Finite Time Distributed Private Control of Complex Dynamical Networks

1st Qidong Liu
School of Automation Engineering
University of Electronic Science and Technology of China
Chengdu, China

***Abstract*—This paper investigates the problem of finite-time distributed control for complex dynamical networks while preserving privacy. In modern networked systems, maintaining the confidentiality of sensitive data during the control process is increasingly critical. We propose a novel control strategy that ensures finite-time stabilization of the networked system while safeguarding the privacy of individual agents' states. The control law is designed to be distributed, requiring only local information and interactions, and employs privacy-preserving mechanisms based on differential privacy principles. Theoretical analysis is provided to prove the finite-time stability of the closed-loop system.**

***Index Terms*—Finite-time control, Distributed control, Privacy, Complex dynamical networks, Differential privacy.**

I. Introduction

In recent years, complex dynamical networks have become a fundamental framework for modeling a wide range of systems in engineering, biology, economics, and social sciences. These networks, composed of interconnected agents or nodes, exhibit rich dynamical behaviors due to the interactions among their components. The control of such networks has attracted significant attention, particularly in ensuring stability and achieving desired performance metrics in a distributed manner. Distributed control strategies are especially relevant for large-scale networks where centralized control is impractical due to scalability issues.

A critical aspect of modern networked systems is the need to preserve the privacy of individual agents' information. In many applications, agents represent sensitive entities such as individuals, organizations, or sensors collecting confidential data. The challenge, therefore, lies in designing control strategies that not only stabilize the network in finite time but also protect the privacy of the agents' states from being inferred by adversaries or even by other agents in the network.

Finite-time control is particularly desirable in applications where a rapid response is essential, and the system needs to reach a desired state within a specific time frame. Unlike traditional asymptotic control, which guarantees convergence over an infinite time horizon, finite-time control ensures that the system stabilizes in a finite time, which is critical for time-sensitive applications. This concept becomes even more challenging in a distributed setting, where each agent in the network must achieve its objective based only on local information and limited communication with its neighbors.

Recent advances in control theory have explored various aspects of distributed control for dynamical networks, focusing on issues such as consensus, synchronization, and robustness against disturbances. However, integrating privacy-preserving mechanisms into the control process while ensuring finite-time stabilization remains relatively unexplored. Differential privacy, a concept originally developed in the context of data privacy, offers a promising approach to safeguarding sensitive information during the control process. By introducing carefully calibrated noise into the control signals, differential privacy ensures that the true states of the agents are obscured, preventing their exact values from being inferred.

In this paper, we propose a novel distributed control framework that achieves finite-time stabilization of complex dynamical networks while preserving the privacy of individual agents' states. The main contributions of this work are as follows:

Here are the sentences revised into passive voice:

1. A finite-time control law is designed to operate in a distributed manner, requiring only local interactions among agents. The control law is augmented with a privacy-preserving mechanism based on differential privacy principles.

2. A rigorous mathematical analysis is provided to demonstrate that the proposed control law guarantees finite-time stabilization of the network. The analysis is based on Lyapunov functions and employs tools from finite-time control theory.

3. It is shown that the proposed control strategy effectively preserves the privacy of agents' states, preventing adversaries from accurately inferring individual states based on the control signals.

II. Main Results

Consider a complex dynamical network consisting of N interconnected agents, each described by the following dynamics:

$$\dot{x}_i(t) = f_i(x_i(t)) + \sum_{j\in\mathcal{N}_i} a_{ij}\phi(x_j(t) - x_i(t)) + u_i(t),$$

where $x_i(t) \in \mathbb{R}^n$ represents the state of the i-th agent, $f_i(\cdot)$ denotes the intrinsic dynamics of the agent, a_{ij} represents the coupling strength between agents i and j, $\mathcal{N}_i$ denotes the set of neighbors of agent i, and $\phi(\cdot)$ is a nonlinear function representing the interaction between connected agents. The control input $u_i(t)$ is designed to ensure that the entire network achieves a desired state within a finite time.

To achieve privacy-preserving finite-time stabilization, we propose the following control law for each agent:

$$u_i(t) = -k_i \text{sgn}(x_i(t) - \hat{x}_i(t))|x_i(t) - \hat{x}_i(t)|^\alpha + \eta_i(t),$$

where $k_i > 0$ is a control gain, $\alpha \in (0, 1)$ ensures finite-time convergence, and $\eta_i(t)$ is a noise term designed according to differential privacy principles to preserve the privacy of the state $x_i(t)$. The noise $\eta_i(t)$ is calibrated to balance the trade-off between control performance and privacy.

The finite-time convergence of the network under the proposed control law is analyzed using a Lyapunov function $V_i(t)$, which for agent i is defined as:

$$V_i(t) = \frac{1}{2}\|x_i(t) - \hat{x}_i(t)\|^2.$$

The time derivative of $V_i(t)$ along the trajectories of the system is given by:

$$\begin{aligned}\dot{V}_i(t) =& (x_i(t) - \hat{x}_i(t))^T \\ & \left[f_i(x_i(t)) + \sum_{j \in \mathcal{N}_i} a_{ij} \phi(x_j(t) - x_i(t)) + u_i(t) \right].\end{aligned} \tag{1}$$

Substituting the control law into the above equation and analyzing the resulting differential inequalities allows us to establish finite-time stability for the entire network.

References

[1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, ”Calibrating noise to sensitivity in private data analysis,” in Theory of Cryptography Conference, 2006, pp. 265-284.

[2] S. P. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, Linear Matrix Inequalities in System and Control Theory, SIAM, 1994.

[3] W. Ren and R. W. Beard, Distributed Consensus in Multi-vehicle Cooperative Control, Springer, 2008.

[4] J. Cortes, ”Finite-time convergent gradient flows with applications to network consensus,” Automatica, vol. 42, no. 11, pp. 1993-2000, 2006.