Resilient Distributed Hypothesis Testing With Time-Varying Network Topology

Bo Wu, Steven Carr, Suda Bharadwaj, Zhe Xu, and Ufuk Topcu

***Abstract*— We study the problem of distributed hypothesis testing, where a team of mobile agents aims to agree on the true hypothesis (out of a finite set of hypotheses) that best explains a sequence of their local and possibly noisy observations. The setting requires collaboration among the agents through a possibly time-varying network topology due to mobility and limited communication range. Furthermore, we assume there is a subset of agents in the team that may deliberately share wrong information to undermine the team objective. We propose a distributed algorithm where each agent maintains two sets of beliefs (i.e., probability distributions over hypotheses), namely *local* and *actual* belief. In every time step, each agent first shares its actual belief in the previous time step with the other agents within its communication range. Then the algorithm updates the local belief of each agent using local observations. After that, each agent updates its actual belief as a function of its local belief and the shared actual beliefs of the other agents. We show that the actual belief for each non-adversarial agent in the proposed algorithm converges almost surely to the true hypothesis. Unlike most of the existing literature, we guarantee the convergence without a connectivity constraint of the time-varying network topology. We illustrate the proposed algorithm on a simulation of a team of unmanned aerial vehicles aiming to classify adversarial agents among themselves.**

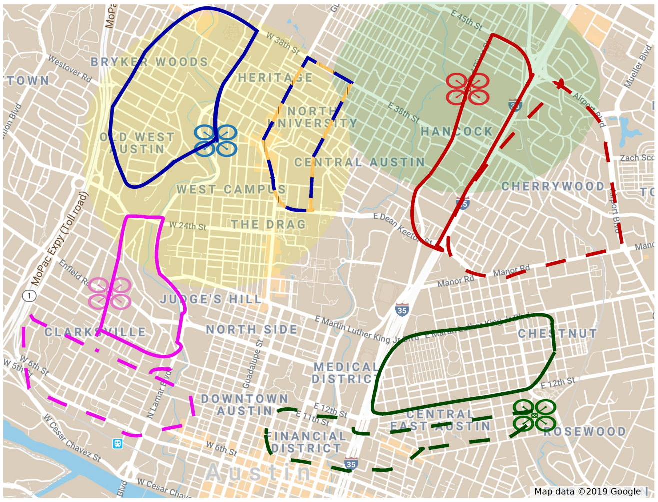


Fig. 1: Running example with four agents (UAVs). Each agent has a sensing range (shaded yellow), a communication range (shaded green), two trajectories (solid lines or dashed lines) based on whether the agent is good or bad. The green agent is bad as its actual trajectory is a dashed line.

I. Introduction

Consider a team of mobile agents where each agent individually performs a given task, for example, persistent surveillance following given trajectories, as shown in Figure 1. An unknown subset of the agents is compromised where the compromised (bad) agents may behave differently. Because of the limited sensor range, noisy sensor data, and individual task constraints, it may not be reasonable to anticipate that a single non-compromised (good) agent can classify all the bad agents. Therefore, the agent team needs to identify those compromised agents in a distributed manner. Each agent can share its local information to its time-varying neighbors, i.e., other mobile agents that are within its communication range at the current time step. The required collaboration raises the question of how to process local and shared information such that every good agent will eventually converge to correctly classify the subset of bad agents. It is worth noting that the shared information could potentially come from a bad agent and thus might have been altered arbitrarily. This classification problem can be studied under the framework of distributed hypothesis testing, where each possible set of bad agents out of the set of all agents is a hypothesis.

In distributed hypothesis testing, a team of agents repeatedly makes local observations and collaboratively infers the unknown true hypothesis that generates their observations. One approach to distributed hypothesis testing is that the agents do not directly communicate with each other but instead send their local information to a fusion center for centralized processing [1], [2], [3]. However, such a setting may place large communication and computation burdens on the fusion center as the number of the agents increases. Furthermore, if the fusion center is compromised, the team objective will fail. To improve the scalability and robustness, distributed solutions where each agent communicates to its neighbors without a fusion center are growing in popularity [4], [5], [6], [7], [8], [9].

In this paper, we study a distributed hypothesis testing problem without a fusion center. In this setting, each agent maintains a *belief*, which is a probability distribution over hypotheses. An agent makes an observation and updates its belief according to some specific rule at each time step. The update rule makes use of the local observation and the beliefs of the neighboring agents.

Typical update rules in existing literature make use of consensus-based belief aggregation with connectivity as-

Bo Wu, Steven Carr, Suda Bharadwaj, Zhe Xu, and Ufuk Topcu are with the Department of Aerospace Engineering and Engineering Mechanics, and the Oden Institute for Computational Engineering and Sciences, University of Texas, Austin, 201 E 24th St, Austin, TX 78712. email: {bwu3, stevencarr, suda.b, zhexu, utopcu}@utexas.edu

sumptions of the (potentially time-varying) network topology, see e.g., [5], [10], [11], [7], [8]. However, none of these methods consider agents with adversarial behaviors that do not follow the update rule and may share arbitrarily altered beliefs. As a result, these rules may fail if there are compromised agents.

The works most related to this paper are [12] and [9], where the update rules are robust against bad agents. These bad agents are described by the *Byzantine* adversary model where they may have access to complete knowledge of the team task, update rule, shared information, and true hypothesis. The adversary may send arbitrarily altered beliefs in a coordinated way to undermine the team objective. In particular, this paper is inspired by [9], where each agent maintains two set of beliefs, namely *local* and *actual* belief. The local belief is updated using a Bayesian rule based on its local observations. The actual belief is updated as a function of its local belief and neighbors' actual beliefs. The update rule robust to adversarial agents [9] is guaranteed to converge to the true hypothesis almost surely. However, the guarantee in [9] assumes fixed network topology, i.e., the neighbors of each agent do not change over time (the extended version [13] considers a time-varying network topology but only applies in settings without an adversary agent). Furthermore, the convergence still relies on some relaxed graph-theoretic connectivity requirement of the network topology.

This paper has two main novelties compared to the existing literature for distributed hypothesis testing. First, we design a robust belief-update rule with *time-varying* network topology. Second, we prove that the proposed rule converges almost surely to the true hypothesis *without* connectivity constraints of the underlying network topology. The proposed approach also naturally extends to settings with no adversarial agents.

In contrast to [9], in the proposed update rule in order to update actual belief each agent needs to determine whether there are enough neighbors to *filter out* the impact of altered beliefs from bad agents. If there are, the agent will make use of the shared information. Otherwise, it will update the actual belief as the function of its local belief and previous actual belief. We give necessary conditions to guarantee almost sure convergence to the true hypothesis in the limit. The simulation with a team of unmanned aerial vehicles (UAVs) demonstrates the validity of the proposed approach.

II. Preliminaries and Modeling Framework

In this paper, we consider a set $\mathcal{N} = \{0, ..., N-1\}$ of agents that are moving in a gridworld with a finite grid set Q. Let $\mathbb{Z}^{\geq 0}$ denote non-negative integers. At time step $t \in \mathbb{Z}^{\geq 0}$, we denote $q_{i,t} \in Q$ as the *state* of an agent i. The movement of each agent is constrained by a directed graph $\mathcal{G}_m = (Q, E_m)$ where an agent can move from q to q' in one time step if and only if $(q, q') \in E_m$.

For agent i, its communication range is characterized by a function $H_i : Q \to 2^Q$. Agent i at q can communicate to another agent j at q' if and only if $q' \in H_i(q)$ (note that $i \in H_i(q)$). Then the network topology at time t for the team of agents is characterized by a directed graph $\mathcal{G}_{c,t} = (\mathcal{N}, E_{c,t})$. An edge $(i,j) \in E_{c,t} \subseteq \mathcal{N} \times \mathcal{N}$ if and only if $q_{j,t} \in H_i(q_{i,t})$. In such a case, we say that agent i is a *neighbor* of agent j at time t. At any time t, we denote $\mathcal{N}_{i,t} := \{j \in \mathcal{N} | q_{i,t} \in H_j(q_{j,t})\} \subseteq \mathcal{N}$ as the set of all neighbors of agent i.

There is a finite set Θ of possible hypotheses. The total number of hypotheses is denoted as $m = |\Theta|$. At each time step, an agent i is at a state $q \in Q$ and makes an observation $s \in S_i$ where S_i denotes a set of observations for agent i. The probability to observe s is given by a conditional likelihood function $l_i(s|\theta^*, q)$, where $l_i(s|\theta^*, q) \in [0,1]$, and $\sum_{s \in S_i} l_i(s|\theta^*, q) = 1$. We denote $\theta^* \in \Theta$ as the unknown but fixed *true* hypothesis to be learned. Agent i has the knowledge of a set of likelihood functions $\{l_i(\cdot|\theta, q) : \forall \theta \in \Theta, q \in Q\}$. By definition, the local likelihood function for θ^* only depends on an agent's current state q. Therefore, the observation sequence for each agent is an i.i.d random process.

For each agent i, from $t = 0$, it moves in the gridworld following a sequence of states $(q_{i,0}, q_{i,1}, q_{i,2}, ...)$ which we denote as a *local state path*. It is easy to see that for any t, $(q_{i,t}, q_{i,t+1}) \in E_m$. In this paper, we assume each agent follows a given local state path. However, the local observation sequence that each agent makes along the local state path is a random process. We define the set of state observation paths as follows.

Definition 1. *Given an agent i and a local state path $(q_{i,0}, q_{i,1}, q_{i,2} ...)$, its set of local state observation paths is defined as $\Omega_i = \{\omega_i | \omega_i = (q_{i,0}, s_{i,0})(q_{i,1}, s_{i,1})(q_{i,2}, s_{i,2},)..., \forall s_t \in S_i, q_{i,t} \in Q, \forall t \in \mathbb{N}\}$ with $P_{\theta^*}(\omega) = \prod_{t=0}^{\infty} l_i(s_{i,t}|\theta^*, q_{i,t})$. The set of global state observation paths is defined as $\Omega = \prod_i \Omega_i$.*

Within the team of agents, there is a subset of non-compromised (good) agents defined as $G \subseteq \mathcal{N}$. Good agents follow their given state paths and the distributed hypothesis testing rule. We assume that for an agent $i \in G$, at any time t, there are at most f bad neighboring agents, even though the identities of these bad agents are not known. The bad agents are characterized by the Byzantine fault model [14]. Each of them has full access to all agents' state paths, their local likelihood functions, any information shared over the network topology and the distributed hypothesis testing rule used by the team. If an agent is bad, it may follow a different but known state path. To prevent the team of agents from achieving the hypothesis testing objective, bad agents may collaboratively share arbitrarily altered information to their neighbors.

The objective of this paper is to design a distributed hypothesis testing rule, such that when $t \to \infty$, every agent $i \in G$ is able to determine the true hypothesis $\theta^* \in \Theta$ almost surely. To this end, we introduce the following definitions.

Definition 2. *Kullback–Leibler (KL) divergence $D(P_1||P_2)$ of two discrete probabilistic distributions P_1 and P_2 is given*

Algorithm 1: Resilient Distributed Hypothesis Testing (RDHT)

```
input : Agent $i$, its location $q_{i,t+1}$, neighbor set
        $\mathcal{N}_{i,t+1}$, and observation $s_{i,t+1}$.
1 for $\theta \in \Theta$ do
2     Compute the new local belief
          $b^l_{i,t+1}(\theta) = \frac{l_i(s_{i,t+1}|\theta, q_{i,t+1}) b^l_{i,t}(\theta)}{\sum_{p=1}^{m} l_i(s_{i,t+1}|\theta_p, q_{i,t+1}) b^l_{i,t}(\theta_p)}.$   (3)
          ▷ Local belief update with Bayesian rule;
3     if for all $\theta' \neq \theta$, $|S(\theta,\theta') \cap \mathcal{N}_{i,t+1}| \geq 2f+1$ then
4         Sort $\{b^a_{j,t+1}(\theta) | j \in \mathcal{N}_{i,t+1}\}$;
5         Remove $f$ neighboring agents with the lowest
            beliefs and save the rest agents to $\mathcal{N}^{\theta}_{i,t+1}$;
6         Compute the new actual belief
              $b^a_{i,t+1}(\theta) = \min\{\{b^a_{j,t}(\theta)\}_{j \in \mathcal{N}^{\theta}_{i,t+1}}, b^l_{i,t+1}(\theta)\}.$   (4)
              ▷ Case one for actual belief update.
      else
7         Compute the new actual belief
              $b^a_{i,t+1}(\theta) = \min\{b^a_{i,t}(\theta), b^l_{i,t+1}(\theta)\}.$   (5)
              ▷ Case two for actual belief update.
      end
  end
8 Normalize actual beliefs $b^a_{i,t+1}(\theta), \forall \theta \in \Theta$ so that they
    sum up to one.
```

by

$$D(P_1||P_2) = \sum_x P_1(x) \log(\frac{P_1(x)}{P_2(x)}). \tag{1}$$

Definition 3. *For a pair of hypothesis θ and $\theta' \in \Theta$ and an agent i, a location q belongs to $O_i(\theta, \theta') \subseteq Q$ if $D(l_i(\cdot|\theta, q)||l_i(\cdot|\theta', q)) > 0$.*

Intuitively, $O_i(\theta, \theta')$ denotes the locations where θ and θ' incur different likelihood functions and thus can be distinguished by agent i based on its local observations.

Definition 4. *For a pair of hypothesis θ and $\theta' \in \Theta$, a local state path $(q_{i,0}, q_{i,1}, q_{i,2}...)$ of an agent i, we say that agent i belongs to $S(\theta, \theta') \subseteq \mathcal{N}$ if*

$$\lim_{T \to \infty} \sum_{t=0}^{T} I(q_{i,t} \in O_i(\theta, \theta')) \to \infty, \tag{2}$$

where $I(.)$ is the indicator function.

From Definition 4, agent i belongs to the set $S(\theta, \theta')$ if it visits at least one state $q \in O_i(\theta, \theta')$ infinitely often.

III. Proposed Robust Distributed Hypothesis Rule

Following [9], before making an observation at time $t+1$, agent i maintains a local and an actual belief:

- The local belief $b^l_{i,t} : \Theta \to [0,1]$, $\sum_{\theta \in \Theta} b^l_{i,t}(\theta) = 1$.
- The actual belief $b^a_{i,t} : \Theta \to [0,1]$, $\sum_{\theta \in \Theta} b^a_{i,t}(\theta) = 1$.

At $t = 0$, $b^l_{i,0}$ and $b^a_{i,0}$ are initialized according to some *a priori* distribution.

In this section, we propose an algorithm that describes the update rule for the local and actual beliefs of each agent. The procedure is summarized in Algorithm 1. At time $t+1$, suppose agent i is at $q_{i,t+1}$ and its observation is $s_{i,t+1}$, the algorithm proceeds as follows.

For each $\theta \in \Theta$, as shown in Line 2 of Algorithm 1, we first update the local belief $b^l_{i,t+1}(\theta)$ with equation (3) following Bayesian rule with likelihood functions $l_i(s|\theta, q)$ for every $\theta \in \Theta$, where $s = s_{i,t+1}$ and $q = q_{i,t+1}$.

Then we move on to update the actual belief as shown from Line 3 to Line 7 of Algorithm 1. The actual belief $b^a_{i,t+1}(\theta)$ is updated according to one of the two cases. As shown in Line 3, if for all $\theta' \neq \theta$, $|S(\theta, \theta') \cap \mathcal{N}_{i,t+1}| \geq 2f+1$, then agent i updates its actual belief in case one. We first sort $b^a_{j,t+1}(\theta)$ for all $j \in \mathcal{N}_{i,t+1}$, then remove f neighbors with the lowest actual beliefs on θ. We denote the set of remaining neighbors as $\mathcal{N}^{\theta}_{i,t+1}$. Then the new actual belief is computed as in (4). On the other hand, if the condition for case one is not satisfied, the actual belief is updated in case two as shown in Line 7 of Algorithm 1. In (5), the actual belief is updated with the smaller value between the newly updated local belief and the actual belief at time t. Then we normalize the actual beliefs to make sure they sum up to one.

The following theorem guarantees that Algorithm 1 almost surely asymptotically convergences to the true hypothesis.

Theorem 1. *For a given agent $i \in G$ and its corresponding local state path $(q_{i,0}, q_{i,1}, q_{i,2}...)$, suppose the following conditions hold.*

1) *The initial beliefs $b^l_{i,0}(\theta) > 0$ and $b^a_{i,0}(\theta) > 0$ for any $\theta \in \Theta$ and any agent i.*
2) *For any agent i, if case one in Algorithm 1 happens only finitely often for a hypothesis $\theta \in \Theta$, then $i \in S(\theta, \theta')$ for any $\theta' \neq \theta$.*

Then Algorithm 1 ensures that $b^a_{i,t}(\theta^*) \to 1$ almost surely for any good agent $i \in G$ as $t \to \infty$.

We start with the following lemma before proving Theorem 1.

Lemma 1. *Consider a good agent $i \in G$, a local state path $(q_{i,0}, q_{i,1}, q_{i,2}...)$ and a pair of hypotheses θ^* and θ, where θ^* denotes the true hypothesis. If $b^l_{i,0}(\theta^*) > 0$ and $i \in S(\theta, \theta^*)$, the following holds.*

$$b^l_{i,t}(\theta) \to 0 \textit{ almost surely}, \tag{6}$$

and

$$b^l_{i,t}(\theta^*) > 0 \textit{ for all } t \textit{ almost surely.} \tag{7}$$

Proof. For any good agent $i \in G$, we define

$$\begin{gathered} \rho_{i,t}(\theta) = \log \frac{b^l_{i,t}(\theta)}{b^l_{i,t}(\theta^*)}, \text{ and} \\ \lambda_{i,t}(\theta) = \log \frac{l_i(s_{i,t}|\theta, q_{i,t})}{l_i(s_{i,t}|\theta^*, q_{i,t})}. \end{gathered} \tag{8}$$

Note that $l_i(s_{i,t}|\theta^*, q_{i,t}) > 0$ for all t, $q_{i,t}$ and $s_{i,t}$ since θ^* is the true hypothesis that generates the observation $s_{i,t}$. Therefore, we know that for any finite t, $b^l_{i,t}(\theta^*) > 0$ and (8) is always well-defined. Then according to the local belief-update rule (3), we have the following equation

$$\rho_{i,t+1}(\theta) = \rho_{i,t}(\theta) + \lambda_{i,t}(\theta)$$

which yields

$$\rho_{i,t+1}(\theta) = \rho_{i,0}(\theta) + \sum_{j=0}^{t} \lambda_{i,j}(\theta). \tag{9}$$

Note that according to equation (2), there are cases where $q_{i,t} \notin O_i(\theta, \theta^*)$, which implies

$$l_i(.|\theta^*, q_{i,t}) = l_i(.|\theta, q_{i,t}).$$

In this case, $\lambda_{i,t}(\theta) = 0$ and does not contribute to the sum in (9). Therefore, we may only focus on the case where $q_{i,t} \in O_i(\theta, \theta^*)$ and thus $\lambda_{i,t}(\theta) \neq 0$.

Note that $\{\lambda_{i,t}(\theta)\}$ is a sequence of independent random variables. For a given t, we have

$$E_{\theta^*}[\lambda_{i,t}(\theta)] = -D(l_i(.|\theta^*, q_{i,t})||l_i(.|\theta, q_{i,t})).$$

We denote a set $Q_\infty \subseteq Q$ for those locations where θ and θ^* can be differentiated and are visited infinite times by agent i. Formally,

$$Q_\infty := \{q | q \in O_i(\theta, \theta^*) \text{ and } \lim_{T\to\infty} \sum_{t=0}^{T} I(q_{i,t} = q) \to \infty\}.$$

We claim that Q_∞ is non-empty by contradiction. If Q_∞ is empty, it implies that none of the states $q \in O_i(\theta, \theta^*)$ is visited infinitely often, which violates the condition implied by $i \in S(\theta, \theta^*)$ and equation (2).

For any $q \in Q_\infty$, the following is true based on the strong law of large numbers.

$$\begin{aligned} &\lim_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} I(q_{i,t} = q)\lambda_{i,t}(\theta) \\ &= -D(l_i(.|\theta^*, q)||l_i(.|\theta, q)) \text{ almost surely.} \end{aligned} \tag{10}$$

We divide both sides of (9) by t and take the limit which yields

$$\begin{aligned} &\lim_{T\to\infty} \frac{1}{T} \rho_{i,T+1}(\theta) = \lim_{T\to\infty} \frac{1}{T}(\rho_{i,0}(\theta) + \sum_{t=0}^{T} \lambda_{i,t}(\theta)) \\ &= \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T} \lambda_{i,t}(\theta) \\ &= -\sum_{q \in Q_\infty} D(l_i(.|\theta^*, q)||l_i(.|\theta, q)) \text{ almost surely.} \end{aligned} \tag{11}$$

Note that for those $q \in O_i(\theta, \theta^*)$ but $q \notin Q_\infty$, their contribution in (11) is zero since they are only visited finite number of times. By definition of $O_i(\theta, \theta^*)$, we know that $D(l_i(.|\theta^*, q)||l_i(.|\theta, q)) > 0$ for $q \in O_i(\theta, \theta^*)$. Then from (11), $\rho_{i,t+1}(\theta) \to -\infty$ almost surely which implies $b^l_{i,t}(\theta) \to 0$ almost surely and proves (6).

For those $\theta \in \Theta$ where

$$\lim_{T\to\infty} \sum_{t=0}^{T} I(q_{i,t} \in O_i(\theta, \theta^*)) < \infty, \tag{12}$$

i.e., $i \notin S(\theta, \theta^*)$, we define a set

$$\bar{\Theta} := \{\theta | i \notin S(\theta, \theta^*)\}$$

to include all such θ that agent i is not able to differentiate. Then for each $\theta \in \bar{\Theta}$, there must exist a time T_θ such that

$$\lim_{T\to\infty} \sum_{t=T_\theta+1}^{T} I(q_{i,t} \in S(\theta, \theta^*)) = 0.$$

That is, there exists a time T_θ after which agent i will never visit any position that can differentiate θ and θ^*. Given any local state observation path $\omega_i = \{(q_{i,0}, s_{i,0}), (q_{i,1}, s_{i,1}), ...\}$ where (6) holds, it is immediate from (9) that

$$\lim_{t\to\infty} \rho_{i,t}(\theta) = \rho_{i,0}(\theta) + \sum_{j=0}^{T_\theta} \lambda_{i,j}(\theta) = C_{\theta,\omega_i} < \infty \tag{13}$$

for some constant C_{θ,ω_i} that depends on both θ and ω_i due to the term $\lambda_{i,j}(\theta)$. For a fixed ω_i, it is then possible to find $\lim_{t\to\infty} b^l_{i,t}(\theta^*)$ from (13) which is nonzero. When combining with the fact that $b^l_{i,t}(\theta^*)$ is nonzero for any finite t, we conclude that (7) is proved. □

Remark 1. *If we define a set of global state observation path $\hat{\Omega} \subseteq \Omega$ such that $\omega \in \hat{\Omega}$ if and only if for any good agent i,*

- *for each $\theta \neq \theta^*$, if $i \in S(\theta, \theta^*)$, $b^l_{i,t}(\theta) \to 0$.*
- $\lim_{t\to\infty} b^l_{i,t}(\theta^*)$ *exists with a given ω_i.*

From Lemma 1 we know that $\hat{\Omega}$ has measure one.

Lemma 1 also states that for a good agent $i \in G$, its local belief $b^l_{i,t}(\theta^*) > 0$ for all t almost surely. But is it possible for the bad agents to influence their neighboring good agents such that the good agent's actual beliefs on θ^* are set to zero? The following lemma shows that this cannot happen with the proposed belief-update rule.

Lemma 2. *For any good agent $i \in G$, $b^a_{i,t}(\theta^*) > 0$ for all t almost surely.*

Proof. We prove this lemma by contradiction. Suppose there is a time t where $b^a_{i,t}(\theta^*) = 0$ for the first time for any good agent i. From Lemma 1 we know that $b^a_{i,t-1}(\theta^*) > 0$ and $b^l_{i,t-1}(\theta^*) > 0$. Consequently from (5) it immediately follows that it cannot happen in case two in Algorithm 1.

Therefore we infer that $b^a_{i,t}(\theta^*) = 0$ can only result from an update in case one in Algorithm 1. From (4), this is only possible when $\min_{j \in \mathcal{N}^{\theta^*}_{i,t}} \{b^a_{j,t-1}(\theta^*)\} = 0$. Note that in case one, we remove f number of lowest beliefs on θ^* as in Line 5 of Algorithm 1. In the worst case, we remove all the f actual beliefs that are zero from the bad agents. Then what is left are the actual beliefs from good agents, which are nonzero from the definition of this time t. For all other cases, the removed f actual beliefs must contain nonzero entries, which implies that all the beliefs for agents in $\mathcal{N}_{i,t}^{\theta^*}$ are nonzero as well since they are sorted. In either case, we have that $\min_{j\in\mathcal{N}_{i,t}^{\theta^*}}\{b_{j,t-1}^a(\theta^*)\} > 0$ which leads to a contradiction. □

IV. Proof to Theorem 1

Now we are ready to give the proof for Theorem 1. We are interested in state observation path set $\hat{\Omega}$ as defined in Remark 1 since $\hat{\Omega}$ has measure one.

The proof consists of two parts. First, we prove that the actual belief over the true hypothesis $b_{i,t}^a(\theta^*)$ for any good agent i is lower-bounded. Then we show that the actual belief over the rest of the hypotheses will become arbitrarily small. These two parts together are sufficient to prove that the $b_{i,t}^a(\theta^*)$ will be arbitrarily close to one with probability one.

We fix a path $\omega \in \hat{\Omega}$ and define $\delta_1 = \min_{i\in G}\lim_{t\to\infty} b_{i,t}^l(\theta^*)$. Then for each good agent $i\in G$, there exists a time t_i and a constant α, such that for all $t\geq t_i$, we have $b_{i,t}^l(\theta^*)\geq\delta_1-\alpha$ where $\alpha<\delta_1$. We define

$$\bar{t}_1 = \max_{i\in G} t_i. \tag{14}$$

We also define $\delta_2 = \min_{i\in G} b_{i,\bar{t}_1}^a(\theta^*)$. By Lemma 2 we know $\delta_2>0$. We further define

$$\delta = \min\{\delta_1-\alpha,\delta_2\}. \tag{15}$$

Then at $t=\bar{t}_1+1$, in Algorithm 1, for actual belief update, either case one or case two happens. If case one happens, (4) is used to update the belief for θ^*, then we will have

$$b_{i,\bar{t}_1+1}^a(\theta^*) = \min\{\{b_{j,\bar{t}_1}^a(\theta^*)\}_{j\in\mathcal{N}_{i,\bar{t}_1+1}^{\theta^*}}, b_{i,\bar{t}_1+1}^l(\theta^*)\}\geq\delta. \tag{16}$$

(16) is true despite possible altered actual beliefs from f bad agents because in the update rule for case one, there is at least one good agent $i\in G$ in $\mathcal{N}_{i,\bar{t}_1+1}^{\theta^*}$ since we only eliminate f smallest beliefs and we have at least $2f+1$ neighbors. As a result, the beliefs remaining in $\mathcal{N}_{i,\bar{t}_1+1}^{\theta^*}$ are lower-bounded by δ.

If case two happens in Algorithm 1, (5) is used and we have

$$b_{i,\bar{t}_1+1}^a(\theta^*) = \min\{b_{i,\bar{t}_1}^a(\theta^*), b_{i,\bar{t}_1+1}^l(\theta^*)\}\geq\delta. \tag{17}$$

Therefore, no matter which case occurs, we have $b_{i,\bar{t}_1+1}^a(\theta^*)\geq\delta$ before normalization. Then we perform normalization as required in Line 8 of Algorithm 1 and can derive the following

$$\begin{aligned}\frac{b_{i,\bar{t}_1+1}^a(\theta^*)}{\sum_{p=1}^m b_{i,\bar{t}_1+1}^a(\theta_p)} &\geq \frac{\delta}{\sum_{p=1}^m b_{i,\bar{t}_1+1}^a(\theta_p)}\\ &\geq \frac{\delta}{\sum_{p=1}^m b_{i,\bar{t}_1+1}^l(\theta_p)} = \delta.\end{aligned} \tag{18}$$

Since for all $t\geq\bar{t}_1$, we have $b_{i,t}^l\geq\delta$, by induction, we can claim that

$$b_{i,t}^a(\theta^*)\geq\delta, \forall t\geq\bar{t}_1, \forall i\in G. \tag{19}$$

Now we are ready to prove the second part, which establishes the fact that the beliefs for hypotheses other than the θ^* are upper-bounded. We pick a small $\epsilon<\delta$. Given a hypothesis $\theta\neq\theta^*$, for any agent $i\in S(\theta,\theta^*)$, by Lemma 1, we know that there exists a time t_i^θ, such that

$$b_{i,t}^l(\theta)\leq\epsilon^3, \forall t\geq t_i^\theta. \tag{20}$$

We further define

$$\bar{t}_2 = \max\{\bar{t}_1, \max_{i\in S(\theta,\theta^*)}\{t_i^\theta\}\}.$$

Note that since $\bar{t}_2\geq\bar{t}_1$, from (19) we have that

$$b_{i,\bar{t}_2+1}^a(\theta^*)\geq\delta.$$

In a similar proof to the first part, for any agent $i\in S(\theta,\theta^*)$, if case one applies for actual belief update in Algorithm 1, then we use (4) to update $\theta\neq\theta^*$ and obtain

$$b_{i,\bar{t}_2+1}^a(\theta) = \min\{\{b_{j,\bar{t}_2}^a(\theta)\}_{j\in\mathcal{N}_{i,\bar{t}_2+1}^{\theta}}, b_{i,\bar{t}_2+1}^l(\theta)\}\leq\epsilon^3. \tag{21}$$

Note that (21) holds even with altered actual beliefs shared from up to f bad agents following a similar reasoning with (16). From belief update condition in case one, there is at least one good agent $i\in G\cap S(\theta,\theta^*)$ in $\mathcal{N}_{i,\bar{t}_1+1}^{\theta^*}$ since we only eliminate f smallest beliefs and we have at least $2f+1$ neighbors that belong to $S(\theta,\theta^*)$. On the other hand, if Algorithm 1 is in the condition of case two, then we have

$$b_{i,\bar{t}_2+1}^a(\theta) = \min\{b_{i,\bar{t}_2}^a(\theta), b_{i,\bar{t}_2+1}^l(\theta)\}\leq\epsilon^3. \tag{22}$$

Therefore, no matter which case occurs, we have that

$$b_{i,\bar{t}_2+1}^a(\theta)\leq\epsilon^3, \forall i\in S(\theta,\theta^*)\cap G.$$

According to the update rule, we will perform normalization as follows.

$$\begin{aligned}\frac{b_{i,\bar{t}_2+1}^a(\theta)}{\sum_{p=1}^m b_{i,\bar{t}_2+1}^a(\theta_p)} &\leq \frac{\epsilon^3}{\sum_{p=1}^m b_{i,\bar{t}_2+1}^a(\theta_p)}\\ &\leq \frac{\epsilon^3}{b_{i,\bar{t}_2+1}^l(\theta^*)}\leq\frac{\epsilon^3}{\delta}<\epsilon^2.\end{aligned} \tag{23}$$

The last inequality is because $\epsilon<\delta$. Therefore, by induction we have proved that for any $i\in S(\theta,\theta^*)\cap G$,

$$b_{i,t}^a(\theta)<\epsilon^2\leq\epsilon, \forall t\geq\bar{t}_2+1, \forall i\in S(\theta,\theta^*). \tag{24}$$

For any $i\notin S(\theta,\theta^*)$ but $i\in G$, by condition 2 in Theorem 1, we know that case one will happen infinitely often. As a result, for such agent i, there exists a time $\bar{t}_{i,1}^\theta\geq\bar{t}_2+1$ such that case one occurs for the first time for $t\geq\bar{t}_2+1$. Then at $\bar{t}_{i,1}^\theta$ from (24) , we know that

$$b_{i,\bar{t}_{i,1}^\theta}^a(\theta)\leq\epsilon^2, \forall i\in S(\theta,\theta^*)\cap G. \tag{25}$$

Following a similar reasoning from (21) to (23), we obtain that after normalization, for agent $i \notin S(\theta, \theta^*)$ but $i \in G$,

$$b^a_{i,\bar{t}^\theta_{i,1}}(\theta) < \epsilon. \tag{26}$$

Then we define another time instant $\bar{t}^\theta_{i,2} \geq \bar{t}^\theta_{i,1} + 1$ where the case one happens for the second time for $t \geq \bar{t}_2 + 1$. Notice that from the conditions in Theorem 1, case two could occurs infinitely often as well for agent $i \notin S(\theta, \theta^*)$. It then follows that case two happens for any $t \in (\bar{t}^\theta_{i,1}, \bar{t}^\theta_{i,2})$. By (5) and (26), we have that

$$b^a_{i,t}(\theta) < \epsilon, \forall t \in (\bar{t}^\theta_{i,1}, \bar{t}^\theta_{i,2}). \tag{27}$$

Combine (26) and (27) we obtain that

$$b^a_{i,t}(\theta) < \epsilon, \forall t \in [\bar{t}^\theta_{i,1}, \bar{t}^\theta_{i,2} - 1]. \tag{28}$$

Note that (28) holds trivially if $\bar{t}^\theta_{i,1} = \bar{t}^\theta_{i,2} - 1$, i.e., there is no occurrence of the case two between two consecutive case one updates. So even if case two happens only finitely often, the proof still holds. Then by induction, for agent $i \notin S(\theta, \theta^*)$ and $i \in G$, we have that

$$b^a_{i,t}(\theta) < \epsilon, \forall t \geq \bar{t}^\theta_{i,1}. \tag{29}$$

We further define

$$\bar{t}_3 = \max_{\theta} \max_{i \notin S(\theta, \theta^*)} \bar{t}^\theta_{i,1}.$$

Since $\bar{t}_3 > \bar{t}_2$,we have the following result

$$b^a_{i,t}(\theta) < \epsilon, \forall t \geq \bar{t}_3, \forall i \in G, \forall \theta \neq \theta^*. \tag{30}$$

Therefore, for any $\omega \in \hat{\Omega}$, $\lim_{t \to \infty} b^a(i,t)(\theta) \to 1$. Since the set $\hat{\Omega}$ has measure one as established in Remark 1, the proof of Theorem 1 is complete.

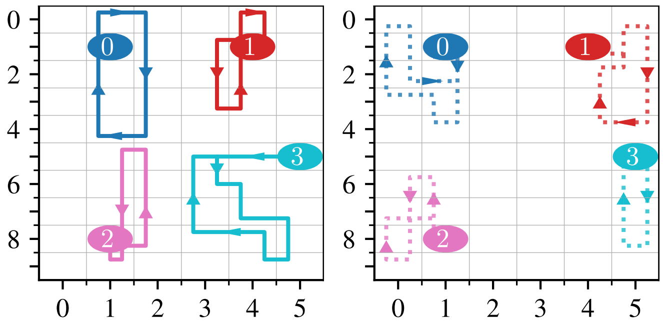
Remark 2. *While the proposed algorithm is among very few solutions to Byzantine-resilient distributed hypothesis testing, there is growing interest to consider Byzantine-resilient distributed machine learning, especially with distributed gradient decent [15], [16]. The main idea of the proposed algorithm is also applicable when a team of agents is deployed to perform a distributed machine learning task.*

V. Case Study

In this section, we consider a case study with a team of UAVs in a gridworld environment as shown in Figure 2. The objective is to identify the unknown set of compromised (bad) UAVs out of the UAV team with our proposed distributed hypothesis testing algorithm.

A. Setting

We assume that all the UAVs are at similar altitudes. Therefore, the state set Q is set of the two-dimensional locations in the gridworld. For agent i at time t, its state is represented by $q_{i,t} = [q^x_{i,t}, q^y_{i,t}]$. In this example, we assume the sensing and communication ranges are the same. Therefore, if agent j is within the sensing range of another agent i, agent i can both sense agent j and share belief $b^a_{i,t}$ with it.



(a) State path for a good agent

(b) State path for a bad agent

Fig. 2: Setting for case study: state paths depending on whether the agent is good (left) or bad (right).

Figure 2 describes the specific scenario. Every agent has a communication and sensor range of 2 units, i.e. they can view the locations that are within a 5×5 square centered around the agent's position q_i (see Figure 3a for an example). Each agent i could be either good or bad, therefore we denote a set Θ_i as $\Theta_i = \{0, 1\}$, where 0 denotes bad and 1 denotes good. The hypothesis set is then $\Theta = \prod_i \Theta_i$. In this particular example all agents are good except for agent 3. Consequently, the true hypothesis θ^* in Figure 2 is the tuple $\theta^* = (1, 1, 1, 0)$.

Each individual agent is assigned a persistent surveillance task. For any agent, depending on whether it is good or bad, it will have two different state paths as shown in Figure 2.

B. Observation Model

1) Sensor: If agent i is at q_i, it will make an observation s^j_i of agent j. We use $\mathcal{Q}_i(q_i) \subseteq Q$ to denote the set of locations that can be observed by agent i at q_i. If $q_j \in \mathcal{Q}_i(q_i)$, the probability to get an observation s^j_i follows a probability distribution over $\mathcal{Q}_i(q_i)$. In this example, the probability distribution is a truncated Gaussian distribution centered around the actual location q_j of agent j and with a prescribed variance σ^2 (see Fig. 3a). As a result, the probability for agent i to obtain observation s^j_i is

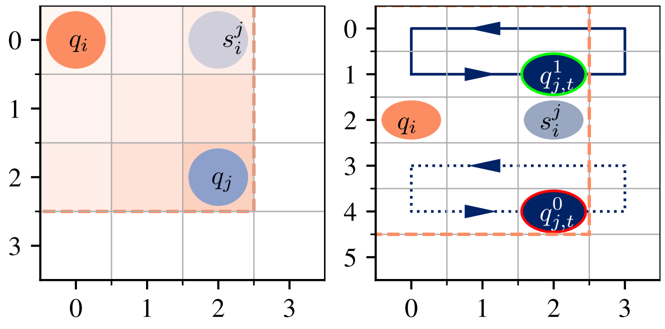
$$P_i(s^j_i | q_j) = \frac{e^{-\frac{1}{2\sigma^2}\|s^j_i - q_j\|^2_2}}{\sum_{q \in \mathcal{Q}_i(q_i)} e^{-\frac{1}{2\sigma^2}\|q - q_j\|^2_2}}. \tag{31}$$

If $q_j \notin \mathcal{Q}_i(q_i)$, agent i cannot observe agent j and thus obtains an empty observation, i.e., $s^j_i = \emptyset$. To summarize, the observation s^j_i follows

$$s^j_i = \begin{cases} q \text{ with probability } P_i(q|q_j) & \text{if } q_j \in \mathcal{Q}_i(q_i), \\ \emptyset \text{ with probability } 1 & \text{otherwise.} \end{cases} \tag{32}$$

From (32), we know that $s^j_i \in Q \cup \emptyset$. The observation set S_i is then $S_i \subseteq \prod_{j \in \mathcal{N}, j \neq i} (Q \cup \emptyset)$.

2) Likelihood Functions: At time t, there are two possible locations of the agent j, namely $q^0_{j,t}$ and $q^1_{j,t}$, depending on the value of $\theta_j \in \{0, 1\}$ (see Fig. 3b).



(a) Sensor

(b) Observation

Fig. 3: (a) An example distribution and sensor output ($s_i^j = [2, 0]$) for agent i (true location $q_i = [0, 0]$) sensing agent j (true location $q_j = [2, 2]$). Darker shades of orange indicate a higher probability of the sensor reading that location (left). (b) An example likelihood function $l_i(s_i^j | q_{i,t}, \theta_j)$ for a pair of agents i and j with the two possible models for agent j ($\theta_j \in \{0, 1\}$). Here $l_i(s_i^j | q_{i,t}, 1) > l_i(s_i^j | q_{i,t}, 0)$, as the sensor reading at s_i^j is more likely to be generated by $q_{j,t}^1$ than $q_{j,t}^0$.

For a given pair of hypothesis θ_j and its corresponding location $q_{j,t}^{\theta_j}$, from (32), the likelihood function $l_i^j(s_i^j | q_{i,t}, \theta_j)$ to get s_i^j for agent i is:

$$l_i^j(s_i^j | q_{i,t}, \theta_j) = \begin{cases} P_i(s_i^j | q_{j,t}^{\theta_j}), & \text{if } s_i^j \neq \emptyset, \\ 0 & \text{if } s_i^j = \emptyset \text{ and } q_{j,t}^{\theta_j} \in \mathcal{Q}_i(q_{i,t}), \\ 1 & \text{if } s_i^j = \emptyset \text{ and } q_{j,t}^{\theta_j} \notin \mathcal{Q}_i(q_{i,t}). \end{cases} \tag{33}$$

The local likelihood function $l_i(s_i | \theta, q_i)$ is then formed by taking the product of (33) across all the agents in the sensing range:

$$l_i(s_i | q_t, \theta) = \prod_{j \in Q, j \neq i} l_i^j(s_i^j | q_{i,t}, \theta_j). \tag{34}$$

C. Results

Fig. 4 shows the evolution of each agent's actual belief on true hypothesis $\theta^* = (1, 1, 1, 0)$. The three good agents' actual beliefs correctly converge to θ^* at time $t = 36$ (see Fig. 5f).[1] Fig. 5 shows snapshots of each agent's belief over the probability simplex. Within the first few timesteps, the good agents relatively quickly identify that each other are good as they both easily observe and communicate with each other (see Fig. 5b). However, since they do not observe agent 3 directly they cannot yet tell if that agent is good or bad. When agent 1 observes agent 3 (Fig. 5c) it approaches the correct actual belief. When all agents can communicate (Fig. 5d) they all start to converge to the correct actual belief. Later agents 1 and 2 converge at time 32 (Fig. 5e), which then communicate with agent 0 (Fig. 5f) at time 36 resulting in the converged result at Fig. 4. Note that agent 3 shares a randomly generated actual belief throughout the process as shown in the last row of Figure 5.

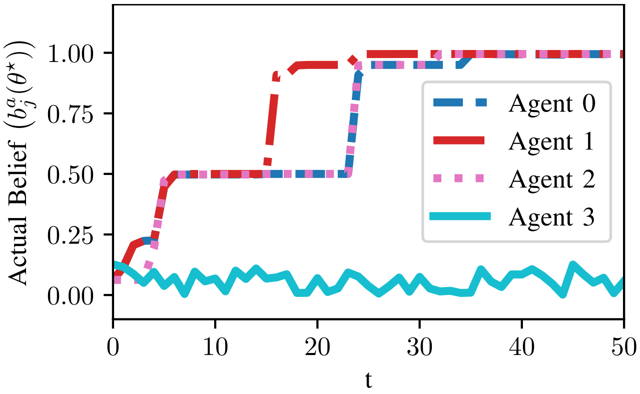


Fig. 4: Each agent's actual belief $b_{j,t}^a(\theta^*)$ for the true system state θ^* where $\theta^*(i) = (1, 1, 1, 0)$ over time t. Agent 3 (cyan) is the bad agent who shares randomly generated beliefs. The beliefs for agents 0 and 2 are very similar until $t = 28$ when agent 2 converges first.

VI. Conclusion

In this paper, we introduce a new robust distributed hypothesis testing algorithm in a time-varying network topology. Each agent makes use of both local and shared information to update its local and actual beliefs over all possible hypotheses. The proposed algorithm is simple to implement and robust to agents with Byzantine behaviors. We also prove that the algorithm guarantees almost sure convergence to the true hypothesis in the limit without global connectivity constraints. The simulation illustrates the validity of the proposed approach. Future work will perform convergence rate analysis and study how to plan the state paths of the team in a distributed manner to satisfy the convergence condition.

References

[1] V. V. Veeravalli, T. Basar, and H. V. Poor, "Decentralized sequential detection with a fusion center performing the sequential test," *IEEE Transactions on Information Theory*, vol. 39, no. 2, pp. 433–442, 1993.

[2] J. B. Rhim and V. K. Goyal, "Distributed hypothesis testing with social learning and symmetric fusion," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6298–6308, 2014.

[3] A. Tarighati, J. Gross, and J. Jaldén, "Decentralized hypothesis testing in energy harvesting wireless sensor networks," *IEEE Transactions on signal processing*, vol. 65, no. 18, pp. 4862–4873, 2017.

[4] M. Alanyali, S. Venkatesh, O. Savas, and S. Aeron, "Distributed bayesian hypothesis testing in sensor networks," in *Proceedings of the 2004 American control conference*, vol. 6. IEEE, 2004, pp. 5369–5374.

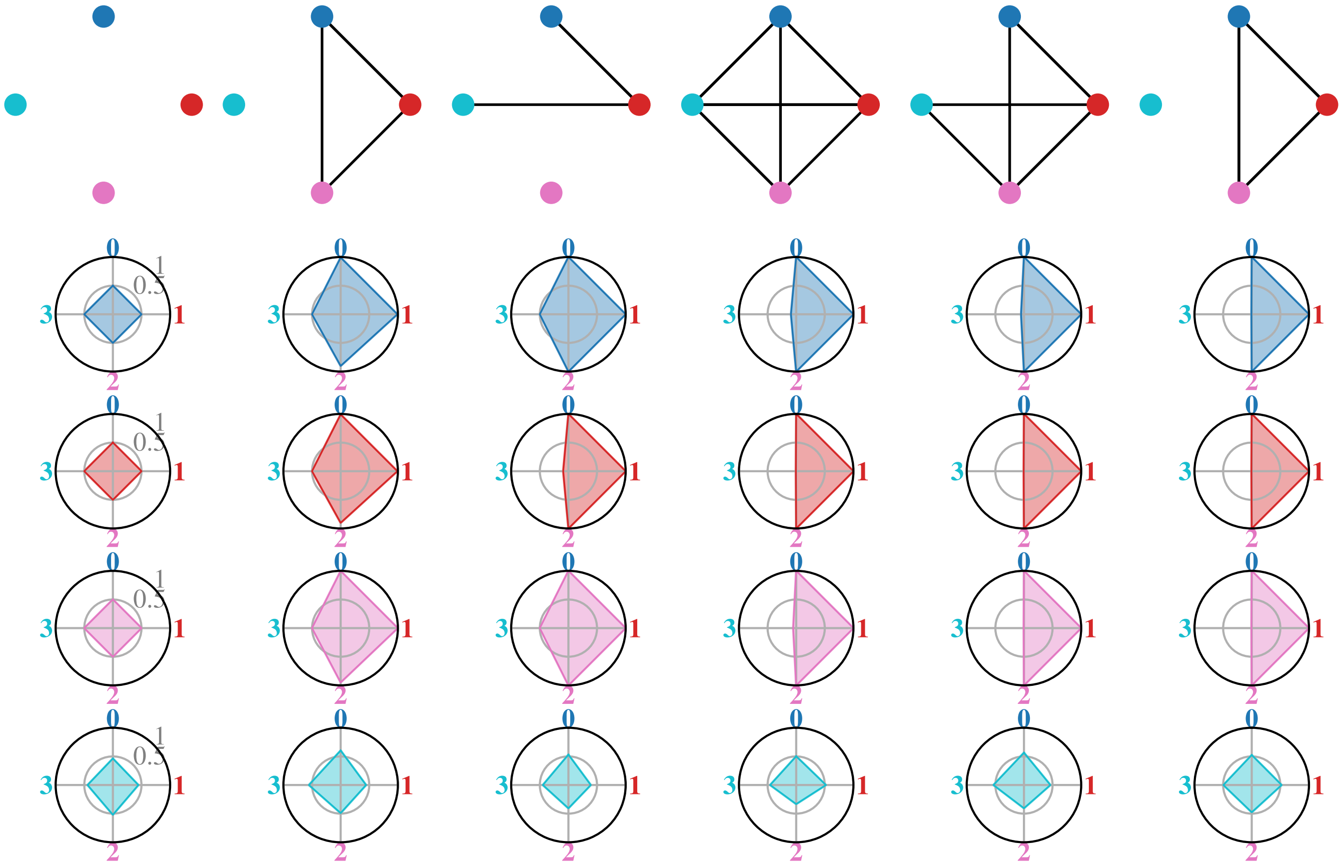
[5] R. Olfati-Saber, E. Franco, E. Frazzoli, and J. S. Shamma, "Belief consensus and distributed hypothesis testing in sensor networks," in *Networked Embedded Sensing and Control*. Springer, 2006, pp. 169–182.

[6] A. Jadbabaie, P. Molavi, A. Sandroni, and A. Tahbaz-Salehi, "Non-bayesian social learning," *Games and Economic Behavior*, vol. 76, no. 1, pp. 210–225, 2012.

[7] A. Nedić, A. Olshevsky, and C. A. Uribe, "Fast convergence rates for distributed non-bayesian learning," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 5538–5553, 2017.

[8] A. Lalitha, T. Javidi, and A. D. Sarwate, "Social learning and distributed hypothesis testing," *IEEE Transactions on Information Theory*, vol. 64, no. 9, pp. 6161–6179, 2018.

[1] A video of this simulation can be found at https://bit.ly/2ncUOhv.



(a) $t = 0$ (b) $t = 5$ (c) $t = 16$ (d) $t = 24$ (e) $t = 32$ (f) $t = 36$

Fig. 5: Evolution of the network topology and actual belief of each agent using radar plots over the probability simplex. The first row shows the time-varying network topology at different time instances. For the radar plots, the closer a vertex is to the edge the higher that the belief of the corresponding agent is good.

[9] A. Mitra, J. A. Richards, and S. Sundaram, "A new approach for distributed hypothesis testing with extensions to byzantine-resilience," in *2019 American Control Conference (ACC)*, July 2019, pp. 261–266.

[10] S. Shahrampour, A. Rakhlin, and A. Jadbabaie, "Distributed detection: Finite-time analysis and impact of network topology," *IEEE Transactions on Automatic Control*, vol. 61, no. 11, pp. 3256–3268, 2015.

[11] A. Nedić, A. Olshevsky, and C. A. Uribe, "Distributed learning with infinitely many hypotheses," in *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 6321–6326.

[12] L. Su and N. H. Vaidya, "Defending non-bayesian learning against adversarial attacks," *Distributed Computing*, vol. 32, no. 4, pp. 277–289, 2019.

[13] A. Mitra, J. A. Richards, and S. Sundaram, "A new approach to distributed hypothesis testing and non-bayesian learning: Improved learning rate and byzantine-resilience," *arXiv preprint arXiv:1907.03588*, 2019.

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

[15] P. Blanchard, R. Guerraoui, J. Stainer *et al.*, "Machine learning with adversaries: Byzantine tolerant gradient descent," in *Advances in Neural Information Processing Systems*, 2017, pp. 119–129.

[16] D. Alistarh, Z. Allen-Zhu, and J. Li, "Byzantine stochastic gradient descent," in *Advances in Neural Information Processing Systems*, 2018, pp. 4613–4623.