Distributed Resilient Interval Observers for Bounded-Error LTI Systems Subject to False Data Injection Attacks

Mohammad Khajenejad*, Scott Brown*, and Sonia Martínez

Abstract—This paper proposes a novel distributed interval-valued simultaneous state and input observer for linear time-invariant (LTI) systems that are subject to attacks or unknown inputs, injected both on their sensors and actuators. Each agent in the network leverages a singular value decomposition (SVD) based transformation to decompose its observations into two components, one of them unaffected by the attack signal, which helps to obtain local interval estimates of the state and unknown input and then uses intersection to compute the best interval estimate among neighboring nodes. We show that the computed intervals are guaranteed to contain the true state and input trajectories, and we provide conditions under which the observer is stable. Furthermore, we provide a method for designing stabilizing gains that minimize an upper bound on the worst-case steady-state observer error. We demonstrate our algorithm on an IEEE 14-bus power system.

I. INTRODUCTION

The control of Cyber-Physical Systems (CPS) relies on the tight integration of various computational, communication, and sensor components that interact with each other and with the physical world in a complex way. Applications of CPS are broad and include, to name a few, industrial infrastructures [1], power grids [2], and intelligent transportation systems [3]. In such safety-critical systems, serious detriment can occur in case of malfunction or if jeopardized by malicious attackers [4]. One of the most serious types of attacks consists of false-data injection, by which counterfeit data signals are injected into the actuator signals and sensor measurements by strategic and/or malicious agents. Such attacks are not well-modeled by zero-mean, Gaussian white noises nor by signals with known bounds, given their strategic nature. On the other hand, most of the centralized approaches to state estimation are computationally expensive, especially for realistic high-dimensional CPS. Consequently, reliable distributed state and unknown input estimation algorithms are indispensable for the sake of resilient control, attack identification, and mitigation.

Motivated by this, several estimation algorithms have been proposed, in which a central entity seeks to estimate both the system state and the unknown disturbance (input). In the context where the noise signals are Gaussian and white, a large body of work proposed different designs for joint input and state estimation via e.g., minimum variance unbiased estimation [5], modified double-model adaptive estimation [6], or robust regularized least square approaches [7]. However, these approaches are not applicable in the context of attack-resilient bounded error worst-case estimation against false data injection attacks, where no information about the distribution of uncertainties is available. In such a setting, numerous approaches were proposed for deterministic systems [8], stochastic systems [9], and bounded-error systems [10]–[12]. These approaches typically yield point estimates, i.e., the most likely or best single estimate, as opposed to set-valued estimates.

Set-valued estimates have the advantage of providing hard accuracy bounds, which are important to guarantee safety [13]–[16]. In addition, the use of fixed-order set-valued methods can help decrease the complexity of optimal observers [17], which grows with time. Hence, fixed-order centralized set-valued observers were presented for different classes of systems [13], [18]–[23], that simultaneously find bounded sets of compatible states and unknown inputs. However, these algorithms do not scale well in a networked setting as the size of the network increases. This motivates the design of distributed input and state filters, which have typically focused on systems with stochastic disturbances [24], [25]. While these methods are more scalable and robust to communication failures than their centralized counterparts, they generally have comparatively worse estimation error. Moreover, they are not applicable in bounded-error settings where no information about the stochastic characteristics of noise/disturbance is available. With that in mind, in our previous work [26] we provided a distributed algorithm to synthesize interval observers for bounded-error LTI systems, without considering unknown input signals (attacks). In this work we aim to extend our design in [26] to address resilience against false data injection attacks, i.e., to synthesize distributed interval observers in the bounded-error settings that are stable and correct in the presence of unknown input/attack signals.

Contributions. This work aims to bridge the gap between distributed resilient estimation algorithms and interval observer design approaches in bounded-error settings and subject to completely unknown and/or distribution-free inputs (attacks). In other words, leveraging the notion of “collective positive detectability over neighborhoods” (CPDN), we provide a distributed algorithm that simultaneously synthesizes tractable and computationally efficient interval-valued estimates for states and unknown inputs of bounded error LTI systems, whose sensors and actuators are subject to false data injection attacks. We provide conditions for the stability of our proposed observer, which is shown to minimize a
computed upper bound for the observer error interval widths.

II. PRELIMINARIES

This section introduces basic notation, preliminary concepts, and graph-theoretic notions used throughout the paper.

Notation. Let \( \mathbb{N}, \mathbb{Z}_{\geq 0}, \mathbb{R}_{\geq 0} \) denote the sets of natural, nonnegative integer and real numbers, respectively. Similarly, \( \mathbb{R}^n \) and \( \mathbb{R}^{n \times p} \) denote the \( n \)-dimensional Euclidean space, and the set of \( n \times p \) matrices, respectively. Given \( A_1, \ldots, A_N \in \mathbb{R}^{n \times n} \), \( \text{diag}(A_1, \ldots, A_N) \in \mathbb{R}^{n \times Nn} \) is the block-diagonal matrix with block-diagonal elements \( A_i, i \in \{1, \ldots, N\} \). For \( M \in \mathbb{R}^{n \times p} \), \( M_i \) and \( M_{ij} \) denote the \( i \)-th row and the \( (i, j) \)-th entry of \( M \), respectively. Furthermore, we define \( M^+ \) and \( M^- \) as \( M^+ \triangleq \max\{M_{ij}, 0\} \) and \( M^- \triangleq M^+ - M \), respectively. All inequalities \( \leq, \geq \), as well as \( \max \) and \( \min \), are considered element-wise. Given \( M \in \mathbb{R}^{n \times n} \), \( \rho(M) \) is used to denote the spectral radius of \( M \). A multidimensional interval is denoted as \( I \triangleq [s, \bar{s}] \subset \mathbb{R}^n \), and is the set of vectors \( x \in \mathbb{R}^n \) such that \( s \leq x \leq \bar{s} \).

Proposition 1. [27, Lemma 1] Let \( A \in \mathbb{R}^{n \times n} \) and \( x \leq \bar{x} \in \mathbb{R}^n \). Then, \( A^+x - A^-\bar{x} \leq Ax \leq A^+\bar{x} - A^-x \). As a corollary, if \( A \) is non-negative, \( A_\bar{x} \leq Ax \leq A\bar{x} \).

Graph-theoretic Notions. A directed graph \( G = (\mathcal{V}, \mathcal{E}) \) is a set of nodes \( \mathcal{V} \triangleq \{1, \ldots, N\} \) and edges \( \mathcal{E} \subseteq \mathcal{V} \times \mathcal{V} \). The neighbors of node \( i \), denoted \( \mathcal{N}_i \), is the set of all nodes \( j \) for which \( (j, i) \in \mathcal{E} \). We will assume that \( i \in \mathcal{N}_i \).

III. PROBLEM FORMULATION

System Assumptions. Consider a multi-agent system (MAS) consisting of \( N \) agents, which interact over a time-invariant communication graph \( G \). The agents are able to obtain individual measurements of a target system as described by the following LTI dynamics:

\[
P : \begin{aligned}
x_{k+1} &= Ax_k + Bu_k + Gd_k, \\
y_k &= Cx_k + D_i y_k^i + H^i d_k, \quad i \in \mathcal{V}, k \in \mathbb{Z}_{\geq 0},
\end{aligned}
\]

where \( x_k \in \mathbb{R}^n \) is the continuous state of the target system, \( d_k \in \mathbb{R}^m \) is a malicious disturbance and \( u_k \in \mathcal{U}_w \triangleq [\underline{w}, \bar{w}] \subset \mathbb{R}^m \) is bounded process noise. At time step \( k \), every agent \( i \in \mathcal{V} \) takes a measurement \( y_k^i \in \mathbb{R}^{m_i} \), known only to itself, which is perturbed by \( y_k^i \in \mathcal{U}_y \triangleq [\underline{y}, \bar{y}] \subset \mathbb{R}^{m_i} \), a bounded sensor (measurement) noise signal. Finally, \( A, B \in \mathbb{R}^{n \times n}, G \in \mathbb{R}^{n \times m}, C_i \in \mathbb{R}^{m_i \times n}, D_i \in \mathbb{R}^{m_i \times m_i}, \) and \( H^i \in \mathbb{R}^{m_i \times m_i} \) are system matrices known to all agents, where \( \text{rank}(H^i) = r_i \). Note that no restriction is made on \( H^i \) to be either the zero matrix (no direct feedthrough), or to have full column rank when there is direct feedthrough. The agents’ goal is to simultaneously estimate the trajectories of (1) as well as the unknown input \( d_k \) in a distributed manner, when states are initialized in an interval \( \mathcal{I}_x \triangleq [\underline{x}, \bar{x}] \subset \mathbb{R}^n \), with \( \underline{x}, \bar{x} \) known to all agents.

\[\text{Unknown Input Signal Assumptions.}\] We make no assumption about the unknown signal \( d_k \), i.e., we require no prior knowledge such as its distribution, dynamics, or bounds.

Remark 1. System (1) can be easily extended to cover the case where different attack signals \( d_k^1 \in \mathbb{R}^{n_1} \) and \( d_k^o \in \mathbb{R}^{n_o} \) with the corresponding matrices \( G \in \mathbb{R}^{n \times n_o} \), and \( H^i \in \mathbb{R}^{m_i \times n_o} \) are injected into the actuators and sensors, respectively. In this case, courtesy of the fact that the unknown input signals can be completely arbitrary, by lumping them into a newly defined unknown input signal \( d_k \triangleq [(d_k^1)^T (d_k^o)^T]^T \in \mathbb{R}^{p_n}, n_o \triangleq n_o + n_s \), as well as defining \( G \triangleq [G_{0x}, G_{0o}], H^i \triangleq [0_m, H^i] \), we can equivalently transform the considered system to a new representation, precisely in the form of (1).

Definition 1 (State and Input Framers). For an agent \( i \in \mathcal{V} \), the sequences \( \{x_k^i, y_k^i\}_{k \geq 0} \subset \mathbb{R}^n \) are called upper and lower local state framers for \( P \) if \( x_k^i \leq x_k \leq x_k^o \) for all \( k \geq 0 \). Moreover, we define the local state framer errors as

\[
e_k^i \triangleq x_k^i - x_k, \quad \delta_k^i \triangleq x_k^o - x_k, \quad \forall k \geq 0.
\]

Finally, the collective state framer error is defined as

\[
e_k \triangleq (e_k^1)^T \cdots (e_k^N)^T (\delta_k^1)^T \cdots (\delta_k^N)^T \in \mathbb{R}^{2Nn}.
\]

The local input framers \( \{d_k^1, d_k^o\} \), the local input framer errors \( \{\delta_k^1, \delta_k^o\} \), and the collective input framer error \( \delta_k \) are defined similarly with respect to the unknown input \( d_k \).

The problem of designing a distributed resilient state and input interval observer addressed here is cast as follows:

Problem 1. Given a multi-agent system, design a distributed resilient interval observer for \( P \), i.e., an algorithm that computes uniformly bounded state and input framers for \( P \).

IV. PROPOSED DISTRIBUTED INTERVAL OBSERVER

In this section, we describe our novel resilient distributed interval observer design, its stability, and a tractable distributed procedure for computing stabilizing observer gains.

A. Distributed Input and State Framer and its Correctness

Before describing our proposed observer, we first transform the system into an equivalent representation which decouples the problem of estimating the state and the adversarial input. Inspired by the work in [13], we carry out a singular value decomposition (SVD) on the feedthrough matrix \( H^i \), which decomposes the unknown input signal into two components \( d^1_{1,k} \) and \( d^2_{2,k} \). Consequently, we obtain two constituents for the measurement signal: \( z^i_{1,k} \), which is affected by the unknown input through an invertible feedthrough matrix \( S^i \in \mathbb{R}^{r_i \times r_i} \), and \( z^2_{2,k} \), which is not compromised by the unknown input signal. Then, (1) can be represented as

\[
\begin{align*}
x_{k+1} &= Ax_k + Bu_k + G^i_1 d^1_{1,k} + G^i_2 d^2_{2,k}, \\
z^i_{1,k} &= C^i_1 x_k + D^i_1 y^i_k + S^i_1 d^1_{1,k}, \\
z^2_{2,k} &= C^i_2 x_k + D^i_2 y^i_k, \\
d^i_k &= V^i_1 d^1_{1,k} + V^i_2 d^2_{2,k}.
\end{align*}
\]
To increase readability, the details of the transformation and how to compute $V_i^1, V_i^2, G_i^1, G_i^2, C_i^1, C_i^2, D_i^1,$ and $D_i^2$ are provided in Appendix A. We further define $M_i^1 \triangleq (S_i)^{-1}$ and the concatenated noise vector $\eta_k^i \triangleq [v_{k-1}^T w_{k-1}^T v_k^T]^T$ with upper and lower bounds:

$$\eta_k^i \triangleq [\bar{\nu}^T \bar{\nu}^T \bar{\nu}^T]^T \text{ and } \bar{\eta}_k^i \triangleq [\bar{\nu}^T \bar{\nu}^T \bar{\nu}^T]^T.$$ 

To obtain input and state estimates, we require that each agent has access to adequate measurements which are not compromised by the unknown input. The following assumption ensures this. We refer the reader to [26, Definition 2] for a detailed description of an ISS interval observer.

**Assumption 1.** $C_i^2 G_i^2$ is full column rank for every $i \in \mathcal{V}$. Hence, there exists $M_i^2 = (C_i^2 G_i^2)^\dagger$ such that $M_i^2 C_i^2 G_i^2 = I$.

It is worth noting that $C_i^2$ and $G_i^2$ are both affine transformations of $C$ and $G$, respectively. Moreover, adequacy of measurements plays an important role when applying a singular value decomposition on the direct feedthrough matrix in the output equation (cf. Appendix A for more details). We are ready to propose our recursive distributed simultaneous state and unknown input observer.

### B. Distributed Input and State Framer and its Correctness

To address Problem 1, we propose a four-step procedure, summarized as the DISTRIBUTED SIMULTANEOUS INPUT & STATE INTERVAL OBSERVER (DSISO) in Algorithm 1.

**i) State Propagation and Measurement Update:** Given $\bar{x}_k^i, \bar{\tau}_k^i, \bar{z}_{1,k}^i, \bar{z}_{2,k}^i$, and $\bar{z}_{2,k+1}^i$, each agent $i \in \mathcal{V}$ performs a state propagation and a local measurement update step using to-be-designed observer gains $L^i$ and $\Gamma^i$ in $\mathbb{R}^{n \times m_i}$:

$$\begin{align*}
\bar{x}_{k+1}^i &= \bar{A}^i \bar{x}_k^i - \bar{A}_{-i}^i \bar{x}_k^i + L^i \bar{y}_k^i - L^i \bar{y}_k^i + \bar{\Psi} \bar{e}_{k+1}^i, \\
\bar{\tau}_{k+1}^i &= \bar{A}^i \bar{\tau}_k^i - \bar{A}_{-i}^i \bar{\tau}_k^i + L^i \bar{\tau}_k^i - L^i \bar{\tau}_k^i + \bar{\Psi} \bar{e}_{k+1}^i,
\end{align*}$$

(5)

where $\bar{A}_i, L_i, \Psi_i$, which define the observer dynamics, depend linearly on $L_i, \Gamma_i$ and $\bar{\Psi}_i$. We also note that $\bar{A}_i$ has the form $\bar{A}_i \triangleq T_i \bar{A}_i - L_i C_i^2$, where $T_i = I - \Gamma_i C_i^2$, and $\bar{A}_i$ depends only on parameters of $\bar{\Psi}_i$.

**ii) State Framer Network Update:** Each agent $i$ shares its local state framers with its neighbors in the network, updating them by taking the tightest interval from all neighbors via intersection:

$$\bar{x}_k^i = \max_{j \in \mathcal{N}_i} \bar{x}_k^j, \quad \bar{\tau}_k^i = \min_{j \in \mathcal{N}_i} \bar{\tau}_k^j.$$ 

(6)

We consider only one iteration of this operation for simplicity; the extension to multiple iterations is straightforward.

**iii) Input Estimation:** Given the state framers (6), agent $i \in \mathcal{V}$ leverages the state dynamics and its measurement of the system to compute local input framers as follows:

$$\begin{align*}
\bar{d}_{k}^{i,0} &= \bar{A}_i^{i} \bar{x}_k^i - \bar{A}_{-i}^i \bar{x}_k^i + \bar{F}_i \bar{\eta}_k^i + \bar{\Phi}_i \bar{e}_{k+1}^i, \\
\bar{d}_{k}^{i} &= \bar{A}_i^{i} \bar{\tau}_k^i - \bar{A}_{-i}^i \bar{\tau}_k^i + \bar{F}_i \bar{\eta}_k^i - \bar{F}_i \bar{\eta}_k^i + \bar{\Phi}_i \bar{e}_{k+1}^i,
\end{align*}$$

(7)

where $\bar{A}_i^i, \bar{F}_i, \bar{\Phi}_i$ are described in Appendix B.

**iv) Input Framer Network Update:** Finally, each agent $i$ shares its local input framers with its neighbors in the network, again taking the intersection,

$$\bar{d}_k^i = \max_{j \in \mathcal{N}_i} \bar{d}_k^j, \quad \bar{\tau}_k^i = \min_{j \in \mathcal{N}_i} \bar{\tau}_k^j.$$ 

(8)

**Remark 2.** There are many existing centralized interval observer designs in the literature that could potentially be used for step i). However, most of these methods rely on similarity transformations [28] which depend on the observation matrices $C_i$. In a multi-agent setting, use of these methods necessitates transforming to and from the original coordinates whenever estimates are shared over the network. Each repeated transformation incurs the so-called “wrapping effect” as a result of Proposition 1, which worsens the estimation error and negates the benefit of exchanging information over the network. We avoid this with the choice of (5), which is computed directly in the original coordinates.

**Algorithm 1 DSISO at node $i$.**

**Input:** $\bar{x}_0^i, \bar{\tau}_0^i$; **Output:** $\{\bar{x}_k^i, \bar{\tau}_k^i, \bar{d}_k^i, \bar{\tau}_k^j\}_{k \geq 0}$.

1: Compute $L^i, \Gamma^i$, and $T^i$ by solving (9);
2: $k \leftarrow 1$
3: **loop**
4: **State propagation and measurement update**
5: Compute $\bar{x}_k^i, \bar{\tau}_k^i$ using (5);
6: **State framer network update**
7: Send $\bar{x}_k^i$ and $\bar{\tau}_k^i$ to $\{j : i \in \mathcal{N}_j\}$
8: Receive $\bar{x}_k^j, \bar{\tau}_k^j$ from $j \in \mathcal{N}_i$
9: $\bar{x}_k^i \leftarrow \max_{j \in \mathcal{N}_i} \bar{x}_k^j, \bar{\tau}_k^i \leftarrow \min_{j \in \mathcal{N}_i} \bar{\tau}_k^j$
10: **Input framer estimation**
11: Compute $\bar{d}_k^{i,0}$ and $\bar{\tau}_k^i$ using (7);
12: **Input framer network update**
13: Send $\bar{d}_k^{i,0}$ and $\bar{\tau}_k^i$ to $\{j : i \in \mathcal{N}_j\}$
14: Receive $\bar{d}_k^j, \bar{\tau}_k^j$ from $j \in \mathcal{N}_i$
15: $\bar{d}_k^i \leftarrow \max_{j \in \mathcal{N}_i} \bar{d}_k^j, \bar{\tau}_k^i \leftarrow \min_{j \in \mathcal{N}_i} \bar{\tau}_k^j$
16: **end loop**
17: return $\{\bar{x}_k^i, \bar{\tau}_k^i, \bar{d}_k^i, \bar{\tau}_k^j\}_{k \geq 0}$

**Lemma 1 (Distributed Framer Construction).** The DSISO algorithm outputs interval state and input framers for $\mathcal{P}$.

**Proof.** See Appendix B.

**C. Distributed Stabilizing and Error Minimization**

In this subsection, we investigate conditions on the observer gains $L^i$ and $\Gamma^i$, as well as the communication graph $\mathcal{G}$, that lead to an input-to-state stable (ISS) distributed...
observer, which equivalently results in a uniformly bounded observer error sequence given in (2)–(3), in the presence of bounded noise. To guarantee stability, we use the following assumption on the agents’ observation matrices and the structure of the network graph.

**Assumption 2** (Collective Positive Detectability over Neighborhoods (CPDN) [26]). For every state dimension \( s \in \{1, \ldots, n\} \) and every agent \( i \in V \), there is an agent \( \ell(i, s) \in N_i \) such that there exist gains \( L^{\ell(i, s)} \) and \( \Gamma^{\ell(i, s)} \) satisfying

\[
\| (T^{\ell(i, s)} A^{\ell(i, s)} - L^{\ell(i, s)} C_2^{\ell(i, s)}) s \|_1 < 1.
\]

Intuitively, this assumption narrows the problem of stability to subgraphs. Within these subgraphs, we require that for each state dimension \( s \), there is a node that, given estimates of all other state dimensions \( \{1, \ldots, s-1, s+1, \ldots, n\} \), can compute an accurate estimate of dimension \( s \). With this assumption in mind, we propose a two-step process to design the observer gains \( L^i \) and \( \Gamma^i \). First, each node executes a procedure (Algorithm 2) which verifies Assumption 2, returning false if it is not satisfied, or else computes some feasible stabilizing gains and the set of state dimensions which a node can contribute to estimating, i.e.,

\[
J^i = \{ s : \exists T^i, L^i, \Gamma^i \text{ s.t. } \| (T^i A^i - L^i C_2^i) s \|_1 < 1 \}.
\]

Then, given this information, each node solves the LP in (9), which simultaneously guarantees stability and minimizes an upper bound on the observer error. This design process improves on the one proposed in [26] in the absence of attacks, by first identifying “stabilizing” agents for each state dimension, then minimizing an upper bound on the error while enforcing the stability condition. In this way, the design includes a sense of noise/error attenuation. The following theorem formalizes our main results on how to tractably synthesize stabilizing and error minimizing observer gains in a distributed manner.

**Theorem 1** (Distributed Input and State Interval Observer Design). Suppose Assumptions 1 and 2 hold and \( L^i_s, T^i_s, \) and \( \Gamma^i_s \) are solutions to the following convex program:

\[
\begin{align*}
\min_{Z^i, L^i, T^i, \Gamma^i} & \quad \| L^i (\bar{\eta}^i - \eta^i) \|_\infty \\
\text{s.t.} & \quad T^i = I - \Gamma^i C_2^i, \\
& \quad \sum_{s=1}^n Z^i_{ss} < 1, \quad \forall j \in J^i, \\
& \quad -Z^i \leq T^i A^i - L^i C_2^i \leq Z^i,
\end{align*}
\]

where \( L^i \) is defined in (5) and \( \bar{\eta}^i \) is calculated using Algorithm 2. Then, the DSISO algorithm, i.e., (5)–(8), with the corresponding observer gains \( L^i_s, T^i_s, \Gamma^i_s \) constructs an ISS distributed input and state interval observer. Moreover, the steady state observer guarantees are bounded to be:

\[
\begin{align*}
\| e^i_k \|_\infty & \leq \frac{1}{\rho^*_e} \max_i \| L^i |\Delta^i_\eta \|_\infty, \\
\| \delta^i_k \|_\infty & \leq \frac{c(A^i_\theta)}{1-\rho^*_e} \max_i \| L^i |\Delta^i_\eta \|_\infty + \max_i \| F^i |\Delta^i_\eta \|_\infty,
\end{align*}
\]

where \( \rho^*_e, A^i_\theta, \) and \( \Delta^i_\theta \) are given in Lemma 2.

In order to prove our main results in Theorem 1, we need to first take two intermediate steps on i) providing closed form expressions for the observer errors and their upper bounds, and ii) ensuring the existence of stabilizing gains, stated via Lemmas 2 and 3, respectively. To begin, we note that equations (5)-(8) result in a switched linear system, with the following set of possible switching signals:

\[
\mathcal{M} \triangleq \left\{ M \in \{0,1\}^{2Nn \times 2Nn} : M_{ij} = 0, \forall j \notin N_i, \sum_{k=1}^{2Nn} M_{ik} = 1 \right\},
\]

which encodes all possible permutations of the operation (6).

**Lemma 2** (Error Bounds). For all \( B \in \mathcal{M} \), the errors of the DSISO observer (5)–(8) are upper bounded as follows:

\[
\begin{align*}
\| e^i_k \|_\infty & \leq \| e^i_0 \|_\infty \rho^*_e + 1 - \rho^*_e \max_i \| L^i |\Delta^i_\eta \|_\infty, \\
\| \delta^i_k \|_\infty & \leq \rho(\mathcal{A}_e) \| e^i_0 \|_\infty + \max_i \| F^i |\Delta^i_\eta \|_\infty,
\end{align*}
\]

where \( \rho^*_e \triangleq \rho(\mathcal{A}_e), A^i_e \triangleq \text{diag}(A^i_1, \ldots, A^i_N), A^i_s \triangleq \left[ A^i_s^1 \quad A^i_s^2 \right]^{\top}, A^i_s \triangleq A^i_s^1 A^i_s^2 = \left[ A^i_s^1 A^i_s^2 \right]^{\top}, A^i_s \triangleq A^i_s^1 A^i_s^2 = \left[ A^i_s^1 A^i_s^2 \right]^{\top}, \forall j \in J^i, \Delta^0 \triangleq \bar{\eta}^i - \eta^i.
\]

**Proof.** Starting from (5)-(8) and following the lines of the proof of [26, Theorem 1], for any \( B \in \mathcal{M} \), the frame errors can be bounded by the positive linear comparison system

\[
e_{k+1} \leq B A e_k + B \gamma^i_k, \quad \delta_k \leq A e_k + \gamma^i_k
\]

where \( \forall s \in \{ x, d \} : \gamma^s_k \triangleq \left[ (A^i_1)^\top \ldots (A^i_N)^\top \right]^{\top}, \xi^s_k \triangleq \left[ (\xi_1^s)^\top \ldots (\xi_N^s)^\top \right]^{\top}, \xi^s_k \triangleq \left[ (\Xi_1^s)^\top \ldots (\Xi_N^s)^\top \right]^{\top}, \forall j \in J^i, \Delta^0 \triangleq \bar{\eta}^i - \eta^i. \]

Moreover, it follows from the solution of (12) that

\[
e_k \leq (B A e_k)^{k-1} e_0 + \sum_{s=1}^{k-1} (B A e_k)^{k-s} \gamma^s_{k-1}. \]

Further, \( \| \gamma^i_k \|_\infty \leq \max_i \| \xi^i \| (\bar{\eta}^i - \eta^i) \) by non-negativity of \( (\Xi_1^i)^\top, (\Xi_N^i)^\top \), and \( \bar{\eta}^i - \eta^i \). The result follows from (12), (13), sub-multiplicativity of norms and the triangle inequality.

**Lemma 3.** If Assumption 2 holds, then there exist \( L^i \) and \( \Gamma^i \) such that, for some \( B \in \mathcal{M} \), \( B A_e \) is Schur stable, i.e., \( \rho(B A_e) < 1 \). Consequently, the DSISO algorithm is ISS.

**Proof.** It follows from combining [26, Theorems 1 & 2].

We are ready to provide a proof for Theorem 1 as follows. **Proof of Theorem 1.** By Lemma 3, Assumption 2 implies the existence of gains that render the DSISO algorithm ISS. It remains to show that the solutions of (9) are stabilizing. First, notice that Algorithm 2 computes \( J^i \) by solving (14). The use of \( J^i \) in the constraints of (9) guarantees that the optimization problem is feasible. Furthermore, we can show that since Assumption 2 holds, there exists \( B \) such that \( \rho(B A_e) < 1 \), and therefore that the DSISO algorithm is ISS. We refer the reader to [26, Theorem 2] for the construction of \( B \). This in combination with Lemmas 2 and 3 ensures that the bounds in (11) converge to their steady state values in (10).

**Remark 3.** It is worth noting that by the following change of variables, the convex program in (1) can be easily and equivalently stated in the form of a linear program (LP):

\[
\begin{align*}
\min & \quad \lambda \\
\text{s.t.} & \quad \theta(\bar{\eta}^i - \eta^i) \leq \lambda_1, \quad -\theta \leq L^i \leq \theta, \\
& \quad T^i = I - \Gamma^i C_2^i, \quad \sum_{s=1}^n Z^i_{ss} < 1, \quad \forall j \in J^i, \\
& \quad -Z^i \leq T^i A^i - L^i C_2^i \leq Z^i,
\end{align*}
\]

which can be considered as complementary to \( H_\infty \)-optimal observer design, e.g., in [18], [19], [29].
Algorithm 2 DSISO initialization at node $i$.

Input: $A$, $C_i$, $N_i$; Output: $J_i$

1: Compute $L_i^*$, $\Gamma_i^*$, and $Z_i^*$ by solving
   \[
   \min_{Z_i} \sum_{t=1}^n \sum_{t=1}^n (Z_i)_st^t \\
   \text{s.t.} \quad -Z_i^* \leq (I - \Gamma_i C_i^2)A_i^t - L_i^t C_i^2 \leq Z_i^*. \tag{14}
   \]

2: $J_i \leftarrow \{ s : \sum_{t=1}^n (Z_i)_st < 1 \}$;
3: $Q_i \leftarrow \{(I - \Gamma_i C_i^2)A_i^t - L_i^t C_i^2 \}$;
4: Receive $Q_i$ from $j \in N_i$;
5: $Q_i \leftarrow \bigcup_{j \in N_i} Q_j$;
6: if $\forall s \in \{1, \ldots, n\}$, $\exists P \in Q_i \text{ s.t. } \|(P)_s\|_1 < 1$ then
7:    return false (i.e., Assumption 2 not satisfied)
8: else
9:    return $J_i$
10: end if

V. SIMULATION

In this section we demonstrate the DSISO algorithm on an IEEE 14-bus system [30]. We refer the reader to [8] for the derivation of the LTI representation of the system, which can be discretized and written in the form of (1). The $n = 10$ dimensional state $x_k^t = [\theta_k^t \ \omega_k^t]^T$ represents the rotor angle and frequency of each of the 5 generators. Each bus in the test case corresponds to a node in the algorithm. The noise signals satisfy $\|w_k\|_\infty < 5$ and $\|v_k\|_2 < 1 \times 10^{-4}$ for all $i \in V$. Similarly to the example in [8], each node (bus) measures its own real power injection/consumption, the real power flow across all branches connected to the node, and for generating nodes, the rotor angle of the associated generator.

In this example, we assume that the generator at node 1 is insecure and potentially subject to attacks. Due to the reduction necessary to eliminate the algebraic constraints of the power system model [8], the disturbance appears directly in the measurements of all nodes, resulting in nonzero $H_i$ matrices. We compute the gains $L_i^*$ and $\Gamma_i^*$ by solving (9). Figures 1 and 2 show the input and state framers, respectively. It is clear that the algorithm is able to estimate the state $x_1$ despite the disturbance with only minor performance degradation. The switching due to (6), which depends on the noise, is also evident. The estimation performance for the other states is comparably better, since they are only affected by (known) bounded noise. Furthermore, all agents are able to maintain an accurate estimate of the disturbance.

VI. CONCLUSION AND FUTURE WORK

This paper introduced a novel distributed algorithm for interval estimates of states and unknown inputs for LTI systems with bounded noise, whose sensors and actuators are compromised by false data injection attacks. Without imposing any restrictive assumptions such as boundedness or stochasticity on the unknown input (attack) signals, we addressed the correctness of the proposed distributed observer, and moreover, analyzed the stability of the observer by considering the switched linear dynamics of the resulting error system. Finally, we provided a tractable method for computing stabilizing gains which aim to minimize the steady state input and state error of the observer. Hence, our approach can serve the purpose of resilient estimation in bounded-error networked cyber-physical systems. In the future, we consider extending our approach to nonlinear and hybrid systems, as well as including other type of adversarial effects such as switching and network attacks in our setting.

APPENDIX

A. Similarity Transformation

Let $r^i \triangleq \text{rank}(H_i)$. Using SVD, $H_i = [U_1^i \ U_2^i] \begin{bmatrix} S^i & 0 \\ 0 & 0 \end{bmatrix} [V_1^i]^T \ [V_2^i]^T$, where $S^i \in \mathbb{R}^{r^i \times r^i}$ is a diagonal matrix of full rank, $U_1 \in \mathbb{R}^{m_r \times r^i}$, $U_2 \in \mathbb{R}^{m_l \times (m_r-r^i)}$, $V_1 \in \mathbb{R}^{n_r \times r^i}$ and $V_2 \in \mathbb{R}^{n_l \times (n_r-r^i)}$, while $U \triangleq [U_1 \ U_2]$ and $V \triangleq [V_1 \ V_2]$ are unitary matrices. Then, $d_k$ can be decoupled into two orthogonal components as:
\( d_{1,k} = (V_1^i)\top d_k, d_{2,k} = (V_2^i)\top d_k, d_k = V_1^i d_{1,k} + V_2^i d_{2,k}, \) which transforms the system dynamics (1) to the representation in (4), where \( G_1 \triangleq GV_1^i, G_2 \triangleq GV_2^i, H_1 \triangleq H^i V_1^i = \eta_1, C_1 \triangleq (U_1^i)\top C^i, C_2 \triangleq (U_2^i)\top C^i, D_1 \triangleq (U_1^i)\top D^i, \) and \( D_2 \triangleq (U_2^i)\top D^i. \)

### B. Proof of Lemma 1

First, note that (4b) implies that
\[
d_{1,k} = M_1^i (z_{1,k} - C_1^i x_k - D_1^i v_k). \tag{15}\]

This, in combination with (4c) and (4a) results in
\[
M^2_{1,k+1} z_{2,k+1} + D_2^i v_{k+1} = M^2_2 (C_2^i x_k + B u_k + G_1 (M_1^i (z_{1,k} - C_1^i x_k - D_1^i v_k) + G_2^i d_{2,k})) + D_{2,k+1}, \tag{16}\]

where given Assumption 1, returns
\[
d_{2,k} = M_2^i \left( z_{2,k+1}^i - C_2^i x_k - D_2^i v_k \right), \tag{17}\]

where \( E^i = M_2^i C_2^i C_1^i D_2^i - C_1^i B - D_2^i \). By plugging \( d_{1,k} \) and \( d_{2,k} \) from (15) and (16) into (4a),
\[
x_{k+1} = \eta_1 x_k + (J^i Q^i z_{2,k} + E^i \eta_{k+1} + 1) + J^i C_1^i D_1^i \]

Combined with the fact that \( \eta = I - \Gamma C_2^i, \) this implies
\[
x_{k+1} = (J^i Q^i z_{2,k} + E^i \eta_{k+1} + 1) + \Gamma C_2^i x_k \tag{18}\]

Plugging in \( C_{2,k+1}^i = \xi_{2,k+1}^i - D_{2,k+1}^i v_{k+1} \) from (14c) and adding the zero term \( L_{1}^i (z_{2,k}^i - C_{2,k}^i z_{2,k} - D_{2,k}^i v_k) \) to the right hand side of (17), then collecting like terms, results in
\[
x_{k+1} = A^i x_k + L_{1}^i \eta_{k+1} + \Psi^i \xi_{1,k+1}^i. \tag{19}\]

By applying Proposition 1 to all the uncertain terms in the right hand side of (18): \( \xi_{1,k}^i \)
\[
\xi_{1,k}^i \leq x_k \leq \eta_{k+1} \Rightarrow \xi_{k+1}^i \leq \rho_{k+1} \leq \rho_{k+1}^i \]

where \( \rho_{k+1}^i, \rho_{k+1}^i \), are given in (5). This means that individual framers/interval estimates are correct. When the framer condition is satisfied for all nodes, the intersection of all the individual estimates of neighboring nodes (cf. (6)) also results in correct interval framers, i.e.
\[
\xi_{k}^i \leq x_k \leq \eta_{k}^i, \forall i \in \mathcal{V} \Rightarrow \xi_{k}^i \leq \eta_{k}^i \leq \eta_{k}^i, \forall i \in \mathcal{V}. \]

Furthermore, plugging \( d_{1,k} \) and \( d_{2,k} \) from (15) and (16) into (4d) and applying Proposition 1 returns the input framers in (7), where their intersection is still a framer (cf. (8)) by the same reasoning as for the state framers. Since the initial state framers are known to all \( i \), by induction (5)-(8) constructs a correct distributed interval state and input framer for (1).