On the Impact of Trusted Nodes in Resilient Distributed State Estimation of LTI Systems

Aritra Mitra, Waseem Abbas and Shreyas Sundaram

***Abstract*— We address the problem of distributed state estimation of a linear dynamical process in an attack-prone environment. A network of sensors, some of which can be compromised by adversaries, aim to estimate the state of the process. In this context, we investigate the impact of making a small subset of the nodes immune to attacks, or "trusted". Given a set of trusted nodes, we identify separate necessary and sufficient conditions for resilient distributed state estimation. We use such conditions to illustrate how even a small trusted set can achieve a desired degree of robustness (where the robustness metric is specific to the problem under consideration) that could otherwise only be achieved via additional measurement and communication-link augmentation. We then establish that, unfortunately, the problem of selecting trusted nodes is NP-hard. Finally, we develop an attack-resilient, provably-correct distributed state estimation algorithm that appropriately leverages the presence of the trusted nodes.**

I. Introduction

Consider a linear time-invariant dynamical process

$$\mathbf{x}[k+1] = \mathbf{A}\mathbf{x}[k], \tag{1}$$

where $k \in \mathbb{N}$ is the discrete-time index, $\mathbf{x}[k] \in \mathbb{R}^n$ is the state vector and $\mathbf{A} \in \mathbb{R}^{n\times n}$ is the system matrix. A network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ of N nodes monitor the state of this system. The i-th node receives a measurement of the state, given by

$$\mathbf{y}_i[k] = \mathbf{C}_i\mathbf{x}[k], \tag{2}$$

where $\mathbf{y}_i[k] \in \mathbb{R}^{r_i}$ and $\mathbf{C}_i \in \mathbb{R}^{r_i\times n}$. We define $\mathbf{C} \triangleq \begin{bmatrix}\mathbf{C}_1^T & \cdots & \mathbf{C}_N^T\end{bmatrix}^T$ and $\mathbf{y}[k] \triangleq \begin{bmatrix}\mathbf{y}_1^T[k] & \cdots & \mathbf{y}_N^T[k]\end{bmatrix}^T$. As a basic necessary condition for state estimation, we assume that the pair $(\mathbf{A}, \mathbf{C})$ is detectable. However, for any given $i \in \mathcal{V}$, the pair $(\mathbf{A}, \mathbf{C}_i)$ may not be detectable. In the classical distributed state estimation problem [1]–[5], the goal of each node is to track the state of the system based on its own measurement set, and the information received from its neighbors in $\mathcal{G}$. The presence of nodes that can act maliciously adds an extra layer of complexity to this otherwise well-explored problem. To solve the distributed state estimation problem in the presence of worst-case adversarial behavior, the authors in [6] developed an attack-resilient filtering algorithm and identified sufficient conditions on the system and network that guaranteed applicability of their approach. The analysis in [6] indicates the need for a certain degree of redundancy in both the measurement structure of the nodes, and the communication graph, so as to counter the effect of adversarial nodes. As an alternative to the conventional approach of increasing robustness through redundancy, the authors in [7] explored the concept of device hardening. Specifically, in the context of consensus dynamics, the authors established that even if a relatively small set of carefully chosen nodes, called *trusted nodes*, are made immune to attacks, then the overall network can still exhibit the same structural robustness as that of a highly connected, dense network.

In light of these recent developments, we seek to understand the impact of making certain nodes *trusted* in the context of collaboratively estimating the state of a dynamical system. Specifically, we ask the following questions.

- Can introducing trusted nodes into a sparse network alleviate the redundancy requirements needed for resilient distributed state estimation?
- How should one choose a set of trusted nodes that provide the network with certain redundancy requirements?

In posing the above questions, our main motivation is to gain insights regarding the design of an attack-resilient, robust sensor network. The multitude of applications of such sensor networks, and the growing need for designing secure networked control systems, justifies the relevance of the questions asked in this paper. In this context, our **contributions** are as follows. First, given a set of trusted sensor nodes, we identify separate necessary and sufficient conditions for the problem under consideration, in Sections III and IV, respectively. For each of the robustness measures identified in the respective sections ("critical-index" in Section III and "strong r-robustness" in Section IV), we demonstrate the utility of making certain nodes trusted. Roughly speaking, we do so by showing that the absence of even a single trusted node needs to be compensated by augmenting the network with several additional measurement and communication resources. Second, in Section V, we establish that the problem of finding the smallest set of trusted nodes to achieve a certain degree of strong-robustness is NP-hard. Finally, in Section VI, we develop a resilient distributed state estimation algorithm that leverages the presence of trusted nodes, and provably guarantees asymptotic state reconstruction for all non-compromised nodes, if the conditions identified in Section IV are met.

II. Notation, Terminology and Problem Setup

Notation: A directed graph is denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, \cdots, N\}$ is the set of nodes and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the edges. An edge from node j to node i, denoted by (j, i), implies that node j can transmit information to node

This work was supported in part by a grant from Sandia National Laboratories, and by NSF grant CMMI-1635014. Aritra Mitra and Shreyas Sundaram are with the School of Electrical and Computer Engineering at Purdue University. Email: {mitra14, sundara2}@purdue.edu. Waseem Abbas is with the Electrical Engineering Department at the Information Technology University, Lahore, Pakistan. Email: w.abbas@itu.edu.pk.

i. The neighborhood (or in-neighborhood) of the i-th node is defined as $\mathcal{N}_i \triangleq \{j \,|\, (j,i) \in \mathcal{E}\}$. A node j is said to be an out-neighbor of node i if $(i,j) \in \mathcal{E}$. By an *induced* subgraph of $\mathcal{G}$ obtained by removing certain nodes $\mathcal{C} \subset \mathcal{V}$, we refer to the subgraph that has $\mathcal{V} \setminus \mathcal{C}$ as its node set, and contains only those edges of $\mathcal{E}$ with both end points in $\mathcal{V} \setminus \mathcal{C}$. The notation $|\mathcal{V}|$ is used to denote the cardinality of a set $\mathcal{V}$. The set of all eigenvalues (or modes) of a matrix $\mathbf{A}$ is denoted by $sp(\mathbf{A}) = \{\lambda \in \mathbb{C} \,|\, det(\mathbf{A} - \lambda \mathbf{I}) = 0\}$, and the set of all unstable eigenvalues by $\Lambda_U(\mathbf{A}) = \{\lambda \in sp(\mathbf{A}) \,||\lambda| \geq 1\}$. For a set $\mathcal{J} = \{m_1, \cdots, m_{|\mathcal{J}|}\} \subseteq \{1, \cdots, N\}$, and a matrix $\mathbf{C} = \begin{bmatrix}\mathbf{C}_1^T & \cdots & \mathbf{C}_N^T\end{bmatrix}^T$, we define $\mathbf{C}_{\mathcal{J}} \triangleq \begin{bmatrix}\mathbf{C}_{m_1}^T & \cdots & \mathbf{C}_{m_{|\mathcal{J}|}}^T\end{bmatrix}^T$. The identity matrix of dimension r is denoted $\mathbf{I}_r$, and $\mathbb{N}_+$ is used to refer to the set of all positive integers. The terms 'communication graph' and 'network' are used interchangeably.

Adversary Model: We consider a subset $\mathcal{A} \subset \mathcal{V}$ of the nodes in the network to be adversarial. The adversaries possess complete knowledge of the network topology, the system dynamics and the algorithm employed by the non-adversarial nodes. The adversarial nodes can act collaboratively, and can even transmit differing state estimates to different neighbors at the same instant of time, based on the Byzantine fault model [8]. To characterize the threat model in terms of the number of adversaries in the network, we will use the following definitions from [9].

Definition 1. *(f-**total set**) A set $\mathcal{C} \subset \mathcal{V}$ is f-total if it contains at most f nodes in the network, i.e., $|\mathcal{C}| \leq f$.* □

Definition 2. *(f-**local set**) A set $\mathcal{C} \subset \mathcal{V}$ is f-local if it contains at most f nodes in the neighborhood of the other nodes, i.e., $|\mathcal{N}_i \cap \mathcal{C}| \leq f$, $\forall i \in \mathcal{V} \setminus \mathcal{C}$.* □

Definition 3. *(f-**local and f-total adversarial models**) A set $\mathcal{A}$ of adversarial nodes is f-locally bounded (resp., f-totally bounded) if $\mathcal{A}$ is an f-local (resp., f-total) set.* □

We will primarily deal with an f-local Byzantine adversary model so as to account for a large number of adversaries in the network. The non-adversarial nodes will be referred to as regular nodes and be represented by the set $\mathcal{R} = \mathcal{V} \setminus \mathcal{A}$. Finally, note that the actual number and identities of the adversarial nodes are not known to the regular nodes; only the upper bound f (on the total number of adversarial nodes in the neighborhood) is known.

Trusted Node Model: We assume that a subset $\mathcal{T} \subseteq \mathcal{V}$ of nodes cannot be compromised by adversaries, i.e., $\mathcal{T} \cap \mathcal{A} = \emptyset$. Furthermore, we assume that each node is aware of the identities of its trusted neighbors.

With $\hat{\mathbf{x}}_i[k]$ representing the estimate of $\mathbf{x}[k]$ (the state of system (1)) maintained by node i, our objective in this paper will be to study the impact of the trusted nodes in solving the following problem.

Problem 1. ***(Resilient Distributed State Estimation Problem)** Given an LTI system (1), a linear measurement model (2), and a time-invariant directed communication graph $\mathcal{G}$, design a set of state estimate update and information exchange rules such that $\lim_{k\to\infty} ||\hat{\mathbf{x}}_i[k] - \mathbf{x}[k]|| = 0$, $\forall i \in \mathcal{R}$, regardless of the actions of any f-locally bounded set of Byzantine adversaries.*

III. Necessary Conditions for Resilient Distributed State Estimation with Trusted Nodes

Given a network $\mathcal{G}$ with a trusted node set $\mathcal{T}$, the main objective of this section is to identify conditions that are necessary for Problem 1 to be solvable via *any* distributed algorithm. In the process, we will define an appropriate robustness metric that blends both system-theoretic and graph-theoretic requirements. Finally, we will demonstrate how the defined robustness metric can be significantly improved by making a small fraction of the nodes trusted. To this end, we require the following definitions.

Definition 4. *(**Critical Set**) A set of nodes $\mathcal{F} \subset \mathcal{V}$ is said to be a critical set if the pair $(\mathbf{A}, \mathbf{C}_{\mathcal{V}\setminus\mathcal{F}})$ is not detectable.* □

Definition 5. *(**Minimal Critical Set**) A set $\mathcal{F} \subset \mathcal{V}$ is said to be a minimal critical set if $\mathcal{F}$ is a critical set and no subset of $\mathcal{F}$ is a critical set.* □

Let $\mathcal{M} = \{\mathcal{F}_1, \cdots, \mathcal{F}_m\}$ denote the set of all minimal critical sets where $m = |\mathcal{M}|$. With each set $\mathcal{F}_i \in \mathcal{M}$, we associate a virtual node s_i as follows. Directed edges are added from s_i to each node in $\mathcal{F}_i$ and the resulting network is denoted by $\mathcal{G}_i^{'} = (\mathcal{V} \cup s_i, \mathcal{E} \cup \mathcal{E}_i)$, where $\mathcal{E}_i$ represents the set of edges from s_i to $\mathcal{F}_i$.

Definition 6. *(f-**local pair and f-total pair cuts with trusted nodes w.r.t.** s_i) Consider a minimal critical set $\mathcal{F}_i \in \mathcal{M}$. A set $\mathcal{H} \subset \mathcal{V}$ is called a cut with trusted nodes w.r.t. s_i if $\mathcal{H} \cap \mathcal{T} = \emptyset$, and removal of $\mathcal{H}$ from $\mathcal{G}_i^{'}$ results in an induced subgraph of $\mathcal{G}_i^{'}$ whose node set can be partitioned into two non-empty sets $\mathcal{X}$ and $\mathcal{Y}$ with $s_i \in \mathcal{X}$, and no directed paths from $\mathcal{X}$ to $\mathcal{Y}$ in the induced subgraph. A cut $\mathcal{H}$ with trusted nodes w.r.t. s_i is called an f-local pair cut (resp., f-total pair cut) with trusted nodes w.r.t. s_i if it can be partitioned as $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2$ such that both $\mathcal{H}_1$ and $\mathcal{H}_2$ are f-local (resp., f-total) in $\mathcal{G}$.* □

The following result identifies a fundamental limitation for f-total (and hence f-local) adversarial models.

Theorem 1. *Suppose there exists an f-total pair cut with trusted nodes w.r.t. s_i in $\mathcal{G}_i^{'}$ for some minimal critical set $\mathcal{F}_i \in \mathcal{M}$. Then, it is impossible for any algorithm to solve the variant of Problem 1 corresponding to an f-total Byzantine adversary model.* □

Proof. The proof proceeds via contradiction. Suppose there exists an f-total pair cut $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2$ with trusted nodes w.r.t. s_i for some minimal critical set $\mathcal{F}_i \in \mathcal{M}$. Based on the definition of $\mathcal{H}$, it is easy to verify that the pair $(\mathbf{A}, \mathbf{C}_{\mathcal{Y}})$ is not detectable since $\mathcal{Y}$ contains no elements of $\mathcal{F}_i$. Thus, there exists an initial condition $\mathbf{x}[0] = \boldsymbol{\eta}$ that causes the measurement set $\mathbf{y}_{\mathcal{Y}}[k]$ corresponding to $\mathcal{Y}$ to be identically zero for all time, while the state $\mathbf{x}[k]$ remains bounded away from zero. The idea of the proof is to appropriately construct an attack such that the nodes in $\mathcal{Y}$ cannot distinguish between

the zero initial condition, and the initial condition $\boldsymbol{\eta}$. This can be achieved by noting that each of the sets $\mathcal{H}_1$ and $\mathcal{H}_2$ are f-total and can act as valid adversarial sets since $\mathcal{H} \cap \mathcal{T} = \emptyset$. The specific details of such an attack are similar to those in [10, Theorem 1], and are hence omitted here. □

The above result yields the following corollary, providing an upper-bound on the total number of adversaries that can be tolerated in a given network with trusted nodes.

Corollary 1. *Let $\kappa_{\mathcal{T}}$ denote the smallest positive integer such that there exists a $\kappa_{\mathcal{T}}$-total pair cut with trusted nodes w.r.t. s_i, for some $\mathcal{F}_i \in \mathcal{M}$. Then, the total number of adversaries f must satisfy $f < \kappa_{\mathcal{T}}$ for Problem 1 to have a solution.* □

Unlike the traditional notion of graph-connectivity, the parameter $\kappa_{\mathcal{T}}$ defined in the above corollary depends on both the measurement structure of the nodes and the topology of the communication graph. For the problem under consideration, $\kappa_{\mathcal{T}}$ can be viewed as a measure of robustness of a given system and network against a Byzantine adversary model. We henceforth refer to $\kappa_{\mathcal{T}}$ as the *critical-index with trusted nodes* of a given system and network. In what follows, we demonstrate that a network with no trusted nodes needs to be augmented with several additional measurement resources and communication links so as to achieve a critical-index equivalent to that of a network with a small number of trusted nodes. To illustrate this equivalence in a simple manner, we consider a scalar unstable system $x[k+1] = \lambda x[k]$, and an associated communication graph $\mathcal{G}$ with a trusted node set $\mathcal{T}$. Based on this system and network model, we construct another model *without* trusted nodes as follows.

- **Connectivity Augmentation**: The new communication graph, denoted $\bar{\mathcal{G}} = (\mathcal{V}, \bar{\mathcal{E}})$ has the same node set as $\mathcal{G}$, but an augmented edge set $\bar{\mathcal{E}}$. Specifically, given any pair of non-adjacent nodes $i, j \in \mathcal{G}$, if there exists a trusted node that is an out-neighbor of i and an in-neighbor of j, or if there exists a directed path from i to j consisting entirely of trusted nodes, then we add an edge (i, j) between such nodes in $\bar{\mathcal{G}}$.
- **Measurement Augmentation**: Let τ be a trusted node in $\mathcal{G}$ with non-zero measurements, i.e., $\mathbf{C}_\tau \neq 0$. Let i be an out-neighbor of τ such that $\mathbf{C}_i = 0$. Then, node i in $\bar{\mathcal{G}}$ is allocated the same measurements as node τ, i.e., $\mathbf{C}_i = \mathbf{C}_\tau$ in $\bar{\mathcal{G}}$.

We have the following result.

Proposition 1. *Consider a scalar unstable system $x[k+1] = \lambda x[k]$, a measurement model of the form (2), and a network $\mathcal{G}$ with a trusted node set $\mathcal{T}$. Let $\kappa_{\mathcal{T}}$ denote the critical-index with trusted nodes of this system and network. Let κ indicate the critical-index of the system and network $\bar{\mathcal{G}}$ obtained from $\mathcal{G}$ via connectivity augmentation and measurement augmentation. Then, $\kappa = \kappa_{\mathcal{T}}$.* □

Proof. Let the set of nodes in $\mathcal{G}$ (resp., $\bar{\mathcal{G}}$) that have non-zero measurements of the state be denoted by $\mathcal{F}$ (resp., $\bar{\mathcal{F}}$). It is easy to see that for the scalar system under consideration, $\mathcal{F}$ and $\bar{\mathcal{F}}$ represent the only minimal critical sets in $\mathcal{G}$ and $\bar{\mathcal{G}}$, respectively. To proceed, we construct the graph $\mathcal{G}'$ (resp., $\bar{\mathcal{G}}'$) from $\mathcal{G}$ (resp., $\bar{\mathcal{G}}$) by associating a virtual node s (resp., $\bar{s}$) with the minimal critical set $\mathcal{F}$ (resp., $\bar{\mathcal{F}}$) and adding directed edges from s (resp., $\bar{s}$) to $\mathcal{F}$ (resp., $\bar{\mathcal{F}}$). We now consider two separate cases.

Case 1: We first consider the case when all trusted nodes in $\mathcal{G}$ have no measurements, i.e., $\mathbf{C}_{\mathcal{T}} = \mathbf{0}$. For this case, we will establish that connectivity augmentation alone suffices to achieve the equivalence stated in the proposition. To see this, first observe that $\bar{\mathcal{F}} = \mathcal{F}$. It is easy to verify that a $k_{\mathcal{T}}$-total pair cut with trusted nodes w.r.t. s in $\mathcal{G}'$ is also a $k_{\mathcal{T}}$-total pair cut w.r.t. $\bar{s}$ in $\bar{\mathcal{G}}'$. Thus, $\kappa \leq \kappa_{\mathcal{T}}$. Conversely, if there exists a $(\kappa_{\mathcal{T}} - 1)$-total pair cut w.r.t. $\bar{s}$ in $\bar{\mathcal{G}}'$, then one can construct a $(\kappa_{\mathcal{T}} - 1)$-total pair cut with trusted nodes w.r.t. s in $\mathcal{G}'$. Thus, $\kappa_{\mathcal{T}} \leq \kappa$. We conclude that $\kappa = \kappa_{\mathcal{T}}$.

Case 2: Consider the case when there exists at least one trusted node $\tau \in \mathcal{G}$ with non-zero measurements. In this case, the only minimal critical set in $\bar{\mathcal{G}}$ is given by $\bar{\mathcal{F}} = \{\mathcal{F}\} \cup \{\bigcup_{\tau \in \mathcal{F} \cap \mathcal{T}} \mathcal{N}_\tau^+\}$, where $\mathcal{N}_\tau^+$ represents the out-neighborhood of the trusted node τ. The last statement follows directly from the measurement augmentation step. Suppose there exists a $k_{\mathcal{T}}$-total pair cut $\mathcal{H}$ with trusted nodes w.r.t. s in $\mathcal{G}'$. Let this cut generate the sets $\mathcal{X}$ and $\mathcal{Y}$ as defined in Definition 6. We observe that $\mathcal{Y}$ cannot contain an out-neighbor of any trusted node belonging to $\mathcal{F}$. Based on this observation, it is clear that $\mathcal{H}$ acts as a $k_{\mathcal{T}}$-total pair cut w.r.t. $\bar{s}$ in the graph $\bar{\mathcal{G}}'$, generating the same two sets $\mathcal{X}$ and $\mathcal{Y}$. Thus, $\kappa \leq \kappa_{\mathcal{T}}$. The converse statement can be established just as in Case 1, leading to the conclusion that $\kappa = \kappa_{\mathcal{T}}$. □

Remark 1. *The above result substantiates our argument that the replacement of a single trusted node requires allocating additional measurement and communication resources to the network so as to preserve the level of robustness (captured by the critical-index) against adversarial attacks. Furthermore, the result also identifies how such resources should be deployed throughout the network so as to achieve the desired equivalence. While this specific result pertaining to a scalar dynamical system serves to highlight the utility of trusted sensor nodes, identifying the exact nature of the measurement augmentation step for more general systems requires further analysis. We reserve this as future work.* □

IV. Sufficient Conditions for Resilient Distributed State Estimation with Trusted Nodes

In the previous section, we explored the benefit of incorporating trusted nodes in the context of meeting certain necessary conditions for Problem 1. The focus of this section will be to further highlight the impact of trusted nodes by investigating sufficient conditions for Problem 1. There are two main goals of this section. First, we shall identify topological conditions that allow Problem 1 to be solved based on an estimation strategy discussed later in Section VI. Second, in line with the underlying theme of this paper, we shall demonstrate how such topological conditions relax those obtained in [6], where no trusted nodes are considered. To this end, we require the following definition from [7].

Definition 7. *(r-**reachable set with trusted nodes**) For a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a trusted node set $\mathcal{T}$, a set $\mathcal{C} \subset \mathcal{V}$, and an integer $r \in \mathbb{N}_+$, $\mathcal{C}$ is an r-reachable set with trusted nodes if there exists an $i \in \mathcal{C}$ such that either $|\mathcal{N}_i \setminus \mathcal{C}| \geq r$, or $|\{\mathcal{N}_i \setminus \mathcal{C}\} \cap \mathcal{T}| > 0$.* □

In other words, a set $\mathcal{C}$ is r-reachable with trusted nodes if it contains at least one node i that either has at least r neighbors outside $\mathcal{C}$ or has at least one trusted neighbor outside $\mathcal{C}$. We now define the key topological property required for solving Problem 1 given a trusted node set $\mathcal{T}$.

Definition 8. *(**strongly r-robust graph with trusted nodes w.r.t. $\mathcal{S}$**) Given a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a trusted node set $\mathcal{T}$, a set $\mathcal{S} \subseteq \mathcal{V}$, and an integer $r \in \mathbb{N}_+$, $\mathcal{G}$ is strongly r-robust with trusted nodes w.r.t. $\mathcal{S}$, if for any non-empty subset $\mathcal{C} \subseteq \mathcal{V} \setminus \mathcal{S}$, $\mathcal{C}$ is r-reachable with trusted nodes.* □

In the absence of any trusted nodes, the conventional notions of r-reachability [11] and strong r-robustness w.r.t. a set $\mathcal{S}$ [6] can be recovered from Definitions 7 and 8 by setting $\mathcal{T} = \emptyset$ in the respective definitions. To proceed, we recall the notion of source nodes introduced in [6].

Definition 9. *(**Source nodes**) For each $\lambda_j \in \Lambda_U(\mathbf{A})$, let the set $\mathcal{S}_j$ be defined as follows:*

$$\mathcal{S}_j \triangleq \{i \in \mathcal{V} | rank \begin{bmatrix} \mathbf{A} - \lambda_j \mathbf{I}_n \\ \mathbf{C}_i \end{bmatrix} = n\}. \tag{3}$$

Then, $\mathcal{S}_j$ will be called the set of source nodes for λ_j. □

Let $\Omega_U(\mathbf{A}) \subseteq \Lambda_U(\mathbf{A})$ contain the set of eigenvalues of $\mathbf{A}$ for which $\mathcal{V} \setminus \mathcal{S}_j$ is non-empty. Given an unstable mode $\lambda_j \in \Omega_U(\mathbf{A})$, estimation of the state corresponding to λ_j requires a secure medium of information flow from the corresponding source nodes $\mathcal{S}_j$ to the non-source nodes $\mathcal{V} \setminus \mathcal{S}_j$. To achieve this objective, the concept of a Mode Estimation Directed Acyclic Graph (MEDAG) was introduced in [6]. In what follows, we modify the definition of a MEDAG to account for the presence of trusted nodes.

Definition 10. *(**Mode Estimation Directed Acyclic Graph (MEDAG) with trusted nodes**) Consider an eigenvalue $\lambda_j \in \Omega_U(\mathbf{A})$. Suppose there exists a spanning subgraph $\mathcal{G}_j = (\mathcal{V}, \mathcal{E}_j)$ of $\mathcal{G}$ with the following properties for all f-local sets $\mathcal{A}$ with $\mathcal{A} \cap \mathcal{T} = \emptyset$, and $\mathcal{R} = \mathcal{V} \setminus \mathcal{A}$.*

(i) *If $i \in \{\mathcal{V} \setminus \mathcal{S}_j\} \cap \mathcal{R}$, then either $|\mathcal{N}_i^{(j)}| \geq (2f+1)$ or $|\mathcal{N}_i^{(j)} \cap \mathcal{T}| > 0$, where $\mathcal{N}_i^{(j)} = \{l | (l, i) \in \mathcal{E}_j\}$ represents the neighborhood of node i in $\mathcal{G}_j$.*

(ii) *There exists a partition of $\mathcal{R}$ into the sets $\{\mathcal{L}_0^{(j)}, \cdots, \mathcal{L}_{T_j}^{(j)}\}$, where $T_j \in \mathbb{N}_+$, $\mathcal{L}_0^{(j)} = \mathcal{S}_j \cap \mathcal{R}$, and if $i \in \mathcal{L}_q^{(j)}$ (where $1 \leq q \leq T_j$), then $\mathcal{N}_i^{(j)} \cap \mathcal{R} \subseteq \bigcup_{r=0}^{q-1} \mathcal{L}_r^{(j)}$. Furthermore, $\mathcal{N}_i^{(j)} = \emptyset, \forall i \in \mathcal{L}_0^{(j)}$.*

Then, we call $\mathcal{G}_j$ a Mode Estimation Directed Acyclic Graph (MEDAG) with trusted nodes for $\lambda_j \in \Omega_U(\mathbf{A})$. □

Construction of a MEDAG with trusted nodes: We briefly discuss an algorithm that can be used to construct a MEDAG with trusted nodes (conditions for the existence of such a MEDAG will be provided below). Suppose we are given a trusted set $\mathcal{T}$. For each $\lambda_j \in \Omega_U(\mathbf{A})$, our objective is to construct the subgraph $\mathcal{G}_j$ defined in Definition 10, and in the process identify the sets $\mathcal{N}_i^{(j)}, \forall i \in \mathcal{V}$. With the sets $\mathcal{N}_i^{(j)}$ in hand, one can implement the resilient distributed state estimation algorithm to be described later in Section VI. The MEDAG construction algorithm requires each node i to maintain a counter $c_i(j)$ and a list of indices $\mathcal{N}_i^{(j)}$ for each $\lambda_j \in \Omega_U(\mathbf{A})$. These parameters are initialized with $c_i(j) = 0$ and $\mathcal{N}_i^{(j)} = \emptyset$, for each $i \in \mathcal{V}$. Subsequently, the algorithm proceeds in rounds where in the first round each node in $\mathcal{S}_j$ broadcasts the message "1" to its out-going neighbors, sets $c_i(j) = 1$, maintains $\mathcal{N}_i^{(j)} = \emptyset$ for all future rounds, and goes to sleep. When a node $i \in \mathcal{V} \setminus \mathcal{S}_j$ either receives "1" from at least $(2f+1)$ distinct neighbors or from a single trusted neighbor, it sets $c_i(j) = 1$, appends the labels of each of the neighbors from which it received "1" to $\mathcal{N}_i^{(j)}$, broadcasts the message "1" to its out-going neighbors, and goes to sleep. The MEDAG construction algorithm "*terminates for λ_j*", if there exists $T_j \in \mathbb{N}_+$ such that $c_i(j) = 1 \ \forall i \in \mathcal{V}$, for all rounds following round T_j. As pointed out earlier, the **objective** of the algorithm is to return a set of sets $\{\mathcal{N}_i^{(j)}\}$, where $\lambda_j \in \Omega_U(\mathbf{A})$, and $i \in \mathcal{V}$.

Theorem 2. *For each $\lambda_j \in \Omega_U(\mathbf{A})$, $\mathcal{G}$ contains a subgraph $\mathcal{G}_j$ satisfying all the properties of a MEDAG with trusted nodes for λ_j, if and only if $\mathcal{G}$ is strongly $(2f+1)$-robust with trusted nodes w.r.t. $\mathcal{S}_j$.* □

Proof. "$\Longleftarrow$" Let $\mathcal{A}$ be any f-local set such that $\mathcal{A} \cap \mathcal{T} = \emptyset$. Set $\mathcal{R} = \mathcal{V} \setminus \mathcal{A}$. To prove sufficiency, we shall construct a subgraph $\mathcal{G}_j$ satisfying the two properties of a MEDAG with trusted nodes in Definition 10. Let $\mathcal{L}_0^{(j)} = \mathcal{S}_j \cap \mathcal{R}$. We can prune the incoming edges of each node in $\mathcal{L}_0^{(j)}$ so that $\mathcal{N}_i^{(j)} = \emptyset$ for each $i \in \mathcal{L}_0^{(j)}$. Consider the set $\mathcal{C} = \{\mathcal{V} \setminus \mathcal{L}_0^{(j)}\} \cap \mathcal{R}$. If such a set is empty, then we are done. If not, let $\mathcal{L}_1^{(j)}$ be the set of all nodes in $\mathcal{C}$ that either have at least $(2f+1)$ neighbors outside $\mathcal{C}$ or have at least one trusted neighbor outside $\mathcal{C}$. Since $\mathcal{G}$ is strongly r-robust with $\mathcal{T}$ w.r.t. $\mathcal{S}_j$, $\mathcal{L}_1^{(j)} \neq \emptyset$. For each node $i \in \mathcal{L}_1^{(j)}$, let $\mathcal{N}_i^{(j)}$ denote the neighbors of node i outside the set $\mathcal{C}$. It follows from the above construction that either $|\mathcal{N}_i^{(j)}| \geq (2f+1)$ or $|\mathcal{N}_i^{(j)} \cap \mathcal{T}| > 0$. Noting that $\mathcal{T} \subseteq \mathcal{R}$, we infer that $\mathcal{N}_i^{(j)} \cap \mathcal{R} \subseteq \mathcal{L}_0^{(j)}$. We can continue the same construction procedure to cover $\mathcal{R}$. Specifically, having constructed the sets $\mathcal{L}_0^{(j)}$ to $\mathcal{L}_{q-1}^{(j)}$, if $\mathcal{C} = \{\mathcal{V} \setminus \bigcup_{r=0}^{q-1} \mathcal{L}_r^{(j)}\} \cap \mathcal{R}$ is non-empty, then we can construct a non-empty set $\mathcal{L}_q^{(j)}$ using the same arguments employed for constructing $\mathcal{L}_1^{(j)}$. Since the set $\mathcal{R}$ is finite, the construction process described above will eventually terminate with $T_j \leq N$, yielding a subgraph $\mathcal{G}_j$ satisfying Definition 10.

"$\Longrightarrow$" We prove necessity via contradiction. Given some $\lambda_j \in \Omega_U(\mathbf{A})$, let there exist a MEDAG $\mathcal{G}_j$ with trusted nodes satisfying Definition 10. Suppose $\mathcal{G}$ is not strongly $(2f+1)$-robust with trusted nodes w.r.t. $\mathcal{S}_j$. Thus, there exists a non-empty set $\mathcal{C} \subseteq \mathcal{V} \setminus \mathcal{S}_j$ that is not $(2f+1)$-reachable with trusted nodes. Consider the trivial f-local set $\mathcal{A} = \emptyset$ that satisfies $\mathcal{A} \cap \mathcal{T} = \emptyset$. The subgraph $\mathcal{G}_j$ must contain a partition

of $\mathcal{R} = \mathcal{V} \backslash \mathcal{A} = \mathcal{V}$ into levels that satisfy the second property of a MEDAG with trusted nodes in Definition 10. With this in mind, let $\mathcal{C}$ be partitioned as $\mathcal{C} = \bigcup_{r=1}^{q} \mathcal{F}_r$, where $\mathcal{F}_r = \mathcal{C} \cap \mathcal{L}_{n_r}^{(j)}$ for some set of integers $\{n_1, \cdots, n_q | 1 \leq n_i \leq T_j \, \forall i \in \{1, \cdots, q\}\}$. Here, $\{\mathcal{L}_{n_r}^{(j)}\}_{r=1}^{q}$ represents a subset of the levels that partition $\mathcal{R}$ in the MEDAG $\mathcal{G}_j$ with trusted nodes. Without loss of generality, let $n_1 < n_2 < \cdots < n_q$. Then, from the definition of a MEDAG with trusted nodes, it follows that for any $i \in \mathcal{F}_{n_1}$, $\mathcal{N}_i^{(j)}$ contains elements from only $\mathcal{V} \backslash \mathcal{C}$. As $\mathcal{C}$ is not $(2f+1)$-reachable with trusted nodes, $|\mathcal{N}_i^{(j)}| < (2f+1)$ and $|\mathcal{N}_i^{(j)} \cap \mathcal{T}| = \emptyset$, thereby violating the first property of a MEDAG with trusted nodes. This leads to the desired contradiction and completes the proof. □

Remark 2. *There are two main implications of the above theorem. First, based on the proof of sufficiency, we observe that if $\mathcal{G}$ is strongly $(2f+1)$-robust with trusted nodes w.r.t. $\mathcal{S}_j$, then the MEDAG construction algorithm (described earlier in this section) is guaranteed to terminate for λ_j. Second, a major take-away point is the fact that checking the existence of a MEDAG with trusted nodes can be completed in polynomial-time. This follows from the observation that for any $\lambda_j \in \Omega_U(\mathbf{A})$, $T_j \leq N$, implying that the MEDAG construction algorithm will take at most N rounds/iterations to terminate for each such λ_j.* □

In Section VI, we shall establish that the existence of a MEDAG with trusted nodes for each $\lambda_j \in \Omega_U(\mathbf{A})$, allows every regular node to employ a resilient consensus based filtering algorithm to estimate the state $\mathbf{x}[k]$ asymptotically. Thus, Theorem 2 characterizes certain topological conditions that allow Problem 1 to be solved. In the absence of any trusted nodes, the approach developed in [6] requires the graph $\mathcal{G}$ to be strongly $(2f+1)$-robust w.r.t. $\mathcal{S}_j, \forall \lambda_j \in \Omega_U(\mathbf{A})$. Our immediate aim will be to demonstrate that the conditions obtained in this paper relax those obtained in [6]. To this end, consider the following result.

Theorem 3. *Let $\mathcal{G}$ be strongly r-robust with trusted nodes w.r.t. $\mathcal{S}_j, \forall \lambda_j \in \Omega_U(\mathbf{A})$. Let $\bar{\mathcal{G}}$ be a graph obtained from $\mathcal{G}$ by replacing each trusted node $\tau \in \mathcal{T}$ with a set of r nodes such that each of the r nodes have (i) the same measurements as τ, and (ii) the same in- and out-neighborhood as τ in $\mathcal{G}$. Then, $\bar{\mathcal{G}}$ is strongly r-robust w.r.t. $\mathcal{S}_j, \forall \lambda_j \in \Omega_U(\mathbf{A})$.* □

A proof of the above theorem is available in [12].

V. Complexity of Selecting Trusted Nodes

In this section, we establish that the problem of finding a set of trusted nodes to achieve a certain degree of strong r-robustness is computationally hard. To prove this result, we first formally define the problem under consideration.

Definition 11. ***(Trusted Strong Robustness Augmentation Problem (TSRAP))*** *Given a system model (1), a measurement model (2), a communication graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, and positive integers r, t, does there exist a set of trusted nodes $\mathcal{T}$ of cardinality t such that $\mathcal{G}$ is strongly r-robust with trusted nodes w.r.t. $\mathcal{S}_j, \forall \lambda_j \in \Omega_U(\mathbf{A})$?* □

To characterize the complexity of TSRAP, we will provide a reduction from the NP-hard Set Cover Problem (SCP), defined as follows.

Definition 12. ***(Set Cover Problem (SCP))*** *Given a collection of elements $\mathcal{U} = \{1, \cdots, p\}$, a set of subsets $\mathcal{F} = \{\mathcal{F}_1, \cdots, \mathcal{F}_m\}$ of $\mathcal{U}$, and a positive integer t, do there exist t subsets in $\mathcal{F}$ whose union is $\mathcal{U}$?* □

Theorem 4. *The TSRAP problem is NP-hard.* □

Proof. Given an instance of SCP, we first construct an instance of TSRAP as follows. We consider a scalar unstable dynamical system $x[k+1] = \lambda x[k]$, and construct an associated communication graph $\mathcal{G}$ with node set $\mathcal{V} = \{u_1, \cdots, u_p, f_1, \cdots, f_m\}$ of cardinality $p+m$. Each node u_i corresponds to an element of $\mathcal{U}$, and each node f_j corresponds to the subset $\mathcal{F}_j \in \mathcal{F}$. If $u_i \in \mathcal{F}_j$, then a directed edge is added from node f_j to node u_i. Each node $f_j \in \mathcal{F}$ is allocated a non-zero measurement of the state $x[k]$. The cardinality of the trusted set $\mathcal{T}$ is taken to be t, and the desired level of strong robustness is given by $r = |\mathcal{F}|$. Clearly, the above TSRAP instance can be constructed in polynomial-time. We now argue that the answer to any given instance of SCP is "yes" if and only if the answer to the constructed instance of TSRAP is "yes".

Suppose the answer to the SCP instance is "yes". Thus, there exists a set of t subsets of $\mathcal{F}$ whose union is $\mathcal{U}$. Without loss of generality, let these subsets be $\{\mathcal{F}_1, \cdots, \mathcal{F}_t\}$. Let the set of trusted nodes $\mathcal{T}$ be $\{f_1, \cdots, f_t\}$. We first observe that the set of source nodes $\mathcal{S}$ (the set of nodes that can detect λ) of $\mathcal{G}$ is precisely the set $\mathcal{F}$. Thus, $\mathcal{T} \subset \mathcal{S}$. To establish that $\mathcal{G}$ is strongly r-robust with trusted nodes w.r.t. $\mathcal{S}$, we pick a non-empty subset $\mathcal{C} \subseteq \mathcal{V} \setminus \mathcal{S} = \mathcal{U}$. Since every node $u_i \in \mathcal{U}$ has a neighbor in $\mathcal{T} \subset \mathcal{S}$, every non-empty subset $\mathcal{C} \subseteq \mathcal{U}$ is r-reachable with trusted nodes. Thus, the answer to the constructed instance of TSRAP is "yes".

To show the converse, we proceed via contraposition. Suppose the answer to the SCP instance is "no". In other words, there does not exist any t subsets of $\mathcal{F}$ that cover $\mathcal{U}$. Consider any set of trusted nodes $\mathcal{T}$ of cardinality t. Let $\mathcal{M} = \mathcal{F} \cap \mathcal{T}$. We first consider the case when $\mathcal{M}$ is non-empty. In this case, there exists at least one node $u_i \in \mathcal{U}$ that has neighbors only in $\mathcal{F} \setminus \mathcal{M}$. Noting that the source set $\mathcal{S} = \mathcal{F}$, we consider the non-empty set $\mathcal{C} = \{u_i\}$ contained in $\mathcal{V} \setminus \mathcal{S} = \mathcal{U}$. Since $r = |\mathcal{F}|$, it follows that u_i neither has a trusted neighbor nor has at least r neighbors. Thus, $\mathcal{C}$ is not r-reachable with trusted nodes. For analyzing the case when $\mathcal{M}$ is empty, we observe that there must exist at least one node $u_i \in \mathcal{U}$ such that $\mathcal{N}_i \subset \mathcal{F}$. It then follows that $\mathcal{C} = \{u_i\}$ is not $|\mathcal{F}|$-reachable with trusted nodes. Consequently, $\mathcal{G}$ is not strongly r-robust with trusted nodes w.r.t. $\mathcal{S}$, regardless of the way t trusted nodes are picked in $\mathcal{G}$. In other words, the answer to the constructed TSRAP instance is "no". This completes the proof. □

A polynomial-time greedy heuristic that finds a (sub-optimal) set of trusted nodes can be found in [12].

VI. Resilient Distributed State Estimation with Trusted Nodes

In this section, we develop an algorithm that leverages the presence of a trusted node set $\mathcal{T}$ to solve Problem 1. For simplicity of notation, we make the following assumption.

Assumption 1. $\mathbf{A}$ *has real, distinct eigenvalues.*

Although the above assumption might seem restrictive, the results that we derive subsequently can be generalized to account for system matrices with arbitrary spectrum using a more detailed technical analysis [10]. Since any $\mathbf{A}$ satisfying Assumption 1 can be diagonalized via an appropriate similarity transformation, we assume without loss of generality that $\mathbf{A}$ is already in diagonal form. Specifically, $\mathbf{A} = diag(\lambda_1, \cdots, \lambda_n)$, where $sp(\mathbf{A}) = \{\lambda_1, \cdots, \lambda_n\}$. Let the component of the state vector $\mathbf{x}[k]$ corresponding to eigenvalue λ_j be denoted by $x^{(j)}[k]$. Building on the general idea developed in [6], for each $\lambda_j \in \Omega_U(\mathbf{A})$, the source nodes $\mathcal{S}_j$ and the non-source nodes $\mathcal{V} \setminus \mathcal{S}_j$ employ separate update rules for estimating $x^{(j)}[k]$. In particular, the source nodes maintain local[1] Luenberger observers for estimating $x^{(j)}[k]$, while the non-source nodes rely on a resilient consensus based protocol to achieve this task. For any node i, let the set of eigenvalues it can detect be denoted by $\mathcal{O}_i$, and let $\mathcal{UO}_i = sp(\mathbf{A}) \setminus \mathcal{O}_i$. Then, the following result from [6] states that node i can estimate the locally detectable portion of $\mathbf{x}[k]$ *without* interacting with its neighbors.

Lemma 1. *Suppose Assumption 1 holds. Then, for each regular node $i \in \mathcal{R}$ and each $\lambda_j \in \mathcal{O}_i$, a local Luenberger observer can be constructed that ensures that $\lim_{k\to\infty} |\hat{x}_i^{(j)}[k] - x^{(j)}[k]| = 0$, where $\hat{x}_i^{(j)}[k]$ denotes the estimate of $x^{(j)}[k]$ maintained by node i.* □

We now develop a filtering algorithm that accounts for the presence of trusted nodes, and allows each regular node to estimate the locally undetectable portion of the dynamics, despite potential adversaries in its neighborhood.

For each $\lambda_j \in \mathcal{UO}_i$, $i \in \mathcal{R}$ updates $\hat{x}_i^{(j)}[k]$ as follows.

1) At each time-step k, it collects the estimates of $x^{(j)}[k]$ received from *only* those neighbors that belong to $\mathcal{N}_i^{(j)} \subseteq \mathcal{N}_i$. (Recall that $\mathcal{N}_i^{(j)}$ represents the neighbor-set of node i in the MEDAG with trusted nodes $\mathcal{G}_j$).
2) If $\mathcal{N}_i^{(j)} \cap \mathcal{T} \neq \emptyset$, then $\hat{x}_i^{(j)}[k]$ is updated as follows:

$$\hat{x}_i^{(j)}[k+1] = \lambda_j \sum_{l \in \mathcal{N}_i^{(j)} \cap \mathcal{T}} \bar{w}_{il}^{(j)} \hat{x}_l^{(j)}[k], \qquad (4)$$

where the weights are non-negative and chosen to satisfy $\sum_{l \in \mathcal{N}_i^{(j)} \cap \mathcal{T}} \bar{w}_{il}^{(j)} = 1$.

3) If $\mathcal{N}_i^{(j)} \cap \mathcal{T} = \emptyset$, then node i ranks the estimates of $x^{(j)}[k]$ received from nodes in $\mathcal{N}_i^{(j)}$ from highest to lowest. It then removes the highest and lowest f estimates (i.e., removes $2f$ estimates in all), and updates $\hat{x}_i^{(j)}[k]$ based on the following rule:

$$\hat{x}_i^{(j)}[k+1] = \lambda_j \sum_{l \in \mathcal{M}_i^{(j)}[k]} w_{il}^{(j)}[k] \hat{x}_l^{(j)}[k], \qquad (5)$$

where $\mathcal{M}_i^{(j)}[k] \subset \mathcal{N}_i^{(j)} (\subseteq \mathcal{N}_i)$ is the set of nodes from which node i chooses to accept estimates of $x^{(j)}[k]$ at time-step k, after removing the f highest and f lowest estimates from $\mathcal{N}_i^{(j)}$. The weights are nonnegative and chosen to satisfy $\sum_{l \in \mathcal{M}_i^{(j)}[k]} w_{il}^{(j)}[k] = 1$.

We refer to the above algorithm as the Local-Filtering based Resilient Estimation algorithm with Trusted nodes (LFRE-T). We have the following result, with a proof in [12].

Theorem 5. *Consider the system (1) and measurement model (2). Let $\mathcal{T} \subset \mathcal{V}$ denote the set of trusted nodes in $\mathcal{G}$. Let the communication graph $\mathcal{G}$ be strongly $(2f+1)$-robust with trusted nodes w.r.t. $\mathcal{S}_j, \forall \lambda_j \in \Omega_U(\mathbf{A})$. Then, the proposed LFRE-T algorithm solves Problem 1.* □

VII. Conclusion

We studied the problem of incorporating trusted nodes to relax the redundancy requirements for resilient distributed state estimation. Given a set of trusted nodes, we identified separate necessary and sufficient conditions for the problem under consideration, and demonstrated the benefit of trusted nodes through such conditions. We studied the complexity of selecting a trusted node set, and proposed an attack-resilient distributed state estimation algorithm adapted to account for the presence of trusted nodes. As future work, we plan to further explore the trade-offs and complexities associated with designing robust sensor networks with trusted nodes.

[1] Here, by 'local' we imply that such observers can be constructed and run without any information from neighbors.

References

[1] U. A. Khan and A. Jadbabaie, "On the stability and optimality of distributed Kalman filters with finite-time data fusion," in *Proc. of the American Control Conference*, 2011, pp. 3405–3410.

[2] I. Matei and J. S. Baras, "Consensus-based linear distributed filtering," *Automatica*, vol. 48, no. 8, pp. 1776–1782, 2012.

[3] S. Park and N. C. Martins, "Design of distributed LTI observers for state omniscience," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 561–576, 2017.

[4] 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, 2018.

[5] A. Mitra and S. Sundaram, "Distributed observers for LTI systems," *IEEE Transactions on Automatic Control*, 2018.

[6] ——, "Secure distributed observers for a class of linear time invariant systems in the presence of Byzantine adversaries," in *55th IEEE Conference on Decision and Control*, 2016, pp. 2709–2714.

[7] W. Abbas, A. Laszka, and X. Koutsoukos, "Improving network connectivity and robustness using trusted nodes with application to resilient consensus," *IEEE Transactions on Control of Network Systems*, 2017.

[8] D. Dolev, N. A. Lynch, S. S. Pinter, E. W. Stark, and W. E. Weihl, "Reaching approximate agreement in the presence of faults," *Journal of the ACM (JACM)*, vol. 33, no. 3, pp. 499–516, 1986.

[9] A. Pelc and D. Peleg, "Broadcasting with locally bounded Byzantine faults," *Information Processing Letters*, vol. 93, pp. 109–115, 2005.

[10] A. Mitra and S. Sundaram, "Resilient distributed state estimation for LTI systems," *arXiv preprint arXiv:1802.09651*, 2018.

[11] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[12] A. Mitra, W. Abbas, and S. Sundaram, "On the impact of trusted nodes in resilient distributed state estimation of LTI systems," *arXiv*, 2018.