2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Resilient State Estimation for Nonlinear Discrete-Time Systems via Input and State Interval Observer Synthesis

Mohammad Khajenejad, Zeyuan Jin, Thach Ngoc Dinh and Sze Zheng Yong

Abstract— **This paper addresses the problem of resilient state estimation and attack reconstruction for bounded-error nonlinear discrete-time systems with nonlinear observations/constraints, where both sensors and actuators can be compromised by false data injection attack signals/unknown inputs. By leveraging mixed-monotone decomposition of nonlinear functions, as well as affine parallel outer-approximation of the observation functions, along with introducing auxiliary states to cancel out the effect of the attacks/unknown inputs, our proposed observer recursively computes interval estimates that by construction, contain the true states and unknown inputs of the system. Moreover, we provide several semi-definite programs to synthesize observer gains to ensure input-to-state stability of the proposed observer and optimality of the design in the sense of minimum $\mathcal{H}_\infty$ gain.**

I. Introduction

State estimation and unknown input reconstruction are indispensable in various engineering applications such as aircraft tracking, fault detection, attack detection and mitigation in cyber-physical systems (CPS) and urban transportation [1]–[3]. Particularly, set-membership approaches have been proposed for bounded-error systems to provide hard accuracy bounds, which is especially useful for obtaining robustness guarantees for safety-critical systems. Moreover, since attackers may be strategic in adversarial settings, the ability to simultaneously estimate states and inputs without imposing any assumptions on the unknown inputs/attack signals is desirable and often crucial.

Literature review. Numerous studies in the literature have investigated *secure estimation*, i.e., how to accurately estimate the states of a system when it is under attack or subject to adversarial signals. For instance, secure state estimation and control problem was addressed in the presence of false data injection attacks on both the actuators and sensors in [4], in which a χ^2 detector was proposed to detect malicious attacks. The research in [5] proposed a sliding-mode observer to simultaneously estimate system states and attacks, while the work in [6] provided a projected sliding-mode observer-based estimation approach to reconstruct system states. Further, the work in [7] reconstructed attack signals from the equivalent output injection signal using a sliding-mode observer, while in [8], an attack was considered as an auxiliary state and estimated by employing a robust switching Luenberger observer assuming sparsity. However, all the aforementioned works considered stochastic/Gaussian noise and hence do not apply to the bounded-error setting we consider in this paper, where noise/disturbance signals are assumed to be distribution-free and bounded.

A related body of literature that could be applied to resilient state estimation in the bounded-error setting is that of unknown input interval observers. Particularly, the works in [9]–[11] considered the problem of designing unknown input interval observers for continuous-time linear parameter varying (LPV), uncertain linear time-invariant (LTI) and discrete-time switched linear systems, respectively, where the authors in [9] formulated the necessary Metzler property as part of a semi-definite program. A similar problem was considered for nonlinear continuous-time systems with linear observations in [12]. However, these approaches are not suitable for general discrete-time nonlinear systems and the unknown input signal does not affect the output/measurement equation (needed for representing false data injection attacks on the sensors) in either of the works in [9]–[12].

On the other hand, while our previous works [13], [14] do consider the design of state and unknown input interval observers for nonlinear discrete-time systems with nonlinear observations, no stabilizing gains were synthesized in [13], [14]. We aim to address this shortcoming in this paper.

Contributions. By leveraging a combination of mixed-monotone decomposition of nonlinear functions [15], [16] and parallel affine outer-approximation of observation functions [17], we synthesize a resilient interval observer, i.e., a discrete-time dynamical system that by construction, *simultaneously* returns interval-valued estimates of states and unknown inputs (representing false data injection signals on both the actuators and sensors) for a broad range of nonlinear discrete-time systems with nonlinear observations. Our proposed design is a significant improvement to our previous input and state interval observer designs [13], [14], in which no stabilizing gains were considered and so the stability of the previous observer designs only hinged upon some dynamical systems properties. Moreover, in contrast to many unknown input (interval) observer designs in the literature, our design considers arbitrary unknown input signals with no assumptions of *a priori* known intervals, being stochastic with zero mean (as is often assumed for noise) or bounded. Further, we provide sufficient conditions for the input-to-state-stability of the proposed observer, which at the same time ensures the optimality of the design in the sense of minimum $\mathcal{H}_\infty$ gain by solving semi-definite programs.

M. Khajenejad is with the University of California, San Diego, CA, USA. Z. Jin is with Arizona State University, Tempe, AZ, USA. T.N. Dinh is with Conservatoire National des Arts et Métiers (CNAM), CEDRIC-Laetitia, Paris, France. S.Z. Yong is with Northeastern University, Boston, MA, USA. (e-mail: mkhajenejad@ucsd.edu, zjin43@asu.edu, ngoc-thach.dinh@lecnam.net, s.yong@northeastern.edu).

This work is partially supported by NSF grant CNS-2313814.

2023 62nd IEEE Conference on Decision and Control (CDC) | 979-8-3503-0124-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CDC49753.2023.10384057

II. PRELIMINARIES

Notation. $\vee$ denotes the logical disjunction (the OR truth-functional operator). $\mathbb{R}^n, \mathbb{R}^{n\times p}, \mathbb{D}_n, \mathbb{N}, \mathbb{N}_n, \mathbb{R}_{\geq 0}$ and $\mathbb{R}_{>0}$ denote the n-dimensional Euclidean space and the sets of n by p matrices, n by n diagonal matrices, natural numbers (including 0), natural numbers from 1 to n, non-negative and positive real numbers, respectively, while $\mathbb{M}_n$ denotes the set of all n by n Metzler matrices, i.e., square matrices whose off-diagonal elements are non-negative. Euclidean norm of a vector $x \in \mathbb{R}^n$ is denoted by $\|x\|_2 \triangleq \sqrt{x^\top x}$. For $M \in \mathbb{R}^{n\times p}$, M_{ij} denotes M's entry in the i'th row and the j'th column, $M^\oplus \triangleq \max(M, \mathbf{0}_{n,p})$, $M^\ominus = M^\oplus - M$ and $|M| \triangleq M^\oplus + M^\ominus$, where $\mathbf{0}_{n,p}$ is the zero matrix in $\mathbb{R}^{n\times p}$, while $\mathrm{sgn}(M) \in \mathbb{R}^{n\times p}$ is the element-wise sign of M with $\mathrm{sgn}(M_{ij}) = 1$ if $M_{ij} \geq 0$ and $\mathrm{sgn}(M_{ij}) = -1$, otherwise. $M \succ 0$ and $M \prec 0$ (or $M \succeq 0$ and $M \preceq 0$) denote that M is positive and negative (semi-)definite, respectively. Further, a function $f : S \subseteq \mathbb{R}^n \to \mathbb{R}$, where $0 \in S$, is positive definite if $f(x) > 0$ for all $x \in S\backslash\{0\}$, and $f(0) = 0$. Finally, an interval $\mathcal{I} \triangleq [\underline{z}, \overline{z}] \subset \mathbb{R}^n$ is the set of all real vectors $z \in \mathbb{R}^{n_z}$ that satisfies $\underline{z} \leq z \leq \overline{z}$ (component-wise), where $\|\overline{z} - \underline{z}\|_\infty \triangleq \max_{i\in\{1,\cdots,n_z\}} |z_i|$ is the interval width of $\mathcal{I}$.

Next, we review some related results and definitions.

Proposition 1 (Jacobian Sign-Stable Decomposition [15, Proposition 2])**.** *If a mapping $f : \mathcal{Z} \subset \mathbb{R}^{n_z} \to \mathbb{R}^p$ has Jacobian matrices satisfying $J^f(x) \in [\underline{J}^f, \overline{J}^f]$, $\forall z \in \mathcal{Z}$, where $\underline{J}^f, \overline{J}^f \in \mathbb{R}^{p\times n_z}$ are known matrices, then the mapping f can be decomposed into an additive remainder-form:*

$$\forall z \in \mathcal{Z}, f(z) = Hz + \mu(z), \tag{1}$$

where the matrix $H \in \mathbb{R}^{p\times n_z}$ satisfies

$$\forall (i,j) \in \mathbb{N}_p \times \mathbb{N}_{n_z}, H_{ij} = \underline{J}^f_{ij} \ \vee H_{ij} = \overline{J}^f_{i,j}, \tag{2}$$

and $\mu(\cdot)$ and Hz are nonlinear and linear Jacobian sign-stable (JSS) mappings, respectively, i.e., the signs of each element of their Jacobian matrices do not change within their domains ($J^\nu_{ij}(\cdot) \geq 0$ or $J^\nu_{ij}(\cdot) \leq 0$, $\nu(z) \in \{\mu(z), Hz\}$).

Definition 1 (Mixed-Monotonicity and Decomposition Functions)**.** *[18, Definition 1], [19, Definition 4] Consider the discrete-time dynamical system $x_{k+1} = g(x_k)$, with initial state $x_0 \in \mathcal{X}_0 \triangleq [\underline{x}_0, \overline{x}_0] \subset \mathbb{R}^n$. Furthermore, $g : \mathcal{X} \subset \mathbb{R}^n \to \mathbb{R}^n$ is the vector field, and $\mathcal{X}$ is the entire state space. A function $g_d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}^n$ is a discrete-time mixed-monotone decomposition mapping for the vector field g if it satisfies the following conditions: i) $g_d(x, x) = g(x)$, ii) g_d is monotone increasing in its first argument, i.e., $\hat{x} \geq x \Rightarrow g_d(\hat{x}, x') \geq g_d(x, x')$, and iii) g_d is monotone decreasing in its second argument, i.e., $\hat{x} \geq x \Rightarrow g_d(x', \hat{x}) \leq g_d(x', x)$.*

Proposition 2 (Tight and Tractable Decomposition Functions for JSS Mappings)**.** *[15, Proposition 4 & Lemma 3] Suppose $\mu : \mathcal{Z} \subset \mathbb{R}^{n_z} \to \mathbb{R}^p$ is a JSS mapping on its domain. Then, for each μ_i, $i \in \mathbb{N}_p$, its tight decomposition function is:*

$$\mu_{d,i}(z_1, z_2) = \mu_i(D^i z_1 + (I_n - D^i) z_2), \tag{3}$$

for any ordered $z_1, z_2 \in \mathcal{Z}$, with a binary diagonal matrix D^i that is determined by the vertex of the interval $[z_1, z_2]$ that minimizes the function μ_i (if $z_1 < z_2$) or the vertex of the interval $[z_2, z_1]$ that maximizes μ_i (if $z_2 \leq z_1$), i.e.,

$$D^i = \mathrm{diag}(\max(\mathrm{sgn}(\overline{J}^\mu_i), \mathbf{0}_{1,n_z})).$$

Moreover, if the JSS mapping μ is a remainder term of a JSS decomposition of a function f as discussed in Proposition 1, then for any interval domain $\underline{z} \leq z \leq \overline{z}$, with $z, \underline{z}, \overline{z} \in \mathcal{Z}$ and $\varepsilon \triangleq \overline{z} - \underline{z}$, the following inequality holds: $\delta^\mu_d \triangleq \mu_d(\overline{z}, \underline{z}) - \mu_d(\underline{z}, \overline{z}) \leq \overline{F}_\mu \varepsilon$, with $\overline{F}_\mu \triangleq 2\max(\overline{J}_f - H, \mathbf{0}_{p,n_z}) - \underline{J}_f + H$ and $H \in \mathbb{R}^{p\times n_z}$ given in Proposition 1.

Consequently, by applying Proposition 2 to the Jacobian sign-stable decomposition obtained using Proposition 1, a tight and tractable decomposition function can be obtained (cf. details in [15]). Furthermore, in the case that the mapping is not JSS, a tractable algorithm has been introduced in [20, Algorithm 1] to compute *tight remainder-form decomposition functions* for a very broad class of nonlinear functions.

Definition 2 (Embedding System)**.** *[16, Definition 6] For a discrete-time dynamical system $x_{k+1} = g(x_k)$ defined over mapping $g : \mathcal{X} \subset \mathbb{R}^n \to \mathbb{R}^n$ with a corresponding decomposition function $g_d(\cdot)$, its embedding system is a $2n$-dimensional system with initial condition $\begin{bmatrix}\overline{x}_0^\top & \underline{x}_0^\top\end{bmatrix}^\top$ defined as $\begin{bmatrix}\underline{x}_{k+1}^\top & \overline{x}_{k+1}^\top\end{bmatrix}^\top = \begin{bmatrix}\underline{g}_d^\top(\underline{x}_k, \overline{x}_k) & \overline{g}_d^\top(\overline{x}_k, \underline{x}_k)\end{bmatrix}^\top$.*

Note that according to [20, Proposition 3], the embedding system in Definition 2 with decomposition function g_d corresponding to the dynamics $x_{k+1} = g(x_k)$ has a *state framer property*, i.e., its solution is guaranteed to frame the unknown state trajectory x_k, i.e., $\underline{x}_k \leq x_k \leq \overline{x}_k$ for all $k \in \mathbb{N}$.

Next, we will briefly restate our previous result in [17], tailoring it specifically for intervals to help with computing affine bounding functions for our functions.

Proposition 3. *[17, Affine Outer-Approximation] Consider the function $g(.) : \mathcal{B} \subset \mathbb{R}^n \to \mathbb{R}^m$, where $\mathcal{B}$ is an interval with $\overline{x}, \underline{x}, \mathcal{V}_\mathcal{B}$ being its maximal, minimal and set of vertices, respectively. Suppose $\overline{A}_\mathcal{B}, \underline{A}_\mathcal{B}, \overline{e}_\mathcal{B}, \underline{e}_\mathcal{B}, \theta_\mathcal{B}$ is a solution of the following linear program (LP):*

$$\begin{aligned}\min_{\theta, \overline{A}, \underline{A}, \overline{e}, \underline{e}} \ & \theta \\ s.t \ & \underline{A}x_s + \underline{e} + \sigma \leq g(x_s) \leq \overline{A}x_s + \overline{e} - \sigma, \\ & (\overline{A} - \underline{A})x_s + \overline{e} - \underline{e} - 2\sigma \leq \theta \mathbf{1}_m, \ \forall x_s \in \mathcal{V}_\mathcal{B},\end{aligned} \tag{4}$$

where $\mathbf{1}_m \in \mathbb{R}^m$ is a vector of ones and σ can be computed via [17, Proposition 1] for different function classes. Then, $\underline{A}_\mathcal{B} x + \underline{e}_\mathcal{B} \leq g(x) \leq \overline{A}_\mathcal{B} x + \overline{e}_\mathcal{B}, \forall x \in \mathcal{B}$.

Corollary 1. *By taking the average of upper and lower affine abstractions and adding/subtracting half of the maximum distance, it is straightforward to "parallelize" the above upper and lower abstractions as $A_g x + \underline{\epsilon} \leq g(x) \leq A_g x + \overline{\epsilon}$, or equivalently $g(x) = A_g x + \epsilon, \epsilon \in [\underline{\epsilon}, \overline{\epsilon}]$, where $A_g \triangleq (1/2)(\overline{A} + \underline{A})$, $\underline{\epsilon} \triangleq (1/2)(\overline{e} + \underline{e} - \theta \mathbf{1}_m)$ and $\overline{\epsilon} \triangleq (1/2)(\overline{e} + \underline{e} + \theta \mathbf{1}_m)$. We call A_g and ϵ the parallel affine outer-approximation slope and outer-approximation error of function g on $\mathcal{B}$, respectively.*

III. Problem Formulation

System Assumptions. Consider the nonlinear discrete-time system with unknown inputs and bounded noise

$$\begin{aligned} x_{k+1} &= f(x_k) + Ww_k + Gd_k, \\ y_k &= h(x_k) + Vv_k + Hd_k, \end{aligned} \tag{5}$$

where at time $k \in \mathbb{N}$, $x_k \in \mathcal{X} \subset \mathbb{R}^n$, $d_k \in \mathbb{R}^p$ and $y_k \in \mathbb{R}^l$ are the state vector, unknown input vector, and measurement vector, respectively. The process and measurement noise signals $w_k \in \mathbb{R}^n$ and $v_k \in \mathbb{R}^l$ are assumed to be bounded, i.e., $w_k \in \mathcal{W} \triangleq [\underline{w}, \overline{w}\}$, $v_k \in \mathcal{V} \triangleq [\underline{v}, \overline{v}]$ with known lower and upper bounds, $\underline{w}$, $\overline{w}$ and $\underline{v}$, $\overline{v}$, respectively. We also assume that lower and upper bounds for the initial state, $\underline{x}_0$ and $\overline{x}_0$, are available, i.e., $\underline{x}_0 \leq x_0 \leq \overline{x}_0$. The functions $f : \mathbb{R}^n \to \mathbb{R}^n$, $h : \mathbb{R}^n \to \mathbb{R}^l$ and matrices W, V, G and H are known and of appropriate dimensions, where G and H encode the *locations* at which the unknown input (or attack) signal can affect the system dynamics and measurements. Note that no assumption is made on H to be either the zero matrix (no direct feedthrough), or to have full column rank when there is direct feedthrough (in contrast to [13]).

Unknown Input (or Attack) Signal Assumptions. The unknown inputs d_k (representing false data injection attack signals) are not constrained to follow any model nor to be a signal of any type (random or strategic), hence no prior 'useful' knowledge of the dynamics of d_k is available (independent of $\{d_\ell\}$ $\forall k \neq \ell$, $\{w_\ell\}$ and $\{v_\ell\}$ $\forall \ell$). We also do not assume that d_k is bounded or has known bounds and thus, d_k is suitable for representing adversarial attack signals.

Next, we briefly introduce a similar system transformation as in [3], which will be used later in our observer structure.

System Transformation. Let $p_H \triangleq \mathrm{rk}(H)$. Similar to [3], by applying singular value decomposition, we have $H = \begin{bmatrix} U_1 & U_2 \end{bmatrix} \begin{bmatrix} \Xi & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} E_1^\top \\ E_2^\top \end{bmatrix}$ with $E_1 \in \mathbb{R}^{p \times p_H}$, $E_2 \in \mathbb{R}^{p \times (p - p_H)}$, $\Xi \in \mathbb{R}^{p_H \times p_H}$ (a diagonal matrix of full rank; so we can define $S \triangleq \Xi^{-1}$), $U_1 \in \mathbb{R}^{l \times p_H}$ and $U_2 \in \mathbb{R}^{l \times (l - p_H)}$. Then, since $D \triangleq \begin{bmatrix} E_1 & E_2 \end{bmatrix}$ is unitary:

$$d_k = E_1 d_{1,k} + E_2 d_{2,k},\ d_{1,k} = E_1^\top d_k,\ d_{2,k} = E_2^\top d_k. \tag{6}$$

Finally, by defining $T_1 \triangleq U_1^\top, T_2 \triangleq U_2^\top$, the output equation can be decoupled, by which system (5) can be rewritten as:

$$\begin{aligned} x_{k+1} &= f(x_k) + Ww_k + G_1 d_{1,k} + G_2 d_{2,k}, \\ z_{1,k} &= h_1(x_k) + V_1 v_k + \Xi d_{1,k}, \\ z_{2,k} &= h_2(x_k) + V_2 v_k, \end{aligned} \tag{7}$$

where $h_i(x_k) = T_i h(x_k), \forall i \in \{1, 2\}$ and $K_i \triangleq T_i K_i, \forall K \in \{V, G\}, \forall i \in \{1, 2\}$.

Moreover, we assume the following, which is satisfied for a broad range of nonlinear functions [21]:

Assumption 1. *Functions f, h have bounded Jacobians over the state space $\mathcal{X}$ with known/computable Jacobian bounds.*

Assumption 2. *The JSS decomposition of $h_2(x_k)$ via Proposition 1 given by $h_2(x_k) = C_2 x_k + \psi_2(x_k)$ is such that ψ_2 is JSS and further, $C_2 G_2$ has full column rank[a]. Consequently, there exists $M_2 \triangleq (C_2 G_2)^\dagger$ such that $M_2 C_2 G_2 = I$.*

[a]In the special case that $G = 0$, we would require G_2 to be empty (and this does happen when H has full rank), in which case $C_2 G_2$ being full rank is satisfied by assumption.

Assumption 3. *(Only needed when the observations are nonlinear, i.e., if $\psi_2(x_k) \neq 0$) The entire state space $\mathcal{X} \subset \mathbb{R}^n$ is bounded. Moreover, A_g is invertible, where $A_g \in \mathbb{R}^{n \times n}$ is the parallel affine outer-approximation slope (cf. Proposition 3 and Corollary 1) of the function $g(x) \triangleq x + G_2 M_2 \psi_2(x)$ over the entire state space.*

Further, we formally define the notions of *framers*, *correctness* and *stability* that are used throughout the paper.

Definition 3 (Interval Framers)**.** *Given the nonlinear plant* (5) *(equivalently* (7)*), the sequences $\{\overline{x}_k, \underline{x}_k\}_{k=0}^\infty \subset \mathbb{R}^n$ and $\{\overline{d}_k, \underline{d}_k\}_{k=0}^\infty \subset \mathbb{R}^p$ are called upper and lower framers for the states and inputs of the system in* (5)*, respectively, if*

$$\forall k \in \mathbb{N}, \forall w_k \in \mathcal{W}, \forall v_k \in \mathcal{V},\ \underline{\nu}_k \leq \nu_k \leq \overline{\nu}_k, \forall \nu \in \{x, d\}.$$

In other words, starting from the initial interval $\underline{x}_0 \leq x_0 \leq \overline{x}_0$, the true state of the system in (5)*, x_k, and the unknown input d_k are guaranteed to evolve within the interval flowpipe $[\underline{x}_k, \overline{x}_k]$ and bounded within the interval $[\underline{d}_k, \overline{d}_k]$, for all $(k, w_k, v_k) \in \mathbb{N} \times \mathcal{W} \times \mathcal{V}$, respectively. Finally, any dynamical system (i.e., tractable algorithm) that returns upper and lower framers for the states and unknown inputs of system 5 is called a resilient interval framer for* (5)*.*

Definition 4 (Framer Error)**.** *Given state and input framers $\{\underline{x}_k \leq \overline{x}_k\}_{k=0}^\infty$ and $\{\underline{d}_k \leq \overline{d}_k\}_{k=1}^\infty$, the sequences $\{e_k^x \triangleq \overline{x}_k - \underline{x}_k\}_{k=0}^\infty$ and $\{e_k^d \triangleq \overline{d}_k - \underline{d}_k\}_{k=1}^\infty$ are called the state and input framer errors, respectively. It easily follows from Definition 3 that $e_k^\nu \geq 0, \forall k \in \mathbb{N}, \forall \nu \in \{x, d\}$.*

Definition 5 (Input-to-State Stability and Interval Observer)**.** *An interval framer is input-to-state stable (ISS), if the framer state error (cf. Definition 4) is bounded as follows:*

$$\forall k \in \mathbb{N},\ \|e_k^x\|_2 \leq \beta(\|e_0^x\|_2, k) + \alpha(\|\delta\|_{\ell_\infty}), \tag{8}$$

where $\delta \triangleq [(\delta^w)^\top\ (\delta^v)^\top]^\top \triangleq [(\overline{w} - \underline{w})^\top\ (\overline{v} - \underline{v})^\top]^\top$, β and α are functions of classes[b] $\mathcal{KL}$ and $\mathcal{K}_\infty$, respectively, and $\|\delta\|_{\ell_\infty} \triangleq \sup_{k \in \mathbb{N}} \|\delta_k\|_2 = \|\delta\|_2$ is the ℓ_∞ signal norm. An ISS resilient interval framer is called a resilient interval observer.

Definition 6 ($\mathcal{H}_\infty$-Optimal Resilient Interval Observer)**.** *A resilient interval framer design is $\mathcal{H}_\infty$-optimal if the $\mathcal{H}_\infty$ gain of the framer error system $\tilde{\mathcal{G}}$, i.e., $\|\tilde{\mathcal{G}}\|_{\mathcal{H}_\infty}$ is minimized, where $\|\tilde{\mathcal{G}}\|_{\mathcal{H}_\infty} \triangleq \sup\{\frac{\|e^x\|_{\ell_2}}{\|\delta\|_{\ell_2}}, \delta \neq 0\}$, and $\|s\|_{\ell_2} \triangleq \sqrt{\sum_0^\infty \|s_k\|_2^2}$ is the ℓ_2 signal norm for $s \in \{e^x, \delta\}$.*

Using the above, we aim to address the following problem.

Problem 1. *Given the nonlinear system in* (5)*, as well as Assumptions 1–3, synthesize an ISS and $\mathcal{H}_\infty$-optimal resilient interval observer (cf. Definitions 3–6).*

IV. Resilient Interval Observer Design

In this section, we describe the proposed resilient interval observer as well as analyze its correctness and ISS properties.

[b]A function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{K}$ if it is continuous, positive definite, and strictly increasing and is of class $\mathcal{K}_\infty$ if it is also unbounded. Moreover, $\lambda : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is of class $\mathcal{KL}$ if for each fixed $t \geq 0$, $\lambda(\cdot, t)$ is of class $\mathcal{K}$ and for each fixed $s \geq 0$, $\lambda(s, t)$ decreases to zero as $t \to \infty$.

A. Interval Framer Design

Our strategy for designing resilient interval observers in the presence of unknown inputs has three steps. First, we obtain an equivalent representation of the system in (5) by introducing some auxiliary state variables, such that the equivalent system is not affected by the attack signal. Then, inspired by our previous work on synthesizing interval observers for nonlinear systems [15], [16] we will design embedding systems (cf. Definition 2) for the equivalent system representation, which returns state framers. Finally, we obtain input framers (with a one-step delay since $d_{2,k}$ does not appear in the measurements $z_{1,k}$ and $z_{2,k}$ in (7)) as functions of the computed state framers.

First, note that from (7) and with $S \triangleq \Xi^{-1}$, $d_{1,k}$ can be computed as a function of the state at current time as follows:

$$d_{1,k} = S(z_{1,k} - h_1(x_k) - V_1 v_k). \tag{9}$$

Next, we introduce an auxiliary state variable as:

$$\xi_k \triangleq x_k - N(z_{2,k} - V_2 v_k - \psi_2(x_k)) = (I - NC_2)x_k, \tag{10}$$

where the equality follows from (7) and Assumption 2. Moreover, $N \in \mathbb{R}^{n\times(l-\tilde{p})}$ is a to-be-designed gain to cancel out the effect of the unknown input in the state equation. This is done through the following lemma.

Lemma 1. *Suppose Assumption 2 holds and let $N = G_2M_2 = G_2(C_2G_2)^\dagger$ and $S \triangleq \Xi^{-1}$. Then, the value of the auxiliary state ξ_k at time step $k+1$ can be computed as:*

$$\xi_{k+1} = (I - NC_2)(f(x_k) + G_1 S(z_{1,k} - h_1(x_k) - V_1 v_k) + W w_k). \tag{11}$$

Proof. By plugging $d_{1,k}$ from (9) into (7), we obtain

$$x_{k+1} = f(x_k) + G_1 S(z_{1,k} - h_1(x_k) - V_1 v_k) + W w_k + G_2 d_{2,k}. \tag{12}$$

This, together with the second equality in (10) and the above choice of N such that $(I - NC_2)G_2 = 0$, returns (11). ■

The evolution of the auxiliary state ξ_k in (11) is independent of the unknown input and hence, we can compute propagated framers for ξ_k leveraging embedding systems (cf. Proposition 2). However, we do not have a way of directly retrieving the propagated framers for the original states, i.e., $\{\underline{x}_k, \overline{x}_k\}$ in terms of $\{\underline{\xi}_k, \overline{\xi}_k\}$ from the second equality of (10), since $I - NC_2 = I - G_2(C_2G_2)^\dagger C_2$ can be shown to be not invertible. To overcome this difficulty, given Assumption 3, we introduce a new auxiliary state:

$$\gamma_k \triangleq x_k - \Lambda(N(z_{2,k} - V_2 v_k) - \epsilon_k), \tag{13}$$

with $\Lambda \triangleq A_g^{-1}$, where A_g and $\epsilon_k \in [\underline{\epsilon}, \overline{\epsilon}]$ are parallel affine outer-approximation slope and approximation error of the mapping $g(x) \triangleq x + G_2M_2\psi_2(x)$ on the entire space $\mathcal{X}$ (cf. Proposition 3, Corollary 1 and Assumption 3).

Proposition 4. *Given Assumption 3, the two auxiliary states γ_k and ξ_k are linearly related as:*

$$\gamma_k = \Lambda \xi_k. \tag{14}$$

Proof. Computing parallel affine outer-approximation of the mapping $g(x_k) = A_g x_k + \epsilon_k$ and applying (10), we obtain

$$g(x_k) \triangleq x_k + N\psi_2(x) = \xi_k + N(z_{2,k} - V_2 v_k)$$
$$\Rightarrow A_g x_k = \xi_k + N(z_{2,k} - V_2 v_k) - \epsilon_k, \quad \epsilon_k \in [\underline{\epsilon}, \overline{\epsilon}],$$

from which and given Assumption 3 (that A_g is invertible, with $\Lambda = A_g^{-1}$), we have

$$x_k = \Lambda(\xi_k + N(z_{2,k} - V_2 v_k) - \epsilon_k), \quad \epsilon_k \in [\underline{\epsilon}, \overline{\epsilon}]. \tag{15}$$

Plugging x_k from (15) into (13) returns the results. ■

We are now ready to propose an input and state resilient interval framer, i.e., the following discrete-time dynamical system (16)–(18), which by construction, outputs/returns framers for the original states $\{x_k\}_{k=0}^\infty$ and the unknown input signal $\{d_k\}_{k=1}^\infty$ of system (5). The details of the framer construction/design will be provided in the proof of Theorem 1. The proposed resilient interval framer is as follows:

$$\begin{aligned}
\underline{\gamma}_{k+1} &= (A - LC_2)^\oplus \underline{\gamma}_k - (A - LC_2)^\ominus \overline{\gamma}_k + \rho_d(\underline{x}_k, \overline{x}_k) \\
&\quad + D^\ominus \underline{\epsilon} - D^\oplus \overline{\epsilon} + L^\ominus \psi_{2,d}(\underline{x}_k, \overline{x}_k) - L^\oplus \psi_{2,d}(\overline{x}_k, \underline{x}_k) \\
&\quad + \hat{V}^\ominus \underline{v} - \hat{V}^\oplus \overline{v} + \hat{W}^\ominus \underline{w} - \hat{W}^\ominus \overline{w} + \hat{z}_k, \\
\overline{\gamma}_{k+1} &= (A - LC_2)^\oplus \overline{\gamma}_k - (A - LC_2)^\ominus \underline{\gamma}_k + \rho_d(\overline{x}_k, \underline{x}_k) \\
&\quad + D^\ominus \overline{\epsilon} - D^\oplus \underline{\epsilon} + L^\ominus \psi_{2,d}(\overline{x}_k, \underline{x}_k) - L^\oplus \psi_{2,d}(\underline{x}_k, \overline{x}_k) \\
&\quad + \hat{V}^\ominus \overline{v} - \hat{V}^\oplus \underline{v} + \hat{W}^\oplus \overline{w} - \hat{W}^\ominus \underline{w} + \hat{z}_k,
\end{aligned} \tag{16}$$

$$\begin{aligned}
\underline{x}_k &= \underline{\gamma}_k + \Lambda N z_{2,k} + \Lambda^\ominus \underline{\epsilon} - \Lambda^\oplus \overline{\epsilon} + (\Lambda N V_2)^\ominus \underline{v} - (\Lambda N V_2)^\oplus \overline{v}, \\
\overline{x}_k &= \overline{\gamma}_k + \Lambda N z_{2,k} + \Lambda^\ominus \overline{\epsilon} - \Lambda^\oplus \underline{\epsilon} + (\Lambda N V_2)^\ominus \overline{v} - (\Lambda N V_2)^\oplus \underline{v},
\end{aligned} \tag{17}$$

$$\begin{aligned}
\underline{d}_{k-1} &= \Phi^\oplus \underline{x}_k - \Phi^\ominus \overline{x}_k + \kappa_d(\underline{x}_{k-1}, \overline{x}_{k-1}) + A_z z_{1,k-1} \\
&\quad + A_v^\oplus \underline{v} - A_v^\ominus \overline{v} + \Phi^\ominus \underline{w} - \Phi^\oplus \overline{w}, \\
\overline{d}_{k-1} &= \Phi^\oplus \overline{x}_k - \Phi^\ominus \underline{x}_k + \kappa_d(\overline{x}_{k-1}, \underline{x}_{k-1}) + A_z z_{1,k-1} \\
&\quad + A_v^\oplus \overline{v} - A_v^\ominus \underline{v} + \Phi^\ominus \overline{w} - \Phi^\oplus \underline{w},
\end{aligned} \tag{18}$$

where $S \triangleq \Xi^{-1}$, $N = G_2M_2$ and $\Lambda \triangleq A_g^{-1}$. Furthermore, $L \in \mathbb{R}^{n\times(l-p_H)}$ is an arbitrary matrix (observer gain) which will be designed later in Theorem 2 to yield stability and optimality of the proposed framers. Moreover, $A \in \mathbb{R}^{n\times n}$ and $\rho : \mathcal{X} \subset \mathbb{R}^n \to \mathbb{R}^n$ are obtained by applying JSS decompositions (cf. Proposition 1) on the mapping $\tilde{f}(x) \triangleq \Lambda(I - NC_2)(f(x) - G_1 S h_1(x))$, while $\psi_{2,d}$ and ρ_d are tight decomposition functions for the JSS mappings ρ and ψ_2, respectively, computed through Proposition 1. Further,

$$\begin{aligned}
&\hat{V} \triangleq (A - LC_2)\Lambda N V_2 + LV_2 + \Lambda(I - NC_2)G_1 S V_1, \\
&\Phi \triangleq E_2 M_2 C_2, A_v \triangleq (\Phi G_1 - E_1) S V_1, A_z \triangleq (E_1 - \Phi G_1) S, \\
&D \triangleq (A - LC_2)\Lambda, \hat{W} \triangleq \Lambda(I - NC_2)W, \\
&\hat{z}_k \triangleq \Lambda(I - NC_2)G_1 S z_{1,k} + (L + (A - LC_2)\Lambda N) z_{2,k},
\end{aligned} \tag{19}$$

and κ_d is the decomposition function of the mapping $\kappa(x) \triangleq (\Phi G_1 - E_1) S h_1(x) - \Phi f(x)$, computed via [19, Theorem 1]. Finally, A_g and $\epsilon_k \in [\underline{\epsilon}, \overline{\epsilon}]$ are computed via Corollary 1.

The following theorem formalizes the state and input framer/correctness property of the proposed resilient interval observer (16)–(18) with respect to the original system (5).

Theorem 1. *Suppose Assumptions 1–3 hold. Then, the sequences $\{\underline{x}_k, \overline{x}_k\}_{k=0}^\infty$ and $\{\underline{d}_k, \overline{x}_k\}_{k=1}^\infty$ obtained from the system* (16)–(18)*, construct framers for the states and unknown input signal of* (5)*, respectively, i.e., $\underline{\nu}_k \le \nu_k \le \overline{\nu}_k, \forall \nu \in \{x, d\}, \forall k \in \mathbb{N}, \forall w_k \in \mathcal{W}, \forall v_k \in \mathcal{V}$.*

Proof. From (11) and (14), we obtain

$$\gamma_k^+ = \Lambda(I - NC_2)(f(x_x) + G_1 S(z_{1,k} - h_1(x_k) - V_1 v_k) + W w_k).$$

Adding the *zero term* $L(z_{2,k} - C_2 x_k - \psi_2(x_k) - V_2 v_k)$ to the right hand side of the above equation and applying mixed-monotone decompositions on the mapping $\tilde{f}(x) \triangleq \Lambda(I - NC_2)(f(x) - G_1 S h_1(x))$ to decompose it as $\tilde{f}(x) = Ax + \rho(x)$ (cf. Proposition 1 for more details), yields:

$$\gamma_{k+1} = (A - LC_2)x_k + \rho(x_k) - L\psi_2(x_k) - \tilde{V} v_k + \tilde{W} w_k + \tilde{z}_k, \tag{20}$$

where $\tilde{V} \triangleq \Lambda(I-NC_2)G_1SV_1+LV_2$, $\tilde{W} \triangleq \Lambda(I-NC_2)W$ and $\tilde{z}_k \triangleq \Lambda(I-NC_2)G_1Sz_{1,k}+Lz_{2,k}$. Then, by computing x_k in terms of γ_k from (13) and plugging it back into the linear terms in the right-hand side of (20), we obtain

$$\begin{aligned}\gamma_{k+1} &= (A-LC_2)\gamma_k+\rho(x_k)-L\psi_2(x_k)\\ &\quad -\hat{V}v_k+\hat{W}w_t-D\epsilon_k+\hat{z}_k,\end{aligned} \tag{21}$$

with $\hat{V}, D, \hat{W}$ and $\hat{z}_k$ given in (19). Next, by applying Proposition 2 and [22, Lemma 1], we construct the embedding system (16) for (21), which implies $\underline{\gamma}_k \le \gamma_k \le \overline{\gamma}_k, \forall k \in \mathbb{N}$, by construction. Further, the results in (17) follow from applying [22, Lemma 1] on (13) to compute framers of x_k in terms of the framers of γ_k.

To obtain input framers, note that multiplying both sides of (12) by M_2C_2 together with Assumption 2 yields $d_{2,k-1} = M_2C_2(x_k - f(x_{k-1}) + G_1Sh_1(x_{k-1}) + G_1S(V_1v_{k-1} - z_{1,k-1}) - Ww_{k-1})$. This, along with (6) and (9), leads to

$$d_{k-1} = \Phi x_k+\kappa(x_{k-1})+A_z z_{1,k-1}+A_v v_{k-1}-\Phi W w_{k-1}. \tag{22}$$

The input framers in (18) are obtained by leveraging [19, Theorem 1] to compute a decomposition function for the nonlinear function κ, as well as applying [22, Lemma 1] to bound the linear terms in the right-hand side of (22). ■

B. ISS and $\mathcal{H}_\infty$-Optimal Interval Observer Synthesis

Next, we provide sufficient conditions to guarantee the stability of the proposed framers, i.e., we seek to synthesize the observer gain L to ensure input-to-state stability (ISS) of the observer state error, $e_k^x \triangleq \overline{x}_k - \underline{x}_k$ in the sense of Definition 4, while ensuring that the design is optimal in the sense of minimizing the $\mathcal{H}_\infty$ gain (cf. Definition 5).

First, we derive the observer error dynamics as follows.

Lemma 2. *Consider the nonlinear system* (5) *and suppose all assumptions in Theorem 2 hold. Then, the state framer error dynamics of the resilient interval observer* (16)–(18) *and its nonlinear comparison system are as follows:*

$$\begin{aligned}e_{k+1}^x &= |A-LC_2|e_k^x+\delta_k^\rho+|L|\delta_k^{\psi_2}+|\hat{W}|\delta^w\\ &\quad +(|V_a-LV_b|-|A-LC_2||\Lambda NV_2|+|\Lambda NV_2|)\delta^v\\ &\quad +(|\Lambda|+|D_a-LD_b|-|A-LC_2||\Lambda|)\delta^\epsilon\\ &\le (|A-LC_2|+\overline{F}_\rho+|L|\overline{F}_{\psi_2})e_k^x+|\hat{W}|\delta^w\\ &\quad +(|V_a-LV_b|-|A-LC_2||\Lambda NV_2|+|\Lambda NV_2|)\delta^v\\ &\quad +(|\Lambda|+|D_a-LD_b|-|A-LC_2||\Lambda|)\delta^\epsilon,\end{aligned} \tag{23}$$

where $\delta_k^\zeta \triangleq \zeta_d(\overline{x}_k,\underline{x}_k)-\zeta_d(\underline{x}_k,\overline{x}_k), \forall \zeta \in \{\psi_2,\rho\}$, $\delta^s \triangleq \overline{s}-\underline{s}, \forall s \in \{w,v,\epsilon\}$, and $\overline{F}_\zeta, \forall \zeta \in \{\psi_2,\rho\}$ are computed through Proposition 2. Moreover,

$$\begin{aligned}V_a &\triangleq A\Lambda NV_2+\Lambda(I-NC_2)G_1SV_1,\\ V_b &\triangleq (C_2\Lambda N-I)V_2, D_a \triangleq A\Lambda, D_b \triangleq C_2\Lambda.\end{aligned} \tag{24}$$

Proof. It follows from (16) that the dynamics of $e_k^\gamma \triangleq \overline{\gamma}_k - \underline{\gamma}_k$ is given by $e_{k+1}^\gamma = |A-LC_2|e_k^\gamma+\delta_k^\rho+|L|\delta_k^{\psi_2}+|\hat{V}|\delta^v+|\hat{W}|\delta^w+|D|\delta^\epsilon$. This, combined with $e_k^x = e_k^\gamma+|\Lambda|\delta^\epsilon+|\Lambda NV_2|\delta^v$ (followed from (17)) results in the equality in (23), which together with the facts that $\delta_k^\zeta \le \overline{F}_\zeta e_k^x, \forall \zeta \in \{\rho,\psi_2\}$ (cf. Proposition 2), yields the inequality in (23). ■

Further, by leveraging slightly different approaches to derive an upper *linear* comparison system for the *nonlinear* error comparison system (23), we derive different sets of sufficient conditions to guarantee the ISS property of the proposed observer, as well as to ensure the optimality of the design in the sense of minimum $\mathcal{H}_\infty$ gain, as follows.

Theorem 2 (ISS & $\mathcal{H}_\infty$-Optimal Resilient Interval Observer Synthesis)**.** *Consider system* (5) *(equivalently the transformed system* (7)*) and suppose Assumptions 1–3 hold. Moreover, suppose there exist matrices $\mathbb{R}^{n\times n} \ni P^* \succ \mathbf{0}_{n,n}, \Gamma^* \in \mathbb{R}_{\ge 0}^{n\times(l-p_H)}$ and $\eta^* \in \mathbb{R}_{>0}$ such that $-P^* \in \mathbb{M}_n$ and the tuple (P^*,Γ^*,η^*) solves the following problem:*

$$\begin{aligned}&\min_{\{\eta,P,\Gamma\}} \eta\\ &s.t. \begin{bmatrix} P & P\tilde{A}-\Gamma\tilde{C} & P\tilde{B}-\Gamma\tilde{D} & 0\\ * & P & 0 & I\\ * & * & \eta I & 0\\ * & * & * & \eta I\end{bmatrix} \succ 0, (P,\Gamma) \in \mathbf{C},\end{aligned} \tag{25}$$

where the matrices $\tilde{A},\tilde{B},\tilde{C},\tilde{D}$, as well as the corresponding additional set of constraints $\mathbf{C}$ can be either of the following:

(i) $\mathbf{C} = \{(P,\Gamma) \mid P\begin{bmatrix}A & V_a & D_a\end{bmatrix} - \Gamma\begin{bmatrix}C_2 & V_b & D_b\end{bmatrix} \ge 0\}$*, if:*

$$\begin{aligned}&\tilde{A} = A+\overline{F}_\rho,\ \tilde{C} = C_2-\overline{F}_{\psi_2},\\ &\tilde{B} = \begin{bmatrix}V_a+(I-A)|\Lambda NV_2| & |\hat{W}| & D_a+(I-A)|\Lambda|\end{bmatrix},\\ &\tilde{D} = \begin{bmatrix}V_b-C_2|\Lambda NV_2| & 0 & D_b-C_2|\Lambda|\end{bmatrix}.\end{aligned}$$

(ii) $\mathbf{C} = \{(P,\Gamma) \mid \Gamma\begin{bmatrix}C_2 & V_b & D_b\end{bmatrix} \ge 0\}$*, if*

$$\begin{aligned}&\tilde{A} = |A|+\overline{F}_\rho,\ \tilde{C} = -C_2-\overline{F}_{\psi_2},\\ &\tilde{B} = \begin{bmatrix}|V_a|+(I-|A|)|\Lambda NV_2| & |\hat{W}| & (I-|A|)|\Lambda|+|D_a|\end{bmatrix},\\ &\tilde{D} = \begin{bmatrix}C_2|\Lambda NV_2|-V_b & 0 & C_2|\Lambda|-D_b\end{bmatrix}.\end{aligned}$$

(iii) $\mathbf{C} = \{(P,\Gamma) \mid PA-\Gamma C_2 \ge 0\}$*, if:*

$$\begin{aligned}&\tilde{A} = A+\overline{F}_\rho,\ \tilde{C} = C_2-\overline{F}_{\psi_2},\ \tilde{D} = \begin{bmatrix}-V_2 & 0 & 0\end{bmatrix},\\ &\tilde{B} = \begin{bmatrix}|\Lambda(I-NC_2)G_1SV_1|+|\Lambda NV_2| & |\hat{W}| & |\Lambda|\end{bmatrix}.\end{aligned}$$

Then, the proposed resilient interval framer (16)–(18) *with the corresponding gain $L = (P^*)^{-1}\Gamma^*$, is a resilient ISS input and state interval observer in the sense of Definition 5 and also is $\mathcal{H}_\infty$-optimal (cf. Definition 6). Finally, in any of the above cases, the LMI in* (25) *is feasible only if the linear comparison system $(\tilde{A},\tilde{B},\tilde{C},\tilde{D})$ is detectable.*

Proof. We will show that in each of the cases (i)–(iii), given the corresponding constraint set $\mathbf{C}$, a linear comparison system for the observer state error dynamics (23) can be computed in the following form:

$$e_{k+1}^x \le (\tilde{A}-L\tilde{C})e_k^x+(\tilde{B}-L\tilde{D})\tilde{w}, \tag{26}$$

with $\tilde{w} \triangleq \begin{bmatrix}\delta^{v\top} & \delta^{w\top} & \delta^{\epsilon\top}\end{bmatrix}^\top$, where the detectability of the pair $(\tilde{A},\tilde{C})$ is a necessary condition for stabilizing the comparison system. If this can be shown, then using the results in [23, Section 9.2.3], the solution (P^*,Γ^*) to the program in (25) returns the optimal observer gain $L^* = (P^*)^{-1}\Gamma^*$ for the linear comparison system (26), and hence, for the original error dynamics (23) in the minimum $\mathcal{H}_\infty$ gain sense with an $\mathcal{H}_\infty$ gain of η^* (cf. Definition 6). This implies that the above linear comparison system (26) satisfies the following asymptotic gain (AG) property [24]:

$$\limsup_{k\to\infty} \|e_k^x\|_2 \le \alpha(\|\tilde{\delta}\|_{\ell_\infty}),\ \forall e_0^x, \forall 0 \le \tilde{\delta} \le [(\delta^w)^\top\ (\delta^v)^\top\ (\delta^\epsilon)^\top]^\top,$$

where $\tilde{\delta}$ is any realization of the augmented noise and outer-approximation error interval width and α is any class $\mathcal{K}_\infty$ function that is lower bounded by $\eta^*\tilde{\delta}$. On the other hand, by setting $\delta = 0$, the LMIs in (25) reduce to their noiseless counterparts in [15, Eq. (19)]. Hence, by [15, Theorem 2],

the comparison system (26) is 0-stable (0-GAS), which in addition to the AG property above is equivalent to the ISS property for (26) by [24, Theorem 1-e]. Thus, the designed observer is also ISS. So, what remains to complete the proof is to show that the comparison system (26) can indeed be computed in each of the cases as follows.

Case (i). Consider the nonlinear comparison system in (23). By satisfying the constraint set $\mathbf{C}$, we enforce $-P$ to be Metzler, as well as $P\tilde{A}-\Gamma\tilde{C}, PV_a-\Gamma V_b$ and $PV_a-\Gamma V_b$ to be non-negative. Also, Γ is non-negative by assumption. Consequently, since P is positive definite, it becomes a non-singular M-matrix, i.e., a square matrix whose negation is Metzler and whose eigenvalues have non-negative real parts, and hence is inverse-positive [25, Theorem 1], i.e., $P^{-1}\geq 0$. Therefore, $L=P^{-1}\Gamma\geq 0$, $A-LC_2=P^{-1}(PA-\Gamma C_2)\geq 0$, $V_a-LV_b=P^{-1}(PV_a-\Gamma V_b)\geq 0$ and $D_a-LD_b=P^{-1}(PD_a-\Gamma D_b)\geq 0$, because they are matrix products of non-negative matrices. So, $|L|=L, |A-LC_2|=A-LC_2, |V_a-LV_b|=V_a-LV_b$ and $|D_a-LD_b|=D_a-LD_b$, which turns (23) into the form of (26).

Case (ii). By applying the triangle inequality, the comparison system in (23) can get upper bounded again as

$$\begin{aligned} e^x_{k+1}\leq\ & (|A|+|LC_2|+\overline{F}_\rho+|L|\overline{F}_{\psi_2})e^x_k+|\hat{W}|\delta^w \\ & +(|V_a|+|LV_b|-|LC_2||\Lambda NV_2|+(I-|A|)|\Lambda NV_2|)\delta^v \\ & +((I-|A|)|\Lambda|+|D_a|+|LD_b|-|LC_2||\Lambda|)\delta^\epsilon. \end{aligned} \tag{27}$$

By a similar argument as in Case (i), enforcing $-P$ to be Metzler along with the constraints set $\mathbf{C}$ results in $|LC_2|=LC_2, |LV_b|=LV_b$ and $|LD_b|=LD_b$, and hence turns (27) into the form of (26).

Case (iii). Note that by the triangle inequality, $|V_a-LV_b|=|(A-LC_2)\Lambda NV_2+LV_2+\Lambda(I-NC_2)G_1SV_1|\leq |(A-LC_2)||\Lambda NV_2|+|L||V_2|+|\Lambda(I-NC_2)G_1SV_1|$, and $|D_a-LD_b|=|(A-LC_2)\Lambda|\leq|(A-LC_2)||\Lambda|$. These two combined with (23) yield

$$\begin{aligned} e^x_{k+1}\leq\ & (|A-LC_2|+\overline{F}_\rho+|L|\overline{F}_{\psi_2})e^x_k+|\hat{W}|\delta^w+|\Lambda|\delta^\epsilon \\ & +(|L||V_2|+|\Lambda NV_2|+|\Lambda(I-NC_2)G_1SV_1|)\delta^v. \end{aligned} \tag{28}$$

The rest of the proof is to enforce that $A-LC_2$ and L are non-negative to turn (28) into the form of (26), which is similar to the the proofs of the previous two cases. ■

V. Illustrative Example

We now illustrate the effectiveness of our proposed resilient observer using a three-area power system [2, Figure 1], where each control area consists of a generator and load buses with transmission lines between areas. The nonlinear continuous-time model of the buses is slightly modified based on [26], with the subscript i being the bus number:

$$\begin{aligned} \dot{f}_1(t) &= -\tfrac{1}{m_1}(\phi_i(t)-(P_{M_1}(t)+d_1(t)))+w_{2,1}(t), \\ \dot{f}_i(t) &= -\tfrac{1}{m_i}(\phi_i(t)-P_{M_i}(t))+w_{2,i}(t),\ i\in\{2,3\}, \\ \dot{\theta}_i(t) &= f_i(t)+w_{1,i}(t), \qquad i\in\{1,2,3\}, \end{aligned}$$

with $\phi_i(t)\triangleq D_if_i(t)+\sum_{l\in S_i}P_{il}(t)+P_{L_i}(t))$, where θ_i is the phase angle, f_i is the angular frequency, $m_i=0.01$, $D_i=0.11$, $P_{M_i}(t)$ is the mechanical power (the control input), $P_{L_i}(t)$ is a known power demand, S_i is the set of neighboring buses of i, and the nonlinear tie line power flow equation is as follows: $P_{il}(t)=-P_{li}(t)=t_{il}\sin(\theta_i(t)-\theta_l(t))$, with $t_{il}=1$. Only the actuator of Control Area 1 is attacked and the false data injection signal is $d_1(t)$.

On the other hand, the output equation is given as follows:

$$\begin{aligned} y_i(t) &= [\theta_i(t)\ f_i(t)]^\top+v_i(t),\ i\in\{1,3\}, \\ y_2(t) &= [\theta_2(t)\ f_2(t)]^\top+d_2(t)+v_2(t), \end{aligned}$$

where only the sensor $y_2(t)$ is injected with a false data signal $d_2(t)$. Thus, the concatenated attack/unknown input signal is $d(t)=[d_1(t)\ d_2(t)]^\top$ and the G and H matrices in (5) corresponding to the attack locations are given by $G=\begin{bmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\end{bmatrix}^\top$ and $H=\begin{bmatrix}0&0&0&0&0&0\\0&0&0&1&0&0\end{bmatrix}^\top$.

In our simulations, the *forward Euler* method is used to discretize the system dynamics with a sampling time $dt=0.01s$ and both $P_{M_i}(t)$ and $P_{L_i}(t)$ were set to be identically zero. Moreover, for $i=1,\ldots,3$, the process noise $w_i(t)$ and the measurement noise $v_i(t)$ were assumed to be bounded within the bounds $\left[\begin{bmatrix}-50&-50\end{bmatrix}^\top,\begin{bmatrix}50&50\end{bmatrix}^\top\right]$ and $\left[\begin{bmatrix}-0.5&-0.5\end{bmatrix}^\top,\begin{bmatrix}0.5&0.5\end{bmatrix}^\top\right]$, respectively.

For the sake of comparison, we first applied our previous input and state observer [14] that does not have stabilizing gains to the above example, which we found to not be able to yield stable interval estimates (i.e., the framer interval width diverges). On the other hand, when implementing the proposed observer in (16)–(18), the optimization problem in (25) was solved with the additional linear constraints in Case (iii), and we obtained the following observer gain:

$$L=\begin{bmatrix}0.70&0&0.27&0&0\\0&0&0.38&0&0\\0&0.83&73.19&0&0\\-0.0022&0.0084&174.55&0.0056&-0.0001\\0&0&0.14&0.70&0.005\\0.0050&0.0098&0.11&0.01&0.62\end{bmatrix}.$$

As shown in Figures 1 and 2, all the states and attack signals are bounded by the framers computed by the proposed observer, demonstrating its correctness and ability to obtain resilient state estimates and to reconstruct attack signals. Finally, as shown in Figure 3, the actual state and input estimation error sequences (i.e., the framer interval widths) converge to steady-state values, demonstrating the input-to-state stability of the proposed interval observer.

VI. Conclusion

In this paper, the problem of resilient state estimation and attack reconstruction for nonlinear discrete-time systems with nonlinear observations/constraints, that are subject to bounded noise signals, was addressed. In the considered setting, both sensors and actuators could be affected by attack signals/unknown inputs. By introducing auxiliary states, as well as taking advantage of mixed-monotone decomposition of nonlinear functions and affine parallel outer-approximation of the observation functions, the proposed observer was shown to be correct, i.e., it recursively computes interval estimates that by construction, contain the true states and unknown inputs of the system. Further, several semi-definite programs were provided to synthesize the proposed observer gains that guarantee input-to-state stability of the observer and optimality of the proposed interval observer design. Future work will include alternative designs for minimizing L_1 gain, similar to [27], as well as an extension to continuous-time nonlinear systems and hybrid systems.

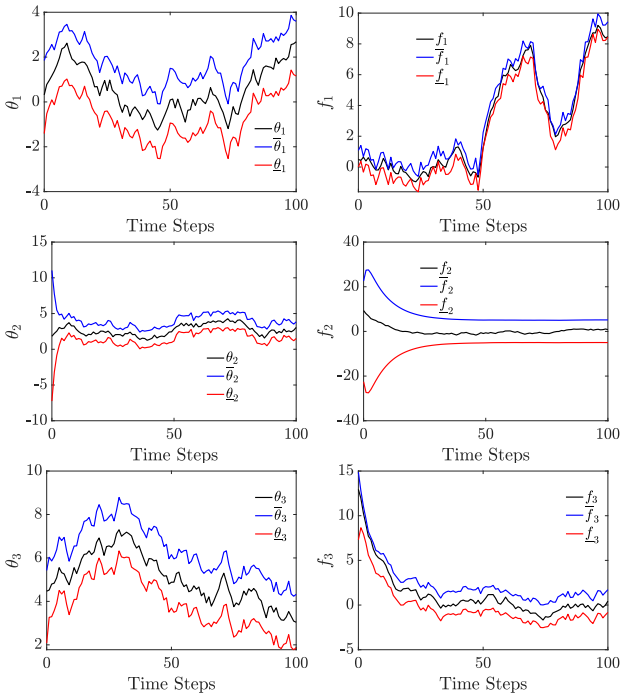

Fig. 1: States: θ_i, f_i, and their upper and lower framers $\overline{\theta}_i, \underline{\theta}_1, \overline{f}_i, \underline{f}_i$, returned by the proposed approach.

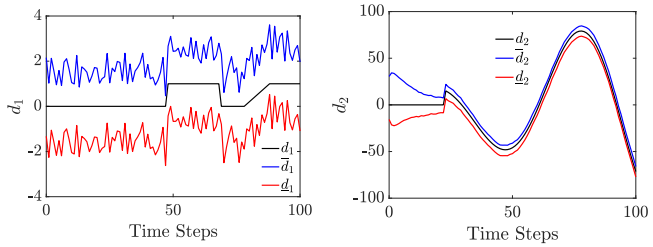

Fig. 2: Attack signals: d_1, d_2, and their upper and lower framers $\overline{d}_1, \underline{d}_1, \overline{d}_2, \underline{d}_2$, returned by the proposed approach.

REFERENCES

[1] W. Liu and I. Hwang, "Robust estimation and fault detection and isolation algorithms for stochastic linear hybrid systems with unknown fault input," *IET Control Theory & Applications*, vol. 5, no. 12, pp. 1353–1368, 2011.

[2] S. Z. Yong, M. Zhu, and E. Frazzoli, "Switching and data injection attacks on stochastic cyber-physical systems: Modeling, resilient estimation and attack mitigation," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 2, p. 9, 2018.

[3] S. Z. Yong, "Simultaneous input and state set-valued observers with applications to attack-resilient estimation," in *American Control Conference (ACC)*. IEEE, 2018, pp. 5167–5174.

[4] G. Chen, Y. Zhang, S. Gu, and W. Hu, "Resilient state estimation and control of cyber-physical systems against false data injection attacks on both actuator and sensors," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 1, pp. 500–510, 2021.

[5] C. Wu, Z. Hu, J. Liu, and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.

[6] E. Mousavinejad, F. Yang, Q. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 11, pp. 3254–3264, 2018.

[7] M. Corradini and A. Cristofaro, "Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes," *IET Control Theory & Applications*, vol. 11, no. 11, pp. 1756–1766, 2017.

[8] A. Lu and G. Yang, "Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer," *Information sciences*, vol. 417, pp. 454–464, 2017.

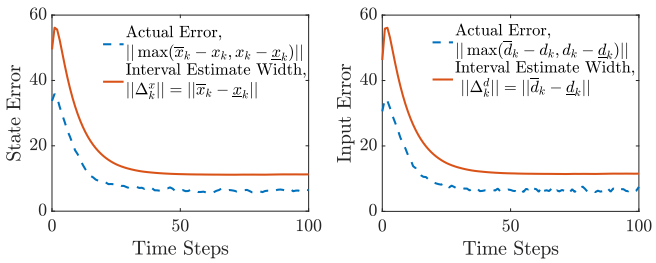

Fig. 3: State and input estimation error sequences.

[9] N. Ellero, D. Gucik-Derigny, and D. Henry, "An unknown input interval observer for LPV systems under L_2-gain and L_∞-gain criteria," *Automatica*, vol. 103, pp. 294–301, 2019.

[10] X. Wang, C. Tan, L. Liu, and Q. Qi, "A novel unknown input interval observer for systems not satisfying relative degree condition," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 7, pp. 2762–2782, 2021.

[11] G. Marouani, T. Dinh, T. Raissi, X. Wang, and H. Messaoud, "Unknown input interval observers for discrete-time linear switched systems," *European Journal of Control*, vol. 59, pp. 165–174, 2021.

[12] L. Wei and W. Yang, "Hybrid observer design for nonlinear systems with unknown inputs," in *2021 China Automation Congress (CAC)*. IEEE, 2021, pp. 4094–4099.

[13] M. Khajenejad and S. Z. Yong, "Simultaneous input and state interval observers for nonlinear systems with full-rank direct feedthrough," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 5443–5448.

[14] ——, "Simultaneous input and state interval observers for nonlinear systems with rank-deficient direct feedthrough," in *2021 European Control Conference (ECC)*. IEEE, 2021, pp. 2311–2316.

[15] M. Khajenejad, F. Shoaib, and S. Z. Yong, "Interval observer synthesis for locally Lipschitz nonlinear dynamical systems via mixed-monotone decompositions," in *2022 American Control Conference (ACC)*. IEEE, 2022, pp. 2970–2975.

[16] M. Khajenejad and S. Z. Yong, "$\mathcal{H}_\infty$-optimal interval observer synthesis for uncertain nonlinear dynamical systems via mixed-monotone decompositions," *IEEE Control Systems Letters*, vol. 6, pp. 3008–3013, 2022.

[17] K. Singh, Q. Shen, and S. Z. Yong, "Mesh-based affine abstraction of nonlinear systems with tighter bounds," in *Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 3056–3061.

[18] M. Abate, M. Dutreix, and S. Coogan, "Tight decomposition functions for continuous-time mixed-monotone systems with disturbances," *IEEE Control Systems Letters*, vol. 5, no. 1, pp. 139–144, 2020.

[19] L. Yang, O. Mickelin, and N. Ozay, "On sufficient conditions for mixed monotonicity," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 5080–5085, 2019.

[20] M. Khajenejad and S. Z. Yong, "Tight remainder-form decomposition functions with applications to constrained reachability and guaranteed state estimation," *IEEE Transactions of Automatic Control*, pp. 1–16, 2023, early access.

[21] L. Yang and N. Ozay, "Tight decomposition functions for mixed monotonicity," in *Conference on Decision and Control (CDC)*, 2019, pp. 5318–5322.

[22] 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.

[23] G. Duan and H. Yu, *LMIs in control systems: analysis, design and applications*. CRC press, 2013.

[24] E. Sontag and Y. Wang, "New characterizations of input-to-state stability," *IEEE Trans. on Automatic Control*, vol. 41, no. 9, pp. 1283–1294, 1996.

[25] R. Plemmons, "M-matrix characterizations. I: nonsingular M-matrices," *Linear Algebra and its Applications*, vol. 18, no. 2, pp. 175–188, 1977.

[26] H. Kim, P. Guo, M. Zhu, and P. Liu, "Attack-resilient estimation of switched nonlinear cyber-physical systems," in *2017 American Control Conference (ACC)*. IEEE, 2017, pp. 4328–4333.

[27] T. Pati, M. Khajenejad, S. P. Daddala, and S. Z. Yong, "L_1-robust interval observer design for uncertain nonlinear dynamical systems," *IEEE Control Systems Letters*, vol. 6, pp. 3475–3480, 2022.