_w(k-s)$. Then, we get

$$\alpha_s z_s^w(k) = \alpha_s\mathcal{H}_{\delta,s}^w\delta_s(k). \tag{29}$$

Thus, W_f is rewritten as

$$W_f = \alpha_s\mathcal{H}_{\delta,s}^w. \tag{30}$$

Note that, α_s should be given in such a way that the minimum singular value of matrix $\alpha_s\mathcal{H}_{\delta,s}^w$ is maximized.

By using Lemma 1, the H_- index used to characterize the attack sensitivity specification is transformed into an H_∞ constraint, and the problem described in $\mathcal{P}_0$ can be converted to $\mathcal{P}_1$

$$\mathcal{P}_1 : \text{minimize } \|v_s\mathcal{H}_s^\delta - \alpha_s\mathcal{H}_{\delta,s}^w\|, \text{ subject to } \|v_s\mathcal{H}_s^d\| < \gamma_0 \tag{31}$$

which is a constraint-type optimization problem and can be solved by the classical Lagrange multiplier method. In order to solve $\mathcal{P}_1$, introducing a Lagrange multiplier λ, the optimal parity vector v_s can be found by minimizing the following objective

$$\begin{aligned} \mathcal{L}(v_s,\lambda) &= \min_{v_s} \|v_s\mathcal{H}_s^\delta - \alpha_s\mathcal{H}_{\delta,s}^w\|^2 + \lambda(\|v_s\mathcal{H}_s^d\|^2 - \gamma_0^2) \\ &= \min_{v_s}[(v_s\mathcal{H}_s^\delta - \alpha_s\mathcal{H}_{\delta,s}^w)(v_s\mathcal{H}_s^\delta - \alpha_s\mathcal{H}_{\delta,s}^w)^T] \\ &\quad + \lambda[(v_s\mathcal{H}_s^d)(v_s\mathcal{H}_s^d)^T - \gamma_0^2] \end{aligned} \tag{32}$$

with

$$\lambda[(v_s\mathcal{H}_s^d)(v_s\mathcal{H}_s^d)^T - \gamma_0^2] = 0. \tag{33}$$

Differentiating $\mathcal{L}(v_s,\lambda)$ with respect to v_s leads to

$$v_s[\mathcal{H}_s^\delta(\mathcal{H}_s^\delta)^T + \lambda\mathcal{H}_s^d(\mathcal{H}_s^d)^T] = \alpha_s\mathcal{H}_{\delta,s}^w(\mathcal{H}_s^\delta)^T \tag{34}$$

On the basis of (33) and the constraint in $\mathcal{P}_1$, we can obtain

$$v_s[\mathcal{H}_s^\delta(\mathcal{H}_s^\delta)^T] = \alpha_s\mathcal{H}_{\delta,s}^w(\mathcal{H}_s^\delta)^T \tag{35}$$

as $\lambda = 0$. Therefore, the solution space containing the optimal parity vectors v_s can be obtained through (35).

Algorithm 1: Data-Driven Mixed Optimization Design of a Residual Generator.

Step 1: Collect the data tuples $(\{y_i,\ u_i\}, i = k-s, k-s+1, \ldots)$ under an input excitation condition. Subsequently, construct $\mathcal{Z}_p$ and $\mathcal{Z}_f$. Perform SVD on $\frac{1}{N}\mathcal{Z}_f\mathcal{Z}_p^T$ to identify $\Gamma_s^{\perp}$ and $\Gamma_s^{\perp}\mathcal{H}_s^u$.

Step 2: Based on the identification results of the original system via the input-output data, calculate $\mathcal{H}_s^d$ and $\mathcal{H}_s^{\delta}$.

Step 3: According to Lemma 1, design a weighting system W_f, and calculate $\mathcal{H}_{\delta,s}^w$ in (30).

Step 4: Solve the constraint-type optimization problem (32) by the classical Lagrange Multiplier method. The optimal parity vector v_s can be derived to build the complete residual generator (12) and (13).

Step 5: Establish the threshold value J_{th} (37), if $J_r(\tau) > J_{th}$, then an attack is detected.

Finally, the residual generator (12) and (13) can be designed using the optimal parity vector to detect the actuator attack signals.

C. Detection Threshold Design

In this section, the threshold for detecting actuator attacks is designed and the detection logic unit is based on the result in [30].

Let the root mean square value which means the average energy of residual signal over a time interval $(k_0,\ k_\tau)$

$$J_r(\tau) = \sqrt{\frac{1}{\tau}\sum_{k=k_0}^{k_\tau} r^T(k)r(k)} \tag{36}$$

be a residual evaluation function, where k_0 stands for the initial evaluation time instant and k_τ denotes the evaluation time.

Let

$$J_{th} = \sup_{d(k)\in L_2, \delta(k)=0} J_r(\tau) \tag{37}$$

as the threshold. According to (37), the occurrence of attacks can be detected by comparing $J_r(\tau)$ and J_{th} based on the following test:

$$\begin{cases} J_r(\tau) > J_{th} \Rightarrow \text{alarm} \\ J_r(\tau) \le J_{th} \Rightarrow \text{no attack} \end{cases} \tag{38}$$

On the basis of above work, the main steps of the designed data-driven attack detection scheme are summarized in Algorithm 1.

IV. Simulation Example

In this section, the networked dc servo motor system is used to verify the effectiveness and advantages of the proposed method.

All the simulation parameters of the dc motor, the digital-to-analog converter, and the optoelectronic encoder are summarized in Table I. The parameters can also be found in [19],

TABLE I
Simulation Parameters of the Motor System

Parameter	Symbol	Value	Unit
Motor constant	$C_{T/I}$	0.06	Nm/A
Voltage constant	$C_{V/\Omega}$	6.27×10^{-3}	V/(r/min)
Armature inductance	L_m	0.003	H
Resistance	R_m	3.13	Ohm
Machine load	T	0.1	Nm
Total inertia	J	80.45×10^{-6}	kg $\times$ m^2
Encoder resolution	E_R	60	Pulses/R
D/A resolution	P_R	12	Bit

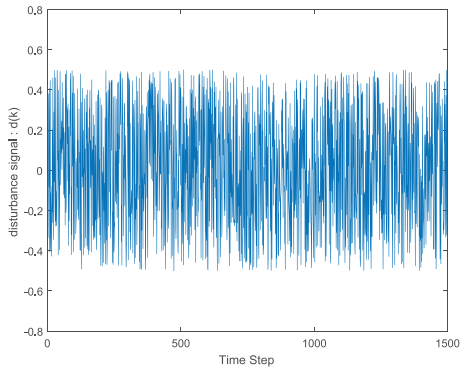

Fig. 2. Disturbance signal $d(k)$.

and the sampling time is set to be 0.1 s. As the parameters are calculated, the above sampling time and zero-order-hold discretization method are adopted, finally the normal networked dc servo motor system is established as

$$\begin{aligned} x(k+1) &= \begin{bmatrix} -0.0022 & -0.0030 \\ 1.0625 & 0.9808 \end{bmatrix} x(k) \\ &\quad + \begin{bmatrix} 0.9516 & 0.0000 \\ 6.1303 & 4.5728 \end{bmatrix} u(k) \\ y(k) &= \begin{bmatrix} 0 & 0.170667 \end{bmatrix} x(k) + d(k). \end{aligned}$$

The considered time-varying random disturbance signal $d(k)$ with the magnitude being 0.5 is shown in Fig. 2.

In practice, it may be difficult to obtain the precise system parameters. Therefore, for the case that the parameters in Table I are completely unknown, a data-driven attack detection approach is given in the article for the considered dc servo motor system. In the following, it is shown that the proposed method not only detects the actuator attack effectively, but also improves the related data-driven detection results in terms of enhancing the detection performances.

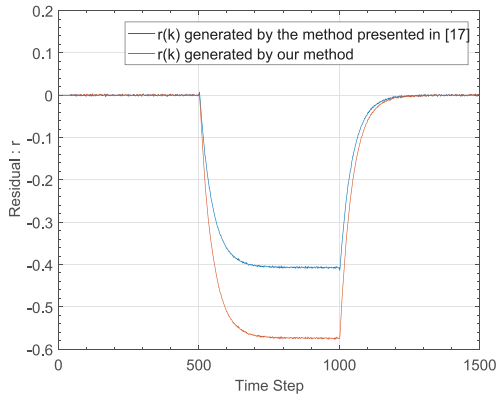

Fig. 3. Residual $r(k)$ with the magnitude of $\delta(k)$ being 5.

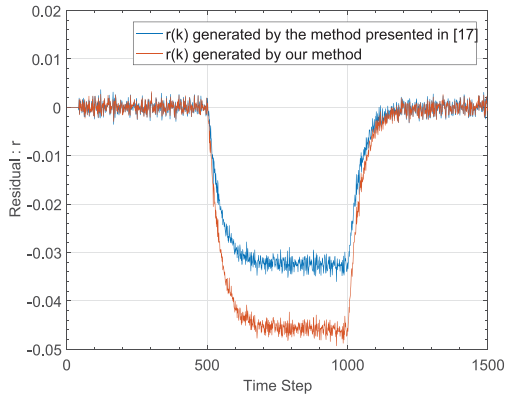

Fig. 5. Residual $r(k)$ with the magnitude of $\delta(k)$ being 0.4.

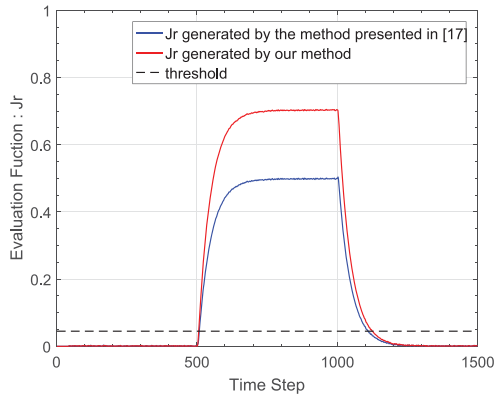

Fig. 4. Residual evaluation function $J_r(\tau)$ with the magnitude of $\delta(k)$ being 5.

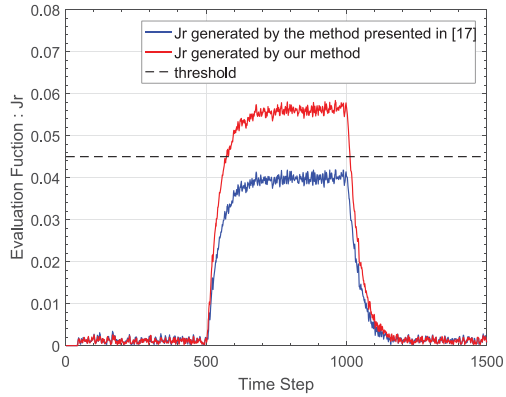

Fig. 6. Residual evaluation function $J_r(\tau)$ with the magnitude of $\delta(k)$ being 0.4.

Referring to [29], the following system matrices of the weighting system:

$$A_w = \begin{bmatrix} 0.3781 & -2.2081 \\ 0.0169 & 0.2202 \end{bmatrix}$$

$$B_w = \begin{bmatrix} -4.4658 & 0.1725 \\ -4.8000 & 2.9185 \end{bmatrix}$$

$$C_w = [0.0034 \quad 0.0004]$$

are selected to design W_f with $\eta = 0.63$ and $\alpha_s = [0.0637, -0.1982, -0.0561, 0.9765]$. Via Lemma 1, one can derive the sensitivity index being $\beta = 0.59$, and from Algorithm 1, the optimal parity vector v_s can be solved as $v_s = [0, 0.1927, -0.0605, 0]$ with $\gamma_0 = 0.5$.

Assuming that at the 500th time step, the actuator attack signal $\delta(k) = [5, 0]^T$ is injected in the system and removed at the 1000th time step. The residuals $r(k)$ derived by using the proposed attack detection scheme and the existing one in [17] are then plotted in Fig. 3. The corresponding residual evaluation functions $J_r(\tau)$ and threshold J_{th} computed by (36) are depicted in Fig. 4.

From Fig. 3, it can be seen that the residual generated by the H_-/H_∞ mixed optimization strategy is more sensitive than the one in [17] generated by using H_∞/H_∞ detection scheme. It should be pointed out that the magnitude of $\delta(k)$ is relatively large compared with the one of the system noise $d(k)$, then the attack can be detected by using both the proposed detection scheme and the one in [17] (see Fig. 4).

In fact, the attack signals might be weak, because the attacks are artificially launched by the adversary. Therefore, the residual generator should be sensitive enough so that the weak attack signals can still be detected. To further verify the advantages of the proposed detection method, it is assumed that the attack signal is $\delta(k) = [0.4, 0]^T$. For the same system noise $d(k)$ given previously, the residual signals $r(k)$ and residual evaluation functions $J_r(\tau)$ generated by the proposed approach and the existing method presented in [17] are reported in Figs. 5 and 6.

As shown in these two figures, the proposed data-driven attack detection approach is still valid when the magnitude of the attack signal is smaller than the one of the system noise, while the existing method in [17] based on the H_∞/H_∞ strategy fails to work in this case. Therefore, the comparison shows the superiority of the proposed H_-/H_∞ detection strategy.

V. Conclusion

This article was concerned with the data-driven attack detection problem for CPSs with the actuator attacks and measurement noise. A residual generator was constructed from the available I/O data. Then, the H_∞ and H_- indices characterizing the robustness of residual generator against measurement noise and sensitivity to attack signals, respectively, were defined. Moreover, by introducing a weighting system expressed as the I/O model, the H_- performance was transformed into an H_∞ constraint, and the H_-/H_∞ mixed optimization problem was formulated into a constraint-type optimization one, which can be solved by the classical Lagrange multiplier. Finally, the proposed design method was applied to the networked dc servo motor system to verify its advantages and effectiveness. Note that future research efforts will focus on designing attack detection scheme for CPSs with measurement and process noise, and relevant secure control strategy within the data-driven framework.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[2] A. A. Crdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proc. 3rd Conf. Hot Topics Secur.*, Berkeley, CA, USA, 2008, pp. 1–6.

[3] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proc. VDE Kongress*, 2004, vol. 116, pp. 213–218.

[4] H. Xu and S. Jagannathan, "A cross layer approach to the novel distributed scheduling protocol and event-triggered controller design for cyber physical systems," in *Proc. 37th Annu. IEEE Conf. Local Comput. Netw.*, 2012, pp. 232–235.

[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[6] A. Mutapcic and S. J. Kim, "Robust signal detection under model uncertainty," *IEEE Signal Process. Lett.*, vol. 16, no. 4, pp. 287–290, Apr. 2009.

[7] X. Cao, L. Liu, W. Shen, A. Laha, J. Tang, and Y. Cheng, "Real-time misbehavior detection and mitigation in cyber-physical systems over WLANs," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 186–197, Feb. 2017.

[8] 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.

[9] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[10] X. J. Li and G. H. Yang, "Fault detection in finite frequency domain for Takagi-Sugeno fuzzy systems with sensor faults," *IEEE Trans. Cybern.*, vol. 44, no. 8, pp. 1446–1458, Aug. 2014.

[11] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

[12] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2618–2624, Sep. 2016.

[13] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[14] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011

[15] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, "Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems," in *Proc. IEEE 55th Conf. Decis. Control*, 2016, pp. 1297–1302.

[16] P. Antsaklis, "Goals and challenges in cyber-physical systems research editorial of the editor in chief," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3117–3119, Dec. 2014.

[17] S. Yin, G. Wang, and H. R. Karimi, "Data-driven design of robust fault detection system for wind turbines," *Mechatronics*, vol. 24, no. 4, pp. 298–306, 2014.

[18] Y. Wang, G. Ma, S. X. Ding, and C. Li, "Subspace aided data-driven design of robust fault detection and isolation systems," *Automatica*, vol. 47, no. 11, pp. 2474–2480, 2011.

[19] J. S. Wang and G. H. Yang, "Data-driven output-feedback fault-tolerant compensation control for digital PID control systems with unknown dynamics," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7029–7039, Nov. 2016.

[20] J. S. Wang and G. H. Yang, "Data-driven output-feedback fault-tolerant tracking control method and its application to a DC servo system," *IEEE/ASME Trans. Mechatronics*, vol. 24, no. 3, pp. 1186–1196, Jun. 2019.

[21] Y. Jiang and S. Yin, "Recursive total principle component regression based fault detection and its application to vehicular cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1415–1423, Apr. 2018.

[22] J. S. Wang and G. H. Yang, "Data-driven methods for stealthy attacks on TCP/IP-based networked control systems equipped with attack detectors," *IEEE Trans. Cybern.*, vol. 49, no. 8, pp. 3020–3031, Aug. 2019.

[23] K. Li, H. Luo, C. Yang, and S. Yin, "Subspace-aided closed-loop system identification with application to DC motor system," *IEEE Trans. Ind. Electron.*, vol. 67, no. 3, pp. 2304–2313, Mar. 2020.

[24] J. S. Wang and G. H. Yang, "Data-driven output-feedback fault-tolerant control for unknown dynamic systems with faults changing system dynamics," *J. Process Control*, vol. 43, pp. 10–23, 2016.

[25] 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.

[26] J. Wang and S. J. Qin, "A new subspace identification approach based on principal component analysis," *J. Process Control*, vol. 12, no. 8, pp. 841–855, 2002.

[27] S. X. Ding, P. Zhang, A. Naik, E. L. Ding, and B. Huang, "Subspace method aided data-driven design of fault detection and isolation systems," *J. Process Control*, vol. 19, no. 9, pp. 1496–1510, 2009.

[28] S. X. Ding, *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Berlin, Germany: Springer-Verlag, 2008.

[29] X. J. Li and G. H. Yang, "Fault detection for T-S fuzzy systems with unknown membership functions," *IEEE Trans. Fuzzy Syst.*, vol. 22, no. 1, pp. 139–152, Feb. 2014.

[30] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

Xiao-Jian Li (M'16) received the B.S. and M.S. degrees in mathematics from Northeast Normal University, Changchun, China, in 2003 and 2006, respectively, and the Ph.D. degree in control theory and engineering from Northeastern University, Shenyang, China, in 2011.

He is currently a Professor with the College of Information Science and Engineering, Northeastern University. His research interests include fault diagnosis, fault-tolerant control, fuzzy control, and cyber-physical systems.

Xin-Yu Shen received the B.S. degree in automation from Shenyang Jianzhu University, Shenyang, China, in 2018. She is currently working toward the M.S. degree in control theory and engineering from Northeastern University, Shenyang.

Her research interests include cyber-physical systems, data-driven controller design, and fault detection.