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

Distributed Resilient Observer: Blended Dynamics Theory Meets ℓ_1-Minimization Approach

Donggil Lee, Junsoo Kim, and Hyungbo Shim

***Abstract*— This paper presents a distributed resilient observer for continuous-time linear time-invariant plants that remains functional even under sensor attacks. The proposed method aims to determine the estimation outcome that matches the majority of sensor measurements, which is formulated as an ℓ_1-minimization problem considering all the observable components of each sensor measurement. A distributed observer based on the blended dynamics theory is then proposed to solve the ℓ_1-minimization problem in a distributed manner. As a result, the distributed resilient estimation is enabled for a broader class of systems compared to previous works. The design procedure is constructive with parameters obtained from a specified condition that is equivalent to the well-known null-space property.**

I. Introduction

In response to recent developments in network communication technology, the *distributed state estimation problem* in sensor networks has been studied extensively [1]–[3]. In the problem, spatially deployed multi-agents are requested to cooperatively estimate the state of a target system, particularly under the localized structure; each agent can use its own sensor measurements and the information received from its neighboring agents through a communication network. Such structure provides benefits of scalability and robustness on its operation [4].

On the other hand, as new threats caused by malicious attacks have been reported (e.g., attacks on sewage control systems [5] and StuxNet malware on SCADA systems [6]), attack-resilient design in networked systems has become one of main concerns [7], [8]. For the sensor networks, such resiliency is essential because the more sensors there are, the more likely they could be compromised by malicious attackers. Under this context, we consider the *distributed resilient state estimation problem* in sensor networks, where attackers could inject false information into sensor measurements.

The key idea to handle the sensor attacks is the *majority voting* from redundant sensor measurements. Specifically, the estimation outcome is determined as a value that coincides with the majority of the measurements. One strand of research is to formulate this idea as an ℓ_0-minimization problem [9], [10], where the resilient estimation can be guaranteed as long as the number of sensor attacks is less than a threshold value. Motivated by this, the authors of [11] address the resilient estimation problem in a distributed manner, where a consensus-based technique is employed for each agent to get a compressed version of all the sensor measurements. However, it suffers from scalability issues due to the NP-hard and combinatorial nature of the ℓ_0-minimization problem. More specifically, significant communication and computation are required for each agent to prepare for a larger number of sensor attacks.

Another strand is to formulate the idea of majority voting as an ℓ_1-minimization problem [10], [12]. This approach can be explained as arguably the tightest convex relaxation of the ℓ_0-minimization, which reduces the computational complexity dramatically [13], [14]. Inspired by this, [15] proposes a scalable distributed algorithm solving the resilient estimation problem, with the help of one technical assumption on system dynamics called the *scalar decomposability*[1]. Under this assumption, the resilient state estimation problem can be decomposed into multiple sub-problems, where each sub-problem is simplified as an ℓ_1-minimization problem with scalar variables only.

In this paper, we extend the method of [15] so that distributed resilient state estimation becomes possible even for systems not satisfying the scalar decomposability condition. To achieve this, we first consider a local partial observer of each agent, and formulate the estimation problem to a general form of an ℓ_1-minimization problem regarding all the partial estimates. Then, we construct a distributed resilient observer that estimates the whole state of a target system by cooperatively solving the ℓ_1-minimization problem. Especially, to guarantee the achievement of resilient estimation, we provide a condition, which has a modified form of the well-known *null-space property* [16] and helps to determine the parameters of the distributed observer.

As a tool for the design of distributed observer, we employ the *blended dynamics theory* [17]. To be more specific, let us consider a heterogeneous multi-agent system

$$\dot{x}_i = f_i(t, x_i) + \gamma \sum_{j \in \mathcal{N}_i} (x_j - x_i), \quad i \in \mathcal{N} := \{1, \cdots, N\} \quad (1)$$

where x_i is the state, $f_i(t, x_i)$ is the individual vector field, $\mathcal{N}$ represents the set of agent indices, and $\mathcal{N}_i$ is the index set of neighbor agents connected to agent i. Under an undirected and connected communication graph, if the coupling gain $\gamma > 0$ is sufficiently large, then each state $x_i(t)$ of (1) obeys

This work was supported in part by the National Research Foundation of Korea(NRF) grant funded by the Korea government(Ministry of Science and ICT) (No. RS-2022-00165417), and in part by Seoul National University of Science and Technology.

D. Lee and H. Shim are with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Korea.

J. Kim is with the Department of Electrical and Information Engineering, Seoul National University of Science and Technology, Korea.

[1]There exists a uniform basis such that all the unobservable subspaces of each sensor measurement have a basis that can be represented as a subset of the uniform basis.

the solution $s(t)$ of the so-called *blended dynamics* defined as

$$\dot{s} = \frac{1}{N}\sum_{i=1}^{N} f_i(t,s)$$

as long as the blended dynamics is stable in some sense. Thus, we design the f_i's so that the blended dynamics becomes a gradient flow dynamics[2] for the ℓ_1-minimization problem. Thanks to the convexity of the problem, the solution $s(t)$ may converge to the minimizer under some conditions. Therefore, we conjecture that every agent obtains the correct estimation outcome.

The remainder of the paper is organized as follows. In Section II, we rigorously formulate the distributed resilient estimation problem in the sensor networks, along with the required assumptions. In Section III, details of the proposed algorithm are presented, followed by the main result. Section IV shows simulation results of the proposed scheme, and Section V concludes this paper.

Notation: Let $1_N \in \mathbb{R}^N$ be a vector comprising all ones, and $I_N \in \mathbb{R}^{N\times N}$ be the identity matrix. For a matrix B, $\|B\|_p$ denotes the induced matrix p-norm. For a finite set C, $|C|$ represents the cardinality of C. For $s \in \mathbb{R}$, we denote the signum function by $\mathrm{sign}(s) = 0$ if $s = 0$ and $\mathrm{sign}(s) = s/|s|$ otherwise. For a vector $x = [x_1, \cdots, x_k]^T \in \mathbb{R}^k$, let $\mathrm{sign}(x) := [\mathrm{sign}(x_1), \mathrm{sign}(x_2), \cdots, \mathrm{sign}(x_k)]^T \in \mathbb{R}^k$ be the componentwise signum function, by abuse of notation. Let $S^n := \{r \in \mathbb{R}^n \,|\, \|r\|_2 = 1\}$ be the surface of n-dimensional unit sphere. A communication topology is represented by an unweighted graph $\mathcal{G} := \{\mathcal{N}, \mathcal{E}\}$, where $\mathcal{N} = \{1, \cdots, N\}$ is a finite nonempty set of agent indices, and $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$ is an edge set of ordered pairs of agent indices. We denote $\mathcal{N}_i = \{j \in \mathcal{N} \,|\, (j,i) \in \mathcal{E}\}$ as the index set of agents who can give information to the agent i, and the Laplacian matrix of the graph $\mathcal{G}$ as $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{N\times N}$, where l_{ij} is $|\mathcal{N}_i|$ if $i = j$, -1 if $j \in \mathcal{N}_i$, and 0 otherwise. For discontinuous dynamical systems, the solution is considered in the sense of Filippov.

II. Problem Formulation

For a linear time-invariant plant given by

$$\dot{x} = Ax \tag{2}$$

where $x \in \mathbb{R}^n$ is the state with $\|x(0)\|_2 < M$ for $M > 0$, we consider N agents, whose goal is to estimate the state $x(t)$. Each agent i can communicate with neighboring agents $j \in \mathcal{N}_i$, and measure an output $y_i(t)$ of the plant

$$y_i(t) = C_i x(t) + a_i(t) \quad \in \mathbb{R}^{p_i} \tag{3}$$

where $a_i(t) \in \mathbb{R}^{p_i}$ is the attack signal that may corrupt the measurement $y_i(t)$ to an arbitrary value.

The distributed resilient state estimation problem is of interest; that is to design a distributed observer for the system (2) and (3) such that each agents obtains the correct state $x(t)$, even when some sensors are compromised by attackers. We particularly propose the distributed observer having a localized structure, which is characterized as follows:

i) *(local measurement)*: Each agent i utilizes the measurement $y_i(t)$, which may not be sufficient to estimate the whole state $x(t)$.
ii) *(local communication)*: To compensate such insufficient measurement, each agent communicates with neighbors, according to a communication network represented by an undirected and connected graph $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$.

If the majority of measurements $\{y_i(t)\}_{i\in\mathcal{N}}$ are corrupted by attack signals, then the accurate state estimation becomes impossible. To deal with this, we assume that the malicious attacker can compromise at most q out of N agent outputs.

Assumption 1: There exist at least $N - q$ agents that are not attacked for all t, i.e., $|U| \geq N - q$, where

$$U := \{i \in \mathcal{N} \,|\, a_i(t) \equiv 0\}. \tag{4}$$

The set U is unknown to the agents.

III. Proposed Scheme

In this section, we present a distributed estimation scheme for obtaining the state $x(t)$ of (2), even when some sensors suffer from the attack signals. In the proposed approach, each agent $i \in \mathcal{N}$ runs two observers. The first observer is a standard partial observer that estimates the observable components from $y_i(t)$, but not the entire state $x(t)$. The second observer is designed to decode the whole state $x(t)$ of the target system (2), by solving an ℓ_1-minimization problem regarding all the partial estimates in a distributed manner. This distributed approach enables the correct state estimation even when some sensors are compromised.

A. Design of Partial Observer

Let us construct a partial observer of the agent $i \in \mathcal{N}$ for the system (2) regarding the measurement $y_i(t)$. For the observability matrix with respect to the pair (A, C_i) given by $\mathcal{O}_i := \mathrm{col}_{k=1}^n(C_i A^{k-1})$ with $\mathrm{rank}(\mathcal{O}_i) = d_i$, one can find two matrices $Z_i \in \mathbb{R}^{d_i\times n}$ and $W_i \in \mathbb{R}^{(n-d_i)\times n}$ such that their rows are orthonormal basis of $\mathrm{Im}(\mathcal{O}_i^T)$ and $\ker(\mathcal{O}_i)$, respectively. With the coordinate change of $z_i(t) := Z_i x(t)$ and $w_i(t) := W_i x(t)$, the system (2) is rewritten as

$$\begin{aligned}\dot{z}_i &= Z_i A Z_i^T z_i \\ \dot{w}_i &= W_i A Z_i^T z_i + W_i A W_i^T w_i \\ y_i &= C_i Z_i^T z_i + a_i\end{aligned}$$

with the pair $(Z_i A Z_i^T, C_i Z_i^T)$ being observable. Thus, there exists a gain L_i such that $Z_i A Z_i^T - L_i C_i Z_i^T$ is Hurwitz, and hence, each agent i runs the following partial observer:

$$\dot{\hat{z}}_i = Z_i A Z_i^T \hat{z}_i + L_i(y_i - C_i Z_i^T \hat{z}_i) \in \mathbb{R}^{d_i} \tag{5}$$

with $\|\hat{z}_i(0)\|_2 \leq M$. The design of the injection gain L_i guarantees the existence of constants[3] $B_\epsilon > 0$ and $\alpha > 0$

[2]For a differentiable function $F : \mathbb{R}^n \to \mathbb{R}$, a gradient flow dynamics is $\dot{s} = -\nabla F(s)$, which flows along the route of the steepest descent direction.

[3]Since the matrix $Q_i := Z_i A Z_i^T - L_i C_i Z_i^T$ is Hurwitz, $V_i(t) = \epsilon_i^T(t) P_i \epsilon_i(t)$ is a Lyapunov function for $\epsilon_i(t)$, where $P_i > 0$ is the solution of $Q_i^T P_i + P_i Q_i + I_n = 0$. Therefore, the constants can be given by $B_\epsilon := 2M \cdot \max_{i\in\mathcal{N}} \sqrt{\frac{\lambda_{\max}(P_i)}{\lambda_{\min}(P_i)}}$ and $\alpha := \min_{i\in\mathcal{N}} \frac{1}{2\lambda_{\max}(P_i)}$.

such that the estimation error $\epsilon_i(t) := \hat{z}_i(t) - z_i(t)$ satisfies

$$\|\epsilon_i(t)\|_2 \leq B_\epsilon e^{-\alpha t}, \quad \forall i \in U. \tag{6}$$

Therefore, for all $i \in U$ with arbitrary σ_ϵ, one can obtain

$$\|\epsilon_i(t)\|_2 \leq B_\epsilon, \quad \forall t \geq 0, \tag{7a}$$

$$\|\epsilon_i(t)\|_2 \leq \sigma_\epsilon, \quad \forall t \geq T_\epsilon := \frac{1}{\alpha} \ln\Big(\frac{B_\epsilon}{\sigma_\epsilon}\Big). \tag{7b}$$

On the other hand, for $i \in \mathcal{N} \setminus U$, the estimation error $\epsilon_i(t)$ may not converge to zero due to the attack signal $a_i(t)$.

B. Design of Distributed Observer

We now design a distributed observer that estimates the whole state $x(t)$ of (2) based on an ℓ_1-minimization problem regarding the partial observer of (5). To this end, let us stack all the partial estimates as follows:

$$\begin{aligned}\hat{z}(t) &= z(t) + \epsilon(t) = Zx(t) + \epsilon(t) \\ &= \begin{bmatrix} Z_1 \\ \vdots \\ Z_N \end{bmatrix} x(t) + \begin{bmatrix} \epsilon_1(t) \\ \vdots \\ \epsilon_N(t) \end{bmatrix} = \begin{bmatrix} \hat{z}_1(t) \\ \vdots \\ \hat{z}_N(t) \end{bmatrix} \in \mathbb{R}^{\sum_{i=1}^N d_i}. \end{aligned} \tag{8}$$

Then, the state estimation problem at a time instant t can be interpreted as decoding the state $x(t)$ from the relation (8), where the matrix Z is a known linear code and the partial estimate $\hat{z}(t)$ is available instead of $z(t)$.

To recover the state $x(t)$, we consider an estimator at a time instant t based on the ℓ_1-minimization problem:

$$\min_{\hat{x} \in \mathbb{R}^n} \ \|Z\hat{x} - \hat{z}(t)\|_1 = \min_{\hat{x} \in \mathbb{R}^n} \ \sum_{i=1}^N \|Z_i\hat{x} - \hat{z}_i(t)\|_1. \tag{9}$$

It should be noted that the problem (9) is convex, and hence, the existence of a minimizer is guaranteed. More specifically, the set $\mathcal{M}(t)$ of the optimal solutions for (9), defined as

$$\mathcal{M}(t) := \Big\{ x^* \in \mathbb{R}^n \ \Big| \ \|Zx^* - \hat{z}(t)\|_1 = \min_{\hat{x} \in \mathbb{R}^n} \|Z\hat{x} - \hat{z}(t)\|_1 \Big\}$$

is non-empty. Moreover, the minimizer can be efficiently obtained using the gradient descent dynamics, which contrasts with the estimators based on ℓ_0-minimization problem [10].

However, the minimizer of the problem (9) may not coincide with the state $x(t)$, due to the estimation error $\{\epsilon_i(t)\}_{i=1}^N$ of the partial observers. In order to deal with this issue, we consider a condition on the matrix Z, as follows.

Definition 1: For an index set $\mathcal{I} \subset \mathcal{N} = \{1, \cdots, N\}$, a block column matrix $Z = \text{col}_{i=1}^N(Z_i)$ is said to have the *ℓ_1-recovery property with an intensity* $\beta_\mathcal{I} > 0$, if

$$-\sum_{i \in \mathcal{I}} \|Z_i\hat{r}\|_1 + \sum_{i \in \mathcal{N} \setminus \mathcal{I}} \|Z_i\hat{r}\|_1 \leq -\beta_\mathcal{I} \tag{10}$$

for all $\hat{r} \in S^n = \{r \in \mathbb{R}^n \mid \|r\|_2 = 1\}$.

In the following proposition, we find an upper bound on the distance between the state $x(t)$ and the minimizer $x^* \in \mathcal{M}(t)$ under the ℓ_1-recovery property of Z for the index set U, where U is the index set of uncompromised agents defined in (4). Its proof can be found in Appendix A.

Proposition 1: For the index set U in (4), suppose that the matrix Z has the ℓ_1-recovery property with an intensity $\beta_U > 0$. Then, we have, for each t,

$$\|x^* - x(t)\|_2 \leq \frac{2}{\beta_U} \sum_{i \in U} \|\epsilon_i(t)\|_1, \quad \forall x^* \in \mathcal{M}(t).$$

As it can be seen in (6), the estimation error $\epsilon_i(t)$ converges to zero for all $i \in U$. From this and Proposition 1, $\|x^* - x(t)\|_2$ converges to zero, if the matrix Z has the ℓ_1-recovery property for U. Therefore, the state $x(t)$ can be obtained with arbitrary precision by solving the problem (9) after a sufficiently large time interval.

Remark 1: The condition of Z having the ℓ_1-recovery property for U is stronger than the observability of the pair $(A, \text{col}_{i \in U}(C_i))$. Specifically, from (10) with $\mathcal{I} = U$, we have $-\sum_{i \in \mathcal{U}} \|Z_i\hat{r}\|_1 < 0$ for all $\hat{r} \in S^n$. This implies that $\text{col}_{i \in U}(Z_i)$ has full column rank. In other words, $(A, \text{col}_{i \in U}(C_i))$ is observable.

Remark 2: According to Proposition 1, when $\epsilon_i(t) \equiv 0$ for all $i \in U$, the ℓ_1-recovery property for $\mathcal{I} = U$ is sufficient for the exact state recovery. Indeed, there exists a well-known necessary and sufficient condition for exact state recovery, the *null-space property* [16] relative to $\mathcal{N} \setminus \mathcal{I}$, given by

$$-\sum_{i \in \mathcal{I}} \|Z_i r\|_1 + \sum_{i \in \mathcal{N} \setminus \mathcal{I}} \|Z_i r\|_1 < 0, \quad \forall r \in \mathbb{R}^n \setminus \{0\}.$$

Notably, the null-space property relative to $\mathcal{N} \setminus \mathcal{I}$ is equivalent to the ℓ_1-recovery property for $\mathcal{I}$ with some $\beta_\mathcal{I} > 0$.

Motivated by above observations, we propose the distributed resilient observer for each agent $i \in \mathcal{N}$, given by

$$\dot{\hat{x}}_i = A\hat{x}_i - kZ_i^T \text{sign}(Z_i\hat{x}_i - \hat{z}_i) + k\gamma \sum_{j \in \mathcal{N}_i} (\hat{x}_j - \hat{x}_i) \tag{11}$$

with $\|\hat{x}_i(0)\|_2 \leq M$, where $\hat{x}_i \in \mathbb{R}^n$ is the state, $\hat{z}_i \in \mathbb{R}^{d_i}$ is the state of the partial observer (5), and the parameters k and γ will be designed later. The first term is the copy of system (2). The second term serves the injection of estimation error, inspired by the gradient descent flow for the local cost function $\|Z_i\hat{x}_i(t) - \hat{z}_i(t)\|_1$ of the problem (9). Last term is the coupling that enforces synchronization of all the $\hat{x}_i(t)$'s.

The intuition for the form (11) is rooted in the blended dynamics theory [17]. Let us check the blended dynamics of (11), which comprises the average of all the individual vector fields as follows:

$$\dot{s} = As - \frac{k}{N} Z^T \text{sign}(Zs - \hat{z}) \quad \in \mathbb{R}^n \tag{12}$$

where the gradient flow $-Z^T\text{sign}(Zs - \hat{z})$ for the problem (9) is inflated k/N times. Note that the system (12) is not globally stable in general, and thus, careful analysis on the convergence of the system (11) will be addressed.

As stated in Assumption 1, the agents lack knowledge what sensor measurements are being attacked. Consequently, it is challenging to design the observer's parameters k and γ because information about U is not available. Nevertheless, to achieve resilient estimation, we assume the followings.

Assumption 2: Let $\mathcal{U}$ be the collection of all index sets $U' \subset \mathcal{N}$ satisfying $|U'| \geq N-q$. For all $U' \in \mathcal{U}$, the matrix Z has the ℓ_1-recovery property with the intensity $\beta_{U'} > 0$.

Note that the cardinality of the collection $\mathcal{U}$ is finite. Thus, from Assumption 2, one can find $\beta > 0$ satisfying $\beta_{U'} \geq \beta$ for all $U' \in \mathcal{U}$. Moreover, since $U \in \mathcal{U}$ from Assumption 1,

$$-\sum_{i\in U}\|Z_i\hat{r}\|_1 + \sum_{i\in\mathcal{N}\setminus U}\|Z_i\hat{r}\|_1 \leq -\beta, \quad \forall \hat{r}\in S^n \tag{13}$$

which will be utilized for designing the parameters k and γ.

C. Main Result

The main result of this paper is as follows:

Theorem 1: Under Assumptions 1, 2, and the graph $\mathcal{G}$ being undirected and connected, all the agents run the distributed observer of (5) and (11). For arbitrary $\eta > 0$ and $M > 0$, there exist k^* and γ^* such that, if $k > k^*$ and $\gamma > \gamma^*$, then the solution $\hat{x}_i(t)$, $i \in \mathcal{N}$, of (11) satisfies

$$\|x(t) - \hat{x}_i(t)\|_2 \leq \max\big\{c - \rho\cdot t,\, \eta\big\}, \quad \forall t \geq 0 \tag{14}$$

where $\rho := \frac{\beta}{2N}(k-k^*)$ and

$$c := e^{\|A\|_2 T_\epsilon}\cdot\max\Big\{2M, \frac{2\sqrt{n}N}{\beta}(B_W + B_\epsilon)\Big\} + B_W + \rho T_\epsilon.$$

Here, β is given in (13), $B_W \leq \max\{2M\sqrt{N}, \eta/2\}$, and both B_ϵ and T_ϵ are defined in (7) with $\sigma_\epsilon = \frac{\beta\eta}{16\sqrt{n}N}$.

Proof: Define an error variable $e_i(t) := x(t) - \hat{x}_i(t)$, and consider the following coordination change

$$\begin{bmatrix}\bar{e}(t)\\ \tilde{e}(t)\end{bmatrix} = \begin{bmatrix}\frac{1}{N}(1_N^T\otimes I_n)\\ R^T\otimes I_n\end{bmatrix}\cdot \mathrm{col}_{i=1}^N\big(e_i(t)\big) \tag{15}$$

with its inverse $e_i(t) = \bar{e}(t) + (r_i\otimes I_n)\tilde{e}(t)$, where $r_i \in \mathbb{R}^{1\times(N-1)}$ is the ith row of the matrix R defined in (37). Then, the time derivatives of both $\bar{e}(t)$ and $\tilde{e}(t)$ are

$$\dot{\bar{e}} = A\bar{e} - \frac{k}{N}\sum_{i=1}^N Z_i^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i) \tag{16a}$$

$$\begin{aligned}\dot{\tilde{e}} &= (I_{N-1}\otimes A)\tilde{e} - k\gamma(\Lambda\otimes I_n)\tilde{e}\\ &\quad - k(R^T\otimes I_n)\cdot\mathrm{col}_{i=1}^N\Big(Z_i^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i)\Big)\end{aligned} \tag{16b}$$

where Λ is given in (37) and the vector $\bar{\epsilon}_i(t) := Z_i(r_i\otimes I_n)\tilde{e}(t) + \epsilon_i(t) \in \mathbb{R}^{d_i}$ satisfies

$$\begin{aligned}\|\bar{\epsilon}_i(t)\|_1 &\leq \sqrt{d_i}\|Z_i(r_i\otimes I_n)\tilde{e}(t) + \epsilon_i(t)\|_2\\ &\leq \sqrt{n}\big(\|\tilde{e}(t)\|_2 + \|\epsilon_i(t)\|_2\big), \quad \forall i\in\mathcal{N}.\end{aligned} \tag{17}$$

Meanwhile, the relation $e_i(t) = \bar{e}(t) + (r_i\otimes I_n)\tilde{e}(t)$ yields

$$\|e_i(t)\|_2 \leq \|\bar{e}(t)\|_2 + \|\tilde{e}(t)\|_2. \tag{18}$$

Therefore, to establish the inequality (14), we analyze how upper bounds of $\|\bar{e}(t)\|_2$ and $\|\tilde{e}(t)\|_2$ are determined from the parameters k and γ.

Define $W(t) := \|\tilde{e}(t)\|_2$ whose time derivative along (16) with $W > 0$ is

$$\begin{aligned}\dot{W} &= \frac{\tilde{e}^T}{\|\tilde{e}\|_2}\dot{\tilde{e}} = \frac{\tilde{e}^T}{\|\tilde{e}\|_2}(I_{N-1}\otimes A)\tilde{e} - k\gamma\frac{\tilde{e}^T}{\|\tilde{e}\|_2}(\Lambda\otimes I_n)\tilde{e}\\ &\quad - k\frac{\tilde{e}^T}{\|\tilde{e}\|_2}(R^T\otimes I_n)\cdot\mathrm{col}_{i=1}^N\Big(Z_i^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i)\Big)\\ &\leq -(k\gamma\lambda_2 - \|A\|_2)W + k\sqrt{nN}\end{aligned}$$

where $\lambda_2 > 0$ is given in (36). Thus, for all $\gamma > \gamma^*(k) := \frac{\|A\|_2}{k\lambda_2} + \frac{2\sqrt{nN}}{\lambda_2\sigma_W}$ with some $\sigma_W > 0$, we have

$$\dot{W} < -\frac{2k\sqrt{nN}}{\sigma_W}\Big(W - \frac{\sigma_W}{2}\Big).$$

Hence, from $\|e_i(0)\|_2 \leq 2M$ for all $i \in \mathcal{N}$, we obtain $\bar{W}_0 := 2M\sqrt{N}$ such that $W(0) \leq \bar{W}_0$, and hence

$$W(t) \leq B_W := \max\Big\{\bar{W}_0, \sigma_W\Big\}, \quad \forall t \geq 0, \tag{19a}$$

$$W(t) \leq \sigma_W,\ \forall t \geq T_W(k) := \frac{\sigma_W}{2k\sqrt{nN}}\ln\Big(\frac{2B_W - \sigma_W}{\sigma_W}\Big). \tag{19b}$$

Next, we define $V(t) = \|\bar{e}(t)\|_2$ whose time derivative along (16) with $V > 0$ is

$$\dot{V} = \frac{\bar{e}^T A\bar{e}}{\|\bar{e}\|_2} + \frac{k}{N\|\bar{e}\|_2}\Big(-\sum_{i\in\mathcal{N}}(Z_i\bar{e})^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i)\Big). \tag{20}$$

Note that, by using (13), (17), and (38), we have

$$\begin{aligned}-\sum_{i\in\mathcal{N}}(Z_i\bar{e})^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i) &\leq -\sum_{i\in U}(Z_i\bar{e})^T\mathrm{sign}(Z_i\bar{e}+\bar{\epsilon}_i) + \sum_{i\in\mathcal{N}\setminus U}\|Z_i\bar{e}\|_1\\ &\leq 2\sum_{i\in U}\|\bar{\epsilon}_i\|_1 - \sum_{i\in U}\|Z_i\bar{e}\|_1 + \sum_{i\in\mathcal{N}\setminus U}\|Z_i\bar{e}\|_1\\ &\leq 2\sqrt{n}\sum_{i\in U}(\|\tilde{e}\|_2 + \|\epsilon_i\|_2) - \beta\|\bar{e}\|_2.\end{aligned} \tag{21}$$

Applying $\sum_{i\in U}(\|\tilde{e}\|_2 + \|\epsilon_i\|_2) \leq N(\|\tilde{e}\|_2 + \max_{i\in U}\|\epsilon_i\|_2)$ into (21), the inequality (20) becomes

$$\dot{V} \leq \|A\|_2 V + \frac{2\sqrt{n}k}{V}\Big(\|\tilde{e}\|_2 + \max_{i\in U}\|\epsilon_i\|_2\Big) - \frac{k\beta}{N}. \tag{22}$$

Meanwhile, from $\|e_i(0)\|_2 \leq 2M$ and $\|\epsilon_i(0)\|_2 \leq 2M$ for all $i \in U$, one can find $B_\epsilon > 0$ satisfying (6), and we define $\bar{V}_0 = 2M$ so that $V(0) \leq \bar{V}_0$. Then, in order to make the ultimate bounds on both $W(t)$ and $V(t)$ less than or equal to $\eta/2$, we choose $\sigma_\epsilon := \frac{\beta\eta}{16\sqrt{n}N}$ and $\sigma_W := \min\{\frac{\beta\eta}{16\sqrt{n}N}, \frac{\eta}{2}\}$ of (7b) and (19b), respectively. Moreover, using the definition of $T_W(\cdot)$ in (19b), we define $k_1^* := T_W(T_\epsilon)$ such that $T_W(k_1^*) = T_\epsilon$. Then, the relation $k > k_1^*$ yields $T_W(k) \leq T_\epsilon$,

$$\|\tilde{e}(t)\|_2 + \max_{i\in U}\|\epsilon_i(t)\|_2 \leq B_W + B_\epsilon,\ \forall t \geq 0, \tag{23a}$$

$$\|\tilde{e}(t)\|_2 + \max_{i\in U}\|\epsilon_i(t)\|_2 \leq \sigma_W + \sigma_\epsilon \leq \frac{\beta\eta}{8\sqrt{nN}}, \quad \forall t \geq T_\epsilon. \tag{23b}$$

Therefore, by combining (22) with (23a), $\dot{V} \leq \|A\|_2 V$ for $V \geq \bar{V}_1 := \frac{2\sqrt{n}N}{\beta}\big(B_W + B_\epsilon\big)$, which yields

$$V(t) \leq e^{\|A\|_2 t}\max\{\bar{V}_0, \bar{V}_1\}, \quad \forall t \geq 0. \tag{24}$$

Moreover, the combination of (22) and (23b) yields

$$\dot{V} \leq \|A\|_2 V + \frac{k\beta\eta}{4NV} - \frac{k\beta}{N}, \quad \forall t \geq T_\epsilon. \tag{25}$$

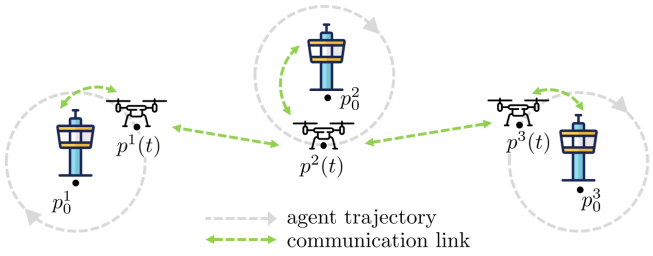

Fig. 1. Agents are patrolling around monitoring towers.

Thus, with $\bar{V}_2 := e^{\|A\|_2 T_\epsilon} \cdot \max\{\bar{V}_0, \bar{V}_1\}$, we choose k satisfying $k > k^* := \max\left\{\frac{2N}{\beta}\|A\|_2 \bar{V}_2, k_1^*\right\}$ so that $k > k_1^*$ (which is required for obtaining (23)) and

$$\|A\|_2 V + \frac{k\beta\eta}{4NV} - \frac{k\beta}{N} < -\frac{\beta}{2N}(k-k^*) \text{ when } \frac{\eta}{2} \le V \le \bar{V}_2.$$

By combining this and (24), we obtain

$$V(t) \le \max\left\{\bar{V}_2 - \frac{\beta(k-k^*)}{2N}\cdot(t-T_\epsilon),\ \frac{\eta}{2}\right\},\ \forall t \ge T_\epsilon. \quad (26)$$

Now, we are ready to prove (14). From (19a) and (24), the inequality (18) becomes, for all $0 \le t \le T_\epsilon$ and $i \in \mathcal{N}$,

$$\|e_i(t)\|_2 \le \bar{V}_2 + B_W. \quad (27)$$

Similarly, from (19b) and (26) with $k > k^*$ and $\gamma > \gamma^*(k^*)$,

$$\|e_i(t)\|_2 \le \max\left\{\bar{V}_2 + \frac{\eta}{2} - \frac{\beta(k-k^*)}{2N}\cdot(t-T_\epsilon), \eta\right\}, \forall t \ge T_\epsilon. \quad (28)$$

From the definitions of $\bar{V}_0$, $\bar{V}_1$, and $\bar{V}_2$, one can find an upper bound of $\bar{V}_2$, and hence, both (27) and (28) imply (14). ■

IV. Simulation Results

We consider $N = 3$ pairs of agents and monitoring towers, where each agent i is patrolling a circular path centered at the position $p_0^i \in \mathbb{R}^2$ of its pair tower and can communicate with neighboring agents and its pair tower, as shown in Fig. 1. We aim to design distributed observers so that each agent estimates all the positions $\{p^i(t) \in \mathbb{R}^2\}_{i=1}^N$ of agents, even when some sensors are compromised by attackers.

The motion of agents are described by the system (2), where $x(t) = \text{col}_{i=1}^N\left(p^i(t) - p_0^i\right) \in \mathbb{R}^{2N}$ is the state and

$$A = I_N \otimes \begin{bmatrix} 0 & \omega \\ -\omega & 0 \end{bmatrix}$$

with some $\omega \in \mathbb{R}$. We assume that all the positions of monitoring towers, $\{p_0^i\}_{i=1}^N$, are known to every agent. Hence, the goal is achieved when each agent obtains the state $x(t)$. Each agent i can measure the relative positions $\bar{y}_i(t) = \text{col}_{j\in\mathcal{N}_i}(p^j(t) - p^i(t))$ of neighbor agents. Then, by combining $\bar{y}_i(t)$ and $\{p_0^i\}_{i=1}^N$, the agent i also obtains

$$y_i(t) = \frac{1}{\sqrt{2}}\text{col}_{j\in\mathcal{N}_i}\Big(\left(p^j(t) - p_0^j\right) - \left(p^i(t) - p_0^i\right)\Big) + a_i(t) \in \mathbb{R}^{2|\mathcal{N}_i|}.$$

Here, $a_i(t)$ is the attack signal. Meanwhile, by labeling ith monitoring tower as $i+N$, we denote its measurement

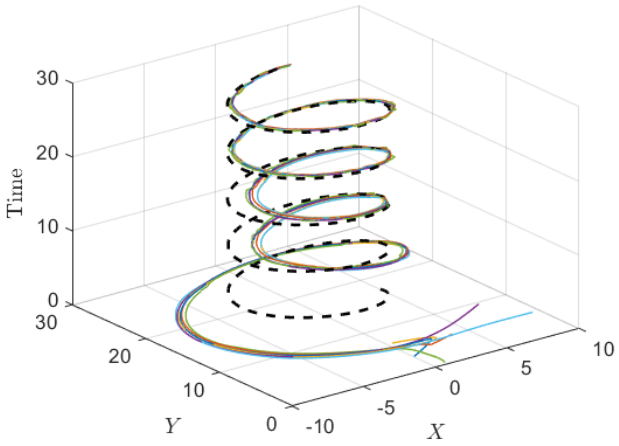

Fig. 2. The position $p^2(t)$ of agent 2 is drawn as black dashed curve, and all the estimation $\hat{p}_i^2(t)$ of each agent i are drawn as colored solid curves.

$y_i(t) = (p^i(t) - p_0^i) + a_i(t)$, for $i = N+1, \cdots, 2N$. Then, the measurement matrix C_i is determined as

$$C_i = \begin{cases} \frac{1}{\sqrt{2}}\cdot\text{col}_{j\in\mathcal{N}_i}\left((v_j^T - v_i^T)\otimes I_2\right), & i = 1, \cdots, N \\ v_{i-N}^T \otimes I_2, & i = N+1, \cdots, 2N \end{cases}$$

where $v_i \in \mathbb{R}^N$ is the standard basis vector, whose ith element is one and the others are zero. Under this setting, the matrix Z_i for (5) can be chosen as C_i for all $i = 1, \cdots, 2N$.

Note that the scalar decomposability is not satisfied in this case[4], and thus, the method in [15] cannot be applied. Suppose that attackers can compromise at most $q = 1$ of $2N$ measurements. Then, Assumption 2 is satisfied, since $Z = \text{col}_{i=1}^{2N}(Z_i)$ has the ℓ_1-recovery property with an intensity $\beta_{U'} \ge \sqrt{2} - 1$ for all $U' \subset \{1, \cdots, 2N\}$ satisfying $|U'| \ge 2N - 1$.

Each agent i runs the observers (5) and (11), where the estimation variable $\hat{x}_i(t)$ is utilized for estimating $p^j(t)$, i.e., $\hat{p}_i^j(t) := (v_j^T \otimes I_2)\hat{x}_i(t) + p_0^j$. Simulation results are in Fig. 2, where the plant parameter is $w = 1$, the observer parameters of (11) are $k = \gamma = 3$, and the attack signal $a_i(t)$ is $10^4 \cdot 1_4$ for $i = 2$ and 0 otherwise. Particularly, we added measurement noise of magnitude 1 when measuring all $y_i(t)$'s. The result shows attack-resilient property of our estimation scheme.

V. Conclusion

We propose a resilient estimation scheme that employs a standard partial observer (5) and a distributed observer (11), which estimates the plant state by solving an ℓ_1-minimization problem in a distributed manner. To ensure accurate state estimation, we specify the conditions on the parameters k and γ, which is available when the matrix Z for the partial observers satisfies the ℓ_1-recovery property. The proposed scheme is scalable, since the amount of computation and communication required at each agent are consistent regardless of the network size or the number of attacks.

[4]If any eigenvalue of A has more than one Jordan block, scalar decomposability is not satisfied generally. For more details, see [15, Appendix B].

REFERENCES

[1] L. Wang and A. S. Morse, "A distributed observer for a time-invariant linear system," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2123–2130, 2017.

[2] A. Mitra and S. Sundaram, "Distributed observers for LTI systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 11, pp. 3689–3704, 2018.

[3] T. Kim, C. Lee, and H. Shim, "Completely decentralized design of distributed observer for linear systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 11, pp. 4664–4678, 2019.

[4] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proceedings of the 2005 International Symposium on Information Processing in Sensor Networks*, 2005, pp. 63–70.

[5] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *Critical Infrastructure Protection*, vol. 253, no. 4, pp. 73–82, 2007.

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security and Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[7] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[8] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Reviews in Control*, vol. 47, pp. 394–411, 2019.

[9] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the 2010 Workshop on Secure Control Systems*, 2010, pp. 1–6.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[11] Y. Mao and P. Tabuada, "Decentralized secure state-tracking in multi-agent systems," *IEEE Transactions on Automatic Control*, early access, 2022, doi:10.1109/TAC.2022.3200951.

[12] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2016.

[13] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Review*, vol. 43, no. 1, pp. 129–159, 2001.

[14] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.

[15] J. G. Lee, J. Kim, and H. Shim, "Fully distributed resilient state estimation based on distributed median solver," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3935–3942, 2020.

[16] A. Cohen, W. Dahmen, and R. DeVore, "Compressed sensing and best k-term approximation," *American Mathematical Society*, vol. 22, no. 1, pp. 211–231, 2009.

[17] J. Kim, J. Yang, H. Shim, J.-S. Kim, and J. H. Seo, "Robustness of synchronization of heterogeneous agents by strong coupling and a large number of agents," *IEEE Transactions on Automatic Control*, vol. 61, no. 10, pp. 3096–3102, 2015.

[18] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

APPENDIX

A. Proof of Proposition 1

We prove this by contradiction. Assume that there exists a minimizer $x^* \in \mathcal{M}(t)$ of (9) satisfying $\bar{\phi} := \|x^* - x(t)\|_2 > \frac{2}{\beta_U}\sum_{i\in U}\|\epsilon_i(t)\|_1$. We claim that there exists $\check{x}$ such that

$$\check{x} \neq x^* \quad \text{and} \quad \|Zx^* - \hat{z}(t)\|_1 - \|Z\check{x} - \hat{z}(t)\|_1 > 0. \quad (29)$$

Note the claim contradicts to the hypothesis of x^* being the minimizer of (9). Define $\check{x} := x(t) + \phi\hat{v}$, where

$$\hat{v} := \frac{x^* - x(t)}{\|x^* - x(t)\|_2}, \quad \phi := \frac{\bar{\phi} + \frac{2}{\beta_U}\sum_{i\in U}\|\epsilon_i(t)\|_1}{2}.$$

Then, we consider the following relation:

$$\|Zx^* - \hat{z}(t)\|_1 - \|Z\check{x} - \hat{z}(t)\|_1 = \|\bar{\phi}Z\hat{v} - \epsilon(t)\|_1 - \|\phi Z\hat{v} - \epsilon(t)\|_1$$
$$= \sum_{i\in\mathcal{N}}\Big(\|\bar{\phi}Z_i\hat{v} - \epsilon_i(t)\|_1 - \|\phi Z_i\hat{v} - \epsilon_i(t)\|_1\Big). \quad (30)$$

For $i \in \mathcal{N}\setminus U$, from the triangular inequality, we have

$$\|\bar{\phi}Z_i\hat{v} - \epsilon_i(t)\|_1 - \|\phi Z_i\hat{v} - \epsilon_i(t)\|_1 \geq (\bar{\phi} - \phi)\big(-\|Z_i\hat{v}\|_1\big). \quad (31)$$

For $i \in U$, define $g_i(\tau) := \|\tau Z_i\hat{v} - \epsilon_i(t)\|_1$ with $\tau \in \mathbb{R}$, then

$$\|\bar{\phi}Z_i\hat{v} - \epsilon_i(t)\|_1 - \|\phi Z_i\hat{v} - \epsilon_i(t)\|_1 = g_i(\bar{\phi}) - g_i(\phi). \quad (32)$$

Since the function g_i is piecewise linear, it follows that

$$g_i(\bar{\phi}) - g_i(\phi) = \int_{\phi}^{\bar{\phi}} (Z_i\hat{v})^T \text{sign}(\tau Z_i\hat{v} - \epsilon_i(t))\, d\tau. \quad (33)$$

From (38) of Lemma 2, it can be obtained that for $\tau > 0$,

$$(Z_i\hat{v})^T\text{sign}(\tau Z_i\hat{v} - \epsilon_i(t)) \geq \Big(\|Z_i\hat{v}\|_1 - \frac{2}{\tau}\|\epsilon_i(t)\|_1\Big).$$

By applying this and (33) into (32), we have, for all $i \in U$,

$$\|\bar{\phi}Z_i\hat{v} - \epsilon_i(t)\|_1 - \|\phi Z_i\hat{v} - \epsilon_i(t)\|_1 \geq \int_{\phi}^{\bar{\phi}} \|Z_i\hat{v}\|_1 - \frac{2}{\tau}\|\epsilon_i(t)\|_1\, d\tau$$
$$\geq \int_{\phi}^{\bar{\phi}} \|Z_i\hat{v}\|_1 - \frac{2}{\phi}\|\epsilon_i(t)\|_1\, d\tau = (\bar{\phi} - \phi)\Big(\|Z_i\hat{v}\|_1 - \frac{2}{\phi}\|\epsilon_i(t)\|_1\Big). \quad (34)$$

Now, let us show (29). From (31) and (34), (30) becomes

$$\|Zx^* - \hat{z}(t)\|_1 - \|Z\check{x} - \hat{z}(t)\|_1$$
$$\geq (\bar{\phi} - \phi)\Big(-\sum_{i\in\mathcal{N}\setminus U}\|Z_i\hat{v}\|_1 + \sum_{i\in U}\Big(\|Z_i\hat{v}\|_1 - \frac{2}{\phi}\|\epsilon_i(t)\|_1\Big)\Big)$$
$$\geq (\bar{\phi} - \phi)\Big(\beta_U - \frac{2}{\phi}\sum_{i\in U}\|\epsilon_i(t)\|_1\Big) \quad (35)$$

where (35) follows from (10) with $\mathcal{I} = U$. Since $\frac{2}{\beta_U}\sum_{i\in U}\|\epsilon_i(t)\|_1 < \phi < \bar{\phi}$ from the definitions of $\bar{\phi}$ and ϕ, the right-hand side of (35) is greater than zero, which shows the claim (29) and completes the proof.

B. Technical lemmas

Lemma 1 ([18]): For the undirected and connected graph $\mathcal{G}$, all the eigenvalues of the Laplacian matrix $\mathcal{L}$ of $\mathcal{G}$ are non-negative real numbers, and there is only one zero eigenvalue. Namely, the eigenvalues can be sorted as

$$0 = \lambda_1 < \lambda_2 \leq \lambda_3 \cdots \leq \lambda_N. \quad (36)$$

Moreover, there exists a matrix $R \in \mathbb{R}^{N\times(N-1)}$ such that

$$1_N^T R, \quad R^T R = I_{N-1}, \quad R^T\mathcal{L}R = \Lambda \quad (37)$$

where $\Lambda := \text{diag}_{i=2}^{N}(\lambda_i) \in \mathbb{R}^{(N-1)\times(N-1)}$.

Lemma 2: For vectors $a, b \in \mathbb{R}^n$, it holds that

$$-a^T\text{sign}(a+b) \leq 2\|b\|_1 - \|a\|_1. \quad (38)$$

Proof: This lemma can be proved as follows:

$$-a^T\text{sign}(a+b)$$
$$= -a^T\text{sign}(a+b) + (a+b)^T\text{sign}(a+b) - (a+b)^T\text{sign}(a+b)$$
$$= b^T\text{sign}(a+b) - \|a+b\|_1$$
$$\leq \|b\|_1 - \|a+b\|_1 = \|b\|_1 - \|a+b\|_1 + \|a\|_1 - \|a\|_1$$
$$\leq 2\|b\|_1 - \|a\|_1. \qquad \blacksquare$$