Automatica 139 (2022) 110182

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control☆

Kaixiang Zhang [a], Zhaojian Li [a,*], Yongqiang Wang [b], Ali Louati [c], Jian Chen [d]

[a] Department of Mechanical Engineering, Michigan State University, East Lansing, MI 48824, USA
[b] Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA
[c] Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[d] State Key Laboratory of Industrial Control Technology, School of Mechanical Engineering, Zhejiang University, Hangzhou 310027, China

ARTICLE INFO

Article history:
Received 9 September 2020
Received in revised form 13 September 2021
Accepted 17 December 2021
Available online 19 February 2022

Keywords:
Dynamic average consensus
Privacy preservation
Non-holonomic mobile robots

ABSTRACT

Dynamic average consensus is a decentralized control/estimation framework where a group of agents cooperatively track the average of local time-varying reference signals. In this paper, we develop a novel state decomposition-based privacy preservation scheme to protect the privacy of agents when sharing information with neighboring agents. Specifically, we first show that an external eavesdropper can successfully wiretap the reference signals of all agents in a conventional dynamic average consensus algorithm. To protect privacy against the eavesdropper, a state decomposition scheme is developed where the original state of each agent is decomposed into two sub-states: one succeeds the role of the original state in inter-node interactions, while the other sub-state only communicates with the first one and is invisible to other neighboring agents. Rigorous analyses are performed to show that (1) the proposed privacy scheme preserves the convergence of the average consensus; and (2) the privacy of the agents is protected such that an eavesdropper cannot discover the private reference signals with guaranteed accuracy. The developed privacy-preserving dynamic average consensus framework is then applied to the formation control of multiple non-holonomic mobile robots, in which the efficacy of the scheme is demonstrated. Numerical simulation is provided to illustrate the effectiveness of the proposed approach.

1. Introduction

Average consensus has been extensively studied in recent years. It underpins many advantages of distributed systems and is emerging as an effective tool for diverse applications, including sensor fusion (Aragues et al., 2012; Olfati-Saber & Shamma, 2005), distributed resource allocation (Kia, 2017), and multi-agent coordination (Montijano et al., 2016; Porfiri et al., 2007). Based on the type of signals to be averaged, average consensus algorithms can be categorized as static (Olfati-Saber et al., 2007; Ren & Beard, 2008; Ren & Cao, 2010) or dynamic (Bai et al., 2010; Chen et al., 2012, 2015; Freeman et al., 2006; Spanos et al., 2005; Zhu & Martínez, 2010). In static average consensus agents seek to reach agreement on the average of initial agent states, whereas the dynamic average consensus is to design a distributed update law such that all agents can track the average of locally available time-varying reference signals. As dynamic average consensus has many emerging applications, such as economic dispatch for a power generating network (Cherukuri & Cortés, 2016), it will be the focus of this paper.

So far, different approaches have been proposed to address the dynamic average consensus problems. The initial work (Spanos et al., 2005) designs a consensus algorithm that can track the average of reference signals with steady states. Based on input-to-state stability property, a proportional–integral (PI) algorithm is proposed in Freeman et al. (2006) to achieve consensus for slowly time-varying and static reference signals. The PI algorithm is further generalized in Bai et al. (2010) and can converge with zero steady-state error if the Laplace transform of reference signals has a common monic denominator polynomial. Moreover, nonsmooth algorithms are developed in Chen et al. (2012, 2015) to accomplish finite-time consensus convergence.

☆ This research was supported by National Science Foundation, USA under award numbers 2045436 and 2030411. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Claudio Altafini under the direction of Editor Christos G. Cassandras.

* Corresponding author.
E-mail addresses: zhangk64@msu.edu (K. Zhang), lizhaoj1@egr.msu.edu (Z. Li), yongqiw@clemson.edu (Y. Wang), a.louati@psau.edu.sa (A. Louati), jchen@zju.edu.cn (J. Chen).

https://doi.org/10.1016/j.automatica.2022.110182
0005-1098/

In the aforementioned dynamic average consensus methods, each agent needs to share the explicit state value with its neighboring agents, which can breach the privacy of participating agents as the state values typically contain privacy-sensitive information such as its local reference signals. For example, an eavesdropper can wiretap the communication channel and infer privacy-sensitive information based on the exchanged signals. When dynamic average consensus is adopted in some specific areas, such as smart grid and intelligent transportation, the disclosure of the privacy-sensitive information may induce safety risk and economic loss (Dötzer, 2005). For example, multiple power generators in the smart grid can exploit the dynamic average consensus to estimate the mismatch in load satisfaction as discussed in Cherukuri and Cortés (2016). The evolving power generated by each generator is used as local reference information in consensus scheme and had to be kept secret since the individual power generation information is sensitive in energy bidding (Fang et al., 2012). Considering the aforementioned issues and growing awareness of security, it is an urgent need to protect the agents' privacy in dynamic average consensus. So far the privacy preservation schemes have been mainly focused on static average consensus while results on the privacy of dynamic average consensus are very sparse. For example, studies in Altafini (2020), He et al. (2020), Huang et al. (2012), Mo and Murray (2017), Nozari et al. (2017), Rezazadeh and Kia (2019) use carefully designed perturbation signals to obfuscate the true state information. One commonly adopted technique is differential privacy (He et al., 2020; Huang et al., 2012; Nozari et al., 2017), which injects uncorrelated noise for state obfuscation but cannot ensure exact consensus convergence. Another idea is to exploit cryptography to improve the resilience of static average consensus algorithms to privacy attacks (Freris & Patrinos, 2016; Hadjicostis & Dominguez-Garcia, 2020; Ruan et al., 2019). In our prior work (Wang, 2019), a state decomposition method is developed for static average consensus, which can guarantee the privacy of all participating agents and is light-weight in calculation. In this work, we extend the state decomposition technique to dynamic average consensus. Note that as dynamic average consensus involves time-varying reference signals, the privacy design in static average consensus cannot be directly applied (Kia et al., 2019; Nozari et al., 2017). The privacy design and analysis herein rely upon algebraic graph theory and Lyapunov-based control theory, which are more challenging as compared to those in Wang (2019).

In this paper, we first illustrate the necessity of privacy protection by designing an attack model where an external eavesdropper can wiretap the reference signals when the agent states are updated following a conventional dynamic average consensus algorithm. We will then develop a state decomposition scheme to decompose the original state of each agent into two sub-states to achieve privacy preservation in dynamic average consensus. Specifically, one sub-state takes the role of the original state to interact with neighboring agents, while the other sub-state is invisible to the outside world and only exchanges information with the first sub-state. To ensure that the consensus algorithm with state decomposition retains the similar average consensus results as the conventional method, the reference signals of the two sub-states are randomly selected from the set of bounded real numbers with their mean equal to the reference signals of the original state. We rigorously show that the proposed state decomposition scheme can protect the private reference signals from being inferred by the external eavesdropper. In addition, a case study on formation control of non-holonomic mobile robots is presented, which shows that the developed approach can be integrated with the tracking controller to accomplish privacy-preserving distributed control. Simulation results are given to validate the performance of the proposed scheme.

2. Preliminaries

2.1. Dynamic average consensus

We first review the dynamic average consensus problem. Consider n agents where each has a time-varying reference $r_i(t) \in \mathbb{R}^m$, $i = 1, 2, \ldots, n$, satisfying the following dynamics:

$$\dot{r}_i(t) = f_i(t). \tag{1}$$

In (1) $f_i(t) \in \mathbb{R}^m$ is the derivative of the reference signal. Each agent i has access to $r_i(t), f_i(t)$ as well as information from a subset of the other agents. This subset is referred to as the neighborhood of agent i and denoted by $\mathcal{N}_i$. A graph $\mathcal{G} \triangleq \{\mathcal{V}, \mathcal{E}\}$ is used to describe the network topology between the agents, where $\mathcal{V} \triangleq \{1, 2, \ldots, n\}$ is the node set and $\mathcal{E} \triangleq \{(i, j) | i \in \mathcal{N}_j, j = 1, 2, \ldots, n\}$ is the edge set. We consider undirected graph where $j \in \mathcal{N}_i$ implies $i \in \mathcal{N}_j$. A graph is connected if and only if there is a path from any node to any other node. The adjacency matrix $A \triangleq [a_{ij}] \in \mathbb{R}^{n\times n}$ of $\mathcal{G}$ is defined as follows: $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$; $a_{ij} = 0$ otherwise. The degree of agent i is $d_i \triangleq \sum_{j=1}^n a_{ij}$, and the degree matrix is given by $D \triangleq \text{diag}(d_1, \ldots, d_n) \in \mathbb{R}^{n\times n}$. The Laplacian matrix of $\mathcal{G}$ is then defined as $L \triangleq D - A \in \mathbb{R}^{n\times n}$.

In addition, each agent i keeps an internal state $x_i(t) \in \mathbb{R}^m$, $i \in \mathcal{V}$, and the objective of the dynamic average consensus is to design a distributed algorithm, such that all agents will finally track the average of the n time-varying reference signals, i.e., $\|x_i(t) - \frac{1}{n}\sum_{j=1}^n r_j(t)\| \to 0$ as $t \to \infty$. Assuming that the graph is undirected and connected, and the signals $r_i(t)$ and $f_i(t)$ are bounded, the following algorithm can be exploited to achieve the dynamic average consensus (Spanos et al., 2005):

$$\begin{aligned} &\dot{x}_i(t) = f_i(t) + \kappa \textstyle\sum_{j=1}^n a_{ij}\left(x_j(t) - x_i(t)\right), \\ &x_i(0) = r_i(0), \quad \forall i \in \mathcal{V}, \end{aligned} \tag{2}$$

where $\kappa \in \mathbb{R}$ is a positive constant. Using a time-domain analysis, Kia et al. (2019) shows that if each input signal $f_i(t)$, $i \in \mathcal{V}$, is bounded, all the agents implementing algorithm (2) over a connected graph are input-to-state stable and the tracking errors are ultimately bounded. Moreover, the convergence rate to the error bound is no worse than $\kappa\lambda_2(L)$, where $\lambda_2(L) \in \mathbb{R}$ is the second smallest eigenvalue of the Laplacian matrix L.

2.2. Privacy definition

As can be seen from (2), the conventional dynamic average consensus algorithm involves the exchange of states among neighboring agents, which can leak privacy-sensitive information such as the local reference signals. In this paper, we consider an eavesdropping attacker who knows the network topology and can wiretap communication channels to access exchanged information. Specifically, we consider the case where the eavesdropper is interested in obtaining the reference signals $r_i(t)$ and $f_i(t)$ from the agents. We next introduce the considered privacy definition as follows.

Definition 1. Let $I(t)$ be the set of information accessible to an eavesdropper having access to all shared messages in the network where the reference signals are $\{r_i(t), f_i(t)\}_{i\in\mathcal{V}}$. After adding arbitrary bounded perturbations to the reference signals of an agent p, i.e., replacing $r_p(t)$ and $f_p(t)$ by $\bar{r}_p(t) = r_p(t) + \epsilon_p(t)$ and $\bar{f}_p = f_p(t) + \delta_p(t)$, respectively, with perturbations $\epsilon_p(t)$ and $\delta_p(t) \in \mathbb{R}^m$, if there always exist $\left\{\bar{r}_i(t), \bar{f}_i(t)\right\}_{i\in\mathcal{V}\setminus\{p\}}$ from the remaining agents such that under the dynamic average consensus mechanism, the set of information $\bar{I}(t)$ accessible to the eavesdropper is the same as $I(t)$, then the privacy of the reference signals $r_p(t)$ and $f_p(t)$ from agent p is preserved.

Several privacy definitions have been utilized in the security community, such as differential privacy, mutual information, and semantic security. Differential privacy injects independent noise to obfuscate a private value, which will inevitably compromise algorithmic accuracy. Mutual information relies on explicit statistical models of source data and side information (Sankar et al., 2013) which, however, is not generally available in the context of dynamic average consensus. Semantic security requires "nothing is learned" by the adversary from outputs, which intrinsically inhibits any meaningful data utility and can resist arbitrary side information (Dwork & Roth, 2014; Lu & Zhu, 2020). In our problem, the eavesdropper has access to all exchanged information that is non-encrypted and necessary for the agents to achieve consensus utility. Thus, semantic security is too restrictive and not applicable to our problem. On the other hand, the considered privacy is defined by virtue of indistinguishability. More precisely, Definition 1 implies that the privacy of each agent is preserved as the available information to the adversary, which is an aggregated output, can correspond to infinitely many realizations of reference signals. This definition is essentially similar to the l-diversity (Machanavajjhala et al., 2007) which has been widely adopted in formal privacy analysis on attribute privacy of tabular datasets and has recently been extended to define privacy in the data release of linear dynamic networks (Lu & Zhu, 2020). l-diversity requires that there are at least l different values for sensitive attributes, and a greater diversity indicates greater indistinguishability. In our problem, the reference signals can be viewed as the sensitive attributes. Definition 1 requires that there exist infinite sets of reference signals that can generate the same accessible information to the adversary, and the difference of the reference signals from the same agent in these sets can be arbitrary bounded values. Such diversity notion is an extension of l-diversity, which makes the adversary unable to find a unique value or even estimate a rough range of the private parameters. Different from differential privacy and mutual information, our privacy notion does not require independent noise injection or statistical model for the multiple agent system. Compared with semantic security, our privacy definition cannot resist arbitrary side information and is weaker than the "nothing is learned" notion.

3. Privacy attack model

We now show that the dynamic consensus algorithm (2) is not privacy preserving, that is, the external eavesdropper can successfully obtain the reference signals $r_i(t)$ and $f_i(t)$ when agents follow the consensus algorithm in (2).

We consider that the eavesdropper has access to the network topology and the exchanged information between agents (based on Eq. (2)). Therefore, the available information to the eavesdropper is $I_{con}(t) \triangleq \{A, \kappa, x_i(t)\}_{i\in\mathcal{V}}$. The eavesdropper's target is to use $I_{con}(t)$ to infer the reference signals $r_i(t)$ and $f_i(t)$. In particular, let $\hat{x}_i(t) \in \mathbb{R}^m$, $\hat{r}_i(t) \in \mathbb{R}^m$, and $\hat{f}_i(t) \in \mathbb{R}^m$ be the eavesdropper's estimates of $x_i(t)$, $r_i(t)$, and $f_i(t)$, respectively. An observer based attack model can be designed to estimate $r_i(t)$ and $f_i(t)$ as follows:

$$\begin{aligned}
\dot{\hat{x}}_i(t) &= \hat{f}_i(t) + \kappa\textstyle\sum_{j=1}^n a_{ij}\left(x_j(t) - x_i(t)\right) + k_1\tilde{x}_i(t),\\
\dot{\hat{r}}_i(t) &= k_2\left(x_i(t) - z_i(t) - \hat{r}_i(t)\right) + \hat{f}_i(t),\\
\hat{f}_i(t) &= k_3 x_i(t) + \hat{f}_i'(t),
\end{aligned} \tag{3}$$

where k_1, k_2, k_3, $k_4 \in \mathbb{R}$ are positive constants to be designed, $\tilde{x}_i(t) \triangleq x_i(t) - \hat{x}_i(t) \in \mathbb{R}^m$ is the estimation error, $\hat{f}_i'(t) \in \mathbb{R}^m$ is an auxiliary variable, and $z_i(t) \in \mathbb{R}^m$ is the local filter. $\hat{f}_i'(t)$ and $z_i(t)$ are updated by

$$\begin{aligned}
\dot{\hat{f}}_i'(t) &= -k_3\left(\hat{f}_i(t) + \kappa\textstyle\sum_{j=1}^n a_{ij}\left(x_j(t) - x_i(t)\right)\right) + k_4\tilde{x}_i(t),\\
\dot{z}_i(t) &= \kappa\textstyle\sum_{j=1}^n a_{ij}\left(x_j(t) - x_i(t)\right), \quad z_i(0) = 0.
\end{aligned} \tag{4}$$

Let $\tilde{r}_i(t) \triangleq r_i(t) - \hat{r}_i(t)$, $\tilde{f}_i(t) \triangleq f_i(t) - \hat{f}_i(t) \in \mathbb{R}^m$ be the reference estimation errors. Then, from (1)–(4), it follows that

$$\begin{aligned}
\dot{\tilde{x}}_i(t) &= \tilde{f}_i(t) - k_1\tilde{x}_i(t),\\
\dot{\tilde{r}}_i(t) &= \tilde{f}_i(t) - k_2\tilde{r}_i(t),\\
\dot{\tilde{f}}_i(t) &= \dot{f}_i(t) - k_3\tilde{f}_i(t) - k_4\tilde{x}_i(t).
\end{aligned} \tag{5}$$

The observer based attack model in (3) is designed via an iterative procedure. The auxiliary variable $\hat{f}_i'(t)$ and local filter $z_i(t)$ are introduced to shape the time derivative of $\tilde{x}_i(t)$, $\tilde{r}_i(t)$, and $\tilde{f}_i(t)$ into the desired form presented in (5). This desired form is derived via Lyapunov-based techniques and will be used to facilitate the stability analysis of the following theorem.

Theorem 1. *When the algorithm in (2) is utilized to achieve dynamic average consensus, the external eavesdropper can infer the reference signals $r_i(t)$ and $f_i(t)$ by using the observer in (3). More precisely, assuming that the signals $r_i(t)$, $f_i(t)$, and $\dot{f}_i(t)$ are bounded, i.e., $r_i(t)$, $f_i(t)$, $\dot{f}_i(t) \in \mathcal{L}_\infty$, then*

1. *The attacker using (3) is guaranteed to obtain the private reference information in the sense that the estimation errors $\tilde{r}_i(t)$ and $\tilde{f}_i(t)$ are uniformly ultimately bounded (UUB).*
2. *If $\dot{f}_i(t)$ is in the $\mathcal{L}_2$-space, the estimation errors $\tilde{r}_i(t)$ and $\tilde{f}_i(t)$ converge to zero asymptotically.*

Proof. See Appendix A. □

Remark 1. The design of the observer in (3) is to illustrate that the consensus algorithm in (2) is vulnerable to privacy attacks. Various techniques can be exploited to construct the attack model, and it is not the focus of this paper. In the following, we will present a privacy scheme and show that the approach can provide privacy protection against the external eavesdropper no matter what attack model is used.

4. Privacy preservation via state decomposition

Building upon our prior work (Wang, 2019), in this section, we extend the state decomposition scheme to dynamic average consensus. Note that here we aim at protecting privacy against *any* eavesdropping scheme (including the example shown in Section 3). More specifically, the state decomposition scheme decomposes the state and reference signals $\{x_i(t), r_i(t), f_i(t)\}$ of each agent into two sub-sets $\left\{x_i^\alpha(t), r_i^\alpha(t), f_i^\alpha(t)\right\}$ and $\left\{x_i^\beta(t), r_i^\beta(t), f_i^\beta(t)\right\}$. The initial values $r_i^\alpha(0)$ and $r_i^\beta(0)$ can be randomly chosen from the set of all bounded real numbers under the following constraint:

$$r_i^\alpha(0) + r_i^\beta(0) = 2r_i(0). \tag{6}$$

Furthermore, $f_i^\alpha(t)$ and $f_i^\beta(t)$ are bounded and chosen to satisfy:

$$f_i^\alpha(t) + f_i^\beta(t) = 2f_i(t). \tag{7}$$

From (6) and (7), it can be obtained that $r_i^\alpha(t) + r_i^\beta(t) = 2r_i(t)$, which implies $\frac{1}{2n}\sum_{j=1}^n\left(r_j^\alpha(t) + r_j^\beta(t)\right) = \frac{1}{n}\sum_{j=1}^n r_j(t)$, i.e., the average consensus value remains the same before and after the state decomposition. Moreover, in the decomposition mechanism, the sub-state $x_i^\alpha(t)$ takes the role of the original state $x_i(t)$ in inter-agent interactions and is the only state value from agent i that is shared with its neighbors. The other sub-state $x_i^\beta(t)$ involves in the distributed updates by (and only by) exchanging information with $x_i^\alpha(t)$ internal to agent i. Therefore, $x_i^\beta(t)$ will affect the evolution of $x_i^\alpha(t)$, but its existence is invisible to the neighbors of agent i and hence the eavesdropper, indicating that the available information for the eavesdropper changes to $I_{dec} \triangleq$

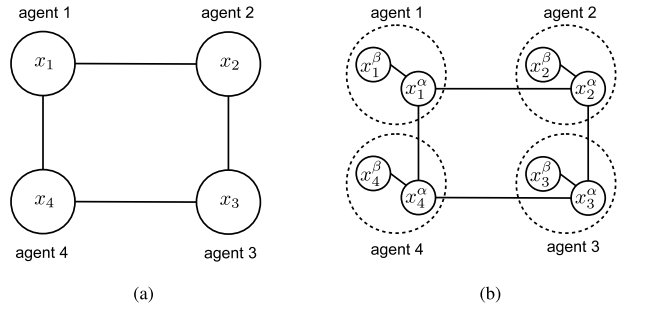


Fig. 1. Illustration of state decomposition: (a) Before decomposition. (b) After decomposition.

$\left\{A, \kappa, x_i^\alpha(t)\right\}_{i\in\mathcal{V}}$. An example is given in Fig. 1 to illustrate the state decomposition of a network with four agents.

Under the decomposition mechanism, the conventional average consensus algorithm in (2) becomes

$$\begin{aligned}
\dot{x}_i^\alpha(t) &= f_i^\alpha(t) + \kappa\textstyle\sum_{j=1}^n a_{ij}\left(x_j^\alpha(t) - x_i^\alpha(t)\right) + \kappa\left(x_i^\beta(t) - x_i^\alpha(t)\right),\\
\dot{x}_i^\beta(t) &= f_i^\beta(t) + \kappa\left(x_i^\alpha(t) - x_i^\beta(t)\right),\\
x_i^\alpha(0) &= r_i^\alpha(0), \quad x_i^\beta(0) = r_i^\beta(0), \quad \forall i\in\mathcal{V}.
\end{aligned} \tag{8}$$

In the following, we first show that all states $x_i^\alpha(t)$ and $x_i^\beta(t)$ will present similar convergence properties as in the conventional case (2). Then, we prove that the privacy of each agent is protected against an external eavesdropper.

Theorem 2. *Under the decomposition mechanism, all sub-states $x_i^\alpha(t)$ and $x_i^\beta(t)$ in (8) are input-to-state stable, and the tracking errors $x_i^\alpha(t) - \frac{1}{n}\sum_{j=1}^n r_j(t)$ and $x_i^\beta(t) - \frac{1}{n}\sum_{j=1}^n r_j(t)$ are ultimately bounded. Moreover, the convergence rate of the tracking errors is no worse than $\frac{\kappa}{2}\left(\lambda_2(L) + 2 - \sqrt{\lambda_2^2(L)+4}\right)$, where L is the Laplacian matrix of graph before state decomposition and $\lambda_2(L)\in\mathbb{R}$ is the second smallest eigenvalue of L.*

Proof. It is clear that the decomposition mechanism ensures that all sub-states also compose a connected graph. Based on the results in Kia et al. (2019), dynamic average consensus can still be achieved, i.e., all sub-states are input-to-state stable, and the convergence errors $x_i^\alpha(t) - \frac{1}{2n}\sum_{j=1}^n\left(r_j^\alpha(t) + r_j^\beta(t)\right)$ and $x_i^\beta(t) - \frac{1}{2n}\sum_{j=1}^n\left(r_j^\alpha(t) + r_j^\beta(t)\right)$ are ultimately bounded. It can be concluded from (6) and (7) that $\frac{1}{2n}\sum_{j=1}^n\left(r_j^\alpha(t) + r_j^\beta(t)\right) = \frac{1}{n}\sum_{j=1}^n r_j(t)$. Therefore, all sub-states $x_i^\alpha(t)$ and $x_i^\beta(t)$ in (8) retain the convergence to the neighborhood of the same average consensus value as the original states.

Let $L^{\alpha\beta}\in\mathbb{R}^{2n\times 2n}$ be the Laplacian matrix of the graph composed by all sub-states. By leveraging the results in Kia et al. (2019), it can be concluded that the convergence rate of the consensus algorithm is no worse than $\kappa\lambda_2(L^{\alpha\beta})$, where $\lambda_2(L^{\alpha\beta})\in\mathbb{R}$ is the second smallest eigenvalue of $L^{\alpha\beta}$. To complete the proof of Theorem 2, we next show that $\lambda_2(L^{\alpha\beta}) = \frac{1}{2}\left(\lambda_2(L) + 2 - \sqrt{\lambda_2^2(L)+4}\right)$. According to the decomposition mechanism, $L^{\alpha\beta}$ can be formulated as

$$L^{\alpha\beta} = \begin{bmatrix} L + I_n & -I_n \\ -I_n & I_n \end{bmatrix}, \tag{9}$$

with $I_n\in\mathbb{R}^{n\times n}$ being the n-dimensional identity matrix. Let $\lambda(L_{\alpha\beta})$, $\lambda(L)\in\mathbb{R}$ be the eigenvalue of $L_{\alpha\beta}$ and L, respectively. Based on (9) and the eigenvalue–eigenvector equation (Horn & Johnson, 2012), it can be derived that $\lambda(L_{\alpha\beta}) = \frac{1}{2}\left(\lambda(L) + 2 \pm \sqrt{\lambda^2(L)+4}\right)$, from which it follows that the second smallest eigenvalue of $L_{\alpha\beta}$, i.e., $\lambda_2(L^{\alpha\beta})$, is $\frac{1}{2}\left(\lambda_2(L) + 2 - \sqrt{\lambda_2^2(L)+4}\right)$, which completes the proof. □

Remark 2. Given a graph topology, the second smallest eigenvalue of Laplacian $\lambda_2(\cdot)$ is a measure of the convergence rate of consensus algorithms (Olfati-Saber et al., 2007). The convergence rate of the algorithm in (2) is no worse than $\kappa\lambda_2(L)$, and after state decomposition, this measure will decrease to $\frac{\kappa}{2}\left(\lambda_2(L) + 2 - \sqrt{\lambda_2^2(L)+4}\right)$ since the connectivity of the graph becomes weaker.

We next show that the decomposition scheme can protect the privacy of the agents against the external eavesdropper.

Theorem 3. *Under the decomposition mechanism, an external eavesdropper cannot infer the reference signals $r_p(t)$ and $f_p(t)$ of any agent p with guaranteed accuracy.*

Proof. Under the decomposition mechanism, the reference signals $\{r_i(t), f_i(t)\}$ of each agent are divided into two sub-sets $\left\{r_i^\alpha(t), f_i^\alpha(t)\right\}$ and $\left\{r_i^\beta(t), f_i^\beta(t)\right\}$, and the information accessible to the eavesdropper is $I_{dec}(t) \triangleq \left\{A, \kappa, x_i^\alpha(t)\right\}_{i\in\mathcal{V}}$. Let $\left\{\bar{r}_i(t), \bar{f}_i(t), \bar{r}_i^\alpha(t), \bar{f}_i^\alpha(t), \bar{r}_i^\beta(t), \bar{f}_i^\beta(t)\right\}$ and $\left\{\bar{x}_i^\alpha(t), \bar{x}_i^\beta(t)\right\}$ be another set of references and their corresponding sub-states, respectively. To show that the privacy of $r_p(t)$ and $f_p(t)$ can be protected against the eavesdropper, it suffices to show that under any bounded perturbations $\epsilon_p(t) = \epsilon_p(0) + \int_0^t \delta_p(\tau)d\tau$ that alter the reference signals to $\bar{r}_p(t) = r_p(t) + \epsilon_p(t)$ and $\bar{f}_p(t) = f_p(t) + \delta_p(t)$, there exists a new constructed set $\left\{\bar{r}_i^\alpha(t), \bar{f}_i^\alpha(t), \bar{r}_i^\beta(t), \bar{f}_i^\beta(t)\right\}_{i\in\mathcal{V}\setminus\{p\}}$ such that the information $\bar{I}_{dec}(t) \triangleq \left\{A, \kappa, \bar{x}_i^\alpha(t)\right\}_{i\in\mathcal{V}}$ accessible to the eavesdropper is exactly the same as the information $I(t)$ cumulated under $\left\{r_i^\alpha(t), f_i^\alpha(t), r_i^\beta(t), f_i^\beta(t)\right\}_{i\in\mathcal{V}}$. This is because the only information available to the eavesdropper is $I_{dec}(t)$, and if $I_{dec}(t)$ could be the outcome of any perturbed values of $r_p(t)$ and $f_p(t)$, then the eavesdropper has no way to even find a range for $r_p(t)$ and $f_p(t)$. Therefore, we only need to prove that for any $\bar{r}_p(t)\neq r_p(t)$ and $\bar{f}_p(t)\neq f_p(t)$, we can always find a set of signals $\left\{\bar{r}_i^\alpha(t), \bar{f}_i^\alpha(t), \bar{r}_i^\beta(t), \bar{f}_i^\beta(t)\right\}_{i\in\mathcal{V}\setminus\{p\}}$ such that $\bar{I}_{dec}(t) = I_{dec}(t)$ holds.

Let agent l be one of the neighbors of agent p. Next we show that given $\bar{r}_p(t)$ (i.e., $\bar{r}_p(0)$ and $\bar{f}_p(t)$), by suitably selecting the values of $\bar{r}_l(0)$, $\bar{r}_p^\alpha(0)$, $\bar{r}_p^\beta(0)$, $\bar{r}_l^\alpha(0)$, $\bar{r}_l^\beta(0)$, $\bar{f}_p^\alpha(t)$, $\bar{f}_p^\beta(t)$, $\bar{f}_l^\alpha(t)$, and $\bar{f}_l^\beta(t)$, $\bar{I}_{dec}(t) = I_{dec}(t)$ could hold under $\bar{r}_p(t)\neq r_p(t)$. Specifically, under the following conditions:

$$\begin{aligned}
&\bar{r}_l(0) = r_l(0) + r_p(0) - \bar{r}_p(0),\\
&\bar{r}_p^\alpha(0) = r_p^\alpha(0),\ \bar{r}_p^\beta(0) = 2\bar{r}_p(0) - r_p^\alpha(0),\\
&\bar{r}_l^\alpha(0) = r_l^\alpha(0),\ \bar{r}_l^\beta(0) = 2\bar{r}_l(0) - r_l^\alpha(0),\\
&\bar{r}_q(0) = r_q(0),\ \bar{r}_q^\alpha(0) = r_q^\alpha(0),\ \bar{r}_q^\beta(0) = r_q^\beta(0),\ \forall q\in\mathcal{V}\setminus\{p, l\},
\end{aligned} \tag{10}$$

and

$$\begin{aligned}
&\bar{f}_l(t) = f_l(t) + f_p(t) - \bar{f}_p(t),\\
&\bar{f}_p^\alpha(t) = f_p^\alpha(t) + 2\kappa\left(\bar{r}_p(t) - \bar{r}_p(t)\right),\ \bar{f}_p^\beta(t) = 2\bar{f}_p(t) - \bar{f}_p^\alpha(t),\\
&\bar{f}_l^\alpha(t) = f_l^\alpha(t) + 2\kappa\left(\bar{r}_p(t) - r_p(t)\right),\ \bar{f}_l^\beta(t) = 2\bar{f}_l(t) - \bar{f}_l^\alpha(t),\\
&\bar{f}_q(t) = f_q(t),\ \bar{f}_q^\alpha(t) = f_q^\alpha(t),\ \bar{f}_q^\beta(t) = f_q^\beta(t),\ \forall q\in\mathcal{V}\setminus\{p, l\},
\end{aligned} \tag{11}$$

and system dynamics

$$\begin{aligned}
&\dot{\bar{x}}_i^{\alpha}(t) = \bar{f}_i^{\alpha}(t) + \kappa \sum_{j=1}^{n} a_{ij}\left(\bar{x}_j^{\alpha}(t) - \bar{x}_i^{\alpha}(t)\right) + \kappa\left(\bar{x}_i^{\beta}(t) - \bar{x}_i^{\alpha}(t)\right),\\
&\dot{\bar{x}}_i^{\beta}(t) = \bar{f}_i^{\beta}(t) + \kappa\left(\bar{x}_i^{\alpha}(t) - \bar{x}_i^{\beta}(t)\right),\\
&\bar{x}_i^{\alpha}(0) = \bar{r}_i^{\alpha}(0), \quad \bar{x}_i^{\beta}(0) = \bar{r}_i^{\beta}(0), \quad \forall i \in \mathcal{V},
\end{aligned} \tag{12}$$

the new sub-state $\bar{x}_i^{\alpha}(t)$ will be the same as $x_i^{\alpha}(t)$, for all $i \in \mathcal{V}$, i.e., $\bar{I}_{dec}(t) = I_{dec}(t)$. Note that the first equations in both (10) and (11) are introduced to ensure that the average consensus value $\frac{1}{n}\sum_{j=1}^{n} \bar{r}_j(t)$ is the same as the original one $\frac{1}{n}\sum_{j=1}^{n} r_j(t)$. Now we prove that $\bar{I}_{dec}(t) = I_{dec}(t)$. First, from (6), (10), and the facts that $\bar{x}_i^{\alpha}(0) = \bar{r}_i^{\alpha}(0)$, $\bar{x}_i^{\beta}(0) = \bar{r}_i^{\beta}(0)$, $x_i^{\alpha}(0) = r_i^{\alpha}(0)$, $x_i^{\beta}(0) = r_i^{\beta}(0)$, $\forall i \in \mathcal{V}$, it can be obtained that

$$\begin{aligned}
&\bar{x}_p^{\alpha}(0) = x_p^{\alpha}(0), \bar{x}_p^{\beta}(0) = x_p^{\beta}(0) + 2\left(\bar{r}_p(0) - r_p(0)\right),\\
&\bar{x}_l^{\alpha}(0) = x_l^{\alpha}(0), \bar{x}_l^{\beta}(0) = x_l^{\beta}(0) + 2\left(r_p(0) - \bar{r}_p(0)\right),\\
&\bar{x}_q^{\alpha}(0) = x_q^{\alpha}(0), \bar{x}_q^{\beta}(0) = x_q^{\beta}(0), \forall q \in \mathcal{V} \setminus \{p, l\}.
\end{aligned} \tag{13}$$

Furthermore, based on (11) and (13), it can be verified that

$$\begin{aligned}
&\bar{x}_p^{\alpha}(t) = x_p^{\alpha}(t), \bar{x}_p^{\beta}(t) = x_p^{\beta}(t) + 2\left(\bar{r}_p(t) - r_p(t)\right),\\
&\bar{x}_l^{\alpha}(t) = x_l^{\alpha}(t), \bar{x}_l^{\beta}(t) = x_l^{\beta}(t) + 2\left(r_p(t) - \bar{r}_p(t)\right),\\
&\bar{x}_q^{\alpha}(t) = x_q^{\alpha}(t), \bar{x}_q^{\beta}(t) = x_q^{\beta}(t), \forall q \in \mathcal{V} \setminus \{p, l\},
\end{aligned} \tag{14}$$

is the solution to (12). It is obvious that the solution (14) satisfies $\forall i \in \mathcal{V}$, $\bar{x}_i^{\alpha}(t) = x_i^{\alpha}(t)$, and thus $\bar{I}_{dec}(t) = I_{dec}(t)$ holds under $\bar{r}_p(t) \neq r_p(t)$. The above analysis shows that no matter what attack model is used, the eavesdropper cannot infer $r_p(t)$ and $f_p(t)$ from $I_{dec}(t)$ with guaranteed accuracy. □

Remark 3. The proposed state decomposition scheme is a general privacy-preserving augmentation to dynamic average consensus algorithms. While the above analysis is based on the dynamic consensus algorithm in (2), the state decomposition framework can be integrated with other dynamic average consensus approaches (e.g., Bai et al., 2010; Chen et al., 2012, 2015; Freeman et al., 2006) to improve the resilience of original methods to privacy attacks.

Remark 4. Generally, the works (Altafini, 2020; Mo & Murray, 2017; Ruan et al., 2019; Wang, 2019) on privacy preservation in static average consensus have an assumption that the honest-but-curious adversary cannot have access to the entire neighborhood set of an agent. However, the considered dynamic average consensus aims at protecting privacy against the external eavesdropper, and it is not subjected to the invariant-state-sum relationship as shown in the static consensus case. Thus such an extra assumption is not needed anymore.

5. Application to formation control

In this section, the privacy-preserving dynamic average consensus is applied to the formation control of non-holonomic mobile robots under the adversarial environment with eavesdropping attackers.

5.1. Formation control objective

In particular, consider n networked non-holonomic mobile robots and n mobile moving targets in the motion plane. Each mobile robot i has access to its own position $s_i(t) \triangleq \left[s_{xi}(t), s_{yi}(t)\right]^T \in \mathbb{R}^2$ and can monitor the mobile target i's position $p_i(t) \triangleq \left[p_{xi}(t), p_{yi}(t)\right]^T \in \mathbb{R}^2$ and velocity $\dot{p}_i(t) = q_i(t) \triangleq \left[q_{xi}(t), q_{yi}(t)\right]^T \in \mathbb{R}^2$. $s_i(t)$, $p_i(t)$, and $q_i(t)$ are all expressed with respect to the inertial coordinate frame. Each mobile robot shares relevant information with its neighbors via wireless communication. We consider the case that the mobile robots and targets are operating in the adversarial environment with eavesdropping attackers. The objective of the networked mobile robots is to follow the set of mobile targets by spreading out in a pre-specified formation while preserving the privacy of mobile targets against the eavesdropper. Specifically, the formation control requires that by using the information received from the communication network, each mobile robot i is driven to a relative vector $b_i(t) \triangleq \left[b_{xi}(t), b_{yi}(t)\right]^T \in \mathbb{R}^2$ with respect to the time-varying geometric center of the mobile targets, i.e., $s_i(t) \to \frac{1}{n}\sum_{i=1}^{n} p_i(t) + b_i(t)$ as $t \to \infty$. Meanwhile, since each mobile robot can only monitor one mobile target, it needs to cooperate with its neighbors to compute the geometric center, which induces the risk of breaching the privacy of mobile targets. An external eavesdropper can use the leaked sensitive information, such as the position and/or velocity information, to maliciously track and attack the mobile targets. Therefore, it is important that the formation control scheme can protect the privacy of mobile targets against the eavesdropping attacker, i.e., an external eavesdropper cannot identify the position and/or velocity of mobile targets based on the network information. An example scenario in which a team of mobile robots tracks a group of mobile targets is depicted in Fig. 2.

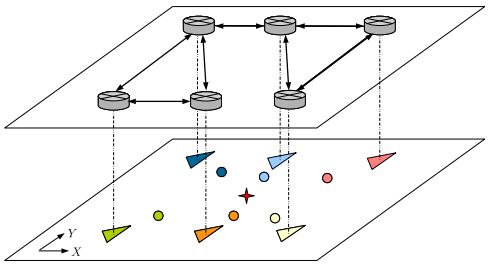


Fig. 2. Dynamic consensus based formation control. The triangles are the non-holonomic mobile robots; the circles are the mobile targets; and the cross is the center of the mobile targets.

5.2. Control design

As discussed in Kia et al. (2019) and Porfiri et al. (2007), the formation control problem in the aforementioned scenario can be addressed with a two-layer method. In the cyber layer, the privacy-preserving dynamic average consensus algorithm is used to estimate the geometric center of mobile targets in a distributed manner, while in the physical layer, the mobile robot i is actuated to follow the estimate of the geometric center with a desired relative bias $b_i(t)$. The implementation details are given now.

In the cyber layer, the state decomposition based dynamic average consensus algorithm presented in Section 4 is utilized for the calculation of the geometric center $\frac{1}{n}\sum_{i=1}^{n} p_i(t)$ and the privacy preservation of mobile targets. Specifically, let $c_i^{\alpha}(t) \triangleq \left[c_{xi}^{\alpha}(t), c_{yi}^{\alpha}(t)\right]^T \in \mathbb{R}^2$ and $c_i^{\beta}(t) \triangleq \left[c_{xi}^{\beta}(t), c_{yi}^{\beta}(t)\right]^T \in \mathbb{R}^2$ be two sub-sets of the geometric center estimates, which are updated by

$$\begin{aligned}
&\dot{c}_i^{\alpha}(t) = q_i^{\alpha}(t) + \kappa \sum_{j=1}^{n} a_{ij}\left(c_j^{\alpha}(t) - c_i^{\alpha}(t)\right) + \kappa\left(c_i^{\beta}(t) - c_i^{\alpha}(t)\right),\\
&\dot{c}_i^{\beta}(t) = q_i^{\beta}(t) + \kappa\left(c_i^{\alpha}(t) - c_i^{\beta}(t)\right),\\
&c_i^{\alpha}(0) = p_i^{\alpha}(0), \quad c_i^{\beta}(0) = p_i^{\beta}(0),
\end{aligned} \tag{15}$$

where $p_i^\alpha(0)$, $p_i^\beta(0)$, $q_i^\alpha(t)$, $q_i^\beta(t) \in \mathbb{R}^2$ are selected to satisfy

$$p_i^\alpha(0) + p_i^\beta(0) = 2p_i(0), \quad q_i^\alpha(t) + q_i^\beta(t) = 2q_i(t). \tag{16}$$

As shown in Theorems 2 and 3, $c_i^\alpha(t)$ will converge to the neighborhood of the geometric center $\frac{1}{n}\sum_{i=1}^n p_i(t)$, and the mobile targets' information cannot be identified by the external eavesdropper.

In the physical layer, the objective now is to design a tracking controller for non-holonomic mobile robot i to ensure that $s_i(t) \to c_i^\alpha(t) + b_i(t)$ as $t \to \infty$. The kinematic model of non-holonomic mobile robot i is described by

$$\dot{s}_{xi}(t) = v_i(t)\cos(\theta_i(t)), \quad \dot{s}_{yi}(t) = v_i(t)\sin(\theta_i(t)), \quad \dot{\theta}_i(t) = \omega_i(t), \tag{17}$$

where $\theta_i(t) \in \mathbb{R}$ is the heading angle expressed in the inertial coordinate frame, and $v_i(t)$, $\omega_i(t) \in \mathbb{R}$ are the linear and angular velocity, respectively. To facilitate the following development, the desired heading angle $\theta_{di}(t) \in \mathbb{R}$ and desired linear velocity $v_{di}(t) \in \mathbb{R}$ are constructed as

$$\theta_{di}(t) = \arctan\left(\frac{\dot{c}_{yi}^\alpha(t)}{\dot{c}_{xi}^\alpha(t)}\right), \quad v_{di}(t) = \sqrt{(\dot{c}_{xi}^\alpha(t))^2 + (\dot{c}_{yi}^\alpha(t))^2}, \tag{18}$$

which indicates that $\dot{c}_{xi}(t)$ and $\dot{c}_{yi}(t)$ can be rewritten as $\dot{c}_{xi}(t) = v_{di}(t)\cos(\theta_{di}(t))$, $\dot{c}_{yi}(t) = v_{di}(t)\sin(\theta_{di}(t))$. Based on coordinate transformation, the system errors are defined as

$$\begin{aligned} e_{xi}(t) &\triangleq \cos(\theta_i(t))(s_{xi}(t) - c_{xi}^\alpha(t) - b_{xi}(t)) \\ &\quad + \sin(\theta_i(t))(s_{yi}(t) - c_{yi}^\alpha(t) - b_{yi}(t)), \\ e_{yi}(t) &\triangleq -\sin(\theta_i(t))(s_{xi}(t) - c_{xi}^\alpha(t) - b_{xi}(t)) \\ &\quad + \cos(\theta_i(t))(s_{yi}(t) - c_{yi}^\alpha(t) - b_{yi}(t)), \\ e_{\theta i}(t) &\triangleq \theta_i(t) - \theta_{di}(t). \end{aligned} \tag{19}$$

It is clear that $s_i(t) \to c_i^\alpha(t) + b_i(t)$ as $\left[e_{xi}(t), e_{yi}(t), e_{\theta i}(t)\right] \to 0$. Note that the mobile robot is subjected to non-holonomic constraint, and thus in general time-varying auxiliary variables are needed to facilitate the controller design (Huang et al., 2013; Jiang & Nijmeijer, 1997; Wang et al., 2015). Considering the non-holonomic constraint, an auxiliary error $\bar{e}_{\theta i}(t) \in \mathbb{R}$ is defined as

$$\bar{e}_{\theta i}(t) \triangleq e_{\theta i}(t) - \rho_i(t), \tag{20}$$

where the time-varying signal $\rho_i(t) \in \mathbb{R}$ is given by

$$\rho_i(t) \triangleq \iota_0 \varpi_i(t)\tanh\left(\iota_1\sqrt{e_{xi}^2(t) + e_{yi}^2(t)}\right)\sin(\iota_2 t) \tag{21}$$

with $\varpi_i(t) \triangleq \exp\left(-\int_0^t |v_{di}(\tau)|d\tau\right) \in \mathbb{R}$ and ι_0, ι_1, $\iota_2 \in \mathbb{R}$ being positive constants. To achieve the formation control, the velocity inputs $v_i(t)$ and $\omega_i(t)$ are designed as

$$\begin{aligned} v_i(t) &= -\gamma_1\tanh(e_{xi}(t)) + \cos(e_{\theta i}(t))v_{di}(t), \\ \omega_i(t) &= -\gamma_2\tanh(\bar{e}_{\theta i}(t)) + \dot{\rho}_i(t) - \gamma_3\mathrm{sgn}(\bar{e}_{\theta i}(t)) \\ &\quad - \gamma_4\frac{\sin(e_{\theta i}(t)) - \sin(\rho_i(t))}{\bar{e}_{\theta i}(t)}v_{di}(t)e_{yi}(t), \end{aligned} \tag{22}$$

where γ_1, γ_2, γ_3, $\gamma_4 \in \mathbb{R}$ are positive control gains, and $\mathrm{sgn}(\cdot)$ is the standard signum function.

Theorem 4. *The controller designed in (22) ensures that the system errors $e_{xi}(t)$, $e_{yi}(t)$, and $e_{\theta i}(t)$, $i \in \mathcal{V}$, asymptotically converge to zero in the sense that*

$$\lim_{t\to\infty} e_{xi}(t), e_{yi}(t), e_{\theta i}(t) = 0. \tag{23}$$

Proof. See Appendix B. □

According to the definition of $e_{xi}(t)$, $e_{yi}(t)$, and $e_{\theta i}(t)$, it can be concluded that $s_i(t) \to c_i^\alpha(t) + b_i(t)$ as (23) holds. Since $c_i^\alpha(t)$ will converge to the neighborhood of the geometric center $\frac{1}{n}\sum_{i=1}^n p_i(t)$, the formation control task is accomplished.

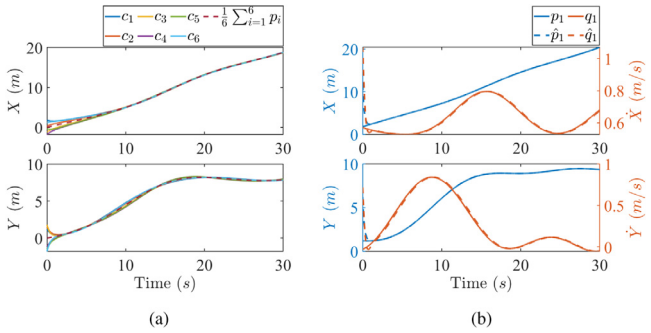


Fig. 3. Simulation results of conventional dynamic average consensus (2): (a) System state convergence. (b) Estimation of $p_1(t)$ and $q_1(t)$ with the eavesdropping scheme developed in Section 3.

6. Simulation results

In this section, simulation is conducted to demonstrate the performance of the developed approach. A team of six mobile robots are employed to follow a group of six mobile targets and maintain a rectangle formation. The network structure of the mobile robots is the same as the one shown in Fig. 2. The initial positions and velocities of mobile targets are as follows: $p_1(0) = \left[1.8, 1.2\right]^T$, $p_2(0) = \left[0.3, 1.5\right]^T$, $p_3(0) = \left[-1.2, 1.8\right]^T$, $p_4(0) = \left[-1.8, -1.2\right]^T$, $p_5(0) = \left[-0.3, -1.5\right]^T$, $p_6(0) = \left[1.2, -1.8\right]^T$, $q_1(t) = q_0(t) + \left[0.1\cos(0.2t), -0.2\cos(0.4t)\right]^T$, $q_3(t) = q_0(t) + \left[-0.2\cos(0.4t), 0.1\cos(0.2t)\right]^T$, $q_2(t) = \frac{q_1(t)+q_3(t)}{2}$, $q_4(t) = q_0(t) + \left[-0.1\cos(0.2t), 0.2\cos(0.4t)\right]^T$, $q_6(t) = q_0(t) + \left[0.2\cos(0.4t), -0.1\cos(0.2t)\right]^T$, $q_5(t) = \frac{q_4(t)+q_6(t)}{2}$, and

$$q_0(t) = (0.75 - 0.25\cos(0.24t))\begin{bmatrix}\cos(\frac{\pi}{9} + 0.5\sin(0.2t)) \\ \sin(\frac{\pi}{9} + 0.5\sin(0.2t))\end{bmatrix}.$$

Furthermore, the initial positions of the mobile robots are selected as $s_1(0) = \left[1.3, 5.2\right]^T$, $s_2(0) = \left[-3.6, 3.9\right]^T$, $s_3(0) = \left[-7.5, 2.6\right]^T$, $s_4(0) = \left[-4.8, -5.5\right]^T$, $s_5(0) = \left[-0.6, -5.35\right]^T$, and $s_6(0) = \left[5.2, -5.2\right]^T$. For the mobile robots, the desired relative positions to the geometric center of mobile targets are given by $b_1(0) = \left[4, 4\right]^T$, $b_2(0) = \left[0, 4\right]^T$, $b_3(0) = \left[-4, 4\right]^T$, $b_4(0) = \left[-4, -4\right]^T$, $b_5(0) = \left[0, -4\right]^T$, and $b_6(0) = \left[4, -4\right]^T$. In the following, we first evaluate the state decomposition based consensus algorithm and then test the formation controller designed in (22).

Suppose that an external eavesdropper is interested in obtaining the information of mobile target 1 and uses the eavesdropping scheme developed in Section 3 to infer $p_1(t)$ and $q_1(t)$. To better demonstrate the performance of the proposed consensus scheme, both the conventional algorithm in (2) and the developed privacy-preserving algorithm are used to estimate the geometric center of mobile targets. Fig. 3 shows the evolution of the network states as well as the eavesdropping states under the conventional algorithm (2). It can be seen that the eavesdropper can successfully infer $p_1(t)$ and $q_1(t)$ when the agents are updated with algorithm (2). The results under the privacy-preserving scheme (15) is illustrated in Fig. 4. It is clear that the proposed scheme can achieve dynamic average consensus while protecting the privacy of the mobile target.

As discussed in Section 5, the dynamic average consensus algorithm is used to estimate the geometric center of mobile targets, and then the mobile robots are driven according to (22) to

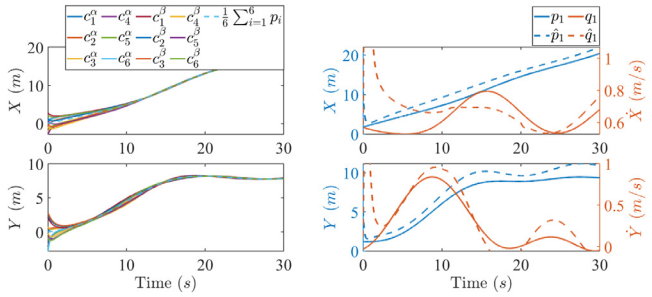


Fig. 4. Simulation results of privacy-preserving dynamic average consensus (15): (a) System state convergence. (b) Estimation of $p_1(t)$ and $q_1(t)$ with the eavesdropping scheme developed in Section 3.

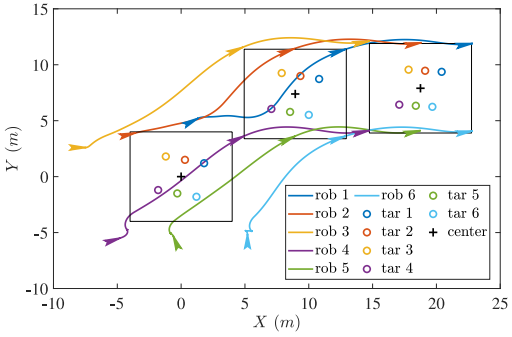


Fig. 5. Motion trajectories of all mobile robots.

achieve the formation task. Fig. 5 depicts the motion trajectories of all mobile robots, showing that all robots follow the geometric center by spreading out in a desired rectangle pattern.

7. Conclusion

This paper developed a state decomposition based privacy-preserving method for continuous-time dynamic average consensus. We showed that existing dynamic consensus algorithm is susceptible to eavesdropping attacks with a carefully designed filter. We then rigorously proved that the state decomposition scheme can enable privacy preservation without affecting the consensus results. Furthermore, the proposed method was successfully applied to achieve formation control for non-holonomic mobile robots. Simulation results showed that by using the proposed method, the group of networked mobile robot can spread out in a pre-specified formation without disclosing private information.

Appendix A. Proof of Theorem 1

Proof. To prove the first claim, a non-negative Lyapunov function $V(t) \in \mathbb{R}$ is introduced, as follows:

$$V(t) \triangleq \frac{1}{2}k_4\tilde{x}_i^T(t)\tilde{x}_i(t) + \frac{1}{2}\tilde{r}_i^T(t)\tilde{r}_i(t) + \frac{1}{2}\tilde{f}_i^T(t)\tilde{f}_i(t), \tag{A.1}$$

from which it follows that $V(t)$ can be bounded by

$$\underline{\mu}y^T(t)y(t) \le V(t) \le \overline{\mu}y^T(t)y(t), \tag{A.2}$$

where $\underline{\mu} \triangleq \min\left\{\frac{1}{2}k_4, \frac{1}{2}\right\}$, $\overline{\mu} \triangleq \max\left\{\frac{1}{2}k_4, \frac{1}{2}\right\} \in \mathbb{R}$, and $y(t) \triangleq \left[\tilde{x}_i^T(t), \tilde{r}_i^T(t), \tilde{f}_i^T(t)\right]^T \in \mathbb{R}^{3m}$ is the augmented estimate vector. Taking the time derivative of (A.1) and substituting it in (5) yield $\dot{V}(t) = -k_1k_4\tilde{x}_i^T(t)\tilde{x}_i(t) - k_2\tilde{r}_i^T(t)\tilde{r}_i(t) - k_3\tilde{f}_i^T(t)\tilde{f}_i(t) + \tilde{r}_i^T(t)\dot{f}_i(t) + \tilde{f}_i^T(t)\dot{f}_i(t)$. According to Young's inequality, we have $\tilde{r}_i^T(t)\dot{f}_i(t) \le \frac{k_2}{2}\tilde{r}_i^T(t)\tilde{r}_i(t) + \frac{1}{2k_2}\dot{f}_i^T(t)\dot{f}_i(t)$ and $\tilde{f}_i^T(t)\dot{f}_i(t) \le \frac{k_3}{2}\tilde{f}_i^T(t)\tilde{f}_i(t) + \frac{1}{2k_3}\dot{f}_i^T(t)\dot{f}_i(t)$. Therefore, $\dot{V}(t)$ can be upper bounded by

$$\begin{aligned}\dot{V}(t) &\le -k_1k_4\tilde{x}_i^T(t)\tilde{x}_i(t) - \frac{k_2}{2}\tilde{r}_i^T(t)\tilde{r}_i(t)\\ &\quad - \left(\frac{k_3}{2} - \frac{1}{2k_2}\right)\tilde{f}_i^T(t)\tilde{f}_i(t) + \frac{1}{2k_3}\dot{f}_i^T(t)\dot{f}_i(t)\\ &\le -\mu y^T(t)y(t) + \varrho(t),\end{aligned} \tag{A.3}$$

where $\mu \triangleq \min\left\{k_1k_4, \frac{k_2}{2}, \frac{k_3}{2} - \frac{1}{2k_2}\right\} \in \mathbb{R}$ and $\varrho(t) \triangleq \frac{1}{2k_3}\dot{f}_i^T(t)\dot{f}_i(t) \in \mathbb{R}$. It is clear that μ is positive provided that k_2 and k_3 are chosen to satisfy $k_3 > \frac{1}{k_2}$. Since $\dot{f}_i(t) \in \mathcal{L}_\infty$, $\varrho(t)$ is bounded. By utilizing (A.2) and (A.3), Theorem 4.18 in Khalil (2002) can be invoked to show that $y(t)$, i.e., $\tilde{x}_i(t)$, $\tilde{r}_i(t)$ and $\tilde{f}_i(t)$, is UUB.

We now prove the second claim. Based on the assumption $\dot{f}_i(t) \in \mathcal{L}_2$, it can be obtained that there exists a bounded positive constant $\iota \in \mathbb{R}$ such that $\forall t \ge 0$, $\int_0^t \frac{1}{2k_3}\dot{f}_i^T(\tau)\dot{f}_i(\tau)d\tau \le \iota$. Let the non-negative function $W(t) \in \mathbb{R}$ be defined as

$$W(t) \triangleq V(t) + \iota - \int_0^t \frac{1}{2k_3}\dot{f}_i^T(\tau)\dot{f}_i(\tau)d\tau. \tag{A.4}$$

Taking the time derivative of (A.4) and utilizing (A.3), it can be concluded that

$$\begin{aligned}\dot{W}(t) &= -k_1k_4\tilde{x}_i^T(t)\tilde{x}_i(t) - \frac{k_2}{2}\tilde{r}_i^T(t)\tilde{r}_i(t) - \left(\frac{k_3}{2} - \frac{1}{2k_2}\right)\tilde{f}_i^T(t)\tilde{f}_i(t)\\ &\le 0.\end{aligned} \tag{A.5}$$

According to (A.4) and (A.5), it follows that $W(t) \in \mathcal{L}_\infty$, i.e., $\tilde{x}_i(t)$, $\tilde{r}_i(t)$, $\tilde{f}_i(t) \in \mathcal{L}_\infty \bigcap \mathcal{L}_2$. The boundedness of $r_i(t)$, $f_i(t)$, $\dot{f}_i(t)$ and the expression in (3) can be used to conclude that $\dot{\tilde{x}}_i(t)$, $\dot{\tilde{r}}_i(t)$, $\dot{\tilde{f}}_i(t) \in \mathcal{L}_\infty$. As $\tilde{x}_i(t)$, $\tilde{r}_i(t)$, $\tilde{f}_i(t) \in \mathcal{L}_\infty \bigcap \mathcal{L}_2$ and $\dot{\tilde{x}}_i(t)$, $\dot{\tilde{r}}_i(t)$, $\dot{\tilde{f}}_i(t) \in \mathcal{L}_\infty$, Barbalat's lemma (Khalil, 2002) can be used to conclude that $\tilde{x}_i(t)$, $\tilde{r}_i(t)$ and $\tilde{f}_i(t)$ converge to zero asymptotically. □

Appendix B. Proof of Theorem 4

Proof. To prove Theorem 4, the Lyapunov function $V_i(t) \in \mathbb{R}$, $i = 1, 2, \ldots, n$ is defined as

$$V_i(t) \triangleq \frac{1}{2}\gamma_4\left(e_{xi}^2 + e_{yi}^2\right) + \frac{1}{2}\bar{e}_{\theta i}^2. \tag{B.1}$$

Based on (17), (19)–(22) and the facts that $\dot{c}_{xi}(t) = v_{di}(t)\cos(\theta_{di}(t))$, $\dot{c}_{yi}(t) = v_{di}(t)\sin(\theta_{di}(t))$, the closed-loop error dynamics can be derived, as follows:

$$\begin{aligned}\dot{e}_{xi}(t) &= -\gamma_1\tanh(e_{xi}(t)) + \omega_i(t)e_{yi}(t),\\ \dot{e}_{yi}(t) &= -\omega_i(t)e_{xi}(t) + \sin(e_{\theta i}(t))v_{di}(t),\\ \dot{\bar{e}}_{\theta i}(t) &= -\gamma_2\tanh(\bar{e}_{\theta i}(t)) - \dot{\theta}_{di}(t) - \gamma_3\mathrm{sgn}(\bar{e}_{\theta i}(t))\\ &\quad - \gamma_4\frac{\sin(e_{\theta i}(t)) - \sin(\rho_i(t))}{\bar{e}_{\theta i}(t)}v_{di}(t)e_{yi}(t).\end{aligned} \tag{B.2}$$

After taking the time derivative of (B.1) and substituting (B.2) into the derivative, it can be determined that

$$\begin{aligned}\dot{V}_i(t) &= -\gamma_1\gamma_4e_{xi}(t)\tanh(e_{xi}(t)) - \gamma_2\bar{e}_{\theta i}(t)\tanh(\bar{e}_{\theta i}(t))\\ &\quad + \gamma_4v_{di}(t)e_{yi}(t)\sin(\rho_i(t)) - \bar{e}_{\theta i}(t)\left(\gamma_3\mathrm{sgn}(\bar{e}_{\theta i}(t)) + \dot{\theta}_{di}(t)\right).\end{aligned} \tag{B.3}$$

If γ_3 is selected sufficiently large to satisfy $\gamma_3 > \sup_{t\in[0,\infty)} |\dot{\theta}_{di}(t)|$, then $\dot{V}_i(t)$ is upper bounded by

$$\begin{aligned}\dot{V}_i(t) &\leq -W_i(t) + \gamma_4|e_{yi}(t)||v_{di}(t)\sin(\rho_i(t))| \\ &\leq \sqrt{2\gamma_4 V_i(t)}|v_{di}(t)\sin(\rho_i(t))|,\end{aligned} \tag{B.4}$$

where $W_i(t) \triangleq \gamma_1\gamma_4 e_{xi}(t)\tanh(e_{xi}(t)) + \gamma_2\bar{e}_{\theta i}(t)\tanh(\bar{e}_{\theta i}(t)) \in \mathbb{R}$ is a non-negative function. From (21), it can be found that $0 \leq \varpi_i(t) \leq 1$, $\dot{\varpi}_i(t) = -|v_{di}(t)|\varpi_i(t)$, and $|\rho_i(t)| \leq \iota_0\varpi_i(t)$. Using these facts and integrating $|v_{di}(t)\sin(\rho_i(t))|$, it can be concluded that

$$\begin{aligned}&\int_0^t |v_{di}(\tau)\sin(\rho_i(\tau))|d\tau \\ &\leq \int_0^t |v_{di}(\tau)||\rho_i(\tau)|d\tau \leq \iota_0\int_0^t |v_{di}(\tau)|\varpi_i(\tau)d\tau \\ &\leq \iota_0\int_0^t -\dot{\varpi}_i(\tau)d\tau \leq \iota_0(\varpi(0) - \varpi(t)) \leq \iota_0.\end{aligned} \tag{B.5}$$

Eq. (B.4) indicates that $\frac{d\sqrt{V_i(t)}}{dt} \leq \sqrt{\frac{\gamma_4}{2}}|v_{di}(t)\sin(\rho_i(t))|$, and then based on (B.5), it can be deduced that $\sqrt{V_i(t)} \in \mathcal{L}_\infty$, i.e., $V_i(t) \in \mathcal{L}_\infty$. Furthermore, it can be inferred from (22), (B.1), and (B.2) that $e_{xi}(t)$, $e_{yi}(t)$, $\bar{e}_{\theta i}(t)$, $v_i(t)$, $\omega_i(t)$, $\dot{e}_{xi}(t)$, $\dot{e}_{yi}(t)$, $\dot{\bar{e}}_{\theta i}(t) \in \mathcal{L}_\infty$. Taking the time derivative of $W_i(t)$ and using the above boundedness analysis, it can be derived that $\dot{W}_i(t) \in \mathcal{L}_\infty$, which is a sufficient condition for $W_i(t)$ being uniformly continuous. Using (B.4), (B.5), and $V_i(t) \in \mathcal{L}_\infty$, it can be concluded that $\int_0^t W_i(\tau)d\tau \in \mathcal{L}_\infty$. Based on $\int_0^t W_i(\tau)d\tau \in \mathcal{L}_\infty$ and the uniform continuity of $W_i(t)$, Barbalat's lemma (Khalil, 2002) can be exploited to obtain that $\lim_{t\to\infty} W_i(t) = 0$, i.e., $\lim_{t\to\infty} e_{xi}(t), \bar{e}_{\theta i}(t) = 0$. With the aid of the extended Barbalat's lemma (Dixon et al., 2000), it can be further deduced that $\lim_{t\to\infty} e_{yi}(t) = 0$. According to (20) and (21), it is clear that $\lim_{t\to\infty} e_{xi}(t), e_{yi}(t), \bar{e}_{\theta i}(t) = 0$ implies $\lim_{t\to\infty} e_{xi}(t), e_{yi}(t), e_{\theta i}(t) = 0$, which completes the proof. □

References

Altafini, C. (2020). A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics. *Automatica*, *122*, Article 109253.

Aragues, R., Cortés, J., & Sagüés, C. (2012). Distributed consensus on robot networks for dynamically merging feature-based maps. *IEEE Transactions on Robotics*, *28*, 840–854.

Bai, H., Freeman, R. A., & Lynch, K. M. (2010). Robust dynamic average consensus of time-varying inputs. In *Proceedings of the IEEE conference on decision and control* (pp. 3104–3109). Atlanta, GA, USA.

Chen, F., Cao, Y., & Ren, W. (2012). Distributed average tracking of multiple time-varying reference signals with bounded derivatives. *IEEE Transactions on Automatic Control*, *57*, 3169–3174.

Chen, F., Ren, W., Lan, W., & Chen, G. (2015). Distributed average tracking for reference signals with bounded accelerations. *IEEE Transactions on Automatic Control*, *60*, 863–869.

Cherukuri, A., & Cortés, J. (2016). Initialization-free distributed coordination for economic dispatch under varying loads and generator commitment. *Automatica*, *74*, 183–193.

Dixon, W. E., Dawson, D. M., Zergeroglu, E., & Behal, A. (2000). *Nonlinear control of wheeled mobile robots*. Springer.

Dötzer, F. (2005). Privacy issues in vehicular ad hoc networks. In *Proceedings of international workshop on privacy enhancing technologies* (pp. 197–209). Cavtat, Croatia.

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, *9*, 211–407.

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid — The new and improved power grid: A survey. *IEEE Communications Surveys and Tutorials*, *14*, 944–980.

Freeman, R. A., Yang, P., & Lynch, K. M. (2006). Stability and convergence properties of dynamic average consensus estimators. In *Proceedings of the IEEE conference on decision and control* (pp. 338–343). San Diego, CA, USA.

Freris, N. M., & Patrinos, P. (2016). Distributed computing over encrypted data. In *Proceedings of the 54th annual allerton conference on communication, control, and computing* (pp. 1116–1122). Monticello, IL, USA.

Hadjicostis, C. N., & Dominguez-Garcia, A. D. (2020). Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus. *IEEE Transactions on Automatic Control*, *65*, 3887–3894.

He, J., Cai, L., & Guan, X. (2020). Differential private noise adding mechanism and its application on consensus algorithm. *IEEE Transactions on Signal Processing*, *68*, 4069–4082.

Horn, R. A., & Johnson, C. R. (2012). *Matrix analysis*. Cambridge University Press.

Huang, Z., Mitra, S., & Dullerud, G. (2012). Differentially private iterative synchronous consensus. In *Proceedings of the ACM workshop on privacy in the electronic society* (pp. 81–90). New York, NY, USA.

Huang, J., Wen, C., Wang, W., & Jiang, Z. -P. (2013). Adaptive stabilization and tracking control of a nonholonomic mobile robot with input saturation and disturbance. *Systems & Control Letters*, *62*, 234–241.

Jiang, Z. -P., & Nijmeijer, H. (1997). Tracking control of mobile robots: A case study in backstepping. *Automatica*, *33*, 1393–1399.

Khalil, H. K. (2002). *Nonlinear systems*. Upper Saddle River, NJ: Prentice-Hall.

Kia, S. S. (2017). Distributed optimal in-network resource allocation algorithm design via a control theoretic approach. *Systems & Control Letters*, *107*, 49–57.

Kia, S. S., Van Scoy, B., Cortés, J., Freeman, R. A., Lynch, K. M., & Martínez, S. (2019). Tutorial on dynamic average consensus: The problem, its applications, and the algorithms. *IEEE Control Systems Magazine*, *39*, 40–72.

Lu, Y., & Zhu, M. (2020). On privacy preserving data release of linear dynamic networks. *Automatica*, *115*, Article 108839.

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*, 3–14.

Mo, Y., & Murray, R. M. (2017). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, *62*, 753–765.

Montijano, E., Cristofalo, E., Zhou, D., Schwager, M., & Sagüés, C. (2016). Vision-based distributed formation control without an external positioning system. *IEEE Transactions on Robotics*, *32*, 339–351.

Nozari, E., Tallapragada, P., & Cortés, J. (2017). Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design. *Automatica*, *81*, 221–231.

Olfati-Saber, R., Fax, J. A., & Murray, R. M. (2007). Consensus and cooperation in networked multi-agent systems. *Proceedings of the IEEE*, *95*, 215–233.

Olfati-Saber, R., & Shamma, J. S. (2005). Consensus filters for sensor networks and distributed sensor fusion. In *Proceedings of the IEEE conference on decision and control* (pp. 6698–6703). Seville, Spain.

Porfiri, M., Roberson, D. G., & Stilwell, D. J. (2007). Tracking and formation control of multiple autonomous agents: A two-level consensus approach. *Automatica*, *43*, 1318–1328.

Ren, W., & Beard, R. W. (2008). *Distributed consensus in multi-vehicle cooperative control*. London: Springer.

Ren, W., & Cao, Y. (2010). *Distributed coordination of multi-agent networks*. London: Springer.

Rezazadeh, N., & Kia, S. S. (2019). Privacy preservation in continuous-time average consensus algorithm via deterministic additive perturbation signals. arXiv preprint arXiv:1904.05286.

Ruan, M., Gao, H., & Wang, Y. (2019). Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, *64*, 4035–4049.

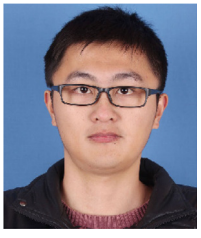
Sankar, L., Rajagopalan, S. R., & Poor, H. V. (2013). Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security*, *8*, 838–852.

Spanos, D. P., Olfati-Saber, R., & Murray, R. M. (2005). Dynamic consensus on mobile networks. In *Proceedings of the IFAC world congress* (pp. 1–6). Prague, Czech Republic.

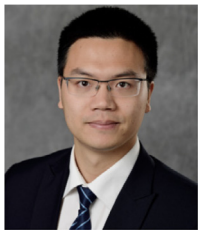
Wang, Y. (2019). Privacy-preserving average consensus via state decomposition. *IEEE Transactions on Automatic Control*, *64*, 4711–4716.

Wang, Y., Miao, Z., Zhong, H., & Pan, Q. (2015). Simultaneous stabilization and tracking of nonholonomic mobile robots: A Lyapunov-based approach. *IEEE Transactions on Control Systems Technology*, *23*, 1440–1450.

Zhu, M., & Martínez, S. (2010). Discrete-time dynamic average consensus. *Automatica*, *46*, 322–329.

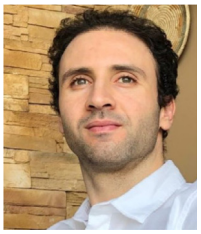


Kaixiang Zhang received the B.Eng. degree in automation from Xiamen University, Xiamen, China, in 2014, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2019. From 2017 to 2018, he was a visiting doctoral student with the National Institute for Research in Computer Science and Automation, Rennes, France. He currently holds a postdoctoral position with the Department of Mechanical Engineering at Michigan State University. His research interests include visual servoing, robotics, and nonlinear control.



Zhaojian Li received his B. Eng. degree from Nanjing University of Aeronautics and Astronautics in 2010. He obtained M.S. (2013) and Ph.D. (2015) in Aerospace Engineering (flight dynamics and control) at the University of Michigan, Ann Arbor. He is currently an Assistant Professor with the Department of Mechanical Engineering at Michigan State University. His research interests include learning-based control, nonlinear and complex systems, and robotics and automated vehicles. He is a recipient of NSF CAREER Award.

Yongqiang Wang was born in Shandong, China. He received the B.Sc. degree in electrical engineering and automation, the B.Sc. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, Shaanxi, China, in 2004, and the M.Sc. and Ph.D. degrees in control science and engineering from Tsinghua University, Beijing, China, in 2009. From 2007–2008, he was with the University of Duisburg–Essen, Germany, as a visiting student. He was a Project Scientist at the University of California, Santa Barbara before joining Clemson University, SC, USA, where he is currently an Associate Professor. His current research interests include decentralized control, optimization, and learning, with an emphasis on privacy. He currently serves as an associate editor for *IEEE Transactions on Automatic Control* and *IEEE Transactions on Control of Network Systems*.



Ali Louati received the B.Sc. and M.Sc. degrees in computer science with business from the University of Sfax, Tunisia in 2010 and 2013, respectively. He received a Ph.D. degree in computer science with business from the ISG, University of Tunis, Tunisia, in 2018. From 2014 until 2018, he served as a Research Assistant at both, IFMA, LIMOS, Clermont-Ferrand, France, and King Saud University, KSA. Currently, he is Assistant Professor at Prince Sattam Bin Abdulaziz University, KSA. He is a member of the SMART Laboratory at ISG, University of Tunis. He has contributed to several research projects in Tunisia, France, and KSA. His research interests include machine learning, artificial immune systems, data mining, optimization, and intelligent transportation systems.

Jian Chen received the B.Eng. and M.Eng. degrees from Zhejiang University, Hangzhou, China, in 1998 and 2001, respectively, and the Ph.D. degree in electrical engineering from Clemson University, Clemson, SC, USA, in 2005. He was a Research Fellow with the University of Michigan, Ann Arbor, MI, USA, from 2006 to 2008. In 2013, he joined the Department of Control Science and Engineering, Zhejiang University, where he is currently a Professor with the School of Mechanical Engineering, Zhejiang University. His research interests include modeling and control of fuel cell systems, vehicle control and intelligence, visual servo techniques, battery management systems, and nonlinear control.