Topology-Preserving Motion Coordination for Multi-Robot Systems in Adversarial Environments

Zitong Wang, Yushan Li, Xiaoming Duan, and Jianping He

***Abstract*—The interaction topology plays a significant role in the distributed motion coordination of multi-robot systems (MRSs) for its noticeable impact on the information flow between robots. However, recent research has revealed that in adversarial environments, the topology can be inferred by external adversaries equipped with advanced sensors, posing severe security risks to MRSs. Therefore, it is of utmost importance to preserve the interaction topology from inference attacks while ensuring the coordination performance. To this end, we propose a topology-preserving motion coordination (TPMC) algorithm that strategically introduces perturbation signals during the coordination process with a compensation design. The major novelty is threefold: i) We focus on the second-order motion coordination model and tackle the coupling issue of the perturbation signals with the unstable state updating process; ii) We develop a general framework for distributed compensation of perturbation signals, strategically addressing the challenge of perturbation accumulation while ensuring precise motion coordination; iii) We derive the convergence conditions and rate characterization to achieve the motion coordination under the TPMC algorithm. Extensive simulations and real-world experiments are conducted to verify the performance of the proposed method.**

***Index Terms*—Multi-robot systems; interaction topology; topology preservation; signal processing; inference attack.**

I. Introduction

A. Background

Over the past few decades, the motion coordination of multi-robot systems (MRSs) has received considerable attention in both civil and military fields, such as robotic surveillance and search [2]–[4], swarm flocking and rendezvous [5]–[7], unmanned warehousing [8] and cooperative localization [9]. In these applications, each robot has limited sensing and communication capacities and needs to coordinate with others through interactions to accomplish specific tasks. In particular, the interaction topology of the MRS characterizes the information flow among robots, and the sensed and received information are processed for achieving further coordination behaviors. The significance of the interaction topology of MRSs is reflected in its impact on autonomy, adaptation, scalability, and efficiency [10].

Although the onboard sensors enable MRSs to achieve cooperative tasks, they can also be maliciously utilized by external adversaries to measure the motion information of MRSs (e.g., displacements and velocities) in the open space. Based on the collected information, the adversaries can further disclose the sensitive interaction topology by the latest inference methods to support more severe and precise attacks [11], leading to severe security breaches. For instance, armed with knowledge of the topology, adversaries can predict the future states of critical robots and execute precise interceptions [12]. Alternatively, they can hijack the important communication links, thereby incapacitating the system [13]. In the load transportation task [14], the attack on the interaction topology will limit the throughput of the transportation network. Similarly, in the surveillance scenarios [3], simple physical attacks can result in hampering surveillance efficiency. Such attacks can severely deteriorate the coordination performance of MRSs, underscoring the importance of topology preservation.

In this paper, we consider a scenario where the sensitive interaction topology of MRSs is vulnerable to being inferred by external adversaries and aim to protect the interaction topology by designing disturbance signals while not harming the motion coordination performance.

B. Motivation

The problem we are addressing is primarily motivated by the fact that the interaction topology of MRSs may be disclosed in adversarial environments. To mitigate the potential security risks resulting from the topology inference attack, it is of great importance to develop more secure algorithms that efficiently protect the actual topology while simultaneously maintaining motion coordination performance for real-world applications.

However, in real-world systems, the topology-preserving problem remains an open issue. Multi-robot systems in practical scenarios often exhibit more complex dynamics than first-order systems, which consequently pose challenges in deriving theoretical results. Furthermore, existing methods in recent literature may not be directly applicable to solving topology-preserving problems in real-world systems due to the disparities in system characteristics and objectives, bringing difficulties in the algorithm design.

C. Related Works

Topology inference methods: Since the MRS is a typical network system, various studies aimed at estimating interaction topology based on accessible observation data can be

This work was supported in part by Shanghai Pujiang Program under Grant 22PJ1404900, the Natural Science Foundation of Shanghai under Grant 23ZR1428900, and the National Natural Science Foundation of China under Grant 62373247 and 62303314. (Corresponding author: Jianping He.)

The authors are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai, China. E-mail address: {wangzitong, yushan_li, xduan, jphe}@sjtu.edu.cn.

The preliminary version of this work was presented at the 62nd IEEE Conference on Decision and Control, 2023 [1]. This paper has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors. The material includes a video of a real-world experiment.

leveraged for topology inference, such as the spectral analysis-based approach [15], causality-based estimator [16], identification method [17], reinforcement learning [18], etc. Numerous researchers have explored the utilization of graphical models to depict relationships between various variables and adopt graph signal processing (GSP) techniques to deduce the concealed topology, as in references [19]–[21]. The primary idea underlying these works is utilizing the information of the sample correlation matrix and subsequently reconstructing the topology. Vector autoregressive analysis [22], [23] also stands as a prevalent tool in this context.

Defense methods: Researchers have addressed specific security issues for the cooperative control of MRSs, such as protecting the privacy of agents [24], [25], bolstering resilience against false data injection attacks [26], and enhancing robustness in dealing with intermittent communications and actuator faults [27]. In these defense mechanisms, dynamic topology and noise-adding algorithms are two commonly employed methods. In the former approach, the interaction topology of the MRS changes over time, significantly increasing the uncertainty regarding the states of the agents, thereby enhancing protection for the MRS [28]–[30]. These methods usually exhibit a strong dependence on topology connectivity and can become complex. On the other hand, noise-adding algorithms add additional noisy signals to the states of the robots, obscuring the state information from potential adversaries [24], [25], [31], [32]. For example, the authors in [24] propose a differential privacy scheme based on Laplace noise to preserve the privacy of the agents' states. For example, a noise-adding algorithm is introduced to preserve the privacy of the initial states while achieving exact average consensus in the sense of mean square convergence in [25].

Topology-preserving approaches: Noise-adding methods are promising choices for designing the topology-preserving motion coordination algorithm due to their flexibility and effectiveness in addressing specific requirements without a strong dependence on topology. Note that although the popular differential privacy has been widely used to characterize the data privacy in noise-adding mechanisms, it is not appropriate to characterize the privacy of an inferred topology, which is highly nonlinear about the system states. Recent work [33] has made prior efforts to preserve the topology of first-order multi-agent systems under the inference error metric. However, the proposed algorithm can not be directly applied to second-order MRSs. This difficulty is caused by the differences between the first-order dynamics and the second-order dynamics. In second-order dynamics, the accumulative effect of the perturbation signals across different dimensions can ultimately deteriorate the convergence of the coordination algorithm. Thus, how to preserve the topology of second-order MRSs remains an open issue.

D. Contribution

Motivated by the above discussions, this paper focuses on achieving topology-preserving motion coordination in MRSs by designing perturbation signals. Specifically, we propose a distributed topology-preserving motion coordination (TPMC) algorithm that leverages sensor data and designs strategically dependent self-compensating perturbation signals, which effectively conceals the actual topology structure from the inference attack without sacrificing the performance of motion coordination. The primary challenge in designing this algorithm is to retain precise motion coordination in a distributed manner while maximizing protection against inference attacks.

Some preliminary results of this paper have been presented in [1], which gives specific algorithm examples that are suitable for undirected networks. In this paper, we extend the previous approach to general directed networks and provide corresponding theoretical guarantees and experimental validations. The main contributions of our work can be summarized as follows:

- We address the problem of topology preservation for MRSs with second-order dynamics, and we propose a distributed algorithm that protects the interaction topology while guaranteeing coordination performance. Both finite and infinite perturbation signals are considered for the preservation design.
- By exploiting the sufficient and necessary conditions on added perturbation signals for achieving precise motion coordination, we propose a general self-compensating perturbation design for the state-updating process of each robot without relying on global system knowledge.
- We obtain the convergence rate of the MRS under the designed perturbation signals, and derive the relationship between the inference errors and the number of observations. Representative simulations and real-world experiments demonstrate the effectiveness of the proposed algorithm when dealing with various attacks with the inferred topology.

Notation: Let $\mathbf{1}$ be an all-one column vector, and $\mathbf{0}$ be an all-zero column vector with compatible dimensions. Let $\mathbb{N}$ and $\mathbb{N}^+$ represent the sets of non-negative integers and positive integers, respectively. Let $\mathbb{R}$ be the set of real numbers. Let $\|\cdot\|$ and $\|\cdot\|_F$ represent the spectral norm and Frobenius norm of a matrix, respectively. For two functions $f(x)$ and $g(x)$, $f(x) = \mathcal{O}(g(x)), x \to \infty$ means that there exists a positive real number M and a real number x_0 such that $\|f(x)\| \leq Mg(x), \forall x \geq x_0$.

The remainder of this paper is organized as follows: Section II provides essential preliminary information and the problem formulation. The proposed algorithm and its analysis are in Section III and Section IV, respectively. Section V shows the simulations and real-world experiments of the algorithm. Finally, Section VI concludes the work.

II. Preliminaries

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a directed graph that models the topology information within the multi-robot system, where $\mathcal{V} = \{1, \ldots, N\}$ is the set of nodes and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of edges. Each node represents a robot, and each edge $(i, j) \in \mathcal{E}$ indicates that a robot i will utilize the sensor to measure the state information of robot j. The weight of the edge indicates to which degree the sensor data is utilized. The adjacency matrix $A_{\mathcal{G}} = [a_{ij}]_{N\times N}$ of a graph $\mathcal{G}$ with N robots specifies the interaction topology of the system, where $a_{ij} > 0$ if $(i, j) \in \mathcal{E}$, otherwise $a_{ij} = 0$. Let $\mathcal{N}_i = \{j \mid (i, j) \in \mathcal{E}\}$ be the neighbor set of robot i and $d_i = |\mathcal{N}_i|$ be its in-degree. Define the Laplacian matrix of $\mathcal{G}$ by $L_{\mathcal{G}} = D_{\mathcal{G}} - A_{\mathcal{G}}$, where $D_{\mathcal{G}}$ is the diagonal matrix of all in-degrees.

A. Motion Coordination Algorithm

In this section, we introduce a basic motion coordination algorithm with second-order dynamics where robots are driven to a prescribed formation. Consider a network of N robots whose interaction relationship is captured by a graph $\mathcal{G}$ with N nodes. Each robot i is a double-integrator described by

$$\dot{p}_i(t) = v_i(t), \quad \dot{v}_i(t) = u_i(t), \quad \forall i \in \mathcal{V}, \tag{1}$$

where $p_i(t) \in \mathbb{R}$ and $v_i(t) \in \mathbb{R}$ are the position and velocity of robot i at time $t \geq 0$, respectively, and $u_i(t) \in \mathbb{R}$ is the corresponding control input signal.

Since control input signals are applied at discrete sampling times in practice, we discretize the dynamics with sampling period T [34]. The system (1) then becomes:

$$\begin{cases} p_i(k+1) = p_i(k) + Tv_i(k) + \frac{T^2}{2}u_i(k), & \forall i \in \mathcal{V}, \\ v_i(k+1) = v_i(k) + Tu_i(k), & \forall i \in \mathcal{V}, \end{cases} \tag{2}$$

where $p_i(k), v_i(k), u_i(k)$ are the position, velocity, and control input signal for robot i at time $t = kT$, respectively. Let Δ_{ij} be the desired position deviation between robot i and robot j in a formation. The objective of the motion coordination algorithm is to drive the robots to the following desired pattern

$$\begin{cases} \lim\limits_{k\to\infty} [p_i(k) - p_j(k)] = \Delta_{ij}, & \forall i, j \in \mathcal{V}, \\ \lim\limits_{k\to\infty} [v_i(k) - v_j(k)] = 0, & \forall i, j \in \mathcal{V}. \end{cases} \tag{3}$$

To simplify the notation, we use the relative position $\tilde{p}_i(k) = p_i(k) - \eta_i$ of robot i in the rest of this paper, where $\eta_i - \eta_j = \Delta_{ij}$. The following algorithm which considers the relative positions and velocities is adopted for motion coordination:

$$u_i(k) = -\sum_{j\in\mathcal{V}} a_{ij} \left[(\tilde{p}_i(k) - \tilde{p}_j(k)) + \alpha(v_i(k) - v_j(k))\right], \tag{4}$$

where α is a positive scalar. In this algorithm, robots seek to achieve the prescribed formation by sensing the relative positions and velocities of the neighbors and leveraging the sensor data to design control input signals. The discrete-time system model (2) under the algorithm (4) can be written in the following matrix form:

$$\begin{bmatrix} \tilde{p}(k+1) \\ v(k+1) \end{bmatrix} = \underbrace{\begin{bmatrix} I_N - \frac{T^2}{2}L_{\mathcal{G}} & TI_N - \alpha\frac{T^2}{2}L_{\mathcal{G}} \\ -TL_{\mathcal{G}} & I_N - \alpha TL_{\mathcal{G}} \end{bmatrix}}_{G} \begin{bmatrix} \tilde{p}(k) \\ v(k) \end{bmatrix}, \tag{5}$$

where $\tilde{p}(k) = \begin{bmatrix} \tilde{p}_1(k) & \cdots & \tilde{p}_N(k) \end{bmatrix}^\intercal$ is the concatenated relative position vector, $v(k) = \begin{bmatrix} v_1(k) & \cdots & v_N(k) \end{bmatrix}^\intercal$ is the concatenated velocity vector, and I_N is an identity matrix.

Assumption 1. *Graph $\mathcal{G}$ has a directed spanning tree and $L_{\mathcal{G}}$ has eigenvalues $\lambda_1 = 0$ and $0 < |\lambda_2| \leq \cdots \leq |\lambda_N|$.*

Define two sets,

$$Q_r = \bigcap_{\substack{\forall \mathrm{Re}(\lambda_i)>0 \\ \mathrm{Im}(\lambda_i)=0}} \left\{(\alpha, T) \mid \frac{T}{2} < \alpha < \frac{2}{\lambda_i T}\right\}, \tag{6a}$$

$$Q_c = \bigcap_{\substack{\forall \mathrm{Re}(\lambda_i)>0 \\ \mathrm{Im}(\lambda_i)\neq0}} \left\{(\alpha, T) \mid \frac{T}{2} < \alpha < \frac{\phi(\lambda_i)}{T}\right\}, \tag{6b}$$

where $\phi(\lambda_i) \triangleq -\frac{8\mathrm{Im}(\lambda_i)^2}{|\lambda_i|^4(T-2\alpha)^2} + \frac{2\mathrm{Re}(\lambda_i)}{|\lambda_i|}$. The following lemma provides the necessary and sufficient conditions for convergence for motion coordination of the MRS.

Lemma 1. *(Theorem 4.2 in [34]) Under Assumption 1, the desired coordination* (3) *can be achieved asymptotically if and only if the parameters $(\alpha, T) \in Q_c \cap Q_r$. Specifically, the velocities and the relative positions of the robots satisfy*

$$\begin{cases} \lim\limits_{k\to\infty} |v_i(k) - \boldsymbol{w}^\intercal v(0)| = 0, & \forall i \in \mathcal{V}, \quad (7a) \\ \lim\limits_{k\to\infty} |\tilde{p}_i(k) - (\boldsymbol{w}^\intercal \tilde{p}(0) + kT\boldsymbol{w}^\intercal v(0))| = 0, & \forall i \in \mathcal{V}, \quad (7b) \end{cases}$$

where $\begin{bmatrix} \boldsymbol{w}^\intercal & \mathbf{0}_N^\intercal \end{bmatrix}^\intercal \in \mathbb{R}^{2N}$ is the left eigenvector of the matrix G associated with $\mu_1 = 1$ satisfying $\boldsymbol{w}^\intercal \mathbf{1}_N = 1$.

Lemma 1 shows that the desired states of the robots in motion coordination are the weighted sums of initial relative velocities and positions of robots in the system, respectively. It is worth noting that (6a) and (6b) are not difficult to satisfy when T is much smaller than 1 and α is chosen properly.

B. Topology Inference Mechanism

Under the motion coordination algorithm, the system model can also be written as:

$$\begin{bmatrix} \tilde{p}(k) \\ v(k) \end{bmatrix} = G^k \begin{bmatrix} \tilde{p}(0) \\ v(0) \end{bmatrix}. \tag{8}$$

The motion coordination process (8) tightly couples with the interaction topology among the robots, and the changes in the relative positions and velocities may reveal important information about the underlying topology of the MRS.

The objective of the adversaries is to obtain the Laplacian matrix $L_{\mathcal{G}}$ of the graph $\mathcal{G}$. In the MRS, the parameters α and T, as well as the Laplacian matrix $L_{\mathcal{G}}$ are all unknown to the adversaries. The parameter T can be identified from observations. The difficulty regarding obtaining the unknown parameter α can be circumvented through inferring the matrix G and subsequently extracting the related matrix $L_{\mathcal{G}}$ from part of G. Consider the scenario where adversaries collect all the position and the velocity data from time 0 to time k and then use the Ordinary Least Squares (OLS) estimator to regress the Laplacian matrix $L_{\mathcal{G}}$. Let $x(k) = \begin{bmatrix} \tilde{p}(k)^\intercal & v(k)^\intercal \end{bmatrix}^\intercal$. Stack the vectors and denote $Y(k) = \begin{bmatrix} x(0) & \cdots & x(k-1) \end{bmatrix}$ and $Z(k) = \begin{bmatrix} x(1) & \cdots & x(k) \end{bmatrix}$. Specifically, we use the notations $Y_\theta(k)$ and $Z_\theta(k)$ when perturbation signals $\theta(k)$ are added to show the difference between the original data and the perturbed data. The regression problem is formulated as:

$$\min_{\hat{G}(k)} \left\| \hat{G}(k)Y_\theta(k) - Z_\theta(k) \right\|_F^2. \tag{9}$$

In the above equation, $\hat{G}(k)$ is the inferred matrix based on data from time 0 to time k. If matrix $Y_\theta(k)^\intercal$ has full column rank, which is generally the case, the optimal solution of (9) is given by $\hat{G}(k)^\star = Z_\theta(k)Y_\theta(k)^\intercal(Y_\theta(k)Y_\theta(k)^\intercal)^{-1}$. Then, the inferred matrix $\hat{G}$ can be divided into four blocks $\hat{G}(k) = \begin{bmatrix}\hat{G}_A(k) & \hat{G}_B(k)\\ \hat{G}_C(k) & \hat{G}_D(k)\end{bmatrix}$, where $\hat{G}_A(k), \hat{G}_B(k)$ can be written as:

$$\hat{G}_A(k) = I_N - \frac{T^2}{2}\hat{L}_{\mathcal{G}A}(k), \quad \hat{G}_B(k) = -T\hat{L}_{\mathcal{G}B}(k).$$

Then the inferred matrix $\hat{L}_{\mathcal{G}}(k)$ can be extracted from $\hat{G}(k)$ by the following function $f(\cdot)$:

$$\begin{aligned}\hat{L}_{\mathcal{G}}(k) = f(\hat{G}(k)) &= \frac{1}{2}\left(\hat{L}_{\mathcal{G}A}(k) + \hat{L}_{\mathcal{G}B}(k)\right)\\ &= \frac{1}{T^2}I_N - \frac{1}{T^2}\hat{G}_A(k) - \frac{1}{2T}\hat{G}_B(k).\end{aligned} \tag{10}$$

Note that if we utilize the right blocks $\hat{G}_C(k)$ and $\hat{G}_D(k)$ of $\hat{G}(k)$, then the inferred matrix $\hat{L}_{\mathcal{G}}(k)$ can be more accurate. However, as the right blocks contain the unknown parameter α, it is complex to solve for these two coupling variables simultaneously. Furthermore, it is sufficient to utilize $\hat{G}_A(k)$ and $\hat{G}_B(k)$ to derive the matrix $\hat{L}_{\mathcal{G}}(k)$ in practice.

After retrieving the estimated Laplacian matrix, the adversaries can launch targeted attacks. The attacks considered in this paper are summarized and categorized as follows:

1) Sensor Attack: This type of attack targets the sensors of a robot, rendering it incapable of sensing the accurate states of its neighbors.
2) Mobility Attack: This type of attack involves immobilizing a robot or impairing its ability to change its states.

If the system maintains a directed spanning tree after attacks, the formation will experience no distortion. Otherwise, the absence of a directed spanning tree can lead to undesirable distortion, posing a significant challenge to motion coordination. Furthermore, it is worth noting that for systems modeled by directed graphs, merely maintaining a spanning tree is insufficient to guarantee the performance of motion coordination. This is because the formation can still deviate from the prescribed formation due to the changes in the interaction topology, which strongly impacts the relative weights in the network.

C. Problem Formulation

In this paper, we mainly consider how to conceal the actual topology of the MRS by adding perturbation signals to the states of the robots. The regular algorithm (4) is revised to

$$\tilde{u}_i(k) = u_i(k) + \theta_i(k), \tag{11}$$

where the design of $u_i(k)$ follows (4) and $\theta_i(k)$ is the perturbation signal. The system (5) can be rewritten as

$$\begin{bmatrix}\tilde{p}(k+1)\\ v(k+1)\end{bmatrix} = G\begin{bmatrix}\tilde{p}(k)\\ v(k)\end{bmatrix} + \begin{bmatrix}\frac{T^2}{2}\theta(k)\\ T\theta(k)\end{bmatrix}, \tag{12}$$

where $\theta(k) \in \mathbb{R}^N$ is the vector of perturbation signals at time k. Generally, the system model can be written as follows:

$$\begin{bmatrix}\tilde{p}(k)\\ v(k)\end{bmatrix} = G^k\begin{bmatrix}\tilde{p}(0)\\ v(0)\end{bmatrix} + \sum_{\ell=0}^{k-1} G^{k-\ell-1}\begin{bmatrix}\frac{T^2}{2}\theta(\ell)\\ T\theta(\ell)\end{bmatrix}. \tag{13}$$

It can be seen that the dynamics of the robots under (11) will be affected not only by the topology information of the system but also by the designed perturbation signals.

The objective of this paper is to develop a topology-preserving algorithm that can effectively prevent adversaries from inferring the topology accurately while guaranteeing the prescribed formation in the MRS. Hence, we formulate an optimization problem as follows.

$$\max_\theta \left\| f\left(\arg\min_{\hat{G}(k)} \left\|\hat{G}(k)Y_\theta(k) - Z_\theta(k)\right\|_F^2\right) - L_{\mathcal{G}}\right\|_F^2 \tag{14}$$

s.t. (7a) and (7b) hold.

Our foremost concern is designing optimal perturbation signals that maximize the inference error for potential adversaries while ensuring precise motion coordination. However, the optimal solution to this problem is intricately tied to the global interaction topology, which contradicts our intention to employ a distributed approach in designing the perturbation signals. Therefore, the solution is constrained to increase the inference error through specific algorithms, without guaranteeing the optimality in this regard. Another challenge stems from the second-order dynamics, which necessitates a careful design to mitigate the accumulative effect of the perturbation signals.

III. Algorithm Design

In this section, we propose the TPMC algorithm to address the challenges mentioned in Section II. First, we demonstrate the key idea that promotes the feasibility of the proposed algorithm. Then, we present the detailed algorithm design.

A. Key Idea

To fulfill the requirements of the formulated problem, the TPMC algorithm is designed consisting of two major parts: inject additive perturbation signals thus enlarging the regression errors, and add compensating perturbation signals to ensure the convergence of the MRS. Instead of adding random signals, we add well-designed self-compensating perturbation signals to the robots, which can ensure precise motion coordination.

According to (5), the subsequent state of a robot depends on the current states of its neighbors and itself. In this way, the perturbation signal of one robot will spread its influence through the topology, thereby affecting the coordination performance of the entire system. To achieve the prescribed formation (3), the following lemma is needed.

Lemma 2. *Under the finite perturbation signal sequence $\{\theta(\ell), \ell = 0, \cdots, k_0\}$, the desired motion coordination can be achieved at time k_0 if and only if*

$$\sum_{\ell=0}^{k_0} \boldsymbol{w}^\intercal\theta(\ell) = 0, \ \sum_{\ell=0}^{k_0} \ell\boldsymbol{w}^\intercal\theta(\ell) = 0. \tag{15}$$

Proof. The proof is provided in Appendix A. □

This lemma indicates that the perturbation signals have an accumulative effect on positions and velocities over time, which poses an inevitable challenge to the algorithm design. Note that the distinction between this lemma and Lemma 3.1 in [33] lies in that they describe the conditions of the perturbation signals in directed and undirected networks, respectively.

However, it is important to recognize that these conditions can only be formulated and evaluated from a centralized perspective. Given our emphasis on designing a distributed approach, the practical conditions for θ tend to be more restrictive for both undirected and directed networks, as elucidated in the following lemma.

Lemma 3. *Under the finite perturbation signal sequence $\{\theta(\ell), \ell = 0, \cdots, k_0\}$, the desired motion coordination can be achieved distributedly if the following condition holds*

$$\sum_{\ell=0}^{k_0} \theta_i(\ell) = 0, \ \sum_{\ell=0}^{k_0} \ell\theta_i(\ell) = 0, \quad \forall i \in \mathcal{V}, \tag{16}$$

where the number of non-zero entries in $\{\theta_i(\ell), \ell = 0, \cdots, k_0\}$ is larger than or equal to 3.

Proof. The proof is also provided in Appendix B. □

Lemma 3 demonstrates that the perturbation signal can be designed for individual robots in a distributed manner without relying on global knowledge of the topology, to guarantee the desired motion coordination. Similar results can be applied to higher-order systems, as the following remark illustrates.

Remark 1. *Similar to Lemma 3 for the second-order systems, the conditions for the motion coordination of n-th order sampled-data discrete-time system under finite perturbation signals can be obtained as the following general form*

$$\sum_{\ell=0}^{k_0} \ell^{n_0}\theta_i(\ell) = 0, \ \forall n_0 \in \{0, \cdots, n-1\}, \ \forall i \in \mathcal{V}, \tag{17}$$

where the number of the non-zero entries in the signal sequence is larger than or equal to $n + 1$.

Note that the non-zero entries in the signal sequence $\{\theta_i(\ell), \ell = 0, \cdots, k_0\}$ can be seen as the free variables in the homogeneous equations in (17). When the number of the non-zero entries is larger than or equal to $n + 1$, the overall system is under-determined, leading to infinite possible non-zero solutions for the sequence. In the next subsection, we will provide an efficient signal design method.

B. Perturbation Signal Design

Let $a_i(k) \in [-\varphi^k, \varphi^k]$ be a random variable with a bounded distribution. Let $F_k(a_i(k))$ be the cumulative distribution functions of $a_i(k)$ and $F_k(a_i(k)) = F_0(\frac{a_i(k)}{\varphi^k})$. The variance of $a_i(k)$ can be written in a general form:

$$\sigma_k^2 = \sigma_0^2\varphi^{2k}, 0 < \varphi \leq 1, \tag{18}$$

where σ_0^2 is the variance of $a_i(0)$. Denote $b_i(k)$ as the additive perturbation signal indicator that follows a Bernoulli distribution, given by

$$\Pr\{b_i(k) = 1\} = \epsilon, \ \Pr\{b_i(k) = 0\} = 1 - \epsilon, \ 0 < \epsilon \leq 1.$$

Algorithm 1: Topology-Preserving Motion Coordination (TPMC) Algorithm

```
Input: $G, T, k_0, \tau_e, \tilde{p}(0), v(0), \epsilon, \varphi$;
Output: Observation data set;
Initialization;
for $k = 0, 1, \ldots$ do
    if $k \leq k_0 - \tau_e$ then
        for $i = 1, \cdots, N$ do
            Generate $b_i(k)$ and $\tau_e$;
            if $b_i(k) = 1$ then
                Randomize $a_i(k) \in [-\varphi^k, \varphi^k]$;
                for $m = 0, \cdots, \tau_e$ do
                    $\omega_i(k + m \,|\, k) = c_m \times a_i(k)$;
                end
            end
            Calculate $\theta_i(k)$ by (21);
        end
    end
    Update $\tilde{p}(k + 1)$ and $v(k + 1)$ by (12);
end
```

Based on Lemma 3, we propose a general algorithm that satisfies (16), thereby guaranteeing the prescribed formation. In the algorithm, the additive perturbation signal $\omega_i(k \,|\, k)$ is added for the i-th robot at time k if $b_i(k) = 1$. To balance its effect on formation, compensating perturbation signals $\omega_i(k + \ell \,|\, k), \ell \in \mathbb{N}^+$ are imposed after several iterations.

Denote $\{c_m\}_{m=0}^{\tau_e}$ as the coefficient of the τ_e-lag time dependence algorithm, which has the following properties:

$$\sum_{m=0}^{\tau_e} c_m = 0, \sum_{m=0}^{\tau_e} mc_m = 0, \text{and } |c_m| < \bar{c}, \forall m \in \{0, \cdots, \tau_e\}, \tag{19}$$

where $\bar{c} < \infty$ is a finite upper bound of $\{c_m\}_{m=0}^{\tau_e}$. The additive perturbation signals and the compensating perturbation signals can be unified in the following form:

$$\omega_i(k + m \,|\, k) = c_m a_i(k), \quad \forall m \in \{0, \cdots, \tau_e\}. \tag{20}$$

Note that this kind of perturbation signal design represents a general form of τ_e-lag time dependence algorithm, with the examples introduced in [1] being particular instances of this concept. Within this general perturbation signal design, $\tau_e \geq 3$ is a variable that can be either fixed manually or randomized within a specified range. Note that the amplitude of the compensating perturbation signal is influenced by both $a_i(k)$ and the configuration of the $\{c_m\}_{m=0}^{\tau_e}$ sequence.

Note that the proposed algorithm generates a sequence of dependent perturbation signals rather than independent signals. If independent perturbation signals were used, then to guarantee the achievement of prescribed formation in the MRS, the amplitudes of the independent perturbation signals should be decaying. However, the inference error of the system will converge to zero in this case, which is undesirable. Therefore, the design of the dependent perturbation signals serves a critical purpose.

In general, the expression of $\theta_i(k)$ is

$$\theta_i(k)=\sum_{\ell=0}^{k}\omega_i(k\,|\,k-\ell)b_i(k-\ell),\tag{21}$$

which shows that at time k, the additive perturbation signal, and the compensating signals are summed up to form the resulting noise $\theta_i(k)$. Specifically, the details of the TPMC algorithm are illustrated in Algorithm 1. Note that in this algorithm, when $k_0-\tau_e<k\leq k_0$, only the compensating perturbation signals are added. Since the compensation period is τ_e+1, it is easy to reach that $\theta_i(k)$ is a sum of at most τ_e+1 non-zero numbers. When $k_0-\tau_e$ is finite, $\varphi\leq 1$ is sufficient for convergent motion coordination, and we call it a finite TPMC algorithm. In contrast, when $k_0-\tau_e$ is infinite, the value of φ should be strictly bounded to $\varphi<1$ to guarantee the convergence of motion coordination, and we call it an infinite TPMC algorithm. Unless otherwise specified, the TPMC algorithm refers to both kinds. Detailed analysis will be presented in the next section.

IV. Performance Analysis

This section presents the performance analysis of the TPMC algorithm, including the convergence analysis and the inference error analysis. In the first part, we prove that the system can reach the exact convergence under the TPMC algorithm, and we use the method in [35] for reference to derive the mean square convergence rate. In the second part, the non-asymptotic error bound of the inference attack is given.

A. Convergence Analysis

When the TPMC algorithm is applied to the system, the added perturbation signals to the robots will confuse not only the adversaries but also the neighboring robots. In order to ensure the normal performance of the system, convergence to the desired motion coordination must be guaranteed.

Theorem 1. *Given any $\tilde{p}(0)$ and $v(0)$ and using the finite TPMC algorithm with $\varphi\leq 1$, the desired motion coordination can be achieved, i.e.,* (7a) *and* (7b) *hold.*

Proof. The proof is provided in Appendix C. □

Theorem 1 shows that the finite TPMC algorithm can always guarantee the prescribed formation even for $\varphi=1$. However, such property does not hold when infinite perturbation signals are used and the prescribed formation can only be ensured in a mean square sense, as shown in the following result.

Theorem 2. *Given any $\tilde{p}(0)$ and $v(0)$ and using the infinite TPMC algorithm with $\varphi<1$, then the prescribed formation can be achieved in the mean square sense, i.e.,*

$$\lim_{k\to\infty}\mathbb{E}\left[\left\|\begin{bmatrix}\tilde{p}(k)\\ v(k)\end{bmatrix}-\begin{bmatrix}\tilde{p}^c(k)\\ v^c(k)\end{bmatrix}\right\|^2\right]=0,\tag{22}$$

where $\begin{bmatrix}\tilde{p}^c(k)^\intercal & v^c(k)^\intercal\end{bmatrix}^\intercal$ is the unperturbed state updated by (4). *Specifically, the smaller φ is, the faster the expectation of the deviation converges to zero.*

Proof. The proof is provided in Appendix D. □

Next, we characterize the convergence rate of the TPMC algorithm. For systems with second-order dynamics, the convergence rate is dominated by the eigenvalues of G. If Assumption 1 is satisfied, matrix G has $2N$ eigenvalues that are not necessarily distinct. Generally, G can be represented by the following Jordan decomposition form

$$G=M\,\mathrm{diag}\left\{J_1,J_2,\cdots,J_q\right\}M^{-1},\tag{23}$$

where $M\in\mathbb{R}^{2N\times 2N}$ is an invertible matrix and $J_q,q\leq N$ are the corresponding Jordan blocks. Specifically, the first Jordan block $J_1=\begin{bmatrix}1&1\\0&1\end{bmatrix}$ always holds. Denote the spectrum as $\mathrm{spec}(G)=\{\mu_1,\mu_2,\cdots,\mu_{2N}\}$ and the essential spectral radius as $\mu_m(G)=\max\{|\mu|\,|\,\mu\in\mathrm{spec}(G)\backslash\{1\}\}$.

The mean square convergence rate under the motion coordination algorithm is defined as

$$\rho_m\triangleq\lim_{k\to\infty}\left(\sup_{\delta(0)\neq 0}\frac{\mathbb{E}[\delta(k)^\intercal\delta(k)]}{\delta(0)^\intercal\delta(0)}\right)^{\frac{1}{k}},\tag{24}$$

where $\delta(k)$ is the deviation between the actual states and the prescribed states, i.e.,

$$\delta(k)=\begin{bmatrix}\tilde{p}(k)\\ v(k)\end{bmatrix}-\begin{bmatrix}\tilde{p}^*(k)\\ v^*(k)\end{bmatrix}=\begin{bmatrix}\tilde{p}(k)\\ v(k)\end{bmatrix}-\begin{bmatrix}\boldsymbol{w}^\intercal(\tilde{p}(0)+kTv(0))\mathbf{1}_N\\ (\boldsymbol{w}^\intercal v(0))\mathbf{1}_N\end{bmatrix}.$$

Applying the TPMC algorithm to the MRS, the mean square convergence rate is determined by the following theorem.

Theorem 3. *Given any $\tilde{p}(0)$ and $v(0)$ and using the TPMC algorithm, the mean square convergence rate of achieving the prescribed formation is given by*

$$\rho_m=\max\left\{(\epsilon C\varphi)^2,\mu_m(G)^2\right\}.\tag{25}$$

where $C=\sum_{m=0}^{\tau_e}|c_m|$ is the constant depending on the perturbation sequence $\{c_m\}_{m=0}^{\tau_e}$.

Proof. The proof is provided in Appendix E. □

The above theorem suggests that the TPMC algorithm can guarantee an exponential mean square convergence, and the convergence rate can be tuned by the parameters ϵ,C,φ in the TPMC algorithm.

B. Inference Error Analysis

To keep the adversaries from inferring the actual topology, we need to enlarge the regression error $\Delta_L(k)=\hat{L}_{\mathcal{G}}(k)-L_{\mathcal{G}}$. As is mentioned in Section II, the optimal solution of the OLS estimator is $\hat{G}(k)^\star=Z_\theta(k)Y_\theta(k)^\intercal(Y_\theta(k)Y_\theta(k)^\intercal)^{-1}$. Then the deviation of the topology inference can be described as $\Delta_G(k)=\hat{G}(k)-G=\Theta(0;k)Y_\theta(k)^\intercal(Y_\theta(k)Y_\theta(k)^\intercal)^{-1}$, where

$$\Theta(0;k)=Z_\theta(k)-\hat{G}(k)Y_\theta(k)=\begin{bmatrix}\frac{T^2}{2}\theta(0)&\cdots&\frac{T^2}{2}\theta(k-1)\\ T\theta(0)&\cdots&T\theta(k-1)\end{bmatrix}$$

indicates the residual of the inference. According to the function $f(\cdot)$ that extracts $\hat{L}_{\mathcal{G}}(k)$ from the inferred matrix $\hat{G}(k)$ in (10), the following theorem reveals the relationship between $\Delta_L(k)$ and $\Delta_G(k)$.

Theorem 4. *The relationship between $\Delta_L(k)$ and $\Delta_G(k)$ can be described by*

$$\|\Delta_L(k)\|_F^2 \leq \max\left\{\frac{1}{T^4}, \frac{1}{4T^2}\right\} \|\Delta_G(k)\|_F^2 .$$

Proof. Following (10), the regression error $\Delta_L(k)$ can be written as

$$\Delta_L(k) = -\frac{1}{T^2}\Delta_{G_A}(k) - \frac{1}{2T}\Delta_{G_B}(k), \tag{26}$$

where $\Delta_{G_A}(k)$ and $\Delta_{G_B}(k)$ describe the inference errors of the upper left block and the lower left block of the matrix $\hat{G}(k)$, respectively. Together with the inequality $\|\Delta_{G_A}(k)\|_F^2 + \|\Delta_{G_B}(k)\|_F^2 \leq \|\Delta_G(k)\|_F^2$, it can be deduced that

$$\begin{aligned}\|\Delta_L(k)\|_F^2 &= \frac{1}{T^4}\|\Delta_{G_A}(k)\|_F^2 + \frac{1}{4T^2}\|\Delta_{G_B}(k)\|_F^2 \\ &\leq \max\left\{\frac{1}{T^4}, \frac{1}{4T^2}\right\} \|\Delta_G(k)\|_F^2 .\end{aligned}$$

The proof is completed. □

The following theorem further exhibits the relationship between the error bound $\|\Delta_L(k)\|$ and time k.

Theorem 5. *Applying the TPMC algorithm to the system* (2)*, the error bound of the OLS estimator is characterized by:*

$$\lim_{k\to\infty} \mathbb{E}\left[\|\Delta_L(k)\|\right] = \begin{cases}\mathcal{O}(1), & \varphi < 1, \\ \mathcal{O}(\sqrt{k}), & \varphi = 1.\end{cases}$$

Proof. The proof is provided in Appendix F. □

Theorem 5 shows that the inference error does not converge with time k approaching infinity. The difficulties in giving a more tight bound of $\|\Delta_L(k)\|$ lie in the following two aspects.

- The system with second-order dynamics is unstable, for the geometric multiplicity of eigenvalue 1 in matrix G equals one and its algebraic multiplicity equals two. Consequently, the influence of the perturbation signals can accumulate and be magnified during the coordination process, which is hard to characterize.
- The added perturbation signals are temporally dependent while decaying with time, and the mainstream analytical techniques (like concentration measures that are mainly for i.i.d. cases [36] and consistency analysis for OLS estimator [23]) are not applicable.

V. Simulations and Experiments

In this section, we verify the effectiveness of the TPMC algorithm via simulations and real-world experiments. To show the motions of unmanned ground vehicles (UGVs) in a real multi-robot system, the experiments are conducted on a two-dimensional plane for both simulations and real-world experiments. The objective of the experiments is motion coordination in the sense that robots converge to the prescribed formation pattern with the same velocity.

TABLE I
THE DISTORTION E_{d1} AND THE DEVIATION E_{d2} UNDER ATTACKS USING DIFFERENT ALGORITHMS

	Sensor Attack		Mobility Attack	
	E_{d1}	E_{d2}	E_{d1}	E_{d2}
Normal Algorithm (4)	0.0144	4886.6082	0.1195	3516.3338
The TPMC algorithm	0.0252	2196.2106	658.3563	766.2431

In the two-dimensional case, the algorithm is applied for the robots on both the x-axis and the y-axis. The relative positions and velocities of the i-th robot at time k are denoted as $\tilde{p}_{x,i}(k)$, $\tilde{p}_{y,i}(k)$, $v_{x,i}(k)$, and $v_{y,i}(k)$.

Following the categorization of attacks in Section II-B, several key concepts are given for a better understanding of the inference attacks.

1) Robot Importance: This metric quantifies the degree to which a robot is important for maintaining a prescribed formation. It can be expressed by the weight of the robot (diagonal elements) in the Laplacian matrix $L_{\mathcal{G}}$ or the number of its out-degree neighbors.
2) Attack Effectiveness: This measures the extent to which the same attack (e.g., attacking robots or links with equivalent numbers, or injecting malicious signals of a certain magnitude) impairs the overall performance of the system.

In the context of motion coordination, the effectiveness of an attack can be assessed through two indicators: the distortion of the prescribed formation pattern and the deviation of the robots from the prescribed formation states, respectively.

A. Simulation Setting

A directed graph with three robots that represents the interaction topology of the system is randomly constructed. Assign all the robots with the specific initial states and interaction links, and define the desired position deviation between robots in a formation. Start the iteration under the TPMC algorithm as in Algorithm 1.

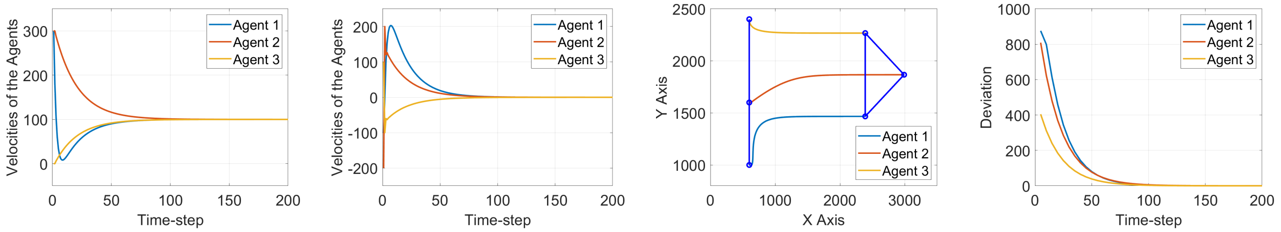
The adjacency matrix $A_{\mathcal{G}}$ and the corresponding Laplacian matrix $L_{\mathcal{G}}$ are set as:

$$A_{\mathcal{G}} = \begin{bmatrix}0 & 1 & 1\\ 0 & 0 & 4\\ 0 & 2 & 0\end{bmatrix},\ L_{\mathcal{G}} = \begin{bmatrix}2 & -1 & -1\\ 0 & 4 & -4\\ 0 & -2 & 2\end{bmatrix}.$$

The detailed settings of initial positions, velocities, and target positions of two dimensions are as follows:

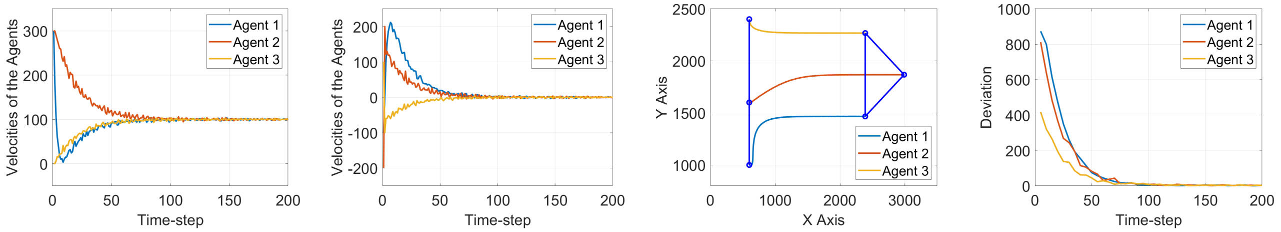
$$\begin{aligned}p_x(0) &= \begin{bmatrix}600\\600\\600\end{bmatrix},\ \eta_x = \begin{bmatrix}600\\1200\\600\end{bmatrix},\ v_x(0) = \begin{bmatrix}300\\300\\0\end{bmatrix}, \\ p_y(0) &= \begin{bmatrix}1000\\1600\\2400\end{bmatrix},\ \eta_y = \begin{bmatrix}1200\\1600\\2000\end{bmatrix},\ v_y(0) = \begin{bmatrix}-100\\-200\\100\end{bmatrix}.\end{aligned}$$

Then, distortion and deviation are used to describe the effectiveness of the attacks. The first indicator reflects the degree of distortion in the formation, and the second indicator displays the deviation between the current states and



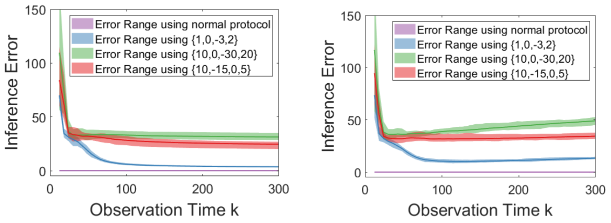
(a) Velocities of robots on the x-axis (b) Velocities of robots on the y-axis (c) Positions of robots (d) Convergence of deviation

Fig. 1. The positions, the velocities and the deviation E_{d2} of robots under the normal algorithm



(a) Velocities of robots on the x-axis (b) Velocities of robots on the y-axis (c) Positions of robots (d) Convergence of deviation

Fig. 2. The positions, the velocities and the deviation E_{d2} of robots under the TPMC algorithm



(a) $\varphi < 1$ (b) $\varphi = 1$

Fig. 3. The error performance of the TPMC algorithm

the prescribed formation states. Specifically, the measure of formation distortion can be written as:

$$E_{d1} = \sqrt{\sum_{i=1}^{N} (\tilde{p}_{x,i}(k) - \bar{p}_x(k))^2 + (\tilde{p}_{y,i}(k) - \bar{p}_y(k))^2},$$

where $(\bar{p}_x(k), \bar{p}_y(k))$ is the centroid of the formation. The deviation can be written as:

$$E_{d2} = \sum_{i=1}^{N} \sqrt{\left(\tilde{p}_{x,i}(k) - \tilde{p}^*_{x,i}(k)\right)^2 + \left(\tilde{p}_{y,i}(k) - \tilde{p}^*_{y,i}(k)\right)^2} + \alpha \sum_{i=1}^{N} \sqrt{\left(v_{x,i}(k) - v^*_{x,i}(k)\right)^2 + \left(v_{x,i}(k) - v^*_{x,i}(k)\right)^2}.$$

Then we would like to verify the protectiveness of the algorithm against the attacks that may be launched by adversaries. As mentioned in Section II, the attacks can be categorized into two kinds in our scenario. In the simulation part, we conduct these kinds of attacks separately to display the danger of the attack and the performance of the topology-preserving algorithm. In the simulations, the attacks are simplified as:

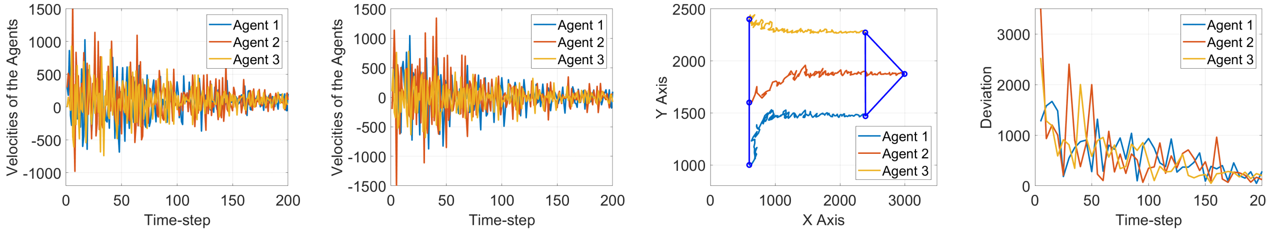
- Sensor Attack: Infer the most important robot i, and set the weight of the edge $(i, j), \forall j \in \mathcal{N}_i$ to 0.
- Mobility Attack: Infer the most important robot i, and set its velocity to 0.

B. Simulation Results

Fig. 1 and Fig. 2 depict changes in the positions and velocities of robots in the system during the formation progress under the normal algorithm and the TPMC algorithm with a perturbation sequence $\{c_m\}_{m=0}^{\tau_e} = \{1, -1, -1, 1\}$, respectively. It can be seen in the figures that the proposed algorithm ensures the prescribed formation, although positions and velocities may fluctuate due to the perturbation signals. Fig. 3 illustrates the error performance of the proposed algorithm with different perturbation sequences $\{c_m\}_{m=0}^{\tau_e}$. Firstly, it demonstrates that the topology of the MRS can be accurately inferred when the normal algorithm is applied, as shown by the purple lines parallel to the x-axis. On the other hand, the proposed TPMC algorithm effectively enlarges the inference error. Fig. 3(a) and Fig. 3(b) depict the error performance of the proposed TPMC algorithm for the cases when $\varphi < 1$ and $\varphi = 1$, respectively. In both cases, the inference error keeps a rather smooth line. The difference in the setting of perturbation sequences exhibits as the primary factor that impacts the inference error. It can also be seen in the figures that when the observation time k is less than 30, the inference error is large due to limited data. Generally, these results are consistent with Theorem 5. Note that the amplitude of the perturbation signals can be large for better protection. The performance of motion coordination can still be guaranteed because the second-order dynamics of the system determine that the changes in positions are limited. Fig. 4 shows the changes in the states of robots under the TPMC algorithm where the perturbation sequence is $\{c_m\}_{m=0}^{\tau_e} = \{100, -100, -100, 100\}$.

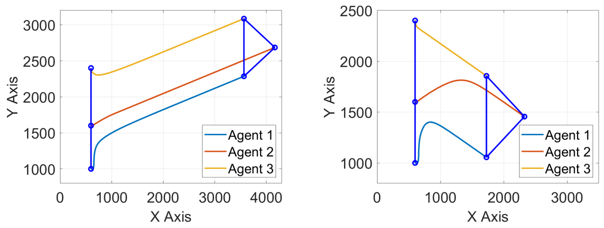
To conclude, the simulation results demonstrate that the TPMC algorithm performs well in addressing the topology preservation problem for MRSs with second-order dynamics. The performance of the TPMC algorithm is significantly impacted by parameter τ_e.

The performance of the algorithm dealing with different



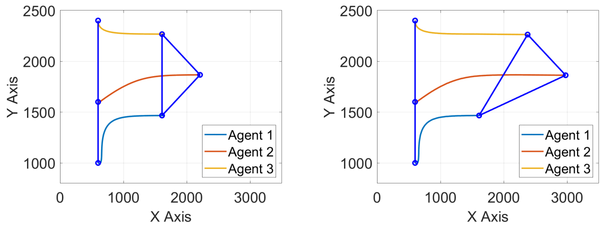
(a) Velocities of robots on the x-axis (b) Velocities of robots on the y-axis (c) Positions of robots (d) Convergence of deviation

Fig. 4. The positions, the velocities and the deviation E_{d2} of robots under the TPMC algorithm with strong perturbation signals



(a) Normal algorithm (4) (b) The TPMC algorithm

Fig. 5. The performance of the normal algorithm and the TPMC algorithm facing sensor attacks



(a) Normal algorithm (4) (b) The TPMC algorithm

Fig. 6. The performance of the normal algorithm and the TPMC algorithm facing mobility attacks

kinds of attacks is shown in Fig. 5 - Fig. 6. The distortion and the deviation under attacks are shown in Table I. Specifically, employing the normal algorithm (4), the Laplacian matrix can be accurately regressed, consequently revealing that robot 2 is the most important robot in this MRS. In contrast, under the TPMC algorithm, the regressed matrix is

$$\hat{L}_{\mathcal{G}}(k)=\begin{bmatrix}29.0412 & 2.6884 & -34.5871\\ -4.4888 & 4.6560 & -3.9448\\ 5.4096 & -1.1154 & -9.4185\end{bmatrix},$$

and the most important node regressed is robot 1.

Under sensor attacks, the matrices $A^a_{\mathcal{G}}, A^b_{\mathcal{G}}$ under normal algorithm (4) and the TPMC algorithm become

$$A^a_{\mathcal{G}}=\begin{bmatrix}0&1&1\\0&0&0\\0&2&0\end{bmatrix},\ A^b_{\mathcal{G}}=\begin{bmatrix}0&0&0\\0&0&4\\0&2&0\end{bmatrix},$$

respectively. Note that $A^a_{\mathcal{G}}$ retains a spanning tree, while the vector $\boldsymbol{w}$ is drastically changed. In contrast, $A^b_{\mathcal{G}}$ loses the spanning tree, but the weight ratio between robot 2 and robot 3 remains. Therefore, the system exhibits less deviation when the TPMC algorithm is applied.

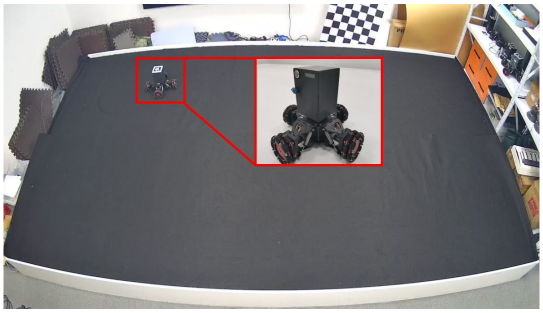


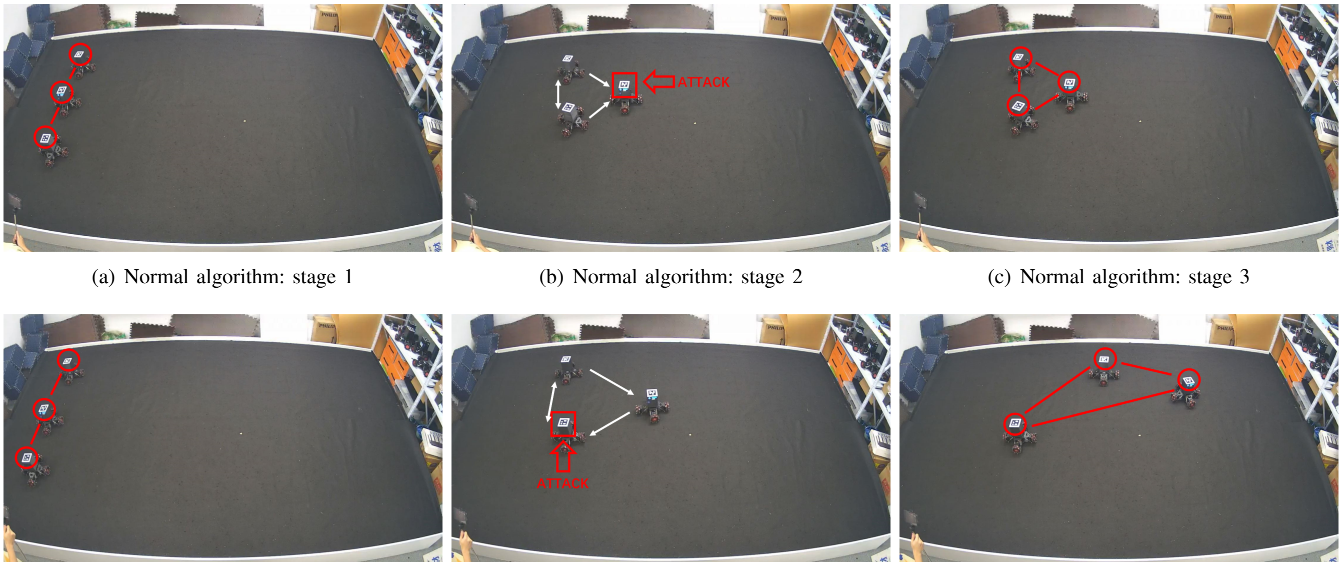
Fig. 7. Overview of the platform

Mobility attacks will not change the topology of the MRS. Due to the inherent characteristic of the MRS, the vector $\boldsymbol{w}=[0,1/3,2/3]$. When robot 2 is attacked, i.e., $v_{x,2}(k)=0$ and $v_{y,2}(k)=0$, the velocities for all the robots will become 0. However, with the protection of the TPMC algorithm, the robot 1 will be attacked, with $v_{x,1}(k)=0$ and $v_{y,1}(k)=0$, which does not interfere with other robots. In this way, the formation will experience a significant distortion, but the unattacked robots can keep their motions.

C. Real-World Experiments

Then we use the self-designed mobile robot platform [37] in our laboratory to implement real-world experiments thus verifying the practicability of the algorithm. The platform contains a 5m × 3m rectangular field and an AprilTag-based real-time localization system, as is shown in Fig. 7. The data of the platform is saved in the database and transferred using the ZigBee protocol. The control commands based on the localization results are implemented by MATLAB R2020b in a VMWare ESXI virtual machine, which is equipped with an Intel(R) Xeon(R) Gold5220R CPU, a 2.20 GHz processor, and a 16GB RAM.

Take mobility attacks as an example, we conduct real-world experiments on our robotic platform with three UGVs. The results can be seen in Fig. 8 with the whole procedure being divided into three stages. In the first stage, the robots start to move from the initial states. Then, the topology is inferred by adversaries, and the most important robot in the inferred topology is attacked. The third stage displays the coordination performance after the attack. Overall, the results of the real-world experiments are in line with the simulations.



(a) Normal algorithm: stage 1

(b) Normal algorithm: stage 2

(c) Normal algorithm: stage 3

(d) TPMC algorithm: stage 1

(e) TPMC algorithm: stage 2

(f) TPMC algorithm: stage 3

Fig. 8. Real-world experiments: mobility attack under the normal algorithm and the TPMC algorithm

VI. Conclusion

In this work, we focus on the topology preservation problem in motion coordination in MRSs with second-order dynamics. To address this problem, we propose the TPMC algorithm, where perturbation signals are designed for robots to make it hard for adversaries to perform topology inference attacks while guaranteeing the achievement of the prescribed formation. The convergence and inference error performance of the MRS under the proposed algorithm are analyzed. Extensive simulations and real-world experiments are conducted to verify the effectiveness of the proposed algorithm in maintaining the precise motion coordination in MRSs and weakening the topology inference ability of the adversaries. Future research directions include expanding our study to more general networks, such as higher-order multi-robot systems with switching topology networks, and exploring algorithms that adapt to other topology inference methods.

Appendix

A. Proof of Lemma 2

Proof. Denote k_0 as the last iteration where the perturbation signal is added to the system. Substitute k_0 into (13),

$$\begin{bmatrix}\tilde{p}(k_0+1)\\ v(k_0+1)\end{bmatrix} = G^{k_0+1}\begin{bmatrix}\tilde{p}(0)\\ v(0)\end{bmatrix} + \sum_{l=0}^{k_0} G^{k_0-\ell-1}\begin{bmatrix}\frac{T^2}{2}\theta(\ell)\\ T\theta(\ell)\end{bmatrix}.$$

Denote $\begin{bmatrix}\theta_{p,\ell}(k)\\ \theta_{v,\ell}(k)\end{bmatrix} = G^{k-\ell-1}\begin{bmatrix}\frac{T^2}{2}\theta(\ell)\\ T\theta(\ell)\end{bmatrix}, \forall \ell\in\{0,\cdots,k_0\}$. It is easy to derive from (7a) and (7b) that:

$$\begin{aligned}&\lim_{k\to\infty}\theta_{v,\ell}(k) = T\mathbf{1}\boldsymbol{w}^\intercal\theta(\ell),\\ &\lim_{k\to\infty}\theta_{p,\ell}(k) = \frac{T^2}{2}\mathbf{1}\boldsymbol{w}^\intercal\theta(\ell) + (k-\ell)T^2\boldsymbol{w}^\intercal\theta(\ell).\end{aligned}$$

Therefore, for a given finite perturbation sequence $\{\theta_i(\ell), \ell = 0,\cdots,k_0\}$ in the infinite run, we generally have

$$\begin{aligned}&\lim_{k\to\infty} G^{k-k_0}\sum_{\ell=0}^{k_0} G^{k_0-\ell-1}\begin{bmatrix}\frac{T^2}{2}\theta(\ell)\\ T\theta(\ell)\end{bmatrix}\\ &= \lim_{k\to\infty}\sum_{\ell=0}^{k_0}\begin{bmatrix}\left(k-\ell+\frac{1}{2}\right)T^2\mathbf{1}\boldsymbol{w}^\intercal\theta(\ell)\\ T\mathbf{1}\boldsymbol{w}^\intercal\theta(\ell)\end{bmatrix}.\end{aligned} \tag{27}$$

Clearly, the impact of $\theta(\ell)$ in the infinite horizon equals 0 if and only if (27) converges to zero, which further yields (15). The proof is completed. □

B. Proof of Lemma 3

Proof. The proof of Lemma 3 follows from the proof of Lemma 2. First, we take an element-wise view on (27). When all elements of the right-hand side (RHS) of (27) are zeros, it is equivalent to

$$\begin{aligned}\lim_{k\to\infty}\left\{\sum_{\ell=0}^{k_0}\boldsymbol{w}^\intercal\theta(\ell)\right\} &= \lim_{k\to\infty}\left\{\sum_{\ell=0}^{k_0}\sum_{i=1}^{N}\boldsymbol{w}_i\theta_i(\ell)\right\}\\ &= \lim_{k\to\infty}\left\{\sum_{i=1}^{N}\boldsymbol{w}_i\sum_{\ell=0}^{k_0}\theta_i(\ell)\right\} = 0,\end{aligned} \tag{28}$$

and

$$\begin{aligned}&\lim_{k\to\infty}\left\{\sum_{\ell=0}^{k_0}\left[\left(k-\ell+\frac{1}{2}\right)\boldsymbol{w}^\intercal\theta(\ell)\right]\right\}\\ &= \lim_{k\to\infty}\left\{\sum_{\ell=0}^{k_0}\left[\left(k-\ell+\frac{1}{2}\right)\sum_{i=1}^{N}\boldsymbol{w}_i\theta_i(\ell)\right]\right\}\\ &= \lim_{k\to\infty}\left\{\sum_{i=1}^{N}\boldsymbol{w}_i\sum_{\ell=0}^{k_0}\left(k-\ell+\frac{1}{2}\right)\theta_i(\ell)\right\} = 0.\end{aligned} \tag{29}$$

It is easy to obtain that if

$$\sum_{\ell=0}^{k_0} \theta_i(\ell) = 0, \ \forall i \in \mathcal{V}, \tag{30}$$

then (28) holds. Similarly, $\sum_{\ell=0}^{k_0} \left(k - \ell + \frac{1}{2}\right) \theta_i(\ell) = 0, \forall i \in \mathcal{V}$ is also sufficient to satisfy (29). Moreover, it can be further simplified by applying the condition (30), yielding that

$$\sum_{\ell=0}^{k_0} \left(k-\ell+\frac{1}{2}\right) \theta_i(\ell) = \left(k + \frac{1}{2}\right) \sum_{\ell=0}^{k_0} \theta_i(\ell) - \sum_{\ell=0}^{k_0} \ell\theta_i(\ell) = 0$$

$$\Rightarrow \ \sum_{\ell=0}^{k_0} \ell\theta_i(\ell) = 0, \ \forall i \in \mathcal{V}. \tag{31}$$

Finally, notice that (30) and (31) together constitute a group of homogeneous equations. To make them simultaneously hold while having multiple solutions, the number of non-zero perturbation variables must be larger than the number of equations. The proof is completed. □

C. Proof of Theorem 1

Proof. In this part, we mainly prove that the perturbation signal design in (20) satisfies the precise motion coordination conditions. Under our overall framework, the second equation of (16) for i-th robot can be written as

$$\begin{aligned} \sum_{\ell=0}^{k_0} \ell\theta_i(\ell) &= \sum_{x=0}^{k_0-\tau_e} \sum_{\ell=x}^{x+\tau_e} \ell\omega_i(\ell \,|\, x) b_i(x) \\ &= \sum_{x=0}^{k_0-\tau_e} \left(\sum_{m=0}^{\tau_e} m c_m\right) b_i(x) a_i(k). \end{aligned} \tag{32}$$

Similarly, we have

$$\begin{aligned} \sum_{\ell=0}^{k_0} \theta_i(\ell) &= \sum_{x=0}^{k_0-\tau_e} \sum_{\ell=x}^{x+\tau_e} \omega_i(\ell \,|\, x) b_i(x) \\ &= \sum_{x=0}^{k_0-\tau_e} \left(\sum_{m=0}^{\tau_e} c_m\right) b_i(x) a_i(k) \end{aligned} \tag{33}$$

Substituting the coefficient condition (19) for $\{c_m\}_{m=0}^{\tau_e}$ into (32) and (33) yields that $\sum_{\ell=0}^{k_0} \ell\theta_i(\ell) = 0$ and $\sum_{\ell=0}^{k_0} \theta_i(\ell) = 0$, which completes the proof. □

D. Proof of Theorem 2

Proof. This part mainly proves the asymptotic convergence of the infinite TPMC algorithm. Since the perturbation sequence is infinite, (16) is not sufficient for the proof in this case.

Based on (13), Equation (22) is equivalent to:

$$\lim_{k\to\infty} \mathbb{E}\left[\left\|\sum_{\ell=0}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2}\theta(\ell) \\ T\theta(\ell) \end{bmatrix}\right\|^2\right] = 0. \tag{34}$$

Recall the definition and the properties of $\{c_m\}_{m=0}^{\tau_e}$, the perturbation signal $\theta_i(\ell)$ can be written in the following form:

$$\theta_i(\ell) = \sum_{m=0}^{\min(\ell,\tau_e)} c_m a_i(\ell - m) b_i(\ell - m).$$

We denote $\Lambda(k) = \sum_{\ell=0}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2}\theta(\ell) \\ T\theta(\ell) \end{bmatrix}$ and derive that

$$\begin{aligned} \Lambda(k) =& \sum_{\ell=0}^{\tau_e} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2} \sum_{m=0}^{\ell} c_m B(\ell-m) a(\ell-m) \\ T \sum_{m=0}^{\ell} c_m B(\ell-m) a(\ell-m) \end{bmatrix} \\ &+ \sum_{\ell=\tau_e+1}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2} \sum_{m=0}^{\tau_e} c_m B(\ell-m) a(\ell-m) \\ T \sum_{m=0}^{\tau_e} c_m B(\ell-m) a(\ell-m) \end{bmatrix} \\ =& \sum_{\ell=0}^{k-\tau_e-1} \left(\sum_{m=0}^{\tau_e} c_m G^{k-\ell-m-1}\right) \begin{bmatrix} \frac{T^2}{2} B(\ell) a(\ell) \\ T B(\ell) a(\ell) \end{bmatrix} \\ &+ \sum_{\ell=k-\tau_e}^{k-1} \left(\sum_{m=0}^{k-\ell-1} c_m G^{k-\ell-m-1}\right) \begin{bmatrix} \frac{T^2}{2} B(\ell) a(\ell) \\ T B(\ell) a(\ell) \end{bmatrix}, \end{aligned} \tag{35}$$

where the matrix $B(\ell) = \operatorname{diag}\{b_1(\ell), \cdots, b_N(\ell)\}$, and the vector $a(\ell) = \begin{bmatrix} a_1(\ell) & \cdots & a_N(\ell) \end{bmatrix}^\mathsf{T}$. Define two auxiliary matrices $\tilde{G}_{c,a}(k,\ell)$ and $\tilde{G}_{c,b}(k,\ell)$ as

$$\begin{aligned} \tilde{G}_{c,a}(k,\ell) &= \sum_{m=0}^{\tau_e} c_m G^{k-\ell-m-1}, \\ \tilde{G}_{c,b}(k,\ell) &= \sum_{m=0}^{k-\ell-1} c_m G^{k-\ell-m-1}. \end{aligned}$$

Then, substituting (35) into (34), the mean square error is further written as

$$\begin{aligned} & \mathbb{E}\left[\left\|\sum_{\ell=0}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2}\theta(\ell) \\ T\theta(\ell) \end{bmatrix}\right\|^2\right] \qquad (36) \\ =& \operatorname{tr}\left(\mathbb{E}\left[\sum_{\ell=0}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2}\theta(\ell) \\ T\theta(\ell) \end{bmatrix} \left(\sum_{\ell=0}^{k-1} G^{k-\ell-1} \begin{bmatrix} \frac{T^2}{2}\theta(\ell) \\ T\theta(\ell) \end{bmatrix}\right)^\mathsf{T}\right]\right) \\ =& \sum_{\ell=0}^{k-\tau_e-1} \operatorname{tr}\left(\epsilon\sigma_\ell^2 \tilde{G}_{c,a}(k,\ell) \begin{bmatrix} \frac{T^4}{4} I_N & \frac{T^3}{2} I_N \\ \frac{T^3}{2} I_N & T^2 I_N \end{bmatrix} \tilde{G}_{c,a}^\mathsf{T}(k,\ell)\right) \\ &+ \sum_{\ell=k-\tau_e}^{k-1} \operatorname{tr}\left(\epsilon\sigma_\ell^2 \tilde{G}_{c,b}(k,\ell) \begin{bmatrix} \frac{T^4}{4} I_N & \frac{T^3}{2} I_N \\ \frac{T^3}{2} I_N & T^2 I_N \end{bmatrix} \tilde{G}_{c,b}^\mathsf{T}(k,\ell)\right) \\ =& \sum_{\ell=0}^{k-\tau_e-1} \left\|\tilde{G}_{c,a}(k,\ell) Q\right\|_F^2 \epsilon\sigma_\ell^2 + \sum_{\ell=k-\tau_e}^{k-1} \left\|\tilde{G}_{c,b}(k,\ell) Q\right\|_F^2 \epsilon\sigma_\ell^2 \\ \le& \underbrace{\epsilon\|Q\|_F^2 \sum_{\ell=0}^{k-\tau_e-1} \left\|\tilde{G}_{c,a}(k,\ell)\right\|_F^2 \sigma_\ell^2}_{\textcircled{1}} + \underbrace{\epsilon\|Q\|_F^2 \sum_{\ell=k-\tau_e}^{k-1} \left\|\tilde{G}_{c,b}(k,\ell)\right\|_F^2 \sigma_\ell^2}_{\textcircled{2}} \end{aligned}$$

where the property $\mathbb{E}[a_i(\ell) b_i(\ell)] = \epsilon\sigma_\ell^2$ is applied in the third row, and $Q \in \mathbb{R}^{2N\times 2N}$ is an orthogonal matrix such that

$$QQ^\mathsf{T} = \begin{bmatrix} \frac{T^4}{4} I_N & \frac{T^3}{2} I_N \\ \frac{T^3}{2} I_N & T^2 I_N \end{bmatrix} \succeq 0. \tag{37}$$

In the following, we can turn to prove that both term ① and term ② will converge to zero as $k \to \infty$.

For term ①, recall that the Jordan decomposition of matrix G can be written as $G = M\,\mathrm{diag}\left\{J_1, J_2, \cdots, J_q\right\} M^{-1}$ with $J_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. In this way, $\tilde{G}_{c,a}(k,\ell)$ is equivalent to

$$\tilde{G}_{c,a}(k,\ell) = M\,\mathrm{diag}\left\{\sum_{m=0}^{\tau_e} c_m J_i^{k-\ell-m-1}, i=1,\cdots,q\right\} M^{-1}.$$

In particular, due to property of $\{c_m\}_{m=0}^{\tau_e}$ given by (19), the first Jordan block of $\tilde{G}_{c,a}(k,\ell)$ satisfies

$$\begin{aligned}\sum_{m=0}^{\tau_e} c_m J_1^{k-\ell-m-1} &= \sum_{m=0}^{\tau_e} c_m \begin{bmatrix} 1 & k-\ell-m-1 \\ 0 & 1 \end{bmatrix} \\ = \sum_{m=0}^{\tau_e} \begin{bmatrix} c_m & c_m(k-\ell-1) \\ 0 & c_m \end{bmatrix} &- \begin{bmatrix} 0 & mc_m \\ 0 & 0 \end{bmatrix} = 0. \qquad (38)\end{aligned}$$

Meanwhile, since the modulus of all eigenvalues of G except $\mu_1 = 1$ is smaller than one, the power of their corresponding Jordan blocks, $J_{q_0}^k (q_0 \neq 1)$, will decay to zero exponentially as $k \to \infty$. Based on the above facts, when the index ℓ is fixed, the non-zero elements of $\tilde{G}_{c,a}(k,\ell)$ will converge to zero exponentially as $k \to \infty$. Hence, there exists a bounded $c_\delta > 0$ and a constant ρ_δ that is sufficiently close to zero and satisfies $\varphi \leq \rho_\delta < 1$, such that $\left\|\tilde{G}_{c,a}(k,\ell)\right\|_F^2$ is upper bounded by

$$\left\|\tilde{G}_{c,a}(k,\ell)\right\|_F^2 \leq c_\delta \rho_\delta^{k-\ell}. \qquad (39)$$

Then, it can be derived that

$$\begin{aligned}\sum_{\ell=0}^{k-\tau_e-1} \left\|\tilde{G}_{c,a}(k,\ell)\right\|_F^2 \sigma_\ell^2 \leq & c_\delta \sigma_0^2 \rho_\delta^k \sum_{\ell=0}^{k-\tau_e-1} \left(\frac{\varphi^2}{\rho_\delta}\right)^\ell \\ \leq & c_\delta \sigma_0^2 \rho_\delta^k (k-\tau_e), \qquad (40)\end{aligned}$$

which will converge to zero when $k \to \infty$.

As for ②, it only contains τ_e terms and will converge to zero when $k \to \infty$, because $\left\|\tilde{G}_{c,b}(k,\ell)\right\|_F^2$ is strictly bounded and $\varphi^{2\ell}$ converges exponentially fast. Finally, we obtain that (36) will converge to zero and complete the proof of (22). □

E. Proof of Theorem 3

Proof. The derivation of ρ_m under the TPMC algorithm strictly follows the definition in (24).

Based on the definition of $\delta(k)$, we obtain

$$\begin{aligned}\delta(k+1) &= \begin{bmatrix} \tilde{p}(k+1) \\ v(k+1) \end{bmatrix} - \begin{bmatrix} \tilde{p}^*(k+1) \\ v^*(k+1) \end{bmatrix} \\ &= G \begin{bmatrix} \tilde{p}(k) \\ v(k) \end{bmatrix} + \begin{bmatrix} \frac{T^2}{2}\theta(k) \\ T\theta(k) \end{bmatrix} - G \begin{bmatrix} \tilde{p}^*(k) \\ v^*(k) \end{bmatrix} \\ &= G\delta(k) + \begin{bmatrix} \frac{T^2}{2}\theta(k) \\ T\theta(k) \end{bmatrix}.\end{aligned}$$

Similar to (13), $\delta(k)$ can be expanded as

$$\delta(k) = G^k \delta(0) + \Lambda(k). \qquad (41)$$

Therefore, it can be derived that

$$\begin{aligned}\delta(k)^\intercal \delta(k) =& \delta(0)^\intercal G^{k\intercal} G^k \delta(0) + \Lambda(k)^\intercal \Lambda(k) \\ &+ \delta(0)^\intercal G^k \Lambda(k) + \Lambda(k)^\intercal G^{k\intercal} \delta(0). \qquad (42)\end{aligned}$$

By taking expectation on $\delta(k)^\intercal \delta(k)$, we have

$$\begin{aligned}&\mathbb{E}[\delta(k)^\intercal \delta(k)] = \delta(0)^\intercal G^{k\intercal} G^k \delta(0) \\ &+\mathbb{E}\left[\sum_{\ell=0}^{k-1} \theta(\ell)^\intercal \begin{bmatrix} \frac{T^2}{2} I_N & TI_N \end{bmatrix} G^{k-\ell\intercal} G^{k-\ell} \begin{bmatrix} \frac{T^2}{2} I_N \\ TI_N \end{bmatrix} \theta(\ell)\right].\end{aligned}$$

Let $M_{k-\ell}^\intercal = \begin{bmatrix} \frac{T^2}{2} I_N & TI_N \end{bmatrix} G^{k-\ell\intercal}$, we have

$$\mathbb{E}[\delta(k)^\intercal \delta(k)] = \delta(0)^\intercal G^{k\intercal} G^k \delta(0) + \sum_{\ell=0}^{k-1} (\epsilon C\varphi)^{2\ell} \mathrm{tr}(M_{k-\ell}^\intercal M_{k-\ell}),$$

where $C = \sum_{m=0}^{\tau_e} |c_m|$ is the constant depending on the perturbation sequence $\{c_m\}_{m=0}^{\tau_e}$, and $\mathrm{tr}(\cdot)$ indicates the trace of a matrix. For any matrices A and B, inequalities $\mathrm{tr}(A^\intercal A) = \|A\|_F^2$ and $\|AB\|_F \leq \|A\|_F \|B\|_F$ hold true. Furthermore, $\left\|\begin{bmatrix} \frac{T^2}{2} I_N & TI_N \end{bmatrix}\right\|_F^2 = N\left(\frac{T^4}{4} + T^2\right)$. Therefore, it can be derived that

$$\begin{aligned}\mathbb{E}[\delta(k)^\intercal \delta(k)] \leq & \delta(0)^\intercal G^{k\intercal} G^k \delta(0) \\ &+ N\left(\frac{T^4}{4} + T^2\right) \sum_{\ell=0}^{k-1} (\epsilon C\varphi)^{2\ell} \|G\|_F^{2k-2\ell},\end{aligned}$$

with both terms on the RHS being non-negative. The factors related to k are $\mu_m(G)^{2k}$ and $\max\{(\epsilon C\varphi)^{2k}, \mu_m(G)^{2k}\}$, respectively. According to (24), we have

$$\rho_m \triangleq \lim_{k\to\infty} \left(\mu_m(G)^{2k} + \max\{(\epsilon C\varphi)^{2k}, \mu_m(G)^{2k}\}\right)^{\frac{1}{k}}. \qquad (43)$$

One thus concludes that the mean square convergence rate is ρ_m, which is dependent on the matrix G and the perturbation signals designed by the algorithm. The proof is completed. □

F. Proof of Theorem 5

Proof. Similar to [36], we consider the compact Singular Value Decomposition (SVD) of $Y_\theta(k)$ as $Y_\theta(k) = U\Sigma V^\intercal$, where $U \in \mathbb{R}^{2N\times 2N}$ and $V \in \mathbb{R}^{k\times k}$ are unitary matrices such that $UU^\intercal = I$ and $VV^\intercal = I$. Note that we have $\Delta_G(k) = \Theta(0;k) Y_\theta(k)^\intercal (Y_\theta(k) Y_\theta(k)^\intercal)^{-1}$, which implies that

$$\begin{aligned}\|\Delta_G(k)\| &= \left\|\Theta(0;k) Y_\theta(k)^\intercal (Y_\theta(k) Y_\theta(k)^\intercal)^{-1}\right\| \\ &\leq \sqrt{1/\lambda_{\min}(Y_\theta(k) Y_\theta(k)^\intercal)}\, \|\Theta(0;k)V\|.\end{aligned}$$

To analyze the characteristic of $\sqrt{1/\lambda_{\min}(Y_\theta(k) Y_\theta(k)^\intercal)}$, we need to recall that

$$\lambda_{\min}(Y_\theta(k) Y_\theta(k)^\intercal) = \lambda_{\min}\left(\sum_{\ell=0}^{k-1} x(\ell) x(\ell)^\intercal\right).$$

According to Theorem 1 in [38], for any matrix G, the following inequality holds true:

$$\lambda_{\min}\left(\sum_{\ell=0}^{k-1} \Gamma_\ell(G)\right) \geq \frac{1}{2\varepsilon^2} \log\left(\frac{1}{3\delta_G}\right),$$

This article has been accepted for publication in IEEE Journal of Selected Topics in Signal Processing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2024.3421898

where $\Gamma_\ell(G) = \sum_{s=0}^{\ell} G^\ell G^{\ell\mathsf{T}}$ is the finite-time controllability Gramian of the system, and ε, δ_G describe the accuracy of the OLS estimator. Therefore, it can be concluded that

$$\sqrt{1/\lambda_{\min}(Y_\theta(k)Y_\theta(k)^\mathsf{T})} = \mathcal{O}(1).$$

Based on (21) and the variances of the perturbation signals, the expectation of $\|\Theta(0;k)\|_F^2$ can be written as

$$\mathbb{E}\left[\|\Theta(0;k)\|_F^2\right] = \left(\frac{T^2}{2}+T\right)N\cdot\mathbb{E}\left[\sum_{x=0}^{k-1}\theta_i(k)^2\right],$$

$$=\left(\frac{T^2}{2}+T\right)N\left[\sum_{x=0}^{\tau_e}\sum_{m=0}^{x}c_m^2\varphi^{2(x-m)}+\sum_{x=\tau_e+1}^{k-1}\sum_{m=0}^{\tau_e}c_m^2\varphi^{2(x-m)}\right].$$

Since $\|A\| \leq \|A\|_F$ holds for every matrix A and the unitary matrix $U \in \mathbb{R}^{n\times n}$ satisfies $\|U\| = 1$, it derives that

$$\mathbb{E}\left[\|\Theta(0;k)V\|\right] = \begin{cases}\mathcal{O}(1), & \varphi < 1,\\ \mathcal{O}(\sqrt{k}), & \varphi = 1.\end{cases}$$

Combining the result in Theorem 4 and

$$\lim_{k\to\infty}\mathbb{E}\left[\|\Delta_G(k)\|\right] = \begin{cases}\mathcal{O}(1), & \varphi < 1,\\ \mathcal{O}(\sqrt{k}), & \varphi = 1,\end{cases}$$

the proof is completed. □

References

[1] Z. Wang, Y. Li, X. Duan, and J. He, "Topology-preserving second-order consensus: A strategic compensation approach," in *IEEE Conference on Decision and Control*, 2023, pp. 399–404.

[2] S.-Y. Tu and A. H. Sayed, "Mobile adaptive networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 4, pp. 649–664, 2011.

[3] D. S. Drew, "Multi-agent systems for search and rescue applications," *Current Robotics Reports*, vol. 2, no. 2, pp. 189–200, 2021.

[4] X. Duan and F. Bullo, "Markov chain–based stochastic strategies for robotic surveillance," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 4, pp. 243–264, 2021.

[5] M. Brambilla, E. Ferrante, M. Birattari, and M. Dorigo, "Swarm robotics: A review from the swarm engineering perspective," *Swarm Intelligence*, vol. 7, pp. 1–41, 2013.

[6] S. Yazdani and M. Haeri, "Flocking of multi-agent systems with multiple second-order uncoupled linear dynamics and virtual leader," *IET Control Theory & Applications*, vol. 10, no. 8, pp. 853–860, 2016.

[7] X. Dong, Y. Zhou, Z. Ren, and Y. Zhong, "Time-varying formation tracking for second-order multi-agent systems subjected to switching topologies with application to quadrotor formation flying," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5014–5024, 2016.

[8] Y. Yang, J. Li, and L. Peng, "Multi-robot path planning based on a deep reinforcement learning DQN algorithm," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 3, pp. 177–183, 2020.

[9] J. Spletzer, A. K. Das, R. Fierro, C. J. Taylor, V. Kumar, and J. P. Ostrowski, "Cooperative localization and control for multi-robot manipulation," in *IEEE International Conference on Intelligent Robots and Systems*, vol. 2, 2001, pp. 631–636.

[10] Y. Emam, S. Mayya, G. Notomista, A. Bohannon, and M. Egerstedt, "Adaptive task allocation for heterogeneous multi-robot teams with evolving and unknown robot capabilities," in *IEEE International Conference on Robotics and Automation*, 2020, pp. 7719–7725.

[11] Y. Li, J. He, L. Cai, and X. Guan, "Local topology inference of mobile robotic networks under formation control," *IEEE Transactions on Automatic Control*, vol. 68, no. 11, pp. 6450–6465, 2023.

[12] J. Li, J. He, Y. Li, and X. Guan, "Unpredictable trajectory design for mobile agents," in *American Control Conference*, 2020, pp. 1471–1476.

[13] M. Taheri, K. Khorasani, I. Shames, and N. Meskin, "Undetectable cyber attacks on communication links in multi-agent cyber-physical systems," in *IEEE Conference on Decision and Control*, 2020, pp. 3764–3771.

[14] H. Bai and J. T. Wen, "Cooperative load transport: A formation-control perspective," *IEEE Transactions on Robotics*, vol. 26, no. 4, pp. 742–750, 2010.

[15] S. Segarra, A. G. Marques, G. Mateos, and A. Ribeiro, "Network topology inference from spectral templates," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 3, pp. 467–483, 2017.

[16] M. Laghate and D. Cabric, "Learning wireless networks' topologies using asymmetric granger causality," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 233–247, 2018.

[17] H. J. van Waarde, P. Tesi, and M. K. Camlibel, "Topology identification of heterogeneous networks: Identifiability and reconstruction," *Automatica*, vol. 123, p. 109331, 2021.

[18] Y. Du, B. Liu, V. Moens, Z. Liu, Z. Ren, J. Wang, X. Chen, and H. Zhang, "Learning correlated communication topology in multi-agent reinforcement learning," in *International Conference on Autonomous Agents and Multi-Agent Systems*, 2021, pp. 456–464.

[19] H. E. Egilmez, E. Pavez, and A. Ortega, "Graph learning from data under Laplacian and structural constraints," *IEEE Journal of Selected Topics in Signal Processing*, vol. 11, no. 6, pp. 825–841, 2017.

[20] G. Mateos, S. Segarra, A. G. Marques, and A. Ribeiro, "Connecting the dots: Identifying network structure via graph signal processing," *IEEE Signal Processing Magazine*, vol. 36, no. 3, pp. 16–43, 2019.

[21] Y. Zhu, M. T. Schaub, A. Jadbabaie, and S. Segarra, "Network inference from consensus dynamics with unknown parameters," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 6, pp. 300–315, 2020.

[22] B. Zaman, L. M. L. Ramos, D. Romero, and B. Beferull-Lozano, "Online topology identification from vector autoregressive time series," *IEEE Transactions on Signal Processing*, vol. 69, pp. 210–225, 2020.

[23] B. Nielsen, "Strong consistency results for least squares estimators in general vector autoregressions with deterministic terms," *Econometric Theory*, vol. 21, no. 3, pp. 534–561, 2005.

[24] T. Dong, X. Bu, and W. Hu, "Distributed differentially private average consensus for multi-agent networks by additive functional Laplace noise," *Journal of the Franklin Institute*, vol. 357, no. 6, pp. 3565–3584, 2020.

[25] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[26] W. Zheng, C. Fang, J. He, and Y. Peng, "Resilient average consensus of second-order multi-agent systems," in *American Control Conference*, 2022, pp. 1466–1471.

[27] M. Sader, Z. Chen, Z. Liu, and C. Deng, "Distributed robust fault-tolerant consensus control for a class of nonlinear multi-agent systems with intermittent communications," *Applied Mathematics and Computation*, vol. 403, pp. 126–166, 2021.

[28] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Transactions on Automatic Control*, vol. 50, no. 5, pp. 655–661, 2005.

[29] W. Ni and D. Cheng, "Leader-following consensus of multi-agent systems under fixed and switching topologies," *Systems & Control Letters*, vol. 59, no. 3-4, pp. 209–217, 2010.

[30] G. Wen, G. Hu, W. Yu, J. Cao, and G. Chen, "Consensus tracking for higher-order multi-agent systems with switching directed topologies and occasionally missing control inputs," *Systems & Control Letters*, vol. 62, no. 12, pp. 1151–1158, 2013.

[31] H. Sun, Z. Wang, J. Xu, and H. Zhang, "Exact consensus error for multi-agent systems with additive noises," *Journal of Systems Science and Complexity*, vol. 33, no. 3, pp. 640–651, 2020.

[32] V. Katewa, A. Chakrabortty, and V. Gupta, "Protecting privacy of topology in consensus networks," in *American Control Conference*, 2015, pp. 2476–2481.

[33] Z. Wang, Y. Li, C. Fang, and J. He, "Distributed topology-preserving collaboration algorithm against inference attack," in *American Control Conference*, 2022, pp. 2166–2171.

[34] W. Ren and Y. Cao, "Convergence of sampled-data consensus algorithms for double-integrator dynamics," in *IEEE Conference on Decision and Control*, 2008, pp. 3965–3970.

[35] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[36] M. Simchowitz, H. Mania, S. Tu, M. I. Jordan, and B. Recht, "Learning without mixing: Towards a sharp analysis of linear system identification," in *Conference on Learning Theory*, 2018, pp. 439–473.

[37] X. Ding, H. Wang, H. Li, H. Jiang, and J. He, "Robopheus: A virtual-physical interactive mobile robotic testbed," *arXiv preprint arXiv:2103.04391*, 2021.

[38] Y. Jedra and A. Proutiere, "Finite-time identification of linear systems: Fundamental limits and optimal algorithms," *IEEE Transactions on Automatic Control*, vol. 68, no. 5, pp. 2805–2820, 2023.

Zitong Wang (Student Member, IEEE) received the B.E. degree in Information Engineering from the School of Electronic Information and Electrical Engineering at Shanghai Jiao Tong University, China, in 2020. She is currently pursuing the Ph.D. degree in Control Science and Engineering at the Department of Automation, Shanghai Jiao Tong University. Her research interests include robotics, cooperative control, and distributed optimization in multi-agent systems.

Yushan Li (Student Member, IEEE) received the B.E. degree in School of Artificial Intelligence and Automation from Huazhong University of Science and Technology, Wuhan, China, in 2018. He is currently working toward the Ph.D. degree with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China.

He is a member of Intelligent of Wireless Networking and Cooperative Control group. His research interests include robotics, security of cyber-physical systems, and distributed computation in multi-agent networks.

Xiaoming Duan (Member, IEEE) obtained his B.E. degree in Automation from the Beijing Institute of Technology in 2013, his Master's Degree in Control Science and Engineering from Zhejiang University in 2016, and his PhD degree in Mechanical Engineering from the University of California at Santa Barbara in 2020. He is currently an assistant professor in the Department of Automation, Shanghai Jiao Tong University. His research interests include robotic surveillance, network systems, and decision making under uncertainties.

Jianping He (Senior Member, IEEE) is currently an associate professor in the Department of Automation at Shanghai Jiao Tong University. He received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013, and had been a research fellow in the Department of Electrical and Computer Engineering at University of Victoria, Canada, from Dec. 2013 to Mar. 2017. His research interests mainly include the distributed learning, control and optimization, security, and privacy in network systems.

Dr. He serves as an Associate Editor for IEEE Trans. Control of Network Systems, IEEE Open Journal of Vehicular Technology, and KSII Trans. Internet and Information Systems. He was also a Guest Editor of IEEE TAC, International Journal of Robust and Nonlinear Control, etc. He was the winner of Outstanding Thesis Award, Chinese Association of Automation, 2015. He received the best paper award from IEEE WCSP'17, the best conference paper award from IEEE PESGM'17, and was a finalist for the best student paper award from IEEE ICCA'17, and the finalist best conference paper award from IEEE VTC'20-FALL.