Received <day> <Month>, <year>; | Revised <day> <Month>, <year>; | Accepted <day> <Month>, <year>

DOI: xxx/xxxx

ARTICLE TYPE

Resilient Time-Varying Formation Tracking for Mobile Robot Networks under Deception Attacks on Positioning

Yen-Chen Liu[1] | Kai-Yuan Liu[1] | Zhuoyuan Song[2]

[1]Department of Mechanical Engineering, National Cheng Kung University, Tainan, Taiwan.
[2]Department of Mechanical Engineering, University of Hawai'i at Mānoa, Honolulu, HI, USA.

Correspondence
*Yen-Chen Liu, Department of Mechanical Engineering, National Cheng Kung University, Tainan, Taiwan. Email: yliu@mail.ncku.edu.tw

Funding Information
This research was supported by the Ministry of Science and Technology (MOST), Taiwan, under grants MOST 111-2636-E-006-004 and MOST 112-2636-E-006-001. Z. Song was partially supported by the U.S. National Science Foundation under awards CISE/IIS–2024928 and OIA-2032522.

Abstract

This paper investigates the resilient control, analysis, recovery, and operation of mobile robot networks in time-varying formation tracking under deception attacks on global positioning. Local and global tracking control algorithms are presented to ensure redundancy of the mobile robot network and to retain the desired functionality for better resilience. Lyapunov stability analysis is utilized to show the boundedness of the formation tracking error and the stability of the network under various attack modes. A performance index is designed to compare the efficiency of the proposed formation tracking algorithms in situations with or without positioning attacks. Subsequently, a communication-free decentralized cooperative localization approach based on extended information filters is presented for positioning estimate recovery where the identification of positioning attacks is based on Kullback–Leibler divergence. A gain-tuning resilient operation is proposed to strategically synthesize formation control and cooperative localization for accurate and rapid system recovery from positioning attacks. The proposed methods are tested using both numerical simulation and experimental validation with a team of quadrotors.

KEYWORDS:
Resilient control, time-varying formation tracking, deception attack, multi-robot systems, cooperative localization, mobile sensor networks.

1 | INTRODUCTION

Formation tracking and control are significant research topics for networked mobile robots such as unmanned ground vehicles[1,2] and autonomous aerial[3,4] or underwater vehicles[5,6]. Owing to the benefits of efficiency, redundancy, robustness, scalability, flexibility, and reliability, maintaining formation during the entire mission in mobile robot networks offers many advantages across various applications such as surveillance, drag reduction, source seeking, environmental sampling, search and rescue operations, aerial refueling, cooperative transportation, and closed-formation flight[7,8,9,10,11,12,13,14]. Although several formation-control approaches have been extensively studied including leader–follower, virtual structure, behavior-based, and consensus-based techniques, a common assumption in such studies has been the availability of inter-agent communication with accurate agent position information. In real-world applications, data transmission over cyber networks and the information shared between agents could become susceptible to not only adverse and malicious threats but also attacks that would crucially compromise or even destroy a networked robotic system[15,16].

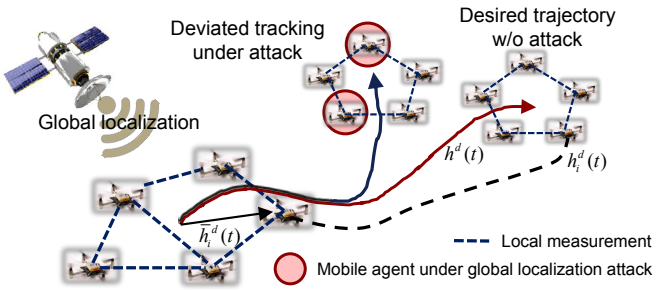

FIGURE 1 An illustration of time-varying formation tracking in mobile robot networks under global positioning attacks.

Although multi-agent systems are advantageous in various tasks with redundancy and scalability, the issues of actuator faults, fallible robots, and vulnerable communications, especially under deception attacks, have recently attracted significant attention[17,18,14,19,20]. Connectivity preservation with respect to robot failures was addressed by[17], where a self-optimization of resilient topologies and experimental validation were provided. The problem of multi-agent systems in achieving a fixed formation under mismatched compasses, which would lead to distortion, has been studied with estimation and compensation algorithms[18]. In[19], the authors proposed a consensus strategy to deal with deception attacks on relative information and keep the normal agents achieving the common value. Alternatively, a similar problem is investigated via distributed optimization in[20] to alleviate the influence of deception attacks. However, most of these works did not consider that the attacked agents might recover and return to the system. The system's performance is degraded if too many agents are considered malicious and cannot contribute to the task. Moreover, there is no performance index to evaluate how the system is affected under failures or attacks.

Accurate localization is a crucial prerequisite for the control and coordination of multi-robot systems. Although decentralized multi-agent coordination methods tend to alleviate the system-wide disruption caused by localization failures of individual agents, the resulting control error eventually leads to sub-optimal performance across the entire network. In many applications, such as underwater robotics and indoor navigation, it is challenging or infeasible to provide constant global positioning information to all agents in a network[21,22,23]. When computational resources allow and the environment is structured, persistently reliable localization can be achieved through simultaneous localization and mapping[24]. Cooperative localization is often applied to enable inter-agent observation and information fusion, thereby reducing the localization error propagation and maximizing the utilization of locally available global positioning information[25,26]. Nonetheless, it is often assumed that inter-agent communication is available, making the system susceptible to communication failures and security complications.

In this paper, we study the time-varying formation control (TVFC) of a mobile robot network in the absence of inter-agent communication, thereby mitigating potential vulnerabilities to global positioning information attacks or failures. The mobile robot network is controlled to track prescribed formations by utilizing global positioning information and local inter-agent relative displacements obtained from proximity and/or bearing sensors. Although certain cyber-attacks can be avoided by adopting a communication-free framework, attacks on global positioning systems could cause catastrophic failures in multi-agent formation control. To retain the desired functionality of such systems under positioning attacks or failures, a fault detection and isolation scheme based on Kullback-Leibler (KL) divergence is proposed for identifying positioning attacks. Subsequently, a communication-free decentralized cooperative localization approach based on extended information filters (EIF) is proposed to enhance the resilience of the mobile robot network in TVFC. The system is designed using a resilient gain-tuning formation-control approach to enhance the resilience and robustness of the multi-agent systems in the presence of adverse effects. Systematic studies and analyses on the proposed approach for multi-robot formation tracking were performed. To provide a deeper understanding of the resilience of a mobile robot network in TVFC, the resilience triangle from the performance index of TVFC is investigated. Results from numerical simulations and experimental implementations on a group of quadrotor flying robots are presented to demonstrate system efficiency and performance in terms of improving the resilience of mobile robot networks.

The main contributions of this paper are summarized as follows:

1. TVFC of mobile robot networks is studied under a hierarchical architecture, with the design of the performance index representing the local and global tracking efficiency.

2. The adversarial effects of three positioning information attacks, i.e. additive attack, hybrid attack, and unstable attack, on the performance of formation control are investigated through Lyapunov stability analysis. Note that unstable attacks are the most dangerous case for the system stability if the attacker has access to the system information.

3. A resilient localization system is presented that identifies positioning attacks based on the KL divergence in fusing global positioning information with inertial navigation, and maintains consistent localization for the compromised agents using a communication-free, decentralized cooperative localization method based on EIF.

4. Resilient operation utilizing the results of cooperative localization is demonstrated to mitigate adverse impacts on a mobile robot network subjected to global positioning attacks. Compared to related works, the agent can return to the system if the attack is gone. This feature plays an important role in keeping the system's resilience.

5. Experimental validation using a group of quadrotor flying robots is presented to demonstrate the efficacy and efficiency of the proposed resilient methods for TVFC of multi-robot systems. Moreover, the proposed performance index is effective in showing the tracking result.

The remainder of this paper is organized as follows. Section 2 addresses the modeling, sensory graph, and problem formulation of TVFC for a mobile robot network. Section 3 presents a theoretical analysis of the mobile robot network and the effects of malicious attacks on the performance of the TVFC. Cooperative localization, attack detection, position recovery, and resilient operation are discussed in Section 4. Section 5 presents an experimental validation of the proposed networked robot system. Section 6 provides a discussion of the proposed resilient robotic systems and summarizes possible future directions on TVFC for mobile robot networks.

2 | PRELIMINARIES AND PROBLEM FORMULATION

2.1 | Robot Modeling and Sensory Graph

In this subsection, the definition of modeling of robots and the sensory graph in this work is provided as preliminaries. Consider a mobile robot network composed of $N \geq 3$ dynamically controlled and fully-actuated mobile agents described as

$$\ddot{x}_i = u_i, \quad i = 1, \dots, N, \tag{1}$$

where $x_i \in \mathcal{Q}$ and $u_i \in \mathcal{U}_i$ with $\mathcal{Q} \subset \mathbb{R}^n$ as the compact set of the state space and $\mathcal{U}_i \subset \mathbb{R}^n$ as the admissible control set of u_i.

The time-varying formation tracking for mobile robot network is studied in this paper in the absence of inter-robot communication so that we have the next assumption.

Assumption 1. The mobile agents in the robot network are equipped with range and bearing sensors that can obtain a reliable relative position with respect to their neighbors. This so-called local displacement measurement is mutual; that is, the i^{th} robot can obtain the measurement from the j^{th} robot and vice versa.

The graph theory[27] is utilized to describe the displacement measurement topologies (sensory graph) among N agents in the network. For an interconnected graph $\mathcal{G}(\mathcal{W})$, the set of vertices is given as $\mathcal{V}(\mathcal{G})$, the set of edges is denoted by $\mathcal{E}(\mathcal{G}) \in \mathcal{V}(\mathcal{G}) \times \mathcal{V}(\mathcal{G})$, and the weight matrix $\mathcal{W} = \{w_{ij}\}$ denotes the weighting for each of the edges in $\mathcal{E}(\mathcal{G})$. With Assumption 1 and the graph describing the sensory topology, $\mathcal{G}(\mathcal{W})$ is undirected such that $w_{ij} = w_{ji}$. The interconnection between the N mobile robots in the network can be described by the weighted Laplacian matrix $L(\mathcal{G}) \in \mathbb{R}^{N\times N}$ [28,17] defined as $L(\mathcal{G}) = D(\mathcal{G}) - A(\mathcal{G})$, where $D(\mathcal{G})$ is the degree matrix of $\mathcal{G}$, and $A(\mathcal{G})$ is the corresponding adjacency matrix with entries $a_{ij} = w_{ij}$. The diagonal terms of the Laplacian matrix are given as $[L(\mathcal{G})]_{ii} = \sum_{j=1}^{N} w_{ij}$, and the off-diagonal elements of the Laplacain matrx are given as $[L(\mathcal{G})]_{ij} = -w_{ij}$ for $i \neq j$.

To achieve formation tracking for the mobile robot network, the graph $\mathcal{G}$ should be connected so that the robots can obtain the inter-robot displacement. The Laplacian matrix of an undirected graph $\mathcal{G}$ exhibits the following property:

Property 1. For an undirected graph $\mathcal{G}$, the eigenvalues of its Laplacian matrix, λ_i $(i = 1, \dots, N)$, are real and can be ordered such that $0 = \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_N$. Additionally, if $\mathcal{G}$ is connected, then λ_2 is positive and called the algebraic connectivity of the graph.

Given a graph $\mathcal{G}(\mathcal{W})$, let us denote $\mathcal{N}_i$ as the set of the neighbors of the i^{th} robot, which has a direct edge to the j^{th} robot for $j \in \mathcal{N}_i$. Thus, the i^{th} robot is able to obtain the displacement to $j \in \mathcal{N}_i$ by using the proximity sensors on the i^{th} robot. By

denoting the displacement vector $r_{ji}(t) = x_i(t) - x_j(t)$, the distance between the i^{th} and j^{th} robots are given as $d_{ji}(t) = \|r_{ji}(t)\|$, where $\|\cdot\|$ denotes the Euclidean norm of the enclosed vector. Since the local displacement measurement is mutual, the sensory topology $\mathcal{G}(\mathcal{W})$ being undirected leads to $r_{ji}(t) = -r_{ij}(t)$ and $d_{ji}(t) = d_{ij}(t)$. The formation of the mobile robot network is constructed by utilizing r_{ji} according to the inter-agent measurement topologies without data exchange[a]. Thus, we have the next assumption for the proposed networked system:

Assumption 2. There is no inter-agent communication or data exchange in the robot network.

2.2 | Global and Local Formation Tracking

Before entering the problem formulation, we first give the definitions of formation tracking to develop our resilient control scheme. The time-varying global trajectory of the desired formation with respect to Σ_W, the world coordinates, is predefined and denoted by $h^d(t) : [0, \infty) \to \mathcal{Q}$, which is a twice differentiable continuous function of time. As illustrated in Fig. 1, the desired formation of mobile robots are described by $\bar{h}_i^d(t) : [0, \infty) \to \mathcal{Q}$, which are time-varying continuous vectors, with respect to $h^d(t)$. Subsequently, the time-varying desired trajectories for each of the mobile robots, $h_i^d(t) \in \mathcal{Q}$, are given as $h_i^d(t) = h^d(t) + \bar{h}_i^d(t)$, $i = 1, \dots, N$. For the mobile agents to achieve time-varying formation, the desired relative displacement between the i^{th} robot and its neighbors, $j \in \mathcal{N}_i$, are expressed by $h_{ji}^d(t) = \bar{h}_i^d(t) - \bar{h}_j^d(t)$, which further leads to $h_{ji}^d(t) = h_i^d(t) - h_j^d(t)$ and $h_{ij}^d(t) = -h_{ji}^d(t)$.

Let $\mathcal{X}_0$ be a subset of the compact set $\mathcal{Q}$ such that $\mathcal{X}_0 \subseteq \mathcal{Q}$ is closed and bounded. Time-varying formation tracking can be defined for local formation tracking and global formation tracking, respectively.

Definition 1. (Local Formation Tracking) The networked robot system (1) is said to achieve local formation tracking if for any given initial states $x_i(0) \in \mathcal{X}_0$, $i = 1, \dots, N$, the states satisfy that $\lim_{t\to\infty} \left[(x_i(t) - x_j(t)) - (\bar{h}_i^d(t) - \bar{h}_j^d(t))\right] = 0$, for all $j \in \mathcal{N}_i$, which implies that $\lim_{t\to\infty} r_{ji}(t) = \lim_{t\to\infty} h_{ji}^d(t)$.

Definition 2. (Global Formation Tracking) The networked robot system (1) is said to achieve global formation tracking if for any given initial states $x_i(0) \in \mathcal{X}_0$, $i = 1, \dots, N$, the states satisfy that $\lim_{t\to\infty} \left(x_i(t) - h_i^d(t)\right) = 0$.

The problem can be considered as a hierarchical framework consisting of local and global formation tracking systems. Therefore, in the proposed mobile robot network, global formation tracking (Definition 2) is the sufficient condition for local formation tracking, and local formation tracking (Definition 1) is necessary for global formation tracking.

2.3 | Problem Formulation

The time-varying formation tracking for a mobile robot network is studied in this paper, as illustrated in Figure 1. Based on the dynamics (1), the N mobile agents are controlled to maintain a time-varying formation based on the global positioning and local relative displacement measurements. The global positioning measurements can be obtained from the GPS (global positioning system) outdoors or other indoor/outdoor positioning and tracking systems. It is noted that we use the term 'GPS' generally to refer to any global positioning systems, e.g. location based service in mobile devices, WiFi positioning system, or optical localization system. In the proposed system, each robot can obtain global positioning data for the global formation tracking as addressed in Definition 2.

The local measurement is implemented by extrinsic sensors on each of the mobile agents to obtain the relative displacement to all its neighbors. Moreover, the relative velocity between two adjacent robots can also be obtained accordingly. The local positioning information is utilized to control the robot network for achieving local formation tracking as stated in Definition 1. Since there is no communication between the mobile agents, the desired trajectories of an agent's neighbors are important in achieving the time-varying formation tracking. Thus, we have the next assumption:

Assumption 3. The desired formation trajectories $h^d(t)$, $h_i^d(t)$, and $h_j^d(t)$ for $j \in \mathcal{N}_i$ are available to the i^{th} robot.

We consider the situation that the signals transmitted from the global positioning systems to the mobile robots may go under deception attacks[29,30,31]. Let us define the position of the i^{th} robot from the global positioning system as $x_i^g(t)$, which might be different from the actual position $x_i(t)$ depending on condition of the positioning system. If the global positioning signal is

[a] The argument of time dependent signals is omitted, for example $r_{ji} \equiv r_{ji}(t)$, unless otherwise required for the sake of clarity.

accurate, we have $x_i^g(t) = x_i(t)$. However, if the global positioning signal is under deception attacks, then the erroneous position data $\hat{x}_i^g(t)$ is described as

$$\hat{x}_i^g(t) = \delta_{xi}(t)x_i(t) + \Delta_{xi}(t), \tag{2}$$

where $\delta_{xi}(t) \in \mathbb{R}$ is a time-varying function, and $\Delta_{xi}(t) \in \mathbb{R}^n$ is a continuous function.

3 | TIME-VARYING FORMATION TRACKING AND DECEPTION ATTACKS

In this section, we propose our controller to achieve formation tracking for mobile robot network and address the influence of deception attack on global positioning signal. According to the definitions given in Section 2, the purpose of our controller is to deal with the global and local formation tracking problem. By doing so, the redundancy of controller is improved for the design of a resilient algorithm. This feature is one of the main contributions in this work. Furthermore, the impact of deception attack is theoretically analyzed and illustrated by numerical examples. To evaluate the influence of attack, the performance index is provided to quantify the tracking performance of the systems.

3.1 | Formation Tracking Control Design and Analysis

For dynamically controlled mobile agents, let us consider the time-varying formation tracking control

$$u_i(t) = \ddot{h}_i^d - \sigma_{fi}(\dot{x}_i - \dot{h}_i^d) - \kappa_{gi} f_i^g(t) - \kappa_f f_i^l(t), \tag{3}$$

where $\sigma_{fi} \in \mathbb{R}^{n\times n}$ is a positive-definite matrix, $\kappa_f, \kappa_{gi} \in \mathbb{R}$ are positive gains for local and global formation tracking, respectively, and

$$f_i^l(t) = \sum_{j\in\mathcal{N}_i} w_{ji}(\dot{r}_{ji} - \dot{h}_{ji}^d) + \sigma_{fi} \sum_{j\in\mathcal{N}_i} w_{ji}\left(r_{ji} - h_{ji}^d\right), \tag{4}$$

$$f_i^g(t) = (\dot{x}_i - \dot{h}_i^d) + \sigma_{fi}\left(x_i^g - h_i^d\right) \tag{5}$$

are the formation tracking control commands. In the control input (3), the relative displacement r_{ji} and velocity $\dot{r}_{ji}$ are obtained by the sensors mounted on each of the mobile robots as mentioned in Section 2. The velocity of the mobile robot $\dot{x}_i$ with respect to Σ_W can be obtained from inertial navigation systems, e.g. an inertial measurement unit (IMU), or an odometry system such as visual odometry. It is noted that the global positioning data, $x_i^g(t)$, are required in formation tracking because the absolute position obtained from the integration of the velocity data are not reliable or accurate enough to be implemented in the formation control due to the accumulative drifting errors.

Assumption 4. All robots start from initial positions that are known or measurable by its neighbors.

By denoting $\tilde{x}_i := x_i - h_i^d$ as the global tracking error and $e_i = \sum_{j\in\mathcal{N}_i} w_{ji}(\tilde{x}_i - \tilde{x}_j)$ as the accumulated inter-agent errors with respect to the weighted Laplacian $L(\mathcal{G})$, we have $r_{ji} - h_{ji}^d = \left(x_i - x_j\right) - (h_i^d - h_j^d) = \tilde{x}_i - \tilde{x}_j$. If the position of the mobile agents in the robot network can be obtained accurately such that $x_i^g(t) = x_i(t)$, the closed-loop dynamics is given as $\ddot{\tilde{x}}_i + \kappa_{gi}\dot{\tilde{x}}_i + \kappa_f\dot{e}_i = -\sigma_{fi}\dot{\tilde{x}}_i - \sigma_{fi}\kappa_{gi}\tilde{x}_i - \sigma_{fi}\kappa_f e_i$. Given $\xi_i = \dot{\tilde{x}}_i + \kappa_{gi}\tilde{x}_i + \kappa_f e_i$, the above equation becomes $\dot{\xi}_i = -\sigma_{fi}\xi_i$. Hence, under Assumptions 1 through 4, we have the following result for the mobile robot network with perfect global positioning information.

Theorem 1. For the mobile robot network described by (1) under a connected and undirected displacement sensory graph $\mathcal{G}$ with weighted Laplacian matrix $L(\mathcal{G})$, if the global positioning data are accurate such that $x_i^g(t) = x_i(t)$ for $i = 1, \ldots, N$, then the control input (3) guarantees that the mobile robot network achieves global formation tracking.

A proof of Theorem 1 is provided in Appendix A.1. This theorem demonstrates that the guarantee of global formation tracking (Definition 2) can also ensure local formation tracking (Definition 1) as addressed in Section 2. The tracking performance of the local and global formation is highly dependent on the values of κ_f and κ_{gi} in (A.1). Let us first consider the case where there is only global formation tracking such that $\kappa_f = 0$, then the closed-loop dynamics becomes $\ddot{\tilde{x}}_i + \kappa_{gi}\dot{\tilde{x}}_i = -\sigma_{fi}\dot{\tilde{x}}_i - \sigma_{fi}\kappa_{gi}\tilde{x}_i$. By denoting $\xi_i^g = \dot{\tilde{x}}_i + \kappa_{gi}\tilde{x}_i$, the given closed-loop system becomes $\dot{\xi}_i^g = -\sigma_{fi}\xi_i^g$. It is noted that there is no inter-agent term in the closed-loop dynamics because this case considers only global positioning signals; thus, the mobile robot network becomes a decoupled system for trajectory tracking. Hence, by considering $V_i^g(\xi_i^g) = \frac{1}{2}(\xi_i^g)^T\sigma_{fi}^{-1}\xi_i^g$, we have $\dot{V}_i^g = -(\xi_i^g)^T\xi_i^g$, which is

negative definite. Therefore, we conclude that $\lim_{t\to\infty} \xi_i^g(t) = 0$ by following the proof of Theorem 1. From the closed-loop control system, we further have $\dot{\tilde{x}}_i = -\kappa_{gi}\tilde{x}_i + \xi_i^g$. As shown in[32,33], if $\xi_i^g(t)$ is a signal that asymptotically converges to zero, and $\tilde{x}_i$ is bounded, then $\lim_{t\to\infty} \tilde{x}_i(t) = 0$, which implies that $\lim_{t\to\infty} \left(x_i(t) - h_i^d(t)\right) = 0$, $i = 1, \ldots, N$. Consequently, the mobile robot network achieves global formation tracking, as stated in Definition 2.

Next, let us consider the case of formation tracking with only local measurements such that $\kappa_{gi} = 0$. For the mobile robot network with an undirected and connected displacement sensory graph $\mathcal{G}$, the closed-loop dynamics is described as $\ddot{\tilde{x}}_i + \kappa_f \dot{e}_i = -\sigma_{fi}\dot{\tilde{x}}_i - \sigma_{fi}\kappa_f e_i$. From $\xi_i^l = \dot{\tilde{x}}_i + \kappa_f e_i$, the stacked dynamics $\dot{\xi}_i^l = -\sigma_{fi}\xi_i^l$ can be proved to be asymptotically stable by considering $V^l(\xi_i^l) = \frac{1}{2}(\xi^l)^T\sigma_{fi}^{-1}\xi^l$, where ξ^l is the stacked vector of ξ_i^l. With $\dot{V}^l = -(\xi^l)^T\xi^l$, we obtain that $\xi^l \in \mathcal{L}_2 \cap \mathcal{L}_\infty$ and $\lim_{t\to\infty} \xi^l(t) = 0$. By following (A.1) in the proof of Theorem 1, the stacked form is given as $\dot{\tilde{x}} = -[(\kappa_f L) \otimes I_n]\tilde{x} + \xi^l$ with $\kappa_{gi} = 0$. For $\xi^l(t)$ converging to the origin, the mobile robot network achieves consensus to the agreement set that is the subspace of $span\{1\}$ such that $\tilde{x}_i(t) = \tilde{x}_j(t)$, $i = 1, \ldots, N$, $j \in \mathcal{N}_i$ when $t \to \infty$[28]. Therefore, from the definition of $\tilde{x}_i(t)$, we obtain $\lim_{t\to\infty} r_{ji}(t) = \lim_{t\to\infty} h_{ji}^d(t)$ so that local formation tracking is guaranteed.

3.2 | Malicious Attacks on Global Positioning Signal

By following the analysis in Section 3.1, we obtain that local formation tracking can be ensured with or without global positioning information. In the proposed system, the resilience of the networked robot system is guaranteed based on the inter-agent position information. If formation tracking errors are abnormally large due to initial conditions, an erroneous judgement could occur and significantly influence the resilient efficacy. Therefore, in this system, we consider the following assumption:

Assumption 5. The mobile robot network has achieved asymptotic stability before any agents are subject to adversarial attacks on global positioning signals such that attacks occur at $t = t_{ai} \geq 0$ and $q_i \in \mathcal{Q}_{as}$, $\forall i = 1, \ldots, N$, where $\mathcal{Q}_{as} = \{q_i := (\tilde{x}_i^T, \dot{\tilde{x}}_i^T)^T \mid \|\tilde{x}_i\|_2, \|\dot{\tilde{x}}_i\|_2 < \epsilon\}$ with sufficiently small ϵ, t_{ai} is the time at which the attack on the ith agent starts.

The influence on the system due to malicious attacks depends on its features[31]. For a deep understanding of the deception attack defined in (2), it is classified into three types, named additive attack, hybrid attack, and unstable attack, to investigate the effect of each parameter in (2). The deception attack with $\delta_{xi} = 1$ is an additive attack; otherwise it's a hybrid attack. Compared with additive attack, hybrid attack is more related to original data x_i. Additionally, an unstable attack is defined as $\hat{x}_i^g(t) = x_i(t) - c_{ai}\xi_i(t)$, where c_{ai} is a coefficient of the attack model. By choosing the same Lyapunov function candidate in Theorem 1, it is derived as $\dot{V}_i = (\kappa_{gi}c_{ai} - 1)\xi_i^T\xi_i$. Obviously, if $\kappa_{gi}c_{ai} > 1$, $\dot{V}_i$ is positive definite, which means that the system is unstable. So far, the influence of attacks is analyzed, but there is no evaluation as a standard to tell how serious the attack is for comparison. How to quantify the influence of attack is an important issue for studying resilient methods.

3.3 | Performance Index

In this section, we design a global performance index , one of main contributions in this work, to quantify the tracking performance of the mobile robot network and evaluate the system's performance under various global positioning attacks through simulation. It is noted that, to the best of the authors' knowledge, this is the first performance index proposed to mobile robot network on time-varying formation tracking.

The design of the performance index depends on both the local and global formation tracking. Global formation tracking errors for the i^{th} agent has been defined previously as $\tilde{x}_i = x_i - h_i^d$. For local tracking, we define $e_i^1 = \sum_{j\in\mathcal{N}_i}(\tilde{x}_i - \tilde{x}_j)$ as the summation of local formation tracking error with a unity weight[b]. Furthermore, the average of local formation errors is given as $\bar{e}_i^1 = e_i^1/n_i$, where n_i is the number of neighbors of the i^{th} mobile agent. Hence, the performance index is defined as

$$\mathcal{I}_f^g = \left(\vartheta + \sum_{i=1}^{N} \|\bar{e}_i^1\|\right) \Big/ \left(\vartheta + \sum_{i=1}^{N} \|\bar{e}_i^1\| + \alpha_f^g \sum_{i=1}^{N} \|\tilde{x}_i\|\right), \tag{6}$$

where ϑ and α_f^g are positive constants. It is noted that $\mathcal{I}_f^g$ is defined globally for formation tracking control.

Based on $\mathcal{I}_f^g$, if the mobile robot network achieves global formation tracking, then the local formation tracking is also guaranteed; therefore, $\tilde{x}_i$ and $\bar{e}_i^1$ all converging to zero gives $\mathcal{I}_f^g = 1$. If the mobile robots only achieve local formation tracking

[b] The design of e_i^1 is similar to the inter-agent errors e_i defined in Section 3 and multi-agent consensus, but this term, without the weights for the graph Laplacian, is considered in the evaluation of the local tracking performance.

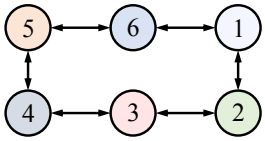

FIGURE 2 Sensory topology of the mobile agents in the networked robotic system considered in the simulation analysis.

but fail to track the global formation, then $\tilde{e}_i^1$ converges to zero but $\tilde{x}_i$ could be non-zero. Thus, $\mathcal{I}_f^g$ is less than one, and its actual value depends on the tracking errors of the global formation. If the system becomes unstable, then $\tilde{x}_i$ diverges so that $\mathcal{I}_f^g$ goes to zero. Hence, the index $\mathcal{I}_f^g$ tells the possibility of the mobile robots being under deception attack on the global positioning data.

3.4 | Numerical Examples - Formation Tracking and Attacks

We consider a mobile robot network composed of six agents under the sensory topology illustrated in Fig. 2. The control algorithm (3) is utilized to control the mobile robot network to form a hexagon, rectangle, and triangle at $t = 0 \sim 15$ sec, $t = 15 \sim 30$ sec, and after $t = 45$ sec, respectively. Moreover, the formation is considered to track a lemniscate time-varying trajectory described by $h^d(t) = \big[-5\sin(2\pi t/15)/\big(2(\cos(2\pi t/15)-3)\big), -12\cos(\pi t/15)/\big(5(\cos(2\pi t/15)-3)\big)\big]^T$. The control gains are selected as $\kappa_f = 2$, $\sigma_{fi} = I_2$, $\kappa_{gi} = 2$ with identical sensory weights of $w_{ji} = 1$, where $I_n \in \mathbb{R}^{n\times n}$ denotes an identity matrix. The performance index (6) is utilized to evaluate formation tracking in the following simulation with $\vartheta = 10$ and $\alpha_f^g = 5$.

For the mobile robot network that is not under positioning attack, the agents' trajectories and performance index are shown in Fig. 3 a. With the unaffected global positioning signals and local displacement measurement, the mobile agents are able to stably keep a time-varying formation while tracking a trajectory. The performance index converges to one if the system is asymptotically stable with guaranteed local and global formation tracking. Next, we consider the case where Agent 1 is under hybrid attack ($\delta_{x1} = 2$ and $\Delta_{x1} = [-2,-2]^T$) starting at $t_{a1} = 15$ sec, which is after the networked robotic system achieving asymptotic stability as stated in Assumption 5. The results in Fig. 3 b show that the hybrid attack affected the motion of Agent 1, which is marked in blue, and the adjacent agents of Agent 1 also deviated from their positions in the desired local formation. Due to malicious positioning attack, the performance index decreased far from one after $t = t_{a1}$, the starting time of attacks.

To compare the evolution of the performance index with respect to different types of attacks designed in Section 3.2, we conducted various analyzes shown in Fig. 4. If the additive attack is with a constant bias signal, then the performance index decreases to a smaller value without time-dependent variation; however, under the hybrid attack, resulting from the multiplicative type δ_{xi}, the variation of the performance index depends on the formation and desired trajectory. From the case where both Agent 1 and Agent 4 were under attack, we can observed that multi-agent attacks would degrade the performance index. Moreover, an unstable attack, due to the unstable term $-c_{ai}\xi_i$, would cause oscillations in the performance index, which result from constant switching between local and global formation tracking control.

Briefly, the results of the proposed formation tracking controller and the influence under deception attacks are investigated in this section. The theoretical results show that an attacker with knowledge of the system can break its stability, as a contribution of this work. Regarding the concern of attacks, the resilient method is necessary for the mobile robot network.

4 | COOPERATIVE LOCALIZATION AND RESILIENT OPERATION

The main focus here is to improve the localization resilience toward potentially faulty global positioning information due to system-originated errors or malicious attacks. For the rest of the paper, we generally refer to the external positioning system that is subject to attacks as GPS. By default, the global tracking of the robot network relies on the localization information from the GPS. Since inter-agent observations are available, we introduce a cooperative localization (CL) scheme as the secondary localization approach in the case of GPS failures or attacks. In this section, we first present a communication-free cooperative localization scheme based on the EIF and then discuss the self-identification and exclusion of GPS attacks.

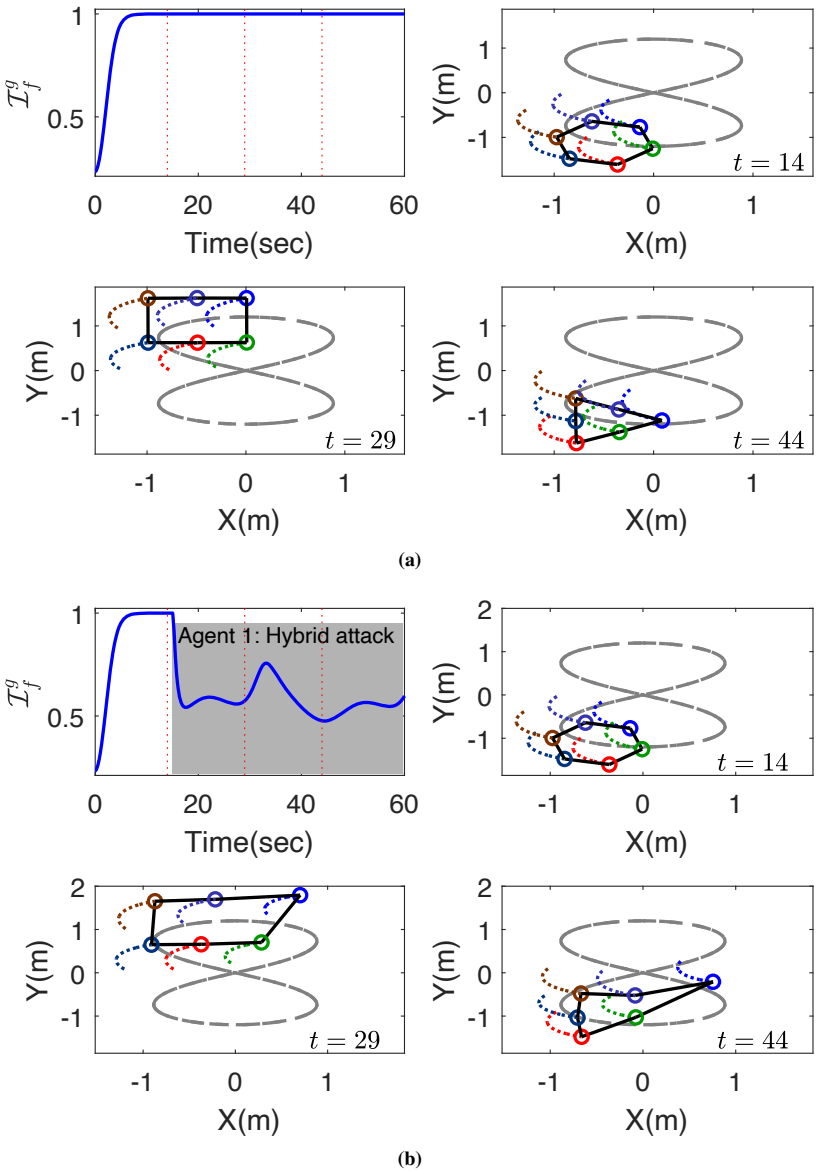

FIGURE 3 Performance index ($\mathcal{I}_f^g$) and trajectory snapshots of the mobile robot network (a) without (b) with global positioning attack. The vertical dashed lines in the sub-figure for $\mathcal{I}_f^g$ represent the time of snapshots in the other three sub-figures.

4.1 | Positioning Recovery

Localization resilience is achieved through redundancy, i.e., a sensor fusion mechanism consisting of proprioceptive sensor measurements, GPS measurements, and inter-agent relative measurements with respect to neighboring agents. It is assumed that only GPS measurements may be subject to attacks. The EIF was chosen as the information fusion method in favor of its efficiency in incorporating multi-modal sensor measurements in multi-step filter updates. Here, we only include the details necessary to understand the proposed positioning recovery method. For a comprehensive treatment of EIF, the readers are referred to[34].

We consider the state estimation problem in discrete time since motion sensors measure state changes at finite frequencies. Let us denote discrete-time variables $x(k) \triangleq x(k\Delta t)$, where $k \in \mathbb{Z}^{0+}$ is the number of time steps, and Δt denotes the sample time step that is assumed uniform. For applications in a three-dimensional space where the agent's velocity can be directly measured,

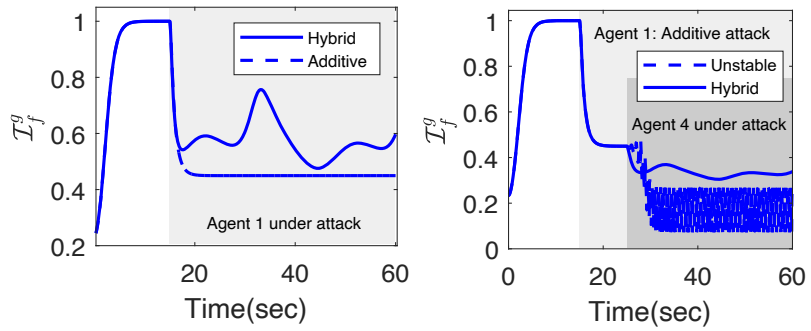

FIGURE 4 Performance indices of mobile robot network subjected to different malicious attacks on global positioning. Left: Only Agent 1 is under attack at $t_{a1} = 15$ sec under either an hybrid attack (as in Fig. 3 b) or additive attack. Right: Agent 1 is under additive attack at $t_{a1} = 15$ sec, and subsequently Agent 4 is under either hybrid or unstable attacks at $t_{a4} = 25$ sec. ($\delta_{x1} = \delta_{x4} = 2$, $\Delta_{x1} = \Delta_{x4} = [-2, -2]^T$, and $c_{a4} = 5$)

the state vector for the i^{th} agent at time k consists of the location of the agent defined as $x_i(k) := [x(k); y(k); z(k)]^T \in \mathbb{R}^3$. The agent's motion model can be approximated by the following piecewise constant-velocity kinematic relationship

$$x_i(k) = x_i(k-1) + [\dot{x}_i(k) + v_i(k)]\Delta t, \tag{7}$$

where $\dot{x}_i(k) \in \mathbb{R}^3$ denotes the agent velocity that can be measured directly, and $v_i(k) \sim \mathcal{N}\big(0, Q(k)\big)$ is the random process noise that follows a zero-mean Gaussian distribution with covariance matrix $Q(k) \in \mathbb{R}^{3\times3}$. The state vector prediction at time k, $\hat{x}_i(k|k-1)$, can be calculated as

$$\hat{x}_i(k|k-1) = \hat{x}_i(k-1|k-1) + \dot{x}_i(k)\Delta t. \tag{8}$$

For applications where acceleration is directly measurable instead of velocity, the agent's velocity can be included in the state vector; (7) and (8) should be updated to full discrete-time kinematic formulas. The covariance of the location estimate for the i^{th} agent, $P_i \in \mathbb{R}^{3\times3}$, is propagated accordingly as

$$\begin{aligned} P_i(k|k-1) = F_i(k)P_i(k-1|k-1)F_i(k)^T \\ + G_i(k)Q(k)G_i(k)^T, \end{aligned} \tag{9}$$

where $F_i(k)$ and $G_i(k)$ are the Jacobian matrices calculated based on the state estimate from (8). Here, $F_i(k) = I_3$ and $G_i(k) = \Delta t \cdot I_3$. The information matrix, $\Phi_i \in \mathbb{R}^{3\times3}$, and information vector, $\varphi_i \in \mathbb{R}^3$, can be found as $\Phi_i(k|k-1) = P_i(k|k-1)^{-1}$ and $\varphi_i(k|k-1) = \Phi_i(k|k-1)\,\hat{x}_i(k|k-1)$, respectively.

During normal operations, each agent updates its location estimate with the GPS measurement. In the event that the GPS measurement is deemed unreliable or faulty, the agent performs location update through cooperative localization instead. The measurement models for these two types of updates are

$$s_i^{\text{GPS}}(k) = x_i(k) + \omega_i^{\text{GPS}}(k), \tag{10}$$

$$s_i^{r_{ij}}(k) = x_j(k) - x_i(k) + \omega_i^{r_{ij}}(k), \tag{11}$$

where $\omega_i^{\text{GPS}}(k)$ and $\omega_i^{r_{ij}}(k)$ are the random noise signals associated with GPS or relative position measurements, both of which are assumed to follow zero-mean Gaussian distributions with covariance matrices $R^{\text{GPS}}(k)$ and $R^{r_{ij}}(k)$, respectively, and $j \in \mathcal{N}_i$ denotes the index of the neighboring agents. Note that (11) does not require information to be sent from the neighbors because the neighbors' desired trajectories are known to others. For either update mode, denoted by a superscript $\square \in \{\text{GPS}, r_{ij}\}$, the updates of the information matrix and vector follow the same EIF procedure such that

$$\Phi_i(k|k) = \Phi_i(k|k-1) + H_i^{\square}(k)^T R_i^{\square}(k)^{-1} H_i^{\square}(k), \tag{12}$$

$$\begin{aligned} \varphi_i(k|k) = \varphi_i(k|k-1) + H_i^{\square}(k)^T R_i^{\square}(k)^{-1}[s_i^{\square}(k) - \hat{s}_i^{\square}(k) \\ + H_i^{\square}(k)\hat{x}_i(k|k-1)], \end{aligned} \tag{13}$$

where $H_i^{\square}$ is the Jacobian matrix calculated from either (10) or (11) with $R_i^{\square}(k)$ being the covariance matrix of the corresponding measurement. Here, $H_i^{\text{GPS}} = I_3$ and $H_i^{r_{ij}} = -I_3$. The measurement predication, $\hat{s}_i^{\square}(k)$, can be found based on either of the measurement models (10) and (11) as

$$\hat{s}_i^{\text{GPS}}(k) = \hat{x}_i(k|k-1), \tag{14}$$

$$\hat{s}_i^{r_{ij}}(k) = h_j^d(k) - \hat{x}_i(k|k-1). \tag{15}$$

Using the updated information matrix and vector, the state estimation vector and covariance matrix can be recovered as

$$\hat{x}_i(k|k) = \Phi_i(k|k)^{-1}\varphi_i(k|k), \tag{16}$$

$$P_i(k|k) = \Phi_i(k|k)^{-1}. \tag{17}$$

Theorem 2. If the control input (3) guarantees that the mobile robot network achieves global formation tracking as stated in Definition 2, the expectation of the position estimation errors, $\tilde{x}_i(k|k) := x_i(k) - \hat{x}_i(k|k)$, $i = 1, \cdots, N$, strictly decreases after the update with inter-agent measurements using measurement model (11).

A proof of Theorem 2 is provided in the Appendix A.2. This theorem provides a theoretical guarantee that, when global tracking is achieved asymptotically, the positioning error will decrease through inter-agent measurement updates using only the desired positions of the neighbors. When the robot network remains connected and at least one agent tracks its desired trajectory faithfully, converging localization performance across the entire agent network can be achieved.

4.2 | Attack Detection

With the communication-free cooperative localization as the secondary positioning approach in the event of GPS attacks, proper detection and isolation of attacks are necessary. Various fault detection and isolation solutions have been proposed[35]. Generally speaking, there are at least two main types of robust state estimator designs. The first type treats estimation as an optimization problem. For instance, Pajic et al.[36] presented an l_0-based state estimator that is resilient to sensor and actuator attacks on cyberphysical systems. The authors formulated the resulting optimization problem into a mixed-integer linear program and showed its convex relaxation based on the l_1 norm. Jeong and Eun[37] adopted the unknown input observer mechanism in their resilient state estimator design for the purpose of estimating the true plant state under both sensor attacks and external disturbances. Their attack resilient state estimation problem was then formulated as an l_2 minimization problem to eliminate the effect of attacks. The second type uses sensor fusion approaches and takes advantage of the redundancy in sensor measurements. Bezzo and coauthors[38] considered multiple velocity measurements for a ground mobile robot and used a recursive filtering technique that estimates the state of the system while being resilient against sensor attacks by adding a shielding gain to amplify the variance of noisy sensor inputs during fusion. Similarly, Mishra et al.[39] proposed a state estimator based on Kalman filters operating over subsets of redundant sensors to search for a sensor subset that is reliable for state estimation.

For attack detection, a popular method is the Chi-squared detector that monitors the residue after fusing the sensor measurement by comparing the sample variance against the inferred sensor variance.[40,41] Recently, machine learning methods was also adopted in navigation sensor attack detection. Dasgupta and coauthors[42] proposed an approach that combines inertial sensors and long short-term memory motion model to predict a vehicle's travel distances in-between GNSS samples in order to check whether GNSS samples are corrupted. In a separate work, Dasgupta et al.[42] demonstrated the use of reinforcement learning and deep Q networks in detection spoofing attack to GNSS measurements for autonomous vehicles. We favor a residual-based method that utilizes the results of EIF-based sensor fusion as introduced previously without the need for additional training. More specifically, the detection of GPS attack is achieved by comparing the residual at the EIF update step with new GPS measurements. This is realized through comparing the Kullback-Leibler (KL) divergence between the state estimate distributions before and after the update against a predefined threshold. A similar approach was used in[39] where the authors conduct a residual check to determine whether the sample average of residual variance within a finite time window is close to the expected attack-free value. As we will explain in more detail later, KL divergence provides probability distribution level of comparison, which is less susceptible to noises and outliers than the first moment based alternative.

The KL divergence is a non-symmetric measure that quantifies the distance between two probability distributions. For two probability density functions, $p(x)$ and $q(x)$, defined in the same probability space, the KL divergence is defined as

$$D_{KL}(p \parallel q) = \int_{-\infty}^{+\infty} p(x) \log\left(\frac{p(x)}{q(x)}\right) \mathrm{d}x. \tag{18}$$

In the case where both p and q are multivariate Gaussian with means μ_p, μ_q and covariance matrices Σ_p, Σ_q, respectively, the KL divergence can be found as

$$D_{KL}(\mathcal{N}_p \,\|\, \mathcal{N}_q) = \frac{1}{2}\Bigg[(\mu_q - \mu_p)^T \Sigma_q^{-1}(\mu_q - \mu_p) + \mathrm{tr}(\Sigma_q^{-1}\Sigma_p) - n + \ln\left(\frac{\det(\Sigma_q)}{\det(\Sigma_p)}\right)\Bigg], \tag{19}$$

where n is the dimension of x.

Before each GPS measurement is used in the update step, the KL divergence between the following two probability density functions is calculated:

$$p_1 = p\big(\hat{x}_i(k|k-1) \,|\, \hat{x}_i(k-1|k-1), \dot{x}_i(k)\big), \tag{20}$$

$$p_2 = p\big(\hat{x}_i(k|k) \,|\, s_i^{\mathrm{GPS}}(k), \dot{x}_i(k)\big). \tag{21}$$

Since both probability density functions are Gaussian distributions, the KL divergence at time k can be calculated as

$$\begin{aligned} &D_{KL}^k(p_1 \,\|\, p_2) \\ &= \frac{1}{2}\Bigg\{\big[\hat{x}(k|k) - \hat{x}(k|k-1)\big]\Phi(k|k)\big[\hat{x}(k|k) - \hat{x}(k|k-1)\big]^T \\ &+ \mathrm{tr}\left(\Phi(k|k)\cdot\Phi_i(k|k-1)^{-1}\right) + \ln\left(\frac{\det\left(\Phi(k|k-1)\right)}{\det\left(\Phi(k|k)\right)}\right) - n\Bigg\}. \end{aligned} \tag{22}$$

A GPS measurement is detected as a faulty signal when the value of $D_{KL}^k(p_1 \,\|\, p_2)$ is above a predefined threshold χ. In addition, a quality measure is defined for the global positioning information to inform the formation control:

$$\beta_i(k) = 1 - \mathrm{sat}\left(\frac{D_{KL}^k(p_1 \,\|\, p_2)}{\chi}\right), \tag{23}$$

where $\mathrm{sat} : \mathbb{R} \to \mathbb{R}$ is the standard saturation function defined as $\mathrm{sat}(x) := \mathrm{sign}(x)\min(1, |x|)$.

Algorithm 1 summarizes the resilient state estimator with GPS attack detection and isolation using the criterion based on the KL divergence. By default, the agents prioritize the global positioning information for localization. In the event of a global positioning failure or attack, the resilient state estimator switches to cooperative localization. This switch occurs instantaneously such that the positioning of the i^{th} agent is not affected by the failure of the global positioning system even if one or multiple neighbors are experiencing similar failures as long as their global tracking is faithful.

4.3 | Resilient Operation: CL-Based Gain-Tuning Approach

In addition to positioning recovery from cooperative localization, the mobile robot network in time-varying formation tracking is a redundant system with both the local and global formation tracking. As mentioned in Section 3.1, if there is no global tracking for a portion of the mobile agents, the formation tracking can still be guaranteed. Therefore, in this section, we propose an autonomous gain-tuning technique to strengthen the resilience of the mobile robot network by taking the advantage of redundancy.

For the proposed networked robot system under global positioning attacks, the analyses in Section 3.2 demonstrate that the tracking gain of global formation κ_{gi} plays an important role in tracking stability. Even though the networked system is under unstable attack, it would keep stable with larger attack gains c_{ai} wit very small κ_{gi}. Therefore, the manipulation of κ_{gi} with respect to the attack identification is a useful resilient feature for the system.

The gain tuning can be designed as a function of $\beta_i \in [0, 1]$, the quality measure of the global positioning signals defined in Section 4.2. If $\beta_i = 1$, there is a higher confidence on the quality of the global positioning signals; whereas for $\beta_i = 0$, the i^{th} agent is considered under attack while the value of $D_{KL}^k(p_1 \,\|\, p_2)$ is above the threshold χ. Therefore, we can set

$$\dot{\kappa}_{gi} = \begin{cases} \gamma_i \tanh\left(\sigma_{\beta_i}(\beta_i - \chi_{\beta_i})\right) & ,0 < \kappa_{gi} < \bar{\kappa}_{gi}. \\ 0 & ,else \end{cases} \tag{24}$$

Algorithm 1 Resilient State Estimator for the i^{th} Agent

Require: $\hat{x}_i(k-1|k-1)$, $P_i(k-1\,|\,k-1)$, $\dot{x}_i(k-1)$, $s_i^{\text{GPS}}(k)$, $\{s_i^{r_{ij}}(k)\,|\,j\in\mathcal{N}_i\}$, χ

Predict $\hat{x}_i(k|k-1)$ and $P_i(k\,|\,k-1)$ ▷ (7)–(9)

Try $\hat{x}_i(k|k)$ and $P_i(k\,|\,k)$ with $s_i^{\text{GPS}}(k)$ ▷ (10), (12)–(13), (17)–(16)

Compute KL divergence $D_{DL}^{i,k}$ ▷ (22)

Compute $\beta_i(k)$ ▷ (23)

if $D_{KL}^{i,k} < \chi$ **then**

  Accept $\hat{x}_i(k|k)$ and $P_i(k\,|\,k)$

else

  Reject $\hat{x}_i(k|k)$ and $P_i(k\,|\,k)$

  for j in $\mathcal{N}_i$ **do**

    Compute $\hat{x}_i(k|k)$ and $P_i(k\,|\,k)$ with $s_i^{r_{ij}}(k)$ ▷ (11), (12)–(13)

  end for

end if

Return: $\hat{x}_i(k|k)$, $P_i(k\,|\,k)$, $\beta_i(k)$

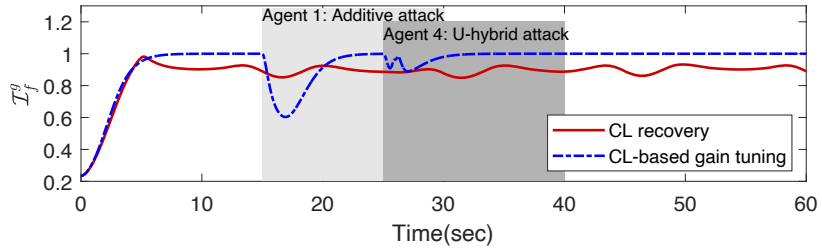

FIGURE 5 Performance indices under global positioning attacks with the proposed resilience operations. Agent 1 is under additive attack at $t_{a1} = 15 \sim 30$ sec, and Agent 4 is under U-hybrid attack at $t_{a4} = 25 \sim 40$ sec with $\delta_{x1} = \delta_{x4} = 2$, $\Delta_{x1} = \Delta_{x4} = [-2,-2]^T$, and $c_{a4} = 5$.

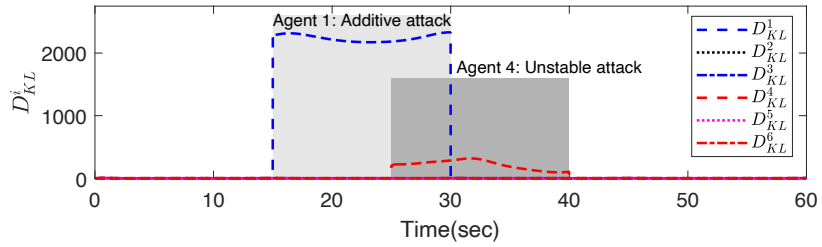

FIGURE 6 KL divergence of the mobile agents under global positioning attacks with the threshold $\chi = 5$.

where $\bar{\kappa}_{gi}$ is the upper bound of κ_{gi}, $\chi_{\beta_i} \in (0,1]$ is the triggering threshold, and σ_{β_i} is the tuning gain for γ_i. In this work, $\bar{\kappa}_{gi}$ is chosen as the initial value of κ_{gi} according to Assumption 5. It is noted that β_i encodes the confidence in global positioning signals. This design of resilience operation utilizes the GPS quality measure β_i from cooperative localization, and therefore is called CL-based (cooperative-localization-based) gain-tuning approach.

4.4 | Numerical Examples - Recovery and Resilient Operation

The effect of the proposed resilient operations is verified through numerical simulations. The sensory topology and control gains in the following simulation are identical to those of Section 3.4. The attack scenarios are satisfied by Assumption 5 and

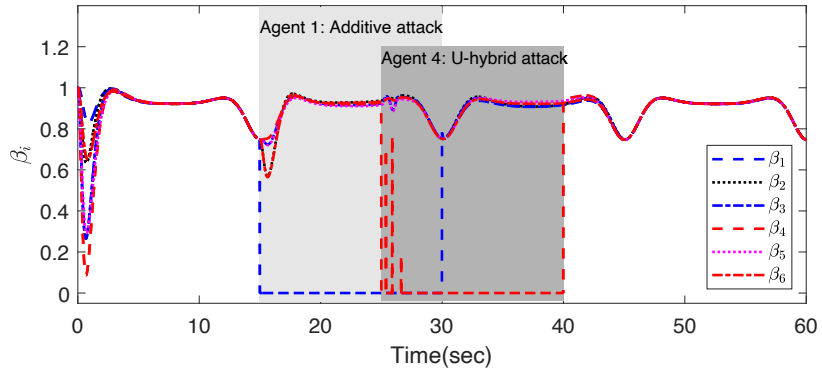

FIGURE 7 Evolution of the GPS quality measure β_i of the mobile robot network under malicious attacks.

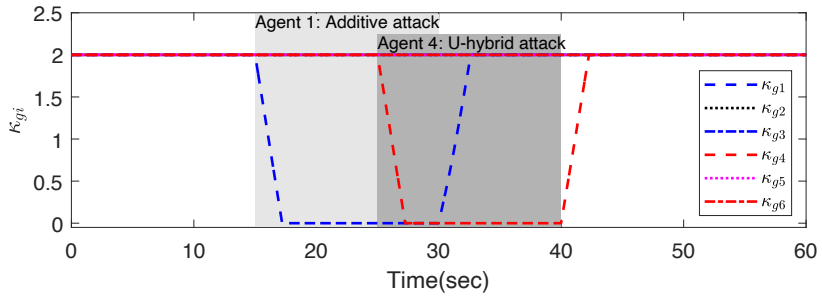

FIGURE 8 Evolution of the global tracking gains by using the proposed CL-based gain-tuning approach.

similar to the case with multiple attacks in Fig. 4, including the unstable attack, but both attacks are removed after 15 sec to show resilience and recovery during and after the attacks. It is noted that the resilient state estimator is active from the start of the simulation, and CL-based gain-tuning starts to regulate global tracking gains κ_{gi} at $t = 10$ sec. The performance indices of the resilient operations are illustrated in Fig. 5.

4.4.1 | CL Recovery Approach

The cooperative localization and the resilient state estimator are implemented in this section with $\chi = 5$ to recover global positioning. From Fig. 5, it can be seen that the CL recovery approach can maintain the performance index at a constant high level during positioning attacks. It shows that the invulnerability of the mobile robot network with the resilient state estimator is evident. The evolution of KL divergence is shown in Fig. 6, where D_{KL}^1 and D_{KL}^4 increase drastically to a relatively higher value when Agents 1 and 4 are under attack. Therefore, it is beneficial to use the state estimation results to inform the controller about the presence of malicious attacks. Although the performance index is insensitive to attacks, it never closely approaches one even when there are no attacks due to the inferior state estimation accuracy than external positioning systems.

4.4.2 | CL-Based Gain-Tuning Approach

To enhance the resilience and recovery performance of the mobile robot network before, during, and after attacks, the CL recovery and gain-tuning approaches are combined to form the CL-based gain-tuning approach. The GPS quality measure (23), obtained from the KL divergence, is utilized to design a mechanism to regulate global tracking gains κ_{gi} in an adaptive fashion. For $\sigma_{\beta_i} = 3$ and $\chi_{\beta_i} = 0.5$ with $\gamma_i = 1$, the simulation results are illustrated in Figs. 5, 7, and 8. It is noted that the CL-based gain-tuning approach is applied for all agents starting at $t = 10$ sec after the system achieves asymptotic stability. Fig. 7 shows that the GPS quality measure decreases when the agent becomes under attack. Therefore, the GPS quality measure can be used to indicate the health condition of the global positioning information. For β_i less than χ_{β_i}, κ_{gi} starts decreasing to zero so that the global positioning information subjected to malicious attacks can be excluded from the control system. At $t = 25$ sec, κ_{g4} also decreases to zero because of the unstable attack on Agent 4 while other normal agents keep their own value. Moreover,

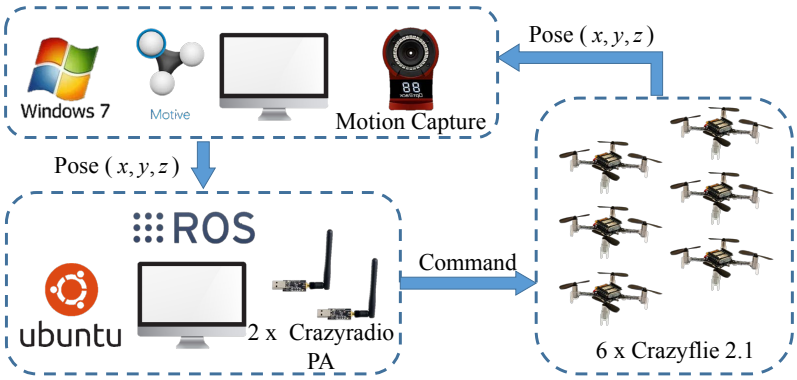

FIGURE 9 Experimental setup of the multi-quadrotor system for the implementation of the resilient TVFC in the presence of positioning attacks.

after the attacks are removed at $t = 30$ sec and $t = 40$ sec, respectively for Agent 1 and Agent 4, κ_{g1} and κ_{g24} can be recovered to the original value before attacks.

To summarize, CL-based gain-tuning approach is verified as the most resilient to deception attacks through the simulation. As one of the main contributions in this work, the influence of attacks can be isolated successfully, and the robot can join back to the system after attacks disappear. The resilience of the systems is retained. To further investigate the effectiveness of the CL-based gain-tuning approach, it is necessary to implement the proposed method on a hardware experiment.

5 | EXPERIMENTAL RESULTS

In this section, we discuss the implementation of the proposed scheme on a group of six quadrotors that are subject to global positioning attacks. It should be noted that our general approach is not limited to flying robots. The experimental setup of the quadrotor network system is illustrated in Fig. 9. Six Crazyflie 2.1, designed by Bitcraze, are used as mobile agents in the mobile robot network, and the system is built upon the Robot Operating System (ROS) and its package "crazyswarm"[43]. The motion of agents is captured by a motion capture (MOCAP) system consisting of IR cameras at 120 Hz, and then the commands from the proposed design are sent to agents at 100 Hz asynchronously. Although our setup is centralized, the proposed control scheme is implemented in a decentralized manner on the computer with limited information from each agent's neighbor in order to satisfy our assumptions.

5.1 | Scenario 1: Time-Varying Formation with Stationary Global Trajectory

To demonstrate the capability of the proposed resilient operations under positioning attacks, the time-varying formation tracking with stationary (time-invariant) global trajectory, $h^d = [0, 0, 0.9]^T$ m, is considered as the first scenario. By considering a stationary global trajectory, the influence from positioning attacks and recovery can be accessed separately with time-invariant trajectories. Six mobile agents arrive in horizontal formations of hexagon, rectangle, and triangle at $t = 10$, 20, and 30 sec, respectively, as shown in Fig. 10. The sensory topology of local positioning measures is represented by the dashed lines in each of the formations in Fig. 10. Moreover, the vertical formations of mobile agents are formed by trajectories of $\bar{h}_i^d$ that are given as $\bar{h}_{iz}^d(t) = 0.15 \sin(0.05\pi t + i\pi)$ m for $i = \{1, \ldots, 6\}$.

The tracking gains for the proposed TVFC are chosen as $\kappa_{gi} = 0.8$, $\kappa_{fi} = 0.4$, $\sigma_{fi} = 0.05 I_3$, and $w_{ij} = 1$. The performance indices of the robot network under different attack settings are illustrated in Fig. 10, where $\vartheta = 20$ and $\alpha_f^g = 3$ in $\mathcal{I}_f^g$. With various positioning attacks, the quadrotors would deviate from their desired positions and cause degradation of the performance indices. In the absence of malicious attack, the performance index $\mathcal{I}_f^g$ stably stays around 0.985 providing satisfactory formation tracking. When an additive attack is applied on Agent 1 with $\Delta_{xi} = [-1.5, -2.5, -1.0]^T$ m at $t_{a1} = 15$ sec, the performance index, $\mathcal{I}_f^g$, degrades significantly without resilient operation as the tracking error of the compromised agent propagates through the network and causes its neighbors to drift away from their desired trajectories. We then consider the same attack situation but now apply the proposed CL-based gain-tuning resilient operation (24) with $\gamma_i = 1$, $\sigma_{\beta_i} = 3$, and $\chi_{\beta_i} = 0.5$. It can be seen

TABLE 1 Modified restoration ($\bar{R}_s^{\text{exp}}$) in experiments for the cases in Scenario 1 ($\int_{15}^{40} Nor(\mathcal{I}_f^g(\tau))d\tau = 24.61$).

Cases in Scenario 1	Resilient Operation	$\bar{R}_s^{\text{exp}}$
Normal (attack-free)	-	0%
Additive attack at $t_{a1} = 15$ s	No	23.78%
Additive attack at $t_{a1} = 15$ s	Yes	8.48%
Additive attack at $t_{a1} = 15$ s Unstable attack at $t_{a4} = 20$ s	Yes	8.99%

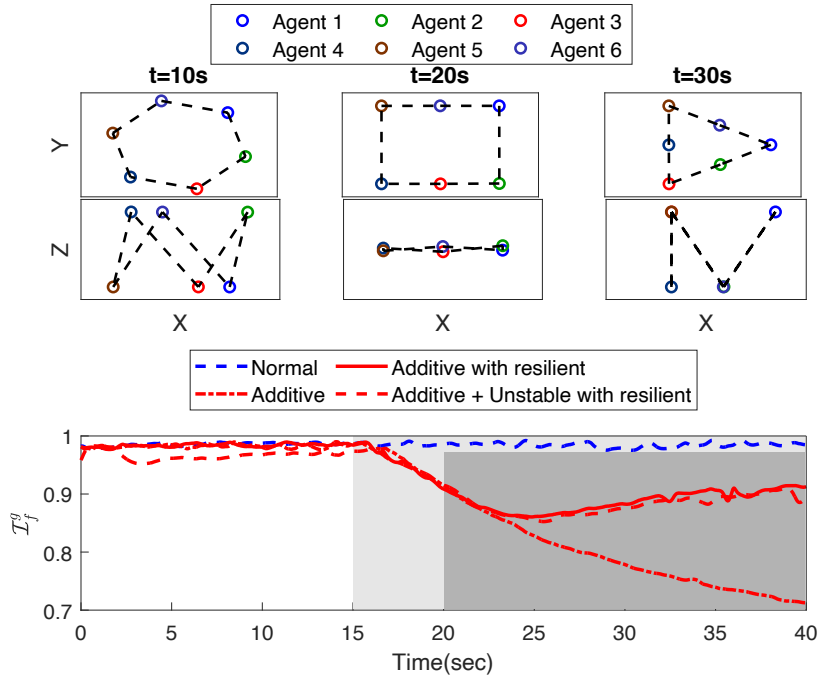

FIGURE 10 Desired formation (top) and performance indices (bottom) for the time-varying formation tracking with stationary global trajectory with/without global positioning attacks. For the cases with additive attack, Agent 1 is subject to attack for $t \geq t_{a1} = 15$ sec. For the case with additional unstable attack, Agent 4 is under attack for $t \geq t_{a4} = 20$ sec.

from Fig. 10 that $\mathcal{I}_f^g$ would gradually increase and the performance improves significantly compared to last case. Here, we chose $Q = 0.02^2 I_n$, $R^{\text{GPS}} = (5 \times 10^{-4})^2 I_n$, $R^{r_{ij}} = (5 \times 10^{-4})^2 I_n$, and $\chi = 4000$ based on the typical precision of the MOCAP system. Furthermore, under an additional unstable attack on Agent 4 with $\delta_{x4} = 1$ and $c_{a4} = 5$ at $t_{a4} = 20$ sec, the robot team maintains a better performance, and $\mathcal{I}_f^g$ is larger than 0.85 and keeps increasing for better formation tracking.

To quantitatively assess the performance of the system in experiments, we define a new measure modified from restoration $\bar{R}_s^{\text{exp}}$

$$\bar{R}_s^{\text{exp}} = \frac{\int_{t_a}^{t_s} \left(Nor(\mathcal{I}_f^g) - Att(\mathcal{I}_f^g) \right) d\tau}{\int_{t_a}^{t_s} Nor(\mathcal{I}_f^g) d\tau}, \tag{25}$$

where $\mathcal{I}_f^g$ is the performance index defined in (6), t_a is the time when an attack occurs, t_s is the terminal time of the experiment, $Nor(\mathcal{I}_f^g(t))$ is the reference of the performance index without attacks, and $Att(\mathcal{I}_f^g(t))$ is the performance index under attacks with/without resilience. Since $Nor(\mathcal{I}_f^g(t))$ is not equal to one, the modified restoration, $\bar{R}_s^{\text{exp}}$, provides a way to compare the resilience performance of the system in experiments to the cases without attacks. It can be seen as the degree of performance degradation from the attack-free case, with 0% representing no degradation and 100% being full degradation. Table 1 summarizes the modified restoration of different cases in Scenario 1. Obviously, the proposed resilient operation holds better better performance even if there is unstable attack.

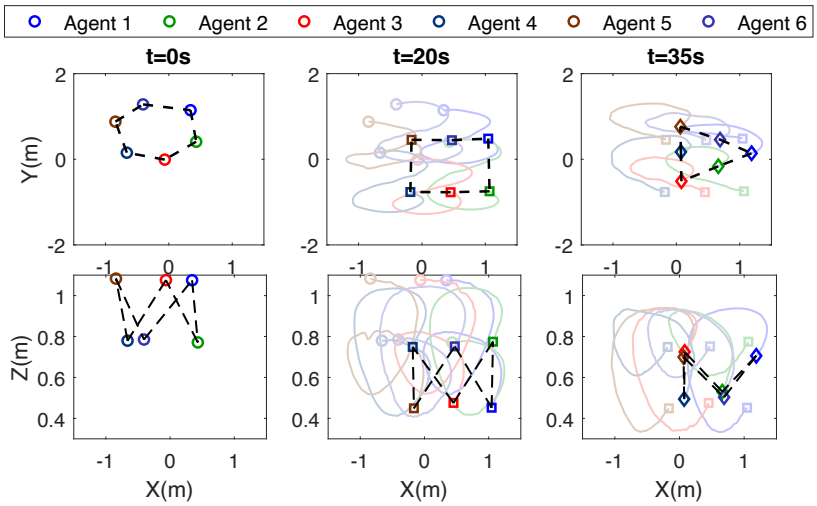

FIGURE 11 Snapshots of the time-varying formation and global trajectory tracking in the absence of global positioning attacks.

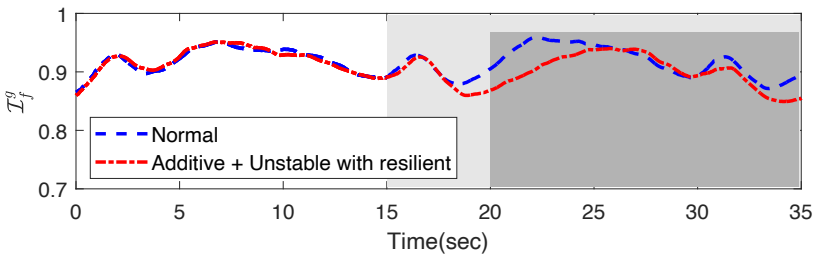

FIGURE 12 Performance indices of the experiments with healthy global positioning, and under additive and unstable attacks with resilient operation. For the case with attacks, Agent 1 is subject to additive attack for $t \geq t_{a1} = 15$ sec, and Agent 4 is under unstable attack for $t \geq t_{a4} = 20$ sec.

5.2 | Scenario 2: Time-Varying Formation and Global Trajectory

To further investigate the effect of the proposed TVFC for mobile robot networks and the resilient operation, two advanced cases are presented where the mobile robot network tracks a predefined global trajectory. The quadrotor team reaches hexagon, rectangle, and triangle horizontal formations at $t = 5$, 20, and 35 sec, respectively. The vertical formation is the same as in the previous case. Additionally, the global trajectory of the mobile agents is defined as $h^d = [1.3\sin(2\pi t/15)/(\cos(2\pi t/15) - 3), -1.2\cos(\pi t/15)/(\cos(2\pi t/15) - 3), 0.2\cos(2\pi t/15) + 0.7]^T$ m, which is a 3D lemniscate trajectory with a time-varying Z-component. The control gains are chosen as $\kappa_{gi} = 0.4$, $\kappa_{fi} = 0.4$, and $\sigma_{fi} = 0.1 I_3$.

The snapshots of the formation tracking without attacks are shown in Fig. 11, where the dashed lines represent the local measurement network among the mobile agents. The performance indices of the proposed control algorithm tracking the global and local trajectories with and without global positioning attacks are shown in Fig. 12. In the absence of attacks, the performance index varies around 0.9, indicating that the mobile robot network can closely track the global trajectory and time-varying formation.

When Agent 1 and Agent 4 are under additive and unstable attacks, respectively, the performance index slightly degrades due to the attacks but the tracking performance remains as satisfactory as the case without attack in Fig. 12. The parameters used in cooperative localization are identical to the previous section with the stationary global trajectory. This result implies that the proposed control algorithm is capable of eliminating severe influence of malicious attacks on agents to protect the systems from attacks and recovery to attack-free performance. The evolution of β_i and κ_{gi} is shown in Fig. 13, where the identification of attacks is via β_i and the corresponding global tracking gains decrease to eliminate the adversarial effect on the mobile robot network.

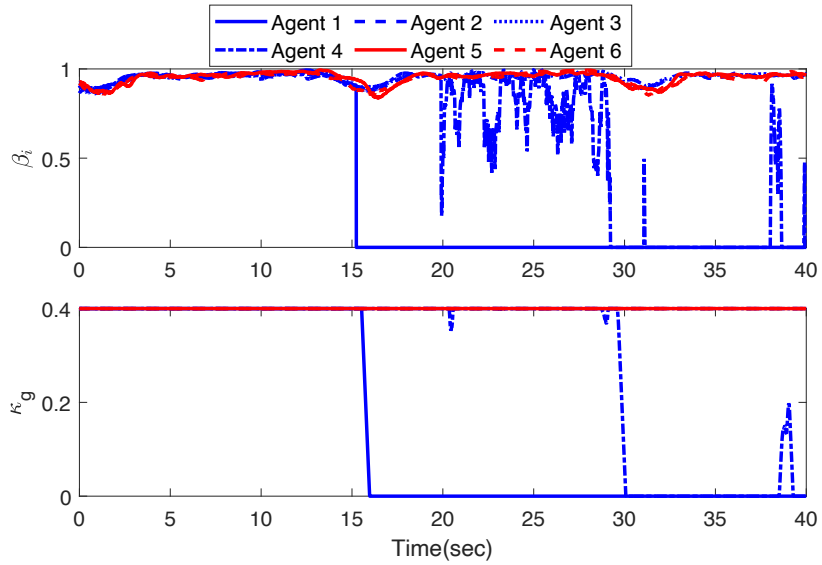

FIGURE 13 Evolution of β and κ_g in the experimental case with both additive attack on Agent 1 and unstable attack on Agent 4. Parameter projection[44,45] is utilized in (24) such that $0 \leq \kappa_{gi} \leq 0.4$.

6 | CONCLUSION

The persistency of maintaining a time-varying formation to track the reference trajectory of a mobile robot network under global positioning attacks is investigated in this paper. Based on the local and global positioning information, control algorithms are presented and studied to ensure formation tracking performance. Subsequently, Lyapunov-based stability analyses are provided in the presence of three types of malicious attacks on the global positioning signals that are additive attack, hybrid attack, and unstable attack. Moreover, a performance index is presented to evaluate the efficiency of mobile robot networks under time-varying formation tracking control with/without compromised agents subjected to adverse impacts. Simulation results and experiments validate the control system and the influence of adversarial attacks on global positioning. Future work will address the resilience in coordinating heterogeneous robotic systems, reaction to sensory/actuator faults, and handling unreliable sensory topologies.

How to cite this article: Liu YC, Liu KY, and Song Z. Resilient Time-Varying Formation Tracking for Mobile Robot Networks under Deception Attacks on Positioning, *Int J Robust Nonlinear Control.*, 202x, .

APPENDIX

A PROOF

A.1 Proof for Theorem 1

Proof. Without loss of generality, let us consider the Lyapunov function candidate for the i^{th} robot in the the mobile robot network as $V_i(\xi_i) = \frac{1}{2}\xi_i^T \sigma_{fi}^{-1} \xi_i$. By taking the time-derivative of V_i along the trajectories of (3.1), we obtain $\dot{V}_i = -\xi_i^T \xi_i$, which is negative definite. Since V_i is positive definite and $\dot{V}_i$ is negative definite, we obtain $V_i(\xi_i(t)) \leq V_i(\xi_i(0))$ so that $\xi_i \in \mathcal{L}_\infty$ because σ_{fi} is a positive definite matrix. Next, by integrating $\dot{V}_i(t)$ with respect to time from 0 to ∞, we have $V_i(t) - V_i(0) = -\int_0^t \xi_i^T(\tau)\xi_i(\tau)d(\tau)$, which results in $\int_0^t \xi_i^T(\tau)\xi_i(\tau)d(\tau) + V_i(t) = V_i(0)$. Since $V_i(\xi_i)$ is positive definite, we can further obtain that $\int_0^t \xi_i^T(\tau)\xi_i(\tau)d(\tau) \leq V_i(0) < \infty$; consequently, we have $\xi_i \in \mathcal{L}_2$. From the closed-loop dynamics (3.1), we further obtain that $\dot{\xi}_i \in \mathcal{L}_\infty$. Since $\xi_i \in \mathcal{L}_2 \cap \mathcal{L}_\infty$ and $\dot{\xi}_i \in \mathcal{L}_\infty$, we get from Barbalat's lemma[46] that $\lim_{t\to\infty} \xi_i(t) = 0$. Therefore, we conclude that ξ_i is asymptotically stable.

Next, let us rewrite $\xi_i = \dot{\tilde{x}}_i + \kappa_{gi}\tilde{x}_i + \kappa_f e_i$ as $\dot{\tilde{x}}_i = -\kappa_{gi}\tilde{x}_i - \kappa_f e_i + \xi_i$, which can be considered as the state equation of $\tilde{x}_i$ with ξ_i as the input. From the definition of e_i with the weighted Laplacian matrix, we have $e = [L \otimes I_n]\tilde{x}$, where $e = [e_1^T, \dots, e_N^T]^T \in \mathbb{R}^{Nn}$ and $\tilde{x} = [\tilde{x}_1^T, \dots, \tilde{x}_N^T]^T \in \mathbb{R}^{Nn}$. By considering $\xi \in \mathbb{R}^{Nn}$ as the stacked vector of ξ_i such that $\xi = [\xi_1^T, \xi_2^T, \dots, \xi_N^T]^T$, the interconnected system becomes

$$\begin{aligned}\dot{\tilde{x}} =& -D_{\kappa_g} \otimes I_n \tilde{x} - \kappa_f [L \otimes I_n]\tilde{x} + \xi \\ =& -[(D_{\kappa_g} + \kappa_f L) \otimes I_n]\tilde{x} + \xi,\end{aligned} \tag{A.1}$$

where $D_{\kappa_g} \in \mathbb{R}^{N\times N}$ denotes a diagonal matrix with the i^{th} diagonal term as κ_g. Since κ_f, κ_{gi} are all positive, we can show that $-(D_{\kappa_g} + \kappa_f L)$ is a Hurwitz matrix[46] because $L(\mathcal{G})$ has an isolated eigenvalue of zero and all others with a positive real part (Property 1). As ξ converges to the origin as time goes to infinity, the linear time-invariant (LTI) system (A.1) with ξ as the input is asymptotically stable. Consequently, $\tilde{x}, \dot{\tilde{x}} \in \mathcal{L}_2 \cap \mathcal{L}_\infty$ so that $\tilde{x} \to 0$ as $t \to \infty$. Furthermore, by observing (A.1), the convergence of $\tilde{x}$ and ξ to the origin lead to $\dot{\tilde{x}} \to 0$ asymptotically. Consequently, $\lim_{t\to\infty} \tilde{x}_i(t) = 0$ and $\lim_{t\to\infty} \dot{\tilde{x}}_i(t) = 0$ demonstrate that $\lim_{t\to\infty} \left(x_i(t) - h_i^d(t)\right) = 0$ and $\lim_{t\to\infty} \dot{x}_i(t) = \lim_{t\to\infty} \dot{h}_i^d(t)$. The mobile robot network achieves global formation tracking. □

A.2 Proof for Theorem 2

Proof. Based on measurement model (11), the measurement error, or innovation, of the i^{th} agent relative to the j^{th} agent can be calculated as

$$\begin{aligned}\tilde{s}_i^{r_{ij}}(k) =& s_i^{r_{ij}}(k) - \hat{s}_i^{r_{ij}}(k) \\ =& x_j(k) - x_i(k) + \omega_i^{r_{ij}}(k) - \left[h_j^d(k) - \hat{x}_i(k|k-1)\right] \\ =& \tilde{x}_j(k) - \tilde{x}_i(k|k-1) + \omega_i^{r_{ij}}(k).\end{aligned} \tag{A.1}$$

Recall that $\tilde{x}_j(k)$ denotes the global tracking error. Based on the definition for information vector, $H_i^{r_{ij}} = -I_3$, and (13), the state estimation error after update with inter-agent measurement can be calculated as

$$\begin{aligned}\tilde{x}_i(k|k) =& x_i(k) - \hat{x}_i(k|k) \\ =& x_i(k) - \Phi_i(k|k)^{-1}\varphi_i(k|k) \\ =& x_i(k) - \Phi_i(k|k)^{-1}\Big\{\varphi_i(k|k-1) \\ & - R_i(k)^{-1}\left[\tilde{s}_i^r(k) - \hat{x}_i(k|k-1)\right]\Big\}.\end{aligned} \tag{A.2}$$

In this proof, we use a simplified notation for the inter-agent measurement covariance matrix: $R_i(k) = R_i^{r_{ij}}(k)$. Left multiplying $\Phi_i(k|k)$ on both sides of (A.2) and rearranging yield

$$\begin{aligned}&\Phi_i(k|k)\tilde{x}_i(k|k) \\ &= \Phi_i(k|k-1)\left[x_i(k) - \hat{x}_i(k|k-1)\right] \\ &\qquad + R_i(k)^{-1}\left[\tilde{s}_i^{r_{ij}}(k) + x_i(k) - \hat{x}_i(k|k-1)\right] \\ &= \Phi_i(k|k-1)\tilde{x}_i(k|k-1) + R_i(k)^{-1}\left[\tilde{s}_i^{r_{ij}}(k) + \tilde{x}_i(k|k-1)\right] \\ &= \Phi_i(k|k-1)\tilde{x}_i(k|k-1) + R_i(k)^{-1}\left[\tilde{x}_j(k) + \omega_i^{r_{ij}}(k)\right],\end{aligned} \tag{A.3}$$

which leads to $\tilde{x}_i(k|k) = \Phi_i(k|k)^{-1}\Big\{\Phi_i(k|k-1)\tilde{x}_i(k|k-1) + R_i(k)^{-1}\left[\tilde{x}_j(k) + \omega_i^{r_{ij}}(k)\right]\Big\}$. Taking the expectation of both sides and the limit when $k \to \infty$ leads to

$$E\left[\tilde{x}_i(k|k)\right] = \Phi_i(k|k)^{-1}\Phi_i(k|k-1)E\left[\tilde{x}_i(k|k-1)\right]. \tag{A.4}$$

Here we applied $\lim_{k\to\infty} \tilde{x}_j(k) = 0$ and $E[\omega_i^{r_{ij}}(k)] = 0$.

To show that $\tilde{x}_i(k|k)$ strictly decreases after the inter-agent measurement update, we show that the scalar-valued quadratic function $V(k|k) := E[\tilde{x}_i(k|k)]^T\Phi_i(k|k)E[\tilde{x}_i(k|k)]$ decreases from $V(k|k-1)$. Using the result from (A.4), we can find that

$$V(k|k) = E[\tilde{x}_i(k|k-1)]^T\Phi_i(k|k-1)^T\Phi_i(k|k)^{-1}$$

$$\Phi_i(k|k-1)E[\tilde{x}_i(k|k-1)]. \tag{A.5}$$

By applying the Woodbury matrix identity, we can find that

$$\begin{aligned}\Phi_i(k|k)^{-1} =&[\Phi_i(k|k-1)+R_i(k)^{-1}]^{-1}\\ =&\Phi_i(k|k-1)^{-1}-[\Phi_i(k|k-1)\\ &+\Phi_i(k|k-1)R_i(k)\Phi_i(k|k-1)]^{-1}.\end{aligned} \tag{A.6}$$

Substituting (A.6) into (A.5) and rearranging lead to

$$\begin{aligned}V(k|k) =&E[\tilde{x}_i(k|k-1)]^T\Phi_i(k|k-1)^T E[\tilde{x}_i(k|k-1)]\\ &-E[\tilde{x}_i(k|k-1)]^T\Phi_i(k|k-1)^T[\Phi_i(k|k-1)\\ &+\Phi_i(k|k-1)R_i(k)\Phi_i(k|k-1)]^{-1}\\ &\Phi_i(k|k-1)E[\tilde{x}_i(k|k-1)].\end{aligned} \tag{A.7}$$

Note that the first term on the right-hand side is $V(k|k-1)$, and the second term is non-positive, i.e., $V(k|k) \leq V(k|k-1)$. This proves that $V(k|k)$ decreases from $V(k|k-1)$ after inter-agent measurement update. □

References

1. Desai JP, Ostrowski JP, Kumar V. Modeling and control of formations of nonholonomic mobile robots. *IEEE Transactions on Robotics and Automation* 2001; 17(6): 905-908.

2. Yan L, Ma B. Adaptive practical leader-following formation control of multiple nonholonomic wheeled mobile robots. *International Journal of Robust and Nonlinear Control* 2020; 30(17): 7216–7237. doi: 10.1002/rnc.5165

3. Dou L, Yang C, Wang D, Tian B, Zong Q. Distributed finite-time formation control for multiple quadrotors via local communications. *International Journal of Robust and Nonlinear Control* 2019; 29(16): 5588–5608. doi: 10.1002/rnc.4687

4. Dong X, Yu B, Shi Z, Zhong Y. Time-varying formation control for unmanned aerial vehicles: Theories and applications. *IEEE Transactions on Control Systems Technology* 2015; 23(1): 340–348.

5. Cui R, Ge S, Voon Ee How B, Choo Y. Leader–follower formation control of underactuated autonomous underwater vehicles. *Ocean Engineering* 2010; 37(17): 1491–1502. doi: https://doi.org/10.1016/j.oceaneng.2010.07.006

6. Das B, Subudhi B, Pati B. Cooperative formation control of autonomous underwater vehicles: An overview. *International Journal of Automation and Computing* 2016; 13(3): 199–225. doi: 10.1007/s11633-016-1004-4

7. Guillet A, Lenain R, Thuilot B, Martinet P. Adaptable robot formation control: adaptive and predictive formation control of autonomous vehicles. *IEEE Robotics & Automation Magazine* 2014; 21(1): 28-39.

8. Giulietti F, Pollini L, Innocenti M. Autonomous formation flight. *IEEE Control Systems Magazine* 2000; 20(6): 34-44.

9. DeVries L, Paley DA. Wake sensing and estimation for control of autonomous aircraft in formation flight. *Journal of Guidance, Control, and Dynamics* 2016; 39(1): 32-41.

10. Dai GB, Liu YC. Distributed coordination and cooperation control for networked mobile manipulators. *IEEE Transactions on Industrial Electronics* 2017; 64(6): 5060-5074.

11. Loría A, Dasdemir J, Jarquin NA. Leader-follower formation and tracking control of mobile robots along straight paths. *IEEE Transactions on Control System Technology* 2016; 24(2): 727-732.

12. Liang X, Liu YH, Wang H, Chen W, Xing K, Liu T. Leader-following formation tracking control of mobile robots without direct position measurements. *IEEE Transactions on Automatic Control* 2016; 61(12): 4131-4137.

13. Yu J, Dong X, Li Q, Ren Z. Practical time-varying formation tracking for high-order nonlinear multi-agent systems based on the distributed extended state observer. *International Journal of Control* 2019; 92(10): 2451-2462.

14. Wang Z, Wu Y, Li T, Zhang H. Adaptive Fault-Tolerant Time-Varying Formation Tracking for Multiagent Systems with Multiple Leaders. *International Journal of Robust and Nonlinear Control* 2019; 29(6): 1807-1822.

15. Bijani S, Robertson D. A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review* 2014; 42(4): 607–636. doi: 10.1007/s10462-012-9343-1

16. Gil S, Kumar S, Mazumder M, Katabi D, Rus D. Guaranteeing spoof-resilient multi-robot networks. *Autonomous Robots* 2017; 41(6): 1383–1400. doi: 10.1007/s10514-017-9621-5

17. Minelli M, Panerati J, Kaufmann M, Ghedini C, Beltrame G, Sabattini L. Self-optimization of resilient topologies for fallible multi-robots. *Robotics and Autonomous Systems* 2020; 124: 103384.

18. Meng Z, Anderson BDO, Hirche S. Formation control with mismatched compasses. *Automatica* 2016; 69: 232-241.

19. Zhu Y, Zhou L, Zheng Y, Liu J, Chen S. Sampled-data based resilient consensus of heterogeneous multiagent systems. *International Journal of Robust and Nonlinear Control* 2020; 30(17): 7370–7381. doi: 10.1002/rnc.5179

20. Fu W, Ma Q, Qin J, Kang Y. Resilient consensus-based distributed optimization under deception attacks. *International Journal of Robust and Nonlinear Control* 2021; 31(6): 1803–1816. doi: 10.1002/rnc.5026

21. Bahr A, Leonard JJ, Fallon MF. Cooperative localization for autonomous underwater vehicles. *The International Journal of Robotics Research* 2009; 28(6): 714-728.

22. Song Z, Mohseni K. Hierarchical underwater localization in dominating background flow fields. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). ; 2013; Tokyo, Japan: 3356–3361

23. Paull L, Saeedi S, Seto M, Li H. AUV navigation and localization: A review. *IEEE Journal of Oceanic Engineering* 2014; 39(1): 131-149. doi: 10.1109/JOE.2013.2278891

24. Saeedi S, Trentini M, Seto M, Li H. Multiple-robot simultaneous localization and mapping: A review. *Journal of Field Robotics* 2016; 33(1): 3-46. doi: 10.1002/rob.21620

25. Wymeersch H, Lien J, Win M. Cooperative localization in wireless networks. *Proceedings of the IEEE* 2009; 97(2): 427-450. doi: 10.1109/JPROC.2008.2008853

26. Kia SS, Rounds S, Martinez S. Cooperative localization for mobile agents: A recursive decentralized algorithm based on Kalman-filter decoupling. *IEEE Control System Magazine* 2016; 36(2): 86–101. doi: 10.1109/MCS.2015.2512033

27. Godsil C, Royle G. *Algebraic Graph Theory*. Springer . 2001.

28. Mesbahi M, Egerstedt M. *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press . 2010.

29. Mahmoud MS. *Resilient Control of Uncertain Dynamical Systems*. Springer, New York . 2004.

30. Modares H, Kiumarsi B, Lewis FL, Ferrese F, Davoudi A. Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators. *IEEE Transactions on Cybernetics* 2020; 50(3): 1240-1250.

31. Hwang I, Kim S, Kim Y, Seah CE. A survey of fault detection, isolation, and reconfiguration methods. *IEEE Transactions on Control Systems Technology* 2010; 18(3): 636-653.

32. Liu YC, Chopra N. Controlled synchronization of heterogeneous robotic manipulators in the task space. *IEEE Transactions on Robotics* 2012; 28(1): 268-275.

33. Sontag ED. A remark on the converging-input converging-state property. *IEEE Transactions on Automatic Control* 2003; 48(2): 313-314.

34. Jazwinski A. *Stochastic Processes and Filtering Theory*. Elsevier Science . 1970.

35. Ding S. *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Springer Berlin Heidelberg . 2008.

36. Pajic M, Lee I, Pappas GJ. Attack-resilient state estimation for noisy dynamical systems. *IEEE Transactions on Control of Network Systems* 2017; 4(1): 82-92. doi: 10.1109/TCNS.2016.2607420

37. Jeong Y, Eun Y. A robust and resilient state estimation for linear systems. *IEEE Transactions on Automatic Control* 2022; 67(5): 2626-2632. doi: 10.1109/TAC.2021.3088780

38. Bezzo N, Weimer J, Pajic M, Sokolsky O, Pappas GJ, Lee I. Attack resilient state estimation for autonomous robotic systems. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). ; 2014: 3692–3698

39. Mishra S, Shoukry Y, Karamchandani N, Diggavi SN, Tabuada P. Secure state estimation against sensor attacks in the presence of noise. *IEEE Transactions on Control of Network Systems* 2017; 4(1): 49-59. doi: 10.1109/TCNS.2016.2606880

40. Hu L, Wang Z, Han QL, Liu X. State estimation under false data injection attacks: Security analysis and system protection. *Automatica* 2018; 87: 176-183. doi: https://doi.org/10.1016/j.automatica.2017.09.028

41. Jovanov I, Pajic M. Relaxing integrity requirements for attack-resilient cyber-physical systems. *IEEE Transactions on Automatic Control* 2019; 64(12): 4843-4858. doi: 10.1109/TAC.2019.2898510

42. Dasgupta S, Rahman M, Islam M, Chowdhury M. A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems* 2022; 23(12): 23559-23572. doi: 10.1109/TITS.2022.3197817

43. Preiss JA, Hönig W, Sukhatme GS, Ayanian N. Crazyswarm: A large nano-quadcopter swarm. In: ; 2017: 3299–3304.

44. Dixon WE. Adaptive regulation of amplitude limited robot manipulators with uncertain kinematics and dynamics. *IEEE Transactions on Automatic Control* 2007; 52(3): 488-493.

45. Liu YC, Khong MH. Adaptive control for nonlinear teleoperators with uncertain kinematics and dynamics. *IEEE/ASME Transactions on Mechatronics* 2015; 20(5): 2550-2562.

46. Khalil HK. *Nonlinear Systems*. New Jersey: Prentice Hall . 2002.