SCIENCE CHINA
Information Sciences

• Supplementary File •

On Distributed Privacy-Preserving k-WTA Network

Yutong LI[1,3], Kewei ZHANG[2], Yongji GUAN[1] & Long JIN[1,2*]

[1] *School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China*
[2] *School of Automation and Electrical Engineering, Lanzhou University of Technology, Lanzhou, 730050, China*
[3] *College of Computer Science and Engineering, Jishou University, Jishou 416000, China*

Appendix A Preliminaries

In this section, preliminaries on the graph theory and dynamic privacy-preserving average consensus are given.

Appendix A.1 Graph theory

A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ is used to describe the relationship among n nodes in a communication topology, where $\mathcal{V}$ is the node set, $\mathcal{E}$ is the edge set, and $\mathcal{A} \in \mathbb{R}^{n\times n} = [a_{ij}]$ with $\forall i \in \mathcal{V}$, $a_{ii} = 0$ being the adjacency matrix. In particular, for an undirected graph, when $i \in \mathcal{V}$, $j \in \mathcal{V}$, and $i \neq j$, if $(i, j) \in \mathcal{E}$, $a_{ij} = 1$, otherwise $a_{ij} = 0$. Besides, if $a_{ij} = 1$, then $j \in \mathbb{N}_i$, where $\mathbb{N}_i$ is the neighbor set of the i-th node. $L = D(\mathcal{A}\mathbf{1}_n) - \mathcal{A}$ is the Laplacian matrix, where $D(\cdot)$ represents a diagonalization operation and $\mathbf{1}_n \in \mathbb{R}^n$ consists of 1. In view of the defination of adjacency matrix $\mathcal{A}$, for an undirected graph, Laplacian matrix $L = [l_{ij}]$ has the following properties [1,2]: $\forall i, j \in \mathcal{V}$ and $i \neq j$, $l_{ij} = l_{ji} \leqslant 0$; $\sum_{j\neq i}^{n} l_{ij} + l_{ii} = 0$; L is positive semidefinite and has only one eigenvalue 0, where the corresponding eigenvector is $\mathbf{1}_n$.

Appendix A.2 Dynamic average consensus and privacy attack

Consider that the i-th individual in the communication topology network corresponds to the following time-varying information:

$$\dot{\boldsymbol{s}}_i(t) = \boldsymbol{u}_i(t).$$

Suppose that there exists an internal state $\boldsymbol{q}_i(t)$ for the i-th individual. A dynamic average consensus filter aims to achieve $\boldsymbol{q}_i(t) \to (\sum_{i=1}^{n} \boldsymbol{s}_i(t))/n$ through local communication so that the global information is estimated. However, the leakage of information exchanged among nodes may lead to the disclosure of node state privacy. That is, an attacker can infer the state privacy of the nodes by using the information exchanged among them. In the relatively earlier consensus work, static average consensus is typically investigated, where each node's input is a constant, meaning that the average consensus of the entire system remains unchanged and is the average of these constants. In this case, random perturbations are considered for encryption purposes. However, unstructured random perturbations can affect the accuracy of the average consensus [3], which might lead to the collapse of systems that require an accurate consensus. In [4], a static average consensus encryption method based on the mask function is designed. It introduces perturbations that decay over time to protect the constant input by the node, which ensures that the accuracy of consensus will not be affected when the perturbations decay to an extremely small level. Unfortunately, on the one hand, this method prevents the average consensus filter from converging to the accurate value until the perturbations have decayed to a certain extent. On the other hand, it is difficult to directly extend it to dynamic average consensus because the characteristic of the perturbations decaying over time can only ensure that the initial state information of the nodes is not leaked. In addition to adding random perturbations, work [5] utilized the state decomposition method to encrypt the static consensus filter without affecting the accuracy of the average consensus. Subsequently, in work [6], the aforementioned state decomposition-based method has also been further extended to the category of dynamic average consensus, and it performs well on continuously slowly changing dynamic signals. However, during our tests, we find that the effect of this method is not satisfactory when dealing with signals that changed rapidly only within a short period of time and remained stable for the rest of the time. Specifically, in [6], For the following dynamic average consensus filter:

$$\begin{aligned} &\dot{\boldsymbol{q}}_i(t) = \boldsymbol{u}_i(t) - \iota \sum\nolimits_{j\in\mathbb{N}_i} (\boldsymbol{q}_i(t) - \boldsymbol{q}_j(t)), \\ &\boldsymbol{q}_i(0) = \boldsymbol{s}_i(0),\ \ i = 1, 2, \cdots, n, \end{aligned} \tag{A1}$$

[*] Corresponding author (email: jinlongsysu@foxmail.com)

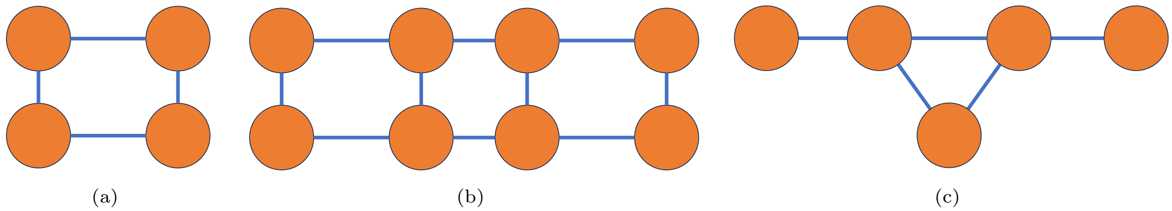


Figure A1 Communication topologies used in this paper. (a) Numerical simulations. (b) Multi-robot coordination simulations. (c) Multi-robot coordination experiments.

a privacy attack model is constructed as follows:

$$
\begin{aligned}
&\dot{\acute{\boldsymbol{q}}}_i(t) = \acute{\boldsymbol{u}}_i(t) - \iota \sum\nolimits_{j\in\mathbb{N}_i} (\boldsymbol{q}_i(t) - \boldsymbol{q}_j(t)) + v_1(\boldsymbol{q}_i(t) - \acute{\boldsymbol{q}}_i(t)),\\
&\dot{\acute{\boldsymbol{s}}}_i(t) = v_2(\boldsymbol{q}_i(t) - \boldsymbol{\xi}_i(t) - \acute{\boldsymbol{s}}_i(t)) + \acute{\boldsymbol{u}}_i(t),\\
&\acute{\boldsymbol{u}}_i(t) = v_3\boldsymbol{q}_i(t) + \check{\boldsymbol{u}}_i(t),\\
&\dot{\check{\boldsymbol{u}}}_i(t) = v_3(-\acute{\boldsymbol{u}}_i(t) + \iota \sum\nolimits_{j\in\mathbb{N}_i} (\boldsymbol{q}_i(t) - \boldsymbol{q}_j(t))) + v_4(\boldsymbol{q}_i(t) - \acute{\boldsymbol{q}}_i(t)),\\
&\dot{\boldsymbol{\xi}}_i(t) = -\iota \sum\nolimits_{j\in\mathbb{N}_i} (\boldsymbol{q}_i(t) - \boldsymbol{q}_j(t)),\ \ \boldsymbol{\xi}_i(0) = 0,
\end{aligned}
\tag{A2}
$$

where $\acute{\boldsymbol{q}}_i(t)$, $\acute{\boldsymbol{s}}_i(t)$, and $\acute{\boldsymbol{u}}_i(t)$ are the estimates of $\boldsymbol{q}_i(t)$, $\boldsymbol{s}_i(t)$, and $\boldsymbol{u}_i(t)$, respectively; v_1, v_2, v_3, and v_4 are positive constants; $\check{\boldsymbol{u}}_i(t)$ and $\boldsymbol{\xi}_i(t)$ are state variables.

Lemma A1. From the dynamic average consensus filter (A1), the privacy attack model (A2) is able to obtain the time-varying information $\boldsymbol{s}_i(t)$ of each individual [6].

Meanwhile, in order to counter such attacks, a dynamic privacy-preserving consensus filter based on state decomposition in [6] is presented as follows:

$$
\begin{aligned}
&\dot{\boldsymbol{q}}_i^1(t) = \boldsymbol{u}_i^1(t) - \iota \sum\nolimits_{j\in\mathbb{N}_i} (\boldsymbol{q}_i^1(t) - \boldsymbol{q}_j^1(t)) + \iota(\boldsymbol{q}_i^2(t) - \boldsymbol{q}_i^1(t)),\\
&\dot{\boldsymbol{q}}_i^2(t) = \boldsymbol{u}_i^2(t) + \iota(\boldsymbol{q}_i^1(t) - \boldsymbol{q}_i^2(t)),\\
&\boldsymbol{q}_i^1(0) = \boldsymbol{s}_i^1(0),\ \ \boldsymbol{q}_i^2(0) = \boldsymbol{s}_i^2(0),\ \ i = 1, 2, \cdots, n,
\end{aligned}
\tag{A3}
$$

where $\boldsymbol{s}_i^1(0) + \boldsymbol{s}_i^2(0) = 2\boldsymbol{s}_i(0)$ and $\boldsymbol{u}_i^1(t) + \boldsymbol{u}_i^2(t) = 2\boldsymbol{u}_i(t)$. Then, we conducted a numerical test on a communication topology consisting of four entities, and the specific topology structure is shown in Fig. A1(a). The four input signals of the above consensus filter are designed as follows: $\boldsymbol{s}_i(t) = 1/(1 + e^{-20(t-5)})$ when $i = 1, 2$; $\boldsymbol{s}_i(t) = 1/(1 + e^{-20(-t+5)})$ when $i = 3, 4$. As shown in Fig. A2, although the dynamic privacy-preserving consensus filter (A3) can ensure that the information obtained by the privacy attack model (A2) is different from the actual information, it only changes the amplitude of the signals and does not affect the overall change pattern of the signals. It also indicates that this method is not applicable for protecting the output of the k-winner-take-all (k-WTA) network. That is, it fails to effectively conceal the task allocation strategy pattern of the k-WTA network: individuals with relatively higher states are the winners and execute the tasks, while individuals with relatively lower states are the losers and remain on standby. Moreover, in [7], another privacy-preserving consensus filter achieves the effect of protecting the original signal by adding a constant bias to the signal. Evidently, it also faces the same problem. In view of this, it is necessary to further design a privacy-preserving dynamic consensus filter suitable for k-WTA networks.

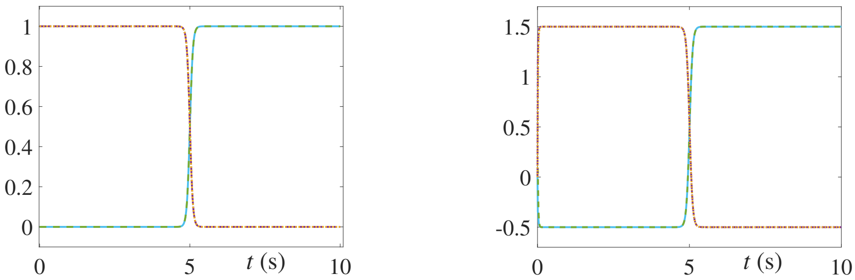
Remark 1. The privacy attack approach considered in this paper mainly restores the original input data of the consensus filter by obtaining the interaction information among individuals in the communication topology, which leads to the disclosure of privacy without destroying the normal operation of the whole system. Although there is no unified privacy attack model for different consensus methods, direct information interaction is always at risk from these attacks. This point will be further explained in the simulations in Appendix C.

Appendix B Theoretical analyses

In this section, we first provide detailed proofs for the three theorems presented in the paper. Additionally, an example demonstrating the existence of lagging errors in an existing k-WTA network [8] is given. Other k-WTA networks can also be proven using a similar method.

Appendix B.1 The proofs of the theorems in the paper

In this paper, we transformed the k-WTA problem with inequality constraints (Eq. (2) in the paper) into a k-WTA problem with only equality constraints (Eq. (3) in the paper) by introducing a class of exponential penalty functions $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ [9]. Before presenting the proofs of the three theorems in the paper, we will elaborate from the following two aspects to discuss the solvability of problem (Eq. (3) in the paper).



(a)

(b)

Figure A2 The protection effect of consensus filter (A3) when faced with a set of sigmoid functions that is designed to satisfy the characteristics of the output of a k-WTA network. (a) The original information. (b) The information obtained by privacy attack model (A2).

On the one hand, from the perspective of designing the penalty function, according to [10], if the solution $\boldsymbol{h}(t)$ satisfies inequality constraints, then the value of the auxiliary function $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ should be a positive number that is very close to zero. Conversely, if the solution $\boldsymbol{h}(t)$ does not satisfy the inequality constraint, then the value of $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ must be a large positive number, which is a punishment for the solution $\boldsymbol{h}(t)$ that is not within the feasible range of the constraint. In other words, the effect of the large positive number is to force the solution to the objective function close to the feasible range of the inequality constraint during the minimization of the objective function. In conclusion, $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ should satisfy the following conditions:

$$\begin{cases} \boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t) \approx 0, & \text{if } 0 \leqslant \boldsymbol{h}_i(t) \leqslant 1, \\ \boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t) \gg 0, & \text{otherwise.} \end{cases} \tag{B1}$$

Meanwhile, the penalty function $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ must be differentiable. It is known that $\boldsymbol{\beta} = [\boldsymbol{\beta}_1; \boldsymbol{\beta}_2; \cdots; \boldsymbol{\beta}_{2n}]$ is a constant vector. In addition, for the i-th element of $\boldsymbol{f}(t) \in \mathbb{R}^{2n}$, when $1 \leqslant i \leqslant n$, $\boldsymbol{f}_i(t) = e^{-\kappa(1-\boldsymbol{h_i}(t))}$ and when $n+1 \leqslant i \leqslant 2n$, $\boldsymbol{f}_i(t) = e^{-\kappa \boldsymbol{h}_{i-n}(t)}$ with κ being a positive constant. Evidently, the penalty function used is differentiable, and when κ is large enough, it also meets condition (B1). On the other hand, from the perspective of problem (Eq. (3) in the paper), since $\varpi\boldsymbol{h}^{\mathrm{T}}(t)\boldsymbol{h}(t) - \boldsymbol{h}^{\mathrm{T}}(t)\boldsymbol{w}(t)$ is strictly convex and $\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{f}(t)$ is convex, the objective function is also strictly convex. Furthermore, the linear equality constraint $\mathbf{1}_n^{\mathrm{T}}\boldsymbol{h}(t) = k$ defines a convex set. Therefore, according to the convex optimization theory, problem (Eq. (3) in the paper) has a unique solution.

Theorem B1. For the proposed DPP-kWTA network (Eq. (8) in the paper), variable $\boldsymbol{b}(t)$, that is, $[\boldsymbol{h}(t); \alpha(t)]$, globally converges to the theoretical solution. In other words, the output $\boldsymbol{h}(t)$ of the proposed DPP-kWTA network (Eq. (8) in the paper) converges to the optimal solution of the k-WTA problem (Eq. (3) in the paper).

Proof. It is worth pointing out that the theoretical solution of variable $\boldsymbol{b}(t)$ should satisfy the Karush-Kuhn-Tucker conditions (Eq. (4) in the paper), that is, $\boldsymbol{\gamma}(t) = \mathbf{0}$. In view of this, a Lyapunov function is first constructed:

$$R_1(t) = \frac{1}{2}\boldsymbol{\gamma}^{\mathrm{T}}(t)\boldsymbol{\gamma}(t). \tag{B2}$$

Then, taking the time derivative of the above equation yields

$$\begin{aligned} \dot{R}_1(t) &= \boldsymbol{\gamma}^{\mathrm{T}}(t)\dot{\boldsymbol{\gamma}}(t) \\ &= -\theta\boldsymbol{\gamma}^{\mathrm{T}}(t)\boldsymbol{\gamma}(t) \leqslant 0. \end{aligned} \tag{B3}$$

In particular, according to eqaution (B2) and equation (B3), it is concluded that $\boldsymbol{\gamma}(t)$ is capable of converging to zero globally based on the Lyapunov stability theorem [11]. Thus, the proof is completed. ■

Theorem B2. The proposed DPP-kWTA network (Eq. (8) in the paper) enables $\boldsymbol{b}(t)$ to converge to the theoretical solution $\boldsymbol{b}^*(t)$ in an exponential form with rate θ.

Proof. Let $\boldsymbol{\varphi}(t) = \boldsymbol{b}(t) - \boldsymbol{b}^*(t)$, and then a Lyapunov function is constructed as follows:

$$R_2(t) = \frac{1}{2}\boldsymbol{\varphi}^{\mathrm{T}}(t)\boldsymbol{\varphi}(t). \tag{B4}$$

Take the derivative of the above equation with respect to time t:

$$\dot{R}_2(t) = \boldsymbol{\varphi}^{\mathrm{T}}(t)\dot{\boldsymbol{\varphi}}(t). \tag{B5}$$

Substituting Eq. (6) in the paper yields

$$\dot{R}_2(t) = \boldsymbol{\varphi}^{\mathrm{T}}(t)(E^{-1}(t)(-\theta(Q\boldsymbol{b}(t) - \boldsymbol{c}(t)) + \boldsymbol{d}(t)) - \dot{\boldsymbol{b}}^*(t)). \tag{B6}$$

Theoretical solution $\boldsymbol{b}^*(t)$ should satisfy the Karush-Kuhn-Tucker conditions (Eq. (4) in the paper). That is, the vector error function $\boldsymbol{\gamma}(t) = Q\boldsymbol{b}(t) - \boldsymbol{c}(t)$ (Eq. (5) in the paper) and its derivative with respect to time $\dot{\boldsymbol{\gamma}}(t) = E(t)\dot{\boldsymbol{b}}(t) - \boldsymbol{d}(t)$

(Eq. (5) in the paper) should both be equal to zero. Thus, it can be concluded that $\dot{\boldsymbol{b}}^*(t) = E^{-1}(t)\boldsymbol{d}(t)$. By combining Eq. (B6), the following equation can be obtained:

$$\begin{aligned}\dot{R}_2(t) &= -\theta\boldsymbol{\varphi}^{\mathrm{T}}(t)(E^{-1}(t)(Q\boldsymbol{b}(t)-\boldsymbol{c}(t)))\\ &= -\theta\boldsymbol{\varphi}^{\mathrm{T}}(t)(E^{-1}(t)\boldsymbol{\gamma}(t)).\end{aligned}\tag{B7}$$

Then, assume $\boldsymbol{\gamma}(t)$ is a smooth function $\boldsymbol{\gamma}(\boldsymbol{b}(t),\, t)$ of $\boldsymbol{b}(t)$. By performing a first-order Taylor expansion around $\boldsymbol{b}^*(t)$, the following equation can be obtained:

$$\boldsymbol{\gamma}(\boldsymbol{b}(t),\, t) \approx \boldsymbol{\gamma}(\boldsymbol{b}^*(t),\, t) + E(t)(\boldsymbol{b}(t) - \boldsymbol{b}^*(t)).$$

Since $\boldsymbol{\gamma}(\boldsymbol{b}^*(t),\, t) = 0$, the above equation can be written as

$$\boldsymbol{\gamma}(\boldsymbol{b}(t),\, t) \approx E(t)(\boldsymbol{b}(t) - \boldsymbol{b}^*(t)).$$

Then, substituting the above equation into Eq. (B7) yields

$$\begin{aligned}\dot{R}_2(t) &= -\theta\boldsymbol{\varphi}^{\mathrm{T}}(t)(E^{-1}(t)E(t)(\boldsymbol{b}(t)-\boldsymbol{b}^*(t)))\\ &= -\theta\boldsymbol{\varphi}^{\mathrm{T}}(t)\boldsymbol{\varphi}(t) \leqslant 0.\end{aligned}\tag{B8}$$

Subsequently, taking the integral of the above equation with respect to time t yields

$$\begin{aligned}\int_0^t \dot{R}_2(\sigma)\mathrm{d}\sigma &= R_2(t) - R_2(0)\\ &= -\theta\int_0^t \boldsymbol{\varphi}^{\mathrm{T}}(\sigma)\boldsymbol{\varphi}(\sigma)\mathrm{d}\sigma.\end{aligned}\tag{B9}$$

Noting that $R_2(0) = 1/2\boldsymbol{\varphi}^{\mathrm{T}}(0)\boldsymbol{\varphi}(0)$ and as $t \to \infty$, $R_2(t) \to 0$. In view of this, the relationship between the convergence rate of $\|\boldsymbol{\varphi}(t)\|_2$ and the parameter θ is as follows:

$$\|\boldsymbol{\varphi}(t)\|_2 \approx \exp(-\theta t)\|\boldsymbol{\varphi}(0)\|_2,\tag{B10}$$

where $\exp(\cdot)$ is the natural exponential function, and $\|\cdot\|_2$ represents the 2-norm. Thus, the proof is completed. ■

Theorem B3. In an undirected communication topology, the key information $\boldsymbol{h}_i(t)$ of the DPP-kWTA network can not be obtained by an external eavesdropper. Specifically, the privacy attack model is only able to obtain the encrypted information from the privacy-preserving consensus filter (Eq. (7) in the paper).

Proof. According to equation (Eq. (7) in the paper), the following formula is able to be obtained:

$$\sum_{i=1}^{n}\boldsymbol{p}_i(t) = \sum_{i=1}^{n}\boldsymbol{q}_i(t) - \sum_{i=1}^{n}\sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_j^i(\epsilon) + \sum_{i=1}^{n}\sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_i^j(\epsilon).$$

Furthermore, combining the Laplacian matrix L of the undirected graph yields

$$\sum_{i=1}^{n}\boldsymbol{p}_i(t) = \sum_{i=1}^{n}\boldsymbol{q}_i(t) + \mathrm{tr}(LH(\epsilon)) - \mathrm{tr}(LH^{\mathrm{T}}(\epsilon)),$$

where $\mathrm{tr}(\cdot)$ means taking the trace of a matrix; if $i = j$, the $(i,\, j)$-th element of matrix $H(\epsilon)$ is 0 and if $i \neq j$, the $(i,\, j)$-th element of matrix $H(\epsilon)$ is $\boldsymbol{\delta}_i^j(\epsilon)$. Note that the Laplacian matrix L of the undirected graph is symmetric. It is obtained that

$$\mathrm{tr}(LH^{\mathrm{T}}(\epsilon)) = \mathrm{tr}(H(\epsilon)L^{\mathrm{T}}) = \mathrm{tr}(H(\epsilon)L) = \mathrm{tr}(LH(\epsilon)).$$

Therefore, it is concluded that

$$\sum_{i=1}^{n}\boldsymbol{p}_i(t) = \sum_{i=1}^{n}\boldsymbol{q}_i(t),$$

which means that the privacy-preserving consensus filter (Eq. (7) in the paper) is equivalent to the following expression:

$$\begin{aligned}\dot{\boldsymbol{p}}_i(t) &= \dot{\boldsymbol{h}}_i(t) - \iota\sum\nolimits_{j\in\mathbb{N}_i}(\boldsymbol{p}_i(t) - \boldsymbol{p}_j(t)),\\ \boldsymbol{p}_i(0) &= \boldsymbol{h}_i(0) - \sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_j^i(\epsilon) + \sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_i^j(\epsilon).\end{aligned}$$

In view of this, based on Lemma 1, one can obtain that the privacy attack model (A2) is only able to recover the signal $\boldsymbol{h}_i(t) - \sum_{j\in\mathbb{N}_i}\boldsymbol{\delta}_j^i(\epsilon) + \sum_{j\in\mathbb{N}_i}\boldsymbol{\delta}_i^j(\epsilon)$. Thus, the proof is completed. ■

Appendix B.2 Proof example of lagging errors

To better illustrate lagging errors, analyses on a state-of-the-art k-WTA network which adopts modified gradient [8] are given as follows. Specifically, the network in [8] can be written as

$$\dot{\boldsymbol{h}}(t) = -\kappa_{\mathrm{c}} S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t)), \tag{B11}$$

where $\boldsymbol{w}(t)$ and $\boldsymbol{h}(t)$ are the inputs and outputs of the k-WTA process, respectively; $\kappa_{\mathrm{c}} \in \mathbb{R}^{+}$ is a convergence parameter; $S_{\mathrm{c}} = E - B(B^{\mathrm{T}}B)^{-1}B^{\mathrm{T}}$ with an identity matrix E and B defined as

$$B = \begin{cases} [\boldsymbol{1}, \boldsymbol{x}(t) - \mathbb{P}_{\Xi}(\boldsymbol{x}(t))], & \text{if} \quad \boldsymbol{x}(t) \notin \Xi, \\ \boldsymbol{1}, & \text{if} \quad \boldsymbol{x}(t) \in \Xi, \end{cases}$$

where $\Xi = \{\boldsymbol{\varsigma} \in \mathbb{R}^m | 0 \leqslant \varsigma_i \leqslant 1\}$, and $\mathbb{P}_{\Xi}(\boldsymbol{x}(t)) = \operatorname{argmin}_{\boldsymbol{o}\in\Xi}\|\boldsymbol{h}(t) - \boldsymbol{o}\|_2$ is a projection operator. Moreover, this network has the following requirements for the initial state of $\boldsymbol{h}(t)$: $\boldsymbol{h}(0) \in \Xi$ and $\boldsymbol{1}^{\mathrm{T}}\boldsymbol{h}(0) = k$. Note that S_{c} is a symmetric matrix which has the following property:

$$S_{\mathrm{c}}S_{\mathrm{c}} = S_{\mathrm{c}}^{\mathrm{T}}S_{\mathrm{c}} = (E - B(B^{\mathrm{T}}B)^{-1}B^{\mathrm{T}})(E - B(B^{\mathrm{T}}B)^{-1}B^{\mathrm{T}}) = S_{\mathrm{c}}.$$

To explore the convergence of network (B11) for solving the k-WTA problem (Eq. (3) in the paper), an auxiliary Lyapunov function candidate is designed as $\mathbb{L}_{\mathrm{c}}(t) = \boldsymbol{\Upsilon}^{\mathrm{T}}(t)\boldsymbol{\Upsilon}(t)/2 \geqslant 0$ with $\boldsymbol{\Upsilon}(t) = S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t))$. Taking the time derivative of $\mathbb{L}_{\mathrm{c}}(t)$ generates

$$\begin{aligned} \dot{\mathbb{L}}_{\mathrm{c}}(t) &= \boldsymbol{\Upsilon}^{\mathrm{T}}(t)\dot{\boldsymbol{\Upsilon}}(t) \\ &= (S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t)))^{\mathrm{T}}(\alpha_{\mathrm{c}}S_{\mathrm{c}}\dot{\boldsymbol{h}}(t) + \alpha_{\mathrm{c}}\dot{S}_{\mathrm{c}}\boldsymbol{h}(t) - S_{\mathrm{c}}\dot{\boldsymbol{w}}(t) - \dot{S}_{\mathrm{c}}\boldsymbol{w}(t)) \\ &= -\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}(S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t)))^{\mathrm{T}}(S_{\mathrm{c}}S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t))) + (S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t)))^{\mathrm{T}}(\alpha_{\mathrm{c}}\dot{S}_{\mathrm{c}}\boldsymbol{h}(t) - S_{\mathrm{c}}\dot{\boldsymbol{w}}(t) - \dot{S}_{\mathrm{c}}\boldsymbol{w}(t)) \\ &= -\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2^2 + \boldsymbol{\Upsilon}^{\mathrm{T}}(t)(\dot{\boldsymbol{\Upsilon}}(t) - \alpha_{\mathrm{c}}S_{\mathrm{c}}\dot{\boldsymbol{h}}(t)). \end{aligned}$$

Considering that there exists an upper bound on the time variational rate of each deterministic and unknown variable, i.e., $\|\dot{\boldsymbol{\Upsilon}}(t)\|_2 \leqslant \nu_1$ and $\|\dot{\boldsymbol{h}}(t)\|_2 \leqslant \nu_2$, it can be obtained that

$$\begin{aligned} \dot{\mathbb{L}}_{\mathrm{c}}(t) &\leqslant -\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2^2 + \|\boldsymbol{\Upsilon}^{\mathrm{T}}(t)\|_2\|\dot{\boldsymbol{\Upsilon}}(t) - \alpha_{\mathrm{c}}S_{\mathrm{c}}\dot{\boldsymbol{h}}(t)\|_2 \\ &\leqslant -\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2^2 + \|\boldsymbol{\Upsilon}^{\mathrm{T}}(t)\|_2(\|\dot{\boldsymbol{\Upsilon}}(t)\|_2 + \alpha_{\mathrm{c}}\|S_{\mathrm{c}}\dot{\boldsymbol{h}}(t)\|_2) \\ &\leqslant -\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2^2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)\|\boldsymbol{\Upsilon}^{\mathrm{T}}(t)\|_2 \\ &= \|\boldsymbol{\Upsilon}(t)\|_2(-\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)), \end{aligned} \tag{B12}$$

where ν_3 is the Frobenius norm of S_{c}. In view of equation (B12), as $\boldsymbol{\Upsilon}(t)$ evolves over time, there will be three cases for $\dot{\mathbb{L}}_{\mathrm{c}}(t)$:

- $-\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3) > 0$: It means that $\dot{\mathbb{L}}_{\mathrm{c}}(t) > 0$ or $\dot{\mathbb{L}}_{\mathrm{c}}(t) < 0$. For the former, $\|\boldsymbol{\Upsilon}(t)\|_2$ increases until $-\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3) = 0$. For the latter, according to $\dot{\mathbb{L}}_{\mathrm{c}}(t) < 0$ and the Lyapunov theory, $\|\boldsymbol{\Upsilon}(t)\|_2$ infinitely approaches $(\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)/(\kappa_{\mathrm{c}}\alpha_{\mathrm{c}})$.
- $-\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3) = 0$: At this point, $\dot{\mathbb{L}}_{\mathrm{c}}(t) = 0$ and $\|\boldsymbol{\Upsilon}(t)\|_2 = (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)/(\kappa_{\mathrm{c}}\alpha_{\mathrm{c}})$ holds.
- $-\kappa_{\mathrm{c}}\alpha_{\mathrm{c}}\|\boldsymbol{\Upsilon}(t)\|_2 + (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3) < 0$: In this case, $\dot{\mathbb{L}}_{\mathrm{c}}(t) < 0$ so that $\|\boldsymbol{\Upsilon}(t)\|_2$ is bound to converge. Considering that $\|\boldsymbol{\Upsilon}(t)\|_2 > (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)/(\kappa_{\mathrm{c}}\alpha_{\mathrm{c}})$, $\|\boldsymbol{\Upsilon}(t)\|_2$ infinitely approaches $(\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)/(\kappa_{\mathrm{c}}\alpha_{\mathrm{c}})$.

In summary, for the residual error $\|\boldsymbol{\Upsilon}(t)\|_2$, it has $\lim\limits_{t\to\infty}\|\boldsymbol{\Upsilon}(t)\|_2 = \lim\limits_{t\to\infty}\|S_{\mathrm{c}}(\alpha_{\mathrm{c}}\boldsymbol{h}(t) - \boldsymbol{w}(t))\|_2 = (\nu_1 + \alpha_{\mathrm{c}}\nu_2\nu_3)/(\kappa_{\mathrm{c}}\alpha_{\mathrm{c}})$. Evidently, $\|\boldsymbol{\Upsilon}(t)\|_2$ is not 0 and varies with time. Hence, the k-WTA network (B11) is of less efficiency in solving the k-WTA problem (Eq. (2) in the paper) with dynamical inputs.

It is worth pointing out that although some k-WTA literatures have solved the lagging error problem [12], they are difficult to be distributed to meet the requirements of multi-robot distributed coordination due to the use of the nonlinear complementarity problem function to deal with inequality constraints. In view of the above discussions, we introduce the exponential penalty function to handle the inequality constraints of the k-WTA problem (Eq. (2) in the paper), and then construct a lagging-error-free and distributable k-WTA network.

Appendix C Simulations and experiments

In this section, comparisons with existing works are provided to verify the privacy protection capability and the lagging-error-free feature of the proposed DPP-kWTA network (Eq. (8) in the paper). In addition, simulations and experiments on a multi-robot platform are performed to further verify the effectiveness of the proposed network.

Appendix C.1 Comparisons

First of all, a comparison of the proposed DPP-kWTA network (Eq. (8) in the paper) with an existing distributed k-WTA network [13] based on numerical simulations is carried out. In particular, before presenting the simulation details, the

Table C1 Comparisons with Existing k-WTA Networks

	Publish year	Communication strategy	Considering privacy protection	Lagging errors	Application scenarios
Our work	—	Distributed	Yes	Free	Moblie robots
Network in [16]	2025	Distributed	No	Non-free	UAVs
Network in [17]	2024	Distributed	No	Non-free	Moblie robots
Network (C1) [13]	2023	Distributed	No	Non-free	NA$_+$
Network in [8]	2023	Centralized	No*	Non-free	NA$_+$
Network in [15]	2023	Distributed	No	Non-free	Robot arms
Network in [12]	2022	Centralized	No*	Free	NA$_+$
Network in [18]	2022	Centralized	No*	Non-free	Multi-agent
Network in [14]	2019	Distributed	No	Non-free	Multi-agent

No*: In a centralized k-WTA network, each individual directly interacts with a preset control center, which may also bring the risk of privacy leakage.
NA$_+$: This work is not further applied to specific scenarios.
UAVs: It is a shortened form of unmanned aerial vehicles.

distributed k-WTA network in [13] is provided as follows:

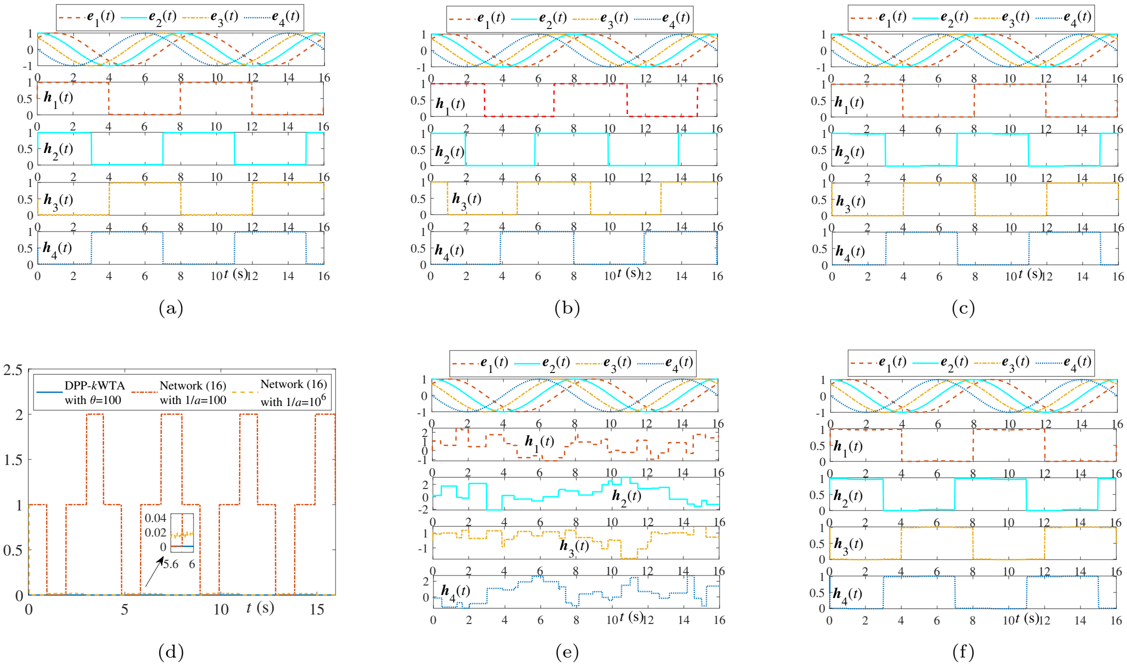
$$\begin{aligned} a\dot{\boldsymbol{y}}(t) &= -\boldsymbol{h}(t) + \frac{k\mathbf{1}_n}{n} - L\boldsymbol{y}(t), \\ \boldsymbol{h}(t) &= \Gamma(\boldsymbol{y}(t) + \frac{\boldsymbol{w}(t)}{\varpi}), \end{aligned} \tag{C1}$$

where $\boldsymbol{y}(t)$ is a state variable; $1/a$ is the convergence parameter; $\Gamma(\boldsymbol{\varepsilon})$ is a projection operation, which is able to be expressed as $\Gamma(\boldsymbol{\varepsilon}) = \text{argmin}_{\boldsymbol{\rho}\in\Upsilon}\|\boldsymbol{\varepsilon} - \boldsymbol{\rho}\|_2$ with $\Upsilon = \{\boldsymbol{\rho} \in \mathbb{R}^n \,|\, 0 \leqslant \boldsymbol{\rho}_i \leqslant 1,\, i = 1,\, 2,\, \cdots,\, n\}$. Furthermore, referring to model (A2), a privacy attack model in compact form for network (C1) is able to be designed as

$$\begin{aligned} \dot{\acute{\boldsymbol{y}}}(t) &= r_1\boldsymbol{\eta}(t) - r_2L\boldsymbol{y}(t) + r_3(\boldsymbol{y}(t) - \acute{\boldsymbol{y}}(t)), \\ \dot{\boldsymbol{\eta}}(t) &= -r_1\boldsymbol{\eta}(t) + r_2L\boldsymbol{y}(t) + r_3(\boldsymbol{y}(t) - \acute{\boldsymbol{y}}(t)), \\ \acute{\boldsymbol{h}}(t) &= -\boldsymbol{\eta}(t) + \frac{k\mathbf{1}_n}{n}, \end{aligned} \tag{C2}$$

where $\acute{\boldsymbol{h}}(t)$ and $\acute{\boldsymbol{y}}(t)$ are the estimates of $\boldsymbol{h}(t)$ and $\boldsymbol{y}(t)$, respectively; $\boldsymbol{\eta}(t)$ is a state variable; r_1, r_2, and r_3 are positive constant.

It is worth pointing out that, due to different construction methods of consensus-based distributed k-WTA networks, designs of corresponding privacy attack models are also different, such as model (A2) and model (C2). In fact, in a communication topology, if all individuals directly exchange information with their neighbors without any protective measures, such consensus-based distributed k-WTA networks are at risk of privacy attacks. Specifically, according to the communication topology in Fig. A1(a), the settings of the numerical simulations are as follows: the number of individuals participating in the competition is set to 4 ($n = 4$); the number of winners is set to 2 ($k = 2$); the i-th individual corresponds to the time-varying signal $\boldsymbol{e}_i(t) = \sin(0.25\pi(t + i))$, which is used as the input $\boldsymbol{w}_i(t)$ of the k-WTA networks. Moreover, for the proposed DPP-kWTA network (Eq. (8) in the paper), it has the following parameter settings: $\varpi = 0.002$; the parameters of the exponential penalty function are set to $\boldsymbol{\beta}_1 = \boldsymbol{\beta}_2 = \cdots = \boldsymbol{\beta}_{2n} = 0.05$ and $\kappa = 500$; the parameter ι of the consensus filter (Eq. (7) in the paper) is set to 100; the convergence parameter $\theta = 100$. In particular, for network (C1), as shown in Fig. C1(b), since its construction ignores the dynamic change of information, it has significant lagging errors under the same convergence parameter ($1/a = \theta = 100$) as DPP-kWTA network (Eq. (8) in the paper). More intuitively, as shown in Fig. C1(d), network (C1) fails to satisfy the constraint that the number of winners is k, that is, $|\mathbf{1}_n^{\mathrm{T}}\boldsymbol{h}(t) - k| \neq 0$ when the convergence parameter $1/a$ is 100, which means that network (C1) is not able to complete the k-WTA opeartion (Eq. (1) in the paper) commendably. In view of this, to better compare the performance of the two networks under privacy attacks in normal operation next, the convergence parameter of network (C1) is set large enough ($1/a = 100000$). Note that at this point, as shown in Fig. C1(c) and Fig. C1(d), network (C1) performs better than before. Nonetheless, in Fig. C1(d), for constraint $|\mathbf{1}_n^{\mathrm{T}}\boldsymbol{h}(t) - k| = 0$, network (C1) still has fluctuations compared to DPP-kWTA network (Eq. (8) in the paper). Furthermore, for DPP-kWTA network (Eq. (8) in the paper) and network (C1) with the convergence parameter $\theta = 100$ and $1/a = 100000$, privacy attack models (A2) and (C2) are used to obtain the information in Fig. C1(a) and Fig. C1(c), respectively, where $v_1 = v_2 = v_4 = 10000$, $v_3 = 100$, and $r_1 = r_2 = r_3 = 10000$. As shown in Fig. C1(e) and Fig. C1(f), privacy attack model (A2) is only able to obtain the encrypted information from DPP-kWTA network (Eq. (8) in the paper), while privacy attack model (C2) is basically able to restore the original information from network (C1), which indicates that the proposed DPP-kWTA network has the ability to protect the privacy of the key information.



(a) (b) (c)

(d) (e) (f)

Figure C1 Simulations based on the input $\boldsymbol{e}_i(t) = \sin(0.25\pi(t+i))$ $i = 1, 2, 3, 4$. (a) The output of the proposed DPP-kWTA network (Eq. (8) in the paper) with $\theta = 100$. (b) The output of network (C1) with $1/a = 100$. (c) The output of network (C1) with $1/a = 100000$. (d) $|\mathbf{1}_n^{\mathrm{T}}\boldsymbol{h}(t) - k|$ about DPP-kWTA network (Eq. (8) in the paper) ($\theta = 100$) and network (C1) ($1/a = 100$ and $1/a = 100000$). (e) The output of DPP-kWTA network (Eq. (8) in the paper) ($\theta = 100$) restored by privacy attack model (A2). (f) The output of network (C1) ($1/a = 100000$) restored by privacy attack model (C2).

Remark 2. When $1/a = 100$, as shown in Fig. C1(b), network (C1) is unable to accurately perform the k-WTA operation (Eq. (1) in the paper) due to the lagging errors. That is, the outputs of network (C1) can not satisfy the constraint $\sum_{i=1}^{n} \boldsymbol{h}_i(t) = k$. It further leads to the fact that the attack model (C2) does not obtain the accurate outputs in Fig. C1(b), but this phenomenon does not mean that network (C1) has the ability for privacy protection. It is meaningless to compare the privacy protection ability of network (C1) when it has already crashed. Therefore, in this section, to better compare the privacy protection performance of the proposed DPP-kWTA network (Eq. (8) in the paper) with that of network (C1), we set the convergence parameter $1/a$ large enough to suppress the lagging errors of network (C1) as much as possible.

Besides, in order to better show the differences and advantages of the proposed DPP-kWTA network (Eq. (8) in the paper) compared to existing works, a comparative table is provided. As shown in Table I, although [13–17] realize the distribution of the k-WTA networks based on consensus methods, these networks have lagging errors when performing the k-WTA operation (Eq. (1) in the paper) because they do not consider the characteristics of dynamic inputs when constructed. This problem also exists in the centralized works [8, 18]. Although [12] overcomes the problem of lagging errors, it is a centralized k-WTA network and not further applied to scenarios with dynamic inputs. Moreover, the above works all carry out direct information interaction, which means that there are risks of privacy disclosure. Overall, the above discussions demonstrate the advantages of the proposed DPP-kWTA network (Eq. (8) in the paper).

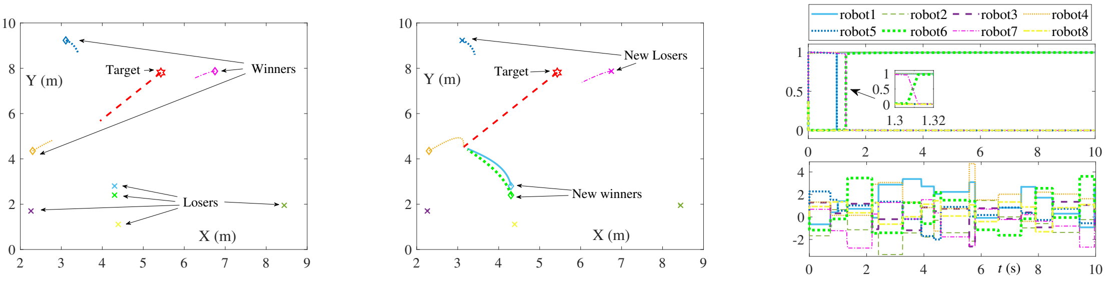
Appendix C.2 Applications to Multi-Robot Task Allocation

To verify the effectiveness of the proposed DPP-kWTA network (Eq. (8) in the paper), simulations of a target capture task based on multiple mobile robots are demonstrated. Specifically, the task is set up as follows: the number of robots is $n = 8$; the number of winners selected to perform the task is $k = 3$; the initial positions of eight robots are randomly generated as $[(4.3, 2.8); (8.44, 1.95); (2.26, 1.7); (2.3, 4.35); (3.11, 9.23); (4.3, 2.4); (6.75, 7.87); (4.39, 1.11)]$ m; the initial position of the target is randomly generated as $(5.43, 7.81)$ m; the communication topology is presented in Fig. A1(b). Moreover, the other parameters are the same as the settings in the numerical simulations. In particular, for i-th robot, it has the following equation:

$$\dot{\varsigma}_i(t) = -\varrho \boldsymbol{h}_i(t) \frac{\varsigma_i(t) - \varsigma_0(t)}{\|\varsigma_i(t) - \varsigma_0(t)\|_2}, \tag{C3}$$

where $\varsigma_i(t)$ is the position vector of the i-th robot so that $\dot{\varsigma}_i(t)$ represents the velocity vector; $\varsigma_0(t)$ is the position vector of the target; ϱ is a positive parameter. It is worth pointing out that in this task, the k robots closest to the target at the current moment are expected to be chosen as winners to perform the task. Thus, for the i-th robot, the input to DPP-kWTA network (Eq. (8) in the paper) is set to

$$\boldsymbol{w}_i(t) = -\|\varsigma_i(t) - \varsigma_0(t)\|_2. \tag{C4}$$



(a) (b) (c)

Figure C2 Simulations based on mobile robots. (a) At the beginning of the task, the three robots ($k = 3$) closest to the target track and surround the target. (b) As the target moves, two new winners replace the previous two robots to perform the task and the target is eventually captured. (c) The outputs $\boldsymbol{h}(t)$ of DPP-kWTA network (Eq. (8) in the paper) and the information recovered by privacy attack model (A2).

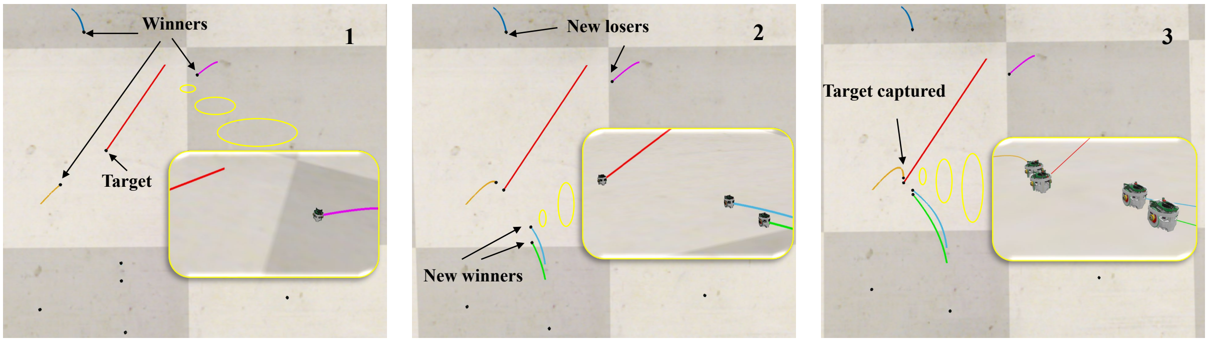


Figure C3 Snapshots of simulations based on CoppeliaSim platform and E-puck2 robots.

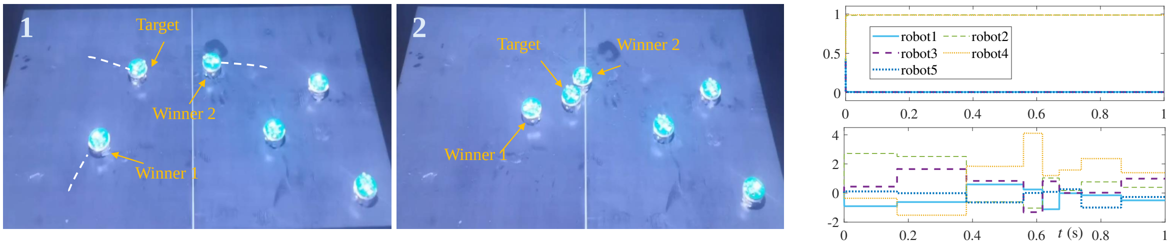
Specifically, as shown in Fig. C2(a), at the beginning of the task, according to the input of each robot (C4), three robots start to track and surround the target. Then, the input of each robot (C4) changes due to the movement of the target and the robots, which leads to a change in the robots performing the task as performed in Fig. C2(b). That is, new winners are generated to replace the robots that are no longer suitable to continue the task. Overall, the output $\boldsymbol{h}_i(t)$ of DPP-kWTA network (Eq. (8) in the paper) that controls whether the i-th robot acts or not is presented in the subgraph of the upper half of Fig. C2(c). Similarly, as demonstrated in another subgraph of Fig. C2(c), privacy attack model (A2) is not able to obtain these output information from the direct information interaction among robots. Besides, to make the simulation in Fig. (C2) more visual, the snapshots of simulations based on Coppliasim platform and E-puck2 robots are provided in Fig. C3.

Furthermore, a physical experiment based on six E-puck2 robots is performed, where five robots ($n = 5$) compete and produce two individuals ($k = 2$) that perform a target capture task, while the other one is set as the target. In particular, the communication topology is presented in Fig. A1(c), while the other network parameters are the same as the settings in the simulations. Concretely, as shown in Fig. C4, on a platform with a size of 1.5 m × 0.9 m, facing a target coming from the top left of the platform, the two closest robots start to surround the target and one of them successfully captures it. Therefore, this experiment further verifies the feasibility of the proposed DPP-kWTA network (Eq. (8) in the paper).

Remark 3. In a multi-robot system, the privacy protection is more inclined to protect the real-time strategies and control laws of multiple robots. Therefore, although [6] can also be used to encrypt the output of the k-WTA network to prevent the attacker from obtaining the actual output, as shown in Fig. A2, it cannot hide the control laws of the k-WTA network, that is, the robot with a higher output state performs the task, and the robot with a lower output state is on standby. In contrast, the method we propose does better in this regard. From another perspective, in scenarios where the node state information changes slowly and continuously, [6] is more advantageous than our method.

Appendix D Discussions on future research directions

We will discuss the possible future research directions from two aspects. On the one hand, from an application perspective, the proposed distributed privacy-preserving k-WTA network (Eq. (8) in the paper) can be further extended to different scenarios. For instance, the inputs of the k-WTA network can not only be limited to the distance between each robot and the target. The robots' own attributes such as their battery levels can also be incorporated into the inputs. Moreover, the task allocation objects of the k-WTA network can be further expanded to different robots, such as redundant robots, to complete more complex tasks. On the other hand, the proposed dynamic privacy-preserving consensus filter (Eq. (8) in the paper) utilizes the symmetry of the undirected graph Laplacian matrix to construct a random number sequence,



(a) (b)

Figure C4 Physical experiment based on six E-puck2 robots where five robots compete and produce two individuals that perform a target capture task, while the other one is set as the target. (a) Snapshots of the experiment. (b) The outputs $\boldsymbol{h}(t)$ of DPP-kWTA network (Eq. (8) in the paper) and the information recovered by the privacy attacker based on privacy attack model (A2).

which not only protects privacy but also ensures that the accuracy of the average consensus is not affected. This encryption mechanism based on random number switching can also be applied to other distributed k-WTA networks. To prove this point, we attempted to apply this encryption mechanism to an existing k-WTA work [14].

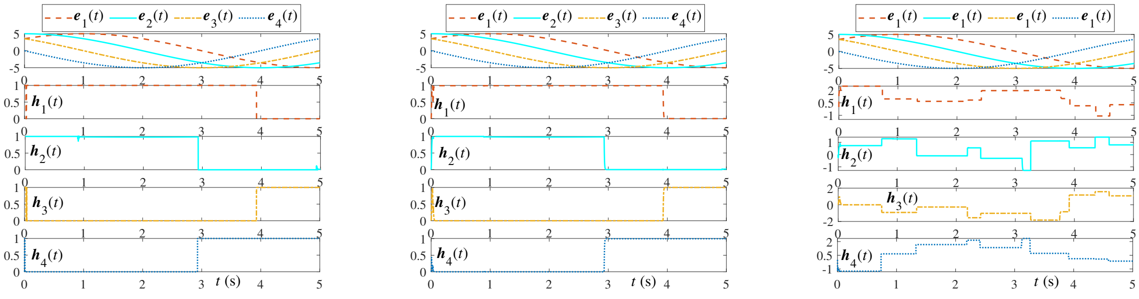
Specifically, in [14], a distributed k-WTA network model is presented as follows:

$$\begin{aligned}
&\nu_1\dot{\boldsymbol{r}}(t) = -\boldsymbol{\phi}(t) + \frac{k\mathbf{1}_n}{n},\\
&\dot{\boldsymbol{\phi}}(t) = \nu_2(\boldsymbol{h}(t) - \boldsymbol{\phi}(t)) - \nu_3 L(\boldsymbol{\phi}(t) + \boldsymbol{\psi}(t)),\\
&\dot{\boldsymbol{\psi}}(t) = -L\boldsymbol{\phi}(t),\\
&\boldsymbol{h}(t) = \Gamma(\boldsymbol{r}(t) + \frac{\boldsymbol{w}(t)}{\varpi}),
\end{aligned} \tag{D1}$$

where $\boldsymbol{r}(t)$ is the state variable; $\boldsymbol{\phi}(t)$ and $\boldsymbol{\psi}(t)$ are the interaction information among nodes; ν_1, ν_2, and ν_3 are positive constants. $\Gamma(\boldsymbol{\varepsilon})$ is a projection operation, which is able to be expressed as $\Gamma(\boldsymbol{\varepsilon}) = \text{argmin}_{\boldsymbol{\rho}\in\chi}\|\boldsymbol{\varepsilon} - \boldsymbol{\rho}\|_2$ with $\chi = \{\boldsymbol{\rho} \in \mathbb{R}^n \,|\, 0 \leqslant \boldsymbol{\rho}_i \leqslant 1,\ i = 1, 2, \cdots, n\}$. Correspondingly, we designed a model that functionally resembles the attack model (A2), which can utilize the interaction information $\boldsymbol{\phi}(t)$ and $\boldsymbol{\psi}(t)$ among nodes to estimate the output $\boldsymbol{h}(t)$ of the k-WTA network model (D1). Specifically, it is as follows:

$$\begin{aligned}
&\dot{\acute{\boldsymbol{\phi}}}(t) = \chi_1(\acute{\boldsymbol{h}}(t) - \boldsymbol{\phi}(t)) - \chi_2 L(\boldsymbol{\phi}(t) + \boldsymbol{\psi}(t)) + \chi_3(\boldsymbol{\phi}(t) - \acute{\boldsymbol{\phi}}(t)),\\
&\dot{\acute{\boldsymbol{h}}}(t) = \chi_1(\acute{\boldsymbol{\phi}}(t) - \acute{\boldsymbol{h}}(t)) + \chi_2 L(\boldsymbol{\phi}(t) + \boldsymbol{\psi}(t)),
\end{aligned} \tag{D2}$$

where $\acute{\boldsymbol{\phi}}(t)$ and $\acute{\boldsymbol{h}}(t)$ are the estimates of the privacy attack model for $\boldsymbol{\phi}(t)$ and $\boldsymbol{h}(t)$, respectively, and χ_1, χ_2, and χ_3 are positive constants. Furthermore, to verify the privacy-stealing effect of the attack model (D2) on the k-WTA network model (D1), we conducted a numerical simulation. In this simulation, the number of network nodes is four ($n = 4$), and the number of winners is two ($k = 2$). Meanwhile, the other parameter settings are as follows: the inputs of the four network nodes are set to $\boldsymbol{e}_i(t) = 5\sin(0.25\pi(t + i))$ with $i = 1, 2, 3, 4$; the communication topology is shown in Fig. A1(a); $\varpi = 0.002$; $\nu_1 = 10^{-6}$; $\nu_2 = 200$; $\nu_3 = 10^6$; $\chi_1 = 200$; $\chi_2 = 10^6$; $\chi_3 = 10^5$. As shown in Fig. D1(a) and Fig. D1(b), the privacy attack model (D2) can successfully estimate the output $\boldsymbol{h}(t)$ of the k-WTA network model (D1). Based on this, we



(a) (b)

Figure D1 Simulations based on the input $\boldsymbol{e}_i(t) = 5\sin(0.25\pi(t + i))$ $i = 1, 2, 3, 4$. (a) The output of model (D1). (b) The output estimated by the attack model (D2) when targeting model (D1). (c) The output estimated by the attack model (D2) when targeting model (D3).

consider combining the random number switching encryption mechanism with the k-WTA network model (D1) to obtain the following new model:

$$\begin{aligned}
&\nu_1\dot{\boldsymbol{r}}(t) = -\tilde{\boldsymbol{\phi}}(t) + \frac{k\mathbf{1}_n}{n},\\
&\dot{\boldsymbol{\phi}}(t) = \nu_2(\boldsymbol{h}(t) - \boldsymbol{\phi}(t)) - \nu_3 L(\tilde{\boldsymbol{\phi}}(t) + \boldsymbol{\psi}(t)),\\
&\dot{\boldsymbol{\psi}}(t) = -L\tilde{\boldsymbol{\phi}}(t),\\
&\tilde{\boldsymbol{\phi}}(t) = \boldsymbol{\phi}(t) - \sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_j^i(\epsilon) + \sum\nolimits_{j\in\mathbb{N}_i}\boldsymbol{\delta}_i^j(\epsilon),\\
&\boldsymbol{h}(t) = \Gamma(\boldsymbol{r}(t) + \frac{\boldsymbol{w}(t)}{\varpi}),
\end{aligned} \tag{D3}$$

where $\boldsymbol{\delta}_j^i$ and $\boldsymbol{\delta}_i^j$ are sequences of random numbers transmitted to the i-th node by the j-th node and to the j-th node by the i-th node, respectively, with the j-th node being a neighbor of the i-th one. Evidently, for encrypted model (D3), the interaction information among nodes obtained by the attack model (D2) becomes $\tilde{\boldsymbol{\phi}}(t)$. At this point, as shown in Fig. 2(c), the attack model (D2) is no longer able to accurately estimate the output of the encrypted model (D3). Overall, the above discussions have verified that the proposed privacy protection mechanism is not limited to a single attack model, and it has certain scalability. It is worth noting that model (D3) can also be referred to as a distributed privacy-preserving k-WTA network. However, it still faces the problem of the lagging errors. Therefore, in terms of performance, it is inferior to the proposed DPP-kWTA network (Eq. (8) in the paper). Furthermore, in addition to the k-WTA networks, in other scenarios [19] where the accurate dynamic average consensus needs to be used and the privacy protection is required, the proposed method may also have certain reference value.

However, it is worth noting that when referring to the encryption mechanism based on random number switching, it still have some limitations. For example, in order to ensure that privacy is protected without affecting the outcome of the average consensus, it relies on the symmetry of the Laplacian matrix and the random number sequence initialized for each network node. Therefore, its application is limited to static undirected graphs. However, considering the variability and complexity of the task environment, in many cases, it is necessary to design and explore dynamic privacy-preserving consensus filters based on directed topologies or time-varying topologies. Besides, since this privacy protection mechanism mainly considers the attack method where an attacker infers the state information of nodes by eavesdropping on the interaction information among nodes, when facing possible direct attacks on the nodes, this method is no longer applicable.

References

1 Shi X, Li Y, Du C. Cooperative output regulation of heterogeneous directed multi-agent systems: A fully distributed model-free reinforcement learning framework. Sci China Inf Sci, 2025, 68, 122202.

2 Wang L, Liu Z, Yuan S, et al. Distributed Nash equilibrium for pursuit-evasion game with one evader and multiple pursuers. Sci China Inf Sci, 2025, 68, 192205.

3 Mo Y, Murray R M. Privacy preserving average consensus. IEEE Trans. Autom. Control, 2017, 62: 753–765.

4 Wang A, He H, Liao X. Event-triggered privacy-preserving average consensus for multiagent networks with time delay: An output mask approach. IEEE Trans. Syst., Man, Cybern. Syst., 2021, 51: 4520–4531.

5 Wang Y. Privacy-preserving average consensus via state decomposition. IEEE Trans. Autom. Control, 2019, 64: 4711–4716.

6 Zhang K, Li Z, Wang Y, et al. Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control. Automatica, 2022, 139: 110182.

7 Gao L, Zhou Y, Chen X, et al. Privacy-preserving dynamic average consensus via random number perturbation. IEEE Trans Circuits Syst II, Exp Briefs, 2023, 70: 1490–1494.

8 Zhang Y, Li S, Geng G. Initialization-based k-winners-take-all neural network model using modified gradient descent. IEEE Trans Neural Netw Learn Syst, 2023, 34: 4130–4138.

9 Li W, Ma X, Comparisons of slack variable, NCP function, and penalty function based ZNNs for solving equality-and inequalityconstrained QP problems with robotic applications. In: Proceedings of the 7th IEEE International Conference on Advanced Robotics and Mechatronics (ICARM), Guilin, Guangxi, China, 2022, pp. 226–231.

10 Han S P, Mangasarian O L. Exact penalty functions in nonlinear programming. Math. Program., 1979, 17: 251–269.

11 Boyd S, Vandenberghe L. Convex optimization. Cambridge university press, 2004.

12 Liu M, Shang M. On RNN-based k-WTA models with time-dependent inputs. IEEE/CAA J Autom Sinica, 2022, 9: 2034–2036.

13 Zhang Y, Li S, Zhou X, et al. Single-state distributed k-winners-take-all neural network model. Inf Sci, 2023, 647: 119528.

14 Jin L, Li S, La M H, et al. Dynamic task allocation in multi-robot coordination for moving target tracking: a distributed approach. Automatica, 2019, 100: 75–81.

15 Kong Y, Zhang C, J. Zhou, et al. Comprehensive understanding of a distributed k-WTA strategy in a competitive behavior. Commun Nonlinear Sci Numer Simul, 2023, 125: 107382.

16 Tan N, Liu Y, Hu R, et al. Multitarget pursuit-evasion based on distributed and competitive mechanisms. IEEE Trans Syst, Man, Cybern Syst, 2024, 54: 5989–6000.

17 Liu K, Zhang Y. Distributed dynamic task allocation for moving target tracking of networked mobile robots using k-WTA network. IEEE Trans Neural Netw Learn Syst, 2025, 36: 5795-5802.

18 Zhao X, Zong Q, Tian B, et al. Finite-time dynamic allocation and control in multiagent coordination for target tracking. IEEE Trans Cybern, 2022, 52: 1872–1880.

19 Liu M, Ma D, Zhang H, et al. Dynamic average consensus-Based reactive power sharing and voltage regulation method in the microgrid. IEEE Trans Ind Inform, doi: 10.1109/TII.2025.3593883.