History Data Driven Distributed Consensus in Networks

Venkatraman Renganathan * **Angela Fontan** **
Karthik Ganapathy ***

*Department of Automatic Control - LTH, Lund University, Lund,
Sweden (e-mail: venkatraman.renganathan@control.lth.se).*
**Division of Decision and Control Systems, KTH Royal Institute of
Technology, Stockholm, Sweden (e-mail: angfon@kth.se)*
*** Department of Mechanical Engineering, The University of Texas at
Dallas, Richardson, TX, USA (e-mail:
karthik.ganapathy@utdallas.edu)*

Abstract: The association of weights in a distributed consensus protocol quantify the trust that an agent has on its neighbors in a network. An important problem in such networked systems is the uncertainty in the estimation of trust between neighboring agents, coupled with the losses arising from mistakenly associating wrong amounts of trust with different neighboring agents. We introduce a probabilistic approach which uses the historical data collected in the network, to determine the level of trust between each agent. Specifically, using the finite history of the shared data between neighbors, we obtain a configuration which represents the confidence estimate of every neighboring agent's trustworthiness. Finally, we propose a History-Data-Driven (HDD) distributed consensus protocol which translates the computed configuration data into weights to be used in the consensus update. The approach using the historical data in the context of a distributed consensus setting marks the novel contribution of our paper.

Keywords: History, Memory, Data-driven, Distributed Consensus, Networked System.

1. INTRODUCTION

We study the problem of consensus in a multi-agent system in the presence of untrustworthy agents in this paper. Many cooperative tasks involving networked agents require them to utilize distributed consensus protocols to coordinate agreement on certain quantities of interest, with applications such as formation control in robotics (Fax and Murray (2004); Ren and Beard (2008)), agreement seeking in opinion dynamics (Hegselmann and Krause (2002); Blondel et al. (2009); Fontan and Altafini (2021)), or cyber-networks comprising of many interconnected smart entities which relies on distributed consensus protocols for efficient operations (Renganathan et al. (2021)). However, Pasqualetti et al. (2012) showed that the distributed nature of networks opens up many attack points for malicious attackers rendering them vulnerable. This work considers the situation where well-behaving agents (called "cooperative" in our notation) in a network seek to achieve consensus in the presence of "untrustworthy" agents (called "potentially non-cooperative" in our notation) using the inference from the past interactions with their neighbors.

A related problem is that of consensus in unreliable networks, which has been largely studied in the literature, see e.g., Lamport et al. (2019); Agmon and Peleg (2004);

Sundaram and Hadjicostis (2008); LeBlanc et al. (2013); Saldaña et al. (2017); Dibaji et al. (2018), and specifically resilient consensus protocols, such as the W-MSR protocol by LeBlanc et al. (2013), have been developed in the recent past to guarantee resiliency by intelligently constructing a nonlinear consensus update. In general, the update rule of these distributed consensus protocols depends upon the current time step information obtained from all the neighboring agents in the network. An exception is the protocol for resilient consensus proposed in Saldaña et al. (2017), named SW-MSR, which extends the classical W-MSR algorithm by introducing a sliding window approach that allows the agents to store the values received from their neighbors at the previous T time steps. While the resilient consensus literature imposes an assumption on the connectivity and the total number of non-cooperative (also called non-reliable or malicious) agents in the network, the recent work by Yemini et al. (2021) departs from such assumptions and uses the notion of trust in order to maintain consensus in a networked system in the presence of malicious agents.

Our aim is to design a distributed consensus protocol that enables each agent to estimate the trustworthiness of its neighbors, represented by a (normalized) non-negative value in $[0, 1]$, where 0 (resp., 1) indicates that the corresponding agents do not trust (resp., trust fully) each other, with the idea that an agreement should be reached only between agents whose trust in each other is nonzero. Similar to Yemini et al. (2021), in this work we do not impose

any structural or connectivity assumption on the network or any assumption on the total number of potentially non-cooperative agents, but we consider the observed history at the previous T time steps to estimate trust between each agent in the network. Such an approach offers a paradigm shift from considering memory-less update in distributed consensus protocols, which do not offer the debugging capabilities of getting to know *when and where* an intentional attack or a fault happened in the network, thereby possibly lacking the retrospecting ability to analyze for anomalies. On the other hand, it is not practical for every agent in a network to have infinite book-keeping abilities to store the shared values of its neighbors information to analyze for any anomalies. However, given a finite memory resource is made available for agents in a network, distributed consensus algorithms can be reinforced with retrospecting abilities to enhance the quality of the decisions that they make and mimic the trust-based decision-making behavior of humans in a distributed setting.

Under the local information model setting, the protocol we propose is related to the bounded confidence models in opinion dynamics (see for instance Hegselmann and Krause (2002)) where each agent updates its state (analogous to its opinion) based only on the states of agents that are within a certain confidence range of its own, enforcing the idea that only trustworthy agents (here intended as agents with similar opinions) can influence each other. Moreover, inspired by Lorenz (2009); Liang et al. (2013); Morarescu and Girard (2011), we assume that the confidence bounds are heterogeneous (i.e., agent-dependent) and time-dependent. The problem of consensus in networks with random weighting matrices was studied in Tahbaz-Salehi and Jadbabaie (2008, 2006). We refer to a closely aligned idea that appeared in Yu and Vorobeychik (2019b,a), where malicious nodes were identified in an uncertain network with high confidence and removed. We consider extending a similar idea as Yu and Vorobeychik (2019a) for designing a distributed consensus protocol using an history data-driven approach. Specifically, at each time step, we use the available finite historical data to estimate the first two moments of an unknown distribution governing the true nature (called "configuration" in our notation) of an agent's neighbors.

Statement Of Contributions: We propose a novel history data-driven distributed consensus protocol for networks. Specifically, our main contributions are as follows:

(1) We model the true nature of neighboring agents of an agent in a network as a random vector (which we term as the "configuration" of neighbors), and we learn the parameters governing its true but unknown distribution from the collected historical data.
(2) We translate the trustworthiness that resulted from the neighbor configuration into weights and propose a new History-Data-Driven (HDD) distributed consensus protocol for networks.
(3) We demonstrate by means of numerical simulation that our proposed design effectively models the neighbor configuration from the historical data, and arrives at a trust-based consensus [1].

---
[1] Notion introduced in Definition 2.

The rest of the paper is organized as follows: The preliminaries of the consensus protocol and the definition of a neighbor configuration are established in section 2. In section 3, the empirical estimation of the configuration parameters from the past historical data is discussed. The proposed HDD distributed consensus protocol is presented in section 4 along with the effect of parameter variations. Our proposed algorithm is then demonstrated in section 5. Finally, the paper is closed in section 6 with a summary and research directions for the future.

NOTATION & PRELIMINARIES

We denote the set of real numbers, integers, non-negative real numbers and non-negative integers by $\mathbb{R}, \mathbb{Z}, \mathbb{R}_{\geq 0}, \mathbb{Z}_{\geq 0}$ respectively. The operator $\setminus$ denotes the set subtraction. The cardinality of the set M is denoted by $|M|$ and its ith element by $\{M\}_i$. The ith element of a vector x is denoted by $[x]_i$ or simply x_i and the Euclidean norm of x is denoted by $\|x\|_2$ or simply $\|x\|$. A vector in $\mathbb{R}^n$ with all its elements being ones is denoted by $\mathbf{1}_n$. The jth column of a matrix A is denoted by A_j. An element in i^{th} row and j^{th} column of matrix A is denoted by A_{ij}. The uniform distribution between $a, b \in \mathbb{R}$, $a < b$ is denoted by $U[a, b]$.

2. PROBLEM FORMULATION

2.1 Consensus Dynamics of a Network

Consider a network having N agents whose connectivity is modeled via an undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ represents the set of agents with $|\mathcal{V}| = N$. A set of time-invariant communication links amongst the agents is represented using $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. We associate with each agent $i \in \mathcal{V}$ a state $x_i(t) \in \mathbb{R}$ at time $t \in \mathbb{Z}_{\geq 0}$. Let the set of inclusive neighbors be defined as $\mathcal{J}_i = \mathcal{N}_i \cup \{i\}$, where $\mathcal{N}_i = \{j \in \mathcal{V} : (j, i) \in \mathcal{E}\}$ is the neighbor set of agent i, whose states are available to agent i via communication links. The degree of i is denoted as $d_i = |\mathcal{N}_i|$, and every agent is assumed to have access to its own state at any time t. At any time t, each agent updates its own state based on its current state and the states of its neighboring agents according to a prescribed memory-less update rule

$$x_i(t+1) = f_i(x_j(t)), \quad j \in \mathcal{J}_i, \ i \in \mathcal{V}. \qquad (1)$$

Typical distributed consensus protocols of the form (1) involve associating a weight corresponding to all inclusive neighbors $j \in \mathcal{J}_i$ and using it in the consensus update. In this work, we consider the weighted averaging type of update protocols, namely $x(t + 1) = W(t)x(t)$ with $x(t) = [x_1(t) \dots x_N(t)]^\top$, that is,

$$x_i(t+1) = \sum_{j \in \mathcal{J}_i} w_{ij}(t)x_j(t), \quad i \in \mathcal{V}, \qquad (2)$$

where $W(t)$ is an element-wise non-negative time-varying weighting matrix with its entries $w_{ij}(t) \geq 0$ modeling the trustworthiness associated by agent i on its inclusive neighboring agents $j \in \mathcal{J}_i$ at each time t. Olshevsky and Tsitsiklis (2009) showed that, under assumptions on the graph (such as connectivity of $\mathcal{G}$) and on the weights of $W(t)$ (e.g., weights chosen according to a convex combination, making $W(t)$ a stochastic matrix), an asymptotic consensus value is guaranteed by (2), that is, $\exists c \in \mathbb{R}$ s.t. $\lim_{t \to \infty} x(t) = c\mathbf{1}_N$.

In this work we consider the situation in which some agents may not follow the update rule (2). To this end, we introduce the notion of cooperative and (potentially) non-cooperative agents.

Definition 1. An agent $i \in \mathcal{V}$ is said to be *cooperative* if it updates its state based on (2). It is said to be *(potentially) non-cooperative* [2], otherwise.

Definition 2. An agent $i \in \mathcal{V}$ is said to be in a *trust-based consensus* with a set of identified trusted neighbors $j \in \overline{\mathcal{N}}_i \subseteq \mathcal{N}_i$ if $\lim_{t \to \infty} \|x_i(t) - x_j(t)\| = 0$ for all $j \in \overline{\mathcal{N}}_i$.

The intuition is that if the cooperative agents manage to correctly identify and distrust non-cooperative agents, effectively trusting only (a subset of) their neighbors, then the sequence $\{x_i(t)\}_{t \geq 0}$ is convergent for all cooperative agents i, i.e., $x_i(t) \to x_i^* \in \mathbb{R}$, and either the agents reach an agreement, i.e., $x_i^* = x_j^*$ for all $i, j \in \mathcal{V}$, or clustering, i.e., $x_i^* = x_j^*$ for all i, j belonging to the same cluster. However, a smart non-cooperative agent, if undetected, may act as a leader and be followed by a set of cooperative agents (whose corresponding sequence $\{x_i(t)\}_{t \geq 0}$ then, in that case, need not be convergent).

2.2 Availability of Historical Data

When a memory-less distributed protocol like (2) is used by the cooperative agents $i \in \mathcal{V}$ under the setting where some agents *might* be non-cooperative, the resulting asymptotic consensus can be easily manipulated by some smart adversaries. Under this setting, the mechanism we propose for each agent with uncertain information on the nature of its neighbors, is to observe the neighbors' shared data for a certain period of time, arrive at an estimate of the neighbors' trustworthiness, and subsequently use it in its update to arrive at a consensus. To facilitate a tractable problem formulation and to make the resulting consensus algorithm suitable for dynamic implementation, we consider a finite historical data of length $T \in \mathbb{Z}_{\geq 0}$ updated in a rolling horizon fashion [3]. At all time steps t, every agent $i \in \mathcal{V}$ is *assumed* to have access to the history of its own values and to its neighboring agents' values $x_j(t), j \in \mathcal{N}_i$ for the past T time-steps. That is, with $\kappa_{t,T} = \{t - l\}_{l=0}^{T-1}$, we have

$$\mathfrak{X}_{i,j}^T(t) = \{x_j(k) \mid j \in \mathcal{N}_i, \ k \in \kappa_{t,T}\},$$
$$\mathfrak{X}_{i,i}^T(t) = \{x_i(k) \mid k \in \kappa_{t,T}\},$$
$$\mathfrak{X}_{i,\mathcal{N}_i}^T(t) = \{\mathfrak{X}_{i,j}^T(t) \mid j \in \mathcal{N}_i\}.$$

Thus, the main purpose of this work is *(i) to design a protocol that allows each cooperative agent $i \in \mathcal{V}$ to estimate the trustworthiness of its neighbors at each time step t, given the history $\mathfrak{X}_{i,\mathcal{N}_i}^T(t)$ and $\mathfrak{X}_{i,i}^T(t)$ for the past T time steps; (ii) to study the role of the estimated trustworthiness in solving the trust-based consensus problem for the cooperative agents, despite the presence of non-cooperative agents in the network.*

---

[2] For instance, an agent $i \in \mathcal{V}$ can act *non-cooperatively* by applying random update function $f_i'(\cdot)$ other than (2) at all time-steps.
[3] Future work will seek to understand the behaviour with growing history over time.

3. SET MEMBERSHIP BASED EMPIRICAL ESTIMATION OF CONFIGURATION

In this section, we describe how to learn the trustworthiness of neighbors, given their T time steps historical data. For each agent $i \in \mathcal{V}$, the *configuration* of neighbors $\mathcal{N}_i$ at time t, denoted by $\pi_t^i \in [0,1]^{d_i}$, encodes the degree of trustworthiness of every neighbor $j \in \mathcal{N}_i$. A neighbor $j \in \mathcal{N}_i$ is said to be completely trustworthy or not trustworthy if $\left[\pi_t^i\right]_j$ equals to 1 or 0, respectively, and any value in $[0,1]$ defines its degree of trustworthiness. Similarly, we define $\bar{\pi}_t^i = \mathbf{1}_{d_i} - \pi_t^i$ to be the configuration representing the degree of non-cooperativeness of the neighbors at time t. Note that π_t^i is a random vector where the jth entry of π_t^i corresponding to the neighbor $j \in \mathcal{N}_i$ is supported on a compact interval $[0,1]$. Further, $\pi_t^i \sim \mathbb{P}_t^i$ with $\mathbb{P}_t^i$ denoting the true but *unknown* distribution of the π_t^i supported on a compact set $[0,1]^{d_i}$. Let $\mu_t^i \in \mathbb{R}^{d_i}$ and $\Sigma_t^i \in \mathbb{R}^{d_i \times d_i}$ denote the true mean and covariance respectively associated with $\mathbb{P}_t^i$. Though in reality $\mathbb{P}_t^i$ is not readily available, it can be estimated from data, that is, using the T time steps history data, it is possible to form an empirical distribution $\hat{\mathbb{P}}_t^i$. Let us denote the mean and the covariance of $\hat{\mathbb{P}}_t^i$ by $\hat{\mu}_t^i$ and $\hat{\Sigma}_t^i$, respectively. Here, $\left[\hat{\mu}_t^i\right]_j$ is agent i's estimated trustworthiness at time t about the neighboring agent $j \in \mathcal{N}_i$ given its past T time steps historical data. We propose a set membership based approach to estimate the parameters of the empirical configuration distribution $\hat{\mathbb{P}}_t^i$ given the historical data $\mathfrak{X}_{i,i}^T(t)$ and $\mathfrak{X}_{i,\mathcal{N}_i}^T(t)$. We base the following discussion on the presumption that a neighbor $j \in \mathcal{N}_i$ is believed to be more trustworthy by agent i, if j's values are in the desired vicinity of agent i's value throughout the considered past.

3.1 The ϵ-Neighborhood Based Set Membership

To define a set membership based estimation, we require a set of confidence neighborhoods for all the past T time steps. Thus, for all $k \in \kappa_{t,T}$, the confidence neighborhood around the $x_i(k)$ is defined as,

$$\mathcal{B}_{x_i(k)}(\epsilon_{i,k}) = \{y \in \mathbb{R} \mid \|y - x_i(k)\|_2 \leq \epsilon_{i,k}\}, \quad (3)$$

where $\epsilon_{i,k} > 0$ is the confidence bound for agent i at time k. To value the recent past more than the distant past, we assume that at each time step t agent $i \in \mathcal{V}$ is free to choose a decreasing sequence of confidence bounds $\epsilon_{i,k}, \forall k \in \kappa_{t,T}$ as follows:

$$\epsilon_{i,t-(T-1)} > \cdots > \epsilon_{i,t-2} > \epsilon_{i,t-1} > \epsilon_{i,t} > 0. \quad (4)$$

Using the confidence neighborhoods $\mathcal{B}_{x_i(k)}(\epsilon_{i,k})$, and the information sets $\mathfrak{X}_{i,i}^T(t), \mathfrak{X}_{i,\mathcal{N}_i}^T(t)$, we define the set membership counter for all time steps $k \in \kappa_{t,T}$ as follows,

$$\mathfrak{N}_k^i = \{j \in \mathcal{N}_i \mid x_j(k) \in \mathcal{B}_{x_i(k)}(\epsilon_{i,k})\}. \quad (5)$$

Here, $\mathfrak{N}_k^i \subseteq \mathcal{N}_i$ accounts for the neighbors $j \in \mathcal{N}_i$ who share their values in the vicinity of the agent i, at time step k of the past history. It is possible that at time $k \in \kappa_{t,T}$, the set $\mathfrak{N}_k^i$ may turn out to be empty, or equal to $\mathcal{N}_i$.

3.2 Estimating Parameters of Configuration Distribution

Now, we illustrate how each agent $i \in \mathcal{V}$ estimates the trustworthiness of its neighbors at each time instant t.

First, a frequency counter and a discounted importance vector are defined for each agent as follows. A frequency counter $\mathcal{C}_j^i(t)$ records, at each time step t, the time indices $k \in \kappa_{t,T}$ where the neighbor $j \in \mathcal{N}_i$ belonged to $\mathfrak{N}_k^i$:

$$\mathcal{C}_j^i(t) = \left\{ k \in \kappa_{t,T} \mid j \in \mathfrak{N}_k^i \right\} \quad j \in \mathcal{N}_i.$$

A discounted importance vector $\mathfrak{d}_j^i \in \mathbb{R}^T$ qualitatively captures how a neighboring agent $j \in \mathcal{N}_i$ behaved with respect to the agent i, by valuing the recent past more than the distant past using a discount factor $\nu_{i,t} \in (0,1)$:

$$\left[\mathfrak{d}_j^i \right]_k = \begin{cases} \nu_{i,t}^{t-k}, & \text{if } k \in \mathcal{C}_j^i(t), \\ 0, & \text{if } k \notin \mathcal{C}_j^i(t). \end{cases}$$

Finally, the estimated mean $\hat{\mu}_t^i$ and estimated covariance $\hat{\Sigma}_t^i$ at time t are computed as:

$$\left[\hat{\mu}_t^i \right]_j = \frac{1}{T} \sum_{k \in \kappa_{t,T}} \left[\mathfrak{d}_j^i(t) \right]_k, \quad j \in \mathcal{N}_i, \tag{6}$$

$$\hat{\Sigma}_t^i = \frac{1}{T-1} \sum_{k \in \kappa_{t,T}} \left(\mathcal{D}_k^i - \hat{\mu}_t^i \right) \left(\mathcal{D}_k^i - \hat{\mu}^i(t) \right)^\top, \tag{7}$$

where the variability matrix [4] $\mathcal{D}^i \in \mathbb{R}^{d_i \times T}$ is given by

$$\mathcal{D}_{jk}^i = \frac{\|x_i(k) - x_j(k)\|}{1 + \|x_i(k) - x_j(k)\|}, \quad j \in \mathcal{N}_i, k \in \kappa_{t,T}. \tag{8}$$

Then an estimate [5] of trustworthy configuration is $\hat{\pi}_t^i = \hat{\mu}_t^i$, and subsequently $\hat{\bar{\pi}}_t^i = \mathbf{1}_{d_i} - \hat{\pi}_t^i$ would be an estimate of non-cooperative configuration. In the next section, we elucidate how an agent $i \in \mathcal{V}$ can use the inferred trustworthiness of its neighbors $j \in \mathcal{N}_i$ to update its value.

4. DESIGN OF AN HISTORICAL DATA-DRIVEN DISTRIBUTED CONSENSUS PROTOCOL

In this section, we use the obtained trustworthiness information of the neighbors of an agent to design a distributed consensus protocol. Following the definition of HDD protocol, we discuss the effect of various parameter variations on the consensus obtained using HDD protocol.

4.1 An HDD Distributed Consensus Protocol

For every collaborative agent $i \in \mathcal{V}$, $\hat{\mu}_t^i$ denotes the estimated trustworthiness of its neighbors given their past historical data. Further, every collaborative agent i has to trust itself completely at all time steps. Therefore, at each time step t, we form the augmented trust vector $z_i^\dagger(t) \in \mathbb{R}^{|\mathcal{J}_i|}$ as

$$z_i^\dagger(t) = \begin{bmatrix} \hat{\mu}_t^i \\ 1 \end{bmatrix}, \quad \text{since } \mathcal{J}_i = \mathcal{N}_i \cup \{i\}. \tag{9}$$

Then, every collaborative agent $i \in \mathcal{V}$ updates its states using the following proposed History-Data-Driven (HDD) distributed consensus protocol as follows

$$x_i(t+1) = \sum_{j \in \mathcal{J}_i} \underbrace{\frac{[z_i^\dagger(t)]_j}{\left\| z_i^\dagger(t) \right\|_1}}_{:=w_{ij}(t)} x_j(t), \tag{10}$$

where the weights $w_{ij}(t) \in [0,1], \forall i \in \mathcal{V}, j \in \mathcal{J}_i$, and $\sum_{j \in \mathcal{J}_i} w_{ij}(t) = 1$. Moreover, $w_{ij}(t) = 0$ if and only if $j \notin \mathcal{J}_i$ or $j \notin \mathfrak{N}_k^i$ for all $k \in \kappa_{t,T}$.

Remark 1. The weights $w_{ij}(t)$ given by (10) translates the trustworthiness information of neighboring agents into weights for the distributed consensus update rule. The HDD protocol is actually a nonlinear consensus update, such as the W-MSR protocol, as the weight $w_{ij}(t)$ computed by agent i for its neighbor $j \in \mathcal{N}_i$ with an informed choice of the parameters $T, \epsilon_{i,k}$ and $\nu_{i,t}$ may turn out to be zero based on the inference using the historical data, meaning that at time t, agent i neglects neighbor j's contribution.

Remark 2. Following the proof of Proposition 1 present in Morarescu and Girard (2011), it is possible to prove that, no matter the choice of $T \geq 1$ and $\nu_{i,t}$, the sequence $\{x_i(t)\}_{t \geq 0}$ is convergent for all cooperative agents i, that is, $x_i(t) \to x_i^*$, if, for each cooperative agent i, the confidence bounds $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}}$ at each instant t are chosen so that $\epsilon_{i,t-T+1}$ is time-decaying and eq. (4) is satisfied [6]. Possible choices are, for instance, $\epsilon_{i,t-T+1} = R_i e^{-\rho_i(t-T+1)}$ or $\epsilon_{i,t-T+1} = R_i \rho_i^{t-T+1}$, where $R_i \in \mathbb{R}_{\geq 0}$ and $\rho_i \in (0,1)$.

4.2 Effects of Parameter Variations

The design parameters of our algorithm are $T \in \mathbb{Z}_{\geq 0}$ (T finite), $\{\nu_{i,t}\}_{i \in \mathcal{V}, t \in \mathbb{R}_+}$, and $\{\epsilon_{i,k}\}_{i \in \mathcal{V}, k \in \kappa_{t,T}}$. The parameter $\nu_{i,t} \in (0,1)$ can be regarded as the forgetting factor for an agent $i \in \mathcal{V}$ at time t and thus influences how much an agent is willing to remember its neighbors' past interactions from the time t given the history length T (defined respecting the available memory constraints). For instance, $\nu_{i,t}$ closer to 1 indicates that the agent emphasizes its recent past interactions with its neighbors more and hence its forgetfulness decreases rather slowly over time. On the other hand, $\nu_{i,t}$ closer to 0 indicates that the agent forgets quickly. The next parameter confidence bound $\epsilon_{i,k}$ at time k is the agent i's freedom to choose its desired vicinity area around its values to value its neighbors appropriately. For instance, a cautious agent $i \in \mathcal{V}$ would tend to have a small $\epsilon_{i,k}$ even at its distant past, while a relaxed agent may tend to choose a generous $\epsilon_{i,k}, \forall k \in \kappa_{t,T}$. Given that $\mathfrak{N}_k^i$ for an agent $i \in \mathcal{V}$ directly depends upon the $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}}$ and which in turn defines the $\hat{\mu}_t^i$, it is clear that the resulting consensus is directly impacted by the choice of the confidence bound that an agent chooses according to its behavioural aspects. Though the efficacy of the proposed update protocol is limited upon the memory constraint defining the parameter T, its freedom in the design of other design parameters makes it both an interesting and powerful consensus protocol.

Remark 3. The collected historical data can be used to predict the neighbors value using machine learning techniques and if the neighbor shares a value closer to the

---

[4] Several choices for defining the matrix $\mathcal{D}^i$ exist other than (8).

[5] This style of inferring the trustworthiness has the potential of being vulnerable with smarter adversaries as they can manipulate the estimated parameters $\hat{\mu}_t^i$ and $\hat{\Sigma}_t^i$ to render them off from their respective true values μ_t^i and Σ_t^i. Future research will seek to address this using the distributionally robust stochastic program (DRSP) model described in Delage and Ye (2010).

[6] Future research will explore this direction and seek to address provable convergence to *finite-time* trust-based consensus.

predicted value, agent i can allocate an higher trust to value their contribution more and thereby define *data-driven predictive consensus* protocol. Another variation to HDD protocol would be to remove neighbors whose trustworthiness fall below a specified trust-threshold and subsequently using only the remaining neighbors values. Future work will seek address above variations and to investigate adaptive designs of discount factor $\nu_{i,t}$ and confidence bounds $\epsilon_{i,k}, \forall k \in \kappa_{t,T}$.

5. A NUMERICAL EXAMPLE

In this section, we elaborate the simulation results that we performed to demonstrate our proposed HDD distributed consensus protocol. We considered an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $|\mathcal{V}| = N = 13$ agents. Further, the first 10 agents were assumed to be cooperative, and are denoted by $\mathcal{V}_c = \{1, \ldots, 10\}$, and the rest $\mathcal{V}_{nc} = \mathcal{V} \backslash \mathcal{V}_c$ to be non-cooperative. The cooperative nodes $i \in \mathcal{V}_c$ were randomly connected with probability $p = 0.4$ (here, p denotes the probability of an edge between two nodes), while each non-cooperative node $i \in \mathcal{V}_{nc}$ was connected to all cooperative nodes. All agents were given a random fixed history of data generated for a considered history of length T. The HDD protocol was demonstrated for a total of $T_t = 200$ time steps with the new state trajectories of neighboring agents being used to update the historical data in a rolling horizon fashion. Each agent $i \in \mathcal{V}$ was given random confidence bounds (decreasingly sorted) for all t where each $\epsilon_{i,k}$ was drawn from $U[\underline{\epsilon}, \overline{\epsilon}]$ with the lower limit set to a constant value, $\underline{\epsilon} = 0.01$ and the upper limit was varied as $\overline{\epsilon} \in \{0.5, 1, 1.5\}$ to observe different behaviours. Every agent $i \in \mathcal{V}$ was given the same discount factor $\nu_{i,t} = \nu \in (0,1)$ at a given time step t. The HDD protocol was executed by varying one of the parameters T, ν, $\overline{\epsilon}$ while keeping the rest fixed.

The results of our simulation are shown in Figure 1. It is assumed that every non-cooperative agent follows a random state update rule. On all the sub-figures of Figure 1, the discount factor variations with $\nu \in \{0.05, 0.50, 0.95\}$ are shown. With low values of the discount factor, we observed clustering behaviour between agents, and with higher values of discount factor, the normal consensus convergence is observed. This is due to the fact that higher values of ν enabled the agents to remember the past interactions of their neighbors to a greater extent. The effect of varying the confidence bounds are shown in sub-figures 1a, 1b and 1c, respectively for $\overline{\epsilon} = 0.5, 1.0, 1.5$. Higher values of confidence bounds encouraged the agents to cooperate with each other, while lower values of confidence bounds resulted in delayed cooperation and in clustering behaviour between agents. Finally, when the history length was reduced to $T = 5$, the agents converged quickly thanks to small memory and big enough confidence bound. If the agents were to safeguard themselves against non-cooperative agents, their best bet would be to have small confidence bounds; however, such a strategy might lead to clustering behaviour. This explains that there is a definite trade-off that the agents have to observe if they plan on safely interacting with their neighbors. A detailed investigation of the effects of the parameters on the resulting HDD protocol weights and the final consensus value is available in the appendix of Renganathan

et al. (2022). The code used to obtain the simulation results is made publicly available at https://github.com/venkatramanrenganathan/HDDConsensus.

6. CONCLUSION & FUTURE OUTLOOKS

We proposed a novel historical data-driven distributed consensus protocol for uncertain networks. Our proposed approach formulates the uncertainty about the trustworthiness of neighbors of an agent as a random vector termed as configuration, and learns the parameters defining its unknown but true distribution via history data-driven approach. Subsequently, the trustworthiness of all neighbors of an agent is inferred leading to the proposed HDD distributed consensus protocol. Our simulation results demonstrated the effectiveness of our proposed idea. As a future work, we seek to investigate the moment uncertainty along with the losses due to mistakenly associating wrong trust with neighbors given their historical data using distributionally robust optimization techniques. Other promising directions are investigating adaptive designs for confidence bounds and discount factors, and to design an history data-driven predictive consensus algorithm.

REFERENCES

Agmon, N. and Peleg, D. (2004). Fault-tolerant gathering algorithms for autonomous mobile robots. 1070–1078.

Blondel, V.D., Hendrickx, J.M., and Tsitsiklis, J.N. (2009). On krause's multi-agent consensus model with state-dependent connectivity. *IEEE Transactions on Automatic Control*, 54(11), 2586–2597.

Delage, E. and Ye, Y. (2010). Distributionally robust optimization under moment uncertainty with application to data-driven problems. *Operations research*, 58(3), 595–612.

Dibaji, S.M., Ishii, H., and Tempo, R. (2018). Resilient randomized quantized consensus. *IEEE Transactions on Automatic Control*, 63(8), 2508–2522.

Fax, J. and Murray, R. (2004). Information flow and cooperative control of vehicle formations. *IEEE Transactions on Automatic Control*, 49(9), 1465–1476.

Fontan, A. and Altafini, C. (2021). The role of frustration in collective decision-making dynamical processes on multiagent signed networks. *IEEE Transactions on Automatic Control*, to appear.

Hegselmann, R. and Krause, U. (2002). Opinion Dynamics and Bounded Confidence Models, Analysis and Simulation. *Journal of Artificial Societies and Social Simulation*, 5(3), 1–33.

Lamport, L., Shostak, R., and Pease, M. (2019). The byzantine generals problem. In *Concurrency: the Works of Leslie Lamport*, 203–226.

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

Liang, H., Yang, Y., and Wang, X. (2013). Opinion dynamics in networks with heterogeneous confidence and influence. *Physica A: Statistical Mechanics and its Applications*, 392(9), 2248–2256.

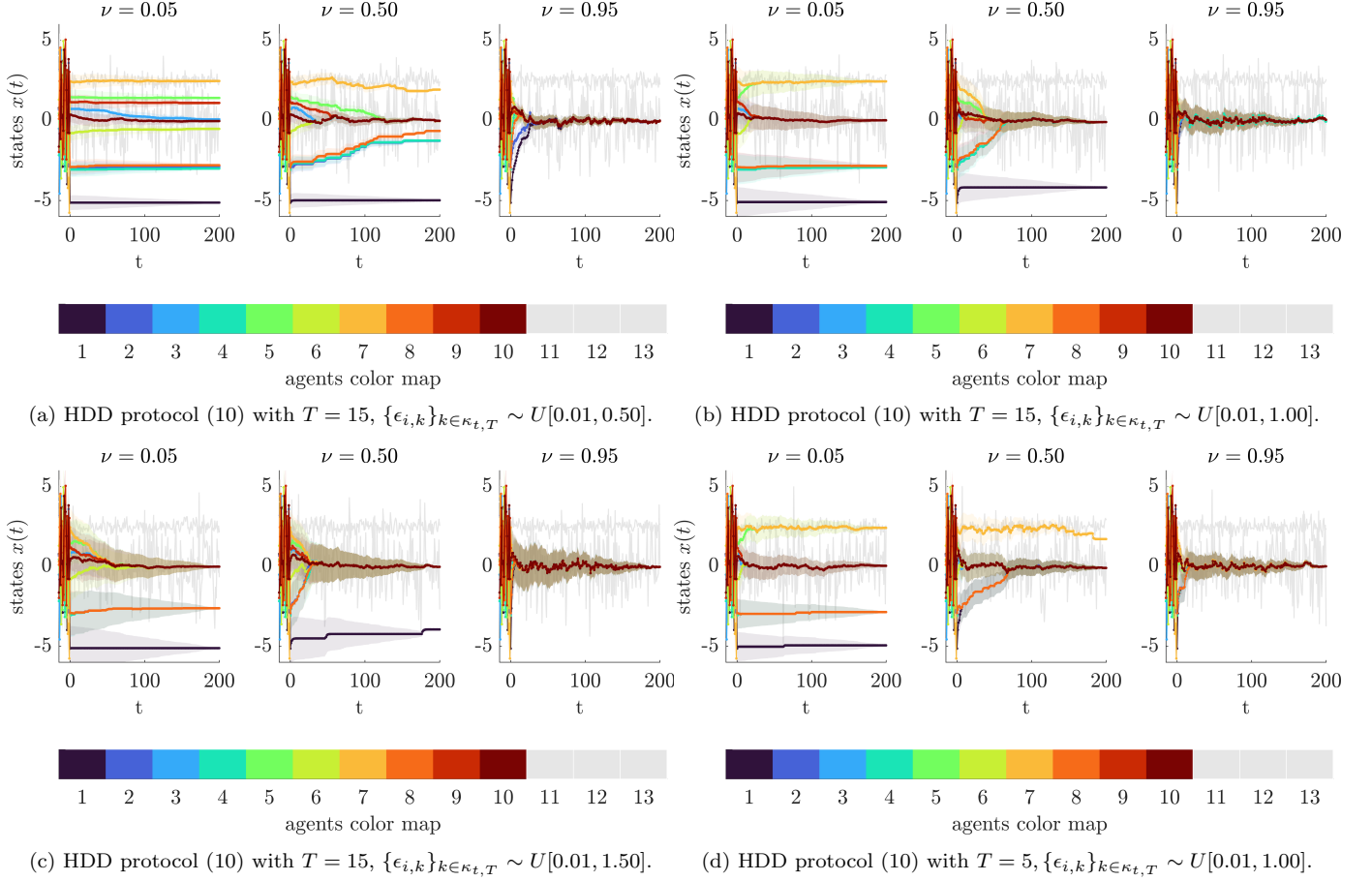Lorenz, J. (2009). Heterogeneous bounds of confidence: Meet, discuss and find consensus! *Complexity*, 15(4), 43–52.

Fig. 1. Effect of parameters variation for the HDD protocol (10): states' trajectories $x(t)$. The color map indicates cooperative agents (i.e., $i \in \mathcal{V}_c$), while non-cooperative agents (i.e., $i \in \mathcal{V}_{nc}$) are shown in grey color. Each panel shows the evolution of agents' states $x_i(t)$, $i \in \mathcal{V}$, for $\nu = 0.05, 0.5, 0.95$, with the confidence bounds $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[\underline{\epsilon}, \overline{\epsilon}]$ represented by shaded areas. (a),(b),(c): Effect of varying the confidence bounds; here $T = 15$, $\underline{\epsilon} = 0.01$ and $\overline{\epsilon} = \{0.5, 1.0, 1.5\}$. (d): Effect of varying the history length T; here $T = 5$, $\underline{\epsilon} = 0.01$ and $\overline{\epsilon} = 1$.

Morarescu, I.C. and Girard, A. (2011). Opinion dynamics with decaying confidence: Application to community detection in graphs. *IEEE Transactions on Automatic Control*, 56(8), 1862–1873.

Olshevsky, A. and Tsitsiklis, J.N. (2009). Convergence speed in distributed consensus and averaging. *SIAM journal on control and optimization*, 48(1), 33–55.

Pasqualetti, F., Bicchi, A., and Bullo, F. (2012). Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1), 90–104.

Ren, W. and Beard, R.W. (2008). *Distributed Consensus in Multi-vehicle Cooperative Control*. Springer, London.

Renganathan, V., Fathian, K., Safaoui, S., and Summers, T. (2021). Spoof resilient coordination in distributed and robust robotic networks. *IEEE Transactions on Control Systems Technology*, 1–8.

Renganathan, V., Fontan, A., and Ganapathy, K. (2022). History data-driven distributed consensus in networks. URL https://github.com/venkatramanrenganathan/DataDrivenDynamicConsensus/blob/master/HDD_Consensus.pdf.

Saldaña, D., Prorok, A., Sundaram, S., Campos, M.F.M., and Kumar, V. (2017). Resilient consensus for time-varying networks of dynamic agents. In *2017 American Control Conference (ACC)*, 252–258.

Sundaram, S. and Hadjicostis, C.N. (2008). Distributed function calculation via linear iterations in the presence of malicious agents — part ii: Overcoming malicious behavior. In *2008 American Control Conference*, 1356–1361.

Tahbaz-Salehi, A. and Jadbabaie, A. (2006). On consensus over random networks. In *44th Annual Allerton Conference*. Citeseer.

Tahbaz-Salehi, A. and Jadbabaie, A. (2008). A necessary and sufficient condition for consensus over random networks. *IEEE Transactions on Automatic Control*, 53(3), 791–795.

Yemini, M., Nedic, A., Goldsmith, A.J., and Gil, S. (2021). Characterizing trust and resilience in distributed consensus for cyberphysical systems. *IEEE Transactions on Robotics*, 1–21.

Yu, S. and Vorobeychik, Y. (2019a). Distributionally robust removal of malicious nodes from networks. *arXiv preprint arXiv:1901.11463*.

Yu, S. and Vorobeychik, Y. (2019b). Removing malicious nodes from networks. In *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, 314–322.

Appendix A. PARAMETER VARIATIONS ON HDD PROTOCOL

A basic illustration of our approach with constant $\epsilon_{i,k}, k \in \kappa_{t,T}$ is shown in Fig. A.3. Now, consider the same example presented in section 5 as shown in Fig. 1. The resulting trust-based consensus or (clustering) value at time $t = 200$ is plotted in Fig. A.1. When the forgetting factor was small in addition to the confidence bounds ϵ_t being small, we observed a "clustering" behavior: this is due to the fact that the HDD protocol values only the most recent past. For instance, for $\nu < 0.1$, $\nu^{t-k} \approx 0$ for $k = t - T + 1, \ldots, t - 2$, that is, the agents "forget quickly". Instead, when the forgetting factor is close to 1, the states tend to converge to consensus, due to the ability of the agents to remember past events (such as remembering agent j in its ϵ_k-neighborhood for a certain time $k \in \{t - T + 1, \ldots, t\}$). Fig. A.2 shows the elements of the jth ($j = 2, 11, 12, 13$) column of $W(t)$ when $t = 200$, for increasing values of ν. Remember that each element w_{ij} ($i \in \mathcal{V}_c, j = 2, 11, 12, 13$) represents the trust that each agent i has on its neighbor j; then, the intuition is that if there exists a value of ν such that $w_{ij}(200) = 0$ for all $i \in \mathcal{V}_c$ and $j \in \mathcal{V}_{nc}$, it means that the cooperative agents correctly decide to not trust the non-cooperative agents. For instance, Fig. A.2 shows that the non-cooperative agents $11, 12$ are "detected" for most values of ν (except for agent 7 in yellow which almost always believes the non-cooperative neighbors ($j \in \mathcal{V}_{nc}$) no matter what values of confidence bounds and discount factor are used). One could think that $\nu \approx 1$ corresponds to an optimal choice; this is however not the case if a non-cooperative agent adopts a smart behavior (see agent 13 and bottom-right panel of all sub-figures in Fig. A.2) and obtains the trust of all the other agents. Finally, it is interesting to notice that in order to achieve cooperation, an agent needs to trust its neighbors' states and lower the certainty in its own state (see the element $w_{22}(200)$ depicted in blue in the top-left panel of all four sub-figures in Fig. A.2). Specifically, a cooperative agent (like agent 2) under smaller confidence bounds is stubborn initially with smaller discount factor and then relaxes its certainty upon itself with higher discount factor resulting in consensus. On the other hand, when the confidence bounds increased, the rate at which it relaxes its certainty increases and, as a result, a faster cooperation is observed. Under the effect of different history lengths depicted by the top right and bottom right sub-figures of Fig. A.2, we see that under shorter history length, the cooperative agents relax a lot faster their certainties leading to faster cooperation as their memory is smaller. Note that if the cooperative agents were to relax their certainty and cooperate faster, it might come at the expense of *potentially* starting to believe non-cooperative neighbors. Future work will seek to design an adaptive sequence of confidence bounds and discount factor at each time step to rectify this phenomenon and encourage agents to include neighbors with more distant opinions.

(a) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 0.50]$.

(b) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.00]$.

(c) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.50]$.

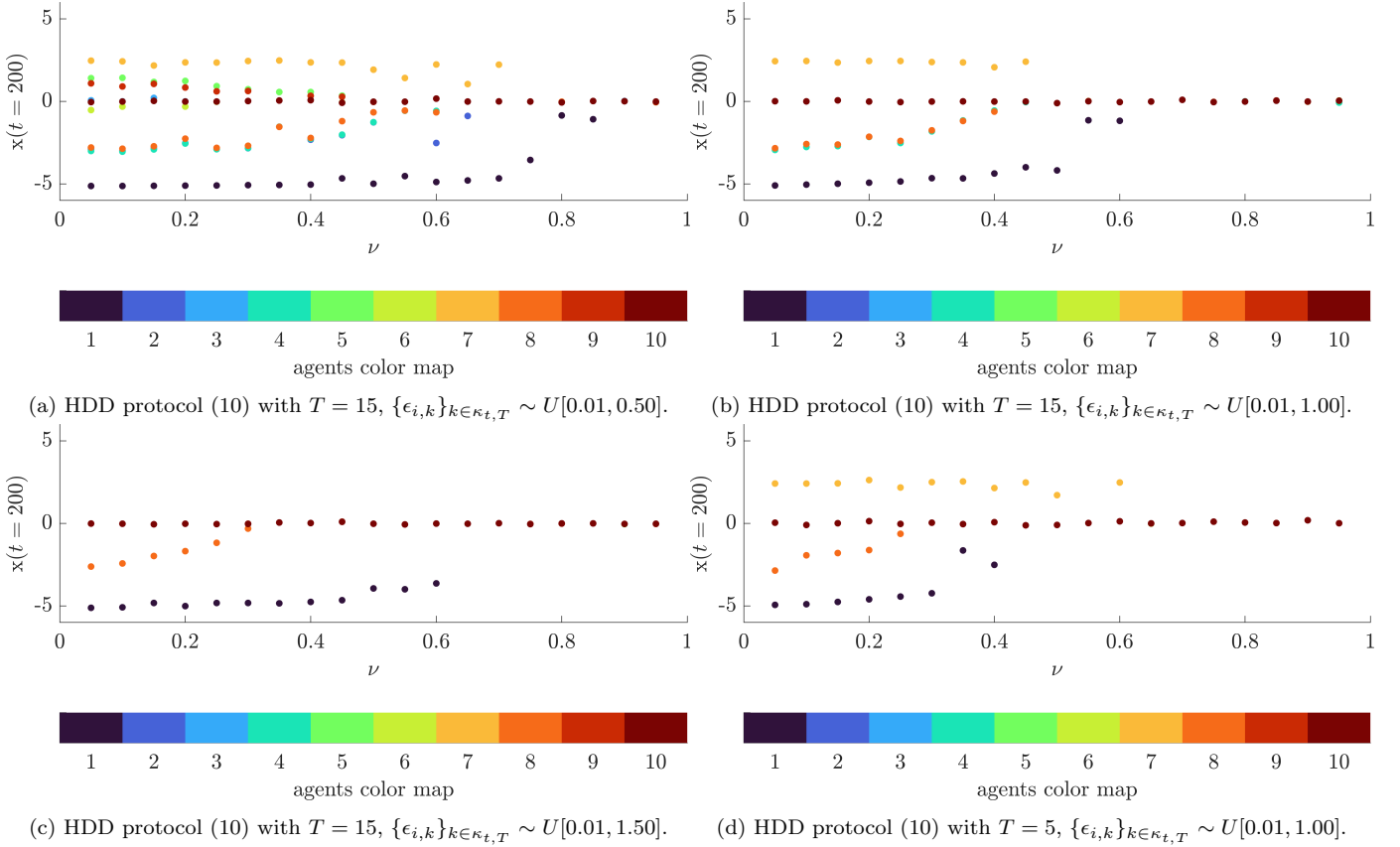(d) HDD protocol (10) with $T = 5$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.00]$.

Fig. A.1. Effect of parameters variation for the HDD protocol (10): agreement vs. clustering. The color map indicates cooperative agents (i.e., $i \in \mathcal{V}_c$). Each panel shows the states of cooperative agents $x_i(t)$, $i \in \mathcal{V}_c$, at time $t = 200$ for increasing values of $\nu \in \{0.05, 0.1, \ldots, 0.95\}$, with confidence bounds $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[\underline{\epsilon}, \bar{\epsilon}]$. Clustering and consensus behaviour is consistently observed on all four subplots with respect to lower discount factor and higher discount factor settings respectively.
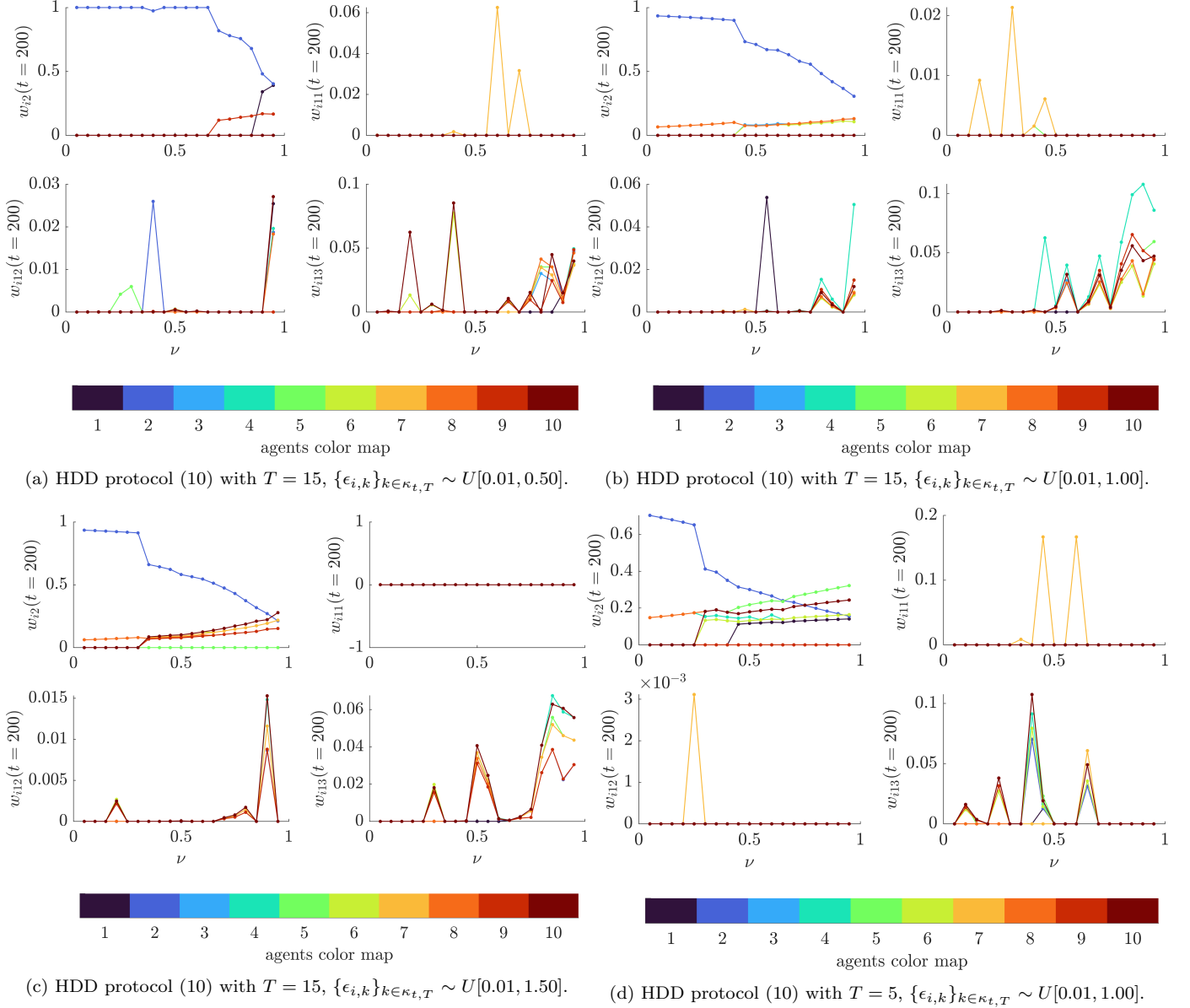
(a) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 0.50]$.

(b) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.00]$.

(c) HDD protocol (10) with $T = 15$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.50]$.

(d) HDD protocol (10) with $T = 5$, $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[0.01, 1.00]$.

Fig. A.2. Effect of parameters variation for the HDD protocol (10): matrix $W(t)$. The color map indicates cooperative agents (i.e., $i \in \mathcal{V}_c$). Each panel shows the elements $w_{ij}(t)$ for $i \in \mathcal{V}_c$ (i.e, cooperative agents) and $j = 2, 11, 12, 13$ (top-left top-right, bottom-left, bottom-right, respectively) at time $t = 200$, for increasing values of $\nu \in \{0.05, 0.1, \ldots, 0.95\}$, with confidence bounds $\{\epsilon_{i,k}\}_{k \in \kappa_{t,T}} \sim U[\underline{\epsilon}, \overline{\epsilon}]$.
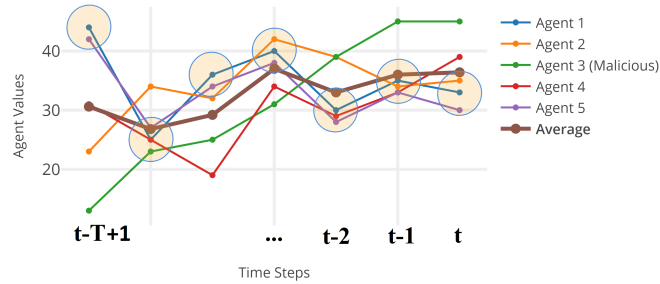

Fig. A.3. An ϵ-neighborhood based set membership for agent **1**, namely $\mathcal{B}_{x_1(k)}(\epsilon_{i,k})$ with $\epsilon_{i,k} = \epsilon > 0, \forall k \in \kappa_{t,T}$ corresponding to the past T time steps historical data is illustrated here. In our work, we propose to have the ϵ balls to be decreasing when time moves forward along with other parameters.