Improved Interval Estimation Method for Cyber-Physical Systems Under Stealthy Deception Attacks

Jianwei Fan, Jun Huang, *Member, IEEE*, and Xudong Zhao, *Member, IEEE*

***Abstract*—This paper investigates the problem of interval estimation for cyber-physical systems subject to stealthy deception attacks. The cyber-physical system is supposed to be compromised by malicious attackers and on the basis of that, a stealthy attack strategy is formulated. Moreover, the stealthiness of the attack strategy against χ^2-detector is analyzed. To accomplish interval estimation, the interval observer is designed by the monotone system method. Then, a novel method which combines reachable set analysis with H_∞ technique is proposed. Theoretical comparison between the monotone system method and the proposed method is presented and it shows that the proposed method is able to improve the estimation accuracy. Finally, two illustrative examples are provided to demonstrate the superiority and effectiveness of the improved method.**

***Index Terms*—Cyber attacks, interval observers, reachable set analysis.**

I. Introduction

A CYBER-PHYSICAL system (CPS) is a synthesis of physical process, efficient computation, communication and effective control [1]. Structurally, a CPS system, which is depicted in Fig. 1, consists of perception layer, networking layer and control layer [2]. CPSs are widely applied in power grid, health-care, industrial manufacturing and so on. However, security vulnerabilities are intrinsic to the cyber parts of CPSs. The malicious adversaries are able to formulate various attack strategies by compromising CPSs' availability, confidentiality or integrity [3]–[6]. Roughly speaking, cyber attacks in the literature can be divided into three categories, namely, Denial of service (Dos) attacks, Replay attacks and Deception attacks [7]. The most common attacks seen in the literature are the Dos attacks. Cyber attacks degrade system performances or, worse, cause enormous economic losses and even may put people's lives in danger. Hence, attack detection has drawn great attention in the works [8]–[10] herein. From the system-theoretic and graph-theoretic perspectives, the authors of [8] characterized undetectable cyber attacks and designed centralized and distributed monitors. [9] focused on the research of detection and mitigation of data injection attacks in gossip algorithm and proposed two decentralized strategies to detect attackers. The aforementioned works considered the case where the plant is compromised by a single kind of attacks, however, as the adversaries continually optimize their attack strategies, the defenders must prepare themselves for more complicated and serious situation, including combinations of different attack types. Concerning that the physical layer and cyber layer are simultaneously compromised by false data injection attacks and jamming attacks, Y. Guan *et al.* [10] constructed resilient attack detection estimators to accomplish secure estimation and attack detection.

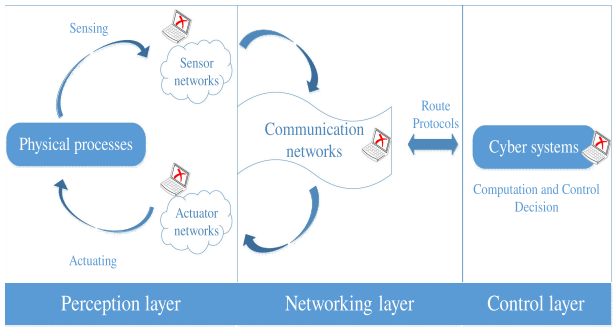


Fig. 1. The diagram of Basic CPS.

On the other hand, since the interval observer was first proposed by Gouzé *et al.* [11], great attention has been paid to it [12], [13]. The interval observer is particularly well adapted for systems subject to disturbances on account of its robustness. Generally speaking, the sufficient condition for the existence of interval observers is that the error systems need to be both cooperative and ultimately uniformly bounded, and it is a strict requirement. Therefore, the coordinate transformation as an effective approach to reduce constraints was proposed in [14], [15]. Furthermore, this method was applied in interval observer design for several specific systems, such as [16]–[20]. Nevertheless, the coordinate transformation technique is restricted by imposing conservatism on interval observers, which results in undesirable performance degradation. Recently, the set-membership

Manuscript received May 11, 2021; revised August 9, 2021 and October 22, 2021; accepted December 4, 2021. Date of publication December 10, 2021; date of current version December 29, 2021. This work was supported in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK2021-1309 and in part by the Open Fund for Jiangsu Key Laboratory of Advanced Manufacturing Technology under Grant HGAMTL-2101. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Yue Gao. *(Corresponding author: Jun Huang.)*

Jianwei Fan and Jun Huang are with the Department of Mechanical and Electrical Engineering, Soochow University, Suzhou 215131, China (e-mail: 15058428720@163.com; cauchyhot@163.com).

Xudong Zhao is with the School of Control Science and Engineering, Dalian University of Technology, Dalian 116000, China (e-mail: xdzhao-hit@gmail.com).

Digital Object Identifier 10.1109/TSIPN.2021.3134097

estimation has been verified to be a significant approach in the design of interval observers. Concerning discrete-time LTI systems, the authors of [21] proposed a two-step interval estimation method which combined reachability analysis with robust observer design. The two-step method was then used in [22] to investigate the interval observer design problem for switched systems. Moreover, the main results in [22] were extended to asynchronous switched systems [23]. Meanwhile, [24] further developed the interval estimation method for switched systems. Following the line, the authors in [25] addressed the functional interval observer design problem for a class of discrete time switched systems. The previous works [21]–[25] have demonstrated that the set-membership method is able to improve the performance of the interval observers. Besides, the current works are also characterized by increasing complexity in system modeling. For instance, T. Chevet *et al.* [26] addressed the interval observer design problem for discrete-time linear systems with unknown inputs. While, A. Tahir *et al.* [27] proposed a procedure to design interval observers for nonlinear discrete-time systems. To the best of the authors' knowledge, the investigation on the interval observer design for CPSs under cyber attacks has rarely been reported except for [28], [29]. However, the conventional interval observer design method was presented while the estimation accuracy was not discussed in [28], [29].

Motivated by the above discussion, this paper considers the problem of interval estimation for CPSs under stealthy deception attacks. The contributions can be summarized in the following aspects. (i) It is the first time to study the accuracy of state estimation for CPSs under stealthy attacks. (ii) A novel interval estimation approach for the considered systems under stealthy attacks is proposed, and it is able to overcome the shortcomings of the monotone system method. (iii) The advantage of the proposed method over the conventional interval observer is strictly proved. The rest of this paper is organized as follows: Section II presents some background knowledge as well as the considered problem; Section III reviews the interval observers designed by the monotone system method; In Section IV, the novel interval estimation method is provided. Comparisons between the proposed method and the monotone system method are discussed in Section V. Finally, two examples are presented in Section VI to verify the effectiveness of the proposed method.

*Notations:*Throughout this paper, R^n and $R^{m\times n}$ denote the n and $m \times n$ dimensional Euclidean space, respectively. For a matrix L, $L^+ = \max\{0,\ L\}$, $L^- = L^+ - L$. The matrix I denotes identity matrix with proper dimensions. For a matrix L, $L > 0 (\geq 0)$ means that any element of it is positive(non-negative). The set $R^n_+ = \{s \in R^n : s > 0\}$, $R^{m\times n}_+ = \{s \in R^{m\times n} : s > 0\}$. The symbol $\oplus$ stands for the Minkowski sum of two sets $\mathbf{E}$ and $\mathbf{F}$, i.e. $\mathbf{E} \oplus \mathbf{F} = \{e + f : e \in \mathbf{E}, f \in \mathbf{F}\}$ while $\bigoplus$ represents the Minkowski sum of a sequence of sets, i.e., $\bigoplus_{i=1}^m \mathbf{E}_i = \mathbf{E}_1 \oplus \mathbf{E}_2 \cdots \oplus \mathbf{E}_m$. Moreover, for a real symmetric matrix L, $L \succ 0 (\prec 0)$ indicates that L is positive (negative) definite. For a vector s, $\|s\|$ denotes its 2-norm. In a symmetric block matrix, $*$ represents a term that can be induced by symmetry. $\overline{eig}(L)$ and $\underline{eig}(L)$ are the largest and smallest of real part of eigenvalues of the matrix L, respectively.

II. Preliminaries and Problem Formulation

In this paper, the following system is considered:

$$\begin{cases} x_{k+1} = Ax_k + B\omega_k, \\ y_k = Cx_k + v_k, \end{cases} \tag{1}$$

where $x_k \in R^{n_x}$, $y_k \in R^{n_y}$ are the state and output respectively. $\omega_k \in R^{n_\omega}$ is the unknown process noise and $v_k \in R^{n_y}$ denotes the measurement error. $A \in R^{n_x\times n_x}$, $B \in R^{n_x\times n_\omega}$ and $C \in R^{n_y\times n_x}$ are given constant matrices. For system (1), when its sensor networks are attacked by falsifying the transmission data, the dynamic equation is

$$\begin{cases} x_{k+1} = Ax_k + B\omega_k, \\ y_k = Cx_k + v_k + a_k, \end{cases} \tag{2}$$

where $a_k \in R^{n_y}$ is the attack signal. It is noteworthy that this paper focuses on how to estimate the state when the the plant is under cyber attack, whose mathematical model is described by (2).

Assumption 1: The initial state x_0, process noise ω_k and measurement error v_k of system(2) satisfy the following inequalities

$$\underline{x} \leq x_0 - c_0 \leq \bar{x}, \quad \underline{\omega} \leq \omega_k \leq \bar{\omega}, \quad \underline{v} \leq v_k \leq \bar{v}, \tag{3}$$

where $\underline{x} = -\bar{x}, \underline{\omega} = -\bar{\omega}, \underline{v} = -\bar{v}$. $c_0 \in R^{n_x}$, $\bar{x} \in R^{n_x}$, and $\bar{\omega} \in R^{n_\omega}$, $\bar{v} \in R^{n_v}$ are all known vectors.

Assumption 2: The attackers have access to the measurement y_k of system (2).

The system (2) is supposed to be equipped with a χ^2-detector which calculates the measurement residual $r = y_k - C\tilde{x}_k$, where $\tilde{x}_k$ is generated by $\tilde{x}_k = (C^TVC)^{-1}C^TVy_k$, and V is a diagonal matrix, i.e.,

$$V = \begin{bmatrix} \sigma_1^{-2} & & & \\ & \sigma_2^{-2} & & \\ & & \ddots & \\ & & & \sigma_{n_y}^{-2} \end{bmatrix},$$

where σ_i is the variance of the i-th component of measurement. The detector subsequently compares residual with a threshold τ and affirms the existence of attacks if $\|r\| > \tau$. Given initial condition $x_0 \in R^{n_x}$, $x(x_0, \omega_{k-1})$ represents the state vector at time instant k. Furthermore, we denote $y(x_0, \omega_{k-1})$ as the measurable output of the system under no attacks, and denote $y(x_0, \omega_{k-1}, a_k)$ as that under nonzero attacks, consequently, we have

$$\begin{aligned} y(x_0, \omega_{k-1}, a_k) &= Cx(x_0, \omega_{k-1}) + a_k \\ &= y(x_0, \omega_{k-1}) + a_k. \end{aligned} \tag{4}$$

The objective of the attackers is to disrupt the measurements of system and stay undetected in the meantime. Such an attack strategy is called a stealthy attack, which can be described by the following lemma.

Lemma 1: For system (2), the nonzero attack a_k is undetectable if there exist two distinct initial conditions $x_0^{(1)}, x_0^{(2)} \in$

$[c_0+\underline{x}, c_0+\bar{x}]$ and process noise $\omega_{k-1}^{(1)}, \omega_{k-1}^{(2)} \in [\underline{\omega}, \bar{\omega}]$ such that

$$y(x_0^{(1)}, \omega_{k-1}^{(1)}, a_k) = y(x_0^{(2)}, \omega_{k-1}^{(2)}). \tag{5}$$

Proof: It is deduced from (5) that $a_k = C[x_k(x_0^{(2)}, \omega_{k-1}^2) - x_k(x_0^{(1)}, \omega_{k-1}^1)]$. For simplicity, we denote $\triangle_k = x_k(x_0^{(2)}, \omega_{k-1}^{(2)}) - x_k(x_0^{(1)}, \omega_{k-1}^{(1)})$. Denote $\tilde{x}_{k,bad}$ as the state estimation obtained by disrupted measurement, and we have

$$\begin{aligned}\tilde{x}_{k,bad} &= (C^TVC)^{-1}C^TVy(x_0, \omega_{k-1}, a_k)\\ &= (C^TVC)^{-1}C^TV(y(x_0, \omega_{k-1}) + a_k)\\ &= \tilde{x}_k + (C^TVC)^{-1}C^TVa_k.\end{aligned}$$

In view of the fact that $a_k = C\triangle_k$, the following expression holds:

$$\begin{aligned}&\|y(x_0, \omega_{k-1}, a_k) - C\tilde{x}_{k,bad}\|\\ &= \|y(x_0, \omega_{k-1}) + a_k - C(\tilde{x}_k + (C^TVC)^{-1}C^TVa_k)\|\\ &= \|y(x_0, \omega_{k-1}) - C\tilde{x}_k + (C\triangle_k - C(C^TVC)^{-1}C^TVC\triangle_k)\|\\ &= \|y(x_0, \omega_{k-1}) - C\tilde{x}_k\|\\ &\le \tau.\end{aligned} \tag{6}$$

This completes the proof.

Remark 1: Since the attackers have access to the measurement y_k, i.e., Assumption 2 holds, equation (5) indicates that by recording two different measurement sequences when the plant operates normally, the attackers can construct an attack sequence to inject bias into y_k while the attack sequence remains undetectable.

In what follows, some definitions and properties about box and zonotope are presented.

Definition 1: An interval vector $\boldsymbol{\eta} \subset R^n$ or a box is defined as

$$\boldsymbol{\eta} = \{s : s \in R^n, u_i \le s_i \le v_i, i = 1, \ldots, n\}. \tag{7}$$

For simplicity, $\boldsymbol{\eta}$ is rewritten as $\boldsymbol{\eta} = [u, v]$, where $u = [u_1, \ldots, u_n]^T$ and $v = [v_1, \ldots, v_n]^T$. Furthermore, an interval vector $\boldsymbol{\eta} \subset R^m$ with all its elements equal to $[-1, 1]$ is called a hypercube, which is denoted as $\mathbf{B}^m = [-1, 1]^m$.

Property 1: Given two interval vectors $[u_1, v_1] \subset R^n$ and $[u_2, v_2] \subset R^n$, the following equation holds:

$$[u_1, v_1] \oplus [u_2, v_2] = [u_1 + u_2, v_1 + v_2].$$

Definition 2: The smallest interval vector containing a given set $\mathbf{E} \subset R^n$ is defined as its interval hull, which can be expressed as $\mathbf{E} \subseteq Box(\mathbf{E}) = [u, v]$, where $u = [u_1, \ldots, u_n]^T$ and $v = [v_1, \ldots, v_n]^T$. The smallest interval vector indicates that for any vector $s \in \mathbf{S}$, $u_i \le s_i \le v_i$, $i = 1, \ldots, n$, $[u_i, v_i]$ is the smallest interval containing it.

Property 2: For a series of sets $\mathbf{E_i} \subset R^n, i = 1, \ldots, k$, we have

$$Box(\bigoplus_{i=1}^{k} \mathbf{E_i}) = \bigoplus_{i=1}^{k} Box(\mathbf{E_i}).$$

Definition 3: A zonotope $\Upsilon \subset R^n$ is obtained by applying affine transformation to an m-order hypercube $\mathbf{B}^m$, which can be described by $\Upsilon = \langle c, G\rangle = \langle c + Gz, z \in \mathbf{B}^m\rangle$, where $c \in R^n$ is the center of Υ and $G \in R^{n\times m}$ is the generator matrix which determines the shape and volume of Υ.

Property 3: The following equalities hold for zonotopes

$$\begin{aligned}\langle c_1, G_1\rangle \oplus \langle c_2, G_2\rangle &= \langle c_1 + c_2, [G_1, G_2]\rangle,\\ L \odot \langle c, G\rangle &= \langle Lc, LG\rangle,\\ \langle c, G\rangle &\in \langle c, \bar{G}\rangle,\end{aligned}$$

where $c_1, c_2, c \in R^n, G_1, G_2, G \in R^{n\times m}$, and $L \in R^{l\times n}$. $\bar{G}$ is a diagonal matrix with $\bar{G}_{i,i} = \sum_{j=1}^{m} |G_{i,j}|, i = 1, \ldots, n$.

Property 4: Given a zonotope $\Upsilon = \langle c, G\rangle \subset R^n$, the components of its interval hull Box(Υ)$=[u, v]$ can be determined by

$$\begin{cases} u_i = c_i - \sum_{j=0}^{m} |G_{i,j}|, i = 1, \ldots, n,\\ v_i = c_i + \sum_{j=0}^{m} |G_{i,j}|, i = 1, \ldots, n.\end{cases}$$

According to Definition 3, (3) can be written as:

$$x_0 \in \langle c_0, G_0\rangle, \quad \omega_k \in \langle 0, D_\omega\rangle \triangleq \mathbf{W}, \quad v_k \in \langle 0, D_v\rangle \triangleq \mathbf{V},$$

where G_0, D_ω, D_v are diagonal matrices whose diagonal elements equal to corresponding elements in x_0, ω_k, v_k.

III. Design of Interval Observer Based on the Monotone System Method Under Stealthy Attack

In this section, we first present the reachable set of a_k and then obtain its upper and lower boundaries. On the basis of that, interval observers are designed for system (2) subject to stealthy attacks.

Theorem 1: For system (2), if Assumption 1 holds, then a_k is bounded by the interval estimation $[\underline{a}_k, \bar{a}_k]$, where $\underline{a}_k$ and $\bar{a}_k$ are determined by

$$\begin{aligned}[\underline{a}_k, \bar{a}_k] &= Box(\boldsymbol{\Lambda})\\ &= Box(CA^k\langle 0, 2G_0\rangle) \oplus \bigoplus_{i=0}^{k-1} Box(2CA^iB\mathbf{W}),\end{aligned}$$

where $\boldsymbol{\Lambda}$ is the reachable set of a_k, and it is determined by

$$\boldsymbol{\Lambda} = CA^k\langle 0, 2G_0\rangle \oplus \bigoplus_{i=0}^{k-1} 2CA^iB\mathbf{W}.$$

Proof: According to the definition of stealthy attacks, one can obtain $y(x_0^{(1)}, \omega_{k-1}^{(1)}) + a_k = y(x_0^{(2)}, \omega_{k-1}^{(2)})$, thus

$$a_k = C\triangle_k, \tag{8}$$

where $\triangle_k = x(x_0^{(2)}, \omega_{k-1}^{(2)}) - x(x_0^{(1)}, \omega_{k-1}^{(1)})$. In view of $\triangle_0 = (x_0^{(2)} - x_0^{(1)}) \in \langle 0, 2G_0\rangle$, we have

$$\triangle_{k+1} = A\triangle_k + B(\omega_k^{(2)} - \omega_k^{(1)}). \tag{9}$$

Subsequently, from (8) and (9), a_k can be computed by

$$\begin{aligned} a_k &= C\triangle_k \\ &= C[A\triangle_{k-1} + B(\omega_{k-1}^2 - \omega_{k-1}^{(1)})] \\ &= \cdots \\ &= CA^k\triangle_0 + C\sum_{i=0}^{k-1} A^i B(\omega_{k-1-i}^{(2)} - \omega_{k-1-i}^{(1)}). \end{aligned}$$

Denote the reachable set of a_k as $\mathbf{\Lambda}$. It indicates that

$$\mathbf{\Lambda} = CA^k\langle 0, 2G_0\rangle \oplus \bigoplus_{i=0}^{k-1} 2CA^iB\mathbf{W}.$$

Then, the interval hull of $\mathbf{\Lambda}$ can be written as

$$\begin{aligned} [\underline{a}_k, \bar{a}_k] &= Box(\mathbf{\Lambda}) \\ &= Box(CA^k\langle 0, 2G_0\rangle) \oplus \bigoplus_{i=0}^{k-1} Box(2CA^iB\mathbf{W}). \end{aligned} \tag{10}$$

This completes the proof.

Remark 2: From (10), $\underline{a}_k$ and $\bar{a}_k$ can be calculated by using Property 4. Moreover, we can also obtain the interval estimation of a_k by constructing interval observers, however, more conservatism will be introduced. For more detail, please refer to [28].

For system (2), an interval observer based on the monotone system method is constructed as

$$\begin{aligned} \bar{z}_0 &= T^+\bar{x}_0^t - T^-\underline{x}_0^t, \\ \underline{z}_0 &= T^+\underline{x}_0^t - T^-\bar{x}_0^t, \end{aligned} \tag{11}$$

$$\begin{aligned} \bar{z}_{k+1} &= K\bar{z}_k + THy_k + \bar{g}, \\ \underline{z}_{k+1} &= K\underline{z}_k + THy_k + \underline{g}, \end{aligned} \tag{12}$$

$$\begin{aligned} \bar{x}_{k+1}^t &= (T^{-1})^+\bar{z}_{k+1} - (T^{-1})^-\underline{z}_{k+1}, \\ \underline{x}_{k+1}^t &= (T^{-1})^+\underline{z}_{k+1} - (T^{-1})^-\bar{z}_{k+1}, \end{aligned} \tag{13}$$

where

$$\begin{cases} \bar{g} = & (TB)^+\bar{\omega} - (TB)^-\underline{\omega} + (-TH)^+\bar{v} - (-TH)^-\underline{v} \\ & +(-TH)^+\bar{a}_k - (-TH)^-\underline{a}_k, \\ \underline{g} = & (TB)^+\underline{\omega} - (TB)^-\bar{\omega} + (-TH)^+\underline{v} - (-TH)^-\bar{v} \\ & +(-TH)^+\underline{a}_k - (-TH)^-\bar{a}_k, \end{cases} \tag{14}$$

We now can state the following theorem.

Theorem 2: If there exist a matrix $H \in R^{n_x\times n_y}$ and an invertible matrix $T \in R^{n_x\times n_x}$ such that $A - HC$ is Schur and $K = T(A - HC)T^{-1}$ is nonnegative, then

$$\underline{x}_k^t \le x_k \le \bar{x}_k^t, \forall k \ge 0 \tag{15}$$

with the condition that $\underline{x}_0^t \le x_0 \le \bar{x}_0^t$.

The proof of Theorem 2 can be referred to [28], and we just omit it here.

IV. Improved Interval Estimation Approach for System Under Stealthy Attack

In this section, an improved interval estimation method is presented. First, an optimal H_∞ observer is designed and then the reachability analysis technique is employed to obtain higher accuracy in state estimation when the system is under stealthy attacks.

First, a Luenberger observer is constructed as follows

$$\hat{x}_{k+1} = A\hat{x}_k + H(y_k - C\hat{x}_k), \tag{16}$$

where $\hat{x}_k$ is the state of the observer and $H \in R^{n_x\times n_y}$ is the observer gain. Denote the error by $e_k = x_k - \hat{x}_k$. The objective is to obtain an interval vector $[\underline{e}_k, \bar{e}_k]$ which satisfies $\underline{e}_k \le e_k \le \bar{e}_k$ such that $\hat{x}_k + \underline{e}_k \le x_k \le \hat{x}_k + \bar{e}_k$. The upper and lower bounds of x_k can thus be defined as

$$\begin{cases} \bar{x}_k = \hat{x}_k + \bar{e}_k, \\ \underline{x}_k = \hat{x}_k + \underline{e}_k. \end{cases} \tag{17}$$

By subtracting (16) from (2), the error dynamics can be described by

$$\begin{aligned} e_{k+1} &= (A - HC)e_k + B\omega_k - Hv_k - Ha_k \\ &= A_e e_k + B_e d_k, \end{aligned} \tag{18}$$

where $A_e = A - HC$, $B_e = [B \quad -H \quad -H]$, $d_k = [w_k^T \quad v_k^T \quad a_k^T]^T$.

Definition 4: Observer (16) is regarded as an H_∞ observer of plant (2), if

1) $d_k = 0$, $e_k \to 0$ as $k \to \infty$;

2) $d_k \ne 0$, the following inequalities hold with $e_0 = 0$

$$\sum_{k=0}^{\infty} e_k^T e_k \le \gamma \sum_{k=0}^{\infty} d_k^T d_k, \tag{19}$$

where $\gamma > 0$ represents the disturbance attenuate level.

Then, the following theorem gives the sufficient conditions of the existence of the H_∞ observer (16).

Theorem 3: Given a constant $0 < \xi < 1$, if there exist a scalar $\gamma > 0$ and a matrix $P \succ 0$ such that

$$\begin{bmatrix} A_e^T PA_e - \xi P + I & * \\ B_e^T PA_e & B_e^T PB_e - \gamma I \end{bmatrix} \prec 0, \tag{20}$$

then (16) is an H_∞ observer of (2)

Proof: Choose the Lyapunov candidate function as

$$V_k = e_k^T Pe_k.$$

We will use the following two steps to complete the proof.

(i) $d_k = 0$. Taking the forward difference of V_k along the error system (18) yields

$$\triangle V_k = V_{k+1} - V_k = e_k^T[A_e^T PA_e - P]e_k. \tag{21}$$

(20) implies that $A_e^T PA_e - \xi P + I < 0$, and (21) becomes

$$\triangle V_k \le (\xi - 1)e_k^T Pe_k - e_k^T e_k \le (\xi - 1)V_k,$$

which indicates

$$V_{k+1} \le \xi V_k \le \cdots \le \xi^{k+1} V_0. \tag{22}$$

By the fact that $V_k \geq \underline{eig}(P)\|e_k\|^2$ and $V_0 \leq \overline{eig}(P)\|e_0\|^2$, one gets

$$\underline{eig}(P)\|e_k\|^2 \leq V_k \leq \xi^k V_0 \leq \xi^k \overline{eig}(P)\|e_0\|^2,$$

i.e.,

$$\|e_k\| \leq \sqrt{\frac{\xi^k \overline{eig}(P)}{\underline{eig}(P)}}\|e_0\|. \tag{23}$$

Given that $0 < \xi < 1$, it is deduced from (23) that $\lim_{k\to\infty}\|e_k\| = 0$.

(ii) $d_k \neq 0$. Let $J = \sum_{k=0}^{\infty} e_k^T e_k - \gamma \sum_{k=0}^{\infty} d_k^T d_k = \sum_{k=0}^{\infty}[e_k^T e_k - \gamma d_k^T d_k]$. By considering $e_0 = 0$, it follows that

$$\begin{aligned}&\sum_{k=0}^{\infty} \triangle V_k \\ &= \lim_{k\to\infty}\{V_k - V_{k-1} + V_{k-1} - V_{k-2} + \cdots + V_1 - V_0\} \\ &= \lim_{k\to\infty} V_k \geq 0.\end{aligned}$$

Therefore, $J \leq \sum_{k=0}^{\infty}[e_k^T e_k - \gamma d_k^T d_k + \triangle V_k]$. Premultiplying both sides of (20) by $\begin{bmatrix} e_k^T & d_k^T \end{bmatrix}$ and postmultiplying them by $\begin{bmatrix} e_k & d_k \end{bmatrix}^T$, we have

$$\begin{aligned}&e_k^T[A_e^T P A_e - \xi P + I]e_k + 2d_k^T B_e^T P A_e e_k \\ &+ d_k^T[B_e^T P B_e - \gamma I]d_k < 0.\end{aligned} \tag{24}$$

Denote that $T_k = e_k^T e_k - \gamma d_k^T d_k + \Delta V_k$, it is derived from (24) that

$$\begin{aligned}T_k &= e_{k+1}^T P e_{k+1} + e_k^T(I - P)e_k - \gamma d_k^T d_k \\ &= e_k^T(A_e^T P A_e - P + I)e_k + 2d_k^T B_e^T P A_e e_k \\ &\quad + d_k^T(B_e^T P B_e - \gamma I)d_k \\ &\leq (\xi - 1)e_k^T P e_k < 0.\end{aligned}$$

Therefore, $J \leq \sum_{k=0}^{\infty} T_k \leq 0$, i.e.,

$$\sum_{k=0}^{\infty} e_k^T e_k - \gamma \sum_{k=0}^{\infty} d_k^T d_k \leq 0,$$

$$\sum_{k=0}^{\infty} e_k^T e_k \leq \gamma \sum_{k=0}^{\infty} d_k^T d_k.$$

The proof is completed.

Then, the following processes are employed to transform (20) into a linear matrix inequality (LMI):

Step 1: Recast (20) as:

$$\begin{bmatrix} I - \xi P & * \\ 0 & -\gamma I \end{bmatrix} + \begin{bmatrix} A_e^T \\ B_e^T \end{bmatrix} P \begin{bmatrix} A_e & B_e \end{bmatrix} \prec 0. \tag{25}$$

Step 2: By using Schur complement, (25) becomes

$$\begin{bmatrix} I - \xi P & * & * \\ 0 & -\gamma I & * \\ PA_e & PB_e & -P \end{bmatrix} \prec 0. \tag{26}$$

Step 3: Let $Y = PH$, Substituting $A_e = A - HC$ and $B_e = \begin{bmatrix} B & -H & -H \end{bmatrix}$ into (26), it becomes

$$\begin{bmatrix} I - \xi P & * & * & * & * \\ 0 & -\gamma I_{n_\omega} & * & * & * \\ 0 & 0 & -\gamma I_{n_y} & * & * \\ 0 & 0 & 0 & -\gamma I_{n_y} & * \\ PA - YC & PB & -Y & -Y & -P \end{bmatrix} \prec 0. \tag{27}$$

The maximal robustness of observer (16) can be achieved by solving the following optimization problem:

$$min\ \gamma,\ subject\ to\ (27).$$

Finally, the observer gain is determined by $H = P^{-1}Y$.

Following determination of the observer gain H, Theorem 4 is given below to calculate the interval estimation of x_k.

Theorem 4: For system (2) and robust observer (16), interval estimation $[\underline{x}_k, \bar{x}_k]$ can be completed based on (17) given that $\hat{x}_0 = c_0$, where $\bar{e}_k$ and $\underline{e}_k$ are deduced from

$$\begin{aligned}[\underline{e}_k, \bar{e}_k] = Box((A - HC)^k\langle 0, G_0\rangle) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A - HC)^i B\mathbf{W}) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A - HC)^i(-H\mathbf{V})) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A - HC)^i(-H\mathbf{\Lambda})),\end{aligned} \tag{28}$$

with

$$[\underline{e}_0, \bar{e}_0] = Box(\langle 0, G_0\rangle). \tag{29}$$

Proof: From the error system (18), we obtain that

$$\begin{aligned}e_{k+1} &= (A - HC)e_k + B\omega_k - Hv_k - Ha_k \\ &= (A - HC)[(A - HC)e_{k-1} + B\omega_{k-1} - Hv_{k-1} \\ &\quad - Ha_{k-1}] + B\omega_k - Hv_k - Ha_k \\ &= \cdots \\ &= (A - HC)^{k+1}e_0 + \sum_{i=0}^{k}(A - HC)^i B\omega_{k-i} \\ &\quad + \sum_{i=0}^{k}(A - HC)^i(-Hv_{k-i}) \\ &\quad + \sum_{i=0}^{k}(A - HC)^i(-Ha_{k-i}).\end{aligned} \tag{30}$$

Denote the reachable set of e_k as $\mathbf{\Omega_k}$, then it follows from (30) that

$$\begin{aligned}\mathbf{\Omega_k} = (A-HC)^k\mathbf{\Omega_0} \oplus \bigoplus_{i=0}^{k-1}(A-HC)^iB\mathbf{W} \\ \oplus \bigoplus_{i=0}^{k-1}(A-HC)^i(-H\mathbf{V}) \\ \oplus \bigoplus_{i=0}^{k-1}(A-HC)^i(-H\mathbf{\Lambda}).\end{aligned} \tag{31}$$

From (31) and Property 2, the interval hull of $\mathbf{\Omega_k}$ is determined by

$$\begin{aligned}Box(\mathbf{\Omega_k}) = Box((A-HC)^k\mathbf{\Omega_0}) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^iB\mathbf{W}) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i(-H\mathbf{V})) \\ \oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i(-H\mathbf{\Lambda})).\end{aligned} \tag{32}$$

Additionally, $\hat{x}_0 = c_0$ indicates that $e_0 \in \langle 0, G_0\rangle$ since $x_0 \in \langle c_0, G_0\rangle$, which implies $\mathbf{\Omega}_0 = \langle 0, G_0\rangle$. Therefore, we have

$$[\underline{e}_k, \bar{e}_k] = Box(\mathbf{\Omega}_k), \forall k \geq 0. \tag{33}$$

On account of $e_k \in \mathbf{\Omega}_k \subseteq Box(\mathbf{\Omega}_k)$, one can obtain that $e_k \in [\underline{e}_k, \bar{e}_k]$, i.e. $\underline{e}_k \leq e_k \leq \bar{e}_k$. Finally, from (17), we have $\underline{x}_k \leq x_k \leq \bar{x}_k$. This completes the proof.

Remark 3: The steps for designing an improved interval observer for CPSs subject to stealthy attacks are given in the algorithm below.

Remark 4: In this section, interval estimation of state vector is completed by calculating the sum of the interval estimation of the error e_k and the state estimation of the robust Luenberger observer. For the purpose of obtaining higher accuracy of state estimation $[\underline{x}_k, \bar{x}_k]$ than that by interval observers, the key lies in two aspects: (i) the established observer is robust against disturbances and stealthy attacks; (ii) the approximated boundaries of estimation error are small enough.

Algorithm 1: *Algorithm for Interval Estimation for CPSs Subject to Stealthy Attacks.*

Input: A, C, c_0, G_0, $\mathbf{W}$, $\mathbf{V}$, ξ
Output: $\bar{x}_k$, $\underline{x}_k$
Given the values of matrices A, C **and zonotope** $\mathbf{W}$;
do
$\mathbf{\Lambda} = CA^k\langle 0, 2G_0\rangle \oplus \bigoplus_{i=0}^{k-1} Box(2CA^iB\mathbf{W})$;
Output: $\mathbf{\Lambda}$;
Given the values of matrices A, B, C ***and scalar*** ξ***;***
Solve LMI (27);
Output: γ, Y;
do
$H = P^{-1}Y$;
Given zonotope $\mathbf{V}$, $\mathbf{W}$ ***and initial values:***
$\hat{x}_0 = c_0$, $[\underline{e}_0, \bar{e}_0] = Box(\langle 0, G_0\rangle)$;
for $k \geq 0$, ***do***
$\hat{x}_{k+1} = A\hat{x}_k + H(y_k - C\hat{x}_k)$;
$[\underline{e}_k, \bar{e}_k] = Box((A-HC)^k\langle 0, G_0\rangle)$
$\oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^iB\mathbf{W})$
$\oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i(-H\mathbf{V}))$
$\oplus \bigoplus Box((A-HC)^i(-H\mathbf{\Lambda}))$;
$\bar{x}_k = \hat{x}_k + \bar{e}_k$, $\underline{x}_k = \hat{x}_k + \underline{e}_k$;
end for

V. Comparison Between the Method Based on the Monotone System Method and the Improved Method

In this section, the objective is to compare the improved method with the monotone system method to theoretically verify the superiority of the proposed method. To begin with, the following lemmas are presented.

Lemma 2: [30] Given a vector $s \in R^n$ and a matrix $L \in R^{m\times n}$, if there exist $\underline{s}, \bar{s} \in R^n$ satisfying $\underline{s} \leq s \leq \bar{s}$, then

$$L^+\underline{s} - L^-\bar{s} \leq Ls \leq L^+\bar{s} - L^-\underline{s}. \tag{34}$$

Lemma 3: [21] Given a nonnegative matrix $M \in R^{m\times n}$ and an interval vector $\boldsymbol{\eta} = [u, v] \subset R^n$, the following equality holds

$$Box(M\boldsymbol{\eta}) = M\boldsymbol{\eta} = [Mu, Mv].$$

Theorem 5: For system (2) with the same initial conditions that $\bar{x}_0^t = \bar{x}_0$ and $\underline{x}_0^t = \underline{x}_0$, the following inequalities

$$\begin{cases} \bar{x}_k^t \geq \bar{x}_k, \\ \underline{x}_k^t \leq \underline{x}_k, \end{cases}$$

hold for the interval estimation obtained by the improved method and that by (11)-(13).

Proof: The proof will be done in two steps.

(i) $T = I$. In this case, we can recast the interval observer (11)-(13) as:

$$\begin{cases} \bar{x}_{k+1}^t = (A-HC)\bar{x}_k^t + Hy_k + \bar{f}, \\ \underline{x}_{k+1}^t = (A-HC)\underline{x}_k^t + Hy_k + \underline{f}, \end{cases} \tag{35}$$

where

$$\begin{cases} \bar{f} = B^+\bar{\omega} - B^-\underline{\omega} + (-H)^+\bar{v} - (-H)^-\underline{v} \\ \qquad +(-H)^+\bar{a}_k - (-H)^-\underline{a}_k, \\ \underline{f} = B^+\underline{\omega} - B^-\bar{\omega} + (-H)^+\underline{v} - (-H)^-\bar{v} \\ \qquad +(-H)^+\underline{a}_k - (-H)^-\bar{a}_k. \end{cases} \tag{36}$$

Define

$$\begin{cases} \bar{e}_k^o = \bar{x}_k^t - \hat{x}_k, \\ \underline{e}_k^o = \underline{x}_k^t - \hat{x}_k. \end{cases} \tag{37}$$

By subtracting (16) from (35), we have

$$\begin{cases} \bar{e}_k^o = (A-HC)^k\bar{e}_0^o + \sum_{i=0}^{k-1}(A-HC)^i\bar{f}, \\ \underline{e}_k^o = (A-HC)^k\underline{e}_0^o + \sum_{i=0}^{k-1}(A-HC)^i\underline{f}. \end{cases} \tag{38}$$

Define $\breve{\mathbf{\Omega}}_{\mathbf{k}}$ as

$$\begin{aligned}\breve{\mathbf{\Omega}}_{\mathbf{k}} &= Box((A-HC)^k Box(\mathbf{\Omega_0}))\\ &\oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i Box(B\mathbf{W}))\\ &\oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i Box(-H\mathbf{V}))\\ &\oplus \bigoplus_{i=0}^{k-1} Box((A-HC)^i Box(-H\mathbf{\Lambda})).\end{aligned} \tag{39}$$

According to Lemma 3, we have

$$\begin{aligned}\breve{\mathbf{\Omega}}_{\mathbf{k}} &= (A-HC)^k Box(\mathbf{\Omega_0}) \oplus \bigoplus_{i=0}^{k-1}(A-HC)^i Box(B\mathbf{W})\\ &\oplus \bigoplus_{i=0}^{k-1}(A-HC)^i Box(-H\mathbf{V})\\ &\oplus \bigoplus_{i=0}^{k-1}(A-HC)^i Box(-H\mathbf{\Lambda})\\ &= (A-HC)^k Box(\mathbf{\Omega_0}) \oplus \bigoplus_{i=0}^{k-1}(A-HC)^i Box(B\mathbf{W}\\ &\oplus (-H\mathbf{V}) \oplus (-H\mathbf{\Lambda})) \supseteq Box(\mathbf{\Omega_k}).\end{aligned}$$

Furthermore, by Lemma 2, (36) indicates $\underline{f} \le B\omega_k - Hv_k - Ha_k \le \bar{f}$. Then it follows that

$$Box(B\mathbf{W} \oplus (-H\mathbf{V}) \oplus (-H\mathbf{\Lambda})) = [\underline{f}, \bar{f}].$$

Therefore, $\breve{\mathbf{\Omega}}_{\mathbf{k}}$ can be recast as

$$\breve{\mathbf{\Omega}}_{\mathbf{k}} = (A-HC)^k[\underline{e}_0, \bar{e}_0] \oplus \bigoplus_{i=0}^{k-1}(A-HC)^i[\underline{f}, \bar{f}] \triangleq [\underline{e}_k^{\omega}, \bar{e}_k^{\omega}],$$

where

$$\begin{cases} \bar{e}_k^{\omega} = (A-HC)^k \bar{e}_0 + \sum_{i=0}^{k-1}(A-HC)^i \bar{f}, \\ \underline{e}_k^{\omega} = (A-HC)^k \underline{e}_0 + \sum_{i=0}^{k-1}(A-HC)^i \underline{f}. \end{cases} \tag{40}$$

By comparing (32) with (39), we obtain that $Box(\mathbf{\Omega_k}) \subseteq \breve{\mathbf{\Omega}}_{\mathbf{k}}$. Moreover, it follows from (38) and (40) that

$$\begin{cases} \bar{e}_k \le \bar{e}_k^{\omega} = \bar{e}_k^{o}, \\ \underline{e}_k \ge \underline{e}_k^{\omega} = \underline{e}_k^{o}. \end{cases} \tag{41}$$

Finally, (41) implies that

$$\begin{cases} \bar{x}_k^t = \hat{x}_k + \bar{e}_k^o \ge \hat{x}_k + \bar{e}_k = \bar{x}_k, \\ \underline{x}_k^t = \hat{x}_k + \underline{e}_k^o \le \hat{x}_k + \underline{e}_k = \underline{x}_k. \end{cases}$$

(ii) $T \ne I$. Substituting the coordinate transformation $\hat{z}_k = T\hat{x}_k$ into (16) yields

$$\hat{z}_{k+1} = TAT^{-1}\hat{z}_k + TH(y_k - CT^{-1}\hat{z}_k).$$

Define $e_k^z = z_k - \hat{z}_k$, we have $e_k^z = Te_k$. Denote the reachable set of e_k^z by $\mathbf{\Omega_k^z}$, then $\mathbf{\Omega_k^z} = T\mathbf{\Omega_k}$. Define that $Box(\mathbf{\Omega_k^z}) = [\underline{e}_k^z, \bar{e}_k^z]$, then $\underline{e}_k^z \le e_k^z \le \bar{e}_k^z$. Let

$$\begin{cases} e_k^{z\uparrow} = \bar{z}_k - \hat{z}_k = T\bar{e}_k^o, \\ e_k^{z\downarrow} = \underline{z}_k - \hat{z}_k = T\underline{e}_k^o. \end{cases}$$

Premultiplying both sides of (41) by T, we obtain

$$\begin{cases} \bar{e}_k^z \le e_k^{z\uparrow}, \\ \underline{e}_k^z \ge e_k^{z\downarrow}. \end{cases} \tag{42}$$

Denote the parallelotope described by $\underline{e}_k^z \le Te_k \le \bar{e}_k^z$ as $\mathbf{P}$. In view of the fact that $\mathbf{\Omega_k}$ is the reachable set of e_k, the relationship $\mathbf{\Omega_k} \subseteq \mathbf{P}$ holds since $\mathbf{P}$ represents the set of e_k after being multiplied by matrix T (In particular, $\mathbf{\Omega_k} \equiv \mathbf{P}$ when $T \equiv I$). Moreover, define a new parallelotope $\hat{\mathbf{P}}$ representing the set of e_k, and it is described by $e_k^{z\downarrow} \le Te_k \le e_k^{z\uparrow}$. It can be deduced directly from (42) that $\mathbf{P} \subseteq \hat{\mathbf{P}}$. Therefore, we have

$$\mathbf{\Omega_k} \subseteq \mathbf{P} \subseteq \hat{\mathbf{P}}. \tag{43}$$

Moreover, (13) implies that

$$\begin{cases} \bar{x}_k^t = (T^{-1})^+ \bar{z}_k - (T^{-1})^- \underline{z}_k, \\ \underline{x}_k^t = (T^{-1})^+ \underline{z}_k - (T^{-1})^- \bar{z}_k. \end{cases} \tag{44}$$

Define

$$\begin{cases} \bar{e}_k^t = \bar{x}_k^t - \hat{x}_k, \\ \underline{e}_k^t = \underline{x}_k^t - \hat{x}_k. \end{cases}$$

Note that $\hat{x}_k = T^{-1}\hat{z}_k = [(T^{-1})^+ - (T^{-1})^-]\hat{z}_k$, subtracting it from (44) yields

$$\begin{cases} \bar{e}_k^t = (T^{-1})^+ e_k^{z\uparrow} - (T^{-1})^- e_k^{z\downarrow}, \\ \underline{e}_k^t = (T^{-1})^+ e_k^{z\downarrow} - (T^{-1})^- e_k^{z\uparrow}. \end{cases} \tag{45}$$

In addition, if $e_k^{z\downarrow} \le e_k^z = Te_k \le e_k^{z\uparrow}$, i.e., $e_k \in \hat{\mathbf{P}}$, we have $T^{-1}e_k^{z\downarrow} \le e_k \le T^{-1}e_k^{z\uparrow}$, then, according to (45) and Lemma 2, the following inequality holds

$$\underline{e}_k^t \le e_k \le \bar{e}_k^t, \tag{46}$$

then $[\underline{e}_k^t, \bar{e}_k^t] = Box(\hat{\mathbf{P}})$. Furthermore, (43) means that $Box(\mathbf{\Omega_k}) \subseteq Box(\hat{\mathbf{P}})$. Subsequently, we have

$$\begin{cases} \bar{e}_k^t \ge \bar{e}_k, \\ \underline{e}_k^t \le \underline{e}_k, \end{cases} \tag{47}$$

which implies that

$$\begin{cases} \bar{x}_k^t = \hat{x}_k + \bar{e}_k^t \ge \hat{x}_k + \bar{e}_k = \bar{x}_k, \\ \underline{x}_k^t = \hat{x}_k + \underline{e}_k^t \ge \hat{x}_k + \underline{e}_k = \underline{x}_k. \end{cases}$$

The proof is completed here.

Remark 5: Note that when $T = I$, the observer gain matrix H is designed such that $A - HC$ is both Schur and nonnegative, which is not a trivial work. However, when $T \ne I$, the interval observer is designed by using coordinate transformation, which is able to relax the design constraint of matrix L by only requiring $A - HC$ to be Schur and $K = T^{-1}(A - HC)T$ to be nonnegative. No matter which case the matrix T is, it is proved that the improved method is better than the traditional

method. Moreover, since the H_∞ observer does not need to satisfy the cooperative condition, it is no longer necessary to find an appropriate coordinate transformation.

VI. Illustrative Examples

In this section, two examples are provided to verify the main results of this paper.

A. Example 1

Let us consider a DC motor with one tacho generator and one incremental encoder [31], whose dynamics can be described by

$$\begin{bmatrix}\dot{\theta}(t)\\ \dot{\alpha}(t)\\ \dot{i}(t)\end{bmatrix}=\begin{bmatrix}0 & 1 & 0\\ 0 & -\frac{b}{J} & \frac{K}{J}\\ 0 & -\frac{K}{L} & -\frac{R}{L}\end{bmatrix}\begin{bmatrix}\theta(t)\\ \alpha(t)\\ i(t)\end{bmatrix}+\begin{bmatrix}0\\ 0\\ \frac{1}{L}\end{bmatrix}V \tag{48}$$

where $\theta(t)$ is the angular velocity of the motor, $\alpha(t)$ is the angular acceleration, $i(t)$ is the armature current, $b=0.1482[Nms]$ is frictional coefficient, $J=0.0985[kgm^2]$ is the armature moment of inertia, $K=0.4901[Vs/rad]$ stands for both the motor torque constant and the back emf constant, $L=1.3726[H]$ is the inductance, $R=0.0062[\Omega]$ is the resistance, and V is the voltage source applied to the motor armature. Here, we consider the zero input response of (48), i.e., $V=0$, $x(0)=\begin{bmatrix}\theta(0) & \alpha(0) & i(0)\end{bmatrix}^T\neq\mathbf{0}$. In the sequel, we choose the measured output $y(t)=\theta(t)$, by using the Euler method with sampling time $T_s=0.1\,s$ and considering the effect of unknown process noise ω_k, measurement error v_k and cyber attack a_k, the dynamics of DC motor can be discretized as

$$\begin{cases}x_{k+1}=Ax_k+B\omega_k,\\ y_k=Cx_k+v_k+a_k,\end{cases} \tag{49}$$

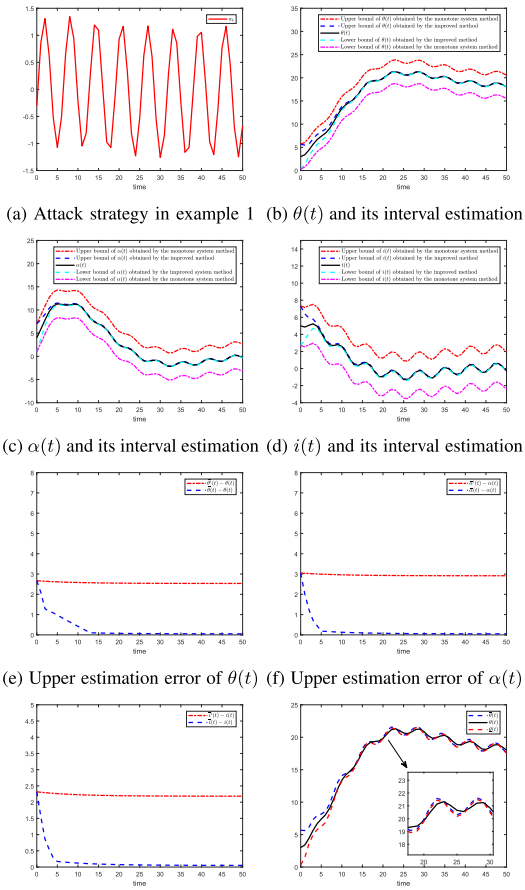
where

$$A=\begin{bmatrix}1.0000 & 0.1000 & 0\\ 0 & 0.8495 & 0.4977\\ 0 & -0.0357 & 0.9995\end{bmatrix},B=\begin{bmatrix}0.1\\ 0.1\\ 0.1\end{bmatrix},$$
$$C=\begin{bmatrix}1 & 0 & 0\end{bmatrix}.$$

Choose $H_1=\begin{bmatrix}1.515 & 0.3729 & -0.3495\end{bmatrix}^T$ such that $A-H_1C$ is Schur, and then apply coordinate transformation $z_k=Tx_k$, where T is given by

$$T=\begin{bmatrix}0.0605 & 0.1645 & 0.0032\\ 0.8929 & 0.9474 & 0.6360\\ 0.8426 & 0.1248 & 0.1151\end{bmatrix}.$$

Therefore, $K=T^{-1}(A-H_1C)T$ is both Schur and nonnegative. The process noise and measurement error are assumed to be bounded by $|\omega_k|\leq 0.5, |v_k|\leq 0.5$ and the initial condition is chosen as



(a) Attack strategy in example 1 (b) $\theta(t)$ and its interval estimation

(c) $\alpha(t)$ and its interval estimation (d) $i(t)$ and its interval estimation

(e) Upper estimation error of $\theta(t)$ (f) Upper estimation error of $\alpha(t)$

(g) Upper estimation error of $i(t)$ (h) Response of $\theta(t)$,$\bar{\theta}(t)$,$\underline{\theta}(t)$

Fig. 2. Simulation results of Example 1.

$$x(0)=\begin{bmatrix}\theta(0)\\ \alpha(0)\\ i(0)\end{bmatrix}=\begin{bmatrix}3\,rd/s\\ 4\,rd/s^2\\ 5\,A\end{bmatrix}.$$

By solving LMI (27), we obtain $H_2=\begin{bmatrix}0.7020 & 0.5818 & 1.2166\end{bmatrix}^T$. The attack strategy is shown in Fig. 2(a). Since the adversaries are assumed to have access to the output y_k, they can generate such attack strategy according to Remark 1. Thus, it can be verified that a_k shown in Fig. 2(a) satisfies (5), i.e., the attack remains undetectable. The simulation results are shown in Fig. 2(b)–2(d).

It can be concluded from Fig. 2(b)–2(d) that under zero input condition, the DC motor accelerated from its initial value $\theta(0)=3\,rd/s$ to $21\,rd/s$ in the first 23 s and then converged to its steady state value with the armature current decreasing to zero. Moreover, despite the existence of stealthy attacks causing disrupted measurement, interval estimation for the parameters of DC motor with considerably high accuracy can still be achieved by using the proposed method. Fig. 2(e)-2(g) represent the estimation error of $\theta(t)$, $\alpha(t)$, $i(t)$ obtained by the two methods, respectively. To further illustrate the effectiveness of the proposed method, Table I is provided to illustrate the conservatism as well as computational complexity of the two methods. Table I

TABLE I
METHOD COMPARISON

	the monotone system method	the improved method
Estimation error of $\theta(t)$	2.5354	0.0512
Design conditions	$T^{-1}(A-HC)T \geq 0$	-
Algorithm steps	11	15

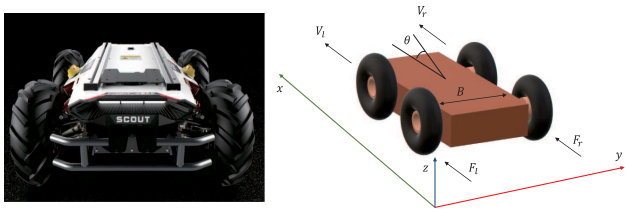
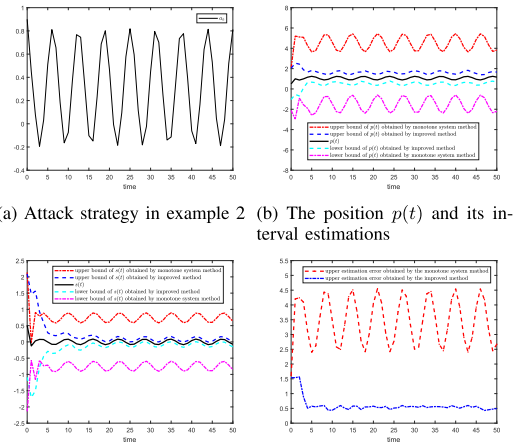


Fig. 3. The diagram of UGV.



(a) Attack strategy in example 2 (b) The position $p(t)$ and its interval estimations

(c) The velocity $s(t)$ and its interval estimations (d) Upper estimation error of p(t)

Fig. 4. Simulation results of Example 2.

indicates that, as is proved in Section V, interval estimation via the improved method is of higher accuracy than that via the monotone system method. Moreover, due to a relatively simple structure, less algorithm steps are needed to construct an interval observer by the monotone system method. However, the employment of the monotone system method requires stronger conditions than that of the improved method. It should be noted that for the monotone system method, the superiority of lower algorithm complexity is not significant enough compared to the improved method. Furthermore, it is not a trivial work to find a gain matrix H and a coordinate transformation matrix T to satisfy the design conditions. Therefore, interval estimation for CPSs via the improved method has some superiority.

In addition, it is worth noting that if the reachable set of a_k is not taken into account in Theorem 4, i.e., the terms containing $\mathbf{\Lambda}$ in (28) are removed, then the inequality $\underline{x}_k \leq x_k \leq \bar{x}_k$ does not hold, that is to say, the proposed method may not work. Thus, Theorem 1 is essential. For this case, we also do the simulation, the result of which is shown in Fig. 2(h).

B. Example 2

An Unmanned Ground Vehicle(UGV) [32] shown in Fig. 3 is considered in this example. It is assumed that the UGV travels in straight lines and then begins to rotate. In that case, the dynamics of the UGV can be described by

$$\begin{cases} \begin{bmatrix} \dot{p}(t) \\ \dot{s}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & \frac{-W}{M} \end{bmatrix} \begin{bmatrix} p(t) \\ s(t) \end{bmatrix} + \begin{bmatrix} \frac{-1}{M} & 0 \\ 0 & \frac{-1}{M} \end{bmatrix} \omega(t), \\ y(t) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} p(t) \\ s(t) \end{bmatrix} + v(t) + a(t), \end{cases} \tag{50}$$

where $p(t)$, $s(t)$, W, M and $\omega(t)$ are the position, velocity, translational friction coefficient, mechanical mass and process noise, respectively. $y(t)$ is the output, $v(t)$ and $a(t)$ are the measurement error and attack signal, respectively. It is assumed that $M = 0.8, W = 1$. Similar to Example 1, (50) can be discretized as

$$\begin{cases} x_{k+1} = Ax_k + B\omega_k, \\ y_k = Cx_k + v_k + a_k, \end{cases}$$

where

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -0.25 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

The process noise and measurement error are bounded as follows:

$$|\omega_k| \leq \begin{vmatrix} 0.1 \\ 0.1 \end{vmatrix}, |v_k| \leq \begin{vmatrix} 0.1 \\ 0.1 \end{vmatrix}.$$

Note that there is no matrix H such that $A - HC$ is both Schur and nonnegative. Consider the coordinate transformation $z = Tx$, where

$$T = \begin{bmatrix} -0.9942 & 2.2350 \\ -0.0264 & -2.0213 \end{bmatrix}.$$

Choose $H_1 = \begin{bmatrix} 0.5173 & -0.1637 \end{bmatrix}^T$ such that

$$K = T(A - H_1C)T^{-1} = \begin{bmatrix} 0.9160 & 0.8696 \\ 0.3419 & 0.1411 \end{bmatrix}$$

is a Schur and nonnegative matrix. Furthermore, by solving LMI (27), we obtain that $H_2 = \begin{bmatrix} 1.9208 & 0.0195 \end{bmatrix}^T$. The initial conditions are selected as $x_0 = \begin{bmatrix} 0.5 & 0.5 \end{bmatrix}^T$, and the initial estimations are chosen as $\bar{x}_0^t = \bar{x}_0 = \begin{bmatrix} 2 & 2 \end{bmatrix}^T$, $\underline{x}_0^t = \underline{x}_0 = \begin{bmatrix} -2 & -2 \end{bmatrix}^T$. In order to satisfy (5), the attack strategy is chosen as shown in Fig. 4(a). The simulation results are shown in Fig. 4(b) and Fig. 4(c).

It can be seen from Fig. 4(b) and Fig. 4(c) that the UGV moves forward with decreasing velocity and then starts to rotate with a periodical change of speed. The proposed method provides a precise estimation of the position and velocity after necessary initialization.

VII. Conclusion

This paper investigates interval estimation methods for CPSs under stealthy attacks. The upper and lower boundaries of stealthy attacks are obtained using set-membership estimation method. By combining the monotone system method with the boundaries of stealthy attacks, an interval observer is designed to estimate states against stealthy attacks. In order to improve the estimation accuracy, the reachability analysis is introduced combined with H_∞ techniques. Comparisons between the monotone system method and the improved method are also presented. Finally, illustrative examples are given to demonstrate the effectiveness of the main results of this paper. Possible future work includes the research of interval estimation methods for distributed CPSs.

References

[1] X. Cao, P. Cheng, J. Chen, and Y. Sun, "An online optimization approach for control and communication codesign in networked cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 439–450, Feb. 2013.

[2] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4242–4268, 2014.

[3] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[4] Y. Chen, S. Kar, and J. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Control Netw. Syst.*, vol. 5, no. 3, pp. 1157–1168, Sep. 2018.

[5] Q. Zhang, K. Liu, Y. Xia, and A. Ma, "Optimal stealthy deception attack against cyber-physical systems," *IEEE Trans. Syst., Man, Cybern.*, vol. 50, no. 9, pp. 3963–3972, Sep. 2020.

[6] A. Lu and G. Yang, "Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer," *Inf. Sci.*, vol. 417, no. 1/2, pp. 454–464, 2017.

[7] D. Ding, Q. 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, no. 18, pp. 1674–1683, 2018.

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

[9] R. Gentz, S. Wu, H. Wai, A. Scaglione, and A. Leshem, "Data injection attacks in randomized gossiping," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 2, no. 4, pp. 523–538, Dec. 2016.

[10] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[11] J. Gouzé, A. Rapaport, and M. Hadj-Sadok, "Interval observers for uncertain biological systems," *Ecological Model.*, vol. 133, no. 1, pp. 45–56, 2000.

[12] X. Wang, H. Su, F. Zhang, A. Zemouche, and G. Chen, "Interval observer design and consensus of multiagent systems with time-varying interval uncertainties," *SIAM J. Control Optim.*, vol. 59, no. 5, pp. 3392–3417, 2021.

[13] X. Wang, X. Wang, H. Su, and J. Lam, "Reduced-order interval observer based consensus for mass with time-varying interval uncertainties," *Automatica*, vol. 135, 2022, Art. no. 109989.

[14] F. Mazenc and O. Bernard, "Interval observers for linear time-invariant systems with disturbances," *Automatica*, vol. 47, no. 1, pp. 140–147, 2011.

[15] T. Raïssi, D. Efimov, and A. Zolghadri, "Interval state estimation for a class of nonlinear systems," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 260–265, Jan. 2012.

[16] H. Ethabet, D. Rabehi, D. Efimov, and T. Raïssi, "Interval estimation for continuous-time switched linear systems," *Automatica*, vol. 90, no. 90, pp. 230–238, 2018.

[17] D. Efimov, W. Perruquetti, T. Raïssi, and A. Zolghadri, "Interval observers for time-varying discrete-time systems," *IEEE Trans. Autom. Control*, vol. 58, no. 12, pp. 3218–3224, Dec. 2013.

[18] D. Efimov, L. Fridman, T. Raïssi, A. Zolghadri, and R. Seydou, "Interval estimation for LPV systems applying high order sliding mode techniques," *Automatica*, vol. 48, no. 9, pp. 2365–2371, 2012.

[19] G. Zheng, D. Efimov, F. Bejarano, W. Perruquetti, and H. Wang, "Interval observer for a class of uncertain nonlinear singular systems," *Automatica*, vol. 71, no. 71, pp. 159–168, 2016.

[20] K. Degue, D. Efimov, and J. Ny, "Interval observer approach to output stabilization of linear impulsive systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 5085–5090, 2017.

[21] W. Tang, Z. Wang, Y. Wang, T. Raïssi, and Y. Shen, "Interval estimation methods for discrete-time linear time-invariant systems," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4717–4724, Nov. 2019.

[22] J. Huang, X. Ma, H. Che, and Z. Han, "Further result on interval observer design for discrete-time switched systems and application to circuit systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 11, pp. 2542–2546, Nov. 2020.

[23] J. Huang, X. Ma, X. Zhao, H. Che, and L. Chen, "Interval observer design method for asynchronous switched systems," *IET Control Theory Appl.*, vol. 14, no. 8, pp. 1082–1090, 2020.

[24] H. Zhang, J. Huang, H. Che, and Z. Han, "Optimal interval observer for discrete-time switched systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, to be published, doi: 10.1109/TCSII.2021.3101585.

[25] J. Huang, H. Che, T. Raïssi, and Z. Wang, "Functional interval observer for discrete-time switched descriptor systems," *IEEE Trans. Autom. Control*, to be published, doi: 10.1109/TAC.2021.3079193.

[26] T. Chevet, T. Dinh, J. Marzat, Z. Wang, and T. Raïssi, "Zonotopic Kalman filter-based interval estimation for discrete-time linear systems with unknown inputs," *IEEE Contr. Syst. Lett.*, vol. 6, pp. 806–811, Jun. 2021.

[27] A. Tahir and B. Acikmese, "Synthesis of interval observers for bounded jacobian nonlinear discrete-time systems," *IEEE Contr. Syst. Lett.*, vol. 6, pp. 764–769, Jun. 2021.

[28] K. Degue, D. Efimov, J. Ny, and E. Feron, "Interval observers for secure estimation in cyber-physical systems," in *Proc. IEEE Conf. Decis. Control*, 2018, pp. 4559–4564.

[29] X. Li, G. Wei, and D. Ding, "Interval observer design under stealthy attacks and improved event-triggered protocols," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 6, pp. 570–579, Jul. 2020.

[30] D. Efimov, T. Raïssi, S. Chebotarev, and A. Zolghadri, "Interval state observer for nonlinear time varying systems," *Automatica*, vol. 49, no. 1, pp. 200–205, 2013.

[31] M. Buciakowski, M. Witczak, M. Mrugalski, and D. Theilliol, "A quadratic boundedness approach to robust DC motor fault estimation," *Control Eng. Pract.*, vol. 66, pp. 181–194, 2017.

[32] Y. Shoukry, P. Nuzzo, A. Puggelli, A. Sangiovanni-Vincentelli, S. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Trans. Autom. Control*, vol. 62, no. 10, pp. 4917–4932, Oct. 2017.

Jianwei Fan received the B.S. degree in electrical engineering and automation from Ningbo University, Ningbo, China, in 2020. He is currently working toward the M.S. degree in control engineering from Soochow University, Suzhou, China. His current research interests include cyber-physical systems and interval observers.

Jun Huang (Member, IEEE) received the M.S. degree in mathematics from East China Normal University, Shanghai, China, in 2008, and the Ph.D. degree in automation from Shanghai Jiao Tong University, Shanghai, China, in 2012. He is currently an Associate Professor with the School of Mechanical and Electrical Engineering, Soochow University, Suzhou, China. He has authored or coauthored more than 50 papers in refereed international journals. His current research interests include multiagent systems, the theory of interval observer design, nonlinear control and adaptive control.

Xudong Zhao (Member, IEEE) received the B.S. degree in automation from the Harbin Institute of Technology, Harbin, China, in 2005, and the Ph.D. degree from the Control Science and Engineering from Space Control and Inertial Technology Center, Harbin Institute of Technology, in 2010. Since December 2015, he has been with the Dalian University of Technology, Dalian, China, where he is currently a Professor. His research interests include hybrid systems, positive systems, multi-agent systems, and control of aero engine. He is an Associate Editor for the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, *Nonlinear Analysis: Hybrid Systems*, *Neurocomputing*, *International Journal of General Systems*, *ACTA Automatica Sinica*, *Assembly Automation*, and *Journal of Aeronautics*. He was awarded as the 2017-2020 Web of Science Highly Cited Researcher in Engineering.