MIT Open Access Articles

Cooperative distributed state estimation: resilient topologies against smart spoofers

Cooperative distributed state estimation: resilient topologies against smart spoofers

Cooperative distributed state estimation: Resilient topologies against smart spoofers

Mostafa Safi[1*]

[1*] Amirkabir University of Technology, Hafez, Tehran, 424, Iran.

Corresponding author(s). E-mail(s): halebi@aut.ac.ir;

Abstract

A network of observers is considered, where through asynchronous (with bounded delay) communications, they cooperatively estimate the states of a linear time-invariant (LTI) system. In such a setting, a new type of adversary might affect the observation process by impersonating the identity of the regular node, which is a violation of communication authenticity. These adversaries also inherit the capabilities of Byzantine nodes, making them more powerful threats called *smart spoofers*. We show how asynchronous networks are vulnerable to smart spoofing attack. In the estimation scheme considered in this paper, information flows from the sets of source nodes, which can detect a portion of the state variables each, to the other follower nodes. The regular nodes, to avoid being misguided by the threats, distributively filter the extreme values received from the nodes in their neighborhood. Topological conditions based on strong robustness are proposed to guarantee the convergence. Two simulation scenarios are provided to verify the results.

Keywords: Cyber-physical systems, smart spoofing, distributed resilient algorithm, secure observers

1 Introduction

Security is becoming an increasingly important concern for the stability and safety of networked control systems. Nowadays, in large-scale control systems, communication channels connecting various physical components for real-time measurement and control mostly make use of general purpose cyber-networks such as the Internet and wireless networks, which create vulnerabilities to adversarial intrusions. While conventional network security-based measures may be partially effective, novel resiliency methods explicitly taking the dynamical nature of physical components into account should be developed as any failure in security of the cyber components in such systems may turn into irrecoverable harms to the physical infrastructure.

Security experts define various security goals including (i) *Confidentiality*, ensuring privacy of important data against outside eavesdroppers; (ii) *Integrity*, maintaining fidelity of system signals; (iii) *Availability*, capability of timely having access to the required signals; (iv) *Authenticity*, verifying identity of each signal; (v) *Authorization*, adjusting legitimacy of access by each component to other parts of the system; and (vi) *Accountability*, detection of any potential attacks and faults in the system [1].

In this paper, we consider *masquerading*, *spoofing*, or *impersonation* attack strategy on cyber-physical networked systems, which is a threat of authenticity. A broad range of wired and wireless networks including sensor networks, in-vehicle networks, and Internet-based networks are susceptible to be threatened by spoofing. For instance, the reader can refer to [2] for satellite mobile communication networks, [3] for

mobile ad hoc networks, and [4] for CAN-based networks. Spoof-resiliency techniques would be essential for all of these network setups to detect and/or mitigate the adversarial effects. However, mostly in literature, the spoof-resilient algorithms are studied for the interactions between only two agents: a spoofer and a normal [5–9]. For example, [6] presents an application of spatial processing methods for spoofing detection and mitigation. Also, a GPS spoofing scenario is formulated as a constrained optimization problem and an effective solution is provided to compute the falsified GPS measurement of each time instant [7]. The false-data injection attack on unmanned vehicles is investigated in [8]. Although, this differs a little from spoofing attacks. The attacker masquerades as a disturbance for control system of a vehicle and deviates its path smoothly. Furthermore, a game-theoretic approach is developed in [9] to counteract spoofing attacks. However, a common point all the above researches share is that there is no network of agents. Only two-side interplay scenarios are considered, where the spoofing or masquerading is the attacking method. Recently though, [10] and [11] focused on the sequels of spoofing attack on the network of agents. However, both of these references use physical fingerprints of communication signals to undo the attacks, which is a different approach and cannot resist against omnniscient adversaries in practice. Despite [10], in our work, the attackers do not leave any sign and thus the regular nodes cannot identify them. Also, omniscient attackers in our setup could break any type of signal encryption and perform masquerading. Particularly, our emphasis is on the resiliency of a network in terms of its topology that is a more basic level of counteraction to cyber threats. Moreover, in [10], attackers cause an availability threat by jamming the server with fake identities, which is a special case of our adversarial model. We combine adversarial capabilities of the so-called *Byzantine* model, which is an integrity attack capable of sending inconsistent erroneous signals to the receivers introduced and used in [12,13], with spoofing, that is use of other nodes' identities to send data on their behalf, and introduce a novel and more powerful adversarial model called *smart spoofer*. In [14], resiliency of synchronous networks is investigated against mobile Byzantine adversaries that are different from our adversarial model. In our setting, smart spoofers can use the asynchrony of network communications to mislead the nodes with impersonated identities.

One of the targets of spoofers in network systems would be inserting erroneous values into the distributed state estimations performed by the nodes. Distributed state estimation algorithms are extensively studied in the literature [15–18]. However, all these research works focused on the interaction between dynamic system, observers and the graph topology. A minimum cost communication graph which enables limited communication for decentralized estimation is investigated in [15] . The interplay between network connectivity, global observability, and system instability is studied in [16]. Necessary and sufficient conditions for existence of distributed observers are studied in [17]. Also, [18] generalizes distributed observer design for LTI systems with singular transition matrices. None of the above research works consider communication security among the physical and cyber layers. The resilience of distributed observers against cyber attacks has recently received more attention. For instance, the resiliency of LTI systems has been investigated in [19,20] against Byzantine attacks. However, our adversarial model is more complex by considering the impersonation capability of adversaries. We also consider asynchrony and delays in communications and propose a randomization strategy for relaxing the imposed topology constraints for secure distributed estimation problem.

In the current paper, we consider impersonation on a network of distributed observers for an LTI system. Like the network communication settings in [21,22], the observers communicate with bounded delays and asynchrony; however, they must deal with stronger attacks, i.e., smart spoofing. Similar to [19], the regular (un-attacked) nodes are partitioned to source nodes and follower nodes, where source nodes can detect the corresponding eigenvalues and via distributively constructing a directed acyclic graph (DAG), the associated state estimates disseminate through the network. In both DAG construction and estimation propagation, smart spoofers interfere to avoid convergence. We present a strategy based on local filtering that is able to defend against smart spoofing and define local subgraphs to mimic the graph behavior for analysis of the estimation convergence, turning into sufficient conditions on network topology based on graph robustness that is a connectivity measure (see [13,23] for application of similar filtering algorithms in consensus problem). Consistency of the defined spoofing model with the network security literature, consideration of delays, asynchrony, and accurate assumptions

in network communications make our proposed algorithms, update rule, and concluding results more practical in real world applications. In the development of our results and the proofs, we adopted the concept of motifs, the smallest possible subgraphs of the original network with certain properties, as a new proof technique. We analyze how the information is disseminated through the motifs. All in all, the main contributions of this paper to the literature are:

- Introducing, modeling and formulating a new type of cyber attack in asynchronous network settings which inherits the properties of both Byzantine adversaries and spoofing agents, called smart spoofing.
- Analyzing the vulnerability of asynchronous networks to smart spoofers and proposing a resilient distributed state estimation strategy for a class of LTI systems.
- Using motifs, as the smallest possible repeating patterns in a network, to mathematically analyze the topology constraints required for convergence of the distributed state estimation.
- Presenting a randomized update rule to relax the spoof-resilient topology constraint required for convergence of the distributed state estimation.

The paper is organized as follows. The preliminaries and problem statement come in Sect. 2. In Sect. 3, we take a look at the resilient distributed estimation scheme and the local filtering-based algorithm that we used in this paper. Our main results are presented in Sect. 4. We put forward the simulation results in Sect. 5. Finally, we conclude the paper and discuss the future tendency of the research in Sect. 6.

2 Preliminaries and problem statement

2.1 Notations

2.1.1 Graph theory

A directed graph is represented by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where the set of nodes and edges are represented by $\mathcal{V} = \{1, \ldots, N\}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ respectively. An edge from node j pointing to node i implies data transmission from node j to node i and is denoted by (j, i). The neighbourhood of the i-th node is defined by the set $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\}$. A node j is said to be an outgoing neighbour of node i if $(i, j) \in \mathcal{E}$. A spanning sub-graph for $\mathcal{G}$ is a sub-graph of $\mathcal{G}$ which

contains every vertex of $\mathcal{G}$. Consider node v_1 to v_p of $\mathcal{G}$. A path is a sequence $(v_1, v_2, \ldots, v_p)$ in which $(v_i, v_{i+1}) \in \mathcal{E}$ for $i = 1, \ldots, p - 1$. The length of a path is measured by its number of edges. A cycle is a sequence $(v_1, v_2, \ldots, v_p, v_1)$ in which $(v_i, v_{i+1}) \in \mathcal{E}$ for $i = 1, \ldots, p - 1$ and $(v_p, v_1) \in \mathcal{E}$. A directed acyclic graph (DAG) is a directed graph which has no cycles.

For the consensus-based state estimation rule designed in this paper, the critical topological notion is graph robustness, which is a connectivity measure of graphs (see [24]).

Definition 1 *(r-reachable set) For a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and a set $\mathcal{C} \subset \mathcal{V}$, we say that $\mathcal{C}$ is an r-reachable set if there exists an $i \in \mathcal{C}$ such that $|\mathcal{N}_i \setminus \mathcal{C}| \geq r$, where $r \in \mathbb{N}_+$.*

Definition 2 *(Strongly r-robust w.r.t. $\mathcal{S}$) For a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, a set of nodes $\mathcal{S} \subset \mathcal{V}$ and $r \in \mathbb{N}_+$, we say that $\mathcal{G}$ is strongly r-robust with respect to $\mathcal{S}$, if for any non-empty subset $\mathcal{C} \subseteq \mathcal{V} \setminus \mathcal{S}$, $\mathcal{C}$ is r-reachable.*

2.1.2 Linear algebra

The set of all eigenvalues of a matrix A is denoted by $\sigma(A)$. The set of all marginally stable and unstable eigenvalues of a matrix A is denoted by $\sigma_U(A) = \{\lambda \in \sigma(A) | |\lambda| \geq 1\}$. We use $a_A(\lambda)$ and $g_A(\lambda)$ to denote the algebraic and geometric multiplicities, respectively, of an eigenvalue $\lambda \in \sigma(A)$. An eigenvalue λ is said to be simple if $a_A(\lambda) = g_A(\lambda) = 1$.

2.2 System dynamics and distributed observers

Consider the following discrete-time LTI system:

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

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

$$y_i[k] = C_i x[k], \tag{2}$$

where $y_i[k] \in \mathbb{R}^{r_i}$ and $C_i \in \mathbb{R}^{r_i \times n}$. For computational or control purposes, each node needs to estimate the entire system state $x[k]$. Nodes of the network $\mathcal{G}$ are called *distributed observers* if they maintain

and update the estimates using only their own measurements and those received from their neighbors. Fig. 1 shows the layout of a typical cyber-physical system threatened by adversarial nodes. Let $\hat{x}_i[k]$ denote the state estimate of node i at each time step k. The following definition describes the objective of the distributed estimation scheme.

Definition 3 *(Omniscience) Over the N-node network $\mathcal{G}$, the distributed observers are said to achieve omniscience if* $\lim_{k \to \infty} |\hat{x}_i[k] - x[k]| = 0, \forall i \in \{1, 2, \ldots, N\}$.
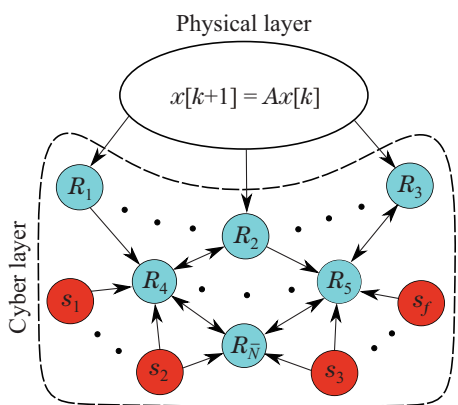
Physical layer

Figure 1 A typical cyber-physical system: In the physical layer, the plant dynamic (maybe unstable in some modes) propagates over time. In the cyber layer, the plant's outputs are monitored by a network of distributed observers $(R_1, R_2, \ldots, R_{\bar{N}})$ while only some of them are directly connected to the plant. The network is threatened by adversarial nodes $(s_1, s_2, \ldots, s_f)$.

2.3 Adversarial model

We consider an adversarial model that is able to threaten the following system protection services: *authentication*, *authorization*, *confidentiality*, *integrity* and *availability*. In what follows, we formally define the abilities of such an adversarial node.

Definition 4 *(Smart spoofer) An adversarial node is called a smart spoofer if it has the following capabilities:*

1) *The adversarial node can have complete knowledge about the topology, plant dynamics, and information flow over the network at all time steps.*
2) *The adversarial node can refuse to perform any pre-assigned algorithm and can send arbitrary values to each of its neighbors at the same time step.*

3) *The adversarial node can send its data with intended delays and asynchrony.*
4) *The adversarial node can impersonate other nodes and send arbitrary data with their identities.*

The first two actions are performed by Byzantine adversaries, while the last one is performed by a threat called *spoofing* or *masquerading* in [1] that directly threatens the authentication among systems' protection services. In fact, the introduced adversarial model is an advanced spoofing threat with additional capabilities of Byzantine adversaries that we call *smart spoofing*. Note that we use the terms "spoof" and "impersonate" interchangeably in this paper.

It is apparent that no distributed estimation algorithm would succeed if all the nodes are adversarial. Therefore, the set of nodes $\mathcal{V}$ is partitioned into two subsets of regular nodes and adversarial nodes denoted by $\mathcal{R}$ and $\mathcal{A} = \mathcal{V} \setminus \mathcal{R}$, respectively. In the literature of distributed fault-tolerant algorithms, a common assumption is to assign an upper bound f to the total number of adversarial nodes in the network, which is known as f-total adversarial model. To consider a large number of adversaries in large scale networks, locally bounded fault models are used, as in [25], defined below.

Definition 5 *(f-local smart spoofer model) A set $\mathcal{A}$ of smart spoofers is f-locally bounded if it contains at most f smart spoofers in the neighbourhood of any of the regular nodes, i.e., $|\mathcal{N}_i \cap \mathcal{A}| \leq f, \forall i \in \mathcal{V} \setminus \mathcal{A}$.*

Similarly, any distributed estimation algorithm fails if a smart spoofer can impersonate all the network nodes. Thus, to tackle the problem, we impose an upper bound for the number of nodes that smart spoofers can send data on their behalf as follows.

Definition 6 *(Capacity of smart spoofers) The maximum number of nodes that a smart spoofer can send data on their behalf at each time step, including itself, represents its capacity and is denoted by $\alpha \geq 1$.*

2.4 Problem statement

We aim to formulate the resilient version of omniscience problem (Definition 3), where the network is under smart spoofers' attack with two challenging

constraints on the network communications, i.e., asynchrony and delays. Accordingly, we set the following assumptions on the network communications protocol remarking the practical aspects of our results.

Assumption 1 *All nodes update by a global clock. This means that the sampling time T is the same for all observers.*

Assumption 2 *All nodes communicate through serial links and have access to only the last data packet they have received from neighbor nodes.*

Assumption 3 *All nodes make, at least, one update within $\bar{k}$ steps and communication delays are upper-bounded by $\bar{\tau}$.*

Referring to the introduced LTI dynamic system and the observation model of the network, we put forth a more complicated version of the standard omniscience problem (Definition 3) in the following definition.

Definition 7 *(Resilient omniscience) Given a system dynamics of the form (1), a network represented by the graph $\mathcal{G}$, and an observer model at each node given by (2), a state estimation design is said to achieve resilient omniscience if $\lim_{k\to\infty} |\hat{x}_i[k] - x[k]| = 0, \forall i \in \mathcal{R}$, regardless of the actions of any f-locally bounded set of smart spoofers.*

This paper investigates the design of a distributed estimation scheme, proper to cope with smart spoofers threatening a given cyber network that is observing an LTI system. For this purpose, based on the assumptions on the network communications protocol and the smart spoofer adversarial model, we first present the distributed estimation scheme under a specific network topology. Next, we analyze the required topology constraints which guarantee resilient omniscience of all regular nodes that update their estimates using the proposed estimation strategy.

3 Resilient distributed observers

Under Byzantine adversarial model introduced in [12], the network achieves omniscience by distributed observers proposed in [19]. The design performs observation task by separating detectable and undetectable eigenvalues of the system and the related states. Here, we use a similar scheme with a different distributed estimation rule, proper for resilient omniscience defined

in Definition 7. To this end, consider a Jordan canonical decomposition of state transition matrix A with the following assumption on its eigenvalues. This assumption is made for sake of simplicity, is not restrictive, and can be relaxed by some extra mathematical efforts and the techniques denoted in [19], which is not the focus of this paper.

Assumption 4 *Eigenvalues of A are real and simple.*

This assumption allows us to diagonalize A by the coordinate transformation matrix $\Psi = [\psi_1, \ldots, \psi_n]$, where $\psi_1, \ldots, \psi_n$ are n linearly independent eigenvectors of A. With $z[k] = \Psi^{-1}x[k]$, the system (1) is transformed into the form

$$\begin{cases} z[k+1] = \bar{A}z[k], \\ y_i[k] = \bar{C}_i z[k], \ \forall i \in \{1, \ldots, N\}, \end{cases} \quad (3)$$

where $\bar{A} = \Psi^{-1}A\Psi$ is a diagonal matrix, and $\bar{C}_i = C_i\Psi$. The eigenvalues of $\bar{A}$ (which are the same as those of A) are denoted by $\lambda_1, \ldots, \lambda_n$. Each regular node i distinguishes its detectable and undetectable eigenvalues by PBH test and divides them into the sets $\mathcal{D}_i$ and $\mathcal{U}_i$, respectively. Also, the set of regular nodes are partitioned into sets of *source nodes* and *follower nodes* as defined below.

Definition 8 *(Source nodes and follower nodes) For each $\lambda_j \in \sigma_U(A)$, the set of nodes that can detect λ_j is denoted by $\mathcal{S}_j$, and is called the set of source nodes for λ_j. The rest of the nodes are called follower nodes.*

Each regular node, depending on being a source node or a follower node for λ_j, adopts a different strategy for estimating the related states.

3.1 State estimation by source nodes

Referring to [19], each regular node i relies on its own measurements and uses a local Luenberger observer to estimate a patch of the states $\hat{z}_{\mathcal{D}_i}$ associated to all $\lambda_j \in \mathcal{D}_i$. To this end, let $\Lambda_i \in \mathbb{R}^{\rho_i \times \rho_i}$ (recall $\rho_i = |\mathcal{D}_i|$) be a diagonal matrix consists of the detectable eigenvalues in $\mathcal{D}_i$ and $\bar{C}_{\mathcal{D}_i} \in \mathbb{R}^{r_i \times \rho_i}$ stand for the columns of $\bar{C}_i$ corresponding to those eigenvalues. Then we have:

$$\hat{z}_{\mathcal{D}_i}[k+1] = \Lambda_i \hat{z}_{\mathcal{D}_i}[k] + L_i(y_i[k] - \bar{C}_{\mathcal{D}_i}\hat{z}_{\mathcal{D}_i}[k]), \ (4)$$

where $L_i^j \in \mathbb{R}^{\rho_i \times r_i}$ is the observer gain matrix at node i. Since the pair $(\Lambda_i, \bar{C}_{\mathcal{D}_i})$ is detectable, L_i can be chosen in a way that $(\Lambda_i - L_i \bar{C}_{\mathcal{D}_i})$ is Schur stable, so $\lim_{k \to \infty} |\hat{z}_i^j[k] - z^j[k]| = 0$ based on Assumption 4.

3.2 Distributed state estimation by follower nodes

A regular node i cannot estimate a portion of the states associated with its undetectable eigenvalues of the system. In fact, the regular node i is a follower node in estimating the sub-state related to the eigenvalues $\lambda_j \in \mathcal{U}_i$ and needs to receive information from its neighbors through a directed acyclic graph for each λ_j (defined later) rooted in the set of associated source nodes. In what follows, we propose an updating rule for the follower node i accomplishing its estimation task in a network with communication delays and *partial asynchrony*[1].

There is a major difference between resilient distributed state estimation rather than resilient consensus using local filtering presented in previous research works such as [22]. Considering asynchronous network communications and observability of dynamics of the physical layer is a new challenge in design of the update rule and leads to a totally different convergence analysis. Combining the ideas behind the consensus update rules in [19] and [22], we present a novel update rule with the following algorithm based on local filtering method for node i to update its own state estimate for $\lambda_j \in \mathcal{U}_i$.

1) Each regular node i, at each time step k when it wants to update its estimate, gathers the state estimate of $z^j[k]$ *lastly* received from only the nodes in $\mathcal{N}_i^j \subseteq \mathcal{N}_i$ ($\mathcal{N}_i^j$ represents the set of neighbors in the DAG related to λ_j that is selected by Algorithm 1 for each regular node i, which will be proposed later) and arranges them from the largest to the smallest.

2) Node i drops the largest and smallest $(\beta + 1)f$ estimates (β will be defined later) and executes the following update rule:

$$\hat{z}_i^j[k+1] = \lambda_j \sum_{\ell \in \mathcal{N}_i^j} \omega_{i\ell}^j[k] \hat{z}_\ell^j[k - \widetilde{k}_{i\ell}[k] - \tau_{i\ell}[k]],$$
$$(5)$$

---

[1]The term *partial asynchrony* refers to the case where nodes share some level of synchrony by having the same sampling times; however, they make updates at different times based on bounded information delays [26]

where $\tau_{i\ell}[k]$ is the time delay of the last data packet that node i has received from node ℓ until time instant k (it may be time-varying), $\widetilde{k}_{i\ell}[k]$ is the time steps elapsed from the time that node i receives the packet of the node ℓ sent the last time before time k up to the time it makes an update ($\widetilde{k}_{i\ell}[k] < \bar{k}$), and $\omega_{i\ell}^j[k]$ is the weight that the i-th node dedicates to the ℓ-th node at the k-th time instant for the estimation of $z^j[k]$. The weights are non-negative and chosen to comply $\sum_{\ell \in \mathcal{N}_i^j} \omega_{i\ell}^j[k] = 1, \forall \lambda_j \in \mathcal{U}_i$. Node i removes the $(\beta + 1)f$ largest and $(\beta + 1)f$ smallest estimates from $\mathcal{N}_i^j$ by setting their associated weights to 0. Note that delays have an upper bound ($\tau_{i\ell} < \bar{\tau}$).

In practice, each node i has a memory for each of its neighbors where stores the most recently received data. Node i uses the most recent estimate values received from its neigbours in $\mathcal{N}_i^j$ in update rule (5), regardless of delays and asynchrony in communications.

4 Main results

In this section, we provide the main results of the paper giving the analysis of the spoof-resilient distributed estimation strategy and the topology constraints under which our adopted algorithms and update rule succeed.

First, we consider how harsh the misbehaviour effects of a smart spoofer would be in the network. In Definition 6, we introduced the spoofing capacity in each time step. In the following lemma, we generalize capacity of smart spoofers for a period of time.

Lemma 1 *Let Assumption 3 hold and capacity of a smart spoofer be α. Then, each smart spoofer is able to send data on behalf of $\beta = \alpha \bar{k} - 1$ regular nodes within each consecutive $\bar{k}$ steps.*

Proof According to Definition 6, a smart spoofer can send data on behalf of α nodes including itself at each time step. Also, according to Assumption 3, all nodes have to make at least one update within consecutive $\bar{k}$ steps (note that if a node does not follow this rule can be detected as an adversarial node by the regular nodes). Consider the time interval $k + 1 \leq t \leq k + \bar{k}$. Let the smart spoofer choose to make an update with its own identity at $t = k_s$, where $k + 1 \leq k_s \leq k + \bar{k}$. Considering each consecutive $\bar{k}$ steps, the smart spoofer s has $\alpha - 1$ capacity for impersonation at

k_s and α capacity in other $\bar{k} - 1$ steps. Therefore, the smart spoofer is able to impersonate $\alpha\bar{k} - 1$ nodes overall within $\bar{k}$ steps, i.e., $\alpha - 1 + \alpha(\bar{k} - 1) = \alpha\bar{k} - 1$. $\qquad\square$

In fact, Lemma 1 indicates that we cannot simply replace the smart spoofers and impersonated nodes with Byzantine nodes. Because the key question is that how many Byzantine nodes have the same effect of a smart spoofer with capacity α. This is what we mathematically clarified in Lemma 1. Asynchrony lets the adversarial nodes spoof a specific number of regular nodes within each $\bar{k}$ time-steps. Besides, from adversarial nodes' perspective, this spoofing (and sending false data packets) must be continued for all the future time – in every $\bar{k}$ steps – in order to be effective. Thus, the distributed algorithms of regular nodes must be modified to be resilient against the attack. In other words, network providers need to be aware that in a network with asynchrony (almost all the networks are practically asynchronous), there is the possibility of stronger attacks rather than Byzantine attacks. The following necessary condition on the network communications formally states when a smart spoofer can impersonate regular nodes.

Proposition 1 *Consider a network of nodes interconnected by complete graph $\mathcal{G}$, which contains smart spoofer $s \in \mathcal{N}_i^j$, where $i \in \mathcal{R}$. Suppose that s is able to impersonate, at least, one regular node within each consecutive $\bar{k}$ steps ($\beta > 0$). Smart spoofer s can impersonate a regular node $\ell \in \mathcal{N}_i^j \cap \mathcal{R}$ for node i at a time instant $t > k$ only if the packet which is broadcast by node ℓ at time instant $t = k$ is received by node i with delay $\widetilde{k}_{i\ell}[k] + \tau_{i\ell}[k] > 0$.*

Proof We prove by contradiction. Considering Assumption 1, let node $\ell \in \mathcal{N}_i^j$ broadcast a data packet at $t = k$ and node $i \in \mathcal{R}$ receives the packet at the same time ($\tau_{i\ell}[k] = 0$) and use it for its next update at the same time ($\widetilde{k}_{i\ell}[k] = 0$). Also, suppose that smart spoofer s decides to impersonate node ℓ for node i. There are two possibilities for the arrival time of the packet sent by s to i. The packet can arrive either before or after the time $t = k$ (the time instant $t = k$ is excluded as it contradicts Assumption 2). In case the packet sent by s arrives at any time $t > k$, the node i has already accepted the last packet it received, that is, the packet of node ℓ received at $t = k$, and has already made an update. Otherwise, if the packet sent by s arrives at any time $t < k$, then i will receive the packet sent by node ℓ at $t = k$ and since, according to Assumption 2, all nodes only access the last data packet they receive. In either case, the smart spoofer s fails to impersonate node ℓ for node i, which is a contradiction. This completes the proof. $\qquad\square$

Note that the necessary condition of Proposition 1 is independent of amounts of communication delays. This is because we would like to deal with smart spoofers that can impose arbitrarily bounded amount of delays on their links to the regular nodes, that is, if a smart spoofer wants to impersonate node $\ell \in \mathcal{N}_i^j$, it can arrange to send the packet to node i after node ℓ with appropriate delay so that it will be received after the packet sent by node ℓ. Then, node i accepts a packet sent by s with identity of node ℓ as it is the last packet received.

According to Proposition 1, the best case for the regular node i is that both $\widetilde{k}_{i\ell}[k] = 0$ and $\tau_{i\ell}[k] = 0$, so the smart spoofers in the neighborhood of i cannot impersonate neighbors of the node i. However, even if we suppose that $\widetilde{k}_{i\ell}[k] = 0$, i.e., node i has not any lag in updating its estimate using the last data received from node ℓ, regular nodes cannot be sure about spoofing attack. In practice, the regular nodes cannot guess, before receiving a packet, whether it will be received with delay and, if so, how much the delay will be (although communication links' delays in real network systems are inevitable). Besides, as we said, smart spoofers can send data packets with intended delays. Therefore, the regular nodes must be aware that all the communications may be done with delays in each time step. Therefore, to consider the worst case, we develop our further results on required topology constraints by assuming that the necessary condition on delays is satisfied for all time in the network.

4.1 Spoof-resilient mode estimation directed acyclic graph (SR-MEDAG)

Recall the local filtering for resilient consensus based estimation law (5). Inspired by the algorithm presented in [19], for construction of directed acyclic graphs associated with undetectable eigenvalues of an LTI system, we present a spoof-resilient algorithm which is distributively executed by all the regular nodes. The overall distributed estimation scheme constitutes the construction of these sub-graphs and the prescribed local filtering-based algorithm which are performed in parallel. In what follows, we define the directed acyclic graphs that are paths for information flow over the network.

Definition 9 *(SR-MEDAG) For each eigenvalue $\lambda_j \in \sigma_U(A)$, the spanning sub-graph $\mathcal{G}^j = (\mathcal{V}, \mathcal{E}^j)$ of $\mathcal{G}$ is Spoof-Resilient Mode Estimation Directed Acyclic Graph (SR-MEDAG) if it has the following properties:*

Algorithm 1 SR-MEDAG Construction Algorithm

1: **while** $k \leq \bar{K}_j$ **do**
2:    **for** $\lambda_j \in \sigma_U(A)$ **do** $c_i(j) = 0, \mathcal{N}_i^j = \emptyset$.
3:       **if** $i \in \mathcal{S}_j$ **then**
4:          Node i updates $c_i(j)$ to 1, sets $\mathcal{N}_i^j = \emptyset$ and broadcasts a message
5:          χ_j (e.g., "110") to its neighbors.
6:       **end if**
7:       **if** $i \in \mathcal{V} \setminus \mathcal{S}_j$ **then**
8:          **if** ($c_i(j) = 0$, and node i has received m_j from at least $2(\beta+1)f+1$ distinct neighbors) **then**
9:             Node i updates $c_i(j)$ to 1 and stores the labels of the neighbors from which it received χ_j to $\mathcal{N}_i^j$.
10:          **end if**
11:          **if** $c_i(j) = 1$ **then**
12:             Node i broadcasts χ_j to its neighbors.
13:          **end if**
14:       **end if**
15:    **end for**
16: **end while**
17: **Result**: $\mathcal{N}_i^j, \forall \lambda_j \in \sigma_U(A)$

---

1) If $i \in (\mathcal{V} \setminus \mathcal{S}_j) \cap \mathcal{R}$, then $|\mathcal{N}_i^j| \geq 2(\beta+1)f+1$.

2) There is a partition of $\mathcal{R}$ into the sets $\mathcal{L}_0^j, \mathcal{L}_1^j, \ldots,$ $\mathcal{L}_{\xi_j}^j$, such that $\mathcal{L}_0^j = \mathcal{S}_j \cap \mathcal{R}$, and $\mathcal{N}_i^j \cap \mathcal{R} \subseteq \bigcup_{r=0}^{m-1} \mathcal{L}_r^j$ for $i \in \mathcal{L}_m^j$, where $1 \leq m \leq \xi_j$.

Also, $\mathcal{N}_i^j \cap \mathcal{R}$ is the set of parent nodes of node i and $\mathcal{L}_m^j$ is the m-th layer of $\mathcal{G}^j$. In fact, for each λ_j, we can organize the set of regular nodes of the graph $\mathcal{G}$ as a directed acyclic graph $\mathcal{G}_j$. In $\mathcal{G}_j$, the set of regular source nodes are denoted by $\mathcal{L}_0^j$. Also, the set of regular nodes which have at least one path with length of m to $\mathcal{L}_0$ are in the m-th layer of $\mathcal{G}_j$ denoted by $\mathcal{L}_m$. Each regular node in m-th layer has at least $2(\beta+1)f+1$ parent nodes from the previous layers ($\bigcup_{r=0}^{m-1} \mathcal{L}_r^j$).

Each regular node $i \in \mathcal{R}$ distributively executes the SR-MEDAG construction algorithm, presented as Algorithm 1. The final result of the algorithm for node i is the set $\mathcal{N}_i^j$ associated with every undetectable eigenvalue $\lambda_j \in \sigma(A)$. By executing the algorithm at each time step k, node i stores a counter value $c_i(j)$ and a list of indices $\mathcal{N}_i^j$ in persistent memories for each undetectable eigenvalue λ_j. The stored values in $\mathcal{N}_i^j \subseteq \mathcal{N}_i$ are the parent nodes' indices of node i in

the SR-MEDAG of λ_j. Each regular node i starts with $c_i(j) = 0$ and $\mathcal{N}_i^j = \emptyset$. If node i was a source node for λ_j, i.e., $i \in \mathcal{S}_j$, it sets $c_i(j) = 1$ and $\mathcal{N}_i^j = \emptyset$, then it begins and keeps broadcasting an arbitrary preset message χ_j to its neighbors[2] for at least $\bar{K}_j$ steps (later we prove that $\bar{K}_j$ is bounded). If node i was a follower node for λ_j, i.e., $i \in \mathcal{V} \setminus \mathcal{S}_j$, it waits until it receives χ_j from at least $2(\beta+1)f+1$ distinct neighbors. Then, it sets $c_i(j) = 1$, saves the indices of the neighbors from which it received χ_j as $\mathcal{N}_i^j$, begins and keeps broadcasting χ_j to its neighbors for at least $\bar{K}_j$ steps. Finally, we say that *SR-MEDAG construction algorithm terminates for node i* if the counter value $c_i(j) = 1, \forall \lambda_j \in \sigma_U(A)$. Also, we say that *SR-MEDAG construction phase terminates for λ_j* if the counter value $c_i(j) = 1, \forall i \in \mathcal{R}$.

Interestingly, it is not necessary for the regular nodes to know $\bar{K}_j$ (in that case, they have to execute the construction algorithm for all the future time not up to $\bar{K}_j$). Indeed, each regular node i can begin updating its state estimates in parallel as soon as it sets $c_i(j) = 1$ for λ_j although the SR-MEDAG construction phase has not been terminated yet. However, we know that the construction phase will be terminated at some time instant in the future (bounded by $\bar{K}_j$) when all regular nodes will be able to update their own state estimates corresponding to each of the undetectable eigenvalues using the distributed consensus-based rule (5). In this regard, consider that delay and asynchrony do not affect the output of the algorithm for each regular node i. Because node i waits until it receives the predefined message χ_j from a specified number of nodes regardless of the time it takes. Indeed, asynchrony and bounded delays only postpone termination of the algorithm.

Furthermore, one may concern that some of the regular nodes are exposed to be impersonated by smart spoofers at any time while they are executing the construction algorithm. In fact, each smart spoofer not only can impersonate regular nodes (by sending arbitrary messages other than the true message χ_j on behalf of them) but also can misbehave as follows:

i) It chooses to transmit any message different from the true message χ_j from start to termination of the construction phase.

---

[2]We used the term *broadcast* considering the case of wireless networks. Regular nodes may transmit the information to their known outgoing neighbors in wired networks.

ii) It transmits the true message before the counter value is triggered by a regular node.

iii) It chooses not to transmit a message at all.

In the first case, regular nodes are able to identify the adversarial node as it goes against the rules of Algorithm 1. In the latter two cases, the adversarial node is undetectable by regular nodes relying just on local information. However, later we discuss constraints on the graph topology so that adversarial nodes fail to make any problem neither for the construction algorithm nor the estimation process.

It is noteworthy that the upper bound for the parameter $\bar{K}_j$ in Algorithm 1 is a function of the parameter β, which is the capacity that asynchrony provides for smart spoofers to impersonate regular nodes. This upper bound would be different if we consider simply more Byzantine nodes instead of spoofers and impersonated nodes. Actually, another contribution of our paper with respect to [19] is the MEDAG construction algorithm and its convergence time. In the case of synchronous networks, each regular node updates only once and goes to sleep, while, in asynchronous networks, regular nodes have to continue updating up to $\bar{K}_j$ time-steps in order to complete the SR-MEDAG construction.

In the following theorem, we show that the sub-graphs distributively found by the regular nodes, after termination of the construction phase, satisfy properties of the SR-MEDAG.

Theorem 1 *If the SR-MEDAG construction phase terminates for $\lambda_j \in \sigma_U(A)$, there exists a sub-graph $\mathcal{G}^j$ satisfying all the properties of an SR-MEDAG.*

Proof First, we prove by contradiction that the spanning sub-graph $\mathcal{G}^j$ is a directed acyclic graph. Suppose there is a directed cycle iPi, where i and the nodes in P belongs to $\mathcal{R}$. The path P originates from i which changes its counter value $c_i(j)$ from 0 to 1 and begins transmitting χ_j to its neighbors at a time instant $t = k_i^j$. Let the last node on the path P be ℓ. Clearly, node i receives data from node ℓ at a time instant $t > k_i^j$. As an edge from ℓ is pointing to node i, node i is supposed to receive the message χ_j from node ℓ even when its counter value $c_i(j)$ is set to 1. This contradicts what node i has to do according to Algorithm 1. The same argument holds for every regular node belonging to $\mathcal{G}^j$.

Next, we associate the notion of path length, referring to graph theory, to the found sub-graphs after the termination of the SR-MEDAG construction phase to show that the set $\mathcal{R}$ in $\mathcal{G}^j$ is partitioned to the sets $\mathcal{L}_0^j, \mathcal{L}_1^j, \ldots, \mathcal{L}_{\xi_j}^j$. To this end, let a regular node i update its counter value $c_i(j)$ from 0 to 1 at a time instant $t = k_i^j$. Then, we say that the node i belongs to $\mathcal{L}_m^j$ of $\mathcal{G}^j$ if length of its longest path to a node in S_j be m at k_i^j. Apparently, $\mathcal{L}_{\xi_j}^j$ is set of the nodes which have at least a path with maximum length (among all acyclic paths of $\mathcal{G}^j$) to a node in $\mathcal{S}_j$ as $1 \leq m \leq \xi_j$. Accordingly, node i belongs to $\mathcal{L}_0^j$ of $\mathcal{G}^j$ if $i \in \mathcal{S}_j \cap \mathcal{R}$. Now, suppose that the SR-MEDAG construction phase terminates for $\lambda_j \in \sigma_U(A)$. Since all the nodes update their counter values from 0 to 1 at some time instant, it is concluded that $\bigcup_{r=0}^{\xi_j} \mathcal{L}_r^j = \mathcal{R}$. Moreover, a regular node in $\mathcal{R}$ cannot update its counter value at two different time steps (the converse contradicts the rules of Algorithm 1). Thus $\mathcal{L}_r^j \cap \mathcal{L}_s^j = \emptyset, \ \forall r \neq s$. This completes the proof according to the definition of the sets $\mathcal{L}_m^j \ (0 \leq m \leq \xi_j)$. □

Remark 1 *Since the network communications are asynchronous and because each regular node does not know the communication delays between other nodes, regular nodes in the sets $\mathcal{L}_0^j, \mathcal{L}_1^j, \ldots, \mathcal{L}_{\xi_j}^j$ do not update their counter values in the same order as their layer number.*

We intentionally used the minimum number of variables to be communicated in SR-MEDAG so as to avoid potential masquerading threats caused by those variables. For example, it is not possible for regular nodes to realize their layer order in $\mathcal{G}^j$ as they cannot identify which of their parent nodes are spoofed. To clarify this, consider a regular node i in $\mathcal{L}_m^j$. The regular node has to receive $2(\beta + 1)f + 1$ incoming edges from the nodes in $\bigcup_{r=0}^{m-1} \mathcal{L}_r^j$ which broadcast their layer numbers so that the node i can realize its own layer number by sorting the received values and selecting the maximum as the previous layer number. However, smart spoofers can impersonate some of these nodes and send a wrong layer number behind of them. Thus, the node i can be deceived about the maximum layer number it received. Interestingly, in our method, there is no need that the regular nodes know their layer orders since they only needs to know $2(\beta+1)f+1$ of their parent nodes to succeed in the estimation phase. Therefore, the construction algorithm can still be executed distributedly. Moreover, our strategy succeeds even if some of the source nodes in $\mathcal{S}_j$ are smart spoofers.

4.2 Analysis of the resilient distributed estimation strategy

In this section, we introduce a repeating pattern sub-graph which is used to simplify the analysis of our distributed estimation scheme. These sub-graphs are constructed and organized for each regular node according to its incoming edges from smart spoofers and other regular neighbors. Note that they may have overlaps in specific nodes and are defined as follows.

Definition 10 *(Motifs) Consider a regular node* $i \in \mathcal{L}_m^j$ *at time instant* k *and* $\lambda_j \in \sigma_U(A)$. *Partition* $\mathcal{N}_i^j$ *into subsets* $\{q\}$, $\{p_r\}$, $r = \{1, 2, \ldots, \underline{r}\}$, *and* $\{h_l\}$, $l = \{1, 2, \ldots, \overline{l}\}$, *where* q *and* p_r *are the parent nodes of node* i *that are not impersonated and* h_l *is a smart spoofer in* $\mathcal{N}_i^j$ *or an impersonated parent node of the node* i. *Then,* $\mathcal{G}_i^j(l, r) = (\mathcal{V}_i^j(l, r), \mathcal{E}_i^j(l, r))$ *is a sub-graph of* $\mathcal{G}^j$ *indicating the the motif associated with* h_l *and* p_r *around the node* i, *where* $\mathcal{V}_i^j(l, r) = \{i, p_r, q, h_l\}$ *and* $\mathcal{E}_i^j(l, r) = \{(p_r, i), (q, i), (h_l, i)\}$.

We aim to associate each motif $\mathcal{G}_i^j$ to each node i to ensure that a smart spoofer or an impersonated node cannot deviate the estimation of the node i. In fact, each motif is the smallest sub-graph of $\mathcal{G}^j$ which is resilient against Byzantine attacks. Note that impersonated regular nodes are potential Byzantine adversaries since smart spoofers can use their identities to send arbitrary values to their neighbors.

Definition 11 *(Independent and common nodes) Consider* $\overline{\gamma}$ *motifs associated with* h_l *and* p_r *around the regular node* i *denoted by* $\mathcal{G}_i^j(l, r)$, $r = 1, 2, \ldots, \overline{\gamma}$. *Let* p_γ *be a regular node in the set* $\mathcal{V}_j^i(l, r)$, $r = \gamma$. *Then,* p_γ *is an independent node if* $p_\gamma \notin \mathcal{V}_j^i(l, r) \ \forall r \neq \gamma$. *A node that is not independent is called common.*

The analysis strategy is to find the set of motifs around node $i \in \mathcal{L}_m^j$ such that they have only one common node. The following lemma determines the number of such motifs and investigates the possibility of this strategy (see Fig. 2 for an example).
x

Lemma 2 *Consider the network* $\mathcal{G}$ *which contains an SR-MEDAG* $\mathcal{G}^j$ *for each* $\lambda_j \in \sigma_U(A)$. *There exist at least* $(\beta + 1)f$ *motifs around each regular node* $i \in \mathcal{L}_m^j$, *where each motif has at least an independent node.*
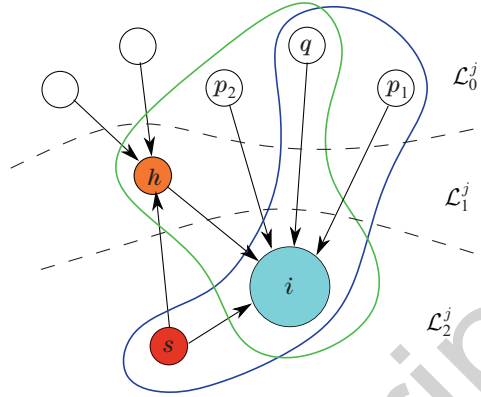

Figure 2 Motifs found in SR-MEDAG of $\mathcal{G}^j$ for $f = 1$ and $\beta = 1$ with the regular node i in $\mathcal{L}_2^j$, three regular parent nodes of i in $\mathcal{L}_0^j$ (p_1 and p_2 are independent nodes of the motifs and q is a common node) and a parent node in $\mathcal{L}_1^j$ which can be impersonated by a smart spoofer. Here, node h is impersonated by the smart spoofer s for the node i.

Proof For each regular node $i \in \mathcal{L}_m^j$, referring to Definition 10, consider partitioning of $\mathcal{N}_i^j$ into subsets $\{q\}$, $\{p_r\}$, $r = \{1, 2, \ldots, \underline{r}\}$, and $\{h_l\}$, $l = \{1, 2, \ldots, \overline{l}\}$. Based on the first property of SR-MEDAG $\mathcal{G}^j$, we have $\mathcal{N}_i^j \geq 2(\beta + 1)f + 1$. Under f-local smart spoofer model, there are at most f smart spoofers around the node i, i.e., $|\mathcal{N}_i^j \cap \mathcal{R}| \geq (2\beta + 1)f + 1$. These regular nodes are parent nodes of i based on the second property of SR-MEDAG $\mathcal{G}^j$. According to Lemma 1, at most βf of these parent nodes may be impersonated by the smart spoofers. Thus, at most $(\beta + 1)f$ of the nodes in $\mathcal{N}_i^j$ are whether smart spoofers or impersonated parent nodes of the node i which are partitioned as $\{h_l\}$, $l = \{1, 2, \ldots, \overline{l}\}$, i.e., $\overline{l} \leq (\beta + 1)f$. We can organize at least $(\beta + 1)f + 1$ of the remaining parent nodes, which cannot be impersonated, to construct the motifs around the node i. Based on Definition 10 and Definition 11, we pick a parent node q as a common node and leave the rest in the set of independent parent nodes $\{p_r\}$, $r = 1, 2, \ldots, \underline{r}$, i.e., $\underline{r} \geq (\beta + 1)f$. Since $\underline{r} \geq \overline{l}$, we can find at least $(\beta + 1)f$ motifs around the regular node i such that all of them have one common parent node q and each associated with an independent parent node p_r and a node h_l. This completes the proof. □

Fig. 2 exhibits two overlapping motifs. In this example, there is a smart spoofer node around the regular node i, i.e., $f = 1$. Also, it is supposed that $\beta = 1$. Thus, according to Lemma 2, two motifs are found around node i. Note that smart spoofer s can impersonate node h, so a motif has to be constructed with the node h as the adversarial node. Also, node q is selected as the common node while p_1 and p_2 are the two independent parent nodes of node i.

Next, we use the notion of motifs to analyze estimation resilience of the network $\mathcal{G}$ enhanced by the distributed estimation update rule (5) at each node against the adversarial nodes in the presence of communication delays and asynchrony. We start with regular node $i \in \mathcal{L}_m^j$ and generalize our analysis to the whole network afterwards.

Lemma 3 *Consider the network $\mathcal{G}$ which contains an SR-MEDAG $\mathcal{G}^j$ for each $\lambda_j \in \sigma_U(A)$. Suppose that the state estimates of regular parent nodes of node $i \in \mathcal{L}_m^j$, for the state related to λ_j, converge to z^j asymptotically. Then, the local filtering-based algorithm governed by update rule (5) ensures that $\lim_{k \to \infty} |\hat{z}_i^j[k] - z^j[k]| = 0$ in the presence of communication delays and asynchrony under f-local smart spoofer model.*

Proof Based on Lemma 2, node i has at most $(\beta + 1)f$ potential threats and at least $(\beta + 1)f$ motifs around node i such that they have one common node. Consider the motifs around node i: $\mathcal{G}_i^j(l, r)$, $r = 1, 2, \ldots, \underline{r}$, $l = 1, 2, \ldots, \bar{l}$, where $\underline{r} \geq (\beta + 1)f$ and $\bar{l} \leq (\beta + 1)f$. Let p_r be an independent parent node of the node i, q the common parent node, and h_l the potential Byzantine adversarial node in $\mathcal{G}_i^j(l, r)$, where the state estimation of p_r and q converge to z^j asymptotically for the state related to λ_j. For simplicity of notations, we define $k_{i\ell} = k - \widetilde{k}_{i\ell}[k] - \tau_{i\ell}[k]$. Note that $\tau_{i\ell}[k]$ and $\widetilde{k}_{i\ell}$ are upper bounded by $\bar{\tau}$ and $\bar{k}$, thus $k_{i\ell} = k$ if $k \to \infty$. Therefore, for each node i, we calculate the *asymptotic estimation error* of node $\ell \in \mathcal{N}_i^j$ for $z^j[k]$ by the last transmitted data to the node i: $e_\ell^j[k] = \hat{z}_\ell^j[k_{i\ell}] - z^j[k]$, $k \to \infty$. Also, the asymptotic estimation error of the node i for $z^j[k]$ is denoted by $e_i^j[k] = \hat{z}_i^j[k] - z^j[k]$, $k \to \infty$. Then, subtracting $z^j[k + 1]$ from both sides of (5) and noting that $z^j[k + 1] = \lambda_j z^j[k]$ based on (3), we derive Equation 6 from (5). Equation (6) represents that the estimation error of the node i is a linear combination of the estimation errors of its neighbors which are grouped as motifs. Note that $\sum_{\ell \in \mathcal{N}_i^j} \omega_{i\ell}^j[k] = 1$. For the un-impersonated parent nodes of node i, we have $\lim_{k \to \infty} e_q^j[k] = 0$ and $\lim_{k \to \infty} e_{p_r}^j[k] = 0$, $r = 1, 2, \ldots, \underline{r}$.

Now, consider the motifs $\mathcal{G}_i^j(l, r)$, $l = r = 1, 2, \ldots, \bar{l}$ (note that $\underline{r} \geq \bar{l}$) for the adversarial nodes h_ℓ, $l = 1, 2, \ldots, \bar{l}$. In construction of the motifs, we arbitrarily pick the common node q; so we suppose that $\hat{z}_{p_r}^j[k] \leq \hat{z}_q^j[k]$, $r = 1, 2, \ldots, \bar{l}$. The following two cases are possible regarding the estimation values of the nodes in the motif $\mathcal{G}_i^j(l, r)$: (i) $\hat{z}_{h_l}^j[k] < \hat{z}_{p_r}^j[k_{ip_r}]$ or $\hat{z}_{h_l}^j[k] > \hat{z}_q^j[k]$, (ii) $\hat{z}_{p_r}^j[k] \leq \hat{z}_{h_l}^j[k] \leq \hat{z}_q^j[k]$. In the former case, according to the local

filtering algorithm, values of the node h_l will be removed by setting $\omega_{ih_l}[k] = 0$. From the latter case, we infer that $e_{p_r}^j[k] \leq e_{h_l}^j[k] \leq e_q^j[k]$; the asymptotic estimation error of the adversarial node h_l will be trapped by the estimation errors of the parent nodes p_r and q in motif $\mathcal{G}_i^j(l, r)$ at time step k and will be sandwiched by them over time as they converge to 0 asymptotically. Therefor, we conclude that $\lim_{k \to \infty} e_{h_l}^j[k] = 0$.

$$
\begin{aligned}
&e_i^j[k + 1] \\
&= \lambda_j \sum_{\ell \in \mathcal{N}_i^j} \omega_{i\ell}^j[k] \hat{z}_\ell^j[k_{i\ell}] - \lambda_j \Big(\sum_{\ell \in \mathcal{N}_i^j} \omega_{i\ell}^j[k] \Big) z^j[k] \\
&= \sum_{l=r=1}^{\bar{l}} \Big(\lambda_j \omega_{ip_r}^j[k] \hat{z}_{p_r}^j[k_{ip_r}] - \lambda_j \omega_{ip_r}^j[k] z^j[k] \\
&\quad + \lambda_j \omega_{ih_l}^j[k] \hat{z}_{h_l}^j[k_{ih_l}] - \lambda_j \omega_{ih_l}^j[k] z^j[k] \Big) \\
&\quad + \sum_{r=\bar{l}+1}^{\underline{r}} \Big(\lambda_j \omega_{ip_r}^j[k] \hat{z}_{p_r}^j[k_{ip_r}] - \lambda_j \omega_{ip_r}^j[k] z^j[k] \Big) \\
&\quad + \lambda_j \omega_{iq}^j[k] \hat{z}_q^j[k_{iq}] - \lambda_j \omega_{iq}^j[k] z^j[k] \\
&= \lambda_j \sum_{l=r=1}^{\bar{l}} \Big(\omega_{ip_r}^j[k] e_{p_r}^j[k] + \omega_{ih_l}^j[k] e_{h_l}^j[k] \Big) \\
&\quad + \lambda_j \sum_{r=\bar{l}+1}^{\underline{r}} \omega_{ip_r}^j[k] e_{p_r}^j[k] + \lambda_j \omega_{iq}^j[k] e_q^j[k].
\end{aligned}
\tag{6}
$$

The same argument holds for all adversarial nodes $h_l \in \mathcal{G}_i^j(l, r)$, $l = 1, 2, \ldots, \bar{l}$. Therefore, the estimation error $e_i^j[k + 1]$, which is the linear combination of the estimation errors $e_{p_r}^j[k]$, $r = 1, 2, \ldots, \underline{r}$, $e_{h_l}^j[k]$, $l = 1, 2, \ldots, \bar{l}$ and $e_q^j[k]$, converges to 0 asymptotically, i.e., $\lim_{k \to \infty} e_i^j[k] = \lim_{k \to \infty} |\hat{z}_i^j[k] - z^j[k]| = 0, \forall i \in \mathcal{L}_m^j$. $\square$

Now, we analyze resilience of the estimation of all the follower nodes in the whole network $\mathcal{G}$ with communication delays and asynchrony against f-local smart spoofer model.

Lemma 4 *Consider the network $\mathcal{G}$ which contains an SR-MEDAG $\mathcal{G}^j$ for each $\lambda_j \in \sigma_U(A)$. Then, for each regular node $i \in \mathcal{R}$ and each $\lambda_j \in \mathcal{U}_i$, the local filtering-based algorithm governed by update rule (5) ensures that $\lim_{k \to \infty} |\hat{z}_i^j[k] - z^j[k]| = 0$ in the presence of communication delays and asynchrony under f-local smart spoofer model.*

Proof As $\mathcal{G}$ contains an SR-MEDAG for each $\lambda_j \in \sigma_U(A)$, the sets $\mathcal{L}_0^j, \mathcal{L}_1^j, \ldots, \mathcal{L}_{\xi_j}^j$ form a partition of the set $\mathcal{R}$. To prove, we use induction on the layer number m.

For $m = 0$, by definition of the set $\mathcal{L}_0^j$, all the regular nodes in $\mathcal{L}_0^j$ belong to the set $\mathcal{S}_j$ and can estimate $z^j[k]$

asymptotically. Then, consider the regular node i belonging to the set $\mathcal{L}_1^j$. Suppose that the regular node i has f incoming edges from adversarial nodes. Then, according to Lemma 2, we can find at least $(\beta + 1)f$ motifs around node i with each of them having an independent regular source node from the set $\mathcal{L}_0^j$. Each smart spoofer is able to impersonate at most βf parent nodes of i. Therefore, there are at most $(\beta + 1)f$ Byzantine adversarial nodes (including smart spoofers and impersonated regular nodes) around node i. However, we infer from Lemma 3 that the state estimate value of each adversarial node is trapped and sandwiched by one of the motifs according to the local filtering algorithm. Thus, the state estimate of node i converges to z^j asymptotically.

Next, suppose the result holds for the regular nodes of all layers from 0 to m (where $1 \leq m \leq \xi_j - 1$). By induction, it is concluded that the result holds for all the regular nodes in $\mathcal{L}_{m+1}^j$ as well based on the definition of SR-MEDAG.
□

Due to the linear dynamics of the local Luenberger observers for source nodes and since the estimation error of each follower node is a linear combination of its un-impersonated parents, we infer the following corollary about the convergence rate of the follower nodes' estimation error.

Corollary 1 *Estimation convergence rate of all the follower nodes in the network is exponential as the estimation error of the source nodes converges to* 0 *exponentially.*

Theorem 2 *Consider the network $\mathcal{G}$ which contains an SR-MEDAG for each $\lambda_j \in \sigma_U(A)$. Then, the distributed estimation scheme governed by the Luenberger observers described by (4), and the local filtering-based algorithm governed by update rule (5), achieves resilient omniscience in the presence of communication delays and asynchrony under f-local smart spoofer model.*

Proof Based on the observable canonical decomposition represented by (3), for each regular node i, states of the dynamics system (1) are mapped and partitioned into two sub-states $z_{\mathcal{D}_i}[k]$ and $z_{\mathcal{U}_i}[k]$ corresponding to the detectable and undetectable eigenvalues of the node i, respectively. Using the designed Luenberger observers, $\hat{z}_{D_i}[k]$ converges to $z_{D_i}[k]$ asymptotically. As an SR-MEDAG exists for each $\lambda_j \in \sigma_U(A)$, the result of Lemma 4 also holds. Consequently, node i is able to estimate $z_{\mathcal{U}_i}[k]$ asymptotically even in the presence of communication delays, asynchrony and adversarial actions of smart spoofers. Combining these results, we infer that node i can estimate the entire state $z[k]$ which leads to resiliently observing $x[k]$ using the transformation $x[k] = \Psi z[k]$. This completes the proof. □

4.3 Spoof-resilient graph topologies

In this section, we characterize graph topologies which ensures termination of the SR-MEDAG construction phase for each $\lambda_j \in \sigma_U(A)$ under misbehavior of smart spoofers.

Lemma 5 *The SR-MEDAG construction phase terminates for $\lambda_j \in \sigma_U(A)$ if $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$.*

Proof Contradiction is used for the proof. Consider any $\lambda_j \in \sigma_U(A)$ and let $\mathcal{G}$ be strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. the set of source nodes $\mathcal{S}_j$. If the SR-MEDAG construction phase does not terminate for λ_j, there exists a set of regular nodes $\mathcal{C} \subseteq \mathcal{V} \setminus \mathcal{S}_j$ which never update their counter values $c_i(j)$ from 0 to 1 for $i \in \mathcal{C}$. As $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, it follows that $\mathcal{C}$ is $\big(3(\beta + 1)f + 1\big)$-reachable, i.e., there exists a node $i \in \mathcal{C}$ which has at least $3(\beta + 1)f + 1$ neighbors outside $\mathcal{C}$. Under the f-local smart spoofer model, at most f of these nodes are smart spoofers which are able either to misbehave themselves or to impersonate βf regular nodes during the SR-MEDAG construction phase. Therefore, at least, $2(\beta+1)f+1$ of them are regular nodes with $c_i(j) = 1$ which must have transmitted χ_j to node i. Thus, node i must have changed $c_i(j)$ from 0 to 1 at some point of time, according to the rules of Algorithm 1. This is a contradiction.
□

Proposition 2 *Suppose that $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall \lambda_j \in \sigma_U(A)$, and let the SR-MEDAG construction phase starts at $k = 0$. Then, $\bar{K}_j$ in Algorithm 1 is upper bounded by $\bar{l}_j\big((\eta + 1)\bar{k} + \bar{\tau} + 1\big)$ where $\eta = \beta\lfloor(\bar{\tau} - \bar{k})/\bar{k}\rfloor$ and $\bar{l}$ is length of the longest path of $\mathcal{G}^j$.*

Proof Since $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, according to Lemma 5, each regular node has at least $2(\beta + 1)f + 1$ parent nodes which remain safe from spoofing and transmit χ_j at least once to the regular node. Each of these parent nodes has to make at least an update within $\bar{k}$ consecutive steps.

We consider two separate cases: i) $\bar{\tau} \leq \bar{k}$ and ii) $\bar{\tau} > \bar{k}$. Let node i be in $\mathcal{L}_1^j$ of $\mathcal{G}^j$. In the first case, each smart spoofer $s \in \mathcal{N}_i^j$ is able to impersonate at most βf parent nodes of node i in each consecutive $\bar{k}$ steps. Therefore, the other $2(\beta + 1)f + 1$ parent nodes will remain safe and transmit χ_j to node i. For the second case, we consider the worst case where all these parent nodes postpone their updates by $\bar{k} - 1$ steps and communicate to their neighbors with $\bar{\tau}$ steps delay (because we are seeking the maximum time steps that

a smart spoofer can prevent exactly $2(\beta + 1)f + 1$ parent nodes to transmit χ_j to their neighbors). As $\bar{\tau} > \bar{k}$, the smart spoofer has more $\eta = \beta\lfloor(\bar{\tau} - \bar{k})/\bar{k}\rfloor$ capacity after the first update to impersonate more parent nodes. However, they cannot do it permanently, i.e., at some time the parent nodes will transmit χ_j to node i. Suppose that the smart spoofer use this additional capacity to impersonate just one additional parent node. In fact, η updates of this parent node will be spoofed which takes $\eta\bar{k}$ time steps. Considering the first $\bar{k} - 1$ steps that the parent node may postpone its first update and $\bar{\tau}$ steps delay of its last update, the overall time that the spoofed parent node succeeds to transmit χ_j to node i will be $(\eta + 1)\bar{k} + \bar{\tau} + 1$ steps.

Now, consider the last node in the longest path of $\mathcal{G}^j$ which is the last node that updates its counter value from 0 to 1. Let the length of the longest path of $\mathcal{G}^j$ be $\bar{l}_j$ and each node in this path updates its counter value from 0 to 1 after at most $(\eta + 1)\bar{k} + \bar{\tau} + 1$. Then the maximum time needed for each regular node to keep transmitting χ_j is bounded by $\bar{l}_j\big((\eta + 1)\bar{k} + \bar{\tau} + 1\big)$. □

Remark 2 *The maximum time that is needed for each regular node $i \in \mathcal{L}_m^j$ to keep transmitting χ_j is bounded by $(\bar{l}_j - m)\big((\eta + 1)\bar{k} + \bar{\tau} + 1\big)$. However, as the regular nodes cannot characterize their layer numbers, they have to keep transmitting the message χ_j up to $\bar{K}_j$ steps.*

Finally, we propose the overall constraint on the network topology which makes sure that the network achieves resilient omniscience despite of smart spoofing actions.

Theorem 3 *Resilient omniscience of a network with communication delays and asynchrony under f-local smart spoofer model is achieved using the proposed estimation scheme if $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall\lambda_j \in \sigma_U(A)$.*

Proof According to Lemma 5, the SR-MEDAG construction phase terminates for every undetectable eigenvalue λ_j if $\mathcal{G}$ is strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall\lambda_j \in \sigma_U(A)$. Thus, based on Theorem 1, as SR-MEDAG exists for every $\lambda_j \in \sigma_U(A)$. Finally, from Theorem 2, the existence of an SR-MEDAG for every $\lambda_j \in \sigma_U(A)$ leads to resilient omniscience by using our proposed distributed estimation scheme in a network with communication delays and asynchrony under f-local smart spoofer model. □

Remark 3 *Suppose that smart spoofers impersonate none of the regular nodes during SR-MEDAG construction phase. Then, the sufficient constraint on the network topology to achieve resilient omniscience is strongly $\big(2(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall\lambda_j \in \sigma_U(A)$.*

Note that the presented sufficient conditions on the topology will be the same as the case of Byzantine attacks, proposed in [19], if we set the parameter $\beta = 0$. It means that the estimation will converge for all regular nodes under a simpler topology, i.e., strongly $(3f + 1)$-robust w.r.t. $\mathcal{S}_j$, $\forall\lambda_j \in \sigma_U(A)$. This is consistent with the most important massage of our paper which asserts that asynchronous networks are more susceptible against cyber attacks; asynchronous networks can be threaten by adversaries that are stronger than Byzantine nodes, i.e., smart spoofers, which can use free time-steps between updates of regular nodes to impersonate some of them in order to mislead the others.

4.4 Time-varying networks

In the presented results so far, the observers over network $\mathcal{G}$ were supposed to be fixed, that is, the edge set $\mathcal{E}$ was time invariant. We now reconsider the results with a partially asynchronous time-varying network $\mathcal{G}[k] = (\mathcal{V}, \mathcal{E}[k])$ instead of the original time-invariant graph $\mathcal{G}$ earlier. To this end, similar to what is presented in [21], we define a jointly graph robustness measure as follows.

Definition 12 *(Jointly strongly r-robust w.r.t. $\mathcal{S}$) The time-varying graph $\mathcal{G}[k] = (\mathcal{V}, \mathcal{E}[k])$ is said to be jointly strongly r-robust w.r.t. $\mathcal{S}$ if there exists a fixed $\bar{\mu} \geq 0$ such that $\bigcup_{\mu=0}^{\bar{\mu}} \mathcal{G}[k - \mu]$, $k \in \mathbb{Z}_{\geq\bar{\mu}}$, is strongly r-robust w.r.t. $\mathcal{S}$.*

Referring to Lemma 1, the capacity of smart spoofers for impersonating regular nodes is bounded within each consecutive $\bar{k}$ steps by β. Thus, the horizon parameter $\bar{\mu}$ of time-varying graph $\mathcal{G}[k]$ has to satisfy the following inequality:

$$\bar{\mu} \leq \bar{k}. \tag{7}$$

Note that, otherwise, each smart spoofer would have extra capacity to impersonate more than β regular nodes after each $\bar{k}$ steps.

Now, the following result states the extension of our main result (Theorem 3) for the case of time-varying networks.

Corollary 2 *Resilient omniscience of a network with communication delays and asynchrony under f-local smart spoofer model can be achieved using the proposed estimation scheme if $\mathcal{G}$ is jointly strongly $\big(3(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall \lambda_j \in \sigma_U(A)$, under condition (7).*

Similarly, reconsidering the case where smart spoofers do not impersonate any of the regular nodes during the SR-MEDAG construction phase, the following result holds for time-varying networks.

Corollary 3 *Suppose that smart spoofers impersonate none of the regular nodes during SR-MEDAG construction phase. Then, the sufficient topology constraint on the network $\mathcal{G}[k]$ to achieve resilient omniscience is jointly strongly $\big(2(\beta + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall \lambda_j \in \sigma_U(A)$, with condition (7).*

These results follow Lemmas 3 to 5 as the time-invariant nature of the original graph $\mathcal{G}$ is not used in the proofs.

4.5 Randomized update rule

Consider the case that each regular node, at each time instant, randomly decides whether to update its state estimate or not. That is, the follower node $i \in \mathcal{R}$ updates its state estimate at each time instant k with the probability of $P_i[k]$. Note that with such updates, the algorithm remains fully distributed. Even the probabilities $P_i[k]$ need not be identical. Intuitively, this is in alignment with Assumption 3 as the regular node will update at least once within each consecutive $\bar{k}$ steps. With this strategy, the topology constraint required for resilient omniscience can be relaxed. This is because the smart spoofers cannot predict the update times in advance and need to use more of their spoofing capacity to make sure that the regular nodes, at each time step, receive and accept false data with fake identities; they cannot impersonate other nodes in a systematic manner in each consecutive $\bar{k}$ steps. In fact, regular nodes utilized randomization in update times as a defensive means against smart spoofers.

What follows is the modification of Theorem 3 for the suggested network with randomized updating strategy.

Theorem 4 *Resilient omniscience of a network with communication delays and asynchrony under the f-local smart spoofer model can be achieved using the proposed estimation scheme if each follower node $i \in \mathcal{R}$, at each time instant*

k, *updates using rule (5) with the probability of $P_i \in (0, 1]$ and if $\mathcal{G}$ is strongly $\big(3(\beta' + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall \lambda_j \in \sigma_U(A)$, where $\beta' = \lfloor \beta/\bar{k} \rfloor + 1$.*

Proof Referring to Lemma 1, each smart spoofer was able to impersonate at most β regular nodes within $\bar{k}$ steps in case the smart spoofers knew when exactly each regular node updates its state estimate. Now, consider that each regular node i make an update at each time instant k randomly with a probability of $P_i[k] \in (0, 1]$. Then, each smart spoofer $s \in \mathcal{N}_i$ cannot predict when exactly the node i updates; so it has to impersonate the incoming neighbors of the node i for all the time steps within each consecutive $\bar{k}$ steps, that is $\bar{k}$ times. As a result, the smart spoofers need to dedicate more capacity to produce faulty data packets with the mimicked identities of the neighbors of the node i. Thus, the smart spoofers will be able to impersonate $\lfloor \beta/\bar{k} \rfloor$ regular nodes for any of $\bar{k}$ steps and one regular node for a limited number of time-steps, i.e., less than $\bar{k}$. In this situation, to ensure that the smart spoofers cannot impersonate any extra regular nodes, we define $\beta' = \lfloor \beta/\bar{k} \rfloor + 1$. Accordingly, similar to the proof of Theorem 3, the required topology constraint for omniscience based on the parameter β' is strongly $\big(3(\beta' + 1)f + 1\big)$-robust w.r.t. $\mathcal{S}_j$, $\forall \lambda_j \in \sigma_U(A)$. □

Remark 4 *Based on Lemma 1, we have $\beta' = \lfloor (\alpha\bar{k} - 1)/\bar{k} \rfloor$. On the other hand, we know $\bar{k} \geq 1$. Therefore, it is concluded that $\beta' = \alpha - 1$ in the case of a synchronous network ($\bar{k} = 1$) and $\beta' = \alpha$ in an asynchronous network ($\bar{k} > 1$).*

5 Simulation results

In this section, we present a simulation example to demonstrate how a smart spoofer can misbehave and how it can be restrained in a given network of distributed observers. In particular, we show why the constraints on the network topology, proposed in Theorems 2 and 3, are critical for achieving resilient omniscience under f-local smart spoofer model in the presence of asynchronous communications and delays.

To this end, consider the network illustrated in Fig. 3. The directed edges of the graph represent all to one connections and edges pointing in both directions represent all to all connections. The network has three sets of regular nodes $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, and a smart spoofer s ($f = 1$). The capacity of s is assumed to be $\alpha = 1$ and all of the nodes are supposed to make, at least, an update within $\bar{k} = 2$ steps. Thus, the parameter is set as $\beta = 1$. There are $2(\beta + 1)f$ nodes in each of the sets $\mathcal{R}_1$ and $\mathcal{R}_2$ and $2(\beta + 1)f + 1$ nodes in the

set $\mathcal{R}_3$, where the nodes within each set are not connected. Furthermore, communication delays over the network are defined as follows:

$$\tau_{ij} = \begin{cases} 3, & \text{if } (i \in \mathcal{R}_3 \text{ and } j \in \mathcal{R}_2), \\ 2, & \text{if } (i \in \mathcal{R}_2 \text{ and } j \in \mathcal{R}_3) \\ & \text{or } (i \in \mathcal{R}_3 \text{ and } j \in \mathcal{R}_1), \\ 1, & \text{if } (i \in \mathcal{R}_1 \text{ and } j \in \mathcal{R}_3) \\ & \text{or } (i \in \mathcal{R}_3 \text{ and } j = s), \\ 0, & \text{if } i = s \text{ and } (j \in \mathcal{R}_1 \text{ or } j \in \mathcal{R}_2). \end{cases}$$

Note that the smart spoofer fully knows the dynamic system and the observation models of the regular nodes and calculates its own and the impersonated states estimations in a way that the targeting regular nodes fail to reach omniscience. Thus, to give a better intuition, we deal with the transformed dynamic system and states in our simulations; the original system can be analyzed accordingly. For sake of simplicity, we use the terms "send" and "receive" with $\hat{z}_1^i$ (or $\hat{z}_2^i$), while our purpose is the original state $\hat{x}_1^i$ associated to the $\hat{z}_1^i$.
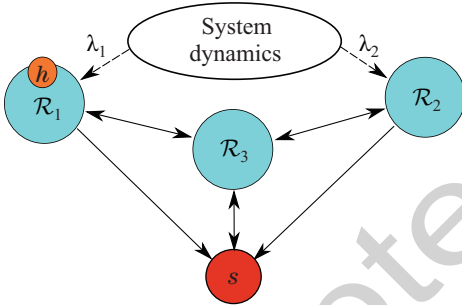

Figure 3 A sample network that is $\left(2(\beta+1)f+1\right)$-robust w.r.t. λ_j. Node $h \in \mathcal{R}_1$ is impersonated by the smart spoofer s for the nodes in set $\mathcal{R}_3$.

The transition matrix of the original dynamic system and the initial state are assumed to be

$$A = \begin{bmatrix} 0.98 & 0.02 \\ -0.04 & 1.04 \end{bmatrix}, \; x_0 = \begin{bmatrix} 2 \\ 5 \end{bmatrix},$$

which, according to (3), are transformed by

$$\Psi = \begin{bmatrix} 0.1 & 1 \\ 0.2 & 1 \end{bmatrix}$$

into the following diagonal system and initial state:

$$\bar{A} = \begin{bmatrix} 1.02 & 0 \\ 0 & 1 \end{bmatrix}, \; z_0 = \begin{bmatrix} 30 \\ -1 \end{bmatrix}.$$

The first eigenvalue of the system ($\lambda_1 = 1.02$) is unstable and the second one ($\lambda_2 = 1$) is marginally stable. The observation model of the network system is assumed to be $C_i = [-10 \; 10], \forall i \in \mathcal{R}_1, C_i = [2 \; -1], \forall i \in \mathcal{R}_2$ and $C_i = 0, \forall i \in \mathcal{R}_3$. The transformation of the observation model is given by Ψ as $\bar{C}_i = [1 \; 0], \forall i \in \mathcal{R}_1, \bar{C}_i = [0 \; 1], \forall i \in \mathcal{R}_2$ and $\bar{C}_i = 0, \forall i \in \mathcal{R}_3$. This means that the nodes in $\mathcal{R}_1$ are source nodes for λ_1 and followers for λ_2 as they can only detect λ_1, the nodes in $\mathcal{R}_2$ are source nodes for λ_2 and followers for λ_1, and the nodes in $\mathcal{R}_3$ are followers for both λ_1 and λ_2. Also, the nodes in the set $\mathcal{R}_3$ and the node s update at all time instants and the nodes in $\mathcal{R}_1$ and $\mathcal{R}_2$ update at time instants $k = m\bar{k}, \; m \in \mathbb{Z}_+$.

We present the simulation results in two test scenarios. In both scenarios, the smart spoofer just impersonate only one node in $\mathcal{R}_1$ and only for the state z_1. Thus, all the nodes of the network will accurately estimate the state z_2. In scenario 1, we show that the follower nodes for λ_1 can asymptotically estimate z_1 even though the smart spoofer s tries to mislead the follower nodes but the network finally achieves omniscience. However, in scenario 2, the follower nodes cannot reach a true estimate of z_1 as the required topology constraint for estimation (Theorem 2) is not satisfied.

Scenario 1 *The smart spoofer sends the message $\chi_s = 1$ to all the nodes in $\mathcal{R}_3$ to pretend that it is a parent node for λ_1. Although the smart spoofer can impersonate a regular node during the SR-MEDAG construction phase, it decides not to do so and goes through the estimation phase. The initial estimates of z_1 for nodes in $\mathcal{R}_1$ are $\hat{z}_1^i[0] = 100, \; i = 1,2$ and $\hat{z}_1^i[0] = 0, \; i = 3,4$. Also, we have $\hat{z}_1^i[0] = 0, \; i \in \mathcal{R}_2$, and $\hat{z}_1^i[0] = 0, i \in \mathcal{R}_3$. Moreover, each regular node $i \in \mathcal{R}_1$ uses a Luenberger observer with the gain $L_i^1 = 0.5$ to estimate z_1. Starting the estimation phase, the smart spoofer s sends two sequences of estimate values to all the nodes in $\mathcal{R}_3$ in a way that the receiving estimate values from the nodes in $\mathcal{R}_1$ are eliminated in local filtering: i) the estimate value $\hat{z}_1^s[k] = 60$, where $k = m\bar{k} - 1, m \in \mathbb{Z}_+$, which keeps the smart spoofer s among the accepted neighbors of the nodes in $\mathcal{R}_3$ as each node has to send a data packet at least in each consecutive $\bar{k}$ steps, ii) a false estimate value $\hat{z}_1^h[k] = 30$, where $k = m\bar{k}, m \in \mathbb{Z}_{\geq 0}$, on behalf of the node $h = 1, h \in \mathcal{R}_1$ to the nodes in $\mathcal{R}_3$. As shown in Fig. 4, all the regular nodes can estimate z_1*

although the smart spoofer caused a deviation in the estimations of the nodes in $\mathcal{R}_3$ (and accordingly the nodes in $\mathcal{R}_2$) up to time instant $k = 12$. Note that the estimate value of $\hat{z}_1^h[k]$ will not be filtered only if it converges to z_1. In fact, referring to Lemma 3, estimate values of the smart spoofer are sandwiched by estimate values of the regular parent nodes, thanks to our proposed rule (5) and the network topology constraint discussed in Theorem 2.
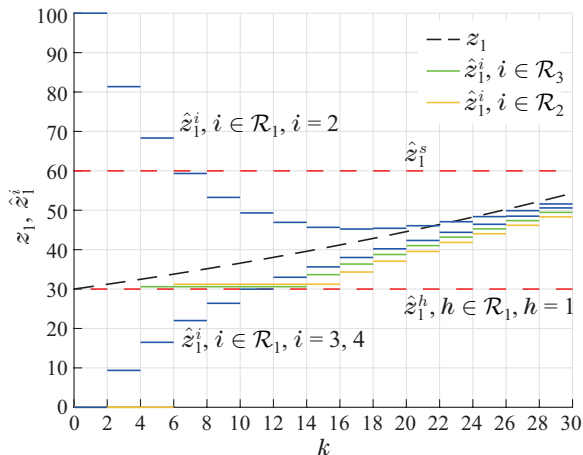

Figure 4 Omniscience of the sample network: the regular source nodes in $\mathcal{R}_1$ asymptotically estimate z_1 using Luenberger observers. The follower nodes in $\mathcal{R}_2$ and $\mathcal{R}_3$ can asymptotically estimate z_1 despite of the efforts smart spoofer does for misleading them by impersonating the node $h \in \mathcal{R}_1$. They also estimate z_2 since there is no spoofing for λ_2.

Scenario 2 *Here, the smart spoofer s sends a message $\chi_s = 1$ to the nodes in $\mathcal{R}_3$ while it impersonates the node $p = 1, p \in \mathcal{R}_1$ in the SR-MEDAG construction phase by setting the message $\chi_p = 0$, i.e., the node p cannot be a parent node of the nodes in $\mathcal{R}_3$ for λ_1. In other words, Algorithm 1 does not terminate in the case of λ_1 for the nodes in $\mathcal{R}_3$. In fact, the constraint on the network topology is not satisfied for the estimation of z_1 since the nodes in $\mathcal{R}_3$ recognizes only $2(\beta + 1)f$ parent nodes for λ_1. However, assume that the nodes in $\mathcal{R}_3$ decide to start the estimation regardless of the termination of the SR-MEDAG construction phase. As a result, the smart spoofer is able to impersonate one more regular node of the set $\mathcal{R}_1$ this time in the estimation phase. The initial estimates of z_1 are given as $\hat{z}_1^i[0] = 10, i \in \mathcal{R}_1, i = 2$, $\hat{z}_1^i[0] = 0$, $i \in \mathcal{R}_1, i = 3, 4$, $\hat{z}_1^i[0] = 6$, $i \in \mathcal{R}_2$, and $\hat{z}_1^i[0] = 7, i \in \mathcal{R}_3$. Again, the smart spoofer s sends two sequences of estimate values to the nodes in $\mathcal{R}_3$ in a way that the estimate values of the nodes $i \in \mathcal{R}_1, i = 3, 4$, are eliminated in local filtering: i) the estimate value $\hat{z}_1^s[k] = 8$, where $k = m\bar{k} - 1, m \in \mathbb{Z}_+$, which*

keeps the smart spoofer s among the accepted neighbors of the nodes in $\mathcal{R}_3$, ii) a false estimate value $\hat{z}_1^h[k] = 9$, where $k = m\bar{k}, m \in \mathbb{Z}_{\geq 0}$, on behalf of the node $h = 1, h \in \mathcal{R}_1$, to the nodes in $\mathcal{R}_3$. Fig. 5 shows the consequence of spoofing in the estimations. The initial estimate values of the nodes in $\mathcal{R}_2$ and $\mathcal{R}_3$ remain constant for all the future time. It is noteworthy that, not only the nodes in $\mathcal{R}_3$ are affected by the spoofing, but the nodes in $\mathcal{R}_2$ are also affected indirectly and none of them can reach omniscience for z_1.
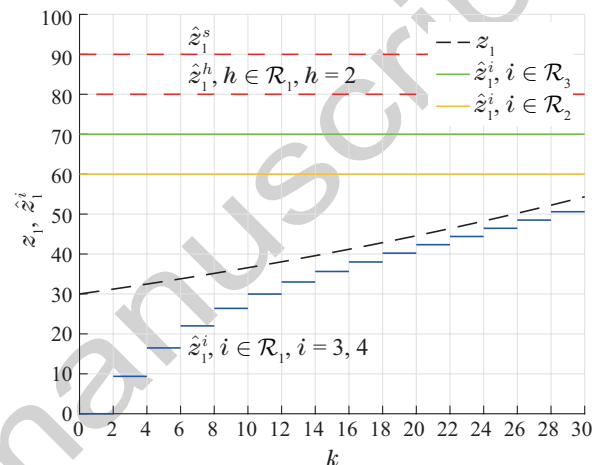

Figure 5 The smart spoofer s prevents the follower nodes for λ_1 in $\mathcal{R}_2$ and $\mathcal{R}_3$ to estimate z_1 by sending false estimate values on behalf of node $h \in \mathcal{R}_1$ to all the nodes in $\mathcal{R}_3$.

While we primarily analyzed the success or failure of the network omniscience in the transformed dynamic system, the main results are valid for the original dynamic system with different time histories of state values (Fig. 6 and Fig. 7).

6 Conclusions

Combining Byzantine adversarial model and spoofing as a misbehaving technique, we introduced a new type of cyber attack called smart spoofing. Then, we investigated the problem of distributed observer design for LTI systems in the presence of this attack which uses the asynchrony in communications to threaten the network. Using a two-step distributed mechanism, including a pre-executing algorithm for recognizing the trusted neighbors and a local-filtering algorithm for removing possible incorrect values induced by the adversarial nodes, the regular nodes can achieve resilient observation over so-called strongly robust graphs. We proposed resilient topology constraints on static and
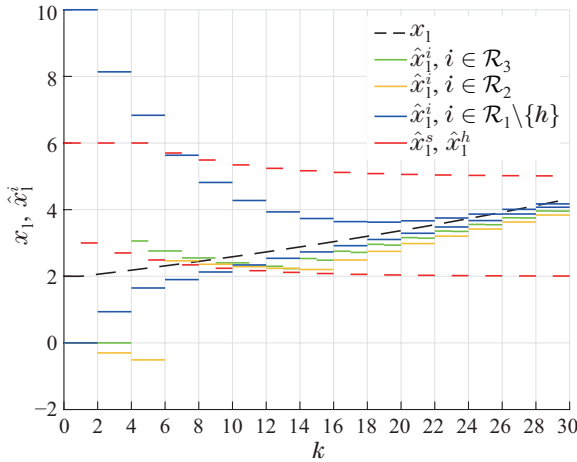
Figure 6 All the regular nodes truly estimate x_1 while the smart spoofer s impersonates the node $h \in \mathcal{R}_1$ for the nodes in $\mathcal{R}_3$.
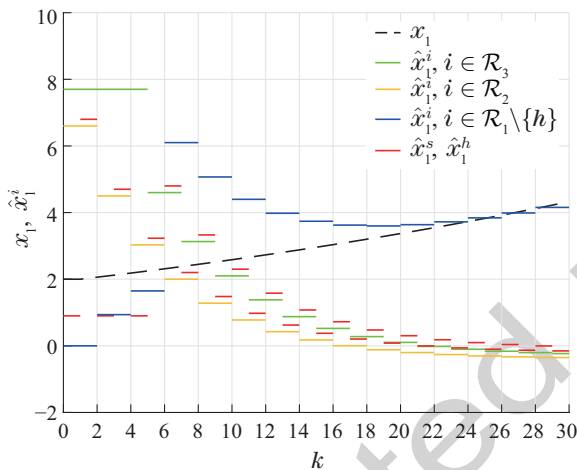

Figure 7 The regular nodes in $\mathcal{R}_2$ and $\mathcal{R}_3$ fail to estimate x_1 if the smart spoofer s impersonates the node $h \in \mathcal{R}_1$ for the nodes in $\mathcal{R}_3$.

time-varying networks under the proposed adversarial threat. Numerical simulations with a sample network validate our analytic results. The proposed designs are applicable to a vast range of networked systems. In future studies, we consider resilient consensus problems prone to the smart spoofing attacks.

Acknowledgements

References

[1] Daswani, N., Kern, C., Kesavan, A.: Foundations of Security: What Every Programmer Needs to Know. Dreamtech Press, ??? (2007)

[2] Zheng, G., Ma, H.-T., Cheng, C., Tu, Y.-C.: Design and logical analysis on the access authentication scheme for satellite mobile communication networks. IET Information Security **6**(1), 6–13 (2012)

[3] Villalba, L.G., Matesanz, J.G., Canas, D.R., Orozco, A.S.: Secure extension to the optimised link state routing protocol. IET Information Security **5**(3), 163–169 (2011)

[4] Ueda, H., Kurachi, R., Takada, H., Mizutani, T., Inoue, M., Horihata, S.: Security authentication system for in-vehicle network. SEI Technical Review **81**, 5–9 (2015)

[5] Sun, C., Hu, C., Liu, B.: Sack2: effective syn flood detection against skillful spoofs. IET Information Security **6**(3), 149–156 (2012)

[6] Magiera, J., Katulski, R.: Detection and mitigation of GPS spoofing based on antenna array processing. Journal of Applied Research and Technology **13**(1), 45–57 (2015)

[7] Su, J., He, J., Cheng, P., Chen, J.: A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. Proc. of IFAC Workshop NECSYS, 291–296 (2016)

[8] Dutta, A., Langbort, C.: Confiscating flight control system by stealthy output injection attack. Journal of Aerospace Information Systems **14**(4), 203–213 (2017)

[9] Zhang, T., Zhu, Q.: Strategic defense against deceptive civilian GPS spoofing of unmanned aerial vehicles. Proc. of Int. Conference on Decision and Game Theory for Security, 213–233 (2017)

[10] Gil, S., Kumar, S., Mazumder, M., Katabi, D., Rus, D.: Guaranteeing spoof-resilient multirobot networks. Autonomous Robots **41**(6), 1383–1400 (2017)

[11] Renganathan, V., Summers, T.: Spoof resilient

coordination for distributed multi-robot systems. Proc. of Int. IEEE Symposium on Multi-Robot and Multi-Agent Systems (MRS), 135–141 (2017)

[12] Lynch, N.A.: Distributed Algorithms. Morgan Kaufmann, ??? (1996)

[13] Dibaji, S.M., Safi, M., Ishii, H.: Resilient distributed averaging. Proc. of American Control Conference, 96–101 (2019)

[14] Bonnet, F., Défago, X., Nguyen, T.D., Potop-Butucaru, M.: Tight bound on mobile Byzantine agreement. Theoretical Computer Science **609**, 361–373 (2016)

[15] Alexandru, A.B., Pequito, S., Jadbabaie, A., Pappas, G.J.: On the limited communication analysis and design for decentralized estimation. Proc. of IEEE Conference on Decision and Control, 1713–1718 (2017)

[16] Khan, U.A., Kar, S., Jadbabaie, A., Moura, J.M.: On connectivity, observability, and stability in distributed estimation. Proc. of IEEE Conference on Decision and Control, 6639–6644 (2010)

[17] Park, S., Martins, N.C.: Design of distributed LTI observers for state omniscience. IEEE Transactions on Automatic Control **62**(2), 561–576 (2017)

[18] Wang, L., Morse, A.: A distributed observer for a time-invariant linear system. Proc. of American Control Conference, 2020–2025 (2017)

[19] Mitra, A., Sundaram, S.: Resilient distributed state estimation for LTI systems. arXiv preprint arXiv:1802.09651 (2018)

[20] Mitra, A., Sundaram, S.: Secure distributed state estimation of an LTI system over time-varying networks and analog erasure channels. Proc. of American Control Conference, 6578–6583 (2018)

[21] Dibaji, S.M., Ishii, H.: Resilient consensus of second-order agent networks: Asynchronous update rules with delays. Automatica **81**, 123–132 (2017)

[22] Dibaji, S.M., Ishii, H., Tempo, R.: Resilient randomized quantized consensus. IEEE Transaction on Automatic Control (2017)

[23] Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., Chakrabortty, A.: A systems and control perspective of CPS security. Annual Reviews in Control (2019)

[24] LeBlanc, H.J., Zhang, H., Koutsoukos, X., Sundaram, S.: Resilient asymptotic consensus in robust networks. IEEE Journal on Selected Areas in Communications **31**(4), 766–781 (2013)

[25] Pelc, A., Peleg, D.: Broadcasting with locally bounded Byzantine faults. Information Processing Letters **93**(3), 109–115 (2005)

[26] Bertsekas, D.P., Tsitsiklis, J.N.: Parallel and Distributed Computation: Numerical Methods. Prentice Hall, ??? (1989)

Mostafa Safi obtained his B.Sc. and M.Sc. degrees in Aerospace Engineering, both from Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2011 and 2013, respectively. His major was Dynamics and Control during his studies. Since 2017, he has started doing research in network control systems and resilient distributed algorithms with several conference and journal publications in these areas. Currently, his main focus is on electrical and electronic automotive platforms and cyber security of connected vehicles.