

Distributed Learning with Adversarial Agents Under Relaxed Network Condition

Pooja Vyavahare*, Lili Su[†], Nitin H. Vaidya[‡]

*Coordinated Science Laboratory, University of Illinois at Urbana-Champaign
Email: poojav@illinois.edu

[†]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—This work studies the problem of non-Bayesian learning over multi-agent network when there are some adversarial (faulty) agents in the network. At each time step, each non-faulty agent collects partial information about an unknown state of the world and tries to estimate true state of the world by iteratively sharing information with its neighbors. Existing algorithms in this setting require that all non-faulty agents in the network should be able to achieve consensus via local information exchange.

In this work, we present an analysis of a distributed algorithm which does not require the network to achieve consensus. 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—Byzantine fault-tolerance, non-Bayesian learning

I. INTRODUCTION

Distributed algorithms in multi-agent networks for various network settings have been studied since long time [13], [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 in different settings like in the presence of a fusion center [16], [12] and when there is no fusion center [2], [1], [5].

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. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

Non-Bayesian learning with the use of iterative distributed consensus algorithm was first proposed by Jadbabaie et. al. [4]. The approach proposed in [4] 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 [7] 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., 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 [9], [10]. The algorithm in [9] uses a geometric averaging update similar to that used in other works [6], [8].

The algorithm analysis in [9], [10] 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 [9], [10] 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.

A. Preview

We introduce the system model in Section II and present the algorithm to estimate true state in presence of adversarial agents (which is first introduced in [9]) 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 conclude the work in Section IV.

II. PROBLEM FORMULATION

We consider a system model similar to that in [15], [14]. We consider a set of agents which are connected

via directed links thus forming a directed network $G = (\mathcal{V}, \mathcal{E})$ where $|\mathcal{V}| = n$. We consider synchronous system setting. Maximum f agents can suffer with Byzantine faults at each execution of the algorithm. Any agent with Byzantine fault may send arbitrary different information to different neighbors. Adversarial agents can collaborate with each other and have full knowledge of the system. Let $\mathcal{F}$ be the set of faulty agents and $\mathcal{N}$ be set of non-faulty (good) agents in an execution. Each good agent at every execution knows the upper bound on number of faulty agents, i.e., f , but does not know the set $\mathcal{F}$. Let $|\mathcal{F}| = \phi$.

Every agent collects some partial information about the world. The aim of every fault-free agent is to estimate the true state of the world by iteratively sharing information with neighbors. For this we use the same model as presented in [4], [10]. Let there be m possible states of the world and we represent the set of states by: $\Theta = \{\theta_1, \theta_2, \dots, \theta_m\}$. Out of m possible states, there is one true state $\theta^* \in \Theta$. Initially, at $t = 0$, the true state is unknown to every agent in the network. At every time iteration t , every agent independently observes some information (signal) about the state θ^* . Observed signal space for agent i is represented by $\mathcal{S}_i$ and we assume that $|\mathcal{S}_i| < \infty$. Let $\ell_i(\cdot|\theta)$ be the marginal distribution of the signal observed by agent i when the true state is θ . Each agent i knows the structure of its observed signal which is represented by a set of marginal distributions $\mathcal{D}_i = \{\ell_i(\omega_i|\theta) | \theta \in \Theta, \omega_i \in \mathcal{S}_i\}$. We also assume that $\forall \omega_i \in \mathcal{S}_i$ and $\forall \theta \in \Theta$, $\ell_i(\omega_i|\theta) > 0$. In other words, the support of the distribution $\ell_i(\cdot|\theta)$ is the whole signal space. Let $s_{1,t}^i$ be the signal history observed by agent i up to time t . 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 WITH FAULTY AGENTS

In this section we present the algorithm for non-Bayesian learning when some agents in the network are faulty. Note that Algorithm 1 was first presented in [9] 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 of this manuscript. For more details refer to [9], [11], [15].

For convenience of presentation, we assume that the non-faulty agents are numbered $1, 2, \dots, n - \phi$ (where $\phi = |\mathcal{F}|$ is the number of faulty agents at every time iteration). At each time iteration t , every non-faulty agent i maintains a vector $\mu_t^i \in \mathbb{R}^m$ of the possible states of the world. μ_t^i is a stochastic vector over all states $\theta \in \Theta$

with $0 \leq \mu_t^i(\theta) \leq 1$ and $\sum_{\theta} \mu_t^i(\theta) = 1 \forall i$. We assume that initially at $t = 0$, $\mu_0^i(\theta) = 1/m \forall i, \forall \theta \in \Theta$.

Algorithm 1: [9] Non-Bayesian learning with faulty agents: for agent i

```

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

The Tverberg point is guaranteed to be in the convex hull of values received from non-faulty agents. See [15] for definition of Tverberg point. As shown in [9], the dynamics of η_t^i for fault free agent i ($1 \leq i \leq n - \phi$) of Algorithm 1 can be written as:

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

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 [15], $\mathbf{A}[t]$ 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:

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

Following the analysis in [9] the evolution of $\psi_t^i(\theta, \theta^*)$ can be written as:

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

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

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

Many concepts of this section were presented in [14], [9] 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 [15] 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. [15] 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 m_f 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 [9] assumes that every reduced graph contains only one source component. This assumption is shown [9], [15] 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 [9] 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.

It was shown in [14] 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. For more details on this relationship and definition of β refer to [14]. Now we present a new result which will be used for the analysis.

Lemma 1. For $\Phi(t, r+1)$, 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 $\Phi_{ij}(t, r+1) \geq \beta^\nu/n$ 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 $\Phi(t, r+1) = \mathbf{A}[t] \dots \mathbf{A}[r+1]$ 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,

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

The product $\Phi(t, r+1)$ 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 $\Phi(t, r+1)$. 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 $j \in P_r^i$, $\Phi_{ij}(t, r+1) \geq \beta^\nu > \beta^\nu/n$. 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

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

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

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

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

B. Analysis of Algorithm 1

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 $l_j(\cdot|\theta^*)$ and marginal of any other state $l_j(\cdot|\theta)$. The Kullback-Leiber divergence is defined as:

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

Assumption 2. Let $\mathfrak{H}$ 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 $P \in \mathfrak{P}_{\mathcal{H}}$ for every reduced graph $\mathfrak{P}_{\mathcal{H}}$ the following holds:

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

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 [9] 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:

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

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

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

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

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 $\ell_j(\cdot|\theta)$ is the whole signal space $\mathcal{S}_j$ for each $j \in \mathcal{V}$, it is easy to observe that

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

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 $\theta \neq \theta^*$:

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

Proof. The lemma statement is similar (but not identical) to Lemma 3 of [9]. The proof of Lemma 3 of [9] requires each row of Φ to converge to an identical stochastic vector. We do not have this requirement; moreover under Assumption 1 a row of $\Phi(t, r+1)$ may not converge as t goes to infinity. The proof is presented in Appendix A. $\square$

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 $\lim_{t \rightarrow \infty} \mu_t^i \xrightarrow{\text{a.s.}} 0$ 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 $|\sum_{j=1}^{n-\phi} \Phi_{ij}(t, r+1) H_j(\theta, \theta^*)| \leq C_0 < \infty$ for each agent $i \in \mathcal{N}$. Note that $\Phi(t, r+1)$ is a row stochastic matrix. Due to finiteness of $\sum_{j=1}^{n-\phi} \Phi_{ij}(t, r+1) H_j(\theta, \theta^*)$ by adding and subtracting $r \sum_{j=1}^{n-\phi} \Phi_{ij}(t, r+1) H_j(\theta, \theta^*)$ from (3), we get,

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

We first derive bound for the second term.

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

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), $H_j(\theta, \theta^*) \leq 0$.

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

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

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

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 $\theta \neq \theta^*$. $\square$

IV. CONCLUSION

In this work, we presented an analysis of a distributed algorithm for non-Bayesian learning over multi-agent network with adversaries which is based on a weaker assumption on the underlying network than the one present in literature [10], [11]. 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.

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 [9], [6] 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 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. In addition to that we assume the network to be static, i.e., neighborhood of any agent is not changing over the course of execution of the algorithm. We believe that our results can be easily generalized to the dynamic networks where the network topology is changing with time.

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, P. Molavi, A. Sandroni, and A. Tahbaz-Salehi. Non-baysian social learning. *Games and Economic Behavior*, 76:210–225, 2012.
- [5] 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.
- [6] 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.
- [7] 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.

- [8] 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.
- [9] L. Su and N. H. Vaidya. Defending non-bayesian learning against adversarial attacks. <https://arxiv.org/abs/1606.08883>, 2016.
- [10] 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.
- [11] 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.
- [12] J. N. Tsitsiklis. Decentralized detection. In *Advances in Statistical Signal Processing*, pages 297–344. JAI Press, 1993.
- [13] J. N. Tsitsiklis and M. Athans. Convergence and asymptotic agreement in distributed decision problems. *IEEE Transactions on Automatic Control*, 29(1):42–50, 1984.
- [14] N. H. Vaidya. Matrix representation of iterative approximate byzantine consensus in directed graphs. [available at https://arxiv.org/abs/1203.1888](https://arxiv.org/abs/1203.1888), 2012.
- [15] N. H. Vaidya. Iterative byzantine vector consensus in incomplete graphs. *Distributed Computing and Networking*, pages 14–28, 2014.
- [16] 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 $t \geq t_\epsilon$,

$$\frac{1}{t^2} \left| \sum_{r=1}^t \sum_{j=1}^{n-\phi} \Phi_{ij}(t, r+1) \left(\sum_{k=1}^r \mathcal{L}_k^j(\theta, \theta^*) - rH_j(\theta, \theta^*) \right) \right| \leq \epsilon. \quad (11)$$

For ease of notations, we will represent the left hand side of (11) by $\frac{1}{t^2}Q(1, t)$. We prove this by dividing r into two ranges $r \in \{1, \dots, \sqrt{t}\}$ and $r \in \{\sqrt{t} + 1, \dots, t\}$. For $r \in \{1, \dots, \sqrt{t}\}$, we have,

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

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 $t \geq t_\epsilon^2$,

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

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 (11) holds almost surely and Lemma 2 is proved.