

Designing communication networks for discrete-time consensus for performance and privacy guarantees

Guilherme Ramos^{a,b,*}, Sérgio Pequito^c

^a Departamento de Informática, Instituto Superior Técnico, Universidade de Lisboa, Portugal

^b Instituto de Telecomunicações, 1049-001 Lisbon, Portugal, Portugal

^c Division of Systems and Control, Department of Information Technology, Uppsala University, Sweden

ARTICLE INFO

Article history:

Received 3 January 2023

Received in revised form 23 May 2023

Accepted 9 August 2023

Available online 26 August 2023

Keywords:

Consensus

Average consensus

Privacy

LTI systems

ABSTRACT

Discrete-time consensus plays a key role in multi-agent systems and distributed protocols. Unfortunately, due to the self-loop dynamics of the agents (an agent's current state depends only on its own immediately previous state, i.e., one time-step in the past), they often lack privacy guarantees. Therefore, in this paper, we propose a novel design that consists of a network augmentation, where each agent uses the previous iteration values and the newly received ones to increase the privacy guarantees. To formally evaluate the privacy of a network of agents, we define the concept of privacy index, which intuitively measures the minimum number of agents that should work in coalition to recover all the initial states. Moreover, we aim to explore if there is a trade-off between privacy and accuracy (rate of convergence) or if we can increase both. We unveil that, with the proposed method, we can design networks with higher privacy index and faster convergence rates. Remarkably, we further ensure that the network always reaches consensus even when the original network does not. Finally, we illustrate the proposed method with examples and present networks that lead to higher privacy levels and, in the majority of the cases, to faster consensus rates.

© 2023 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The pervasiveness of interconnected devices having communication capabilities triggered a growing interest in distributed systems and distributed methods. These large-scale systems of devices (or, generically speaking, agents) are usually spatial distributed. Hence, there is a frequent interest in jointly compute a function on data from all the agents in the system via vicinity interactions, i.e., where the agents transmit/receive data only from the neighbors [1–9].

It is of utmost importance to study and ensure beyond accuracy properties in this type of distributed agents' systems such as privacy [10–12]. The common approaches that aim to study/achieve privacy in consensus methods may be categorized in one of the following classes: homomorphic encryption-based (*HE-based*); differential privacy-based (*DP-based*); and observability-based (*O-based*).

Briefly, HE-based average consensus methods demand for costly computations and communications, resulting in a potentially prohibitory cost of use in applications with limited computation and communication power [13–20]. DP-based approaches

try to gain privacy by introducing uncertainty through the addition of noise to shared information [21–29]. In this scenario, the consensus obtained will be in the expected value which may have uncertainty, it may not be suitable for proper decision making, and its implementation and the finite time analysis becomes a harder problem to study [30,31]. Also, noise generation is usually achieved via a pseudo-random generation that depends on the initial seed. Consequently, the privacy assurances depend on the seed used (that should be secret) or the use of an expensive random number generator device [32].

With a different approach to privacy, in [33], the authors introduce a privacy-preserving finite transmission event-triggered quantized average consensus algorithm for battery-powered or energy-harvesting wireless networks. The algorithm ensures efficient communication and transmission ceasing, thereby preserving available energy. The study establishes topological conditions for maintaining node privacy comparing the method with existing algorithms.

In contrast, our work is aligned with the O-based approaches that focus on curious agents that try to retrieve other agent's states by considering the dynamics evolution, and therefore, estimate the states that were deemed to be private. Therefore, *observability* (in dynamical systems) yields necessary and sufficient conditions to obtain an estimator capable of retrieving

* Corresponding author.

E-mail addresses: guilherme.ramos@tecnico.ulisboa.pt (G. Ramos), sergio.pequito@it.uu.se (S. Pequito).

agents' initial states that agents wanted to be unknown to the remaining parties [11,34].

In [35], the authors propose a distributed average information consensus algorithm that ensures confidentiality of each agent's initial state without introducing noise to the state values. They achieve privacy using concealing factors assigned to agents by a central authority before initiating the consensus algorithm. The method also requires a balancing constraint on the edge weights. In contrast, our approach does not rely on a central authority and eliminates the need for a balancing constraint.

The work in [29] derives closed-form expressions for both the optimal distributed estimation and privacy parameters. Moreover, in [31], the authors propose a privacy-preserving approach based on state decomposition for the network average consensus problem, where each node decomposes its state into sub-states with random initial values. Our method differs by not requiring closed-form expressions and state decomposition.

In [36], it is proposed a dynamic average consensus algorithm, which ensures accuracy and privacy of initial values under topological restrictions. However, their algorithm creates a virtual network with a complexity of $\mathcal{O}(n^2)$ nodes, whereas our methods require only $\mathcal{O}(n)$ nodes. The work in [11] analyzes the interplay between network topologies and observability subspace.

Finally, in [37], the authors use observability and optimization techniques to present an algorithm for network synthesis with privacy guarantees. Their method optimizes communication graph weights to maximize node privacy. However, the design complexity and privacy guarantee for all agents are challenging to achieve, which distinguishes our method.

Main contributions. We propose a novel design that consists of a network augmentation, where each agent uses the previous iteration values and the newly received ones to increase the privacy guarantees. We define the concept of privacy index, to formally assess the privacy of a network of agents, which intuitively measures the minimum number of agents that should work in coalition to recover all the initial states. Furthermore, we aim to explore if there exists a trade-off between privacy and accuracy (rate of convergence) or if we can improve both. We unveil that, with the proposed method, we can design networks with a higher privacy index and attain higher convergence rates. Furthermore, we ensure that the network always reaches consensus even when the original network does not.

Paper structure. In Section 1.1, we summarize the concepts and notation used in this paper. In Section 2, we formally state the problem we aim to address. In Section 3, we present a discrete-time consensus method that allows to augment the privacy-level of consensus networks. We show illustrative examples in Section 4, and Section 5 closes the paper with future research directions.

1.1. Preliminaries & terminology

We denote vectors with lower-case letter (e.g., x) and matrices with upper-case letters (e.g., A). We denote the set of integers from 1 to n by $\mathbf{n} = \{i \in \mathbb{Z} : 1 \leq i \leq n\}$. We denote the i th entry of vector $x \in \mathbb{R}^n$ by x_i , with $i \in \mathbf{n}$, the i th row of matrix $A \in \mathbb{R}^{n \times m}$ by A_i , and we use A_{ij} to denote the j th entry of the i th row of A , where $i \in \mathbf{n}$ and $j \in \mathbf{m}$. Moreover, we denote by e_i^n the i th canonical n -dimensional column vector, a vector of size n with all entries equal to zero, except the i th entry that is one. We denote by I_n the $n \times n$ identity matrix. Analogously, we denote by $\mathbf{1}_{n \times m}$ an $n \times m$ matrix with all entries equal to 1, by $\mathbf{0}_{n \times m}$ an $n \times m$ matrix with all entries equal to 0, and when $m = 1$ we simply drop the m to denote a vector of size n (e.g., $\mathbf{1}_n$). Moreover, we denote the transpose of a square-matrix A by A^\top . If $A \in \mathbb{R}^{n \times m}$ and

$\mathcal{I} \subset \mathbf{m}$, we denote by $A(\mathcal{I})$ the matrix composed by the columns of A with indices in \mathcal{I} .

Additionally, we denote by $\text{span}(A)$ the linear span of $A \in \mathbb{R}^{n \times n}$ and its spectrum (set of eigenvalues) by $\sigma(A)$. A matrix $A \in \mathbb{R}^{n \times n}$ is *row-stochastic* if the following hold: (a) $A_{ij} \geq 0$, for all $i, j = 1, \dots, n$, and (b) $\sum_{j=1}^n A_{ij} = 1$, for all $i = 1, \dots, n$. Similarly, a matrix $A \in \mathbb{R}^{n \times n}$ is *column-stochastic* if A^\top is row-stochastic. If A is both row- and column-stochastic then we say that A is *doubly-stochastic*. We denote the structure of a matrix $A \in \mathbb{R}^{n \times m}$ by \bar{A} , where $\bar{A} \in \{0, \star\}^{n \times m}$, with $\bar{A}_{ij} = \star$ whenever $A_{ij} \neq 0$ and $\bar{A}_{ij} = 0$, otherwise.

A (directed) *network of agents* is a graph $\mathcal{G} = \langle \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \rangle$, where $\mathcal{X} = \mathbf{n}$ are the *nodes* that denote the set of n agents, and $\mathcal{E}_{\mathcal{X}, \mathcal{X}} \subset \mathcal{X} \times \mathcal{X}$ are the (directed) *edges* that correspond to pairs of agents (nodes). If $(i, j) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ then the agent i transmits to agent j . Given a matrix $A \in \mathbb{R}^{n \times n}$, we associate to it a directed network of agents via a digraph representation $\mathcal{G}(A) = \langle \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \rangle$, where $\mathcal{X} = \mathbf{n}$ and $(i, j) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ if and only if $A_{ij} \neq 0$.

For a network of agents (communication graph) $\mathcal{G} = \langle \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \rangle$ and an agent $i \in \mathcal{X}$ in the network of agents \mathcal{G} , we denote the *in-neighborhood* of agent i by $\mathcal{N}_i^{\text{in}}$, where $\mathcal{N}_i^{\text{in}} = \{j : (j, i) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}\}$. Similarly, we denote the *out-neighborhood* of agent i by $\mathcal{N}_i^{\text{out}}$, where $\mathcal{N}_i^{\text{out}} = \{j : (i, j) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}\}$. A network is *strongly connected* if there is a path between each pair of nodes (i.e., if for each $x \in \mathcal{X}$ there is a sequence of nodes x, x_1, \dots, x_k, y for all $y \in \mathcal{X}$ such that $(x, x_1), (x_k, y), (x_i, x_{i+1}) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ for all $i = 1, \dots, k-1$).

2. Problem statement

Consider a discrete-time consensus method modeled as a linear time-invariant system (LTI)

$$x(k+1) = Ax(k) \text{ such that } \lim_{k \rightarrow \infty} x(k) = x_\infty \mathbf{1}_n, \quad (1)$$

where $k \in \mathbb{N}$, $x(k)$ is a vector collecting the states of all the agents, $x(k) \in \mathbb{R}^n$, with $x_i(k)$ denoting the state of agent i at time k , A is a row-stochastic matrix, and $x(0) = x_0$ is the initial state.

Furthermore, we will work under the following commonly adopted assumption in the context of consensus.

A₁ The network of agents described by $\mathcal{G}(A)$ is strongly connected.

Now, suppose that a set of one or more agents, in coalition, seeks to determine the initial states of all the other agents, i.e., *observe* the system's states in (1) according to

$$y(k) = Cx(k), \quad (2)$$

where $C \in \mathbb{R}^{m \times n}$ is the *output matrix*. Under this setup, we say that the system in (1) is *observable* if and only if given the values of $y(k)$ for $k = 0, \dots, n-1$, we can uniquely determine x_0 , under the additional assumption that system (1)–(2) described by the pair (A, C) is known.

Remark 1. We can study observability in a generic sense, *structural observability* [38], by looking at A which simply represents which entries of A are fixed zero or not. A pair (\bar{A}, \bar{C}) is *structurally observable* if there is a pair (A, C) respecting the sparsity pattern in (\bar{A}, \bar{C}) that is observable [38]. Moreover, if a pair (\bar{A}, \bar{C}) is structurally observable, then almost all pairs (A, C) that respect the sparsity pattern are observable. Finally, if the pair (A, C) is observable then the pair (\bar{A}, \bar{C}) is structurally observable.

In other words, Remark 1 states that structural observability is a necessary condition for observability. Subsequently, given a dynamics matrix A , with $\mathcal{G} \equiv \mathcal{G}(A)$, we denote by $|\mathcal{G}|_0$ the minimum number of state variables that we need to measure such that the system is structurally observable. This, allow us to introduce the notion of *privacy index* as follows.

Definition 1. Given a system modeled as in (1) with network of agents $\mathcal{G}(A)$, we define the **privacy index** $|\mathcal{G}(A)|_0$ as $|\mathcal{G}(A)|_0 = \arg \min_{\mathcal{I} \subset \{1\}} |\mathcal{I}|$ such that the pair $(A, C \equiv I_{\mathcal{I}}(\mathcal{I}))$ is structurally observable. In other words, the number of agents' states (which can be one or more state variables) uniquely measured by a sensor required so that the network is structural observable.

In a broadcast scenario, each agent sends its state multiplied by the corresponding dynamics matrix weight. Hence, an agent trying to recover other agents initial states corresponds to placing an output in that agent. In this setup, the privacy index counts the minimum number of agents that should collude to recover all the agents' initial state. Note that, if we need to observe $|\mathcal{G}_0|$ agents' states to ensure structural observability, then with $|\mathcal{G}_0| - 1$ the system is not structurally observable and not observable, by Remark 1.

Another important property of a consensus method is how fast it converges. Given the dynamics matrix A , the *rate of convergence* [39] is computed using the spectral gap of A as:

$$R_A = 1 - \rho(A), \quad (3)$$

where $\rho(A) = \max \{|\lambda| : \lambda \in \sigma(A) \setminus \{1\}\}$. In particular, the higher the spectral gap R_A the fastest is the convergence of the consensus protocol.

It is a common belief that there exists a trade-off between privacy and accuracy, which we measure here as the rate of convergence. Therefore, we aim to explore if such trade-offs exists or if we can increase privacy and still increase the rate of convergence. Hereafter, we will see that there are several cases where we do not need to compromise accuracy to increase the privacy level.

Subsequently, we devote the remainder of this work to answering the following problem.

P₁ Given N agents with a communication digraph $\mathcal{G} = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$, if there exists a minimum size augmented dynamics augment the dynamics such that (i) the state is $\tilde{x}_i(k+1) = [x_i(k+1) \ \hat{x}_i(k)]$, with $\hat{x}_i(k) \in \mathbb{R}$, and (ii) initial condition $\tilde{x}_i(0) \in \mathbb{R}^2$

– **Augmented Dynamics** –

$$\bullet \tilde{x}(k+1) = \tilde{A}\tilde{x}(k), \text{ with } \tilde{x}(k) = [\tilde{x}_1(k) \dots \tilde{x}_N(k)] \quad (4a)$$

such that the following properties hold:

– **Specifications** –

Consensus

$$\bullet \lim_{k \rightarrow \infty} \tilde{x}_i(k) = p_{\infty}^T x_0 [1 \ 1], \quad (4b)$$

where p_{∞} is the limit distribution of A (the left-eigenvector of A associated with the eigenvalue 1, normalized to sum 1). Moreover, we want to ensure this even when A has more than one eigenvalues with absolute value 1 (and cannot reach consensus);

Privacy

$$\bullet \text{ the privacy index improves, } |\mathcal{G}(\tilde{A})|_0 > |\mathcal{G}(A)|_0, \quad (4c)$$

where $|\mathcal{G}(\tilde{A})|_0 = \arg \min_{\mathcal{I} \subset \{1\}} |\mathcal{I}|$ such that the pair $(A, C(\mathcal{I}))$ is structurally observable, and $C = [\sum_{j=1}^2 e_j^{2N} \dots \sum_{j=1}^2 e_{2(N-1)+j}^{2N}]$ (i.e., each output measures the augmented states);

Rate of convergence

$$\bullet \text{ the rate of convergence improves, } R_{\tilde{A}} > R_A. \quad (4d)$$

Notice that this is an idyllic problem that we aim to address. Unfortunately, as we will see, the proposed solution has some cases where all the conditions in **P₁** cannot be achieved. Nonetheless, we identify several cases where the proposed solution is able to ensure all the conditions of **P₁**.

If we consider a simple averaging scheme modeled by a row-stochastic dynamics matrix with zero diagonal entries, then we end up with a plethora of networks which do not reach consensus. Such approach would increase the privacy index but would fail, in several cases, to reach consensus. Hence, we propose a new scheme to overcome this limitation.

3. Designing communication networks for discrete-time consensus with privacy guarantees: can the past help?

In this section, we address problem **P₁**. We propose an augmentation of the system that encodes the idea of each agent using the its previous state together with the received neighbors' states to the state update phase. We show that the proposed extended system reaches consensus in Theorem 1, and show that the final consensus is the same as the one of the original dynamics in Theorem 2. In Corollary 1 and Remark 4, we show how the proposed method can be used to reach average consensus. Finally, we present a lower bound for the converge rate of the augmented system in Theorem 3.

The following observation will be important to tackle the problem that we identify in this work.

Remark 2. If the original row stochastic dynamics matrix $A \in \mathbb{R}^{N \times N}$ has eigenvalues with magnitude 1 besides the eigenvalue 1, i.e., $\sigma(A) \setminus \{1\} = \{\lambda_1, \dots, \lambda_{N-1}\}$ and $|\lambda_i| = 1$ for some $i \in \{1, \dots, N-1\}$, then the system in (1) does not reach consensus, and it reaches a periodic behavior (Perron–Frobenius Theorem [40]). ◦

First, we propose to do an augmentation network design, aiming to improve the overall network of agents' privacy. To this end, we propose that an agent share with the neighbors not only its current state but also its previous state as captured in the following update rule: let $x(0) = 0$, $x(1) = \frac{3}{2}x_0$, and

$$x_i(k+2) = \left(\sum_{j \in \mathcal{N}_i^{\text{in}}} x_j(k+1) + \sum_{j \in \mathcal{N}_i^{\text{in}}} x_j(k) \right) / 2|\mathcal{N}_i^{\text{in}}|. \quad (5)$$

Notice that (5) can be written as in (1), where A is the result of normalizing the rows of the agents' network adjacency matrix. Notwithstanding, we may start from any A that is row stochastic and generalize (5) as the following discrete LTI:

$$\tilde{x}(k+1) = \tilde{A}\tilde{x}(k), \quad (6)$$

where

$$\tilde{A} = \begin{bmatrix} \mathbf{0}_{N \times N} & \mathbf{I}_N \\ \frac{A}{2} & \frac{A}{2} \end{bmatrix} \text{ and } \tilde{x}_0 = \begin{bmatrix} 0 \\ \frac{3}{2}x_0 \end{bmatrix}. \quad (7)$$

We would like to notice that, from the representation point of view, in both the case of self-loops and the augmented network scheme proposed above the states are locally available to an agent. However, the dynamics generated by integrating these augmented states does not lead to the existence of self-loops. Hence, the overall dynamics matrix does not have non-zero elements in its diagonal (i.e., no self-loops).

To illustrate how this augmentation changes the network of agents, consider the network represented by black nodes and

edges in Fig. 1, the digraph representation of $A = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$. After

the augmentation in (6), the network gains the additional red nodes (the augmented states) and red edges, depicted in Fig. 1,

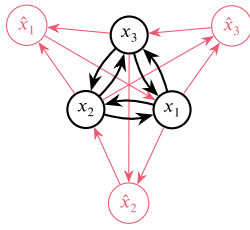


Fig. 1. Virtual network of agents representing the dynamics of (6) for the original network of agents depicted by the black nodes and edges (i.e., $\mathcal{G}(\tilde{A})$, with \tilde{A} given as in (6)). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the digraph representation of

$$\tilde{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 \end{bmatrix}.$$

Subsequently, we show that this augmented dynamics achieves consensus, i.e., the second part of \mathbf{P}_1 (4b).

Theorem 1. *The extended system in (6)–(7) reaches consensus.*

Proof. We start by verifying that 1 is an eigenvalue of \tilde{A} associated with the eigenvector $\mathbf{1}_{2n}$ and the remaining eigenvalues have all magnitude strictly smaller than 1. Let λ be an eigenvalue of A associated with the eigenvector v . Then, it readily follows that

$$\tilde{v}_1 = \begin{bmatrix} v \\ \alpha_1 v \end{bmatrix} \text{ and } \tilde{v}_2 = \begin{bmatrix} v \\ \alpha_2 v \end{bmatrix}$$

are eigenvectors of \tilde{A} associated with the eigenvalues α_1 and α_2 . Specifically,

$$\begin{bmatrix} \mathbf{0}_{n \times n} & I_n \\ \frac{A}{2} & \frac{A}{2} \end{bmatrix} \begin{bmatrix} v \\ \beta v \end{bmatrix} = \gamma \begin{bmatrix} v \\ \beta v \end{bmatrix},$$

which is equivalent to

$$\begin{bmatrix} \beta v \\ \frac{A}{2} v + \beta \frac{A}{2} v \end{bmatrix} = \gamma \begin{bmatrix} v \\ \beta v \end{bmatrix},$$

and, because $Av = \lambda v$, it follows that

$$\begin{bmatrix} \beta v \\ \frac{\lambda}{2} v + \frac{\beta \lambda}{2} v \end{bmatrix} = \gamma \begin{bmatrix} v \\ \beta v \end{bmatrix}$$

if and only if

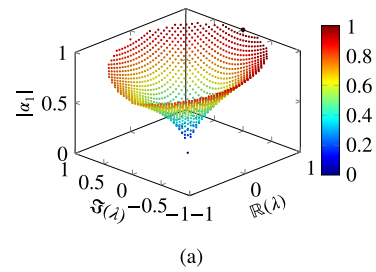
$$\begin{cases} \gamma = \beta \\ \frac{\lambda}{2} v + \frac{\beta \lambda}{2} v = \gamma \beta \end{cases} \Leftrightarrow \begin{cases} \gamma = \beta \\ \frac{\lambda}{2} v + \frac{\beta \lambda}{2} v = \beta^2 \end{cases}$$

from which we conclude that

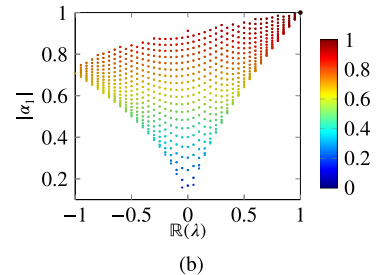
$$\begin{cases} \gamma = \beta \\ \beta = \frac{1}{4} (\lambda \pm \sqrt{\lambda(8+\lambda)}). \end{cases}$$

Therefore, we just need to set $\alpha_1 = \frac{1}{4} (\lambda + \sqrt{\lambda(8+\lambda)})$ and $\alpha_2 = \frac{1}{4} (\lambda - \sqrt{\lambda(8+\lambda)})$.

Finally, we need to ensure that there is only one eigenvalue of \tilde{A} equal to 1 and that the remaining ones have strictly smaller magnitude. Let $\lambda = 1$ be the eigenvalue of A associated with the eigenvector $\mathbf{1}_n$. We have that $\alpha_1 = 1$ is an eigenvalue of \tilde{A} associated with the eigenvector $[\mathbf{1}_n \ \mathbf{1}_n]^T = \mathbf{1}_{2n}$. Moreover, for



(a)



(b)

Fig. 2. Plot views of the complex function $|\frac{1}{4} (\lambda \pm \sqrt{\lambda(8+\lambda)})|$ for $\lambda \in \mathbb{C}$ and $|\lambda| \leq 1$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

$\lambda = 1$ we have that $\alpha_2 = -\frac{1}{2}$. Additionally, we have that for $|\lambda| \leq 1$ since

$$\begin{aligned} \left| \frac{1}{4} (\lambda \pm \sqrt{\lambda(8+\lambda)}) \right| &\leq \frac{1}{4} (|\lambda| + |\sqrt{\lambda(8+\lambda)}|) \\ &\leq \frac{1}{4} (1 + |\sqrt{\lambda(8+\lambda)}|). \end{aligned}$$

Next, since $\arg \max_{\lambda \in \mathbb{C}, |\lambda| \leq 1} |\sqrt{\lambda(8+\lambda)}| = 3$, we have that

$$\frac{1}{4} (1 + |\sqrt{\lambda(8+\lambda)}|) \leq \frac{1}{4} (1 + \sqrt{8+1}) = 1.$$

In fact, $|\frac{1}{4} (\lambda \pm \sqrt{\lambda(8+\lambda)})| = 1$ only for $\lambda = 1$ – see illustration in Fig. 2. \square

Remark 3. Even if the original dynamics matrix A has eigenvalues with magnitude 1 besides the eigenvalue 1 then the system in (6)–(7) reaches consensus, as asserted by Theorem 1, with $x_\infty = p_\infty^T x_0$, where p_∞ is the left-eigenvector of A associated with the eigenvalue 1, by Theorem 2. \circ

Notice that Remark 3 states that we no longer need to carefully select the network of agents to avoid networks that do not reach consensus, see examples in Table 1. In other words, we have a more flexible choice concerning the consensus network, and \mathbf{P}_1 (4b) holds.

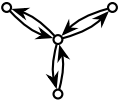
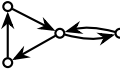
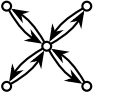
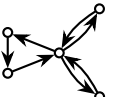
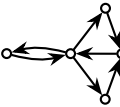

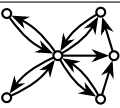
The next result states that if the agents in the original discrete LTI system (1) reach the consensus value x_∞ then the agents using (6)–(7) not only reach consensus but also converge to x_∞ .

Theorem 2. *Consider the discrete LTI system in (1), with A a row-stochastic matrix. If the state of (1) is such that $\lim_{k \rightarrow \infty} x(k) = x_\infty \mathbf{1}_n$, then the state of (6)–(7) is such that $\lim_{k \rightarrow \infty} x(k) = x_\infty \mathbf{1}_{2n}$.*

Proof. If A is a row-stochastic matrix then it corresponds to a Markov-chain. Moreover, the limit distribution is given by the normalized (to sum up to 1) left-eigenvector associated with the eigenvalue 1. The existence of this limit distribution is guaranteed by the result in Theorem 1. We denote this limit distribution by

Table 1

Examples of networks and respective privacy index according to the consensus protocol, the symbol “-” means that, in that case, the network cannot reach consensus.

Network	Privacy index		
	Metropolis	RowStochastic	PastConsensus
	1 ($R_A = 0.25$)	-	2 ($R_A \approx 0.293$)
	1 ($R_A \approx 0.333$)	1 ($R_A \approx 0.293$)	1 ($R_A \approx 0.331$)
	1 ($R_A = 0.2$)	-	3 ($R_A \approx 0.293$)
	1 ($R_A = 0.25$)	2 ($R_A \approx 0.423$)	2 ($R_A \approx 0.423$)
	1 ($R_A = 0.25$)	2 ($R_A \approx 0.293$)	2 ($R_A \approx 0.331$)
	1 ($R_A \approx 0.167$)	-	4 ($R_A \approx 0.293$)
	1 ($R_A \approx 0.167$)	2 ($R_A \approx 0.062$)	2 ($R_A \approx 0.315$)

p_∞ . The left-eigenvalue of \tilde{A} associated with the eigenvalue 1 can be computed by solving the following:

$$[v_1^\top \quad v_2^\top] \tilde{A} = [v_1^\top \quad v_2^\top],$$

which is the same as

$$[v_1^\top \quad v_2^\top] \begin{bmatrix} \mathbf{0}_{n \times n} & I_n \\ \frac{A}{2} & \frac{A}{2} \end{bmatrix} = [v_1^\top \quad v_2^\top].$$

Therefore,

$$\begin{cases} v_2^\top \frac{A}{2} = v_1^\top \\ v_1^\top + v_2^\top \frac{A}{2} = v_2^\top \end{cases} \Leftrightarrow \begin{cases} v_2^\top \frac{A}{2} = v_1^\top \\ 2v_1^\top = v_2^\top \end{cases}$$

and

$$\begin{cases} v_2^\top \frac{A}{2} = v_1^\top \\ 2v_1^\top = v_2^\top \end{cases} \Leftrightarrow \begin{cases} v_2^\top A = 2v_1^\top \\ 2v_1^\top = v_2^\top \end{cases} \Leftrightarrow \begin{cases} v_2^\top A = v_2^\top \\ 2v_1^\top = v_2^\top \end{cases}.$$

In fact, $v_2 = p_\infty$ because it is the left-eigenvector of A associated with the eigenvalue 1. Hence, the left-eigenvector of \tilde{A} is $u^\top = [\frac{1}{2}p_\infty^\top \quad p_\infty^\top]$, and, when normalized to sum up to 1, is $u^\top = \frac{u}{\|u\|_1}$. Notice that, since $\|p_\infty^\top\|_1 = 1$, we have that $\|u\|_1 = \frac{1}{2} + 1 = \frac{3}{2}$. Thus, $u^\top = [\frac{1}{3}p_\infty^\top \quad \frac{2}{3}p_\infty^\top]$. Finally, we have that $x_\infty = p_\infty^\top x_0$, and,

consequently,

$$u^\top \begin{bmatrix} 0 \\ \frac{3}{2}x_0 \end{bmatrix} = \frac{1}{3}p_\infty^\top 0 + \frac{2}{3}p_\infty^\top \frac{3}{2}x_0 = x_\infty.$$

Hence, the consensus value is as desired. \square

It immediately follows from [Theorem 2](#) that average consensus can be attained under the following setting.

Corollary 1. *If the original dynamics matrix A in (1) is doubly-stochastic then the system in (6) reaches **average** consensus.* \circ

Nonetheless, when the objective is to do the design to reach average consensus and the conditions of [Corollary 1](#) do not hold, we can do it considering the following observation.

Remark 4. If we aim to achieve average consensus, then we just need to re-weight the initial agents state according to the limit distribution p_∞ , setting the new initial state of agent i as $\hat{x}_i(0) = \frac{x_i(0)}{(p_\infty)_i}$. \circ

Lastly, we would like to see how the convergence rate of the original dynamics matrix and the augmented version relate.

Theorem 3. *Let A be the dynamics matrix of (1) and \tilde{A} the dynamics augmented matrix of (6)–(7). Let $\sigma(A) = \{\lambda_1, \dots, \lambda_{n-1}, 1\}$ and*

$R_A = 1 - |\lambda|$, where $\lambda = \arg \max_{\lambda' \in \sigma(A) \setminus \{1\}} |\lambda'|$. Then, the following hold:

- (i) $\sigma(\tilde{A}) = \{\alpha_1^1, \alpha_2^1, \dots, \alpha_1^{n-1}, \alpha_2^{n-1}, -\frac{1}{2}, 1\}$, where α_1^i, α_2^i are the eigenvalues associated with λ_i , computed in the proof of Theorem 1;
- (ii) $R_{\tilde{A}} = 1 - |\alpha|$, where $\alpha = \arg \max_{\alpha' \in \sigma(\tilde{A}) \setminus \{1\}} |\alpha'|$;
- (iii) $R_{\tilde{A}} \leq \min\{1 - |\alpha_1|, 1 - |\alpha_2|\}$, where α_1, α_2 are the eigenvalues associated with λ . \circ

Proof. We have that (i) follows directly from the proof of Theorem 1, and (ii) follows from the definition of rate of convergence in (3). Concerning (iii) the proof follows from noticing that λ is the second eigenvalue of A with higher absolute value that is transformed into α_1 and α_2 , two eigenvalues of \tilde{A} . Therefore $R_{\tilde{A}} \leq \min\{1 - |\alpha_1|, 1 - |\alpha_2|\}$, where α_1, α_2 are the eigenvalues obtained in the proof of Theorem 1. \square

It is worth noticing that we could use the proposed augmentation with two additional nodes or even more. However, the structure of the respective augmented matrix would have repeated blocks. Therefore, such a strategy may be adopted and explored but it will not lead to a better privacy index.

3.1. Theoretical guarantees

Given the dynamics matrix $A \in \mathbb{R}^{N \times N}$, consider its structure $\bar{A} \in \{0, \star\}^{N \times N}$, where $\bar{A}_{ij} = 0$ if and only if $A_{ij} = 0$ and $\bar{A}_{ij} = \star$, otherwise. Let $\mathcal{I} \subset [N]$ denote the agents that are measured. This corresponds to have an output matrix structure $\bar{C} = [\bar{\mathbf{I}}_N(\mathcal{I})]$, i.e., $\bar{C} \in \{0, \star\}^{|\mathcal{I}| \times N}$ that is the structural matrix composed by the subset of rows of $\bar{\mathbf{I}}_N$ indexed by \mathcal{I} .

The system with dynamics matrix \bar{A} and observed state variables indexed by \mathcal{I} is structurally observable if and only if

$$\text{grank} \left(\begin{bmatrix} \bar{A} \\ \bar{C} \end{bmatrix} \right) = N,$$

where the *grank* (generic rank) of a structural matrix $\bar{M} \in \{0, \star\}^{N_1 \times N_2}$ is the maximum rank achievable with a matrix $M' \in \mathbb{R}^{N_1 \times N_2}$ such that $M' = \bar{M}$ [38]. In other words, the structural output matrix \bar{C} compensates the *grank* deficiency of \bar{A} .

Subsequently, the following result relates the privacy index of a network without self-loops with its augmentation.

Theorem 4. Consider a connected network of agents with adjacency matrix $A \in \mathbb{R}^{N \times N}$ without self-loops. If A has privacy index k then \bar{A} , as described in (7), also has privacy index k . \circ

Proof. Suppose that $A \in \mathbb{R}^{N \times N}$ has privacy index k . It follows that $\text{grank}(\bar{A}) = N - k$, where $\bar{A} \in \{0, \star\}^{N \times N}$ is the structural matrix. In other words, there is a generic rank deficiency of k in \bar{A} to achieve a generic full rank (i.e., N) [38]. Moreover, the value k yields the number of agents that should be measured to attain structural observability. Now, consider the augmented matrix

$$\tilde{A} = \begin{bmatrix} \mathbf{0}_{N \times N} & \mathbf{I}_N \\ \frac{A}{2} & \frac{A}{2} \end{bmatrix}.$$

The structural pattern is

$$\tilde{\bar{A}} = \begin{bmatrix} \bar{\mathbf{0}}_{N \times N} & \bar{\mathbf{I}}_N \\ \bar{A} & \bar{A} \end{bmatrix}.$$

In this case, it is easy to see that

$$\begin{aligned} \text{grank}(\tilde{\bar{A}}) &= \text{grank} \left(\begin{bmatrix} \bar{\mathbf{0}}_{N \times N} & \bar{\mathbf{I}}_N \\ \bar{A} & \bar{\mathbf{0}}_{N \times N} \end{bmatrix} \right) \\ &= N + (N - k) = 2N - k. \end{aligned}$$

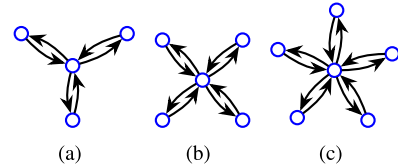


Fig. 3. Star networks with 4, 5 and 6 agents in (a), (b) and c, respectively.

Hence, there is the same rank deficiency, and the privacy index of \tilde{A} is also k . \square

Next, we identify a class of networks, referred to as star-networks (see Fig. 3 depicting a star network for $N = 4, 5, 6$), where the proposed approach always yield a higher privacy index.

Corollary 2. Consider a star network with $N \geq 4$ agents. Up to a label permutation of the agents' numbering, the structural pattern $\bar{A} \in \{0, \star\}^{N \times N}$ of the adjacency matrix of a star network with N agents, and the respective structural consensus matrix for this network $\bar{W} \in \{0, \star\}^{N \times N}$ are as follows:

$$\bar{A} = \begin{bmatrix} 0 & \star & \cdots & \star \\ \star & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \star & 0 & \cdots & 0 \end{bmatrix}, \text{ and } \bar{W} = \begin{bmatrix} \star & \star & \cdots & \star \\ \star & \star & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \star & 0 & \cdots & \star \end{bmatrix}.$$

Then the privacy index of the network without self-loops (\bar{A}) is $N - 2$ and the privacy index of the network with self-loops (\bar{W}) is 1. \circ

Proof. We can easily see that $\text{grank}(\bar{W}) = N$, by considering the diagonal parameters to be different from zero and setting the off-diagonal ones to zero. Therefore, with an output in any of the agents (i.e., setting $\bar{C} = \bar{e}_i$, where \bar{e}_i is the i th canonical row vector in \mathbb{R}^N corresponding to measure the state of agent i), we obtain a structurally observable system since

$$\text{grank} \left(\begin{bmatrix} \bar{A} \\ \bar{C} \end{bmatrix} \right) = N.$$

That is, by observing a single agent the system is structurally observable.

On the other hand, we have that $\text{grank}(\bar{A}) = 2$, meaning we need to observe $N - 2$ agents to ensure that the system is structurally observable, i.e., it follows by definition that privacy index equals $N - 2$. By Theorem 4, it readily follows that the privacy index of \tilde{A} is also $N - 2$. \square

4. Illustrative examples

It is common that the agents update their states using information received by neighbors together with their current state, which corresponds to have non-zero diagonal elements in the dynamics matrix A . A well-known way of selecting the dynamics matrix entries (making use of non-zero diagonal entries) is by using the so-called *Metropolis weights* [41], which are given as follows:

$$A_{ij} = \begin{cases} \frac{1}{1 + \max\{|\mathcal{N}_i^{in}|, |\mathcal{N}_j^{in}|\}} & \text{if } j \in \mathcal{N}_i^{in} \text{ and } i \neq j, \\ 0 & \text{if } j \notin \mathcal{N}_i^{in} \text{ and } i \neq j, \\ 1 - \sum_{k \in \mathcal{N}_i^{in}} A_{ik} & \text{if } i = j. \end{cases} \quad (8)$$

This self-loop dynamics makes possible that an external entity, by observing any agent's state evolution, is able to observe the entire system, leading to low privacy guarantees. In fact, under this

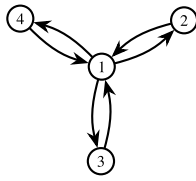


Fig. 4. Star network of 4 agents.

dynamics, the privacy index is always 1. We use the Metropolis weights to compare with the proposed approach.

In the examples that follow, in addition to the rate of convergence, we mark in the consensus evolution plots the point where the maximum absolute difference between the agents states (error) starts to be less than a specific value. This property further illustrates how fast the methods are converging.

Consider the network of agents \mathcal{G} depicted by the black nodes and edges in Fig. 4. If we use, for instance, the Metropolis weights to design the dynamics matrix utilized to do consensus, then the network of agents becomes the one depicted by black nodes and edges and red edges in Fig. 4. In Fig. 5(a), we depict the agents' states evolution from the initial state $x_0 = [0.1 \ 0.3 \ 0.6 \ 1]^T$ when using the dynamics of (1) and A is defined with the Metropolis weights. In this case, we have a privacy index of 1. In the case where we do not consider self-loop dynamics and we use a row-stochastic matrix A in the dynamics of (1), we actually cannot reach consensus, as noticed in Remark 3, see Fig. 5(b).

Notwithstanding, when we use the proposed augmented consensus (6)–(7), we increase the privacy index to 2, and we can reach consensus. In Fig. 5(c), we portray this scenario, but we only show the second half of agents' states evolution, i.e., we omit the first half that corresponds to the past and is equal if we start all the states with 0 and shift the presented ones a time unit ahead.

To further illustrate the proposed consensus method and concept of privacy index, consider the network of agents \mathcal{G}_1 , depicted in Fig. 6.

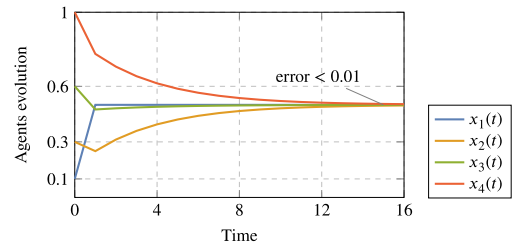
In Fig. 7, we show the agents' states evolution for the initial state $x_0 = [0 \ 1.5 \ -0.8 \ 2.4 \ -1.7 \ 3.9 \ 0.6 \ 4.7 \ -3.1 \ 5.5 \ -4.3 \ 6]^T$. Again, notice that when using the Metropolis weights, we achieve a privacy index of 1, and with the proposed consensus method we get a privacy index of 3.

Finally, in Table 1, we present some networks of agents and evaluate their privacy index depending on the used consensus protocol. Notice that in the majority of the reported cases, besides ensuring consensus, the proposed method reaches a higher privacy level and a higher rate of convergence.

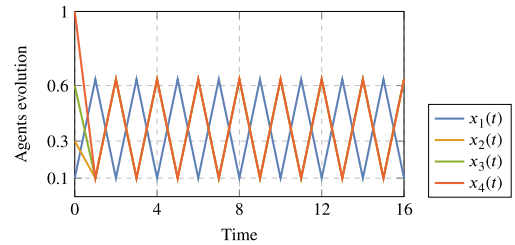
It is worth noticing that star-like networks do not allow to reach consensus when we do not consider self-loop dynamics. Notwithstanding, with the proposed augmentation we not only achieve consensus but also increase both the privacy index and the rate of convergence, as we may see in the first, third and penultimate networks of Table 1.

5. Conclusions

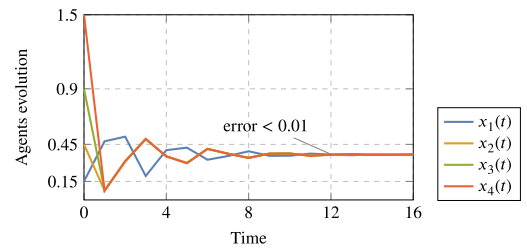
In this paper, we developed a discrete-time consensus method where each agent uses the previous iteration values together with the recently received ones. The proposed method consists of, at each time step, the agents computing the average of the neighbors' received states from the current and previous iterations. Furthermore, we do not consider the agent to have self-loop dynamics, i.e., they do not use their own states in the state update phase, as this would prevent the network from reaching some privacy level. In other words, an external entity can recover all the agents' states by observing merely one agent. Notwithstanding, it



(a) Consensus evolution using (1) with dynamics matrix given by (8) (Metropolis weight), the network **privacy index** is 1 and $R_A = 0.25$.

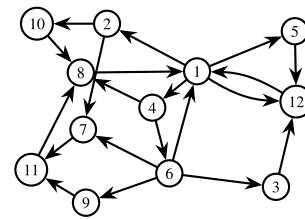


(b) Row-stochastic A , without self-node dynamics (1), which **cannot reach consensus**, with **privacy index 2**.



(c) The proposed **past consensus** (6), the network **privacy index** is 2 and $R_A \approx 0.293$.

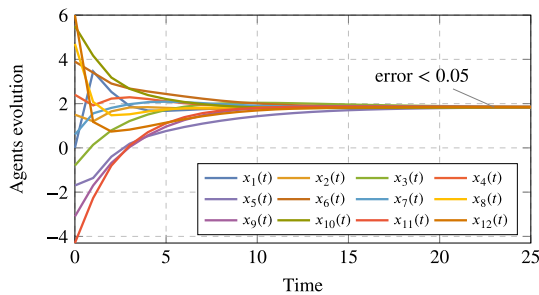
Fig. 5. Consensus evolution for the network of agents depicted by the black nodes and edges Fig. 4 (black nodes and edges and red edges for the Metropolis weights). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Fig. 6. Network of agents \mathcal{G}_1 .

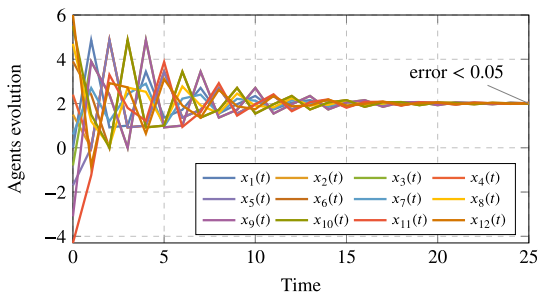
is known that if an agent averages the neighbors' states (without considering its own state), then it may reach a periodic behavior (instead of conducting consensus).

We unveil that, with the proposed method, we can not only design networks with higher privacy levels but also ensure that the network always reaches consensus. Moreover, we unveil that we may do so without compromising (most of the times) the rate of convergence and further (most of the times) we actually increase the rate of convergence.

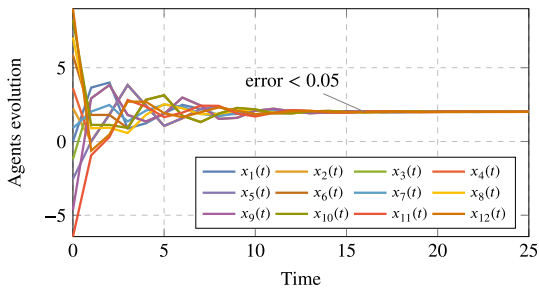
Additionally, if the initial dynamics matrix is doubly-stochastic, the proposed method reaches average consensus. We illustrate the proposed method with examples and present networks that lead to higher privacy levels and, in the majority of



(a) Consensus evolution using (1) with dynamics matrix given by (8), the network **privacy index** is **1** and $R_A = 0.2$.



(b) Row-stochastic A , without self-node dynamics (1), reaches consensus, the network **privacy index** is **3** and $R_A \approx 0.196$.



(c) The proposed **past consensus** (6), which reaches consensus faster than (b), the network **privacy index** is **3** and $R_A \approx 0.261$.

Fig. 7. Consensus evolution for the network of agents \mathcal{G}_1 depicted if Fig. 6. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the cases, to a faster consensus (higher rate of convergence). Future work includes building upon this approach to assess the design problem of given a set of states that are required to be private, what should be the network topology that guarantees such requirement.

CRediT authorship contribution statement

Guilherme Ramos: Conceptualization, Writing – original draft, Investigation, Methodology, Software, Writing – review & editing, Validation, Formal analysis. **Sérgio Pequito:** Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article

References

- [1] F. Bullo, J. Cortés, S. Martinez, Distributed Control of Robotic Networks: A Mathematical Approach to Motion Coordination Algorithms, Princeton University Press, 2009, <http://dx.doi.org/10.1515/9781400831470>.
- [2] G. Ramos, D. Silvestre, C. Silvestre, A general discrete-time method to achieve resilience in consensus algorithms, in: Proceedings of the 59th IEEE Conference on Decision and Control, 2020, pp. 2702–2707, <http://dx.doi.org/10.1109/CDC42340.2020.9304107>.
- [3] S.M. Dibaji, H. Ishii, Consensus of second-order multi-agent systems in the presence of locally bounded faults, Systems Control Lett. 79 (2015) 23–29, <http://dx.doi.org/10.1016/j.sysconle.2015.02.005>.
- [4] D. Saldana, A. Prorok, S. Sundaram, M.F.M. Campos, V. Kumar, Resilient consensus for time-varying networks of dynamic agents, in: Proceedings of the American Control Conference, 2017, pp. 252–258, <http://dx.doi.org/10.23919/ACC.2017.7962962>.
- [5] S. Sundaram, B. Ghahsifard, Distributed optimization under adversarial nodes, IEEE Trans. Automat. Control (2018) 1, <http://dx.doi.org/10.1109/TAC.2018.2836919>.
- [6] G. Ramos, D. Silvestre, C. Silvestre, General resilient consensus algorithms, Internat. J. Control 95 (6) (2022) 1482–1496, <http://dx.doi.org/10.1080/00207179.2020.1861331>.
- [7] G. Ramos, D. Silvestre, A.P. Aguiar, A resilient continuous-time consensus method using a switching topology, Systems Control Lett. 169 (2022) 105381, <http://dx.doi.org/10.1016/j.sysconle.2022.105381>.
- [8] G. Ramos, D. Silvestre, C. Silvestre, Node and network resistance to bribery in multi-agent systems, Systems Control Lett. 147 (2021) 104842, <http://dx.doi.org/10.1016/j.sysconle.2020.104842>.
- [9] G. Ramos, D. Silvestre, C. Silvestre, A discrete-time reputation-based resilient consensus algorithm for synchronous or asynchronous communications, IEEE Trans. Automat. Control (2023).
- [10] J.M. Such, A. Espinosa, A. García-Fornes, A survey of privacy in multi-agent systems, Knowl. Eng. Rev. 29 (3) (2014) 314–344, <http://dx.doi.org/10.1017/S0269888913000180>.
- [11] S. Pequito, S. Kar, S. Sundaram, A.P. Aguiar, Design of communication networks for distributed computation with privacy guarantees, in: Proceedings of the 53rd IEEE Conference on Decision and Control, IEEE, 2014, pp. 1370–1376, <http://dx.doi.org/10.1109/CDC.2014.7039593>.
- [12] N. Gupta, J. Katz, N. Chopra, Privacy in distributed average consensus, IFAC-PapersOnLine 50 (1) (2017) 9515–9520, <http://dx.doi.org/10.1016/j.ifacol.2017.08.1608>, Proceedings of the 20th IFAC World Congress.
- [13] R. Lazerretti, S. Horn, P. Braca, P. Willett, Secure multi-party consensus gossip algorithms, in: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE, 2014, pp. 7406–7410, <http://dx.doi.org/10.1109/ICASSP.2014.6855039>.
- [14] N.M. Freris, P. Patrinos, Distributed computing over encrypted data, in: Proceedings of the 54th Annual Allerton Conference on Communication, Control, and Computing, IEEE, 2016, pp. 1116–1122, <http://dx.doi.org/10.1109/ALLERTON.2016.7852360>.
- [15] M. Kishida, Encrypted average consensus with quantized control law, in: Proceedings of the IEEE Conference on Decision and Control, IEEE, 2018, pp. 5850–5856, <http://dx.doi.org/10.1109/CDC.2018.8619855>.
- [16] T. Yin, Y. Lv, W. Yu, Accurate privacy preserving average consensus, IEEE Trans. Circuits Syst. II 67 (4) (2019) 690–694, <http://dx.doi.org/10.1109/TCSII.2019.2918709>.
- [17] M. Ruan, H. Gao, Y. Wang, Secure and privacy-preserving consensus, IEEE Trans. Automat. Control 64 (10) (2019) 4035–4049, <http://dx.doi.org/10.1109/TAC.2019.2890887>.
- [18] C.N. Hadjicostis, A.D. Domínguez-García, Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus, IEEE Trans. Automat. Control 65 (9) (2020) 3887–3894, <http://dx.doi.org/10.1109/TAC.2020.2968876>.
- [19] R.L. Lagendijk, Z. Erkin, M. Barni, Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation, IEEE Signal Process. Mag. 30 (1) (2012) 82–105, <http://dx.doi.org/10.1109/MSP.2012.2219653>.
- [20] K. Kogiso, T. Fujita, Cyber-security enhancement of networked control systems using homomorphic encryption, in: Proceedings of the 54th IEEE Conference on Decision and Control, IEEE, 2015, pp. 6836–6843, <http://dx.doi.org/10.1109/CDC.2015.7403296>.
- [21] J. Cortés, G.E. Dullerud, S. Han, J. Le Ny, S. Mitra, G.J. Pappas, Differential privacy in control and network systems, in: Proceedings of the IEEE 55th Conference on Decision and Control, IEEE, 2016, pp. 4252–4272, <http://dx.doi.org/10.1109/CDC.2016.7798915>.
- [22] Z. Huang, S. Mitra, G. Dullerud, Differentially private iterative synchronous consensus, in: Proceedings of the ACM Workshop on Privacy in the Electronic Society, 2012, pp. 81–90, <http://dx.doi.org/10.1145/2381966.2381978>.
- [23] E. Nozari, P. Tallapragada, J. Cortés, Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design, Automatica 81 (2017) 221–231, <http://dx.doi.org/10.1016/j.automatica.2017.03.016>.

- [24] X. Wang, J. He, P. Cheng, J. Chen, Privacy preserving average consensus with different privacy guarantee, in: Proceedings of the Annual American Control Conference, IEEE, 2018, pp. 5189–5194, <http://dx.doi.org/10.23919/ACC.2018.8431023>.
- [25] L. Gao, S. Deng, W. Ren, Differentially private consensus with an event-triggered mechanism, *IEEE Trans. Control Netw. Syst.* 6 (1) (2018) 60–71, <http://dx.doi.org/10.1109/TCNS.2018.2795703>.
- [26] D. Fiore, G. Russo, Resilient consensus for multi-agent systems subject to differential privacy requirements, *Automatica* 106 (2019) 18–26, <http://dx.doi.org/10.1016/j.automatica.2019.04.029>.
- [27] Y. Mo, R.M. Murray, Privacy preserving average consensus, *IEEE Trans. Automat. Control* 62 (2) (2016) 753–765, <http://dx.doi.org/10.1109/TAC.2016.2564339>.
- [28] J. He, L. Cai, P. Cheng, J. Pan, L. Shi, Consensus-based data-privacy preserving data aggregation, *IEEE Trans. Automat. Control* 64 (12) (2019) 5222–5229, <http://dx.doi.org/10.1109/TAC.2019.2910171>.
- [29] J. He, L. Cai, X. Guan, Preserving data-privacy with added noises: Optimal estimation and privacy analysis, *IEEE Trans. Inform. Theory* 64 (8) (2018) 5677–5690, <http://dx.doi.org/10.1109/TIT.2018.2842221>.
- [30] E. Nozari, P. Tallapragada, J. Cortés, Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design, *Automatica* 81 (2017) 221–231, <http://dx.doi.org/10.1016/j.automatica.2017.03.016>.
- [31] Y. Wang, Privacy-preserving average consensus via state decomposition, *IEEE Trans. Automat. Control* 64 (11) (2019) 4711–4716.
- [32] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, Q. Xu, A survey on true random number generators based on chaos, *Discrete Dyn. Nat. Soc.* 2019 (2019) <http://dx.doi.org/10.1155/2019/2545123>.
- [33] A.I. Rikos, C.N. Hadjicostis, K.H. Johansson, Finite-time privacy-preserving quantized average consensus with transmission stopping, in: 2022 IEEE 61st Conference on Decision and Control, CDC, IEEE, 2022, pp. 6762–6768.
- [34] D. Boutat, G. Zheng, Observability and observer for dynamical systems, in: Observer Design for Nonlinear Dynamical Systems, Springer, 2021, pp. 1–29, http://dx.doi.org/10.1007/978-3-030-73742-9_1.
- [35] N. Gupta, N. Chopra, Confidentiality in distributed average information consensus, in: 2016 IEEE 55th Conference on Decision and Control, CDC, IEEE, 2016, pp. 6709–6714, <http://dx.doi.org/10.1109/CDC.2016.7799302>.
- [36] I.L.D. Ridgley, R.A. Freeman, K.M. Lynch, Private and hot-pluggable distributed averaging, *IEEE Control Syst. Lett.* 4 (4) (2020) 988–993.
- [37] A. Alaeddini, K. Morgansen, M. Mesbahi, Adaptive communication networks with privacy guarantees, in: 2017 American Control Conference, ACC, IEEE, 2017, pp. 4460–4465.
- [38] G. Ramos, A.P. Aguiar, S. Pequito, An overview of structural systems theory, *Automatica* 140 (2022) 110229, <http://dx.doi.org/10.1016/j.automatica.2022.110229>.
- [39] A. Olshevsky, J.N. Tsitsiklis, Convergence speed in distributed consensus and averaging, *SIAM rev.* 53 (4) (2011) 747–772, <http://dx.doi.org/10.1137/110837462>.
- [40] O. Perron, Zur theorie der matrices, *Math. Ann.* 64 (2) (1907) 248–263.
- [41] N. Metropolis, A.W. Rosenbluth, M.N. Rosenbluth, A.H. Teller, E. Teller, Equation of state calculations by fast computing machines, *J. Chem. Phys.* 21 (6) (1953) 1087–1092, <http://dx.doi.org/10.1063/1.1699114>.