Distributed Learning over Time-Varying Graphs with Adversarial Agents

Pooja Vyavahare*, Lili Su†, Nitin H. Vaidya‡
*Department of Electrical Engineering, Indian Institute of Technology, Tirupati
Email: poojav@iittp.ac.in
†Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology
Email: lilisu@mit.edu
‡Department of Computer Science, Georgetown University
Email: nitin.vaidya@georgetown.edu

***Abstract*—In this work, we study the problem of non-Bayesian learning in time-varying (dynamic) networks when there are some adversarial (faulty) agents in the network. The set of faulty agents is fixed across time. The connectivity graph of the network is changing at each time step and is unknown to the agents. In every time step, each non-faulty agent collects partial information about an unknown state of the environment. Each non-faulty agent tries to estimate the true state of the environment by iteratively sharing information with its neighbors at each time step.**

We first present an analysis of a distributed algorithm in static communication network with faulty agents which does not require the network to achieve consensus. Existing algorithms in this setting require that all non-faulty agents in the network should be able to achieve consensus via local information exchange. We then extend this analysis to dynamic networks with relaxed network condition. We show that if every non-faulty agent can receive enough information (via iteratively communicating with neighbors) to differentiate the true state of the world from other possible states then it can indeed learn the true state.

***Index Terms*—Time-varying networks, Byzantine fault-tolerance, non-Bayesian learning**

I. Introduction

Distributed algorithms in multi-agent networks for various network settings have been investigated [14], [3]. In this work, we consider a set of agents which are connected by directed links, thus forming a directed network. Each agent is attached to a sensor which senses some partial information about the state of the world (environment) in which the network is present. There is only one true state of the world and the aim for each agent is to estimate the true state by iteratively sharing information with its neighbors. *Distributed learning* has been studied like in the presence of a fusion center [17], [13] and when there is no fusion center [2], [1], [6].

Non-Bayesian learning with the use of iterative distributed consensus algorithm was first proposed by Jadbabaie et al. [5]. The approach proposed in [5] requires the network formed by the agents to achieve consensus in order to learn the true state. Since then the non-Bayesian learning has been applied in various network settings; see [8] for a survey of results in this area.

Our aim is to study a network of agents in which an unknown set of agents is adversarial. We assume that an adversarial agent suffers Byzantine faults, i.e., a faulty agent may send arbitrary information to its neighbors and may not follow the specified algorithm. Learning the true state of the world in a network with adversarial agents was first studied by [10], [11]. The algorithm in [10] uses a geometric averaging update similar to that used in other works [7], [9].

The algorithm analysis in [10], [11] requires that the network topology be such that non-faulty agents can achieve consensus by iteratively sharing their information with their neighbors. In this work we circumvent this limitation. We analyze the algorithm proposed in [10], [11] and show that in order to estimate the true state of the world by non-faulty agents, achieving distributed consensus is not required. Intuitively, we show that if the set of agents that can reach an agent can collectively estimate the true state then the agent can also estimate the true state almost surely. For our main analysis we assume that the underlying communication network is static across time, i.e., the communication network does not change.

Non-Bayesian learning on time-varying (dynamic) communication networks was studied in [7]. The analysis in [7] requires the sequence of communication networks to be uniformly strongly connected in order to estimate the true state of the world. We extend our analysis to dynamic networks with faulty agents under relaxed network conditions. Our analysis does not

Research reported in this paper was sponsored in part by the Army Research Laboratory under Cooperative Agreement W911NF-17-2-0196, and by National Science Foundation awards 1421918 and 1610543. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the the Army Research Laboratory, National Science Foundation or the U.S. Government.

require the sequence of communication networks to be uniformly strongly connected.

A. Preview

We introduce the system model for static communication network in Section II and present the algorithm to estimate true state in presence of adversarial agents (which is first introduced in [10]) in Section III. In Section III-A we state our assumption on network along with our main contribution (Lemma 1). We use this lemma to analyze Algorithm 1 in Section III-B. We extend our analysis for dynamic communication networks in Section IV by first presenting the system model for dynamic networks. We conclude the work in Section V.

II. System Model

We consider a set of n agents; each agent i observes a signal $s_t^i \in \mathcal{S}_i$ at time step $t = 1, \ldots$ which is independent of any other agent. $\mathcal{S}_i$ represents the signal space of agent i and we assume that $|\mathcal{S}_i| < \infty$. We assume that there are m states of the environment and each observed signal gives some partial information about the true state of the environment. Let the set of the possible states be $\Theta := \{\theta_1, \ldots, \theta_m\}$ and the true state be $\theta^* \in \Theta$. Observed signals of agents are governed by a set of marginal distribution $\mathcal{D}_i := \{l_i(\omega_i|\theta)|\theta \in \Theta, \omega_i \in \mathcal{S}_i\}$. We assume that $l_i(\omega_i|\theta) > 0, \forall \omega_i \in \mathcal{S}_i, \theta \in \Theta$. Let $s_{1,t}^i$ be the set of all signals observed by agent i from time step 1 to t.

At every time step t, agents try to estimate the true state of the environment by communicating information with their neighbors. The communication pattern at any time is represented by a directed graph $\mathcal{G} := (\mathcal{V}, \mathcal{E})$ where $\mathcal{V} = \{1, 2, \ldots, n\}$ is the set of n agents and $\mathcal{E}$ represents the set of directed communication links. In Section IV, we present the system model and analysis of the algorithm for dynamic graphs.

At any time step, there are at most f adversarial (faulty) agents in the network. Adversarial agents suffer with Byzantine faults and share incorrect information with their neighbors. Faulty agents can collaborate with each other and have full knowledge of the network at every time step. Let $\mathcal{F}$ be the set of faulty agents and $\mathcal{N}$ be the set of non-faulty agents in the network. Non-faulty agents do not know the identity of faulty agents but know the upper bound f on the number faulty agents. Let $|\mathcal{F}| = \phi$ and $\phi \leq f$. Without loss of generality, at each time step we represent the non-faulty agents by $\{1, 2, \ldots, n - \phi\}$.

At each time step t, every non-faulty agent i maintains a stochastic vector $\mu_i^t \in \mathbb{R}^m$ over all possible states $\theta \in \Theta$. We assume that at time 0 when no signal is observed by any agent, $\mu_0^i(\theta) = 1/m, \forall \theta \in \Theta$. Throughout this work, log of any vector $\mathbf{x}$ is defined as a vector $\mathbf{y}$ with $\mathbf{y}[i] := \log(\mathbf{x}[i])$, i.e., the log operation on a vector is element-wise.

III. Non-Bayesian learning in static communication network

In this section, we present the algorithm for non-Bayesian learning when some agents in the network are faulty. Throughout this section we assume that the communication network is fixed and does not change across time. Note that Algorithm 1 was first presented in [10] and in this work we present an improved analysis which circumvent the need to achieve consensus in order to learn the true state by non faulty agents. Algorithm 1 and some related concepts are presented here for the sake of completeness. For more details refer to [10], [12], [16].

For convenience of presentation, we assume that the non-faulty agents are numbered $1, 2, \ldots, n - \phi$ (where $\phi = |\mathcal{F}|$ is the number of faulty agents).

Algorithm 1: [10] Non-Bayesian learning with faulty agents: steps of agent i in t-th iteration

$Z^i \leftarrow \emptyset$;
$\mathbf{x}^i \leftarrow \log \mu_{t-1}^i$; ($\mathbf{x}^i$ *is a vector over all states with* $\mathbf{x}^i(\theta) := \log \mu_{t-1}^i(\theta)\ \forall \theta \in \Theta$)
Transmit $\mathbf{x}^i$ on all outgoing links.;
Receive messages on all incoming links. Let these multiset of messages be R^i.
for *every* $C \subseteq R^i \cup \{\mathbf{x}^i\}$ *such that* $|C| = (m+1)f + 1$ **do**
  add to Z^i a *Tverberg point* of multiset C
end
$\eta_t^i \leftarrow \frac{1}{1+|Z^i|}\left(\mathbf{x}^i + \sum_{\mathbf{z} \in Z^i} \mathbf{z}\right)$;
Observe s_t^i;
for $\theta \in \Theta$ **do**
  $\ell_i(s_{1,t}^i|\theta) \leftarrow \ell_i(s_t^i|\theta)\, \ell_i(s_{1,t-1}^i|\theta)$;
  $\mu_t^i(\theta) \leftarrow \frac{\ell_i(s_{1,t}^i|\theta) \exp\left(\eta_t^i(\theta)\right)}{\sum_{p=1}^m \ell_i(s_{1,t}^i|\theta_p) \exp\left(\eta_t^i(\theta_p)\right)}$;
end

The *Tverberg point* is guaranteed to be in the convex hull of values received from non-faulty agents. See [16] for definition of *Tverberg point*. As shown in [10], the dynamics of η_t^i for fault free agent i ($1 \leq i \leq n - \phi$) of Algorithm 1 can be written as:

$$\eta_t^i(\theta) = \log \prod_{j=1}^{n-\phi} \mu_{t-1}^j(\theta)^{\mathbf{A}_{ij}[t]}, \quad \forall \theta \in \Theta, \qquad (1)$$

where $\mathbf{A}[t]$ is a $(n-\phi) \times (n-\phi)$ row stochastic matrix corresponding to the execution of Algorithm 1 at time t. As shown in [16], $\mathbf{A}[t]$ is affected by the behavior

of faulty agents. For any $\theta_1, \theta_2 \in \Theta$, and for any agent $i \in \mathcal{V}$, let $\psi_t^i(\theta_1, \theta_2)$ and $\mathcal{L}_t(\theta_1, \theta_2)$ be as follows:

$$\boldsymbol{\psi}_t^i(\theta_1, \theta_2) \triangleq \log \frac{\mu_t^i(\theta_1)}{\mu_t^i(\theta_2)}, \quad \mathcal{L}_t^i(\theta_1, \theta_2) \triangleq \log \frac{\ell_i(s_t^i|\theta_1)}{\ell_i(s_t^i|\theta_2)}. \tag{2}$$

Following the analysis in [10] the evolution of $\boldsymbol{\psi}_t^i(\theta, \theta^*)$ can be written as:

$$\psi_t^i(\theta, \theta^*) = \sum_{r=1}^{t} \sum_{j=1}^{n-\phi} \boldsymbol{\Phi}_{ij}(t, r+1) \sum_{k=1}^{r} \mathcal{L}_k^j(\theta, \theta^*). \tag{3}$$

where $\boldsymbol{\Phi}_{ij}(t, r)$ is (i, j)-th element of $\boldsymbol{\Phi}(t, r) = \mathbf{A}[t] \dots \mathbf{A}[r]$ for $1 \leq r \leq t+1$. By convention, $\boldsymbol{\Phi}(t, t) = \mathbf{A}[t]$ and $\boldsymbol{\Phi}(t, t+1) = \mathbf{I}$.

A. Properties of $\boldsymbol{\Phi}(t, r)$

Many concepts of this section were presented in [15], [10] and we present them here for the sake of completeness of this manuscript. Recall that $\mathbf{A}[t]$ is a row stochastic matrix which defines the run of Algorithm 1 at time t. Note that Algorithm 1 uses Tverberg points to generate η_t^i which is obtained by rejecting extreme values received from neighbors. It is shown in [16] that this can be seen as removing some incoming links at each round of the algorithm and the effective network can be characterized by *reduced graph* of $G(\mathcal{V}, \mathcal{E})$.

Definition 1. *[16] A reduced graph $\mathcal{H}(\mathcal{N}, \mathcal{E}_{\mathcal{F}})$ of network $G(\mathcal{V}, \mathcal{E})$ is obtained by:*

1) *removing all faulty agents $\mathcal{F}$ and all the links incident on these agents*
2) *for all non-faulty agents, removing up to mf additional incoming links.*

Let the set of all such reduced graphs be $\mathcal{R}_{\mathcal{F}}$. By the definition of reduced graph and finiteness of G note that the number of possible reduced graphs of G is finite, i.e., $|\mathcal{R}_{\mathcal{F}}| = r_f < \infty$. A *source component* in a reduced graph is a strongly connected set of agents which does not have any incoming links from outside that set. We make the following assumption in our analysis.

Assumption 1. *Every reduced graph contains one or more source components and each agent in the reduced graph is either a part of a source component or has a directed path from one or more source components.*

Remark: Note that analysis in [10] assumes that every reduced graph contains only one source component. This assumption is shown [10], [16] to be sufficient to achieve approximate Byzantine vector consensus. We do not assume that there is a unique source component in each reduced graph. Thus, under our assumption, consensus on arbitrary inputs is not necessarily guaranteed. However, under Assumption 2 stated below regarding the sensor observations, the learning problem is solvable.

Assumption 1 is different than the one made in [10] and thus is not sufficient to achieve consensus among fault free agents. The key contribution of this work is to show correctness of Algorithm 1 under Assumption 1.

Note that a reduced graph is formed by removing all the faulty agents, their associated edges and extra mf edges from each non-faulty agent from graph G. Thus $mf + f_i$ edges are removed from each non-faulty agent where $f_i \leq f$ is the number of faulty agents in the neighborhood of agent i. Assumption 1 states that each non-faulty agent in the reduced graph is either a part of a source component or connected to at least one source component thus each agent in the reduced graph has at least one incoming edge. As largest possible f_i is f thus every agent in G has at least $mf+f+1$ incoming edges.

It was shown in [15] that for any $\mathbf{A}[t]$ there exists a reduced graph of G, say $\mathcal{H}[t]$ whose transition matrix is $\mathbf{H}[t]$, such that $\mathbf{A}[t] \geq \beta \mathbf{H}[t]$ where $0 < \beta < 1$ is a constant. The same result holds true under Assumption 1 which can be proved by using the bound on minimum number of incoming edges for any agent in the network. For more details on this relationship and definition of β refer to [15]. Now we present a new result which will be used for the analysis.

Lemma 1. *For $\boldsymbol{\Phi}(t, r+1)$, with $t - r \geq \nu := r_f(n-\phi)$, there exists a reduced graph $\mathcal{H}_r$ such that the following holds for each i, $1 \leq i \leq n-\phi$: there exists a source component $P_r^i \in \mathcal{H}_r$ such that $\boldsymbol{\Phi}_{ij}(t, r+1) \geq \beta^\nu / n$ for each agent j in that source component of $\mathcal{H}_r$.*

Proof. We will prove the result for two cases. First for $t - r = \nu$, recall the product matrix $\boldsymbol{\Phi}(t, r+1) = \mathbf{A}[t] \dots \mathbf{A}[r+1]$ and for any $\mathbf{A}[x] \geq \beta \mathbf{H}[x]$ where $\mathbf{H}[x]$ is the adjacency matrix of the reduced graph corresponding to x-th round of Algorithm 1. Thus,

$$\boldsymbol{\Phi}(t, r+1) \geq \beta^\nu \prod_{x=r+1}^{t} \mathbf{H}[x].$$

The product $\boldsymbol{\Phi}(t, r+1)$ contains $\nu = r_f(n-\phi)$ reduced graphs of G. As there are r_f distinct reduced graphs, there is one reduced graph $\mathcal{H}_r$ which will occur at least $(n-\phi)$ times in $\boldsymbol{\Phi}(t, r+1)$. By Assumption 1, every agent has a directed path from at least one source component in $\mathcal{H}_r$ and let P_r^i be any one source component which has a directed path to i in $\mathcal{H}_r$. As the maximum length of any path in $\mathcal{H}_r$ is $(n-\phi-1)$, for each agent i, $(\prod_{x=r+1}^{t} \mathbf{H}[x])_{ij} \geq 1$ for all $j \in P_r^i$. Thus for each agent i, and $j \in P_r^i$, $\boldsymbol{\Phi}_{ij}(t, r+1) \geq \beta^\nu > \beta^\nu / n$. Hence the result is proved when $t - r = \nu$.

Now, for any value of t, r such that $t - r = \nu + k$ where $k \geq 1$ is an integer, we get

$$\begin{aligned} \boldsymbol{\Phi}(t, r+1) &= \mathbf{A}[t] \dots \mathbf{A}[t-k+1] \mathbf{A}[t-k] \dots \mathbf{A}[r+1] \\ &= \boldsymbol{\Phi}(t, t-k+2) \boldsymbol{\Phi}(t-k+1, r+1). \end{aligned}$$

Let the i-th row of $\mathbf{\Phi}(t-k+1, r+1)$ be K_i and that of $\mathbf{\Phi}(t, r+1)$ be L_i. Then L_i can be written in terms of K_i as:

$$L_i = \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, t-k+2) K_j.$$

Recall that $\mathbf{\Phi}(t, t-k+2)$ is a $(n-\phi) \times (n-\phi)$ row stochastic matrix thus for every i, there exists some j such that $\mathbf{\Phi}_{ij}(t, t-k+2) \geq 1/(n-\phi) \geq 1/n$. By first part of the proof, there exists a reduced graph $\mathcal{H}_r$ such that for each row j of $\mathbf{\Phi}(t-k+1, r+1)$ there exists a source component of $\mathcal{H}_r$ such that $\mathbf{\Phi}_{jp}(t-k+1, r+1) \geq \beta^\nu$ where p belongs to that source component. Thus, for each row L_i of $\mathbf{\Phi}(t, r+1)$ there exists a reduced graph $\mathcal{H}_r$ such that there exists a source component P_r^i of $\mathcal{H}_r$ such that $\mathbf{\Phi}_{ip}(t, r+1) \geq \beta^\nu/n$ where p belongs to P_r^i. □

B. Analysis of Algorithm 1 for static networks

In this section we present the analysis of Algorithm 1 under Assumption 1 which does not require the network topology to achieve distributed consensus. We make the following assumption on agents' capacity to identify the true state of the world based on the Kullback-Leiber divergence between the true state's marginal $l_j(.|\theta^*)$ and marginal of any other state $l_j(.|\theta)$. The Kullback-Leiber divergence is defined as:

$$D(l_j(.|\theta^*)||l_j(.|\theta) = \sum_{\omega_i \in \mathcal{S}_j} l_j(\omega_i|\theta^*) \log \frac{l_j(\omega_i|\theta^*)}{l_j(\omega_i|\theta)}.$$

Assumption 2. *Let $\P_{\mathcal{H}}$ be the set of all source components in any reduced graph $\mathcal{H}$ of $G(\mathcal{V}, \mathcal{E})$. Then, for any $\theta \neq \theta^*$, for every source component $P \in \P_{\mathcal{H}}$ for every reduced graph $\P_{\mathcal{H}}$ the following holds:*

$$\sum_{j \in P} D(l_j(.|\theta^*)||l_j(.|\theta)) \neq 0.$$

Intuitively, Assumption 2 states that in any reduced graphs all agents in any source component can collaboratively detect the true state. Before presenting our main result we define few notations from [10] which will be used to prove our main result. For each $\theta \in \Theta$ and $i \in \mathcal{V}$ define $H_i(\theta, \theta^*)$ as:

$$\begin{aligned} H_i(\theta, \theta^*) &\triangleq \sum_{\omega_i \in \mathcal{S}_i} \ell_i(\omega_i|\theta^*) \log \frac{\ell_i(\omega_i|\theta)}{\ell_i(\omega_i|\theta^*)} \\ &= -D(\ell_i(.|\theta^*)||\ell_i(.|\theta)) \leq 0. \end{aligned} \tag{4}$$

Let $\mathcal{H}$ be any arbitrary reduced graph with a set of source components $\P_{\mathcal{H}}$ and $\P = \cup_{\mathcal{H} \in \mathcal{R}_\mathcal{F}} \P_{\mathcal{H}}$ be the set of all possible source components for all the reduced graph. Then we define C_0 and C_1 as:

$$-C_0 \triangleq \min_{i \in \mathcal{V}} \min_{\theta_1, \theta_2 \in \Theta; \theta_1 \neq \theta_2} \min_{\omega_i \in \mathcal{S}_i} \left(\log \frac{\ell_i(\omega_i|\theta_1)}{\ell_i(\omega_i|\theta_2)} \right), \tag{5}$$

$$C_1 \triangleq \min_{P \in \P} \min_{\theta, \theta^* \in \Theta; \theta \neq \theta^*} \sum_{i \in P} D(\ell_i(.|\theta^*)||\ell_i(.|\theta)). \tag{6}$$

Due to finiteness of Θ and $\mathcal{S}_i$ for each agent i, we know that $C_0 < \infty$ and $C_0 \geq 0$. Also under Assumption 2 we get $C_1 > 0$. Since the support of $\ell_j(.|\theta)$ is the whole signal space $\mathcal{S}_j$ for each $j \in \mathcal{V}$, it is easy to observe that

$$\begin{aligned} 0 \geq H_j(\theta, \theta^*) &\geq \min_{w_j \in \mathcal{S}_j} \left(\log \frac{\ell_j(w_j|\theta)}{\ell_j(w_j|\theta^*)} \right) \\ &\geq -C_0 > -\infty. \end{aligned} \tag{7}$$

The following lemma is used to prove our main result.

Lemma 2. *Under Assumption 2, for Algorithm 1 the following statement is true for any $\theta \neq \theta^*$:*

$$\frac{1}{t^2} \sum_{r=1}^{t} \left(\sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) \sum_{k=1}^{r} \mathcal{L}_k^j(\theta, \theta^*) - r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*) \right) \xrightarrow{\text{a.s.}} 0.$$

Proof. The lemma statement is similar (but not identical) to Lemma 3 of [10]. The proof of Lemma 3 of [10] requires each row of $\mathbf{\Phi}$ to converge to an identical stochastic vector. We do not have this requirement; moreover under Assumption 1 a row of $\mathbf{\Phi}(t, r+1)$ may not converge as t goes to infinity. The proof is presented in Appendix A. □

Now we present our main result for non-Bayesian learning when some agents in the network are faulty.

Theorem 1. *Under Assumption 2, for Algorithm 1 every agent i will concentrate its vector on the true state θ^* almost surely, i.e., $\mu_t^i(\theta) \xrightarrow{\text{a.s.}} 0 \ \forall \theta \neq \theta^*$.*

Proof. For any $i \in \mathcal{N}$ to show $\lim_{t \to \infty} \mu_t^i \xrightarrow{\text{a.s.}} 0$ for $\theta \neq \theta^*$, it is enough to show that $\psi_t^i(\theta, \theta^*) \xrightarrow{\text{a.s.}} -\infty$. By (7) we know that $|\sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*)| \leq C_0 < \infty$ for each agent $i \in \mathcal{N}$. Note that $\mathbf{\Phi}(t, r+1)$ is a row stochastic matrix. Due to finiteness of

$\sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*)$ by adding and subtracting $r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*)$ from (3), we get,

$$\psi_t^i(\theta, \theta^*) = \sum_{r=1}^{t} \left(\sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) \sum_{k=1}^{r} \mathcal{L}_k^j(\theta, \theta^*) - r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*) \right) + \sum_{r=1}^{t} r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*). \quad (8)$$

We first derive bound for the second term.

$$\sum_{r=1}^{t} r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*) \leq \sum_{r: t-r \geq \nu} r \sum_{j \in P_r^i} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*), \quad (9)$$

where for agent i, P_r^i is a source component of $\mathcal{H}_r$ for which the lower bound of Lemma 1 holds. The above inequality holds because by (7), $H_j(\theta, \theta^*) \leq 0$.

$$\begin{aligned} &\sum_{r=1}^{t} r \sum_{j=1}^{n-\phi} \mathbf{\Phi}_{ij}(t, r+1) H_j(\theta, \theta^*) \\ &\leq \sum_{r: t-r \geq \nu} r \left(\sum_{j \in P_r^i} \frac{\beta^\nu}{n} H_j(\theta, \theta^*) \right) \\ &\quad \text{By Lemma 1} \\ &\leq - \sum_{r: t-r \geq \nu} r \left(\frac{\beta^\nu}{n} C_1 \right) \qquad \text{by (6) and (4)} \\ &\leq - \frac{(t-\nu)^2}{2} \frac{\beta^\nu}{n} C_1. \end{aligned} \quad (10)$$

Therefore by (8), (10) and Lemma 2, we get

$$\lim_{t \to \infty} \frac{1}{t^2} \psi_t^i(\theta, \theta^*) \leq - \frac{1}{2n} \beta^\nu C_1.$$

Thus, $\psi_t^i(\theta, \theta^*) \xrightarrow{\text{a.s.}} -\infty$ and $\mu_t^i(\theta) \xrightarrow{\text{a.s.}} 0$ for all non-faulty agents and $\theta \neq \theta^*$.

□

IV. Extension to time varying communication network

In this section we analyze Algorithm 1 when the communication network is changing at every time step. At any time t, the communication among agents is represented by $\mathcal{G}_t = (V, \mathcal{E}_t)$ where V is the set of agents and $\mathcal{E}_t$ is the set of directed communication links at time t. All other system assumptions remain same as presented in Section II. We assume that the set of faulty agents ($\mathcal{F}$) and the set of non-faulty agents ($\mathcal{N}$) remain same across all time steps and only the communication pattern among the agents changes at each time step.

A straight forward extension of the analysis of Section III-B to dynamic networks is by making the Assumption 2 on every reduced graph of each communication network $\{\mathcal{G}_t | t = 1, 2, \ldots\}$ in an execution of the algorithm. Intuitively this assumption states that every source component of each reduced graph of the communication network $\mathcal{G}_t$ for $t = 1, 2, \ldots$ can estimate the true state of the world. This restricts the possible communication graphs in the sequence $\{\mathcal{G}_t | t = 1, 2, \ldots\}$. The result of Lemma 1 still holds with the reduced graph $\mathcal{H}_r$ following this assumption and thus the result of Theorem 1 also holds.

However, we present a different analysis of Algorithm 1 here which makes the assumption on agents' capacity to identify the true state by taking the union of B reduced graphs. Our assumption can be seen analogous to the assumption made in [7] on B-strongly connected sequence of graphs in case of time-varying networks. Note that [7] does not consider adversarial agents in the networks. We consider the adversarial agents in the network and also our analysis does not require the non-faulty agents to achieve consensus.

A. Analysis of Algorithm 1 for dynamic networks

The sequence of communication networks in the execution of the algorithm is denoted by $\{\mathcal{G}_t | t = 1, 2, \ldots\}$. Note that in this case, the set of incoming and outgoing links for each agent is changing at every time step t for Steps 3,4 of Algorithm 1. Even in static networks, due to behavior of faulty agents the execution matrix $\mathbf{A}[t]$ changes at every time step t. In case of dynamic networks, $\mathbf{A}[t]$ is affected by the graph $\mathcal{G}_t$ and the behavior of faulty agents at time step t. A reduced graph $\mathcal{H}(\mathcal{N}, \mathcal{E}_{t,\mathcal{F}})$ of communication graph $\mathcal{G}_t$ can be defined similar to Definition 1. We make Assumption 1 on every reduced graph of communication graph $\mathcal{G}_t$ for every $t = 1, 2, \ldots$. We also make the following assumption on the union of $B \geq 1$ reduced graphs.

Assumption 3. *Let $\mathcal{H}_{1,B} = \cup_{k=1}^{B} \mathcal{H}_k$ be the union of any B reduced graphs where each $\mathcal{H}_k$ be a reduced graph of $\mathcal{G}_t$ for some $t = 1, 2, \ldots$. Then $\mathcal{H}_{1,B}$ contains one or more source components and each non-faulty agent is either a part of a source component or has a directed path from one or more source components.*

We will use the following lemma to prove our result.

Lemma 3 (Lemma 2 of [4])**.** *Let $C_1, C_2, \ldots, C_B$ be $B \geq 1$ non negative $(n-\phi) \times (n-\phi)$ matrices with diagonal elements of each C_i being positive. Let μ and*

ρ be the smallest and largest of all diagonal elements respectively. Then,

$$C_1C_2\dots C_B \geq \left(\frac{\mu^2}{2\rho}\right)^{B-1}(C_1+C_2+\dots C_B).$$

Note that for a network with n agents, number of possible communication graphs is $2^{n(n-1)} < \infty$ which is finite. Let $R_{\mathcal{G}_i}$ be the set of all reduced graphs of the communication graph $\mathcal{G}_i$ at time step i. Each communication graph has finite number of possible reduced graphs due to finiteness of the faulty set $\mathcal{F}$ and the finiteness of the communication graph. Therefore, there are finite number of reduced graphs in any execution of the algorithm. Let $\mathcal{U}_B$ be the set of union of B reduced graphs. As number of possible communication graphs and the number of reduced graphs of a communication graph both are finite, the set $\mathcal{U}_B$ is finite, i.e., $|\mathcal{U}_B| = u_B < \infty$.

Now we will prove a bound on elements of the matrix $\mathbf{\Phi}(t, r+1)$ in case of dynamic network. Recall that we proved a similar bound in Lemma 1 for static graphs.

Lemma 4. *For $\mathbf{\Phi}(t, r+1)$, with $t-r \geq \nu := u_B B(n-\phi)$, there exists an union of B reduced graphs $\mathcal{H}_{1,B} = \cup_{k=1}^{B}\mathcal{H}_k$ such that the following holds for each i, $1 \leq i \leq n-\phi$: there exists a source component $P_B^i \in \mathcal{H}_{1,B}$ such that $\mathbf{\Phi}_{ij}(t, r+1) \geq \gamma/n$ for each agent $j \in P_B^i$. Here the graph $\mathcal{H}_k$ is a reduced graph of the communication graph $\mathcal{G}_k$ and γ is a constant.*

Proof. First we will prove the result for $t-r = \nu$ and $\mathbf{\Phi}(t, r+1) = \mathbf{A}[t]\dots\mathbf{A}[t-B+1]\dots\mathbf{A}[r+1]$. By [16] for each weight matrix $\mathbf{A}[t]$ there is a reduced graph $\mathcal{H}_t$ of $\mathcal{G}_t$ such that $\mathbf{A}[t] \geq \beta\mathbf{H}[t]$ where $0 < \beta < 1$ is a constant and $\mathbf{H}[t]$ is the adjacency matrix of the reduced graph. Thus,

$$\mathbf{\Phi}(t, r+1) \geq \beta^{\nu}\mathbf{H}[t]\dots\mathbf{H}[t-B+1]\dots\mathbf{H}[r+1]. \quad (11)$$

The adjacency matrix of any reduced graph is a non-negative matrix with $\mathbf{H}_{ij}[t] = 1$ if $j = i$ or there is an edge from j to i in the reduced graph. Therefore, by taking B matrices at a time and applying Lemma 3, we get,

$$\mathbf{H}[t]\dots\mathbf{H}[t-B+1] \geq (2)^{-B+1}(\mathbf{H}[t]+\dots\mathbf{H}[t-B+1]).$$

Note that $\mathbf{H}[t]+\dots\mathbf{H}[t-B+1] \geq \mathbf{H}_{t,t-B+1}$ where $\mathbf{H}_{t,t-B+1}$ is the adjacency matrix of the union of reduced graphs corresponding to $\mathbf{H}[t], \dots, \mathbf{H}[t-B+1]$. Thus,

$$\mathbf{H}[t]\dots\mathbf{H}[t-B+1] \geq \left(\frac{1}{2}\right)^{B-1}\mathbf{H}_{t,t-B+1}. \quad (12)$$

Observe that there are ν matrices in the product in (11) and by definition ν is a multiple of B. Therefore taking B matrices at a time and applying the arguments of (12), we get,

$$\mathbf{\Phi}(t, r+1) \geq \beta^{\nu}\left(\frac{1}{2}\right)^{\frac{\nu(B-1)}{B}}\prod_{k=1}^{\nu/B}\mathbf{H}_{t-kB+B,t-kB+1}. \quad (13)$$

Recall that in this product the matrix $\mathbf{H}_{t_1,t_2}$ is the adjacency matrix of the union of B reduced graphs where each reduced graph comes from a different communication network. Recall $\nu/B = u_B(n-\phi)$. As there are u_B possible different $\mathbf{H}_{t_1,t_2}$, one of them, say $\bar{\mathbf{H}}$, will occur at least $(n-\phi)$ times in the product of (13). Let $\bar{\mathbf{H}}$ be the adjacency matrix corresponding to union graph $\mathcal{H}_{1,B} = \cup_{k=1}^{B}\mathcal{H}_k$. By Assumption 3, every agent i has a directed path from at least one source component $P_B^i \in \mathcal{H}_{1,B}$. Maximum length of any path in $\bar{\mathbf{H}}$ is $(n-\phi-1)$ therefore for each node i, $\prod_{k=1}^{\nu/B}\mathbf{H}_{t-kB+B,t-kB+1}(i,j) \geq 1$ for all $j \in P_B^i$. Thus for each agent i, and $j \in P_B^i$, $\mathbf{\Phi}_{ij}(t, r+1) \geq \gamma > \gamma/n$, where $\gamma = \beta^{\nu}\left(\frac{1}{2}\right)^{\frac{\nu(B-1)}{B}}$.

Now, for any value of t, r such that $t-r = \nu+k$ where $k \geq 1$ is an integer, we get

$$\begin{aligned}\mathbf{\Phi}(t, r+1) &= \mathbf{A}[t]\dots\mathbf{A}[t-k+1]\mathbf{A}[t-k]\dots\mathbf{A}[r+1]\\ &= \mathbf{\Phi}(t, t-k+2)\mathbf{\Phi}(t-k+1, r+1).\end{aligned}$$

Let the i-th row of $\mathbf{\Phi}(t-k+1, r+1)$ be R_i and that of $\mathbf{\Phi}(t, r+1)$ be C_i. Then C_i can be written in terms of R_i as:

$$C_i = \sum_{j=1}^{n-\phi}\mathbf{\Phi}_{ij}(t, t-k+2)R_j.$$

Recall that $\mathbf{\Phi}(t, t-k+2)$ is a $(n-\phi)\times(n-\phi)$ row stochastic matrix thus for every i, there exists some j such that $\mathbf{\Phi}_{ij}(t, t-k+2) \geq 1/(n-\phi) \geq 1/n$. By first part of the proof, there exists a union of reduced graph $\mathcal{H}_{1,B}$ such that for each row j of $\mathbf{\Phi}(t-k+1, r+1)$ there exists a source component of $\mathcal{H}_{1,B}$ such that $\mathbf{\Phi}_{jp}(t-k+1, r+1) \geq \gamma$ where p belongs to that source component. Thus, for each row C_i of $\mathbf{\Phi}(t, r+1)$ there exists a union of B reduced graph $\mathcal{H}_{1,B}$ such that there exists a source component P_r^i of $\mathcal{H}_{1,B}$ such that $\mathbf{\Phi}_{ip}(t, r+1) \geq \gamma/n$ where p belongs to P_r^i. □

We make the following assumption on the capacity to identify the true state by agents.

Assumption 4. *In any execution of algorithm with sequence of communication graphs $\{\mathcal{G}_t | t = 1, 2, \dots\}$, there exists an integer $1 \leq B < \infty$ such that the following is true: Let $\mathcal{R}_{\mathcal{G}_t}$ be the set of all reduced graphs of $\mathcal{G}_t$, $\forall t$. Then for every source component*

$P_{jB,(j+1)B-1}$ *of* $\mathcal{H}_{jB,(j+1)B-1} = \cup_{i=jB}^{(j+1)B-1} \mathcal{L}_i$ *for all* $j \geq 0$ *where* $\mathcal{L}_i \in \mathcal{R}_{\mathcal{G}_i}$, *for any* $\theta \neq \theta^*$,

$$\sum_{k \in P_{jB,(j+1)B-1}} D(l_k(.|\theta^*)||l_k(.|\theta)) \neq 0. \qquad (14)$$

Recall that for the static network we make the similar assumption on every source component of each reduced graph of the communication network. For time varying networks, we make the assumption on source components of the union of B reduced graphs. Assumption 4 is analogous to the assumption made for time varying graphs in [7] wherein the strong connectivity assumption is on union B graphs rather than one static graph of [5]. The following result shows that non-faulty agents can detect the true state of the world by running Algorithm 1 when communication network is changing with time.

Theorem 2. *In a time varying network, with sequence of communication graphs* $\{\mathcal{G}_t | t = 1, 2 \ldots\}$, *under Assumption 4, every agent* i *will concentrate its vector on the true state* θ^* *almost surely, i.e.,* $\mu_t^i(\theta) \xrightarrow{\text{a.s.}} 0 \ \forall \theta \neq \theta^*$.

Proof. It is easy to observe that the statement of Lemma 2 also holds under Assumption 4. The proof of the theorem follows the same line of argument as that of Theorem 1 by using Lemma 4 instead of Lemma 1. We do not present the proof for the lack of space in this manuscript. □

Remark: Note that Assumption 2 can be relaxed for the union of B reduced graphs for static networks and Lemma 4 can be used to analyze Algorithm 1 under this relaxed condition.

V. Conclusion

In this work, we presented an analysis of a distributed algorithm for non-Bayesian learning over multi-agent static network with adversaries which is based on a weaker assumption on the underlying network than the one present in literature [11], [12]. Our analysis does not need the network to achieve consensus among all the fault-free agents. It shows that if all the agents, whose information can reach an agent, can collaboratively correctly estimate the true state of the world then the agent itself can estimate the true state. The analysis presented here proves a sufficient network topological condition and global identifiability of the network to correctly estimate the true state by all fault-free agents. It will be interesting to prove this condition also being the necessary to estimate true state in a network with adversarial agents.

We extended the analysis of static networks to time-varying networks in Section IV. We made a relaxed assumption on the capacity of agents to detect the true state by considering union of B reduced graphs. This analysis can also be done for static graphs with relaxed assumption on the detect ability of true state.

The analysis also extends to a network with no adversaries, i.e., $f = 0$, and leads to much weaker assumption on the network as compared to the one present in literature. Previous analysis in [10], [7] for fault-free network assume that the network is strongly connected thus capable of achieving distributed consensus. The analysis of Section III can be extended to fault-free network that can have more than one connected components and each connected component may not be strongly connected.

In this work, for both static and time-varying graphs, we assume a synchronous system, i.e., in each round of the algorithm every agent sends its information at the same time to all its neighbors. In future, we would like to extend this work in case of asynchronous setting.

References

[1] F. S. Cattivelli and A. H. Sayed. Distributed detection over adaptive networks using diffusion adaptation. *IEEE Transactions on Signal Processing*, 59(5):1917–1932, May 2011.

[2] D. Gale and S. Kariv. Bayesian learning in social networks. *Games and Economic Behavior*, 45:329–346, 1988.

[3] R. G. Gallager. Finding parity in simple broadcast networks. *IEEE Trans. on Info. Theory*, 34:176–180, 1988.

[4] A. Jadbabaie, J. Lin, and A. S. Morse. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48:988–1001, 2003.

[5] A. Jadbabaie, P. Molavi, A. Sandroni, and A. Tahbaz-Salehi. Non-baysian social learning. *Games and Economic Behavior*, 76:210–225, 2012.

[6] D. Jakovetić, J. M. Moura, and J. Xavier. Distributed detection over noisy networks: Large deviations analysis. *IEEE Transactions on Signal Processing*, 60(8):4306–4320, 2012.

[7] A. Nedić, A. Olshevsky, and C. A. Uribe. Nonasymptotic convergence rates for cooperative learning over time-varying directed graphs. In *American Control Conference (ACC)*, pages 5884–5889, 2015.

[8] A. Nedić, A. Olshevsky, and C. A. Uribe. A tutorial on distributed (non-bayesian) learning: Problem, algorithms and results. In *55th IEEE Conf. on Decision and Control*, pages 6795–6801, 2016.

[9] S. Shahrampour and A. Jadbabaie. Exponentially fast parameter estimation in networks using distributed dual averaging. In *IEEE Conference on Decision and Control (CDC)*, pages 6196–6201. JAI Press, 2013.

[10] L. Su and N. H. Vaidya. Defending non-bayesian learning against adversarial attacks. *https://arxiv.org/abs/1606.08883*, 2016.

[11] L. Su and N. H. Vaidya. Non-bayesian learning in the presence of byzantine agents. In *International Symposium on Distributed Computing*, pages 414–427. Springer, 2016.

[12] L. Su and N. H. Vaidya. Defending non-bayesian learning against adversarial attacks. *Distributed Computing https://doi.org/10.1007/s00446-018-0336-4*, 2018.

[13] J. N. Tsitsiklis. Decentralized detection. In *Advances in Statistical Signal Processing*, pages 297–344. JAI Press, 1993.

[14] J. N. Tsitsiklis and M. Athans. Convergence and asymptotic agreement in distributed decision problems. *IEEE Transactions on Automatic Control*, 29(1):42–50, 1984.

[15] N. H. Vaidya. Matrix representation of iterative approximate byzantine consensus in directed graphs. *available at https://arxiv.org/abs/1203.1888*, 2012.

[16] N. H. Vaidya. Iterative byzantine vector consensus in incomplete graphs. *Distributed Computing and Networking*, pages 14–28, 2014.

[17] P. K. Varshney. *Distributed Detection and Data Fusion*. Springer Science & Business Media, 2012.

APPENDIX A
PROOF OF LEMMA 2

To prove Lemma 2, we will show that almost surely for any $\epsilon > 0$ there exists sufficiently large t_ϵ such that for all $t \geq t_\epsilon$,

$$\frac{1}{t^2}\left|\sum_{r=1}^{t}\sum_{j=1}^{n-\phi}\mathbf{\Phi}_{ij}(t,r+1)\left(\sum_{k=1}^{r}\mathcal{L}_k^j(\theta,\theta^*) - rH_j(\theta,\theta^*)\right)\right| \leq \epsilon. \quad (15)$$

For ease of notations, we will represent the left hand side of (15) by $\frac{1}{t^2}Q(1,t)$. We prove this by dividing r into two ranges $r \in \{1,\cdots,\sqrt{t}\}$ and $r \in \{\sqrt{t}+1,\cdots,t\}$. For $r \in \{1,\cdots,\sqrt{t}\}$, we have,

$$\begin{aligned}\frac{1}{t^2}Q(1,\sqrt{t}) &\leq \frac{1}{t^2}\sum_{r=1}^{\sqrt{t}}\sum_{j=1}^{n-\phi}\mathbf{\Phi}_{ij}(t,r+1)\,(2rC_0)\\ &= \frac{1}{t^2}\,(2C_0)\sum_{r=1}^{\sqrt{t}} r \leq C_0\left(\frac{1}{t}+\frac{1}{t^{\frac{3}{2}}}\right).\end{aligned}$$

Here first inequality is due to (7) and finiteness of $|\ell_k^j(\theta,\theta^*)|$. Thus, there exists t_ϵ^1 such that for all $t \geq t_\epsilon^1$, $\frac{1}{t^2}Q(1,\sqrt{t}) \leq \frac{\epsilon}{2}$.

As $\mathcal{L}_k^j(\theta,\theta^*)$'s are i.i.d., due to Strong Law of Large Numbers, we get $\frac{1}{r}\sum_{k=1}^{r}\mathcal{L}_k^j(\theta,\theta^*) - H_j(\theta,\theta^*) \xrightarrow{\text{a.s.}} 0$. Thus for each convergent sample path, there exists r_ϵ such that for any $r \geq r_\epsilon$, $\left|\frac{1}{r}\sum_{k=1}^{r}\mathcal{L}_k^j(\theta,\theta^*) - H_j(\theta,\theta^*)\right| \leq \frac{\epsilon}{2}$. Thus for $r \geq \sqrt{t}$ there exists sufficiently large t_ϵ^2 such that for all $t \geq t_\epsilon^2$, $r \geq \sqrt{t}$ is large enough and

$$\left|\frac{1}{r}\sum_{k=1}^{r}\mathcal{L}_k^j(\theta,\theta^*) - H_j(\theta,\theta^*)\right| \leq \frac{\epsilon}{2}.$$

For all $t \geq t_\epsilon^2$,

$$\begin{aligned}\frac{1}{t^2}Q(\sqrt{t},t) &\leq \frac{1}{t}\sum_{r=\sqrt{t}+1}^{t}\sum_{j=1}^{n-\phi}\mathbf{\Phi}_{ij}(t,r+1)\frac{r}{t}\frac{\epsilon}{2}\\ &= \frac{1}{t}\sum_{r=\sqrt{t}+1}^{t}\frac{r}{t}\frac{\epsilon}{2} = \frac{\epsilon}{2}\frac{1}{t^2}\sum_{r=\sqrt{t}+1}^{t} r\\ &= \frac{\epsilon}{4}\frac{1}{t^2}\left(t^2-\sqrt{t}\right) \leq \frac{\epsilon}{2}.\end{aligned}$$

Therefore, for every convergent path for any $\epsilon > 0$, there exists $t_\epsilon = \max\{t_\epsilon^1, t_\epsilon^2\}$, such that for any $t \geq t_\epsilon$, $\frac{1}{t^2}Q(1,t) \leq \epsilon$. Thus (15) holds almost surely and Lemma 2 is proved.