Privacy-Preserving Dynamic Average Consensus via Random Number Perturbation

Lan Gao, *Member, IEEE*, Yiqun Zhou, Xin Chen, Runfeng Cai, Guo Chen, *Member, IEEE*, and Chaojie Li

***Abstract*—This brief focuses on the study of privacy preservation of dynamic average consensus (DAC) in multi-agent networks. A privacy-preserving DAC (PP-DAC) algorithm is proposed based on a carefully designed random number perturbation mechanism. The PP-DAC algorithm is able to protect agents from the leakage of sensitive information without compromising their tracking accuracy. Furthermore, the privacy analysis for different scenarios is given to show that the PP-DAC algorithm works well unless all neighbors of the target agent collude with each other to attack this agent. Also, some numerical simulations are given to illustrate the validity of the proposed algorithm.**

***Index Terms*—Dynamic average consensus, privacy-preserving consensus, private consensus, multi-agent networks.**

I. Introduction

CONSIDERING a connected network composed of a group of autonomous agents, DAC problems involve designing a distributed algorithm that allows agents to track the average of multiple time-varying reference signals by only exchanging information with their neighbors. The DAC problem has been intensively studied over the past decade due to its universality and significance in the implementation of multi-agent coordination. Its solutions are applied in various fields including data fusion [1], distributed mapping [2], formation control [3] and distributed optimization [4].

Manuscript received 19 September 2022; accepted 24 October 2022. Date of publication 7 November 2022; date of current version 29 March 2023. This work was supported in part by the National Key Research and Development Plan of Ministry of Science and Technology of China under Grant 2020YFC2007902; in part by the National Natural Science Foundation of China under Grant 62203034; in part by the Chongqing Technology Innovation and Application Development Special Key Project under Grant cstc2019jscx-fxydX0054; in part by the Venture and Innovation Support Program for Chongqing Overseas Returnees under Grant cx2019106; in part by the China Postdoctoral Science Foundation under Grant 2022M710326; and in part by the Australian Research Council under Grant IH180100020, Grant DP200101197, and Grant DE210100274. This brief was recommended by Associate Editor W. Gao. *(Corresponding author: Xin Chen.)*

Lan Gao is with the School of Information Science and Technology, Hangzhou Normal University, Hangzhou 310030, China, and also with the Hangzhou Innovation Institute, Beihang University, Hangzhou 310051, China (e-mail: langaouc@gmail.com).

Yiqun Zhou is with the School of Computer Science, Chongqing University, Chongqing 400044, China (e-mail: zhouyiqun@cqu.edu.cn).

Xin Chen and Runfeng Cai are with the School of Big Data and Software Engineering, Chongqing University, Chongqing 400044, China (e-mail: xinchen@cqu.edu.cn; crf@cqu.edu.cn).

Guo Chen and Chaojie Li are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: andyguochen@gmail.com; cjlee.cqu@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSII.2022.3219929.

Digital Object Identifier 10.1109/TCSII.2022.3219929

The early work of DAC is presented in [5], which proposes a distributed algorithm to track the average of dynamic input signals with steady-state values under prescribed initialization conditions. A proportional (P) algorithm and a proportional-integral (PI) one are both proposed in [6] to solve the DAC problem with bounded error. The PI algorithm is then extended in [7], which achieves dynamic average consensus with zero steady-state error for some special classes of inputs, such as polynomial or sinusoidal reference signals. DAC algorithms utilizing discontinuous signum functions and nonlinear protocols to track the accurate average of multiple time-varying inputs are presented in [8] and [9]. DAC algorithms for undirected and directed networks to achieve both zero steady-state error and initialization robustness are proposed in [10]. The discrete-time and event-triggered communication are considered for DAC problems in [11], [12].

In the aforementioned DAC literature, each agent has to communicate with its neighbors honestly to reach an agreement. However, the direct information exchange might lead to disclosure of sensitive information in some practical applications. For example, for a group of unmanned vehicles, some individuals might want to keep their position private while coordinating with others to obtain the global geometric center of dynamic positions of all vehicles. Furthermore, in a smart grid, each agent would like to obtain the average power consumption of the whole network to achieve load balancing while keeping its own consumption data private. In recent years, extensive works have been published to address this issue. Differentially private average consensus is investigated in [13], [14], [15] due to the verified security properties of differential privacy. With carefully designed perturbation signals and state decomposition, accurate average consensus can be achieved by applying the privacy-preserving schemes proposed in [16], [17]. The Paillier cryptosystem and homomorphic encryption schemes are introduced in [18], [19], [20] to achieve average consensus with privacy preservation. To quantify the degree of privacy preservation, the work in [21] provides a theoretical analysis framework.

Compared with the static average consensus mentioned above, there are few works focusing on privacy-preserving schemes for dynamic average consensus. The dynamic average consensus algorithm proposed in [22] guarantees that both internal and external adversaries cannot reconstruct the input signals while the objective signal is able to be tracked. The work in [23] extends the static privacy-preserving scheme based on a state decomposition method such that it can be applied to dynamic average consensus. However, there still

exist several issues to be solved. First, it is not reasonable to assume that the time derivatives of the dynamic input signals can be always accessed. Second, the existing algorithms cannot guarantee zero steady-state error for general input signals. Specifically, the static input signals are required in [22] and some prescribed initialization conditions are required in [23] to achieve zero steady-state error.

To overcome the aforementioned issues, we aim to consider both privacy and robustness in the study of DAC problems. First, a privacy-preserving DAC (PP-DAC) algorithm is proposed by introducing a random number perturbation mechanism. The proposed privacy-preserving scheme employs some carefully designed random signals to confuse the original time-varying reference signals so that the attackers cannot infer the real reference signals by eavesdropping on communication channels. The carefully designed random signals play a key role in achieving accurate objective tracking since the impacts of the additional random signals can be finally eliminated from the viewpoint of the whole network. Furthermore, some different scenarios for the PP-DAC algorithm are discussed. It is concluded that the privacy of each agent can be preserved as long as at least one of its neighbors refuses to collude with the attackers. In addition, some numerical examples are provided to validate the effectiveness of the proposed algorithm.

Notation: Let $\mathcal{G}(\mathcal{V},\mathcal{E})$ denote a connected undirected graph composed of N nodes. The node set and edge set are represented as $\mathcal{V}=\{v_1,v_2,\ldots,v_N\}$ and $\mathcal{E}=\mathcal{V}\times\mathcal{V}$ respectively. Let $\mathcal{N}_i=\{v_j\in\mathcal{V}:(v_i,v_j)\in\mathcal{E}\}$ denote the set of neighbors of node i and the number of node i's neighbors can be denoted as $N_i=|\mathcal{N}_i|$. The graph Laplacian associated with the adjacency matrix A is defined by $L=(l_{ij})\in\mathbb{R}^{N\times N}$, where $l_{ij}=-a_{ij}, i\neq j$ and $l_{ii}=\sum_{j=1,j\neq i}^{N}a_{ij}$. Note that L is a symmetric positive semidefinite matrix, whose eigenvalues can be denoted as $0=\lambda_1\leq\lambda_2\leq\cdots\leq\lambda_N$ in an ascending order. Let $\mathbf{1}_n$ denote an n-dimensional vector of all ones and the p-norm of a vector x is denoted as $\|x\|_p$, where $p\in[1,\infty]$.

II. Problem Formulation and Preliminaries

Consider a connected network composed of N autonomous agents with each agent i having a time-varying reference signal $\phi_i(t)$. The DAC problem aims to develop a distributed control law to track the average value of multiple time-varying reference signals by using only local interaction. That is, the objective signal that needs to be tracked can be denoted by

$$\bar{\phi}(t)=\frac{1}{N}\sum_{i=1}^{N}\phi_i(t), \tag{1}$$

where $\phi(t)=(\phi_1,\ldots,\phi_N(t))^T$. Note that the reference signal $\phi_i(t)$ can be position, attitude, power consumption and other interested physical quantities that mainly depend on practical application scenarios. For simplicity, we here assume that the reference signal $\phi_i(t)$ is a scalar, which can be extended to multi-dimensional cases by the incorporation of Kronecker product.

Assumption 1: For each agent $i\in\{1,\ldots,N\}$, $\phi_i(t)$ and $\dot{\phi}_i(t)$ are both bounded, i.e., there exist positive constants φ and ϱ such that

$$\begin{aligned}&\sup_{t\in[t_0,\infty)}||\phi(t)||_\infty\leq\varphi<\infty,\\&\sup_{t\in[t_0,\infty)}||\dot{\phi}(t)||_\infty\leq\varrho<\infty,\end{aligned} \tag{2}$$

where $\dot{\phi}(t)=[\dot{\phi}_1(t),\ldots,\dot{\phi}_N(t)]^T$ is the time derivative of the reference signal $\phi(t)$.

Remark 1: Note that the reference signal is always limited by mechanical or electrical properties in practice, which implies that the reference signal and its time derivative are always bounded. Also, the upper boundedness of the time derivative implies that the time-varying reference signal does not change too rapidly since the accurate tracking needs more time to overcome communication and computation delays.

To track the objective signal (1), a robust DAC algorithm is proposed in [24] as follows

$$\dot{z}_i(t)=-\gamma z_i(t)-\alpha\sum_{j\in\mathcal{N}_i}\operatorname{sgn}\{x_i(t)-x_j(t)\}, \tag{3a}$$

$$x_i(t)=z_i(t)+\phi_i(t), \tag{3b}$$

where $x_i(t)$, $z_i(t)$, $\phi_i(t)$ represent the estimator state, the internal state and the time-varying reference signal, respectively. The parameter α is the control gain, and $\gamma>0$ is the design parameter.

Lemma 1 [24]: For a connected undirected network, under Assumption 1, the DAC algorithm (3) guarantees that all estimates $x_i(t)$ exponentially converge to the objective signal (1) with any initial condition of $z_i(t)$ when the control gain α is chosen such that

$$\alpha\geq\frac{2\sqrt{2N}(\varrho+\gamma\varphi)+1}{\sqrt{\lambda_2}}. \tag{4}$$

Remark 2: We here consider a simple average case even though a more general case called dynamic weighted average consensus (DWAC) is considered in [24]. That is, the result in [24] will degenerate to Lemma 1 if all the weights in DWAC are set as 1.

III. Main Results

A. Privacy-Preserving Scheme via Random Number Perturbation

In the previous section, the DAC algorithm assumes that the information interaction between agents is direct, which implies that the malicious attackers (inside or outside the network) can obtain or infer the sensitive information (e.g., the local time-varying reference signals) of agents using the observer-based methods in [23]. To protect agents' sensitive information from potential leakage while achieving an agreement via neighboring interaction, we aim to propose a lightweight privacy-preserving scheme for the DAC algorithm by introducing a random number perturbation mechanism.

The privacy-preserving DAC (PP-DAC) algorithm is proposed as follows

$$\dot{z}_i(t)=-\gamma z_i(t)-\alpha\sum_{j\in\mathcal{N}_i}\operatorname{sgn}\{\hat{x}_i(t)-\hat{x}_j(t)\}, \tag{5a}$$

$$\hat{x}_i(t)=z_i(t)+\hat{\phi}_i(t), \tag{5b}$$

Algorithm 1 The Execution Process of the PP-DAC Algorithm

1: **Initialize:**
Each agent i generates N_i random numbers $\left\{\theta_i^{i_1}, \ldots, \theta_i^{i_{N_i}}\right\}$, where $N_i = |\mathcal{N}_i|$ is the total number of its neighbors.
Agent i transmits a random number to its each neighbor respectively. For example, $\theta_i^{i_1}$ is sent to agent i's neighbor i_1.
Agent i collects the random numbers $\left\{\theta_j^i, j \in \mathcal{N}_i\right\}$ received from its neighbors.
2: **repeat**
3: Each agent i computes the perturbed reference signal

$$\hat{\phi}_i(t) = \phi_i(t) + \sum_{j\in\mathcal{N}_i} \theta_i^j - \sum_{j\in\mathcal{N}_i} \theta_j^i$$

based on its own generated random numbers and the received random numbers from its neighbors.
4: The algorithms (5a)-(5b) are executed.
5: The iteration time is updated.
6: **until** stop condition is satisfied

$$\hat{\phi}_i(t) = \phi_i(t) + \sum_{j\in\mathcal{N}_i} \theta_i^j - \sum_{j\in\mathcal{N}_i} \theta_j^i, \tag{5c}$$

where θ_i^j denotes the random number generated by agent i and will be transmitted to neighbor j, and θ_j^i denotes the random number received from neighbor j in agent i. $\hat{x}_i(t)$ and $\hat{\phi}_i(t)$ are the estimator state and the reference signal perturbed by the random number.

To execute the PP-DAC algorithm (5), each agent first generates a set of random numbers whose amount is equal to the number of its neighbors and then transmits one random number to each neighbor. After each agent receives the random numbers from its neighbors, it begins to compute the perturbed reference signal which is composed of its real reference signal, its own random number set and the set of the received random numbers. Once the computation of the perturbed reference signal is finished in each agent, the estimator state will be computed and then transmitted to its neighbors. To describe the random number perturbation mechanism clearly, the following Algorithm 1 is provided to show the execution process.

Note that the computation of the perturbed reference signal is carefully designed such that the additional random number perturbation has no direct impact on the final tracking accuracy. Specifically, the combination of each agent's own random numbers and its neighbors' random numbers plays a key role in eliminating the impact of additional random numbers from the viewpoint of the whole network. It is worth emphasizing that the additional communication cost is trivial because the random number exchange between agents only happens in the initialization period and it is a one-time operation. Next, we show that the PP-DAC algorithm has no direct impact on the final tracking accuracy.

Theorem 1: For a connected undirected network, given Assumption 1 and control gain α satisfying (4), the proposed PP-DAC algorithm (5) guarantees that the objective signal (1) can be tracked accurately, i.e., $\lim_{t\to\infty} \hat{x}_i(t) - \bar{\phi}(t) = 0$.

Proof: Based on Lemma 1, all estimator states $x_i(t), i \in \{1, \ldots, N\}$ converge to the objective signal $\bar{\phi}(t)$ in finite time, which implies that $\lim_{t\to\infty} x_i(t) = \frac{1}{N}\sum_{i=1}^N \phi_i(t)$. Thus, it follows that the convergence result of the algorithm (5) can be denoted by

$$\lim_{t\to\infty} \hat{x}_i(t) = \frac{1}{N}\sum_{i=1}^N \hat{\phi}_i(t). \tag{6}$$

According to (5c), we have

$$\frac{1}{N}\sum_{i=1}^N \hat{\phi}_i(t) = \frac{1}{N}\sum_{i=1}^N \phi_i(t) + \frac{1}{N}\sum_{i=1}^N \sum_{j\in\mathcal{N}_i} \theta_i^j - \frac{1}{N}\sum_{i=1}^N \sum_{j\in\mathcal{N}_i} \theta_j^i. \tag{7}$$

Since the network topology is undirected, it follows that

$$\sum_{i=1}^N \sum_{j\in\mathcal{N}_i} \theta_i^j = \sum_{i=1}^N \sum_{j\in\mathcal{N}_i} \theta_j^i. \tag{8}$$

Thus, we can derive

$$\frac{1}{N}\sum_{i=1}^N \hat{\phi}_i(t) = \frac{1}{N}\sum_{i=1}^N \phi_i(t), \tag{9}$$

which implies that

$$\lim_{t\to\infty} \hat{x}_i(t) = \frac{1}{N}\sum_{i=1}^N \hat{\phi}_i(t) = \frac{1}{N}\sum_{i=1}^N \phi_i(t). \tag{10}$$

The proof is completed. ■

Remark 3: Note that the key point is that the total sum of the perturbed reference signals remains equal to that of the real reference signals, which implies that each agent is able to track the accurate average signal of all time-varying reference signals once all agents reach an agreement. Therefore, the use of the virtual reference signal perturbed by additional random numbers not only hides the real reference signal but does not compromise the final convergence accuracy even if the attackers might infer the virtual reference signal using the observer-based methods.

Remark 4: It is worth emphasizing that the random number perturbation mechanism including random number generation and random number distribution has to run again once the network topology is changed. If not, the invariant property (the sum of the generated random numbers is equal to that of the received random numbers) in (8) will be destroyed, which implies that the final convergence point is not the objective signal (1). Regarding the risk of information leakage in the period of random number distribution, an effective solution is to employ a traditional cryptography scheme in the communication process. Since the distribution of random numbers is only a one-time operation, the computation cost of the cryptography scheme is trivial and negligible.

Remark 5: For the real-time communication issue of the PP-DAC algorithm (5), some sampled control methods including periodic sampling [11] and event-triggered sampling [12], [25] can be applied to schedule the interaction between agents so that the communication frequency can be reduced.

B. Privacy Analysis of the PP-DAC Algorithm

Since the additional random numbers are introduced to perturb the real reference signals, the attackers cannot infer the exact value of the real reference signal even if they obtain the exchanged information between agents by eavesdropping communication channels. In this sense, the sensitive information of individual agents in a network is preserved. However, the validity of the proposed PP-DAC algorithm depends on the degree of cooperation between the target agent and its neighbors. Next, we derive a key security condition as follows.

Corollary 1: The proposed PP-DAC algorithm (5) guarantees that each agent $i, i \in \{1, \ldots, N\}$ is able to preserve its privacy while interacting with its neighbors unless all its neighbors collude with each other to infer its sensitive information.

Proof: Assume that agent k is curious about the reference signal of its neighboring agent i and obtains the perturbed reference signal $\hat{\phi}_i(t)$ using an observer-based method presented in [23]. If agent i has only one neighbor k, the privacy of i cannot be preserved since its real reference signal can be inferred easily as follows

$$\phi_i(t) = \hat{\phi}_i(t) - \theta_k^i + \theta_i^k, \tag{11}$$

since agent k knows both θ_k^i and θ_i^k.

In another scenario, agent i has other neighboring agents besides agent k, then the PP-DAC algorithm does not work when all the neighbors of agent i are willing to collude with each other to infer the reference signal of agent i. In other words, the privacy of agent i cannot be preserved when all its neighbors are willing to share their generated and received random numbers with agent k. In this case, the additional random number items $\sum_{j\in\mathcal{N}_i} \theta_i^j$ and $\sum_{j\in\mathcal{N}_i} \theta_j^i$ can be computed by agent k. Then the real reference signal $\phi_i(t)$ can be inferred as follows

$$\phi_i(t) = \hat{\phi}_i(t) - \sum_{j\in\mathcal{N}_i} \theta_i^j + \sum_{j\in\mathcal{N}_i} \theta_j^i. \tag{12}$$

In contrast, if agent k fails to collude with all of agent i's neighbors, agent k will not obtain the full knowledge of random numbers θ_i^j and θ_j^i $(j \in \mathcal{N}_i)$. As a result, the privacy of the target agent i can be preserved. The proof is completed. ∎

In a word, the privacy of the target agent can be preserved unless all of its neighbors are willing to collude with each other to attack the target agent. Also, if the malicious agent does not have prior knowledge about the network topology, the target agent can preserve its privacy because the malicious agent fails to collect the random numbers of all neighbors of the target agent and thus cannot compute and infer the real reference signal of the target agent.

Remark 6: Compared with the previous work in [24], the novelty of this brief is concluded as follows. First, a random number perturbation mechanism is introduced in the proposed PP-DAC algorithm (5) and the detailed execution process is provided in Algorithm 1. In algorithm (5), some carefully designed random numbers are employed to perturb the original reference signal so that the real reference signal cannot be inferred by eavesdropping on communication channels. Moreover, it is proved that the carefully designed random numbers have no impact on the final convergence accuracy, which implies that the privacy of each agent can be preserved while achieving accurate objective tracking. In addition, the security condition of the PP-DAC algorithm is provided. The analysis of different scenarios verifies that the noncooperation of the target agent's neighbors plays a key role in protecting the target agent's privacy.

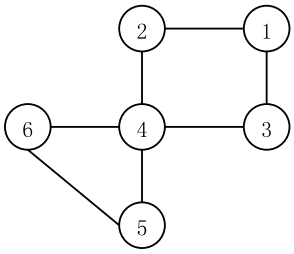

Fig. 1. The network topology with 6 nodes.

TABLE I
THE RANDOM NUMBERS GENERATED IN THE INITIALIZATION PERIOD

Nodes	1	2	3	4	5	6
1		0.02	1.03	-6.19		
2	5.22			1.35		
3	8.83				1.12	
4	-7.77	-0.72	-4.26		0.72	-0.31
5			2.04	3.24		3.88
6				5.77	-3.35	

IV. SIMULATION

In this section, for the sake of simplicity and length limit, some simulation results instead of practical examples are provided to validate the effectiveness of the proposed algorithm. For a practical example, one can refer to the work [23]. Consider an undirected network composed of 6 nodes given in Fig. 1. For each agent i, the time-varying reference signal $\phi_i(t)$ is selected as

$$\phi_i(t) = \begin{cases} \left(\frac{i-1}{2} - 7\right)\sin\left[w_i t + \left(\frac{2i}{N} - 1\right)\pi\right], & \forall i \in \{1, 2, 3\}, \\ \left(\frac{i-1}{2} - 7\right)\cos\left[w_i t + \left(\frac{2i}{N} - 1\right)\pi\right], & \forall i \in \{4, 5, 6\}, \end{cases}$$

where $w_i = \frac{i+1}{4}$. The initial value of each agent's internal state $z_i(t)$ is randomly generated within the range of $[0, 1]$. The design parameter and the control gain are set as $\gamma = 0.12$ and $\alpha = 5.5$ according to Lemma 1.

For the PP-DAC algorithm (5), each agent generates its own random numbers as shown in Table I, and then transmits a random number to its each neighbor. Note that the random number specified by the ith line and the jth column in Table I

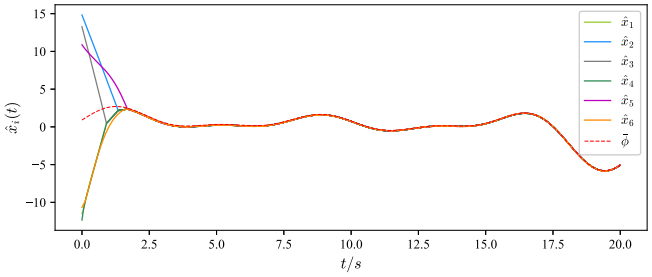

Fig. 2. The evolution of the estimator state of the PP-DAC (5).

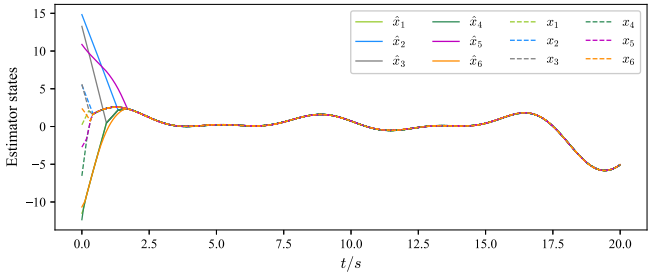

Fig. 3. The comparison of the estimator states between the PP-DAC (5) and the DAC (3).

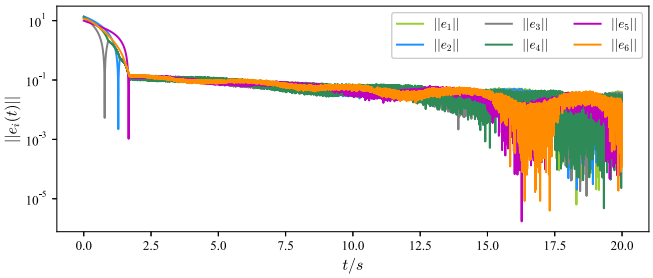

Fig. 4. The evolution of the steady-state error of the PP-DAC (5).

denotes that the random number is generated by node i and is transmitted to its neighboring node j. The evolution of the estimator state $x_i(t)$ is shown in Fig. 2, from which we can see that all state estimates asymptotically convergence to the objective signal $\bar{\phi}(t)$ denoted by a dashed orange line. The comparison of the estimator states between the PP-DAC algorithm (5) and the DAC algorithm (3) are shown in Fig. 3, from which we can see that the perturbed reference signal has no direct impact on the final convergence even though the estimator states might be perturbed in the initial period. The evolution of the steady-state error is shown in Fig. 4, where the error is nonzero level, which is due to the chatting effect of the discontinuous signum function.

V. Conclusion

This brief proposed a PP-DAC algorithm by introducing a random number perturbation mechanism. The proposed PP-DAC algorithm is able to achieve accurate objective tracking while preserving the privacy of sensitive information of individual agents in a network. Future works will extend the results to the case of general directed topologies in the study of DAC problems.

References

[1] R. Olfati-Saber and J. S. Shamma, "Consensus filters for sensor networks and distributed sensor fusion," in *Proc. 44th IEEE Conf. Decis. Control*, 2005, pp. 6698–6703.
[2] R. Aragues, J. Cortes, and C. Sagues, "Distributed consensus algorithms for merging feature-based maps with limited communication," *Robot. Auton. Syst.*, vol. 59, nos. 3–4, pp. 163–180, 2011.
[3] P. Yang, R. A. Freeman, and K. M. Lynch, "Multi-agent coordination by decentralized estimation and control," *IEEE Trans. Autom. Control*, vol. 53, no. 11, pp. 2480–2496, Dec. 2008.
[4] A. Nedić, A. Olshevsky, and W. Shi, "Achieving geometric convergence for distributed optimization over time-varying graphs," *SIAM J. Optim.*, vol. 27, no. 4, pp. 2597–2633, 2017.
[5] D. P. Spanos, R. Olfati-Saber, and R. M. Murray, "Dynamic consensus on mobile networks," in *Proc. IFAC World Congr.*, 2005, pp. 1–6.
[6] R. A. Freeman, P. Yang, and K. M. Lynch, "Stability and convergence properties of dynamic average consensus estimators," in *Proc. 45th IEEE Conf. Decis. Control*, 2006, pp. 338–343.
[7] H. Bai, R. A. Freeman, and K. M. Lynch, "Robust dynamic average consensus of time-varying inputs," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, 2010, pp. 3104–3109.
[8] F. Chen, Y. Cao, and W. Ren, "Distributed average tracking of multiple time-varying reference signals with bounded derivatives," *IEEE Trans. Autom. Control*, vol. 57, no. 12, pp. 3169–3174, Dec. 2012.
[9] S. Nosrati, M. Shafiee, and M. B. Menhaj, "Dynamic average consensus via nonlinear protocols," *Automatica*, vol. 48, no. 9, pp. 2262–2270, 2012.
[10] J. George and R. A. Freeman, "Robust dynamic average consensus algorithms," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4615–4622, Nov. 2019.
[11] E. Montijano, J. I. Montijano, C. Sagüés, and S. Martínez, "Robust discrete time dynamic average consensus," *Automatica*, vol. 50, no. 12, pp. 3131–3138, 2014.
[12] J. George, X. Yi, and T. Yang, "Distributed robust dynamic average consensus with dynamic event-triggered communication," in *Proc. IEEE Conf. Decis. Control (CDC)*, 2018, pp. 434–439.
[13] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.
[14] L. Gao, S. Deng, and W. Ren, "Differentially private consensus with an event-triggered mechanism," *IEEE Trans. Control Netw. Syst.*, vol. 6, no. 1, pp. 60–71, Mar. 2019.
[15] L. Gao, S. Deng, W. Ren, and C. Hu, "Differentially private consensus with quantized communication," *IEEE Trans. Cybern.*, vol. 51, no. 8, pp. 4075–4088, Aug. 2021.
[16] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.
[17] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, Nov. 2019.
[18] T. Yin, Y. Lv, and W. Yu, "Accurate privacy preserving average consensus," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 4, pp. 690–694, Apr. 2020.
[19] 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.
[20] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.
[21] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan, "Privacy-preserving average consensus: Privacy analysis and algorithm design," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 1, pp. 127–138, Mar. 2019.
[22] S. S. Kia, J. Cortés, and S. Martinez, "Dynamic average consensus under limited control authority and privacy requirements," *Int. J. Robust Nonlinear Control*, vol. 25, no. 13, pp. 1941–1966, 2015.
[23] K. Zhang, Z. Li, Y. Wang, A. Louati, and J. Chen, "Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control," *Automatica*, vol. 139, May 2022, Art. no. 110182.
[24] K. Xu, L. Gao, F. Chen, C. Li, and Q. Xuan, "Robust finite-time dynamic average consensus with exponential convergence rates," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 7, pp. 2578–2582, Jul. 2021.
[25] S. Hu, X. Chen, J. Qiu, F. Zhao, X. Jiang, and Y. Du, "Dynamic event-triggered bipartite consensus of multiagent systems with estimator and cooperative-competitive interactions," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 7, pp. 3309–3313, Jul. 2022.