Received 30 March 2023; revised 19 June 2023; accepted 12 July 2023. Date of publication 27 July 2023;
date of current version 9 August 2023. Recommended by Senior Editor Fabio Pasqualetti.

Digital Object Identifier 10.1109/OJCSYS.2023.3299521

Exploiting the Synchronization of Nonlinear Dynamics to Secure Distributed Consensus

CAMILLA FIORAVANTI [1] (Student Member, IEEE), VALERIA BONAGURA [2] (Student Member, IEEE), GABRIELE OLIVA [1] (Senior Member, IEEE), CHRISTOFOROS N. HADJICOSTIS [3] (Fellow, IEEE), AND STEFANO PANZIERI [2] (Member, IEEE)

(Synchronization in Natural and Engineering Systems)

[1] University Campus Bio-Medico of Rome, 00128 Rome, Italy
[2] University Roma Tre, 00146 Rome, Italy
[3] University of Cyprus, 1678 Nicosia, Cyprus

CORRESPONDING AUTHOR: GABRIELE OLIVA (e-mail: g.oliva@unicampus.it)

ABSTRACT Distributed cooperative multi-agent operations, which are emerging as effective solutions in countless application domains, are prone to eavesdropping by malicious entities due to their exposure on the network. Moreover, in several cases, agents are reluctant to disclose their initial conditions (even to legitimate neighbors) due to their sensitivity to private data. Providing security guarantees against external readings by malicious entities and the privacy of exchanged data while allowing agents to reach an agreement on some shared variables is an essential feature to foster the adoption of distributed protocols. In this article, we propose to implement a secure and privacy-preserving consensus strategy that exploits, for this purpose, the performance of synchronization of nonlinear continuous-time dynamical systems. This is achieved by splitting the initial conditions into two information fragments, one of which is subject to nonlinear manipulation. In this way, the information being exchanged in the network will always be subject to the influence of nonlinear dynamics. However, by exploiting the ability of such dynamics to synchronize, the combination of the two fragments still converges to a weighted average of each node's actual initial conditions. Furthermore, due to the dependence of the hidden dynamics on a coordinate transformation known only to the legitimate nodes, message security is ensured even once consensus is reached; our approach relies on the assumption that a secure communication channel is available during an initialization phase. The article is complemented by a simulation campaign aimed at numerically demonstrating the effectiveness of the proposed approach.

INDEX TERMS Chua oscillators, distributed algorithms, distributed consensus, nonlinear synchronization, privacy preservation, security.

I. INTRODUCTION

Consensus [1], [2] and distributed agreement algorithms in general [3], [4] provide a strong foundation for composing the information available at each agent in a network. These algorithms are relevant for modeling collective dynamics [5] and have several engineering applications, including distributed estimation [6] or mobile robot coordination [7]. Although efficient, these systems typically lack security and privacy assurances since agents exchange their states, thus revealing potentially sensitive information to other entities and exposing the entire network to the risk of eavesdropping. The need to avoid revealing sensitive information emerges especially when several organizations with competing interests are involved, such as smart grids [8], [9] or Industrial Internet of Things (IIoT) applications [10], [11].

A. STATE OF THE ART

Several approaches have been proposed to ensure security and privacy in the context of distributed consensus. Some authors explore the case of honest but curious nodes that aim to gain insights into the initial conditions of other nodes. In contrast, others account for malicious eavesdroppers who are not legitimate network agents.

In [13], [14], [15], information on the initial state is hidden by adding and subtracting random noise values to the information exchanged during the consensus process in a way that guarantees that the exact average of initial values is eventually computed. Such a class of approaches has been extended to the case of delays [16] and quantization [17]. The authors of [18] consider a continuous-time average consensus process and investigate the possibility of preserving the privacy of the reference value of the agents by adding admissible perturbation signals to the local dynamics, i.e., perturbations designed in a way that does not modify the final agreement value. This idea also appears in other approaches [19], [20] that rely on obfuscation, i.e., the injection of carefully designed noise signals to hide actual state values. In [21], [22], [23], security and privacy-preservation are enforced by resorting to Paillier semi-homomorphic encryption, whereby the information exchanged by the agents is encrypted, and the agents manipulate the encrypted values in a way that guarantees that the result is the encryption of the final consensus value. Such value is later decrypted, so the agents can compute the consensus value without disclosing their initial conditions.

Given the amount of time needed for the encryption and decryption processes, this approach may not be appropriate in some situations where hard real-time constraints must be satisfied. To overcome this issue, several approaches have been proposed in the literature. The solution proposed in [24] aims to balance cipher strength and processing time through quantization. In general, approaches based on cryptography are computationally expensive, while noise-based methods trade off accuracy for privacy. Achieving high accuracy and privacy in a distributed averaging process with differential privacy is still challenging. One notable approach is proposed in [25], where each node decomposes its state into two sub-states to guarantee privacy in average consensus. The additive-noise strategy presented in [26] exchanges noise for several rounds before exchanging data to ensure robustness, but it is only partially immune to attacks. Another interesting protection mechanism is digital watermarking [27], which can be used to protect signals from unauthorized access, copying, and distribution.

Notably, thanks to their nonlinearity, sensitivity to initial conditions, and long-time unpredictability, chaotic systems have been used to encrypt or mask information [28], [29], [30]. In particular, some encryption techniques based on keys generated by the Chua oscillator are present in the literature (such as [31]). Still, they only focus on the method of encrypting the message without investigating the more complex mechanism of privacy preservation. Currently, Chua's oscillators are mainly used for image encryption [32], [33].

B. CONTRIBUTION

In this article, we present a novel consensus method that takes advantage of the synchronization of a network of nonlinear dynamic systems (e.g., Chua oscillators) via partial state coupling, with the final aim of masking the initial conditions of the agents to their peers and preventing malicious third parties from eavesdropping. In particular, we consider a situation where the agents are interconnected by a directed and strongly connected graph topology and aim to compute a weighted average of their initial conditions. Notably, this includes, as a particular case, the actual average (i.e., when the graph is also *balanced*, as discussed later in the article). To this end, such an initial value is suitably split to initialize: 1) a distributed synchronization process for a network of nonlinear dynamical systems characterized by noise, partial information sharing, and time-varying coupling; 2) a linear average consensus process that is suitably influenced by the nonlinear synchronization. As a result, each agent can locally reconstruct the weighted average consensus value, even though partial information is exchanged, and neither of the above processes may reach a steady state. Interestingly, the key aspect of the proposed methodology lies in the combination of consensus control and chaotic synchronization, aimed at ensuring privacy and security while allowing legitimate agents to retrieve the final consensus value. Notice that our approach relies on the assumption that a secure communication channel is available during an initialization phase that involves the exchange of a common vector for the coordinate transformation. Interestingly, with respect to previous approaches in the literature, the proposed solution does not introduce quantization errors, unlike encryption schemes. Finally, methods based on noise injection typically require keeping track of the injected noise's integral (in order to remove it later). In contrast, in the proposed approach, noise only needs to equalize at each agent after a transient. In this view, an agreed-upon noise value (used while the nonlinear systems are synchronized) represents another layer of protection (e.g., another shared key).

This article extends our preliminary conference article [34] with several improvements. First, the approach in [34] only considered the synchronization of a network of Chua oscillators over an undirected graph with static coupling and in the absence of noise. In this article, on the other hand, we consider a general framework for the synchronization of networks of nonlinear systems, which are characterized by possibly directed interaction topologies, time-varying coupling, and the presence of noise. Moreover, we investigate the privacy and security characteristics of the framework. Finally, in the context of the considered synchronization framework, we establish an interesting relation between synchronization and the fact that the overall dynamics, also considering the effect of the coupling term, amounts to a gradient descent along a strongly convex function.

C. PAPER OUTLINE

The outline of the article is as follows: Section II collects some preliminary notations and definitions; Section III provides an overview of the synchronization of networks of nonlinear dynamical systems; Section IV characterizes the problem at hand in this article and develops the proposed algorithm; Section V investigates the characteristics of the proposed approach in terms of privacy and security; Section VI provides a simulation campaign to demonstrate the effectiveness of the proposed approach experimentally; finally, Section VII provides some conclusive remarks and future work directions.

II. PRELIMINARIES

A. NOTATION

We denote vectors with boldface lowercase letters and matrices with uppercase letters. We refer to the (i, j)-th entry of a matrix A by A_{ij}. We represent by $\mathbf{0}_n$ and $\mathbf{1}_n$ vectors with n entries, all equal to zero and to one, respectively. Given a vector $\boldsymbol{p} \in \mathbb{R}^n$, we use $\mathtt{diag}(\boldsymbol{p})$ to denote the $n \times n$ diagonal matrix such that $\mathtt{diag}_{ii}(\boldsymbol{p}) = p_i$. We denote the Euclidean norm using $\|\cdot\|$. Given two matrices $A \in \mathbb{R}^{n\times m}$ and $B \in \mathbb{R}^{p\times q}$, we use $A \otimes B$ to denote their Kronecker product.

Let us use $\mathcal{W}$ to denote the set of square $n \times n$ real matrices with zero row sums and nonpositive off-diagonal elements. In contrast, $\mathcal{W}_S$ is the set of irreducible symmetric matrices in $\mathcal{W}$. Given a function $g : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$, we use $\nabla_{\boldsymbol{y}} g(\boldsymbol{y}, t) \in \mathbb{R}^n$ to denote the gradient of $g(\cdot)$ with respect to the first argument, evaluated at $\boldsymbol{x} = \boldsymbol{y}$ and at a given time t. The function $g(\boldsymbol{x}, t)$ is said to be strongly convex (e.g., see [35]) in $\boldsymbol{x}$ if, for all $t \geq 0$, it holds

$$(\nabla_{\boldsymbol{x}} g(\boldsymbol{x}, t) - \nabla_{\boldsymbol{y}} g(\boldsymbol{y}, t))^T (\boldsymbol{x} - \boldsymbol{y}) \geq \mu \|\boldsymbol{x} - \boldsymbol{y}\|^2, \qquad (1)$$

for some $\mu > 0$. Equivalently, the function $g(\boldsymbol{x}, t)$ is strongly convex if and only if its Hessian matrix has eigenvalues that are lower bounded by a positive constant.

B. GRAPH THEORY

Let $G = \{V, E\}$ be a *graph* with n nodes $V = \{v_1, v_2, \ldots, v_n\}$ and e edges $E \subseteq V \times V$, where $(v_i, v_j) \in E$ captures the existence of a link from node v_i to node v_j. A graph is said to be *undirected* if the existence of an edge $(v_i, v_j) \in E$ implies the presence of $(v_j, v_i) \in E$, while it is said to be *directed* otherwise. A directed graph is *strongly connected* if each node can be reached by each other node via a sequence of edges, respecting their orientation.

Let the in-neighborhood $\mathcal{N}_i^{\text{in}}$ of a node v_i be the set of nodes v_j such that $(v_j, v_i) \in E$; similarly, the out-neighborhood $\mathcal{N}_i^{\text{out}}$ of a node v_i is the set of nodes v_j such that $(v_i, v_j) \in E$. The *in-degree* d_i^{in} of a node v_i is the number of its incoming edges, i.e., $d_i^{\text{in}} = |\mathcal{N}_i^{\text{in}}|$; similarly, the *out-degree* d_i^{out} of a node v_i is the number of its outgoing edges, i.e., $d_i^{\text{out}} = |\mathcal{N}_i^{\text{out}}|$. A graph is *balanced* if for all nodes $v_i \in V$ it holds $d_i^{\text{in}} = d_i^{\text{out}}$.

Given a graph $G = \{V, E\}$ with n nodes, we define the Laplacian matrix L as the $n \times n$ matrix such that

$$L_{i,j} = \begin{cases} d_i^{\text{in}}, & \text{if } i = j \\ -1, & \text{if } (v_j, v_i) \in E, \\ 0, & \text{otherwise.} \end{cases}$$

It is well known [36] that when G is strongly connected, L has a unique eigenvalue equal to zero and that the corresponding left eigenvector $\boldsymbol{\zeta}^T$ has just positive entries. In contrast, the corresponding right eigenvector is $\mathbf{1}_n^T$. Moreover, when G is also balanced, the left eigenvector corresponding to the zero eigenvalue coincides with the right one and is given by $\mathbf{1}_n^T$.

C. DISTRIBUTED CONSENSUS

Let us consider a network of n agents interconnected by a graph $G = \{V, E\}$. Suppose each agent i holds an initial condition $w_i(0)$ and interacts according to the protocol

$$\dot{w}_i(t) = \sum_{j\in\mathcal{N}_i^{\text{in}}} \left(w_j(t) - w_i(t)\right), \qquad (2)$$

which, in a compact form, corresponds to $\dot{\boldsymbol{w}}(t) = -L\boldsymbol{w}(t)$, where $\dot{\boldsymbol{w}}(t), \boldsymbol{w}(t) \in \mathbb{R}^n$ collect the entries $\dot{w}_i(t)$ and $w_i(t)$), respectively.

It is well known [1] that if G is directed and strongly connected, then the agents asymptotically reach an agreement such that

$$\lim_{t\to\infty} \boldsymbol{w}(t) = \mathbf{1}_n \boldsymbol{\zeta}^T \boldsymbol{w}(0), \qquad (3)$$

where $\boldsymbol{\zeta}^T$ is the left eigenvector of L corresponding to the zero eigenvalue, suitably scaled so that $\mathbf{1}_n^T \boldsymbol{\zeta} = 1$; in other words, the agents reach consensus to a weighted average of their initial conditions, where the weights correspond to the entries of $\boldsymbol{\zeta}$. Notably, if G is also balanced, then

$$\lim_{t\to\infty} \boldsymbol{w}(t) = \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T \boldsymbol{w}(0),$$

i.e., the agents asymptotically reach the average of their initial conditions.

D. PRIVACY-PRESERVING CONSENSUS

Suppose the agents aim to compute a weighted average of their initial conditions $w_i(0)$ with weights encoded by $\boldsymbol{\zeta}$ and, at the same time, want to prevent their neighbors from being able to ascertain their initial conditions. Over a strongly connected directed graph, a possible strategy to achieve this result [13], [21] is to modify the consensus protocol by setting

$$\dot{w}_i(t) = \sum_{j\in\mathcal{N}_i^{\text{in}}} \left(w_j(t) - w_i(t)\right) + u_i(t)$$

where $u_i(t)$ represents artificial noise injected by the i-th agent; in compact form, the dynamics reads

$$\dot{\boldsymbol{w}}(t) = -L\boldsymbol{w}(t) + \boldsymbol{u}(t).$$

In particular, suppose $u_i(t)$ is such that

$$\int_0^{t_i^*} u_i(\tau) d\tau = 0, \quad u_i(t) = 0 \text{ for } t > t_i^* \qquad (4)$$

and $t_i^* \geq 0$. In other words, each agent selects a time instant t_i^* and designs the noise $u_i(t)$ so that the cumulative effect is zero at time t_i^*, while $u_i(t)$ becomes zero afterward. Let us denote by $t_{\max}$ the maximum of the time instants t_i^*, i.e., the time the last cumulative effect reaches zero. Notably, since for all $t > t_{\max}$ the input $\boldsymbol{u}(t)$ is zero, the agents behave as if a standard consensus process was starting at time $t_{\max}$. Moreover, since

$$\boldsymbol{\zeta}^T \dot{\boldsymbol{w}}(t) = -\boldsymbol{\zeta}^T L\boldsymbol{w}(t) + \boldsymbol{\zeta}^T \boldsymbol{u}(t) = \boldsymbol{\zeta}^T \boldsymbol{u}(t),$$

it can be easily shown that

$$\boldsymbol{\zeta}^T \boldsymbol{w}(t) = \boldsymbol{\zeta}^T \boldsymbol{w}(0) + \boldsymbol{\zeta}^T \int_0^{\min\{t,t_{\max}\}} \boldsymbol{u}(\tau)d\tau;$$

hence, for all $t \geq t_{\max}$ it holds $\boldsymbol{\zeta}^T \boldsymbol{w}(t) = \boldsymbol{\zeta}^T \boldsymbol{w}(0)$, i.e., the weighted sum of the initial conditions, with weights encoded by $\boldsymbol{\zeta}$, is preserved for all $t \geq t_{\max}$. This, in turn, implies that the agents reach the desired consensus value without disclosing their actual initial conditions. However, the convergence time has a delay equal to $t_{\max}$. Notably, for all $t \geq t_{\max}$ it holds

$$\begin{aligned} w_i(t) &= w_i(0) + \int_0^t \dot{w}_i(\tau)d\tau \\ &= w_i(0) + \sum_{v_j \in \mathcal{N}_i} \int_0^t w_j(\tau)d\tau - d_i \int_0^t w_i(\tau)d\tau \\ &\quad + \int_0^t u_i(\tau)d\tau. \end{aligned}$$

Hence, since for all $t \geq t_{\max}$ it holds $\int_0^t u_i(\tau) = 0$, we have that for $t \geq t_{\max}$ it holds

$$w_i(0) = w_i(t) + d_i \int_0^t w_i(\tau)d\tau - \sum_{\mathcal{N}_i} \int_0^t w_j(\tau)d\tau. \quad (5)$$

Therefore, an honest but curious node v_ℓ can reconstruct the state of a node v_i provided that it directly observes the state of v_i and all its neighbors, i.e., if v_i is *exposed* to v_ℓ, according to the following definition [34], [37].

Definition 1 (Exposed node): A node v_i is *exposed* to a node v_ℓ if $\mathcal{N}_i^{\text{in}} \cup \{i\} \subseteq \mathcal{N}_\ell^{\text{in}} \cup \{\ell\}$.

Therefore, no privacy guarantees can be provided for exposed nodes; notably, most of the approaches available at state of the art are prone to this vulnerability [13], [14], [21], [37], [38].

III. SYNCHRONIZATION IN NETWORKS OF NONLINEAR CONTINUOUS-TIME DYNAMICAL SYSTEMS

This section reviews the synchronization framework developed in [39] and references therein, which will be the basis for the later developments in this article. In particular, such a synchronization approach can handle time-varying coupling, directed graphs, and the presence of noise. To introduce the framework, let us first consider the following technical definition.

Definition 2 (V-Uniformly Decreasing): Let a function $\boldsymbol{\psi}$:$\mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ and a matrix $V \in \mathbb{R}^{n\times n}$ be given. The function $\boldsymbol{\psi}(\boldsymbol{x}, t)$ is said to be V-uniformly decreasing if, for some $c > 0$, we have

$$(\boldsymbol{x} - \boldsymbol{y})^T V(\boldsymbol{\psi}(\boldsymbol{x}, t) - \boldsymbol{\psi}(\boldsymbol{y}, t)) \leq -c \|\boldsymbol{x} - \boldsymbol{y}\|^2,$$

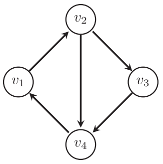

FIGURE 1. Graph topology considered in Example 1.

for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, and for all $t \geq 0$.

Let us now consider a dynamical system with the following structure

$$\dot{\boldsymbol{x}}(t) = \underbrace{\begin{bmatrix} \boldsymbol{f}(\boldsymbol{x}_1(t), t) \\ \vdots \\ \boldsymbol{f}(\boldsymbol{x}_n(t), t) \end{bmatrix}}_{\boldsymbol{f}(\boldsymbol{x}(t),t)} + (P \otimes D(t))\boldsymbol{x}(t) + \boldsymbol{u}(t) \quad (6)$$

where $\boldsymbol{x}_i(t), \boldsymbol{u}_i(t) \in \mathbb{R}^m$,

$$\boldsymbol{x}(t) = \left[\boldsymbol{x}_1^T(t), \ldots, \boldsymbol{x}_n^T(t)\right]^T \in \mathbb{R}^{nm},$$

and

$$\boldsymbol{u}(t) = \left[\boldsymbol{u}_1^T(t), \ldots, \boldsymbol{u}_n^T(t)\right]^T \in \mathbb{R}^{nm}.$$

Matrix $P \in \mathbb{R}^{n\times n}$ is a zero row-sum matrix that describes the coupling topology, whereas $D(t) \in \mathbb{R}^{m\times m}$ represents the time-varying linear coupling matrix between two systems. In particular, matrix P describes the topological structure. Thus it provides information on which pairs of nodes can communicate (i.e., node i receive information from node j if and only if $P_{ij} \neq 0$), on the gain associated to the communication channel (i.e., the numerical value P_{ij}) and on the effect of a node i on itself (i.e., the numerical value P_{ii}). Conversely, the matrix $D(t)$ accounts for the information exchanged among any pair of nodes. In other words, at time t, a node i transmits the quantity $P_{ji}D(t)\boldsymbol{x}_i(t)$ to all its out-neighbors j (while $P_{ii}D(t)\boldsymbol{x}_i(t)$ is the effect of node i on itself), and the information transmitted is the composition of a gain P_{ji} related to the communication channel and a contribution $D(t)\boldsymbol{x}_i(t)$ that models the information shared by the node. The notation $P \otimes D(t)$ represents a compact form to model the two levels of interaction among the agents.

Let us now provide an illustrative example.

Example 1: Let us consider the directed graph topology with four agents shown in Fig. 1, and characterized by the following P matrix

$$P = \begin{bmatrix} 1 & 0 & 0 & -1 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & -1 & 2 \end{bmatrix}.$$

Let us now assume that each agent is characterized by three state variables (i.e., $\boldsymbol{x}_i(t) \in \mathbb{R}^3$) and that the function $\boldsymbol{f}(\boldsymbol{x}_i(t), t)$ for each agent i is $\boldsymbol{f} : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{R}^3$. Furthermore, we assume that the agents interact by exchanging only the first state variable with their neighbors, i.e., we assume $D(t) = D$ constant for simplicity. This scenario is captured by the matrix

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Overall, the information sent by agent i to agent j at time t is given by

$$P_{ji}D\boldsymbol{x}_i(t) = \begin{bmatrix} P_{ji}x_{i1}(t) & 0 & 0 \end{bmatrix}^T.$$

The following definition formalizes the idea of synchronization for the above dynamical system.

Definition 3 (Synchronization Manifold): The synchronization manifold $\mathcal{M}$ is the linear subspace

$$\mathcal{M} = \{\boldsymbol{x} \in \mathbb{R}^{nm} \,|\, \boldsymbol{x}_i = \boldsymbol{x}_j, \forall i, j\}.$$

In particular, (6) is said to *synchronize* if $\boldsymbol{x}(t)$ approaches the set $\mathcal{M}$, i.e., if for all i, j it holds

$$\lim_{t\to\infty} \|\boldsymbol{x}_i(t) - \boldsymbol{x}_j(t)\| = 0.$$

Notice that, given the structure of the synchronization manifold $\mathcal{M}$, we have that $\boldsymbol{x} \in \mathcal{M}$ if and only if $\boldsymbol{x} = \mathbf{1} \otimes \boldsymbol{z}$ for some $\boldsymbol{z} \in \mathbb{R}^m$.

The next definition will help prove the synchronization of (6).

Definition 4 ($\mu(P)$): Given a real matrix P with nonpositive off-diagonal elements, $\mu(P)$ is the supremum of the set of real numbers μ such that $U(P - \mu I) \succeq 0$ for some $U \in \mathcal{W}_S$, where $\mathcal{W}_S$ is the set of irreducible symmetric matrices in $\mathcal{W}$ (see Section II-A). In particular, if P is a Laplacian matrix, then $\mu(P)$ is the minimum over the real parts of the nonzero eigenvalues of P.

Let us now review some conditions that guarantee the reach of synchronization in (6).

Theorem 1: Consider the dynamics in (6) with P being an $n \times n$ matrix with nonpositive off-diagonal elements. Moreover, let $V \in \mathbb{R}^{n\times n}$ be a given symmetric and positive definite matrix and suppose that the following conditions are satisfied:

1) $\lim_{t\to\infty} \|\boldsymbol{u}_i(t) - \boldsymbol{u}_j(t)\| = 0$ for all i, j,
2) $VD(t) = D^T(t)V \preceq 0$ for all t,
3) $\boldsymbol{f}(\boldsymbol{y}, t) + \mu(P)D(t)\boldsymbol{y}$ is V-uniformly decreasing.

Then, (6) synchronizes.

As observed in [39], the condition that a function $\boldsymbol{\psi}(\boldsymbol{y}, t)$ is V-uniformly decreasing for a symmetric and positive definite V implies that $\dot{\boldsymbol{y}} = \boldsymbol{\psi}(\boldsymbol{y}, t)$ is globally asymptotically stable. In particular, when $\boldsymbol{\psi}(\boldsymbol{y}, t) = \boldsymbol{f}(\boldsymbol{y}, t) + K(t)\boldsymbol{y}$, we have that $K(t)\boldsymbol{y}$ is a term that globally stabilizes $\boldsymbol{f}(\boldsymbol{y}, t)$. A classic example in this sense is given by the Chua oscillator, for which $\boldsymbol{y} \in \mathbb{R}^3$ and

$$\boldsymbol{f}(\boldsymbol{y}, t) = \begin{bmatrix} c\alpha(y_2 - y_1 - \theta(y_1)) \\ c(y_1 - y_2 + y_3) \\ -c(\beta y_2 + \gamma y_3) \end{bmatrix},$$

with

$$\theta(y_1) = by_1 + \frac{1}{2}(a - b)\{|y_1 + 1| - |y_1 - 1|\}.$$

Notably, the Chua oscillator is known to synchronize [12] for $K(t) = \mu(P)D(t)$ with

$$V = I_3, \quad D(t) = -\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tag{7}$$

and for a sufficiently large $\mu(P) > 0$.

However, it might be challenging in general to identify $\boldsymbol{f}(\boldsymbol{y}, t)$, V, P and $D(t)$ that guarantee satisfaction of the conditions in Theorem 1. For this reason, in the next result, we provide a constructive way to identify a V-uniformly decreasing function. Specifically, we establish a connection between synchronization and gradient descent by showing that a function is V-uniformly decreasing if and only if it corresponds to the "antigradient" (i.e., the opposite of the gradient) of a strongly convex function.

Theorem 2: Let a matrix $V \in \mathbb{R}^{n\times n}$ be given. A function $\boldsymbol{\psi} : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ is V-uniformly decreasing if and only if there is a function $g : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$ such that

$$V\boldsymbol{\psi}(\boldsymbol{x}, t) = -\nabla_{\boldsymbol{x}} g(\boldsymbol{x}, t) \tag{8}$$

with $g(\boldsymbol{x}, t)$ being strongly convex in $\boldsymbol{x}$ for all $t \geq 0$.

Proof: ($\Rightarrow$) In order to prove sufficiency we observe that if $g(\boldsymbol{x}, t)$ is strongly convex in $\boldsymbol{x}$ then it satisfies (1) for some $\mu > 0$. Therefore, if V and $\boldsymbol{\psi}(\boldsymbol{x}, t)$ satisfy (8), we have that

$$-(\boldsymbol{x} - \boldsymbol{y})^T V(\boldsymbol{\psi}(\boldsymbol{x}) - \boldsymbol{\psi}(\boldsymbol{y})) \geq \mu\|\boldsymbol{x} - \boldsymbol{y}\|^2$$

and thus

$$(\boldsymbol{x} - \boldsymbol{y})^T V(\boldsymbol{\psi}(\boldsymbol{x}) - \boldsymbol{\psi}(\boldsymbol{y})) \leq -\mu\|\boldsymbol{x} - \boldsymbol{y}\|^2,$$

i.e., $\boldsymbol{\psi}(\cdot)$ is V-uniformly decreasing with $c = \mu$.

($\Leftarrow$) In order to prove necessity, suppose $\boldsymbol{\psi}(\cdot)$ is V-uniformly decreasing; then, by construction it holds

$$(\boldsymbol{x} - \boldsymbol{y})^T V(\boldsymbol{\psi}(\boldsymbol{x}) - \boldsymbol{\psi}(\boldsymbol{y})) \leq -c\|\boldsymbol{x} - \boldsymbol{y}\|^2,$$

for some $c > 0$. At this point, let us consider any continuous curve γ in $\mathbb{R}^n$ that starts at $\boldsymbol{x}$ and ends at $\boldsymbol{y}$. By the *gradient theorem* (e.g., see [40]), we have that there is a function $r(\boldsymbol{x}, t)$, differentiable in $\boldsymbol{x}$, with

$$\nabla_{\boldsymbol{x}} r(\boldsymbol{x}, t) = V\boldsymbol{\psi}(\boldsymbol{x}, t)$$

that satisfies

$$\int_\gamma V\boldsymbol{\psi}(z, t)dz = r(\boldsymbol{x}, t) - r(\boldsymbol{y}, t).$$

As a consequence, we have that $g(\boldsymbol{x}, t) = -r(\boldsymbol{x}, t)$ satisfies

$$(\nabla_{\boldsymbol{x}} g(\boldsymbol{x}, t) - \nabla_{\boldsymbol{y}} g(\boldsymbol{y}, t))^T(\boldsymbol{x} - \boldsymbol{y}) \geq c\|\boldsymbol{x} - \boldsymbol{y}\|^2,$$

and is thus strongly convex for $\mu = c$. This completes our proof. ■

The above result allows designing a dynamics that guarantees synchronization by first identifying $g(\cdot)$ and then by computing its antigradient.

A few remarks are now in order.

Remark 3: Let us consider

$$\boldsymbol{\psi}(\boldsymbol{y}, t) = \boldsymbol{f}(\boldsymbol{y}, t) + K(t)\boldsymbol{y}$$

with $VK(t)$ symmetric and negative definite, and suppose

$$V\boldsymbol{f}(\boldsymbol{y}, t) = -\nabla_{\boldsymbol{y}} g(\boldsymbol{y}, t)$$

for some function $g(\boldsymbol{y}, t)$. Since $VK(t)\boldsymbol{y}$ is the antigradient along $\boldsymbol{y}$ of the convex function

$$w(\boldsymbol{y}, t) = -\frac{1}{2}\boldsymbol{y}^T VK(t)\boldsymbol{y},$$

according to the above theorem, synchronization is achieved if and only if $g(\boldsymbol{y}, t) + w(\boldsymbol{y}, t)$ is strongly convex. Therefore, $VK(t)\boldsymbol{y}$ can be regarded as the antigradient of a convexification term that is added to $g(\boldsymbol{y}, t)$ to make it strongly convex so that the dynamics $\dot{\boldsymbol{y}} = \boldsymbol{\psi}(\boldsymbol{y}, t)$ essentially amounts to a gradient descent-like dynamics.

Remark 4: A simple way to choose a strongly convex function $g(\boldsymbol{x}, t)$ is to consider any (not necessarily strongly) convex function $g'(\boldsymbol{x}, t)$ and add a strongly convex function, e.g.,

$$g(\boldsymbol{x}, t) = g'(\boldsymbol{x}, t) + \frac{1}{2}\boldsymbol{x}^T H\boldsymbol{x},$$

where H is symmetric and positive definite. In this case, we have that

$$\boldsymbol{h}(\boldsymbol{x}, t) = -\nabla_{\boldsymbol{x}} g'(\boldsymbol{x}, t) - H\boldsymbol{x}.$$

IV. PROPOSED APPROACH

Let us consider a scenario where a network of n agents is interconnected by a directed and strongly connected graph $G = \{V, E\}$. Each agent is provided with a hidden scalar[1] initial value $h_i(0)$, while

$$\boldsymbol{h}(0) = \left[h_1(0), \ldots, h_n(0)\right]^T \in \mathbb{R}^n$$

denotes the stack of the hidden values for all agents. The purpose of each agent is twofold: on one side, they aim to reach the consensus value without disclosing their initial conditions to their peers in the network (*privacy*); on another side, they aim to hide their states (including both the initial and the final values) from malicious third parties, i.e., eavesdroppers that do not belong to the network (*security*).

To accomplish these tasks, let us consider that each agent maintains locally a state vector $\boldsymbol{x}_i(t) \in \mathbb{R}^m$ and interacts with neighboring agents by implementing the synchronization scheme discussed in (6). Further to that, let us consider a matrix $Q \in \mathbb{R}^{n\times nm}$ with the following structure

$$Q = I_n \otimes \boldsymbol{q}^T,$$

where vector[2] $\boldsymbol{q} \in \mathbb{R}^m$ and $\boldsymbol{q} \neq \boldsymbol{0}_m$.

Notice that, by construction, for any $\boldsymbol{c} \in \mathbb{R}^m$, matrix Q satisfies

$$Q\left(\boldsymbol{1}_n \otimes \boldsymbol{c}\right) = \left(\boldsymbol{q}^T\boldsymbol{c}\right)\boldsymbol{1}_n. \tag{9}$$

Moreover, let us assume that each agent maintains an additional scalar variable $z_i(t)$ whose dynamics, in stacked form for all agents (i.e., considering $\boldsymbol{z}(t) = \left[z_1(t) \quad \ldots z_n(t)\right]^T$), reads as follows

$$\dot{\boldsymbol{z}}(t) = -L\boldsymbol{z}(t) + Q\left(\boldsymbol{f}(\boldsymbol{x}(t), t) + (P \otimes D(t))\boldsymbol{x}(t) + \boldsymbol{u}(t)\right),$$

where the initial conditions $\boldsymbol{x}(0)$ for the synchronizing dynamics and $\boldsymbol{z}(0)$ for the additional dynamics are chosen so that

$$h_i(0) = z_i(0) - \boldsymbol{q}^T\boldsymbol{x}_i(0),$$

which, in stacked form, reads

$$\boldsymbol{h}(0) = \boldsymbol{z}(0) - Q\boldsymbol{x}(0).$$

Finally, we assume that each agent locally computes

$$\boldsymbol{h}(t) = \boldsymbol{z}(t) - Q\boldsymbol{x}(t).$$

Overall, the agents' dynamics can be summarized as follows

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}(t), t) + (P \otimes D(t))\boldsymbol{x} + \boldsymbol{u}(t) \\ \dot{\boldsymbol{z}}(t) = -L\boldsymbol{z}(t) + Q\left(\boldsymbol{f}(\boldsymbol{x}(t), t) + (P \otimes D(t))\boldsymbol{x}(t) + \boldsymbol{u}(t)\right) \\ \boldsymbol{h}(t) = \boldsymbol{z}(t) - Q\boldsymbol{x}(t) \end{cases} \tag{10}$$

where

$$\boldsymbol{u}(t) = [\boldsymbol{u}_1^T(t), \ldots, \boldsymbol{u}_n^T(t)]^T \in \mathbb{R}^{nm}$$

and $\boldsymbol{u}_i(t) \in \mathbb{R}^m$ is a time-varying input locally selected by agent i, such that the condition 1) of Theorem 1 holds. For simplicity, we assume that $P = \eta L$, where L is the Laplacian matrix corresponding to the agents' interaction graph, and $\eta > 0$ is a suitable gain.

Notice that the dynamics of the state vector $\boldsymbol{z}(t)$, dependent on the exchange of $z_i(t)$ with neighboring agents, is distorted by the nonlinear term featuring $\boldsymbol{x}(t)$, which influences the consensus dynamics via the matrix Q; this dependency is introduced to mask the initial conditions from other legitimate nodes in the network and, at the same time, to enforce security by preventing malicious eavesdroppers that do not belong to the network from gaining insights on both the initial and final values. In particular, vector $\boldsymbol{q}$ plays the role of a key that is shared among the legitimate agents. Notably, such a vector could be provided as a hardware key (e.g., see [41]) before the agents are deployed or selected during a secure initialization phase and securely shared (e.g., see [42], [43]). For instance, in the case of networks of mobile agents, one could have the

[1] Note that all the results presented can be trivially generalized to the vectorial case.

[2] Notice that, to guarantee the final consensus reconstruction, the agents must all know $\boldsymbol{q}$ in advance; this requirement can be fulfilled by resorting to a secure communication channel during the initialization phase.

vector $\boldsymbol{q}$ selected when the agents are in a "safe zone", and then they use it after they are deployed in an "unsafe zone" (e.g., see [44], [45], where robots are initially in close spatial proximity and subsequently start exploring an environment).

Moreover, for the nonlinear dynamics of the state vector $\boldsymbol{x}(t)$ the agents need to exchange only a subset of the state variables governed by the time-varying matrix[3] $D(t)$. The dynamics of the hidden consensus vector $\boldsymbol{h}(t)$, on the other hand, is calculated only locally and is never exchanged.

Once the nonlinear dynamics have reached synchronization, thanks to the structure proposed in (10), it will be possible for legitimate agents to trace the consensus value $\boldsymbol{h}(t)$ while maintaining security on the exchanged messages and privacy on the initial conditions. In order to achieve this, we need the following assumption.

Assumption 1: The agents' interaction topology is such that the set of the exposed nodes is empty.

In the remainder of this section, we aim to study the convergence of the hidden state variable $\boldsymbol{h}(t)$. In the next section, we analyze possible strategies that the attacker may deploy in an attempt to breach privacy and security.

The following theorem shows that $h_i(t)$ approaches the weighted average of the initial hidden values for all agents.

Theorem 5: Let us consider a network of n agents interconnected by a directed and strongly connected graph $G = \{V, E\}$ and interacting according to the dynamics in (10). Moreover, let us assume that the dynamics for $\boldsymbol{x}(t)$ satisfies Theorem 1 (and thus synchronizes). Then, it holds

$$\lim_{t\to\infty} \boldsymbol{h}(t) = \mathbf{1}_n \boldsymbol{\zeta}^T \boldsymbol{h}_0,$$

i.e., the local outputs $h_i(t)$ asymptotically converge to a weighted average of the hidden initial states $\boldsymbol{h}(0)$, considering the weights encoded by $\boldsymbol{\zeta}$.

Proof: To prove the result, we observe that

$$\begin{aligned} z(t) &= e^{-Lt}z(0) + \int_0^t e^{-L(t-\tau)} Q\dot{\boldsymbol{x}}(\tau)\, d\tau \\ &= e^{-Lt}z(0) + e^{-Lt}\int_0^t e^{L\tau} Q\dot{\boldsymbol{x}}(\tau)\, d\tau \\ &= e^{-Lt}z(0) + e^{-Lt}\left(e^{Lt}Q\boldsymbol{x}(t) - e^{L0}Q\boldsymbol{x}(0)\right) \\ &\quad - e^{-Lt}\int_0^t Le^{L\tau} Q\boldsymbol{x}(\tau)\, d\tau \\ &= e^{-Lt}\left(z(0) - Q\boldsymbol{x}(0)\right) + Q\boldsymbol{x}(t) \\ &\quad - \int_0^t \underbrace{e^{-Lt}Le^{L\tau}Q\boldsymbol{x}(\tau)}_{s(t,\tau)}\, d\tau. \end{aligned} \tag{11}$$

At this point, we claim that

$$\lim_{t\to\infty} \int_0^t s(t,\tau) = \mathbf{0}_n.$$

In fact we observe that, when t approaches infinity but τ is finite, we have that e^{-Lt} approaches $\mathbf{1}_n\boldsymbol{\zeta}^T$ and thus $e^{-Lt}L$ approaches $\mathbf{1}_n\boldsymbol{\zeta}^T L$, which is zero; since for finite τ, by construction, $e^{L\tau}Q\boldsymbol{x}(\tau)$ is bounded, we conclude that $\boldsymbol{s}(t,\tau)$ approaches zero. If, conversely, both t and τ approach infinity we have that (i) $\boldsymbol{x}(t)$ reaches synchronization by Theorem 1, (ii) $Q\boldsymbol{x}(\tau)$ approaches a vector $\alpha(\tau)\mathbf{1}_n$ for some $\alpha(\tau)$ by (9), and (iii) $e^{L\tau}\mathbf{1}_n = \mathbf{1}_n$ by construction. Thus, we have that $\boldsymbol{s}(t,\tau)$ approaches

$$\mathbf{1}_n\boldsymbol{\zeta}^T L e^{L\tau}\alpha(\tau)\mathbf{1}_n = \alpha(\tau)\mathbf{1}_n\boldsymbol{\zeta}^T L\mathbf{1}_n = \mathbf{0}_n$$

and, also in this latter case, $\boldsymbol{s}(t,\tau)$ approaches zero. In conclusion, in the limit of t approaching infinity, $\boldsymbol{s}(t,\tau)$ is zero for all finite values of τ and when τ approaches infinity. This implies that

$$\lim_{t\to\infty} \int_0^t \boldsymbol{s}(t,\tau)\, d\tau = \mathbf{0}_n$$

and our claim is verified.

As a consequence, we have that

$$\begin{aligned} \lim_{t\to\infty} z(t) - Q\boldsymbol{x}(t) &= \lim_{t\to\infty} e^{-Lt}\left(z(0) - Q\boldsymbol{x}(0)\right) \\ &= \lim_{t\to\infty} e^{-Lt}\boldsymbol{h}(0) \\ &= \boldsymbol{\zeta}_n^T\boldsymbol{h}(0)\mathbf{1}_n \end{aligned}$$

and thus the entries of $\boldsymbol{h}(t) = z(t) - Q\boldsymbol{x}(t)$ converge to the weighted average of $\boldsymbol{h}(0)$, considering the weights encoded by $\boldsymbol{\zeta}$. This completes our proof. ■

A few remarks are now in order.

Remark 6: The proposed approach can easily be applied in cases where the edges in the graph are associated with weights designed to obtain a specific weighted average of the agents' initial conditions. For instance, in [4], a distributed algorithm is provided to rescale the weights of a consensus process to obtain a weighted average specifically designed to minimize the contribution of outliers to the final consensus value.

Remark 7: The proposed approach can easily be extended to guarantee the reach of the actual average of the initial conditions. For instance, an approach based on *ratio consensus* [46], [47] could be adopted, whereby the agents maintain in parallel two weighted average consensus processes, one with the agents' initial conditions and one where all initial conditions are set to one. Then, the actual average can be obtained by taking the ratio of the two consensus variables at each agent. When applied to our framework, this would translate into adding a further weighted average process to the dynamics in (10) where all initial conditions are set to one. Aside from guaranteeing the reach of the actual average, such an extension would not impact privacy (since its initial conditions are all fixed to unity).

V. SECURITY AND PRIVACY

A. SECURITY ANALYSIS

In this section, we discuss the limitations of possible strategies that a malicious eavesdropper can implement. Specifically, we

[3] Notice that the agents are assumed to agree on how $D(t)$ varies with time. An example in this sense is represented by a shared switching policy among a few predetermined matrices at agreed-upon time instants.

assume that a malicious entity aims to identify the consensus value without making changes and disclosing its presence; the following definition captures this behavior.

Definition 5 (Security): A consensus algorithm is said to be *secure* if a third party that is not one of the legitimate nodes in the network (i.e., an eavesdropper that can access the information exchanged but does not tamper such data) cannot reconstruct the state of the legitimate agents, including the hidden initial conditions and the final consensus value.

It is worth mentioning that the injection of noise in the network by a malicious agent could cause a permanent deviation of the hidden variable $\boldsymbol{h}(t)$ from the consensus value. Therefore, an attack with an injection of false data could disrupt synchronization and the achievement of consensus, which is out of the scope of our attack model as this would make it impossible for the attacker to get to know the consensus value.

In the remainder of this subsection, we discuss the challenges of using nonlinear observability analysis to assess the ability of a malicious eavesdropper to observe the agents' state. Moreover, we inspect possible approaches to reconstruct $\boldsymbol{q}$ and show that these strategies are ineffective despite the large amount of knowledge required for the eavesdropper. Finally, we show that the degrees of freedom for the design of the proposed approach are such that the eavesdropper has an infinity of possible alternatives for the vector $\boldsymbol{q}$ and for the hidden consensus trajectory that corresponds to the same evolutions for $\boldsymbol{x}(t)$ and $z(t)$.

1) NONLINEAR OBSERVABILITY

Resorting to nonlinear observability theory (e.g., see [48], [49], [50]) it could be possible, at least in principle, to determine whether or not a malicious eavesdropper provided with some observations of the agents' state can reconstruct the entire state of the system. Notice that such analysis requires full knowledge of the dynamical model and relies on repeated high-order Lie brackets (i.e., up to the number of state variables) to construct a mathematical object that plays the role of the classical observability matrix for LTI systems; however, such a procedure is affected by the "curse of dimensionality". Since the stack of the agents' state encompasses $n(m+1)$ state variables, one would need to be able to compute up to the $n(m+1)$-th order Lie bracket, thus making the endeavor infeasible or impractical, especially for large network size n. What is worse, the theory in [48], [49], [50] requires the dynamics to be smooth, while in the case of Chua oscillators, this is not true due to the presence of the function

$$\theta(y_1) = by_1 + \frac{1}{2}(a-b)\{|y_1+1| - |y_1-1|\},$$

which features absolute values. We would like to point out that, to the best of our knowledge, the only approach available to deal with the observability of nonsmooth, nonlinear systems is to break down the system into different smooth branches [51], [52]. However, this further complicates the analysis; for instance, in the case of a network of n Chua oscillators, it can be shown that the number of points where the derivative of the dynamics is not defined amounts to $2^{2n}-1$, since each agent has two angular points (i.e., $y_1 = 1$ and $y_1 = -1$) and the overall set of angular points encompasses all possible combinations.

In summary, nonlinear observability theory exhibits an overwhelming complexity for both the analyst and the attacker, especially when the number of agents is large, and the synchronizing dynamics are nonsmooth. Moreover, to use observability theory, there is a need to be aware of the overall dynamics. Finally, even if the agents' states were directly available, a lack of knowledge of $\boldsymbol{q}$ would prevent malicious eavesdroppers from reconstructing the hidden consensus dynamics.

In what follows, we investigate possible strategies that a malicious eavesdropper could follow to estimate $\boldsymbol{q}$.

2) FULL KNOWLEDGE ON THE STATES

Let us now consider the worst-case scenario where the eavesdropper has access to the full agents' state vectors at one or more time instants, and let us show that, despite the large amount of information available to the eavesdropper, there is an infinity of possible choices for $\boldsymbol{q}$. In particular, let us assume that a malicious eavesdropper collects the values of $\boldsymbol{x}(t)$ and $z(t)$ at several distinct time instants $t \in \{t_1, \ldots, t_k\}$. Recalling that $h_i(t) = z_i(t) - \boldsymbol{q}^T \boldsymbol{x}_i(t)$, we have that

$$h_i(t) + \boldsymbol{x}_i^T(t)\boldsymbol{q} = z_i(t);$$

stacking the above equation for all agents, we obtain

$$\boldsymbol{h}(t) + \Psi(t)\boldsymbol{q} = z(t), \quad \text{with} \quad \Psi(t) = \begin{bmatrix} \boldsymbol{x}_1(t) & \ldots & \boldsymbol{x}_n(t) \end{bmatrix}^T;$$

in other words, we have that

$$\begin{bmatrix} I_n & \Psi(t) \end{bmatrix} \begin{bmatrix} \boldsymbol{h}(t) \\ \boldsymbol{q} \end{bmatrix} = z(t). \tag{12}$$

The above equation can be extended to consider all times $t \in \{t_1, \ldots, t_k\}$, thus obtaining

$$\underbrace{\begin{bmatrix} I_n & 0 & \ldots & 0 & \Psi(t_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & I_n & \Psi(t_k) \end{bmatrix}}_{\Phi(t_1,\ldots,t_k)} \underbrace{\begin{bmatrix} \boldsymbol{h}(t_1) \\ \vdots \\ \boldsymbol{h}(t_k) \\ \boldsymbol{q} \end{bmatrix}}_{\boldsymbol{r}(t_1,\ldots,t_k)} = \underbrace{\begin{bmatrix} z(t_1) \\ \vdots \\ z(t_k) \end{bmatrix}}_{z(t_1,\ldots,t_k)}. \tag{13}$$

At this point we observe that $\Phi(\cdot) \in \mathbb{R}^{nk\times(nk+m)}$ is in the form

$$\Phi(\cdot) = \begin{bmatrix} I_{nk\times nk} & * \end{bmatrix}$$

and is thus full rank. Therefore, by the Rouché-Capelli Theorem, the above equation admits an infinity of solutions (specifically, ∞^m).

From the point of view of the eavesdropper, this means that there is no obvious way to identify the correct $\boldsymbol{q}$ by collecting observations on $\boldsymbol{x}(t)$ and $z(t)$ at several time instants; notably, this represents the worst case scenario since the agents share $D(t)\boldsymbol{x}_i(t)$ and thus the full vectors $\boldsymbol{x}_i(t)$ are never directly shared.

3) FULL KNOWLEDGE ON THE TOPOLOGY

Interestingly, even if the above strategy is ineffective, an attacker that knows the vector $\boldsymbol{\zeta}$ that encodes the weights of the weighted average consensus process could attempt to use this information to find $\boldsymbol{q}$. In particular, we recall that, by knowing the graph topology, the eavesdropper can compute $\boldsymbol{\zeta}$ as the left eigenvector of the graph's Laplacian matrix associated with the zero eigenvalue. In fact, noting that $\dot{z}(t) = -Lz(t) + Q\dot{\boldsymbol{x}}(t)$, we have that

$$\boldsymbol{\zeta}^T \dot{z}(t) = -\underbrace{\boldsymbol{\zeta}^T Lz(t)}_{\boldsymbol{0}_n} + \boldsymbol{\zeta}^T Q\dot{\boldsymbol{x}}(t) = \sum_{i=1}^{n} \zeta_i \dot{\boldsymbol{x}}_i^T(t)\boldsymbol{q}. \tag{14}$$

Therefore, to derive $\boldsymbol{q}$, an attacker will need at least m linearly independent observations of $\dot{\boldsymbol{x}}(t)$ and m observations of $\dot{z}(t)$. Specifically, it must be able to compute

$$\underbrace{\begin{bmatrix} \sum_{i=1}^n \zeta_i \dot{\boldsymbol{x}}_i^T(t_1) \\ \vdots \\ \sum_{i=1}^n \zeta_i \dot{\boldsymbol{x}}_i^T(t_m) \end{bmatrix}}_{\dot{\mathcal{X}}} \boldsymbol{q} = \underbrace{\begin{bmatrix} \boldsymbol{\zeta}^T \dot{z}(t_1) \\ \vdots \\ \boldsymbol{\zeta}^T \dot{z}(t_m) \end{bmatrix}}_{\dot{\mathcal{Z}}}, \tag{15}$$

from which, assuming $\dot{\mathcal{X}}$ is nonsingular,

$$\boldsymbol{q} = \dot{\mathcal{X}}^{-1}\dot{\mathcal{Z}}. \tag{16}$$

Notably, while the agents exchange $z_i(t)$, they do not directly exchange $\dot{z}_i(t)$; estimating $\dot{z}_i(t)$ would require numerical differentiation of $z_i(t)$, thus introducing errors. Finally, it should be noted that neither $\boldsymbol{x}_i(t)$ nor $\dot{\boldsymbol{x}}_i(t)$ are directly exchanged by the agents (i.e., they exchange $D(t)\boldsymbol{x}_i(t)$).

4) MULTIPLE SOLUTIONS FOR THE SAME AGENTS' STATES

We conclude our security analysis by showing that from the point of view of the attacker, there is an infinity of choices for $\boldsymbol{q}$ and $\boldsymbol{h}(\cdot)$ that correspond to the same agents' states $z(\cdot)$ and $\boldsymbol{x}(\cdot)$.

Proposition 8: Let $\boldsymbol{q}$, $\boldsymbol{h}(0)$ and a set $\mathcal{T} = \{t_1, \ldots, t_k\}$ of nonnegative distinct time instants be given. There is an infinity of choices for $\overline{\boldsymbol{h}}(\cdot)$ and $\overline{\boldsymbol{q}}$ such that

$$\overline{h}_i(t) = z_i(t) - \overline{\boldsymbol{q}}_i^T(t)\boldsymbol{x}_i(t), \quad \forall i \in \{1, \ldots, n\}, \quad \forall t \in \mathcal{T}.$$

Proof: To prove the result, let us consider a specific time instant t; for this proposition to hold, there must be

$$\overline{\boldsymbol{h}}(t) = \boldsymbol{h}(t) + \Delta\boldsymbol{h}(t) \quad \text{and} \quad \overline{\boldsymbol{q}} = \boldsymbol{q} + \Delta\boldsymbol{q}$$

such that (12) holds true, i.e., such that

$$\begin{bmatrix} I_n & \Psi(t) \end{bmatrix} \begin{bmatrix} \boldsymbol{h}(t) + \Delta\boldsymbol{h}(t) \\ \boldsymbol{q} + \Delta\boldsymbol{q} \end{bmatrix} = z(t). \tag{17}$$

But since (12) holds also for the nominal $\boldsymbol{h}(t)$ and $\boldsymbol{q}$, we conclude that it must hold

$$\begin{bmatrix} I_n & \Psi(t) \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{h}(t) \\ \Delta\boldsymbol{q} \end{bmatrix} = \boldsymbol{0}_n. \tag{18}$$

More generally, considering $t \in \mathcal{T}$, with similar reasoning as above, we have that it must hold

$$\Phi(t_1, \ldots, t_k)\, \Delta\boldsymbol{r}(t_1, \ldots, t_k) = \boldsymbol{0}_n, \tag{19}$$

where $\Phi(t_1, \ldots, t_k)$ is defined in (13) and

$$\Delta\boldsymbol{r}(t_1, \ldots, t_k) = \begin{bmatrix} \Delta\boldsymbol{h}^T(t_1) & \ldots & \Delta\boldsymbol{h}^T(t_k) & \Delta\boldsymbol{q}^T \end{bmatrix}^T.$$

At this point we observe that, by construction, $\Phi(t_1, \ldots, t_k)$ is $nk \times (nk + m)$ and is full rank, hence

$$\mathtt{dim}(\mathtt{ker}(\Phi(t_1, \ldots, t_k))) = m,$$

and, thus, there is an infinity of choices for $\Delta\boldsymbol{h}(\cdot)$ and $\Delta\boldsymbol{q}$ that satisfy (19). The proof is complete. ■

B. PRIVACY ANALYSIS

In this section, we aim to evaluate a possible strategy for the violation of privacy on the initial conditions of legitimate nodes and show its failure if Assumption 1 holds. The following definition expresses the concept of privacy preservation to which we refer.

Definition 6 (Privacy): A consensus algorithm is said to be *private* if each node involved cannot reconstruct the initial conditions of its neighbors, or any other node.

Notice that the most interesting aspect of the proposed approach is that the agents exchange $z_i(t)$ and $D(t)\boldsymbol{x}_i(t)$, but locally compute $h_i(t)$, which, under mild hypotheses, is a different combination of the state variables, and is thus not directly shared.

Let us assume an honest but curious node ℓ is an out neighbor of a target node i. Then, node ℓ cannot retrieve the hidden initial value of i if Assumption 1 holds. In fact, we observe that

$$\begin{aligned} z(t) &= z(0) + \int_0^t \dot{z}(\tau)d\tau \\ &= z(0) - L\int_0^t z(\tau)d\tau + Q\boldsymbol{x}(t) - Q\boldsymbol{x}(0). \end{aligned}$$

Therefore, considering the i-th agent and defining $\boldsymbol{e}_i$ as the i-th vector in the canonical basis of $\mathbb{R}^n$, we have that

$$\begin{aligned} z_i(t) &= z_i(0) + \int_0^t \sum_{j \in \mathcal{N}_i^{\text{in}}} \big(z_j(\tau) - z_i(\tau)\big)\, d\tau \\ &\quad + \left(\boldsymbol{e}_i^T \otimes \boldsymbol{q}^T\right)(\boldsymbol{x}(t) - \boldsymbol{x}(0)) \\ &= z_i(0) + \int_0^t \sum_{j \in \mathcal{N}_i^{\text{in}}} \big(z_j(\tau) - z_i(\tau)\big)\, d\tau \\ &\quad + \boldsymbol{q}^T(\boldsymbol{x}_i(t) - \boldsymbol{x}_i(0)) \\ &= z_i(0) - d_i\int_0^t z_i(\tau)d\tau + \sum_{j \in \mathcal{N}_i^{\text{in}}} \int_0^t z_j(\tau)d\tau \\ &\quad + \boldsymbol{q}^T(\boldsymbol{x}_i(t) - \boldsymbol{x}_i(0)); \end{aligned}$$

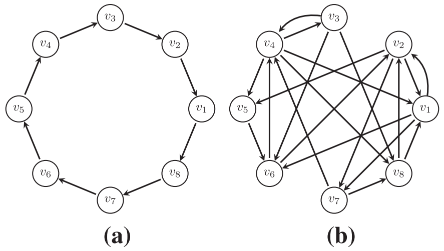

FIGURE 2. Graph topologies considered for the simulations. (a) Ring balanced graph topology G_1 with $|V_1| = 8$ nodes and $|E_1| = 8$ directed edges. (b) Unbalanced graph topology G_2 with $|V_2| = 8$ nodes and $|E_2| = 20$ directed edges.

since $h_i(0) = z_i(0) - \boldsymbol{q}^T \boldsymbol{x}_i(0)$, we have that

$$h_i(0) = z_i(t) + d_i \int_0^t z_i(\tau)d\tau - \sum_{j \in \mathcal{N}_i^{\text{in}}} \int_0^t z_j(\tau)d\tau - \boldsymbol{q}^T \boldsymbol{x}_i(t). \tag{20}$$

Now we can observe from (20) that in order for the curious node to reconstruct $h_i(0)$ according to the above scheme, it must be able to compute

$$\sum_{j \in \mathcal{N}_i^{\text{in}}} \int_0^t z_j(\tau)d\tau, \quad \forall v_j \in \mathcal{N}_i^{\text{in}} \cup \{v_i\},$$

i.e., node i must be exposed to the curious node thus violating Assumption 1.

VI. SIMULATIONS

In this section, we aim to demonstrate the effectiveness of the proposed approach via a simulation scenario. In particular, we choose as a case study for the nonlinear function the dynamics of the chaotic Chua oscillator, setting $\boldsymbol{f}(\boldsymbol{x}(t), t)$, $D(t)$ and V as in (7), and we consider two directed network topologies that satisfy Assumption 1. The first one is a directed ring graph $G_1 = \{V_1, E_1\}$ with $|V_1| = 8$ nodes and $|E_1| = 8$ directed edges (reported in Fig. 2(a)), while the second one is a random topology $G_2 = \{V_2, E_2\}$ with $|V_2| = 8$ nodes and $|E_2| = 20$ directed edges (reported in Fig. 2(b)). Notably, G_2 is *unbalanced*, i.e., the in- and out-degrees do not coincide for all nodes.

For both topologies, the agents aim to achieve the average of their hidden initial conditions cooperatively

$$\boldsymbol{h}_0 = \begin{bmatrix} -32.37 & -10.10 & -27.28 & -24.67 \\ -13.96 & -23.94 & -21.08 & -20.14 \end{bmatrix}^T$$

without disclosing them to each other. To this end, each agent randomly selects a set of initial conditions for the Chua oscillator variables

$$\boldsymbol{x}_{10} = [2.60 \quad 7.37 \ 7.97 \ 0.26 \ 4.97 \ 5.51 \ 3.13 \ 6.58]^T,$$

$$\boldsymbol{x}_{20} = [3.87 \ 3.79 \ 2.69 \ 6.62 \ 4.15 \ 9.73 \ 0.42 \ 2.15]^T,$$

$$\boldsymbol{x}_{30} = [8.32 \ 0.13 \ 5.83 \ 3.88 \ 3.51 \ 1.13 \ 7.38 \ 4.17]^T.$$

Then, to also ensure the security of the approach, agents select a common vector[4] $\boldsymbol{q} = [1 \quad 2 \quad 3]^T$ and each agent i calculates the initial values for the shared variables as $z_{0i} = h_{0i} + \boldsymbol{q}^T \boldsymbol{x}_{0i}$, thus obtaining

$$z_0 = [2.93 \quad 5.24 \ 3.57 \ 0.46 \ 9.83 \ 4.41 \ 5.04 \ 3.24]^T.$$

Notice that, in the simulations, the parameters of the Chua oscillators are set as follows:

$$\alpha = 10, \beta = 15, \gamma = 0.0385, a = -1.5, b = -0.9, c = 3,$$

while each component of the input noise $\boldsymbol{u}_i(t) \in \mathbb{R}^3$ is initially set as $u_{ij}(t) = \sin(10t + \phi_{ij})$, where ϕ_{ij} is chosen uniformly at random in $[0, 2\pi]$, and then becomes a constant value $u_{ij}(t) = 2$ for $t > 2[s]$. Finally, we assume the matrix $P = \eta L$ with $\eta = 100$. Considering the ring topology (in this case $\boldsymbol{\zeta} = \mathbf{1}_n/n$, where $n = 8$), we can observe from Fig. 3(a) that, as the time approaches infinity, each $h_i(t)$ approaches the average of the entries of the initial condition vector $\boldsymbol{h}_0$, i.e., the value -21.69. On the other hand, what circulates in the network and is seen from an external eavesdropper is equal to a chaotically oscillating synchronized variable (the variable $\boldsymbol{z}(t)$ in Fig. 3(b)). Fig. 3(c) shows the trend of the three state variables of the Chua oscillators at each agent, which are shown to synchronize.

Considering the random topology, since the graph is unbalanced, the consensus hidden variable will tend to be a weighted average according to the dominant left eigenvector ζ. In particular, as shown in Fig. 4(a), we have that $\lim_{t \to \infty} h_i(t) = -23.76$. Also, in this case, the dynamics of the exchanged variables $\boldsymbol{z}(t)$ remain oscillatory and synchronized (see Fig. 4(b)), and the state variables of the oscillator $\boldsymbol{x}(t)$ also synchronize (see Fig. 4(c)).

To conclude the section, let us show how the results in Theorem 2 can be used to guide the design of the synchronization dynamics $\boldsymbol{f}(\boldsymbol{x}(t), t)$. Specifically, let us consider $n = 6$ agents, and let us assume that the synchronization dynamics at each agent features $m = 3$ state variables. Moreover, for all $t \geq 0$, let us consider the $n \times n$ matrix $S(t) = (20 + 5\sin(20t))\mathcal{S}$ with

$$\mathcal{S} = \begin{bmatrix} 12 & 0.5 & 5 \\ 0.2 & 3 & 0.3 \\ 3 & 0.1 & 20 \end{bmatrix}.$$

Notably, for all $t \geq 0$, the eigenvalues of $S(t)$ are lower bounded by $\delta \approx 44.85$; therefore, the quadratic time-varying function $g(\boldsymbol{x}, t) = \frac{1}{2}\boldsymbol{x}^T S(t)\boldsymbol{x} + \boldsymbol{\omega}^T(t)\boldsymbol{x}$ is strongly convex. As a consequence, according to Theorem 2,

$$\boldsymbol{f}(\boldsymbol{x}, t) = -\nabla_{\boldsymbol{x}} g(\boldsymbol{x}, t) = -S(t)\boldsymbol{x} - \boldsymbol{\omega}(t) \tag{21}$$

is V-uniformly decreasing with $V = I_n$. In this example, we set

$$\boldsymbol{\omega}(t) = 10e^{2\boldsymbol{x}(t)} \sin(10t).$$

[4] Note that the sharing of this information over the network can be done securely in an initialization phase in which this vector is sent encrypted.

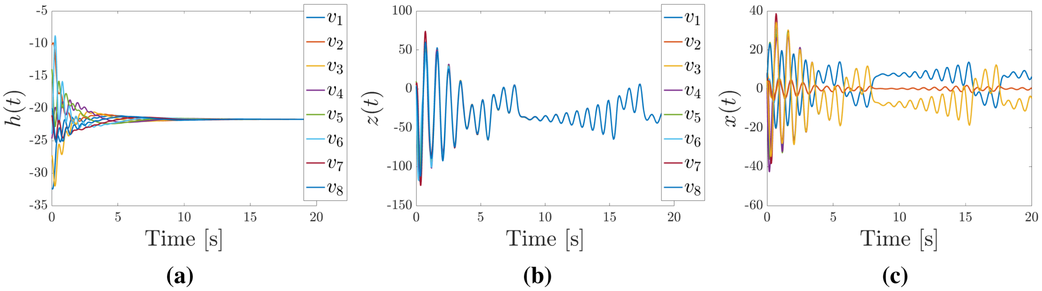

FIGURE 3. The figure shows the temporal evolution of all the dynamics in place considering the topology G_1 of the directed ring graph and the Chua oscillator as nonlinear dynamics. (a) Temporal evolution of local state variable $h(t)$ carrying the hidden consensus value; the consensus on the weighted average of the initial conditions is reached. (b) Temporal evolution of the shared state variable $z(t)$; a consensus is reached but on a time-varying and oscillatory value, far from the actual consensus value. (c) Temporal evolution of the three dynamics $x(t)$ of the Chua oscillator.

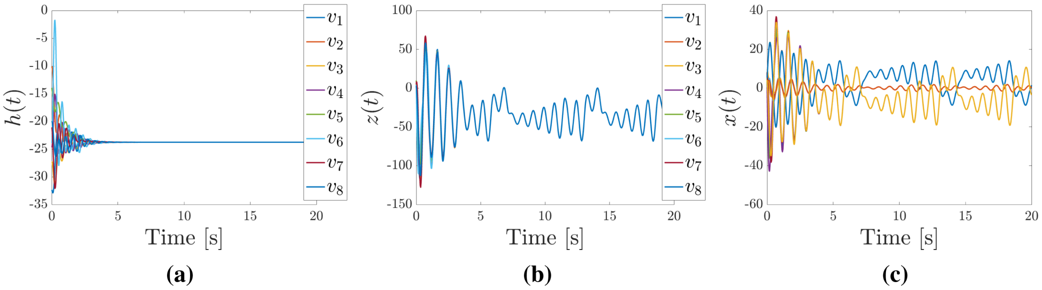

FIGURE 4. The figure shows the temporal evolution of all the dynamics in place considering the topology G_2 of the unbalanced random graph and the Chua oscillator as nonlinear dynamics. (a) Temporal evolution of local state variable $h(t)$ carrying the hidden consensus value; the consensus on the weighted average of the initial conditions is reached. (b) Temporal evolution of the shared state variable $z(t)$; a consensus is reached but on a time-varying and oscillatory value, far from the actual consensus value. (c) Temporal evolution of the three dynamics $x(t)$ of the Chua oscillator.

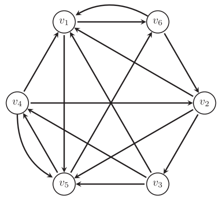

FIGURE 5. Unbalanced graph topology G_3 with $|V_3| = 6$ nodes and $|E_3| = 15$ directed edges.

and we consider the directed unbalanced topology $G_3 = \{V_3, E_3\}$ in Fig. 5 with $|V_3| = 6$ nodes and $|E_3| = 15$ directed edges.

The initial conditions selected by the agents are

$$\boldsymbol{h}_0 = [4.70 \quad 5.20 \quad -0.42 \quad 5.60 \quad 7.57 \quad 4.06]^T,$$

$$\boldsymbol{x}_{10} = [0.28 \quad 0.45 \quad 0.29 \quad 0.68 \quad 0.49 \quad 0.15]^T,$$

$$\boldsymbol{x}_{20} = [0.79 \quad 0.90 \quad 0.13 \quad 0.21 \quad 0.05 \quad 0.59]^T,$$

$$\boldsymbol{x}_{30} = [0.10 \quad 0.29 \quad 0.02 \quad 0.27 \quad 0.57 \quad 0.70]^T,$$

$$z_0 = [6.87 \quad 8.35 \quad 0.18 \quad 7.5 \quad 9.89 \quad 7.48]^T.$$

In this example, we consider a time-varying matrix $D(t)$, which assumes three possible values over time. Specifically, we assume that

$$D(t) = \begin{bmatrix} -9 & 1 & 0 \\ 1 & -5 & 3 \\ 0 & 3 & -10 \end{bmatrix} \quad \text{for } t < 2[s],$$

$$D(t) = \begin{bmatrix} -2 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & -4 \end{bmatrix} \quad \text{for } 2 < t < 5[s],$$

and

$$D(t) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -9 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix} \quad \text{for } t > 5[s],$$

that satisfy Theorem 1. Moreover, $\boldsymbol{q}, \boldsymbol{u}(t)$ and η are chosen as in the previous case. Similarly to what was shown in the previous simulations, the hidden state $\boldsymbol{h}(t)$ reaches the consensus value of 3.49 (Fig. 6(a)), i.e., the weighted average of the initial conditions $\boldsymbol{h}_0$. In contrast, the exchanged variable $z(t)$ is synchronized but continues to oscillate (Fig. 6(b)). Finally, Fig. 6(c) shows the trend of the variable x, which expresses the dynamics of the chosen nonlinear function.

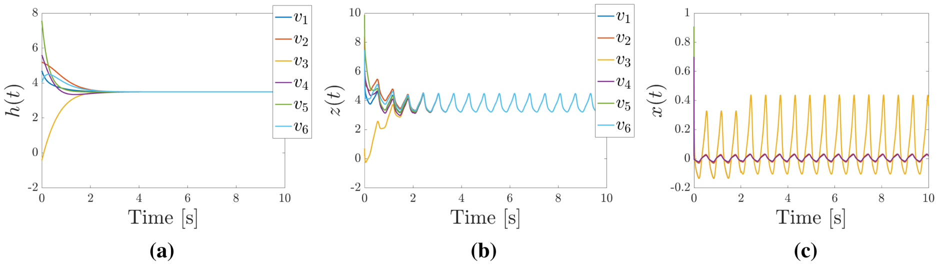

FIGURE 6. The figure shows the temporal evolution of all the dynamics in place considering the topology G_3 of the unbalanced random graph and the generic nonlinear function in (21) as nonlinear dynamics. (a) Temporal evolution of local state variable $h(t)$ carrying the hidden consensus value; the consensus on the weighted average of the initial conditions is reached. (b) Temporal evolution of the shared state variable $z(t)$; a consensus is reached but on a time-varying and oscillatory value, far from the actual consensus value. (c) Temporal evolution of the nonlinear dynamics $x(t)$ corresponding to the nonlinear function $f(\cdot)$ as in (21).

VII. CONCLUSION

In this article, we presented a novel consensus methodology that utilizes the synchronization of a network of nonlinear dynamic systems to guarantee privacy and security against eavesdroppers and malicious third parties. Specifically, we considered a directed and strongly connected graph topology, where agents aim to compute a weighted average of their initial conditions. Our approach splits the initial value to initialize a distributed synchronization process for a network of nonlinear dynamical systems characterized by noise, partial information sharing, and time-varying coupling, and a linear average consensus process influenced by nonlinear synchronization. By relying on nonlinear synchronization, the proposed approach provides a layer of security against malicious third parties who lack knowledge of the nonlinear models and the matrix used to reconstruct the consensus value. Furthermore, the approach ensures privacy by introducing noise and different transients for the agents before synchronization is achieved. Compared to our preliminary conference article, this article presents significant improvements in terms of generality and robustness. We extended the approach from the synchronization of a network of Chua oscillators over an undirected graph with static coupling and in the absence of noise to a general framework for the synchronization of networks of nonlinear systems, characterized by possibly directed interaction topologies, time-varying coupling, and presence of noise. We also investigated the privacy and security characteristics of the framework and established a relation between synchronization and the overall dynamics as a gradient descent along a strongly convex function.

Overall, the proposed approach has promising potential for real-world applications that require secure and private consensus in distributed networks. Expected future work directions include extending the framework to withstand communication delays and applying the methodology to distributed estimation or optimization algorithms.

REFERENCES

[1] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[2] R. Olfati-Saber, J. A. Fax, and R. M. Murray, “Consensus and cooperation in networked multi-agent systems,” *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[3] P. Jia, A. MirTabatabaei, N. E. Friedkin, and F. Bullo, “Opinion dynamics and the evolution of social power in influence networks,” *SIAM Rev.*, vol. 57, no. 3, pp. 367–397, 2015.

[4] G. Oliva, A. I. Rikos, A. Gasparri, and C. N. Hadjicostis, “Distributed negotiation for reaching agreement among reluctant players in cooperative multiagent systems,” *IEEE Trans. Autom. Control*, vol. 67, no. 9, pp. 4838–4845, Sep. 2022.

[5] E. D. Costanzo, M. Menci, E. Messina, R. Natalini, and A. Vecchio, “A hybrid model of collective motion of discrete particles under alignment and continuum chemotaxis,” *Discrete Continuous Dyn. Syst.- Ser. B*, vol. 25, no. 1, pp. 443–472, 2020.

[6] R. Olfati-Saber, “Kalman-consensus filter: Optimality, stability, and performance,” in *Proc. 48th IEEE Conf. Decis. Control, Held Jointly 28th Chin. Control Conf.*, 2009, pp. 7036–7042.

[7] L. Sabattini, C. Secchi, N. Chopra, and A. Gasparri, “Distributed control of multirobot systems with global connectivity maintenance,” *IEEE Trans. Robot.*, vol. 29, no. 5, pp. 1326–1332, Oct. 2013.

[8] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, “Smart grid metering networks: A survey on security, privacy and open research issues,” *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2886–2927, Third quarter 2019.

[9] M. Abdel-Basset, N. Moustafa, and H. Hawash, “Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 995–1005, Jan. 2023.

[10] T. Gebremichael et al., “Security and privacy in the industrial Internet of Things: Current standards and future challenges,” *IEEE Access*, vol. 8, pp. 152351–152366, 2020.

[11] P. Boopalan et al., “Fusion of federated learning and industrial Internet of Things: A survey,” *Comput. Netw.*, vol. 212, 2022, Art. no. 109048.

[12] C. W. Wu and L. O. Chua, “A unified framework for synchronization and control of dynamical systems,” *Int. J. Bifurcation Chaos*, vol. 4, no. 4, pp. 979–998, 1994.

[13] N. E. Manitara and C. N. Hadjicostis, “Privacy-preserving asymptotic average consensus,” in *Proc. Eur. Control Conf.*, 2013, pp. 760–765.

[14] Y. Mo and R. M. Murray, “Privacy preserving average consensus,” *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[15] Y. Xiong and Z. Li, “Privacy preserving average consensus by adding edge-based perturbation signals,” in *Proc. IEEE Conf. Control Technol. Appl.*, 2020, pp. 712–717.

[16] T. Charalambous, N. E. Manitara, and C. N. Hadjicostis, “Privacy-preserving average consensus over digraphs in the presence of time delays,” in *Proc. 57th Annu. Allerton Conf. Commun., Control, Comput.*, 2019, pp. 238–245.

[17] A. I. Rikos, T. Charalambous, K. H. Johansson, and C. N. Hadjicostis, “Distributed event-triggered algorithms for finite-time privacy-preserving quantized average consensus,” *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 1, pp. 38–50, Mar. 2023.

[18] N. Rezazadeh and S. S. Kia, “Privacy preservation in a continuous-time static average consensus algorithm over directed graphs,” in *Proc. Amer. Control Conf.*, 2018, pp. 5890–5895.

[19] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, no. 7, pp. 221–231, 2017.

[20] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, 2019.

[21] C. N. Hadjicostis, "Privary preserving distributed average consensus via homomorphic encryption," in *Proc. IEEE 57th Conf. Decis. Control*, 2018, pp. 1258–1263.

[22] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on Paillier encryption," *Syst. Control Lett.*, vol. 148, 2021, Art. no. 104869.

[23] C. N. Hadjicostis and A. D. Domínguez-García, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3887–3894, Sep. 2020.

[24] M. Kishida, "Encrypted average consensus with quantized control law," in *Proc. IEEE 57th Conf. Decis. Control*, 2018, pp. 5850–5856.

[25] M. Calis, R. Heusdens, and R. C. Hendriks, "A privacy-preserving asynchronous averaging algorithm based on state decomposition," in *Proc. 28th Eur. Signal Process. Conf.*, 2021, pp. 2115–2119.

[26] A. B. Pilet, D. Frey, and F. Taïani, "Robust privacy-preserving gossip averaging," in *Proc. Int. Symp. Stabilizing, Saf., Secur. Distrib. Syst.*, 2019, pp. 38–52.

[27] R. M. Ferrari and A. M. Teixeira, "Detection of cyber-attacks: A multiplicative watermarking scheme," in *Safety, Security and Privacy for Cyber-Physical Systems*. Berlin, Germany: Springer, 2021, pp. 173–201.

[28] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[29] R. Schmitz, "Use of chaotic dynamical systems in cryptography," *J. Franklin Inst.*, vol. 338, no. 4, pp. 429–441, 2001.

[30] X. Liu, C. Li, S. Ge, and D. Li, "Time-synchronized control of chaotic systems in secure communication," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 69, no. 9, pp. 3748–3761, Sep. 2022.

[31] M. Z. D. l. Hoz, L. Acho, and Y. Vidal, "A modified chua chaotic oscillator and its application to secure communications," *Appl. Math. Comput.*, vol. 247, pp. 712–722, 2014.

[32] M. Wang, X. Wang, Y. Zhang, and Z. Gao, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," *Opt. Laser Technol.*, vol. 108, pp. 558–573, 2018.

[33] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.

[34] C. Fioravanti, G. Oliva, S. Panzieri, and C. N. Hadjicostis, "Private consensus using chaotic oscillator-based encryption," in *Proc. 30th Mediterranean Conf. Control Automat.*, 2022, pp. 927–932.

[35] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[36] C. Godsil and G. F. Royle, *Algebraic Graph Theory*, vol. 207. Berlin, Germany: Springer, 2001.

[37] C. Fioravanti, G. Oliva, L. Faramondi, and C. N. Hadjicostis, "A geometrical approach for consensus security," *Syst. Control Lett.*, submitted for publication.

[38] I. L. D. Ridgley, R. A. Freeman, and K. M. Lynch, "Private and hot-pluggable distributed averaging," *IEEE Contr. Syst. Lett.*, vol. 4, no. 4, pp. 988–993, Oct. 2020.

[39] C. W. Wu, *Synchronization in Complex Networks of Nonlinear Dynamical Systems*. Singapore: World Scientific, 2007.

[40] J. Stewart, *Calculus*. Boston, MA, USA: Cengage Learn., 2011.

[41] J. S. Prasath, U. Ramachandraiah, and G. Muthukumaran, "Modified hardware security algorithms for process industries using Internet of Things," *J. Appl. Secur. Res.*, vol. 16, n. 1, pp. 127–140, 2021.

[42] A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad hoc networks," in *Proc. IEEE Workshop Secur. Assurance Ad hoc Netw., Conjunction Int. Symp. Appl. Internet*, 2003, pp. 342–346.

[43] M. D. Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key management for beyond 5G mobile small cells: A survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019.

[44] G. Antonelli, F. Arrichiello, S. Chiaverini, and R. Setola, "A self-configuring MANET for coverage area adaptation through kinematic control of a platoon of mobile robots," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2005, pp. 1332–1337.

[45] P. Brass, F. Cabrera-Mora, A. Gasparri, and J. Xiao, "Multirobot tree and graph exploration," *IEEE Trans. Robot.*, vol. 27, no. 4, pp. 707–717, Aug. 2011.

[46] A. D. Dominguez-Garcia and C. N. Hadjicostis, "Coordination and control of distributed energy resources for provision of ancillary services," in *Proc. Int. Conf. Smart Grid Commun.*, 2010, pp. 537–542.

[47] C. N. Hadjicostis and T. Charalambous, "Average consensus in the presence of delays in directed graph topologies," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 763–768, Mar. 2014.

[48] H. Nijmeijer and A. V. d. Schaft, *Nonlinear Dynamical Control Systems*. New York, NY, USA: Springer-Verlag, 1990.

[49] G. Conte, C. H. Moog, and A. M. Perdon, *Algebraic Methods for Nonlinear Control Systems*, Berlin, Germany: Springer, 2007.

[50] X. Shi and M. N. Chatzis, "Lie symmetries of nonlinear systems with unknown inputs," *Mech. Syst. Signal Process.*, vol. 188, 2023, Art. no. 110027.

[51] M. N. Chatzis, E. N. Chatzi, and A. W. Smyth, "On the observability and identifiability of nonlinear structural and mechanical systems," *Struct. Control Health Monit.*, vol. 22, n. 3, pp. 574–593, 2015.

[52] K. Maes, M. N. Chatzis, and G. Lombaert, "Observability of nonlinear systems with unmeasured inputs," *Mech. Syst. Signal Process.*, vol. 130, pp. 378–394, 2019.

CAMILLA FIORAVANTI (Student Member, IEEE) received the M.Sc. degree in biomedical engineering in 2020 from University Campus Bio-Medico of Rome, Selcetta, Italy, where she is currently working toward the Ph.D. degree in science and engineering for Humans and the Environment, under the supervision of Prof. Gabriele Oliva. She spent a visiting period with the University of Cyprus, Nicosia, Cyprus. Her main research interests include distributed systems, distributed estimation, security and privacy preserving approaches, and fault detection.

VALERIA BONAGURA (Student Member, IEEE) received the M.Sc. degree in automation engineering in 2022 from University of Roma Tre, Rome, Italy, where she is currently working toward the Italian National Ph.D. Programme in Autonomous Systems (DAUSY), under the supervision of Prof. Stefano Panzieri and Prof. Federica Pascucci. Her main research interests include distributed systems, distributed estimation, and model-based fault and anomaly detection.

GABRIELE OLIVA (Senior Member, IEEE) received the M.Sc. and the Ph.D. degrees in computer science and automation engineering from the University Roma Tre of Rome, Rome, Italy, in 2008 and 2012, respectively. He is currently an Associate Professor in automatic control with the University Campus Bio-Medico of Rome, Selcetta, Italy, where he directs the Complex Systems & Security Laboratory (CoserityLab). His main research interests include distributed multi-agent systems, optimization, decision-making, and critical infrastructure protection. Since 2019, he has been an Associate Editor for the Conference Editorial Board of the IEEE Control Systems Society. Since 2020, he has been an Academic Editor for the journal *PLOS ONE* on subject areas such as Systems Science, Optimization and Decision Theory. Since 2022 he has been an Associate Editor for the IEEE CONTROL SYSTEMS LETTERS.

CHRISTOFOROS N. HADJICOSTIS (Fellow, IEEE) received the S.B. degrees in electrical engineering, in computer science and engineering, and in mathematics, the M.Eng. degree in electrical engineering and computer science in 1995, and the Ph.D. degree in electrical engineering and computer science in 1999, from the Massachusetts Institute of Technology, Cambridge, MA, USA. Since 2007, he has been with the Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus, where he is currently Professor and Interim Director of the Daedalus Research Center. His research interests include fault diagnosis and tolerance in distributed dynamic systems, error control coding, monitoring, diagnosis and control of large-scale discrete-event systems, and applications to network security, anomaly detection, energy distribution systems, medical diagnosis, biosequencing, and genetic regulatory models. He is the Editor-in-Chief of the *Journal of Discrete Event Dynamic Systems* and a Senior Editor of IEEE TRANSACTIONS ON AUTOMATIC CONTROL. He was also an Associate Editor for *Automatica*, IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I, and *Hybrid Systems: Nonlinear Analysis*.

STEFANO PANZIERI (Member, IEEE) received the M.Sc. degree in electronic engineering and the Ph.D. degree in systems engineering from the University of Roma La Sapienza, Rome, Italy, in 1989 and 1994, respectively. He is currently a Full Professor with the Department of Civil, Computer Science and Aeronautical Technologies Engineering, University of Roma Tre of Rome, Rome, Italy, where he directs the Models for Critical Infrastructure Protection Laboratory (MCIP lab). His research interests include industrial control systems, robotics, and sensor fusion.

Open Access provided by ‘Università “Campus Bio-Medico” di Roma’ within the CRUI CARE Agreement