Privacy-Preserving Dynamic Average Consensus via State Decomposition: Case Study on Multi-Robot Formation Control

Kaixiang Zhang, Zhaojian Li, Yongqiang Wang, and Jian Chen

Abstract—In this paper, the problem of privacy preservation in the continuous-time dynamic average consensus is addressed by using a state decomposition scheme. We first show that for a conventional dynamic average consensus algorithm, the external eavesdropper can successfully wiretap the reference signals of each local agent. Then, to provide privacy protection against the eavesdropper, a state decomposition scheme is proposed. The main idea of the proposed scheme is to decompose the original state of each agent into two sub-states. One of the two sub-states succeeds the role of the original state in inter-node interactions, while the other sub-state is invisible to other neighboring agents and only communicates with the first sub-state of the same agent. The new reference signals for the two sub-states can be constructed randomly under certain constraints, which ensures that the convergence properties of the consensus algorithm can be retained. Theoretical analysis shows that under the state decomposition scheme, the eavesdropper cannot discover the private reference signals of each agent with any guaranteed accuracy. Moreover, the proposed privacy-preserving consensus algorithm is successfully applied to solve a formation control problem for multiple nonholonomic mobile robots. Numerical simulation is provided to demonstrate the effectiveness of the proposed approach.

Index Terms—Dynamic average consensus, privacy preservation, nonholonomic mobile robots

I. INTRODUCTION

AVERAGEx consensus has been intensively studied in recent years, since it underpins significant functionalities of distributed systems and is emerging as an effective tool for diverse applications, including sensor fusion [1], [2], distributed resource allocation [3], and multi-agent coordination [4], [5]. However, in some scenarios involving sensitive information, the adoption of average consensus algorithms is impeded by concerns over the privacy preservation guarantees. Motivated by the demand for protecting sensitive information, this paper considers the privacy preservation issue in the dynamic average consensus using a state decomposition scheme.

Existing average consensus algorithms can be roughly categorized into static cases [6]–[8] and dynamic cases [9]–[14]. Specifically, based on local interacting information, the agents in static cases aim at reaching agreement on the average of initial agent states, while the dynamic average consensus is to design a distributed updated law such that all the agents can track the average of locally available time-varying reference signals. So far, different approaches have been proposed to address the dynamic average consensus problems. The initial work [10] 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 [11] to achieve consensus task for slowly time-varying and static reference signals. The PI algorithm is further generalized in [12] 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 [13], [14] to accomplish finite-time consensus convergence.

For conventional dynamic average consensus methods, each agent uses local reference signals to update its state and directly transmits the explicit state value to its neighboring agents. Disclosing the state information via this way induces potential privacy problems. The state values contain private information regarding local reference signals, and thus the disclosure of state information might breach the privacy of participating agents. Actually, if there exist eavesdroppers who want to steal information by wiretapping communication channels, exchanging agents’ explicit state values through the communication network is vulnerable. Considering the aforementioned issue and increasing reports on attack events, it is an urgent need to preserve information privacy in dynamic average consensus. By now, several privacy-preserving strategies have been investigated for the static average consensus. One interesting idea is to inject carefully-designed perturbation signals into the state values of the agents, which masks private information and can obfuscate eavesdroppers [15]–[17]. Another common idea is to rely on cryptography to improve the resilience of average consensus algorithms to privacy attacks [18]–[20]. Furthermore, a state decomposition method is developed in [21] for static average consensus, which can guarantee the privacy of all participating agents and is light-weight in calculation. Note that most of the existing privacy-preserving strategies [15]–[21] are proposed for static average consensus, and few results focus on the privacy issue of dynamic average consensus. The static and dynamic average consensus algorithms have diverse agreement objectives and exploit different protocols to update agents’ states. Therefore, the privacy preservation schemes for static average consensus...
cannot be directly applicable to the dynamic one.

In this paper, a state decomposition scheme is proposed for the continuous-time dynamic average consensus to avoid disclosing private reference signals. To illustrate the necessity of preserving the privacy, an attack model is given firstly to show that the external eavesdropper can swimmingly wiretap the reference signals when the agent states are updated with a conventional dynamic average consensus algorithm. Then, by leveraging recent work [2], the original state of each agent is decomposed into two sub-states to achieve the privacy preservation for dynamic average consensus. Specifically, one sub-state takes over the role of the original state to interact with the outside world and only exchanges information with the first sub-state in the same agent. To ensure the consensus algorithm with state decomposition retains the same convergence properties as the conventional method, the reference signals of the two sub-states are selected with their mean equals to the reference signals of the original state. The proposed state decomposition scheme can protect the private reference signals of each agent from tapping by the external eavesdropper. In addition, a case study on formation control for nonholonomic mobile robots is presented, showing 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 state decomposition scheme.

The remainder of this paper is organized as follows. Section II introduces a conventional dynamic average consensus algorithm, and a corresponding eavesdropping strategy is presented in Section III. The state decomposition scheme for privacy preservation is developed in Section IV. The proposed method is used in Section V to accomplish the formation control of nonholonomic mobile robots. Simulation results are provided in Section VI. Finally, the conclusion is given in Section VII.

II. PRELIMINARIES: DYNAMIC AVERAGE CONSENSUS

The dynamic average consensus problem is reviewed firstly. Suppose that there are $n$ agents with $x_i(t) \in \mathbb{R}^m$ being the state of agent $i$, $i = 1, 2, \ldots, n$, and $n$ time-varying reference signals $r_i(t) \in \mathbb{R}^m$, $i = 1, 2, \ldots, n$, satisfying the following dynamics $\dot{r}_i(t) = f_i(t)$. It is assumed that agent $i$ has access to $r_i(t), f_i(t)$, and at time $t > 0$ agent $i$ can obtain information from a subset of the other agents, called its neighbors and denoted by $\mathcal{N}_i(t)$. A graph $G(t) = \{V, E(t)\}$ is used to describe the network topology between the agents at time $t$, where $V = \{1, 2, \ldots, n\}$ is the node set and $E(t) = \{(i, j) | i \in \mathcal{N}_j(t), j = 1, 2, \ldots, n\}$ is the edge set. A graph is undirected if $j \in \mathcal{N}_i$ 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 $G$ is defined as follows: $a_{ij} = 1$ if $(i, j) \in E$; $a_{ij} = 0$ otherwise.

Assumption 1: The graph is undirected and connected.

Assumption 2: The signals $r_i(t), f_i(t)$, and $\dot{f}_i(t)$ are bounded.

The objective of the dynamic average consensus is to design a distributed algorithm for agent $i$ based on $r_i(t), f_i(t)$, and $x_j(t)$, $j \in \mathcal{N}_i(t)$, 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 $t \to \infty$. To achieve the dynamic average consensus, one of the commonly used updated laws is given by [10]

$$\begin{align*}
\dot{x}_i(t) &= f_i(t) + \kappa \sum_{j=1}^{n} a_{ij} (x_j(t) - x_i(t)), \\
x_i(0) &= r_i(0), \quad \forall i \in V,
\end{align*}$$

where $\kappa \in \mathbb{R}$ is a positive constant. Using a time-domain analysis, [2] shows that if each input signal $f_i(t), i = 1, 2, \ldots, n$, is bounded, all the agents implementing algorithm (1) over a connected graph are input-to-state stable and the tracking errors are ultimately bounded.

III. PRIVACY ATTACK MODEL

It can be found from (1) that each agent updates its state by using local reference signals, and hence exchanging state values via the communication network has a high risk to reveal the private information regarding reference signals. Suppose that an external eavesdropper is interested in obtaining the reference signals $r_i(t)$ and $f_i(t)$ of agent $i$. Specifically, the eavesdropper is an external attacker who knows the network topology and can wiretap communication channels and access exchanged information. We now show that the external eavesdropper can successfully obtain the reference signals $r_i(t)$ and $f_i(t)$ of agent $i$ when agents are updated by algorithm (1).

Let $\tilde{x}_i(t) \in \mathbb{R}^m$, $\tilde{r}_i(t) \in \mathbb{R}^m$, and $\tilde{f}_i(t) \in \mathbb{R}^m$ be the estimate of $x_i(t)$, $r_i(t)$, and $f_i(t)$, respectively. An observer based attack model is designed to identify $r_i(t)$ and $f_i(t)$, as follows:

$$\begin{align*}
\dot{\tilde{x}}_i(t) &= \tilde{f}_i(t) + \kappa \sum_{j=1}^{n} a_{ij} (x_j(t) - x_i(t)) + k_1 \tilde{x}_i(t), \\
\dot{\tilde{r}}_i(t) &= k_2 (x_i(t) - z_i(t) - \tilde{r}_i(t)) + \tilde{f}_i(t), \\
\dot{\tilde{f}}_i(t) &= k_3 x_i(t) + \tilde{f}_i(t), \\
\dot{\tilde{z}}_i(t) &= -k_3 \left( \tilde{f}_i(t) + \kappa \sum_{j=1}^{n} a_{ij} (x_j(t) - x_i(t)) \right) + k_4 \tilde{x}_i(t),
\end{align*}$$

where $k_1, k_2, k_3, k_4 \in \mathbb{R}$ are positive constants, $\tilde{x}_i(t) \triangleq x_i(t) - \tilde{x}_i(t) \in \mathbb{R}^m$ is the estimation error, $\tilde{f}_i(t) \in \mathbb{R}^m$ is an auxiliary variable, and $z_i(t) \in \mathbb{R}^m$ is the local filter updated by

$$\begin{align*}
\dot{z}_i(t) &= \kappa \sum_{j=1}^{n} a_{ij} (x_j(t) - x_i(t)), \\
z_i(0) &= 0.
\end{align*}$$

Theorem 1: When algorithm (1) 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 attack model developed in (2). More precisely, (2) ensures that the estimation errors $\tilde{r}_i(t) \triangleq r_i(t) - \tilde{r}_i(t)$, $\tilde{f}_i(t) \triangleq f_i(t) - \tilde{f}_i(t) \in \mathbb{R}^m$ are uniformly ultimately bounded (UUB). Moreover, provided $f_i(t)$ belongs to $L_2$-space, the estimation errors $\tilde{r}_i(t)$ and $\tilde{f}_i(t)$ converge to zero asymptotically.
Proof: A non-negative Lyapunov function $V(t) \in \mathbb{R}$ is introduced to facilitate the proof, as follows:

$$ V(t) \triangleq \frac{1}{2} k_4 \dot{x}_i^T(t) \dot{x}_i(t) + \frac{1}{2} \dot{r}_i^T(t) \dot{r}_i(t) + \frac{1}{2} \dot{f}_i^T(t) \dot{f}_i(t). $$ (4)

It can be obtained from (4) that $V(t)$ can be bounded by

$$ \frac{\mu}{2} \dot{y}^T(t) y(t) \leq V(t) \leq \frac{\mu}{2} \dot{y}^T(t) y(t), $$ (5)

where $\mu \triangleq \min \left\{ \frac{1}{2} k_4, \frac{1}{2} \mu \right\}, \mu \triangleq \max \left\{ \frac{1}{2} k_4, \frac{1}{2} \right\} \in \mathbb{R}$, and $y(t) \triangleq \dot{x}_i^T(t), \dot{r}_i^T(t), \dot{f}_i^T(t) \in \mathbb{R}^{3m_i}$. Taking the time derivative of (4) and substituting in (1) yield

$$ \dot{V}(t) = k_4 \dot{x}_i^T(t) \dot{x}_i(t) + \dot{r}_i^T(t) \dot{r}_i(t) + \dot{f}_i^T(t) \dot{f}_i(t) $$

$$ = -k_1 k_4 \dot{x}_i^T(t) \dot{x}_i(t) - k_2 \dot{r}_i^T(t) \dot{r}_i(t) - k_3 \dot{f}_i^T(t) \dot{f}_i(t) $$

$$ + \dot{f}_i^T(t) \dot{f}_i(t) + \dot{f}_i^T(t) \dot{f}_i(t) $$

$$ \leq -k_1 k_4 \dot{x}_i^T(t) \dot{x}_i(t) - k_2 \dot{r}_i^T(t) \dot{r}_i(t) $$

$$ - \left( \frac{k_3}{2} - \frac{1}{2k_2} \right) \dot{f}_i^T(t) \dot{f}_i(t) + \frac{1}{2k_3} \dot{f}_i^T(t) \dot{f}_i(t) $$

$$ \leq -\mu \dot{y}^T(t) y(t) + \dot{g}(t), $$ (6)

where $\mu \triangleq \min \left\{ k_1 k_4, \frac{k_1 k_4}{k_2} - \frac{1}{k_2} \right\} \in \mathbb{R}$ and $\dot{g}(t) \triangleq \frac{1}{2k_3} \dot{f}_i^T(t) \dot{f}_i(t) \in \mathbb{R}$. It is clear that $\mu$ is positive provided that $k_2$ and $k_3$ are selected to satisfy $k_3 > \frac{1}{2k_2}$. According to Assumption 2, $\dot{g}(t)$ is bounded. By utilizing (5) and (6), Theorem 4.18 in [23] can be invoked to conclude that $y(t)$, i.e., $\dot{x}_i(t)$, $\dot{r}_i(t)$ and $\dot{f}_i(t)$, is UUB.

We now prove the second claim. Based on $\dot{f}_i(t) \in \mathcal{L}_2$, it can be obtained that there exists a bounded positive constant $\lambda \in \mathbb{R}$ such that $\forall t \geq 0$,

$$ \int_0^t \frac{1}{2k_3} \dot{f}_i^T(\tau) \dot{f}_i(\tau) d\tau \leq \lambda. $$

Let the non-negative function $W(t) \in \mathbb{R}$ be defined as

$$ W(t) \triangleq V(t) + \lambda - \int_0^t \frac{1}{2k_3} \dot{f}_i^T(\tau) \dot{f}_i(\tau) d\tau. $$ (7)

Taking the time derivative of (7) and utilizing (6), it can be concluded that

$$ \dot{W}(t) = -k_1 k_4 \dot{x}_i^T(t) \dot{x}_i(t) - k_2 \dot{r}_i^T(t) \dot{r}_i(t) $$

$$ - \left( \frac{k_3}{2} - \frac{1}{2k_2} \right) \dot{f}_i^T(t) \dot{f}_i(t) \leq 0. $$ (8)

According to (7) and (8), it can be obtained that $W(t) \in \mathcal{L}_\infty$, i.e., $\dot{x}_i(t), \dot{r}_i(t), \dot{f}_i(t) \in \mathcal{L}_\infty \cap \mathcal{L}_2$. Assumption 2 and the expression in (3) can be used to conclude that $\dot{x}_i(t), \dot{r}_i(t), \dot{f}_i(t) \in \mathcal{L}_\infty \cap \mathcal{L}_2$. As $\dot{x}_i(t), \dot{r}_i(t), \dot{f}_i(t) \in \mathcal{L}_\infty \cap \mathcal{L}_2$ and $\dot{x}_i(t), \dot{r}_i(t), \dot{f}_i(t) \in \mathcal{L}_\infty$, Barbard's lemma [23] can be used to conclude that $\dot{x}_i(t), \dot{r}_i(t)$ and $\dot{f}_i(t)$ converge to zero asymptotically.

Remark 1: The design of the observer [22] is to illustrate that the consensus algorithm (1) is fragile to privacy attacks. Various techniques can be exploited to construct the attack model, but that is not the topic of this paper. In the following, we will show that the developed approach can provide privacy protection against the external eavesdropper no matter what attack model is used.

IV. PRIVACY PRESERVATION VIA STATE DECOMPOSITION

Inspired by the work [21], a state decomposition scheme is proposed to provide protection against an external eavesdropper. More precisely, the state and reference signals $\{x_i(t), r_i(t), f_i(t)\}$ of each agent are decomposed into two sub-sets $\{x_i^a(t), r_i^a(t), f_i^a(t)\}$ and $\{x_i^b(t), r_i^b(t), f_i^b(t)\}$. The initial values $r_i^a(0)$ and $r_i^b(0)$ can be randomly chosen from the set of all real numbers under the constraint

$$ r_i^a(0) + r_i^b(0) = 2r_i(0). $$ (9)

Furthermore, $f_i^a(t)$ and $f_i^b(t)$ are selected to satisfy

$$ f_i^a(t) + f_i^b(t) = 2f_i(t). $$ (10)

In this decomposition mechanism, the sub-state $x_i^a(t)$ takes over the role of the original state $x_i(t)$ in inter-agent interactions and is the only state value from agent $i$ that will be transmitted to its neighbors. The other sub-state $x_i^b(t)$ also involves in the distributed interaction by (and only by) exchanging information with $x_i^a(t)$. Therefore, $x_i^a(t)$ will affect the evolution of $x_i^a(t)$, but the existence of $x_i^b(t)$ is invisible to neighbors of agent $i$ and the eavesdropper. An example is given in Fig. 1 to present the state decomposition of a network with four agents.

Under the decomposition mechanism, the conventional average consensus algorithm (1) changes to

$$ \dot{x}_i^a(t) = f_i^a(t) + \kappa \sum_{j=1}^n a_{ij} (x_j^a(t) - x_i^a(t)) $$

$$ + \kappa \left( x_i^a(t) - x_i^a(t) \right), $$ (11)

$$ \dot{x}_i^b(t) = f_i^b(t) + \kappa \left( x_i^b(t) - x_i^b(t) \right), $$

$$ x_i^a(0) = r_i^a(0), \quad x_i^b(0) = r_i^b(0), \quad \forall i \in \mathcal{V}. $$

In the following, it is first shown that all states $x_i^a(t)$ and $x_i^b(t)$ will present the same convergence property as in the conventional case (1). Then, we prove that under the decomposition mechanism, the privacy of each agent is protected against the external eavesdropper.

Theorem 2: Under the decomposition mechanism, all sub-states $x_i^a(t)$ and $x_i^b(t)$ in (11) are input-to-state stable, and the tracking errors $x_i^a(t) - \frac{1}{n} \sum_{j=1}^n r_j(t)$ and $x_i^b(t) - \frac{1}{n} \sum_{j=1}^n r_j(t)$ are ultimately bounded.

Proof: It is clear that the decomposition mechanism ensures that all sub-states also compose a connected graph. Based on the result [22], dynamic average consensus can still be achieved, i.e., all sub-states are input-to-state stable, and the convergence errors $x_i^a(t) - \frac{1}{n} \sum_{j=1}^n r_j(t)$ and $x_i^b(t) - \frac{1}{n} \sum_{j=1}^n r_j(t)$ are ultimately bounded. It can be obtained from (9) and (10) that

$$ r_i^a(t) + r_i^b(t) = 2r_i(t), $$ (12)

which implies $\frac{1}{n} \sum_{j=1}^n (r_i^a(t) + r_i^b(t)) = \frac{1}{n} \sum_{j=1}^n r_j(t)$. Therefore, all sub-states $x_i^a(t)$ and $x_i^b(t)$ in (11) retain the same convergence properties as the original states. ■
Specifically, under the following conditions: the information available for the eavesdropper to extract the outcome under any value of the reference signals \( a_j \) could hold. Under the decomposition mechanism, an external eavesdropper cannot infer the reference signals \( r_p(t) \) and \( f_p(t) \) of any agent \( p \) with any guaranteed accuracy.

**Proof:** Under the decomposition mechanism, the information accessible to the eavesdropper at time \( t \) can be defined as \( I(t) \triangleq \{ A, \kappa, x_i^\alpha(t), i = 1, 2, \ldots, n \} \). To show that the privacy of the reference signals \( r_p(t) \) and \( f_p(t) \) can be preserved against the eavesdropper, it suffices to present that under any value \( \bar{r}_p(t) = r_p(0) + \int_0^t f_p(r) d\tau \) satisfying \( r_p(t) \neq r_p(t) \), the information \( \bar{I}(t) \triangleq \{ A, \kappa, \bar{x}_i^\alpha(t), i = 1, 2, \ldots, n \} \) accessible to the eavesdropper could be exactly the same as the information \( I(t) \) cumulated under \( r_p(t) \). This is because the only information available for the eavesdropper to extract the signals \( r_p(t) \) and \( f_p(t) \) is \( I(t) \), and if \( \bar{I}(t) \) could be the outcome under any value of \( r_p(t) \), 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 \( \bar{r}_p(t) \neq r_p(t) \), \( \bar{I}(t) = I(t) \) could hold.

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 \( \bar{R}_1(0), \bar{v}_p^0(0), \bar{v}_p^2(0), \bar{v}_1(0), \bar{f}_p^0(t), \bar{f}_p^2(t), \bar{f}_1(t), \bar{f}_q(t) \), \( \bar{I}(t) = I(t) \) could hold under \( \bar{r}_p(t) \neq r_p(t) \). Specifically, under the following conditions:

\[
\begin{align*}
\bar{r}_1(0) &= r_1(0) + r_p(0) - \bar{r}_p(0), \\
\bar{v}_p^0(0) &= v_p^0(0), \bar{v}_p^2(0) &= 2v_p^2(0) - r_p^0(0), \\
\bar{v}_1(0) &= v_1(0), \bar{v}_1^2(0) &= 2v_1(0) - \bar{v}_1^0(0), \\
\bar{r}_q(0) &= r_q(0), \bar{v}_q^0(0) &= r_q^0(0), \bar{v}_q^2(0) &= \bar{v}_q^0(0), \forall q \in \mathcal{V} \setminus \{p, l\},
\end{align*}
\]  
\[ (13) \]

and system dynamics

\[
\begin{align*}
\dot{x}_i^\alpha(t) &= \bar{f}_i^\alpha(t) + \kappa \sum_{j=1}^n a_{ij} (\bar{x}_j^\alpha(t) - \bar{x}_i^\alpha(t)) \\
&\quad + \kappa (\bar{x}_i^\beta(t) - \bar{x}_i^\alpha(t)), \\
\dot{x}_i^\beta(t) &= \bar{f}_i^\beta(t) + \kappa (\bar{x}_i^\alpha(t) - \bar{x}_i^\beta(t)), \\
\bar{x}_i^\alpha(0) &= \bar{r}_i^\alpha(0), \bar{x}_i^\beta(0) &= \bar{r}_i^\beta(0), \forall i \in \mathcal{V},
\end{align*}
\]  
\[ (15) \]

where 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., \( \bar{I}(t) = I(t) \). Note that the first equations of (13) and (14) are introduced to ensure that the average consensus value \( \frac{1}{n} \sum_{j=1}^n \bar{x}_j(t) \) is the same as the original one \( \frac{1}{n} \sum_{j=1}^n x_j(t) \). Now we prove that \( \bar{I}(t) = I(t) \). First, from (9), (11), (13), and (15), it can be obtained that

\[
\begin{align*}
\bar{x}_i^\alpha(0) &= x_i^\alpha(0), \bar{x}_i^\beta(0) &= x_i^\beta(0) + 2 (\bar{r}_p(0) - r_p(0)), \\
\bar{x}_i^\beta(0) &= x_i^\beta(0), \bar{x}_i^\alpha(0) &= x_i^\alpha(0) + 2 (\bar{r}_p(0) - r_p(0)),
\end{align*}
\]  
\[ (16) \]

Furthermore, based on (14) and (16), it can be verified that

\[
\begin{align*}
\bar{x}_p^\alpha(t) &= x_p^\alpha(t), \bar{x}_p^\beta(t) &= x_p^\beta(t) + 2 (\bar{r}_p(t) - r_p(t)), \\
x_1^\alpha(t) &= x_1^\alpha(t), x_1^\beta(t) &= x_1^\beta(t) + 2 (r_p(t) - \bar{r}_p(t)), \\
x_q^\alpha(t) &= x_q^\alpha(t), x_q^\beta(t) &= x_q^\beta(t), \forall q \in \mathcal{V} \setminus \{p, l\},
\end{align*}
\]  
\[ (17) \]

is the solution to (15). It is obvious that the solution (17) satisfies \( \forall i \in \mathcal{V}, x_i^\alpha(t) = x_i^\alpha(t) \), and thus \( \bar{I}(t) = I(t) \) could hold under \( \bar{r}_p(t) \neq r_p(t) \). Based on the above analysis, it can be concluded that no matter what attack model is used, the eavesdropper cannot infer \( r_p(t) \) and \( f_p(t) \) from \( I(t) \) with any guaranteed accuracy.

**Remark 2:** The proposed state decomposition scheme can be regarded as a privacy-preserving augmentation for consensus algorithm (1). Since the scheme is completely decentralized, it can be integrated with other dynamic average consensus approaches (11)–(14) to improve the resilience of original methods to privacy attacks.

V. APPLICATION TO FORMATION CONTROL

In this section, the dynamic average consensus with privacy preservation is utilized to address a formation control problem for nonholonomic mobile robots.

---

Fig. 1. State decomposition: (a) Before state decomposition. (b) After state decomposition.
A. Formation Control Objective

Suppose that there are $n$ networked nonholonomic mobile robots and $n$ mobile moving targets in the motion plane. Each mobile robot $i$ has access to its own position $s_i(t) \triangleq [x_i(t) \ y_i(t)]^T \in \mathbb{R}^2$ and can monitor the mobile target $i$ with position $p_i(t) \triangleq [x_i(t) \ y_i(t)]^T \in \mathbb{R}^2$ and velocity $\dot{p}_i(t) = q_i(t) \triangleq [\dot{x}_i(t) \ \dot{y}_i(t)]^T \in \mathbb{R}^2$. $s_i(t), p_i(t),$ and $q_i(t)$ are all expressed with respect to the inertial coordinate frame. The network among mobile robots is set up by the communication devices, and each mobile robot can share the information with its neighbors. For the networked mobile robots, the objective is to follow the group of mobile targets by spreading out in a pre-specified formation and protect the privacy of the mobile targets against the eavesdropper. Specifically, the formation control requires that by using the information received from the communication network, each mobile robot is driven to a relative vector $b_i(t) \triangleq [b_{x_i}(t) \ b_{y_i}(t)]^T \in \mathbb{R}^2$ with respect to the time-varying geometric center of the mobile targets, i.e., $s_i(t) \rightarrow \frac{1}{n} \sum_{i=1}^{n} p_i(t) + b_i(t)$ as $t \rightarrow \infty$. Meanwhile, it is also required that 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.

B. Control Design

As discussed in [22], the formation problem in the aforementioned scenario can be addressed with a tow-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.

Since each mobile robot only can monitor one mobile target, it needs to cooperate with its neighbors to compute the geometric center in the cyber layer. The state decomposition based dynamic average consensus algorithm presented in Section [IV] can be 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. More precisely, let $c^\alpha_i(t) \triangleq [c^\alpha_{x_i}(t) \ c^\alpha_{y_i}(t)]^T \in \mathbb{R}^2$ and $c^\beta_i(t) \triangleq [c^\beta_{x_i}(t) \ c^\beta_{y_i}(t)]^T \in \mathbb{R}^2$ be two sub-sets of the estimate of the geometric center, which are updated by

$$
\dot{c}^\alpha_i(t) = q^\alpha_i(t) + \kappa \sum_{j=1}^{n} a_{ij} \left( c^\alpha_j(t) - c^\alpha_i(t) \right) 
+ \kappa \left( c^\alpha_i(t) - c^\beta_i(t) \right), 
$$

$$
\dot{c}^\beta_i(t) = q^\beta_i(t) + \kappa \left( c^\alpha_i(t) - c^\beta_i(t) \right), 
$$

$$
c^\alpha_i(0) = p^\alpha_i(0), \quad c^\beta_i(0) = p^\beta_i(0),
$$

where $p^\alpha_i(0), p^\beta_i(0), q^\alpha_i(t), q^\beta_i(t) \in \mathbb{R}^2$ are selected to satisfy

$$
p^\alpha_i(0) + p^\beta_i(0) = 2 p_i(0), 
q^\alpha_i(t) + q^\beta_i(t) = 2 q_i(t).
$$

As shown in Theorem 2 and 3, $c^\alpha_i(t)$ 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 nonholonomic mobile robot $i$ to ensure that $s_i(t) \rightarrow c^\alpha_i(t) + b_i(t)$ as $t \rightarrow \infty$. The kinematic model of nonholonomic mobile robot $i$ is described by

$$
\dot{s}_i(t) = v_i(t) \cos(\theta_i(t)), 
\dot{\theta}_i(t) = \omega_i(t),
$$

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 developed, the desired heading angle $\theta_{di}(t) \in \mathbb{R}$ and desired linear velocity $v_{di}(t) \in \mathbb{R}$ are constructed as

$$
\theta_{di}(t) = \arctan \left( \frac{c^\alpha_{y_i}(t)}{c^\alpha_{x_i}(t)} \right), 
v_{di}(t) = \sqrt{(\dot{c}^\alpha_{x_i}(t))^2 + (\dot{c}^\alpha_{y_i}(t))^2},
$$

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

$$
\epsilon_{x_i}(t) \triangleq \cos(\theta_i(t))(s_{x_i}(t) - c^\alpha_{x_i}(t) - b_{x_i}(t)) 
+ \sin(\theta_i(t))(s_{y_i}(t) - c^\alpha_{y_i}(t) - b_{y_i}(t)), 
\epsilon_{y_i}(t) \triangleq -\sin(\theta_i(t))(s_{x_i}(t) - c^\alpha_{x_i}(t) - b_{x_i}(t)) 
+ \cos(\theta_i(t))(s_{y_i}(t) - c^\alpha_{y_i}(t) - b_{y_i}(t)), 
\epsilon_{\theta_i}(t) \triangleq \theta_i(t) - \theta_{di}(t).
$$

It is clear that $s_i(t) \rightarrow c^\alpha_i(t) + b_i(t)$ as $[e^\alpha_{x_i}(t) \ e^\alpha_{y_i}(t) \ e^\alpha_{\theta_i}(t)] \rightarrow 0$. Note that the mobile robot is subjected to nonholonomic constraint, and thus in
general time-varying auxiliary variables will be introduced to facilitate the controller design. Considering the nonholonomic constraint, an auxiliary error $\epsilon_{\theta_i}(t) \in \mathbb{R}$ is defined as

$$\epsilon_{\theta_i}(t) \triangleq e_{\theta_i}(t) - \rho_i(t),$$

(23)

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

$$\rho_i(t) \triangleq \lambda_0 \omega_i(t) \tanh \left( \lambda_1 \sqrt{e_{x_i}^2(t) + e_{y_i}^2(t)} \right) \sin(\lambda_2 t)$$

(24)

with $\omega_i(t) \triangleq \exp \left( - \int_{0}^{t} |v_{di}(\tau)| d\tau \right) \in \mathbb{R}$ and $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{R}$ being positive constants. To achieve the formation control, the velocity inputs $v_i(t)$ and $\omega_i(t)$ are designed as

$$v_i(t) = -\gamma_1 \tanh(e_{x_i}(t)) + \cos(e_{\theta_i}(t)) v_{di}(t),$$

$$\omega_i(t) = -\gamma_2 \tanh(\epsilon_{\theta_i}(t)) + \rho_i(t) - \gamma_3 \text{sgn}(\epsilon_{\theta_i}(t))$$

(25)

$$- \gamma_4 \sin(e_{\theta_i}(t)) - \sin(\rho_i(t)) \frac{v_{di}(t)}{\epsilon_{\theta_i}(t)} v_{di}(t) e_{yi}(t),$$

where $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathbb{R}$ are positive control gains, and $\text{sgn}(\cdot)$ is the standard signum function.

**Theorem 4:** The controller designed in (25) ensures that the system errors $e_{x_i}(t)$, $e_{y_i}(t)$, and $e_{\theta_i}(t)$ ($i = 1, 2, \ldots, n$) asymptotically converge to zero in the sense that

$$\lim_{t \to \infty} e_{x_i}(t), e_{y_i}(t), e_{\theta_i}(t) = 0.$$  

**Proof:** See Appendix A.

According to the definition of $e_{x_i}(t)$, $e_{y_i}(t)$, and $e_{\theta_i}(t)$, it can be concluded that $s_i(t) \rightarrow c_i^0(t) + b_i(t)$ as (26) holds. Since $c_i^0(t)$ will converge to the neighbourhood of the geometric center $\frac{1}{n} \sum_{i=1}^{n} \rho_i(t)$, the formation control task is accomplished as (26) holds.

**VI. SIMULATION RESULTS**

In this section, simulation is conducted to demonstrate the performance of the developed approach. A team of four mobile robots are required to follow a group of four 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 selected as follows:

$$p_1(0) = \begin{bmatrix} 1.8 \\ 1.2 \end{bmatrix}, p_2(0) = \begin{bmatrix} -1.2 \\ 1.8 \end{bmatrix},$$

$$p_3(0) = \begin{bmatrix} -1.8 \\ -1.2 \end{bmatrix}, p_4(0) = \begin{bmatrix} 1.2 \\ -1.8 \end{bmatrix},$$

$$q_1(t) = q_0(t) + \begin{bmatrix} 0.1 \cos(0.2t) \\ -0.2 \cos(0.4t) \end{bmatrix},$$

$$q_2(t) = q_0(t) + \begin{bmatrix} -0.2 \cos(0.4t) \\ 0.1 \cos(0.2t) \end{bmatrix},$$

$$q_3(t) = q_0(t) + \begin{bmatrix} -0.1 \cos(0.2t) \\ 0.2 \cos(0.4t) \end{bmatrix},$$

$$q_4(t) = q_0(t) + \begin{bmatrix} 0.2 \cos(0.4t) \\ -0.1 \cos(0.2t) \end{bmatrix},$$

where $q_0(t) \in \mathbb{R}^2$ is given by

$$q_0(t) = (0.75 - 0.25 \cos(0.24t)) \begin{bmatrix} \cos(\frac{\pi}{6} + 0.5 \sin(0.2t)) \\ \sin(\frac{\pi}{6} + 0.5 \sin(0.2t)) \end{bmatrix}. $$

Furthermore, the initial positions of the mobile robots are selected as $s_1(0) = \begin{bmatrix} 1.3 \\ 5.2 \end{bmatrix}^T$, $s_2(0) = \begin{bmatrix} -7.5 \\ 2.6 \end{bmatrix}^T$, $s_3(0) = \begin{bmatrix} -4 \\ -5.5 \end{bmatrix}^T$, and $s_4(0) = \begin{bmatrix} 5.2 \\ -5.2 \end{bmatrix}^T$. For the mobile robots, the desired relative positions to the geometric center of mobile targets are given by $b_1(0) = \begin{bmatrix} 4 \\ 4 \end{bmatrix}^T$, $b_2(0) = \begin{bmatrix} -4 \\ 4 \end{bmatrix}^T$, $b_3(0) = \begin{bmatrix} -4 \\ -4 \end{bmatrix}^T$, and $b_4(0) = \begin{bmatrix} 4 \\ -4 \end{matrix}^T$. In the following, we first evaluate the state decomposition based dynamic average consensus algorithm and then test the formation controller designed in (25).

Suppose that an external eavesdropper is interested in obtaining the information of mobile target 1 and uses the eavesdropping scheme developed in Section III to infer $p_1(t)$ and $q_1(t)$. To better demonstrate the performance of the proposed consensus scheme, both the conventional algorithm (1) and the proposed one are used to estimate the geometric center of mobile targets. Fig. 3 presents the evolution of the network states as well as the eavesdropping states under the conventional algorithm (1). It can be seen that the eavesdropper can successfully infer $p_1(t)$ and $q_1(t)$ when the agents are updated with algorithm (1). The performance of the privacy-preserving scheme (18) is illustrated in Fig. 4. It is clear that the proposed scheme can achieve dynamic average consensus while protect the privacy information of mobile target.

As discussed in Section VII, the dynamic average consensus algorithm is used to estimate the geometric center of mobile targets, and then the mobile robots are driven with the controller (25) to achieve the formation task. Fig. 2 depicts the motion trajectories of all mobile robots, showing that all robots follow the geometric center by spreading out in a desired rectangle pattern. Moreover, the evolution of the formation tracking errors are presented in Fig. 5. From Fig. 6 it can be seen that the tracking errors $e_{x_i}(t)$, $e_{y_i}(t)$, and $e_{\theta_i}(t)$ all asymptotically converge to small values that are close to zero.

**VII. CONCLUSION**

This paper proposed a state decomposition based privacy-preserving method for the continuous-time dynamic average consensus. The key idea of the developed method was to decompose the original state into two sub-states. By suitably selecting the new reference signals of the two sub-states, the convergence properties of the consensus algorithm can be retained, and the reference signals of the original state cannot be discovered by the external eavesdropper. Furthermore, the proposed method was successfully applied to achieve formation control for nonholonomic 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 4**

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

$$V_i(t) = \frac{1}{2} \gamma_4 (e_{x_i}^2 + e_{y_i}^2) + \frac{1}{2} \epsilon_{\theta_i}^2.$$  

(27)
Based on (20), (22)-(25) and the facts that
\[ \dot{c}_{xi}(t) = v_{di}(t) \cos(\theta_{di}(t)), \quad \dot{c}_{yi}(t) = v_{di}(t) \sin(\theta_{di}(t)), \]
the closed-loop error system can be derived, as follows:
\[ \dot{e}_{xi}(t) = -\gamma_1 \tanh(e_{xi}(t)) + \omega_i(t)e_{yi}(t), \]
\[ \dot{e}_{yi}(t) = -\omega_i(t)e_{xi}(t) + \sin(e_{ri}(t))v_{di}(t), \]
\[ \dot{\theta}_{di}(t) = -\gamma_2 \tanh(\bar{e}_{\theta i}(t)) - \dot{\theta}_{di}(t) - \gamma_3 \text{sgn}(\bar{e}_{\theta i}(t)) - \frac{\gamma_4}{\bar{e}_{\theta i}(t)} \sin(\rho_i(t))v_{di}(t)e_{yi}(t). \]

(28)

Fig. 5. Motion trajectories of all mobile robots.

After taking the time derivative of (27) and substituting (28) into the derivative, it can be determined that
\[ \dot{V}_i(t) = -\gamma_1 \gamma_4 e_{xi}(t) \tanh(e_{xi}(t)) - \gamma_2 \bar{e}_{\theta i}(t) \tanh(\bar{e}_{\theta i}(t)) + \gamma_4 v_{di}(t)e_{yi}(t) \sin(\rho_i(t)) - \bar{e}_{\theta i}(t) \left( \gamma_3 \text{sgn}(\bar{e}_{\theta i}(t)) + \dot{\theta}_{di}(t) \right). \]

(29)
If $\gamma_3$ is selected sufficiently large to satisfy $\gamma_3 > \sup_{t \in [0, \infty)} |\dot{\theta}_d(t)|$, then $V_i(t)$ can be upper bounded by

$$V_i(t) \leq -W_i(t) + \gamma_3 |e_{yi}(t)|v_{di}(t) \sin(\rho_i(t)) \leq \sqrt{2}\gamma_3 |V_i(t)|v_{di}(t) \sin(\rho_i(t)),$$

where $W_i(t) \in \mathbb{R}$ is a non-negative function given by

$$W_i(t) \equiv \gamma_1 e_{x_i}(t) \tan(e_{x_i}(t)) + \gamma_2 \dot{\theta}_i(t) \tanh(\dot{\theta}_i(t)).$$

From (24), it can be found that $0 \leq \omega_i(t) \leq 1$, $\dot{\omega}_i(t) = -v_{di}(t)e_{x_i}(t)$, and $|\rho_i(t)| \leq \lambda_0 \omega_i(t)$. Using these facts and integrating $|v_{di}(t) \sin(\rho_i(t))|$, it can be concluded that

$$\int_0^t |v_{di}(\tau) \sin(\rho_i(\tau))| d\tau \leq \lambda_0 \int_0^t |v_{di}(\tau)| \omega_i(\tau) d\tau \leq \lambda_0 \int_0^t -\dot{\omega}_i(\tau) d\tau \leq \lambda_0 (\omega(0) - \omega(t)) \leq \lambda_0.$$