Distributed Estimation over Directed Graphs Resilient to Sensor Spoofing

Shamik Bhattacharyya, Kiran Rokade, and Rachel Kalpana Kalaimani

***Abstract*—This paper addresses the problem of distributed estimation of an unknown dynamic parameter by a multi-agent system over a directed communication network in the presence of an adversarial attack on the agents' sensors. The mode of attack of the adversaries is to corrupt the sensor measurements of some of the agents, while the communication and information processing capabilities of those agents remain unaffected. To ensure that all the agents, both normal as well as those under attack, are able to correctly estimate the parameter value, the Resilient Estimation through Weight Balancing (REWB) algorithm is introduced. The only condition required for the REWB algorithm to guarantee resilient estimation is that at any given point in time, less than half of the total number of agents are under attack. The paper discusses the development of the REWB algorithm using the concepts of weight balancing of directed graphs, and the consensus+innovations approach for linear estimation. Numerical simulations are presented to illustrate the performance of our algorithm over directed graphs under different conditions of adversarial attacks.**

***Index Terms*—Directed Graphs, Distributed Estimation, Resilient Consensus, Weight-balancing**

I. INTRODUCTION

THE advancement in wireless sensor networks (WSNs) has diversified their areas of application to agriculture [1], healthcare [2], and renewable energy [3] to name a few. As a result the scale and complexity of the networks is also on the rise [4], [5]. This necessitates the use of more distributed approaches to signal processing over WSNs, and distributed estimation is a key aspect of it. Distributed estimation is about determining a parameter of interest locally at each sensor node with cooperation between neighboring nodes [6]. The increase in areas of application of WSNs has in turn made them more vulnerable to adversarial attacks [7]. A major mode of such attacks are aimed to manipulate the normal functioning of the sensor nodes and thus disrupt the overall signal processing capability of the WSNs. Some commonly used threat models

are Byzantine [8], malicious [9], sensor spoofing [10], etc. Hence the distributed estimation algorithms need to be resilient to adversarial attacks in order to be more effective.

Different consensus algorithms resilient to adversarial attacks appear in the literature such as Mean-Subsequence-Reduced algorithm [11] and Median Consensus Algorithm [12]. These algorithms ensure consensus only for the normal agents, while the agents under attack may have arbitrary values. We are interested in a resilient distributed estimation algorithm, that will ensure that both the normal agents and the agents under attack can reach consensus over the true value of the parameter to be estimated. The *consensus+innovations* approach illustrated in [13] uses the consensus framework to design resilient algorithms for linear estimation. The Constant weight Saturated Innovation Update (CSIU) algorithm [14] is one such resilient estimation algorithm which ensures that all the agents are able to estimate the parameter of interest, provided less than three-tenth of the total agents are under attack. This was further improved in [15], where the Saturated Innovation Update (SIU) algorithm ensures all the agents' estimate converge to the desired parameter value provided the adversaries attack less than half of the total agents. Also in [14], a new term *resilience index* was used to provide a bound for the fraction of sensor nodes under attack.

Both the CSIU and SIU algorithms are designed on undirected graphs representing bidirectional communication links between the agents. In many practical scenarios, the power levels at which sensor nodes broadcast information or, their interference and noise patterns, differ from node to node [16], [17]. The communication between nodes in such cases is unidirectional which is aptly represented by a directed graph. Here we consider a time-invariant network topology with unidirectional communication links between agents. To the best of our knowledge, an extension of the consensus+innovations approach to directed graphs is non-existent in the literature, except for the recent work [18]. However, we observed that for the algorithm presented in [18], choosing appropriate parameters is not an easy task. In contrast, we propose an algorithm which guarantees convergence over a given range of parameter values. Also, unlike [18], where the set of adversarial agents and the unknown parameter are fixed, our proposed algorithm works even when the set of agents under attack and the unknown parameter changes with time.

The model of attack by the adversaries is designed on the idea of sensor spoofing [10] where the sensor readings of the agents under attack are corrupted through data falsification or

Shamik Bhattacharyya is with the Electrical Engineering Department, Indian Institute of Technology Madras, TN 600036, India (e-mail: ee18d005@smail.iitm.ac.in).

Kiran Rokade is with the Electrical and Computer Engineering Department, Cornell University, Ithaca, NY 14850, USA (e-mail: kvr36@cornell.edu).

Rachel K. Kalaimani is with the Electrical Engineering Department, Indian Institute of Technology Madras, TN 600036, India (e-mail: rachel@ee.iitm.ac.in).

false data injection. Note that such an attack on the agents is restricted to their sensors. In particular, the agents under attack can perform computations and communicate with their neighbours. Also the agents under attack by the adversaries are not known a-priori by the normal agents. Moreover we allow for a more general scenario where the adversaries may attack different agents over time. We present an algorithm, Resilient Estimation through Weight Balancing (REWB), which ensures that all agents asymptotically converge to the value to be estimated provided less than half of the total number of agents are affected by adversaries. The agents operate in a distributed manner using only the local information available to them. The main contribution of this paper is the proposed REWB algorithm which ensures that over a directed communication network, both the normal agents as well as the agents under attack asymptotically estimate the actual value of the unknown parameter in the presence of a sensor spoofing attack by the adversaries.

Technically, the contributions we make in this paper can be summarized as follows:

- We propose a novel REWB algorithm that estimates an unknown time-varying parameter with a decaying bound on its variations in the presence of sensor spoofing attacks by simultaneously balancing the unbalanced directed communication network (Algorithm 1). The REWB algorithm brings together the weight-balancing and consensus+innovation approaches over relative time-scales to achieve this.
- We show that the proposed REWB algorithm ensures convergence of each agent, both normal as well as those under attack, to the actual value of the unknown parameter provided less than half of the total agents are under attack at any given time (Theorem 1).
- As an intermediate result, we provide an explicit rate of convergence of the Laplacian of an unbalanced weighted digraph to the Laplacian of the associated balanced digraph (Lemma 1).

Notations. $\mathbb{R}$ denotes the set of *real* numbers, and $\mathbb{R}^N$ represents the N-dimensional Euclidean space. For any set $\mathcal{S}$, the *cardinality* of the set is denoted by $|\mathcal{S}|$. $\mathbf{1} := (1, 1, \ldots, 1)$ and $\mathbf{0} := (0, 0, \ldots, 0)$, of appropriate dimensions. For a real-valued vector v, v^T denotes the *transpose* of the vector, $||v||$ denotes its l_2-norm and $||v||_\infty$ denotes its ∞-norm. Similarly for a real-valued matrix M, M^T denotes the *transpose* of the matrix, and $||M||$ denotes its *spectral norm*. Among the *eigenvalues* of M, $\lambda_2(M)$ represents the *second lowest* eigenvalue of M in magnitude, while $\lambda_{\max}(M)$ denotes its largest eigenvalue in magnitude. For a real-valued vector v, $\text{diag}(v)$ represents a diagonal matrix with v as the main diagonal.

The rest of the paper is organised as follows. Section-II discusses the details of the problem such as the inter-agent communication network, the threat model of the adversaries and the concept of resilience index. Section-III starts with the development of the REWB algorithm using the weight-balancing approach, followed by the details of the algorithm, finally leading to our main result. Some numerical simulations

are presented in Section-IV to validate the performance of the REWB algorithm. Finally the conclusions are presented in Section-V.

II. PROBLEM FORMULATION

A. System Model

Consider a system of N agents where each agent is equipped with sensing, computing and communication capabilities - it can record measurements using its sensor, can perform computations using its own data and the information received from its neighbouring agents, and can also share its data with the neighbours. The aim of each agent is to estimate an unknown parameter $\theta^*(t) \in \mathbb{R}^M$ in a distributed manner even while some agents' sensor measurements are corrupted by adversaries. The precise model of sensor measurement corruption will be described shortly.

The communication among the agents is modelled as a directed graph $\Gamma = (\mathcal{V}, \mathcal{E})$, where the vertex set $\mathcal{V} = \{1, 2, \ldots, N\}$ represents the set of N agents. The set of directed edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ represents the information exchange links between the agents, where $(i, j) \in \mathcal{E}$ if agent j can send information to agent i. A *directed path* from i to j is the sequence of directed edges $(i, i_1), (i_1, i_2), \ldots, (i_p, j)$. The set of *in-neighbours* of agent j is defined as $\mathcal{N}_j = \{i \in \mathcal{V} : (j, i) \in \mathcal{E}\}$, and the corresponding *in-degree* is denoted as $d_j^{\text{in}} = |\mathcal{N}_j|$. The set of *out-neighbours* of agent-j is defined as $\mathcal{O}_j = \{i \in \mathcal{V} : (i, j) \in \mathcal{E}\}$, and the corresponding *out-degree* is denoted as $d_j^{\text{out}} = |\mathcal{O}_j|$. A corresponding diagonal matrix is defined as $D^{\text{out}} = \text{diag}(d_1^{\text{out}}, \ldots, d_N^{\text{out}})$. The *adjacency matrix*, A is a square matrix of size $N \times N$ defined as $A = [a_{ij}]$ where $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$ otherwise. The *Laplacian*, L is defined as $L := D^{\text{out}} - A$.

*Definition 1 (**Strongly Connected Graph**):* A directed graph is said to be *strongly connected* if there exists a directed path between every pair of vertices in the graph.

The flow of information is such that each agent i is able to receive information from its in-neighbours ($\mathcal{N}_i$), and send its own data to its out-neighbours ($\mathcal{O}_i$). So the information about any agent i can be received by another agent j either directly if a directed communication link exists between them, or indirectly via intermediate agent(s) provided the corresponding directed path exists. In order to ensure that the information about every agent i reaches every other agent $j, (i \neq j; i, j \in \mathcal{V})$, we introduce the following assumption.

Assumption 1: The directed graph Γ is *Strongly Connected*.

Now we proceed to model the effect of the adversaries, which attack the agents with a motive to disrupt the estimation process thus trying to prevent them from correctly estimating the value $\theta^*(t)$. At every time-step $t \geq 0$, the agents which are under attack by the adversaries are termed as the the set of *Bad* (or *affected*) agents, denoted as $\mathcal{B}_t$. The remaining agents form the set of *Good* (or *normal*) agents, denoted as $\mathcal{G}_t$. The set of bad agents can vary with time, and are also not known a-priori to the set of good agents. So for each $t \geq 0$, the set $\mathcal{V}$ is partitioned into $\mathcal{G}_t$ and $\mathcal{B}_t$. Thus $\mathcal{G}_t \cup \mathcal{B}_t = \mathcal{V}, \forall t \geq 0$. The attack model of the adversary is sensor spoofing attacks. Here the adversary introduces spurious signals into

the sensor readings non-invasively [10]. The corruption of sensor readings remains undetected by commonly used filters [19]. So even after nullifying the noise in sensor readings, the effect of the spoofing attack would still percolate into the measurements available to the agent. The agents use these sensor measurements to estimate the unknown parameter. In order to specifically highlight the effect of the adversary, we consider the sensor measurements available to the agents to be free of the effect of any measurement noise. The sensor measurements available to the agents under attack are arbitrary values manipulated by the adversary. Accordingly, we model the sensor measurements recorded by the agents as

$$\text{for all } i \in \mathcal{G}_t \text{ , } y_i(t) = \theta^*(t)$$
$$\text{for all } i \in \mathcal{B}_t \text{ , } y_i(t) = \theta^*(t) + \zeta_i(t) \qquad (1)$$

where $\zeta_i(t) \in \mathbb{R}^M$ is a vector of arbitrary values reflecting the effect of the adversaries. In the above model there is no boundedness assumption or stochastic approximation considered for $\zeta_i(t)$. This preserves the arbitrary nature of the data being manipulated by the adversary. So, if $|\mathcal{B}_t| = 0 \ \forall t \geq 0$, then $y_i(t) = \theta^*(t) \ \forall i \in \mathcal{V}$, and the estimation problem would be trivial as the sensor measurements directly provide the correct value of the parameter. Here we are interested in the non-trivial case where there exists some $t \geq 0$ such that $|\mathcal{B}_t| \neq 0$. This means some of the sensor measurements would be corrupted as $y_i(t) = \theta^*(t) + \zeta_i(t) \ \forall i \in \mathcal{B}_t$. So each agent needs to perform some additional computations in order to estimate the true value of $\theta^*(t)$ in a distributed manner. It should be noted that under this threat model, the bad agents are still able to perform their computations as per design as well as communicate with their neighbours.

The unknown time-varying parameter that is to be estimated is some physical quantity which can be measured by a sensor. So we can safely assume its Euclidean norm to be bounded. Moreover, we also assume that the variations in the unknown parameter asymptotically decay with time.

Assumption 2: The Euclidean norm of the unknown vector quantity that is to be estimated lies within an upper bound known to each agent :

$$\|\theta^*(t)\| \leq \Theta \qquad (2)$$

Also, the Euclidean norm of the variation in the unknown vector quantity has a decaying bound :

$$\|\theta^*(t+1) - \theta^*(t)\| \leq 1/(1+t)^{\theta_1} \qquad (3)$$

As a consequence of (3), we have the time varying parameter $\theta^*(t)$ eventually converging to some constant value $\hat{\theta}$. Specifically, $\theta^*(t) \to \hat{\theta}$ as $t \to \infty$.

Remark : The above assumption focuses on a particular subset of dynamic parameter estimation. Note that this is a modest extension from the *static* parameter estimation case.

Now to estimate $\theta^*(t)$ in a distributed manner, for all $t \geq 0$ each agent i maintains its own estimate of $\theta^*(t)$ denoted by $x_i(t) \in \mathbb{R}^M$, also referred to as the *state* of agent i. In order to update the state, each agent i follows the discrete-time single integrator dynamics :

$$x_i(t+1) = x_i(t) + u_i(t), t \geq 0 \qquad (4)$$

So at every time step, each agent i performs the following steps in the given sequence :

$S1$ - broadcasts its own estimate $x_i(t)$ to its out-neighbours $\mathcal{O}_i$

$S2$ - receives the estimates from its corresponding in-neighbours : $x_j(t), j \in \mathcal{N}_i$

$S3$ - collects sensor measurement of $\theta^*(t)$: $y_i(t)$

$S4$ - updates its own estimate following (4), where $u_i(t) = f(y_i(t), \{x_j(t), j \in \mathcal{N}_i\})$, and f is defined later in Section III-B.

In a distributed estimation problem with $x_i(t)$ as the state of agent i and $\theta^*(t)$ as the parameter of interest, the aim is to achieve

$$x_i(t) \longrightarrow \theta^*(t) \text{ as } t \to \infty \text{ , for all } i \in \mathcal{V} \qquad (5)$$

For the *resilient* estimation problem considered here, the additional challenge is to achieve (5) even in the presence of adversaries attacking some of the agents. In order to quantify how resilient an algorithm is to the adversarial attacks, we use a measure called the *Resilience Index* [15]. The resilience index (s) is an upper bound on the fraction of agents which are under attack by the adversaries at any time-step t. So, $s \geq \frac{|\mathcal{B}_t|}{N}$ for all $t \geq 0$, $s \in \mathbb{R}$. Thus $s = 0$ would indicate the trivial case where bad agents are totally absent. Having $s = 1$ allows for the possibility of all the agents being under attack at any time-step t.

In the sequel, we initially proceed to design an algorithm which provides us with a suitable value of $u_i(t) \ \forall t \geq 0$, for all $i \in \mathcal{V}$ introduced in (4). Then we present our main result on how the newly designed algorithm, under the assumptions made so far, achieves (5).

III. RESULTS

The aim of each agent in the multi-agent system under consideration, is to estimate an unknown static parameter in a distributed manner, as given in (5). The technique used for the distributed estimation of $\theta^*(t)$ is based on the consensus+innovations approach [13]. Based on this approach we proceed to design an algorithm such that the desired objective, $x_i(t) \longrightarrow \theta^*(t)$ as $t \to \infty$, for all $i \in \mathcal{V}$, is achieved through fulfilling the following two smaller goals simultaneously as $t \to \infty$:

$G1$: the state of each agent, $x_i(t)$, approaches the average of the states of all agents, $\bar{x}(t) := (1/N) \sum_{i=1}^{N} x_i(t)$

$G2$: $\bar{x}(t)$ approaches the unknown value to be estimated, $\theta^*(t)$.

A. Weight Balancing

In a Multi-Agent System (MAS), the communication network is usually modelled as a graph, with the nodes of the graph representing the agents and the edges between the nodes representing the corresponding communication links between the agents. When the flow of information between agents is *bi-directional*, the model used is an *undirected* graph. On the other hand, when the flow of information between agents is *unidirectional*, a *directed* graph (or *digraph*) is required
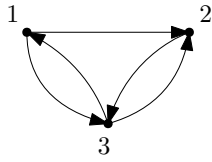
Fig. 1: A directed graph of 3 nodes

to model it. The directed edges of the digraph represent the unidirectional communication links while preserving their direction of information flow. A *weighted* graph has each of its edges assigned a real or integer value, referred to as *edge weights*. Unless specifically mentioned, the edge weights are taken as unity.

In case of an undirected graph, the sum of edge weights of the incoming edges is equal to the sum of the edge weights of the outgoing ones. But this balance in edge weights does not necessarily hold true in the case of a digraph. To overcome this imbalance, we need to find a suitable *weight vector* $w \in \mathbb{R}^N$, where each outgoing edge of agent i is assigned the weight w_i. These weights are said to *balance the graph* if $w_i d_i^{\text{out}} = \sum_{j \in \mathcal{N}_i} w_j$. The notion of a balanced graph is formally defined below.

*Definition 2 (**Balanced Graph**):* A graph Γ of N nodes is said to be *balanced* if there exists $w \in \mathbb{R}^N$ such that

$$L\mathbf{1} = \mathbf{0} \; , \; \mathbf{1}^T L = \mathbf{0}^T \qquad (6)$$

where $L := (D^{\text{out}} - A)\text{diag}(w)$

The weights $(w_1, w_2, \ldots, w_N)$ which balance a given digraph are called the *balancing weights* of the corresponding digraph [17]. Note that an undirected graph is inherently balanced with $w = \mathbf{1}$ as the vector of balancing weights. On the other hand, for a strongly connected digraph the vector of balancing weights is non-trivial. Note that this vector of balancing weights is also unique to the given digraph, up to scaling [17]. For example, consider the strongly connected digraph shown in Fig.1. For this digraph the vector of balancing weights is $w = [0.5, 1.5, 1]^T$, which is non-trivial and unique up to scaling.

The SIU algorithm proposed in [15] for resilient estimation does not work in general for directed graphs. This is later illustrated through a numerical example in Fig.4 in Section IV. We propose to use the idea of balancing weights described above to achieve resilient estimation over digraphs. For the directed graph Γ, we use the following update rule, proposed in [17], to iteratively compute a set of balancing weights. Let $w_i(t) \in \mathbb{R}$ denote the weight at node i at time-step t. The initial set of weights assigned to the agents satisfy : $w_i(0) \leq (1/d_{\text{max}}^{\text{out}})^{2\Phi+1}$, where $d_{\text{max}}^{\text{out}}$ represents the maximum out-degree and Φ represents the diameter of the concerned digraph [17]. Then for all $t \geq 0$,

$$w_i(t+1) = \frac{1}{2}w_i(t) + \frac{1}{d_i^{\text{out}}}\Big(\sum_{j \in \mathcal{N}_i} \frac{1}{2}w_j(t)\Big). \qquad (7)$$

Let $w(t) = (w_1(t), w_2(t), \ldots, w_N(t))$ represent the vector of node-weights at time-step t. Then the corresponding vector representation of (7) is given by :

$$w(t+1) = Pw(t) \qquad (8)$$

where $P := 0.5(I + (D^{\text{out}})^{-1}A)$. So for the limiting case, $\lim_{t \to \infty} w(t) = \lim_{t \to \infty} P^t w(0)$. Now from *Lemma 1* of [17], we know that $\lim_{t \to \infty} P^t$ exists, and that the sequence $\{w(t)\}_{t \geq 0}$ converges to the vector of balancing weights. So we define here the vector of weights which balances the digraph Γ as

$$w^\infty := \lim_{t \to \infty} w(t) = \lim_{t \to \infty} P^t w(0) \qquad (9)$$

The time-varying weighted Laplacian matrix is represented as

$$L(t) = (D^{\text{out}} - A)W(t), \text{ where } W(t) = \text{diag}(w(t)) \qquad (10)$$

Then the Laplacian matrix for the limiting case can be defined using the result from (9) in (10) as

$$L_\infty := (D^{\text{out}} - A)W_\infty, \text{ where } W_\infty = \text{diag}\{w^\infty\} \qquad (11)$$

Now as w^∞ balances the digraph, L_∞ satisfies the desired balancing condition expressed in (6). By definition of $L(t)$ we have $\mathbf{1}^T L(t) = \mathbf{0}^T$ for all $t \geq 0$. So to arrive at the desired balanced graph condition, we need $L(t)\mathbf{1} = \mathbf{0}$ which is eventually achieved with $L(t)$ converging to L_∞ as $t \to \infty$. Next we state a lemma which provides an explicit rate for this convergence and additionally provides the rate of decay of $L(t)\mathbf{1}$ to $\mathbf{0}$.

Lemma 1: Given $L(t) = (D^{\text{out}} - A)W(t)$ and $L_\infty = (D^{\text{out}} - A)W_\infty$, there exists constants $C > 0$ and $\eta \in (0, 1)$, such that $\|L(t) - D^{\text{out}}\| \leq C\eta^t$, $\|L(t)\mathbf{1}\| \leq C\eta^t$ for all $t \geq 0$.

The proof of Lemma 1 is given in Appendix A.

B. Algorithm

Now we introduce our algorithm, *Resilient Estimation through Weight Balancing* (REWB). It consists of two main update steps : one for the state of the agents, and the other for the node weights.

The updates performed by agent i at time-step t are :

i) Updating the estimate

$$\begin{aligned} x_i(t+1) = &\big(1 - \beta(t)w_i(t)d_i^{\text{out}}\big)x_i(t) \\ &+ \beta(t)\Big(\sum_{j \in \mathcal{N}_i} w_j(t)x_j(t)\Big) \\ &+ \alpha(t)k_i(t)\big(y_i(t) - x_i(t)\big) \end{aligned} \qquad (12)$$

ii) Updating the weight

$$w_i(t+1) = \frac{1}{2}w_i(t) + \frac{1}{d_i^{\text{out}}}\Big(\sum_{j \in \mathcal{N}_i} \frac{1}{2}w_j(t)\Big) \qquad (13)$$

The update law (12), used by agents to update their estimate of $\theta^*(t)$, is based upon the consensus+innovation approach. The first two terms, dealing with the agent's own and neighbours' estimates and the corresponding node-weights, constitute the *consensus* part of the update law. The third term, involving the measurements $y_i(t)$ and a scaling factor $k_i(t)$, constitute the *innovation* part. These two parts working simultaneously through the same update law help in achieving the smaller goals $G1$ and $G2$ mentioned before. The above update law uses step-size parameters $\beta(t)$ and $\alpha(t)$ to assign proper

weightage to its consensus and innovation parts respectively. The parameters are defined as :

$$\alpha(t) = \frac{\alpha_0}{(1+t)^{\alpha_1}}, \beta(t) = \frac{\beta_0}{(1+t)^{\beta_1}} \quad (14)$$

where $0 < \alpha_0 \leq 1/(1-2s)$, $0 < \beta_0 < \psi$, $0 < \beta_1 < \alpha_1 < \theta_1$. The constant ψ is defined as $\psi := 2/(Nd_{max}^{in}(d_{max}^{in} + d_{max}^{out}))$. Note that $\beta_1 < \alpha_1$ implies that, in the state update law (12), the weight of the innovation term decays faster than the weight of the consensus term.

The scaling factor, $k_i(t)$, is used in the innovation part in order to ensure that the effect of the adversaries on the state of an agent always remains bounded.

$$k_i(t) := \begin{cases} 1 & , \text{ if } \|y_i(t) - x_i(t)\| \leq \gamma(t) \\ \frac{\gamma(t)}{\|y_i(t)-x_i(t)\|} & , \text{ otherwise} \end{cases} \quad (15)$$

where $\gamma(t)$ is the output of a dynamical system defined as

$$\gamma(t) := \gamma_1(t) + \gamma_2(t) \quad (16)$$

The dynamics of $\gamma_1(t)$ and $\gamma_2(t)$ are defined as

$$\gamma_1(t+1) := \left(1 - c_1\mu(t) + (1+\sqrt{N})\alpha(t)\right)\gamma_1(t)$$
$$+ (1+\sqrt{N})\alpha(t)\gamma_2(t) + c_2\eta^t \quad (17)$$
$$\gamma_2(t+1) := \alpha(t)\gamma_1(t) + \left(1 - \alpha(t)(1-2s)\right)\gamma_2(t)$$
$$+ 1/(1+t)^{\theta_1} \quad (18)$$

where, $\mu(t) = \frac{\mu_0}{(t+1)^{\mu_1}}$, $\mu_0 > 0$, $\beta_1 < \mu_1 < \alpha_1$, $c_1 > 0$, $c_2 > 0$, $0 < \eta < 1$. The above time-varying system in two variables plays a crucial role in proving our main result. From the definition of $k_i(t)$ in (15), a corresponding diagonal matrix is defined as

$$K(t) := \text{diag}(k_1(t), k_2(t), \ldots, k_N(t)) \quad (19)$$

Let $x(t) = (x_1^T(t), x_2^T(t), \ldots, x_N^T(t)) \in \mathbb{R}^{N \times M}$ represent the matrix whose rows are the state vectors of the agents at time-step t. Also let $y(t) = (y_1^T(t), y_2^T(t), \ldots, y_N^T(t)) \in \mathbb{R}^{N \times M}$ represent the matrix whose rows are the sensor measurements of the agents at time-step t. Now we summarise our REWB algorithm as follows :

Algorithm 1 REWB

Given : Graph Γ, $\Theta \geq \|\theta^*(t)\|$, Resilience index s, and θ_1
Initialize : $0 < \alpha_0 \leq 1/(1-2s)$, $0 < \beta_0 < \psi$, $x(0) = 0$, $\mu_0 < (\lambda_m - \beta_0\lambda_M)\beta_0/(2c_1)$, $\gamma_1(0) = 0$, $\gamma_2(0) = \Theta$, $w_i(0) \leq \left(\frac{1}{d_{max}^{out}}\right)^{2\Phi+1}$
Choose : $0 < \beta_1 < \mu_1 < \alpha_1 < \theta_1$
for $t = 0, 1, \ldots$ **do**
- **record** $y(t)$
- **exchange** $x(t)$ among neighbouring agents
- **update** $x(t)$:
  $x(t+1) = (I - \beta(t)L(t))x(t) + \alpha(t)K(t)(y(t) - x(t))$
- **update** $w(t)$:
  $w(t+1) = Pw(t)$
- **update** $\gamma(t)$: using equations (16), (17) & (18)

end for

C. Main Result

The following theorem states our main result on resilient distributed estimation using the REWB algorithm.

Theorem 1: Suppose Assumptions 1 and 2 hold, and the effect of the adversaries is modelled as in (1). Then the REWB algorithm ensures that the state of every agent, $x_i(t)$ converges to $\theta^*(t)$, provided $s \in [0, \frac{1}{2})$. In particular,

$$\lim_{t\to\infty} (t+1)^{\delta_1}\|x_i(t) - \theta^*(t)\| = 0 , \text{ for all } i \in \mathcal{V} \quad (20)$$

where $0 \leq \delta_1 \leq \alpha_1 - \beta_1$
The proof of Theorem-1 is given in Appendix-C. Here we provide a remark on the above theorem.

Remark 1: From Theorem-1 it can be inferred that as long as less than half the total number of agents are under attack by the adversaries, the REWB algorithm ensures that each agent correctly estimates $\theta^*(t)$. Also note that all the agents, even the bad agents, achieve consensus and estimate $\theta^*(t)$ in a distributed manner.

Remark 2: As noted in Lemma 1, the dynamic weights $w(t)$ converge to the balancing weights at an exponential rate (η^t), whereas all time-varying signals in the dynamics of the state update rule converge at a polynomial rate $(\alpha(t) = \alpha_0/(1+t)^{\alpha_1}$ etc.). Thus, the weights converge faster, which are in turn used in the state update rule. This two time-scales approach facilitates convergence of the algorithm.

IV. SIMULATION RESULTS

We evaluate the performance of our proposed REWB algorithm through numerical simulations. A random network, consisting of 100 agents with directed edges, is generated where each possible edge has a probability of 0.5. It models the communication network among the agents. Each agent estimates a scalar time-varying parameter $\theta^*(t) = 25 + 1/(t+1)$ with $\Theta = 50$ and $\theta_1 = 1$. The required algorithm parameters are chosen as : $\alpha_0 = 0.01, \alpha_1 = 0.075, \beta_0 = 0.01, \beta_1 = 0.01, \mu_0 = 0.025, \mu_1 = 0.025, c_1 = 75, c_2 = 75$, and $\eta = 0.5$. The initial weights are chosen as $w_i(0) = 0.1 \; \forall i \in \mathcal{V}$.

The noise term $\zeta_i(t)$ models the effect of the adversaries on the sensor measurements of agent i. For each bad agent $i \in \mathcal{B}_t$, at every time step, $\zeta_i(t)$ takes on a random value uniformly distributed between 0 and $-\Theta$. Note that the REWB algorithm works for any other range also. We select the base resilience index to be $s = 0.405$, and correspondingly choose $|\mathcal{B}_t| = 40$. At first we consider two cases with respect to the set of agents under attack and observe the performance of the REWB algorithm. In Fig. 2a, $\mathcal{B}_t$ has a fixed set of agents, while in Fig. 2b, $\mathcal{B}_t$ is allowed to vary with time. Both the plots in Fig. 2 show the error in estimation of $\theta^*(t)$ by the agents, given by $\|x(t) - \theta^*(t)\mathbf{1}\|$. From the proof of Theorem 1 we have $|x_i(t) - \theta^*(t)| \leq \gamma(t), \; \forall i \in \mathcal{V}, \; \forall t \geq 0$. Then for a set of N agents, we have $\|x(t) - \theta^*(t)\mathbf{1}\| \leq \sqrt{N}\gamma(t)$. Fig. 2 shows that, regardless of adversaries attacking a fixed or varying set of agents, the REWB algorithm ensures that the estimation error always remains bounded by $\sqrt{N}\gamma(t)$, and consequently dies down asymptotically.

Next we use two different variations in operating conditions compared to the one used in Fig. 2a and observe their effect in
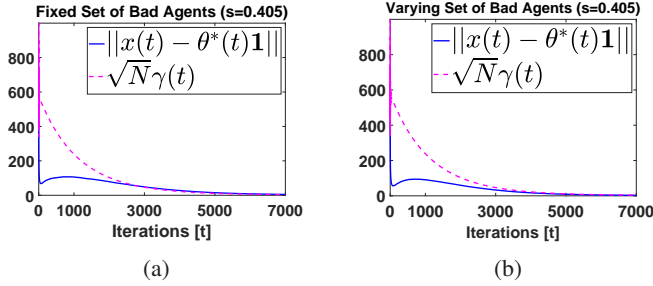
Fig. 2: Performance of REWB with adversarial attacks on 40 agents where the set of bad agents is (a) fixed, and (b) variable.
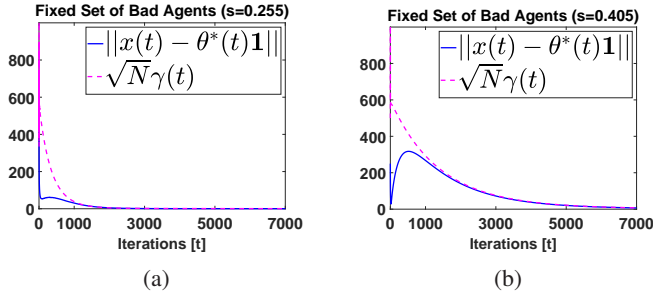

Fig. 3: Performance of REWB with (a) decrease in resilience index, and (b) increased manipulation in sensor measurements by adversaries.

Fig. 4: Performance of (a) the SIU [15] algorithm and (b) the proposed REWB algorithm over directed graphs

the performance of the REWB algorithm in Fig. 3. For the plot in Fig. 3a, the resilience index is decreased to $s = 0.255$ and correspondingly we choose $|\mathcal{B}_t| = 25$. As can be observed the estimation error dies down much faster with a decrease in s. Next for the plot Fig. 3b, we simulate an increase in the degree of manipulation done by the adversaries on the sensor measurements by increasing the noise level. We assign $\zeta_i(t) = 5\Theta \ \forall i \in \mathcal{B}_t, \forall t \geq 0$. As is evident from Fig. 3b, a high value of $\zeta_i(t)$ is also quite efficiently handled by the REWB algorithm, with the estimation error remaining bounded by $\sqrt{N}\gamma(t)$ at all times and eventually converging to 0. From Fig. 2 and Fig. 3 it is evident that the REWB algorithm ensures that even the bad agents are able to eventually correctly estimate the true value of $\theta^*(t)$, along with the good agents. This is in accordance with the Remark stated in Section III-C.

In Section III-A, we mentioned that the SIU algorithm in [15] does not give convergence in general when applied over a directed network of agents. In Fig. 4, we compare the performance of our REWB algorithm with the SIU algorithm in estimating the value of a scalar constant parameter $\theta^* \in \mathbb{R}$ over a directed network of 100 agents with $s = 0.405$. The two plots on the left show how the states of the agents behave with time, while the two plots on the right show the net estimation error. Fig. 4a shows how on applying the SIU algorithm, the states of the agents diverge away from each other and never achieve consensus, leading to a constant estimation error. On the other hand, Fig. 4b shows how our REWB algorithm not only ensures the agents reach consensus but they also correctly estimate the value of θ^*. This is made possible by the introduction of the weight balancing idea while designing the REWB algorithm. The dynamics of the time-varying
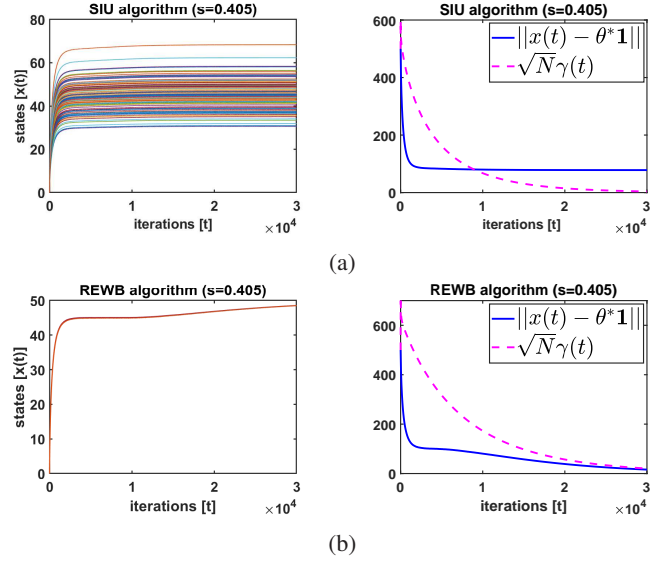
weights ensure that the weighted graph eventually approaches a balanced condition, and thus consensus is achieved.

V. CONCLUSION

In this paper we propose the Resilient Estimation through Weight Balancing (REWB) algorithm. It is a distributed estimation algorithm designed to work for a network of sensor nodes with directed communication links. The REWB algorithm is resilient to sensor spoofing type adversarial attacks while estimating an unknown time-varying parameter with a decaying bound on its variations. It ensures that along with the unaffected agents, even the agents under attack estimate the true value of the parameter in a distributed manner. The proposed algorithm is developed based on the consensus+innovation approach and uses the weight-balancing idea to ensure consensus over directed graph. Through numerical simulations it is shown that the proposed algorithm accurately estimates an unknown parameter under different attack conditions, provided less than half of the agents are under adversarial attack at any given point of time. Future direction of work is to consider other models of adversarial attacks.

APPENDIX A

Proof: [Proof of Lemma 1] By definition, P is a primitive matrix with spectral radius 1 [17]. Then by properties of primitive matrices : $\lim_{t \to \infty} P^t$ exists, and $\lim_{t \to \infty} P^t = P_\infty = uv^T$, where u, v are the right and left eigen-vectors of P corresponding to eigen-value 1, and $v^T u = 1$. Then from (7) and (9) we have :

$$w(t) - w^\infty = (P^t - P_\infty)w(0) \tag{21}$$

Using the properties of P discussed above we get $(P - P_\infty)^t = P^t - P_\infty$, for all $t \geq 1$. Then from (21) we have

$$w(t) - w^\infty = (P^t - P_\infty)w(0) = (P - P_\infty)^t w(0)$$

So by Theorem 8.3 in [20], there exists $c > 0, \eta < 1$ such that for all $t \geq 0$

$$\|w(t) - w^\infty\| \leq c\eta^t \|w(0)\| \tag{22}$$

Using (10) and (11), and applying the properties of sub-multiplicativity of spectral norm we have

$$\|L(t) - L_\infty\| \leq \|D^{\text{out}} - A\| \|W(t) - W_\infty\| \tag{23}$$

Now $W(t), W_\infty$ are diagonal matrices and for any diagonal matrix $M = \text{diag}(m_1, \ldots, m_N)$ we have $\|M\| \leq \|m\|_\infty \leq \|m\|$. Applying this to (23) and using the result from (22) we get

$$\|L(t) - L_\infty\| \leq C_L \eta^t \tag{24}$$

where $C_L = c\|D^{\text{out}} - A\| \|w(0)\| > 0$.
From (10) using the sub-multiplicativity property of the norm and the result from (24) we get

$$\|L(t)\mathbf{1}\| = \|(L(t) - L_\infty)\mathbf{1}\| \leq \sqrt{N} C_L \eta^t \tag{25}$$

By choosing $C \geq \sqrt{N} C_L$ and applying to (24) and (25) we get :

$$\|L(t) - L_\infty\| \leq C\eta^t \ , \ \|L(t)\mathbf{1}\| \leq C\eta^t$$

$\blacksquare$

APPENDIX B

Here we introduce some *intermediate lemmas* which will be useful in the proof of Theorem-1. At first, before proceeding to a time-varying system in two variables, we first analyse the dynamics of a scalar time-varying system. Consider a linear scalar time-varying system -

$$v_{t+1} = (1 - r_1(t)) v_t + r_2(t) \tag{26}$$

where

$$r_1(t) = \frac{c_1}{(1+t)^{\delta_1}}, r_2(t) = \frac{c_2}{(1+t)^{\delta_2}} \tag{27}$$

where c_1, c_2, δ_2 are positive constants, and $0 \leq \delta_1 \leq 1$.

The following result is based upon the results introduced in Lemma 25 in [21] and Lemma 3 in [15]. It provides a relation between δ_1 and δ_2 under which the dynamics of the scalar time-varying system in (26) is bounded. It also gives the condition under which the system dynamics converges to zero, and the corresponding rate of convergence.

Proposition 1: Consider the system given in (26) where $r_1(t), r_2(t)$ is given by (27). Then if $\delta_1 = \delta_2$, there exists $B > 0$, such that for sufficiently large non-negative integers $j < t$,

$$0 \leq \sum_{k=j}^{t-1} \left(\prod_{l=k+1}^{t-1} (1 - r_1(l)) \right) r_2(k) \leq B$$

Moreover the constant B can be chosen independently of t, j. Also, if $\delta_2 > \delta_1$, then for arbitrary fixed j,

$$\lim_{t\to\infty} \sum_{k=j}^{t-1} \left(\prod_{l=k+1}^{t-1} (1 - r_1(l)) \right) r_2(k) = 0$$

and correspondingly $\lim_{t\to\infty} (t+1)^{\delta_0} v_t = 0$ for all $0 \leq \delta_0 < \delta_2 - \delta_1$, and for all initial conditions v_0.

The following result provides the rate of convergence of a scalar system modified from (26).

Proposition 2 (Lemma 4 in [15]): Consider the scalar time-varying linear system :

$$v_{t+1} = (1 - c_3 r_2(t) + c_4 r_1(t)) v_t + c_5 r_1(t) \tag{28}$$

where $r_1(t), r_2(t)$ are given by :

$$r_1(t) = \frac{c_1}{(1+t)^{\delta_1}}, r_2(t) = \frac{c_2}{(1+t)^{\delta_2}}$$

where $c_1, c_2, \ldots, c_5 > 0$, and $0 < \delta_2 < \delta_1 < 1$. The system in (28) satisfies $\lim_{t\to\infty} (t+1)^{\delta_0} v_t = 0$ for all $0 \leq \delta_0 < \delta_1 - \delta_2$, and for all initial conditions v_0.

Now by using the results above we introduce the following lemma which proves the convergence of $\gamma_1(t)$ and $\gamma_2(t)$ introduced in (17) and (18).

Lemma 2: The system in (17) and (18) satisfies

$$\lim_{t\to\infty} (t+1)^{\delta_0} \gamma_1(t) = 0 \tag{29}$$

$$\lim_{t\to\infty} (t+1)^{\delta_0} \gamma_2(t) = 0 \tag{30}$$

where $0 \leq \delta_0 < \alpha_1 - \mu_1$

Proof: Step 1 : As $\alpha(t), \mu(t)$ are decreasing in t, and $\alpha_1 > \mu_1$, there exists a finite $T > 0$ such that for all $t > T$

$$\begin{aligned} 0 &\leq 1 - (1 - 2s)\alpha(t) \leq 1 \\ 0 &\leq 1 - c_1\mu(t) + (1 + \sqrt{N})\alpha(t) \leq 1 \end{aligned} \tag{31}$$

From (18) we can express $\gamma_2(t)$ as

$$\gamma_2(t) = \prod_{\tau=T}^{t-1} (1 - (1 - 2s)\alpha(\tau))\gamma_2(T) +$$

$$\sum_{\tau=T}^{t-1} \left(\prod_{j=\tau+1}^{t-1} (1 - (1 - 2s)\alpha(j)) \right) \left(\alpha(\tau)\gamma_1(\tau) + \frac{1}{(1+\tau)^{\theta_1}} \right). \tag{32}$$

Let $s(t) := \sum_{\tau=T}^{t-1} \left(\prod_{j=\tau+1}^{t-1} (1 - (1 - 2s)\alpha(j)) \right) \frac{1}{(1+\tau)^{\theta_1}}$. Using the second part of Proposition 1, we obtain : $s(t) \to 0$ as $t \to \infty$. Hence, $\exists T > 0$ such that $|s(t)| \leq \gamma_1(T) \ \forall t \geq T$. Using this, along with (31), in (32) provides

$$|\gamma_2(t)| \leq |\gamma_2(T)| + \sigma_1 \sup_{l\in[T,t]} |\gamma_1(l)| \tag{33}$$

for some constant $\sigma_1 > 0$.

Step 2 : From (17) and (31) we have

$$|\gamma_1(t+1)| \leq (1 - c_1\mu(t) + (1 + \sqrt{N})\alpha(t)) \sup_{l\in[T,t]} |\gamma_1(l)| + (1 + \sqrt{N})\alpha(t)|\gamma_2(t)| + c_2\eta^t. \tag{34}$$

Applying (33) we get

$$\therefore |\gamma_1(t+1)| \leq (1 - c_1\mu(t) + \sigma_2\alpha(t)) \sup_{l\in[T,t]} |\gamma_1(l)| + \sigma_3\alpha(t) + c_2\eta^t$$

where $\sigma_2 = (1 + \sqrt{N})(1 + \sigma_1)$ and $\sigma_3 = (1 + \sqrt{N})|\gamma_2(T)|$. Now as $0 < \eta < 1$, there exists $\sigma_4 > 0$ such that for all $t > 0$

$$\sigma_3\alpha(t) + c_2\eta^t < \sigma_4\alpha(t) \tag{35}$$

$\therefore |\gamma_1(t+1)| \leq \left(1 - c_1\mu(t) + \sigma_2\alpha(t)\right) \sup_{l \in [T,t]} |\gamma_1(l)| + \sigma_4\alpha(t)$

We define a new system -

$$m(t+1) = \max\left(m(t), \left(1 - c_1\mu(t) + \sigma_2\alpha(t)\right)m(t) + \sigma_4\alpha(t)\right) \quad (36)$$

for all $t > T$ and initial condition $m(T) = \gamma_1(T)$. So by definition of $m(t)$ we have :

$$m(t) \geq \sup_{l \in [T,t]} |\gamma_1(l)| \quad (37)$$

We define another new system :

$$\tilde{m}(t+1) = \left(1 - c_1\mu(t) + \sigma_2\alpha(t)\right)\tilde{m}(t) + \sigma_4\alpha(t)) \quad (38)$$

for all $t > T$ and initial condition $\tilde{m}(T) = m(T) = \gamma_1(T)$. By definition $\tilde{m}(T) \geq 0$. Also for $t > T$, from (31) we have $1 - c_1\mu(t) + \sigma_2\alpha(t) \geq 0$. Then $\tilde{m}(t) \geq 0$ for all $t \geq T$. Now using Proposition 1 and (38) we have

$$\lim_{t \to \infty} \tilde{m}(t) = 0$$

Step 3 : By virtue of $\tilde{m}(t)$ being a non-negative sequence which converges to 0, there exists a time $T_1 \geq T$ such that $\tilde{m}(T_1 + 1) \leq \tilde{m}(T_1)$. We choose the smallest value among all such possible $T_1 \geq T$. Then from the definition of T_1 we have $\tilde{m}(T) < \tilde{m}(T+1) < \ldots < \tilde{m}(T_1)$. So from (36), $m(t) = \tilde{m}(t)$ for all $t \in [T, T_1]$.

$$\therefore m(t) \leq m(T_1) \text{ , for all } t \in [T, T_1] \quad (39)$$

Also by definition of $T_1, m(t)$ we have $m(T_1 + 1) = m(T_1)$. Let for all $t \geq T_1$

$$\pi(t) := m(T_1) - \left(1 - c_1\mu(t) + \sigma_2\alpha(t)\right)m(T_1) - \sigma_4\alpha(t)$$

By algebraic manipulation

$$\pi(t) = \left(\frac{\sigma_5}{(t+1)^{\mu_1}} - \frac{\sigma_6}{(t+1)^{\alpha_1}}\right)m(T_1)$$

where $\sigma_5 = c_1\mu_0 > 0$, $\sigma_6 = \left(\sigma_2 + \frac{\sigma_4}{m(T_1)}\right)\alpha_0 > 0$.
Now $m(T_1) = 0$, and since $m(T_1 + 1) = m(T_1)$ we have

$$\pi(T_1) \geq 0 \iff T_1 \geq \left(\frac{\sigma_6}{\sigma_5}\right)^{1/(\alpha_1 - \mu_1)} - 1$$

So we have $\pi(t) \geq 0$ for all $t \geq T_1$. Then using (36) we have

$$m(t) = m(T_1) \text{ , for all } t \geq T_1 \quad (40)$$

Now combining the results from (37), (39) and (40) we get

$$\sup_{t \geq 0} |\gamma_1(t)| < \infty \quad (41)$$

Step 4 : Let $\sup_{t \in [T,t]} |\gamma_1(t)| = B_1 < \infty$. Then from (33) we have

$$\sup_{t \geq T} |\gamma_2(t)| \leq |\gamma_2(T)| + \sigma_1 B_1 < \infty \quad (42)$$

As $T < \infty$, we have

$$\sup_{t \in [0,T]} |\gamma_2(t)| < \infty \quad (43)$$

So combining (42) and (43) we have

$$\sup_{t \geq 0} |\gamma_2(t)| < \infty \quad (44)$$

Step 5 : Let $\sup_{t \geq 0} |\gamma_2(t)| = B_2 < \infty$. Then for sufficiently large t, from (34) we have

$$|\gamma_1(t+1)| \leq |1 - c_1\mu(t) + (1+\sqrt{N})\alpha(t)||\gamma_1(t)|$$
$$+ (1+\sqrt{N})\alpha(t)B_2 + c_2\eta^t$$

Now as $0 < \eta < 1$, there exists $C_\eta > 0$ and $T_\eta > 0$ such that for all $t > T_\eta$

$$(1+\sqrt{N})B_2\alpha(t) + c_2\eta^t < C_\eta\alpha(t) \quad (45)$$

For a suitable choice of $C_\eta = \sigma_7$, (45) holds for all $t > 0$.

$$\therefore |\gamma_1(t+1)| \leq |1 - c_1\mu(t) + (1+\sqrt{N})\alpha(t)||\gamma_1(t)| + \sigma_7\alpha(t) \quad (46)$$

As (46) falls under the purview of Proposition 2, we can infer (29).

Step 6 : As a consequence of Proposition 2, there exists $R_1 > 0$ such that $|\gamma_1(t)| < R_1/(t+1)^{\delta_0}$ for all $0 \leq \delta_0 < \alpha_1 - \mu_1$. We choose $\delta_0 \leq \min\{\alpha_1 - \mu_1, \theta_1 - \alpha_1\}$, which ensures $(1+t)^{-\theta_1} \leq (1+t)^{-(\alpha_1+\delta_0)}$. Thus for sufficiently large t we have -

$$|\gamma_2(t+1)| \leq \left(1 - (1-2s)\alpha(t)\right)|\gamma_2(t)| + \frac{\alpha_0 R_1}{(t+1)^{\alpha_1+\delta_0}} \quad (47)$$

As (47) falls under the purview of Proposition 1, we have

$$\lim_{t \to \infty} (t+1)^{\delta_0'}\gamma_2(t) = 0$$

for all $0 \leq \delta_0' < \delta_0$.
By making δ_0 arbitrarily close to $\alpha_1 - \mu_1$ we get (30).

∎

Let us define a new matrix J as $J := I - \frac{1}{N}\mathbf{1}\mathbf{1}^T$.
The following lemma provides a bound for $\|J - \beta(t)L^\infty\|$.

Lemma 3: Given $c_1 > 0$, $L_\infty = \left(D^{\text{out}} - A\right)W_\infty$ where $W_\infty = \text{diag}\left(w^\infty\right)$, $\beta(t) = \frac{\beta_0}{(1+t)^{\beta_1}}$, $\mu(t) = \frac{\mu_0}{(1+t)^{\mu_1}}$ where $0 < \beta_0 < \psi$, $\mu_0 > 0$ and $0 < \beta_1 < \mu_1 < 1$, there exists $T > 0$ such that $\|J - \beta(t)L_\infty\| \leq 1 - c_1\mu(t) < 1$ for all $t \geq T$.

Proof: Using the property $\mathbf{1}^T L_\infty = 0$ we can write

$$\|J - \beta(t)L_\infty\|^2 = \lambda_{\max}\left(J - \beta(t)M_2 + \beta^2(t)M_3\right)$$
$$= \sup_{x \in \mathbb{R}^N, ||x||=1} x^T\left(J - \beta(t)M_2 + \beta^2(t)M_3\right)x \quad (48)$$

where $M_2 = \left(L_\infty^T + L_\infty\right)$ and $M_3 = L_\infty^T L_\infty$. Now by definition $L_\infty\mathbf{1} = 0$. So we have

$$M_2\mathbf{1} = 0 \text{ ; } M_3\mathbf{1} = 0 \quad (49)$$

Also, M_2 and M_3 are the Laplacians of the corresponding graph. As the graphs are strongly connected, we can infer :

$$\lambda_2\left(M_2\right) > 0 \text{ ; } \lambda_2\left(M_3\right) > 0$$

i.e the 2nd lowest eigen-value of each of the Laplacians is strictly positive.
Let $x \in \text{span}\{\mathbf{1}\} \equiv x = \alpha\mathbf{1}, \alpha \in \mathbb{R}$. Then using (49) we have

$$x^T\left(I - \frac{1}{N}\mathbf{1}\mathbf{1}^T - \beta(t)M_2 + \beta^2(t)M_3\right)x = 0 \quad (50)$$

Now suppose $x \in \text{span}\{\mathbf{1}^\perp\} \equiv x^T\mathbf{1} = 0$. Then we have

$$x^T\left(I - \frac{1}{N}\mathbf{1}\mathbf{1}^T - \beta(t)M_2 + \beta^2(t)M_3\right)x \tag{51}$$
$$\leq \left(1 - (\beta(t)\lambda_m - \beta^2(t)\lambda_M)\right)x^T x$$

where $\lambda_m = \lambda_2(M_2)$ and $\lambda_M = \lambda_{\max}(M_3)$.
Having $\beta_0 < \psi$ and $\beta_1 < 1$ ensures that $\beta(t) < \lambda_m/\lambda_M$, and in turn $\|I - \frac{1}{N}\mathbf{1}\mathbf{1}^T - \beta(t)L_\infty\|^2 < 1 \ \forall t \geq 0$. We choose an ϵ such that $0 < \epsilon \leq \lambda_m - \beta(t)\lambda_M$. Then for all $t \geq 0$

$$\beta(t)\lambda_m - \beta^2(t)\lambda_M \geq \beta(t)\epsilon > 0 \tag{52}$$

Then from (48), (50), (51) and (52) we have

$$\|J - \beta(t)L_\infty\| \leq \sqrt{1 - \beta(t)\epsilon} < 1 \tag{53}$$

Now, as $\mu_1 > \beta_1$, there exists time $T > 0$ such that for all $t > T$

$$\frac{1}{(1+t)^{\mu_1 - \beta_1}} \leq \frac{\epsilon\beta_0}{2c_1\mu_0} \implies 2c_1\mu(t) \leq \epsilon\beta(t)$$
$$\implies 1 - \epsilon\beta(t) \leq 1 - 2c_1\mu(t) + c_1^2\mu^2(t)$$
$$\therefore \sqrt{1 - \epsilon\beta(t)} \leq 1 - c_1\mu(t) \tag{54}$$

Also as $c_1 > 0$, we have $1 - c_1\mu(t) < 1$. Then from (53) and (54) we have
$$\|J - \beta(t)L_\infty\| \leq 1 - c_1\mu(t) < 1 \ , \ t \geq T \qquad \blacksquare$$

APPENDIX C

Proof: [Proof of Theorem 1] Let $\bar{x}(t) \in \mathbb{R}^{1 \times M}$ denote the average of the states of the agents : $\bar{x}(t) = (1/N)\mathbf{1}^T x(t)$. We define $p(t)$ as the difference between the state of the agents and their average, and $q(t)$ as the difference between the average value and the unknown parameter $\theta^*(t)$.

$$p(t) := x(t) - \mathbf{1}\bar{x}(t), p(t) \in \mathbb{R}^{N \times M} \tag{55}$$
$$q(t) := \bar{x}^T(t) - \theta^*(t), q(t) \in \mathbb{R}^M. \tag{56}$$

Now the norm of the difference between the state of each agent and $\theta^*(t)$ can be upper bounded as

$$\|x_i(t) - \theta^*(t)\| \leq \|x_i(t) - \bar{x}^T(t)\| + \|\bar{x}^T(t) - \theta^*(t)\|$$
$$\implies \|x_i(t) - \theta^*(t)\| \leq \|p(t)\| + \|q(t)\| \text{ for all } i \in \mathcal{V}. \tag{57}$$

To show that the states converge to $\theta^*(t)$, we express $\|x_i(t) - \theta^*(t)\| \leq \gamma(t)$ and show that $\gamma(t)$ has a dynamics that converges to 0. In what follows, we firstly we use the method of induction to show that

$$\|p(t)\| \leq \gamma_1(t) \text{ and } \|q(t)\| \leq \gamma_2(t) \text{ for all } t \geq 0 \tag{58}$$

and in the process also define the dynamics of $\gamma_1(t)$ and $\gamma_2(t)$. After that we express these dynamics as a linear time-varying system which is asymptotically stable. From there, using (57), (16) and (58) we arrive at our desired result.
Dynamics of $x(t) - \mathbf{1}\bar{x}(t)$:
$$p(t+1) = x(t+1) - \mathbf{1}\bar{x}(t+1) = Jx(t+1)$$

$$\implies p(t+1) = M_1 + \alpha(t)JK(t)(y(t) - x(t)) \tag{59}$$

where $J := I - \frac{1}{N}\mathbf{1}\mathbf{1}^T$, and $M_1 := J(I - \beta(t)L(t))x(t)$. Expanding M_1 and using $\mathbf{1}^T L(t) = 0$ and $J\mathbf{1} = 0$, followed

by applying norm and its properties of triangle-inequality and sub-multiplicativity we get

$$\|M_1\| \leq \|(J - \beta(t)L_\infty)\|\|p(t)\| + \beta(t)\big(\|L(t)\mathbf{1}\|\|q(t)\| + \|(L(t) - L_\infty)\|\|p(t)\| + \|L(t)\mathbf{1}\|\|\theta^*(t)\|\big) \tag{60}$$

Now applying Lemmas 1 and 3, and Assumption-2 in (60) :

$$\|M_1\| \leq (1 - c_1\mu(t))\|p(t)\| + C\beta(t)\eta^t\big(\|p(t)\| + \|q(t)\| + 1 + \Theta\big). \tag{61}$$

Applying norm to (59) and using (19), $\|J\| = \mathbf{1}$ we get

$$\|p(t+1)\| \leq (1 - c_1\mu(t) + C\beta(t)\eta^t)\|p(t)\| \tag{62}$$
$$+ C\beta(t)\eta^t\big(1 + \Theta + \|q(t)\|\big) + \sqrt{N}\alpha(t)\gamma(t).$$

Dynamics of $\bar{x}^T(t) - \theta^*(t)$:

$$q(t+1) = \bar{x}^T(t+1) - \theta^*(t+1) = \bar{x}^T(t) - \theta^*(t)$$
$$+ \frac{\alpha(t)}{N}\mathbf{1}^T K(t)(y(t) - x(t)) + \underbrace{\theta^*(t+1) - \theta^*(t)}_{\Delta\theta^*(t+1)} \tag{63}$$

We define two diagonal matrices $K_\mathcal{G}(t), K_\mathcal{B}(t)$ where $[K_\mathcal{G}(t)]_{ii} := k_i(t)$ if $i \in \mathcal{G}_t$ and $[K_\mathcal{B}(t)]_{ii} := k_i(t)$ if $i \in \mathcal{B}_t$, and rest of the entries are equal to 0.

$$\therefore K_\mathcal{B}(t) + K_\mathcal{G}(t) = K(t) \text{ for all } t \geq 0 \tag{64}$$

Using (1) and (55) in (63), followed by applying the l_2-norm and its properties of triangle-inequality and sub-multiplicativity we get

$$\|q(t+1)\| \leq \|1 - \frac{\alpha(t)}{N}\sum_{i \in \mathcal{G}_t} k_i(t)\|\|q(t)\| + \|\Delta\theta^*(t+1)\|$$
$$+ \frac{\alpha(t)}{N}\|\sum_{i \in \mathcal{G}_t} k_i(t)(x_i(t) - \bar{x}^T(t))\|$$
$$+ \frac{\alpha(t)}{N}\|\sum_{i \in \mathcal{B}_t} k_i(t)(y_i(t) - x_i(t))\| \tag{65}$$

Dynamics of $\gamma_1(t)$ and $\gamma_2(t)$ via method of Induction :
By the method of induction we wish to show (58), and in the process arrive at the dynamics of $\gamma_1(t)$ and $\gamma_2(t)$.
Step 1 : at $t = 0$, $\|p(0)\| = 0$ as $x(0) = \mathbf{0}$, and $\|q(0)\| = \Theta$ as $\|\theta^*(t)\| < \Theta$. Choosing $\gamma_1(0) = 0, \gamma_2(0) = \Theta$ we have

$$\|p(0)\| \leq \gamma_1(0) \ , \ \|q(0)\| \leq \gamma_2(0) \tag{66}$$

Step 2 : for some $t > 0$ we assume that

$$\|p(t)\| \leq \gamma_1(t) \ , \ \|q(t)\| \leq \gamma_2(t) \tag{67}$$

Step 3 : based on the assumption (67) from Step-2, we need to show that

$$\|p(t+1)\| \leq \gamma_1(t+1) \ , \ \|q(t+1)\| \leq \gamma_2(t+1) \tag{68}$$

Applying (67) to (62) and using (16) we have

$$\|p(t+1)\| \leq (1 - c_1\mu(t) + C\beta(t)\eta^t + \sqrt{N}\alpha(t))\gamma_1(t)$$
$$+ (C\beta(t)\eta^t + \sqrt{N}\alpha(t))\gamma_2(t) + C(1 + \Theta)\beta(t)\eta^t$$

Now as $\eta < 1$, there exists $c_2 > 0$ and $T > 0$ such that for all $t > T$

$$C(1 + \Theta)\beta(t)\eta^t \leq c_2\eta^t \ , \text{ and } C\beta(t)\eta^t \leq \alpha(t) \tag{69}$$

By appropriate choice of $\beta_0 < \frac{\alpha_0}{C}$, $c_2 > C(1 + \Theta)\beta_0$ and $\mu_0 < (\lambda_m - \beta_0 \lambda_M)\beta_0/(2c_1)$, (69) and (54) holds for all $t > 0$

$$\therefore \|p(t+1)\| \leq (1 - c_1\mu(t) + (1 + \sqrt{N})\alpha(t))\gamma_1(t) \\ + (1 + \sqrt{N})\alpha(t)\gamma_2(t) + c_2\eta^t \tag{70}$$

We define the dynamics of $\gamma_1(t)$ as -

$$\gamma_1(t+1) := (1 - c_1\mu(t) + (1 + \sqrt{N})\alpha(t))\gamma_1(t) \\ + (1 + \sqrt{N})\alpha(t)\gamma_2(t) + c_2\eta^t \tag{71}$$

Using (16), (57), and (67)

$$k_i(t) = 1 \text{ for all } i \in \mathcal{G}_t \ [\because y_i(t) = \theta^*(t) \forall i \in \mathcal{G}_t] \tag{72}$$

Now from (64), (65), (72) and further using (16), (3) and $\alpha_0 < 1/(1 - 2s)$, $s < 1/2$ we get

$$\|q(t+1)\| \leq (1 - \alpha(t)(1 - 2s))\gamma_2(t) + \alpha(t)\gamma_1(t) + 1/(1+t)^{\theta_1} \tag{73}$$

We define the dynamics of $\gamma_2(t)$ as

$$\gamma_2(t+1) := \alpha(t)\gamma_1(t) + (1 - \alpha(t)(1 - 2s))\gamma_2(t) + 1/(1+t)^{\theta_1} \tag{74}$$

Then from (70), (71) and (73), (74) we can infer (68). Thus from steps 1,2 and 3 we have (58).

Asymptotic stability of $\gamma_1(t)$ and $\gamma_2(t)$:
Using Lemma 2 we can say that a linear time-varying system with state-variables $\gamma_1(t)$ and $\gamma_2(t)$, and state dynamics given by (71) and (74) respectively, is asymptotically stable, i.e $\lim_{t\to\infty}(t+1)^{\delta_0}\gamma_1(t) = 0$, $\lim_{t\to\infty}(t+1)^{\delta_0}\gamma_2(t) = 0$. ∎

APPENDIX D

For our REWB algorithm, the value of a constant ψ, which is an upper bound to the parameter β_0, is defined as $\psi := 2/(N d_{\max}^{in}(d_{\max}^{in} + d_{\max}^{out}))$. Here we provide a detailed proof of how we arrived at this value of ψ.

We have $0 < \beta_0 < \lambda_2(L_\infty^T + L_\infty)/\lambda_{\max}(L_\infty^T L_\infty)$. Now using Gershgorin's Disk Theorem we can write :

$$\lambda_{\max}(L_\infty^T L_\infty) \leq 2\max_i [L_\infty^T L_\infty]_{ii}$$
$$= 2\max_i \left([L_\infty]_{ii}^2 + \sum_{j \in \mathcal{N}_i, j \neq i}[L_\infty]_{ij}^2\right)$$
$$= 2\max_i \left((d_i^{out}w_i^\infty)^2 + \sum_{j \in \mathcal{N}_i, j \neq i}(w_j^\infty)^2\right)$$

Now using $d_i^{out}w_i^\infty \leq 1$ from [17], and $\frac{1}{d_i^{out}} \leq 1$, we have :

$$\lambda_{\max}(L_\infty^T L_\infty) \leq 2\max_i \left(1 + \sum_{j \in \mathcal{N}_i, j \neq i}(\frac{1}{d_i^{out}})^2\right) \leq 2d_{\max}^{in}$$

From the results in [22], we can say : $\lambda_2(L_\infty^T + L_\infty) > \frac{4}{N(d_{\max}^{in} + d_{\max}^{out})}$.

$$\therefore \frac{2}{N d_{\max}^{in}(d_{\max}^{in} + d_{\max}^{out})} < \frac{\lambda_2(L_\infty^T + L_\infty)}{\lambda_{\max}(L_\infty^T L_\infty)}$$

So defining $\psi := 2/(N d_{\max}^{in}(d_{\max}^{in} + d_{\max}^{out}))$ and choosing any non-zero positive value of $\beta_0 < \psi$ satisfies the requirement of our REWB algorithm.

APPENDIX E

In the proof for Lemma 3 in Appendix B, we use the fact that the second eigenvalues of the matrices M_2 and M_3 are non-zero, where $M_2 = (L_\infty^T + L_\infty)$ and $M_3 = L_\infty^T L_\infty$. Here we provide a reasoning for the same.

- zero column sum : from (11) and (6) we have $\mathbf{1}^T L_\infty = \mathbf{0}, L_\infty \mathbf{1} = \mathbf{0}$. Using these, we get

$$\mathbf{1}^T M_2 = \mathbf{1}^T L_\infty^T + \mathbf{1}^T L_\infty = \mathbf{0}; \mathbf{1}^T M_3 = \mathbf{1}^T L_\infty^T L_\infty = \mathbf{0}$$

- positive diagonal elements :

$$[M_2]_{ii} = [L_\infty^T]_{ii} + [L_\infty]_{ii} = 2[L_\infty]_{ii} > 0$$
$$[M_3]_{ii} = [L_\infty^T]_{i:}[L_\infty]_{:i} = \sum_{j=1}^{N}[L_\infty]_{ji}^2 > 0$$

where $[M]_{ii}, [M]_{i:}, [M]_{:i}$ represent the (i,i)-th element, i-th row, and i-th column of matrix M respectively.
- non-diagonal elements in M_2 : $[M_2]_{ij} = [L_\infty]_{ji} + [L_\infty]_{ij}$.
- non-diagonal elements in M_3 :

$$[M_3]_{ij} = [L_\infty^T]_{i:}[L_\infty]_{:j} = \sum_{k=1}^{N}[L_\infty]_{ki}[L_\infty]_{kj}$$

From the expression of the entries of M_2 and M_3, one can deduce that these matrices will have a nonzero entry in the ijth position if the digraph has an edge between i and j. This shows that the connectivity of the graph corresponding to L_∞ would be preserved in the new graph corresponding to M_2 and M_3. Now, as M_2 and M_3 are valid Laplacians, and their corresponding graphs are connected, we can infer that the second eigenvalues of M_2 and M_3 are non-zero.

REFERENCES

[1] L. Hamami and B. Nassereddine, "Application of wireless sensor networks in the field of irrigation: A review," *Computers and Electronics in Agriculture*, vol. 179, p. 105 782, 2020.

[2] C. Habib, A. Makhoul, R. Darazi, and R. Couturier, "Health risk assessment and decision-making for patient monitoring and decision-support using wireless body sensor networks," *Information Fusion*, vol. 47, pp. 10–22, 2019.

[3] E. Fadel, V. Gungor, L. Nassef, N. Akkari, M. A. Malik, S. Almasri, and I. F. Akyildiz, "A survey on wireless sensor networks for smart grid," *Computer Communications*, vol. 71, pp. 22–33, 2015.

[4] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[6] S. He, H.-S. Shin, S. Xu, and A. Tsourdos, "Distributed estimation over a low-cost sensor network: A review of state-of-the-art," *Information Fusion*, vol. 54, pp. 21–43, 2020.

[7] Haowen Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[8] N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *Proceedings of the 2012 ACM Symposium on Principles of Distributed Computing*, 2012, pp. 365–374.

[9] B. Chen, L. Yu, D. W. Ho, and W.-A. Zhang, "Resilient consensus through event-based communication," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 471–482, 2020.

[10] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[11] S. M. Dibaji and H. Ishii, "Resilient consensus of second-order agent networks: Asynchronous update rules with delays," *Automatica*, vol. 81, pp. 123–132, 2017.

[12] H. Zhang and S. Sundaram, "A simple median-based resilient consensus algorithm," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 1734–1741.

[13] S. Kar and J. M. F. Moura, "Consensus + innovations distributed inference over networks," *IEEE Signal Processing Magazine*, pp. 99–109, 2013.

[14] Y. Chen, S. Kar, and J. M. F. Moura, "Resilient distributed estimation : Exponential convergence under sensor attacks," *Proceedings for the IEEE Conference on Decision and Control 2018*, pp. 7275–7282, 2018.

[15] ——, "Resilient distributed estimation : Sensor attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3772–3779, 2019.

[16] A. D. Domínguez-García and C. N. Hadjicostis, "Distributed strategies for average consensus in directed graphs," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 2011, pp. 2124–2129.

[17] A. Makhdoumi and A. Ozdaglar, "Graph balancing for distributed subgradient methods over directed graphs," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 1364–1371.

[18] M. Meng, X. Li, and G. Xiao, "Distributed estimation under sensor attacks: Linear and nonlinear measurement models," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 156–165, 2021.

[19] A. Barua and M. A. Al Faruque, "Special session: Noninvasive sensor-spoofing attacks on embedded and cyber-physical systems," in *2020 IEEE 38th International Conference on Computer Design (ICCD)*, 2020, pp. 45–48.

[20] J. P. Hespanha, *Linear Systems Theory*. Princeton University Press, 2018, ISBN: 9780691179575.

[21] S. Kar, J. M. F. Moura, and K. Ramanan, "Distributed parameter estimation in sensor networks: Nonlinear observation models and imperfect communication," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3575–3605, 2012.

[22] B. Mohar, "Eigenvalues, diameter, and mean distance in graphs," *Graphs and Combinatorics*, vol. 7, 1991.