Unpredictable Trajectory Design for Mobile Agents

Jialun Li, Jianping He, Yushan Li and Xinping Guan

Abstract—Mobile agents have attracted considerable attention for their wide applications in civilian and military fields, where motion planning plays an important role when the agents operate in physical world. During this process, the agents are prone to path information leakage and malicious attacks on trajectories, which lead to individual malfunction or even mission failure. In order to protect the future position information contained in history trajectory and evade physical interception attacks, this paper studies unpredictable trajectory design for mobile agents. The major challenges lie in two parts. First, how to determine the optimal form of control for one agent, in face of unknown observation accuracy and prediction algorithm of the attacker. Second, how to extend the control method of one agent to multiple agents with coupled dynamics. The novelty of our work is threefold: i) Leveraging the stochastic control method, the trajectory design problem is formulated as optimization problems universal for various prediction methods; ii) In the sense of expectation and probability measure, we propose two kinds of optimization objectives which are considered synthetically, and obtain the optimal control for secure movement. iii) We extend the method to multiple agents in formation, and achieve a trade-off between the degradation of formation convergence and the improvement of safety level. Simulations demonstrate and verify the effectiveness of the proposed approach.

I. INTRODUCTION

Mobile agents have wide applications in both civilian and military fields, such as delivery, exploration and search. In these applications, localization, motion planning and control have been widely studied especially when agents navigate in dynamic or unknown environments. To ensure successful mission implementation, the security during running process is a major issue that needs to be tackled, drawing extensive considerations in recent years.

As a typical cyber-physical system (CPS), mobile agents suffer from various attacks from physical to cyber especially when they are deployed in adversarial environments. Cyber attacks on CPS include DoS attacks, deceptions and false data injections, to name a few [1]. Accordingly, a series of attack-modeling analyses, attack-detection mechanisms and resilient algorithms have been presented to increase the resiliency of some common CPS, e.g., smart grids and industrial processes [2]–[4]. With the help of these tools, certain security design of mobile agents is also able to be guaranteed likewise [5]–[7]. The special point lies in that, for mobile agents, motion planning plays an important role and security problems related to motions are different from those of common CPS for several reasons. On one hand, when they operate in physical world, they are physically accessible inevitably. Their trajectories can be observed and communications can be eavesdropped and intervened, which make attacks feasible to conduct, e.g., physical interception attack and information manipulation. On the other hand, the trajectories of agents carry sensitive data about their future positions and the task to be performed. For example, when agents moves in a simple pattern (e.g., uniform linear motion), their future paths are easy to be predicted as well as the destination. Based on future positions, the attacker can elaborately plan attack strategies to accurately intercept them or distort them to the preset trap, leading to individual malfunction or even mission failure. Therefore, path information leakage and possible attack on trajectories, which are not considered in common CPS security, are prominent issues that need to be addressed.

Some works have been carried out to study these problems. For example, in [8], future path information eavesdropped issue is considered and coding scheme is presented to guarantee secrecy. [9] presents a SVR-based attack to lure agents to the preset trap area. This attack is conducted only based on trajectory data without any prior information of the system dynamics. In [10], data tampering targeted on path distortion is analyzed and secure control is designed.

However, in terms of how to quantify secrecy of trajectory itself and designing optimal unpredictable path, related researches are still critically lacking [10]. Different from traditional anti-predator behaviors in biology or classical pursuit-evasion games, this problem is novel and more challenging. First, researches on anti-predator behaviors emphasize on explanations for these mechanisms according to their specific functions and mechanistic underpinning [11]. Although there are evaluation methods of path complexity like information-theoretic approach used in [12], they are hard to design the optimal anti-predator behaviors for mobile agents. Second, in pursuit-evasion games, the interactions between pursuers and evaders are modeled as differential equations and an optimal control problem is set up [13], where the model is known and deterministic to each other, more simple than the interested scenario with security consideration.

Motivated by above observations, in this paper, we focus on quantifying secrecy of trajectory and designing an unpredictable trajectory for mobile agents to increase the security during their operation. Specially, we present a stochastic control method to achieve unpredictable trajectory for mobile agents. Based on this, two optimal distributions of stochastic control are obtained according to proposed expectation and probability indexes. By combining results...
of them, we come to the method to design control for one agent. Then, we extend the results to formation control of multiple mobile agents. The performance degradation of formation convergence introduced by the stochastic control is quantitatively evaluated. The main contributions of our work are summarized as follows.

1. From the perspective of security, we propose a stochastic control method to make the trajectory of an agent unpredictable for attackers. The method is of strong generalization by its insensitivity to various external estimations.
2. We propose the expectation and probability measures as optimization objectives. With both the two factors taken into consideration, we obtain the optimal distributions of the stochastic inputs.
3. By common formation control, we extend our results to multiple mobile agents and evaluate the performance degradation of formation convergence, achieving a tradeoff between the cooperation and security requirements.

This paper is organized as follows. In Section II, the problem is formulated as optimization problems. In Section III, optimization problems are solved and the optimal control is designed for one agent. In Section IV, we extend conclusions to agents in formation. Section V shows the simulation results and Section VI concludes.

II. PRELIMINARIES AND PROBLEM FORMULATION

A. Motion Control of Mobile Agents

Consider $N$ mobile agents moving on 2-D plane with single-integrator kinematics, whose discrete form is

$$x_i((l+1)T_c) = x_i(lT_c) + u_{c,i}(lT_c)T_c, \ i = 1, 2, \ldots, N, \ (1)$$

where $x_i = [x^1_i, x^2_i]^T \in \mathbb{R}^2$ is the position vector and $u_{c,i} = [u^1_{c,i}, u^2_{c,i}]^T \in \mathbb{R}^2$ is the control input without security concern, and $T_c$ is corresponding control period. For convenience, we formulate $u_{c,i}$ by

$$u_{c,i} = g_{i}(x_1, \ldots, x_N) + v_i, \ (2)$$

where $g_{i}(x_1, \ldots, x_N)$ is a function of $\{x_1, \ldots, x_N\}$ and $v_i$ is independent with the position vectors. Clearly, if there is no interaction between agents, $u_{c,i}$ is determined by agent $i$ itself, i.e., $u_{c,i} = g_{i}(x_i) + v_i$.

B. Stochastic Motion and Prediction Model

To make the trajectories of mobile agents unpredictable, an extra input $\theta_i = [\theta^1_i, \theta^2_i]^T$ is added to $u_{c,i}$, i.e.,

$$x_i((l+1)T_c) = x_i(lT_c) + (u_{c,i}(lT_c) + \theta_i(lT_c))T_c. \ (3)$$

We first determine the optimal form of $\theta$ for single agent, then apply the obtained design to formation control for secure cooperation. When considering one agent, we omit the subscript $i$ before discussing situations for multiple agents.

If $\theta$ is a bounded function of time, then the agent position is a series of regular data about time. In this situation, it is not difficult to predict the trajectory by methods like ARIMA or RNN [14]. However, if $\theta$ is chosen as a random vector sequence satisfying certain distribution, then the agent position is random and hard to be predicted accurately based on history trajectory data. Therefore, the randomness design of $\theta$ is leveraged to make the trajectory unpredictable.

The probability density function (PDF) of $\theta$ is $f_\theta(y) = [f_\theta^1(y), f_\theta^2(y)]^T$, where $\theta$ satisfies

$$E(\theta^l) = 0, D(\theta^l) \leq (\sigma^l)^2, \ l = 1, 2. \ (4)$$

Let $T$ be the update period of $\theta$, and we suppose $T = N_T T_o \ (N_T \in \mathbb{N}^+)$. During time slot $[kT, (k+1)T]$, the motion is updated for $N_T$ times, given by

$$x(kT + (l+1)T_o) = x(kT + lT_o) + u_c(kT + lT_o) + \theta(kT)/T_o, \ (5)$$

where $l = 0, 1, \ldots, N_T - 1$.

Suppose there is an attacker, who aims to predict future positions of the agent by observing its position every period $T_o$. For simplicity without losing generality, we take $T = T_o^{-1}$. With the notations simplified, the trajectory update from $k$-th to $(k+1)$-th observation of the attacker is given by

$$x(k+1) = x(k) + \sum_{l=0}^{N_T-1} u_c(k + lT_o/T_o)T_o + \theta(k)T_o$$

$$= x(k) + \pi(k, k+1)T_o + \theta(k)T_o$$

$$= x(k) + u(k, k+1)T_o, \ (6)$$

where $u(k, k+1) = [u^1, u^2]^T$. Since $u(k, k+1)$ is a definite function of time, $u(k, k+1)$ shares the same type of distribution with $\theta$ but different PDF, satisfying

$$E(u^l) = \pi^l, D(u^l) \leq (\sigma^l)^2. \ (7)$$

In order to design unpredictable trajectory, prediction model is given here. The trajectory data obtained at $t = kT$ by attacker is denoted by $z_{l;k} = \{z(1), \ldots, z(k)\}$, and it can be used for further prediction or information fusion, e.g., Kalman Filter. Based on $z_{l;k}$, the prediction of $u(k, k+1)$ is $\hat{u}(k, k+1)$ and the posteriori estimate of $x(k)$ is $\hat{x}(k)$.

Let $\varepsilon(k)$ be the error of posteriori estimate, i.e., $\varepsilon(k) = x(k) - \hat{x}(k) = [\varepsilon^1(k), \varepsilon^2(k)]^T$. Since $\varepsilon(k)$ is relevant to optimal design of $\theta$, we divide $\varepsilon(k)$ into two situations.

**Case 1** ($\varepsilon(k) \equiv 0$): $\hat{x}(k)$ is called optimal iff optimal posteriori estimate $\hat{x}^*(k) = x(k)$.

**Case 2** ($\varepsilon(k)$ is a random vector): $\hat{x}(k)$ is unbiased estimation which means that $E(\varepsilon) = [0, 0]^T$. $\varepsilon(k)$ and $u(k, k+1) - \hat{u}(k, k+1)$ are independent with each other at each time. The PDF of $\varepsilon$ is unknown and unknown variance denotes by $D(\varepsilon) = [\sigma^2_{\varepsilon^1}, \sigma^2_{\varepsilon^2}]^T$.

Next, the position prediction $\hat{x}(k+1|k)$ is given by

$$\hat{x}(k+1|k) = \hat{x}(k) + \hat{u}(k, k+1)T_o. \ (8)$$

C. Problem of Interest

Assuming the attacker aims to predict the future position of $\tau$ steps after current time ($\tau \in \mathbb{N}^+$), then the prediction accuracy of attacker is described by

$$S = \|x(k+\tau) - \hat{x}(k+\tau|k)\|^2. \ (9)$$

1. When $T_o$ is unknown, we suppose $T_o_{min} \leq T_o \leq T_o_{max}$ and then we can use similar analysis to design the control. The details will be discussed in our future work.
We take the case of $\tau = 1$ as basis and extend the results to $\tau \in \mathbb{N}^+$. Since $S$ cannot be optimized directly due to its randomness, we introduce mathematical expectation function $E(S)$ and probability measure $Pr(S \leq \alpha^2)$, respectively, as optimization objective functions to determine the optimal $f_0(y)$. The problems are formulated as

$$\begin{align*}
P_1: \quad & \max \min_{f_0(y)} E(S) \quad \text{s.t. } E(\theta^\ell) = 0, D(\theta^\ell) \leq (\sigma^\ell)^2, \quad (10) \\
\quad & \text{and} \\
P_2: \quad & \min \max_{f_0(y)} Pr(S \leq \alpha^2) \quad \text{s.t. } E(\theta^\ell) = 0, D(\theta^\ell) \leq (\sigma^\ell)^2, \alpha \in \mathbb{R}^+ \quad (11)
\end{align*}$$

Note $E(S)$ reflects the mean deviation between the actual and predicted positions of an agent, and $Pr(S \leq \alpha^2)$ denotes the probability that the prediction accuracy satisfies the preset range. The modeling method of $P_1$ and $P_2$ can be understood from two perspectives. First, they can be viewed as optimizing the worst situations for the agent, i.e., the smallest $E(S)$ and the largest $Pr(S \leq \alpha^2)$ are the best prediction for the attacker [15], and we need to make the prediction less reliable. Second, they can be seen as a game between the agent and attacker [7].

III. STOCHASTIC CONTROL DESIGN FOR ONE AGENT

In this section, we give the optimal forms of $\theta$ for $P_1$ and $P_2$ to make the trajectory of one agent unpredictable.

A. Optimal Distribution of $P_1$

Mathematically, we first give the definition of the optimality in terms of the attacker’s prediction and distribution of $\theta$.

$\textbf{Definition 1: (Optimal input prediction)}$ When $J(S) = E(S)$, if $\forall \hat{u}(k, k+1) \in \mathbb{R}^{2 \times 1}$,

$$J(f_0(y), \hat{u}(k, k+1), \hat{x}(k)) \geq J(f_0(y), \hat{u}^*(k, k+1), \hat{x}(k)),$$

then $\hat{u}^*(k, k+1)$ is an optimal input prediction respect to $\hat{x}(k)$ in the sense of expectation.

$\textbf{Definition 2: (Optimal distribution)}$ In the sense of expectation, if arbitrary $f_0(y)$ satisfies

$$J(f_0(y), \hat{u}^*(k, k+1), \hat{x}(k)) \leq J(f_0^*(y), \hat{u}^*(k, k+1), \hat{x}(k)),$$

$f_0^*(y)$ is the optimal distribution.

$\textbf{Theorem 1:}$ For Case 1, $f_0(y)$ is the optimal distribution for $P_1$ iff

$$D(\theta^\ell) = (\sigma^\ell)^2.$$ 

$\textbf{Proof:}$ The optimal distribution $f_0^*(y)$ is obtained by solving $P_1$ under condition $\hat{x}(k) = x(k)$. We have

$$J = E \left[ ||x(k) + u(k, k+1)T - \hat{x}(k) - \hat{u}(k, k+1)T||_2^2 \right]$$

$$= E \left[ (u^2 - \hat{u}^2)^2 \right] T^2 + E \left[ (u^2 - \hat{u}^2)^2 \right] T^2$$

$$= \frac{1}{2} E(u^2) T^2 + E(u^2)(T^2 - 2E(u^2)) \hat{u}^2$$

$$+ E(u^2)^2 E(u^2)^T T^2. \quad (12)$$

Then, the optimal input prediction and index satisfy

$$\hat{u}^*(k, k+1) = \arg \min_{\hat{u}(k, k+1)} J \left[ E(u^1), E(u^2) \right]^T,$$

$$\min_{\hat{u}(k, k+1)} J = \{D(u^1) + D(u^2)\} T^2. \quad (13)$$

Hence, $f_0(y)$ is optimal distribution iff it makes $D(u^i)$ maximal. According to the relationship between $\theta(k)$ and $u(k, k+1)$ given by (7), we have completed the proof. $\blacksquare$

$\textbf{Remark 1:}$ Theorem 1 indicates that the larger the variances are, the harder attacker makes precise predictions, which is consistent with our intuitions.

In order to obtain corresponding conclusion in Case 2, a lemma is given first.

$\textbf{Lemma 1:}$ Let $X = [X_1, X_2, \cdots, X_n]^T$ and $Y = [Y_1, Y_2, \cdots, Y_n]^T$. Suppose that random variable $X_i$ is independent from random variable $Y_i$ and $E(Y_i) = 0, i = 1, 2, \cdots, n$. Then, we have

$$E((X + Y)^T (X + Y)) = \sum_{i=1}^{n} E(X_i^2) + \sum_{i=1}^{n} E(Y_i^2).$$

Utilizing Lemma 1, we obtain

$$\min_{\hat{u}(k, k+1)} J = [D(u^1) + D(u^2)]T^2 + \sigma_{z_1}^2 + \sigma_{z_2}^2. \quad (14)$$

Compared with the cost $J$ of Case 1 given by (13), there are two more terms $\sigma_{z_1}^2, \sigma_{z_2}^2$ in (14). Since the method to estimate $\hat{x}(k)$ is unknown, it is impossible to give analytical expression about $f_0(y)$ to maximize $E(S)$. Even so, the same result in Theorem 1 is able to be obtained for Case 2 qualitatively. Note $\hat{x}(k)$ is calculated by fusing the prediction $\hat{x}(k|k-1)$ and the measurement $z(k)$ at $kT$, therefore, $z(k)$ is dependent with them. For $\hat{x}(k|k-1)$, larger random input variances will increase the prediction error, which leads to higher $\sigma_{z_1}^2, \sigma_{z_2}^2$ and $E(S)$. As for $z(k)$, an extreme case is that the attacker takes $\hat{x}(k) = z(k)$. Then, $D(x(k) - z(k))$ is relevant to the sensing accuracy instead of the input variances, and $\sigma_{z_1}^2 + \sigma_{z_2}^2$ becomes constant. By combining the two factors, we obtain the same conclusion as that of Case 1.

However, taking objective function $J(S) = E(S)$ brings some drawbacks. On the one hand, with $E(S)$ representing the mean deviation between actual and predicted positions, when $D(S)$ is large, $S$ is much smaller than the mean at some moments. On the other hand, specific function form of $f_0(y)$ cannot be determined. Therefore, we leverage the probability measure as $J(S)$ and formulate problem $P_2$.

B. Optimal Distribution of $P_2$

$\textbf{Definition 3: (Optimal input prediction)}$ For $J = Pr(S \leq \alpha^2)$, if $\exists \alpha_1 \in \mathbb{R}, \forall \hat{u}(k, k+1) \in \mathbb{R}^{2 \times 1}$ and $\alpha \in (0, \alpha_1],$

$$J(f_0(y), \hat{u}(k, k+1), \hat{x}(k), \alpha) \leq J(f_0(y), \hat{u}^*(k, k+1), \hat{x}(k), \alpha),$$

then, $\hat{u}^*(k, k+1)$ is an optimal input prediction respect to $\hat{x}(k)$ in the sense of probability.

$\textbf{Definition 4: (Optimal distribution)}$ In the sense of probability, if arbitrary PDF vector $f_0$ satisfies

$$J(f_0(y), \hat{u}^*(k, k+1), \hat{x}(k), \alpha) \geq J(f_0^*(y), \hat{u}^*(k, k+1), \hat{x}(k), \alpha),$$

then, $f_0^*(y)$ is the optimal distribution.
Theorem 2: For Case 1, $f_\theta(y)$ is the optimal distribution in the sense of probability iff $f_{\theta_1}(y)$ and $f_{\theta_2}(y)$ are uniform distributions with finite maximum variances, i.e.,

$$f^*_{\theta_{1,2}}(y) = \begin{cases} \frac{1}{2\sqrt{3}\sigma^\ell}, & \text{if } y \in [-\sqrt{3}\sigma^\ell, \sqrt{3}\sigma^\ell], \\ 0, & \text{otherwise}. \end{cases}$$

The proof is omitted here due to the space limited.

Corollary 1: For Case 2, $f_\theta(y)$ is the optimal distribution iff elements of $\varepsilon(k) + \theta(k)T$ subject to the uniform distributions with maximum variances and independent with each other.

Remark 2: For both cases, the optimal distribution for $P_1$ and $P_2$ have the same results in variances, but solution of $P_2$ gives the specific form for the PDF of $\theta$.

Note the distribution of $\varepsilon(k)$ is unknown in practice, making it hard to obtain minimum $\max J$. But in Case 2, $\varepsilon(k)$ will not make probability $Pr(S \leq \alpha^2)$ increase and degrade the performance of random input with arbitrary PDF $f_\theta(y)$, which is guaranteed by the following theorem.

Theorem 3: Let $\hat{u}_1^*(k, k+1)$ and $\hat{u}_2^*(k, k+1)$ be the optimal input predictions for $\hat{x}(k) \neq \hat{x}^*(k)$ and $\hat{x}^*(k)$, respectively. Then we obtain $\hat{u}_1^*(k, k+1)$, $\hat{x}(k), \alpha \leq J(f_{\theta_1}(y), \hat{u}_1^*(k, k+1), \hat{x}^*(k), \alpha).

Proof: Let the PDF of $\varepsilon(k) = x(k) - \hat{x}(k)$ be $f_\varepsilon = [(f_{\varepsilon_1}, f_{\varepsilon_2})]^T$. Suppose $\Omega = \{x, y\} - (x - \bar{u}_\alpha)^2 + (y - \bar{u}_\alpha)^2 \leq \alpha^2$, $\alpha_\varepsilon = \frac{\varepsilon}{\alpha}$ and $\Omega = \{(x, y, w, v) : (\frac{\varepsilon}{\alpha} + x - \bar{u}_\varepsilon)^2 + (\frac{\tau}{\alpha} + y - \bar{u}_\varepsilon) \leq \frac{\tau}{\alpha} \}$. Choose arbitrary $\alpha_\varepsilon > 0$ and for all $\alpha \in (0, \alpha_1)$, $u(\hat{u}_1^*(k, k+1) \in \mathbb{R}^2$, it follows that

$$J(f_{\theta_1}(y), \hat{u}_1^*(k, k+1), \hat{x}(k), \alpha) = Pr\{\frac{1}{T}(x(k) - \hat{x}(k)) + (x(k) - \hat{u}_1(k, k+1) - \hat{u}_1^*(k, k+1))^T \leq \frac{\alpha^2}{\alpha^2} \}

= \int_{\mathbb{R}^2} f_\varepsilon(x) f_\theta(y) \, dxdv.$$ 

The equations above also holds for $\hat{u}_2^*(k, k+1)$ and Theorem 3 has been proved.

By combining the results of $P_1$ and $P_2$, we choose $f_\theta = f_{\theta_1}^{\ell}$, given by (15). The reasons for the $f_{\theta_1}^{\ell}$ is the optimal distribution for $P_1$ and Case 1 in $P_2$. i) For Case 2 in $P_2$, the PDF of $\varepsilon(k)$ is unknown and the optimal distribution cannot be achieved. When $E(\varepsilon(k)) \leq E(\theta(k)T)$ and $D(\varepsilon(k)) \leq D(\theta(k)T)$, which is reasonable in practice, $f_{\theta_1}^{\ell}$ is the approximately optimal. Besides, $\varepsilon(k)$ will not degrade the performance of random input with $f_{\theta_1}^{\ell}$.

Remark 3: For $\tau \in \mathbb{N}^+$, we only need to change the $(k, k+1)$ into $(k, k+\tau)$ in above formulation. Then, the same theoretical results still hold for $P_1$. And for $P_2$, it is straightforward to induce in the best distribution is given by

$$\sum_{n=0}^{\tau-1} \theta^\ell((k+n)T) \sim U[-\sqrt{3}\sigma^\ell, \sqrt{3}\sigma^\ell].$$

Note that this $f_\theta(y)$ is not uniform and should be redesigned if $\tau$ is estimable, or we take $\theta^\ell((k+n)T) \sim U[-\sqrt{3}\sigma^\ell, \sqrt{3}\sigma^\ell](n \in \mathbb{N})$ otherwise. Then, the random control sequence is not optimal for Case 1 whose performance will degrade. An extreme example is that with $\tau$ is large enough, $\sum_{n=0}^{\tau-1} \theta^\ell((k+n)T)$ obeys the normal distribution $N(0, \sigma^\ell)^2$ approximately, according to the famous central limit theorem.

IV. STOCHASTIC CONTROL FOR FORMATION CONTROL

When stochastic control designed is adopted by agents in formation, their trajectories are hard to be predicted accurately. However, since random motion of one agent has an effect on others by interactions, the performance of formation degradation is degraded inevitably, which is studied in this part.

A. Formation Convergence Level

To achieve formation control, we set $v_i = v_0 (i = 1, 2, \cdots, N)$ and introduce a virtual agent with input $v_0$ as the reference. Denote $\Delta_i = [\Delta_i^1, \Delta_i^2]^T$ as the desired relative displacement of agent $i$ to the virtual agent. We use a classical consensus-based formation control protocol by

$$g(x_1, \cdots, x_N) = \gamma_i \sum_{j \in N_i} a_{ij}(x_i(T_k - \Delta_j) - x_i(T_k - \Delta_j)).$$

When $\gamma_i = 0$, $G$ must have at least one spanning tree and $T_i \gamma_i d_t \leq 1$ holds to guarantee formation convergence.

We define the convergence level as $E(J_f)$, where $J_f$ is the deviation between the real and desired formation, given by

$$J_f = \frac{1}{4} \sum_{i=1}^{N} \sum_{j=1}^{N} w_{ij}\|x_i(t_k) - x_j(t_k) - (\Delta_i - \Delta_j)\|^2,$$

where $w_{ij} = w_{ji} \geq 0$ and $w_{ii} = 0$.

Suppose the convergence level for $\gamma_i = 0$ is $J_{f_0}$. When $\gamma_i$ is added, the convergence level is $J_{f_1}$. The performance degradation is $\Delta J_f = J_{f_1} - J_{f_0}$. In order to give expression of $\Delta J_f$, $J_{f_0}$ and $J_{f_1}$ are calculated separately by (17).

B. Convergence Level without Stochastic Input

When there is no stochastic input, by (1) and (16), the global dynamics of the formation is formulated as

$$X^\ell((k+1)T) = T_{c}\sum_{j=0}^{N-1} (I - T_c(\Gamma L))^N_{j} \theta^\ell(kT+jT_k).$$

where $X^\ell = [x_1^\ell, \cdots, x_N^\ell]^T \in \mathbb{R}^N$, $\Gamma = diag(\gamma_1, \cdots, \gamma_N)$, $(I - T_c(\Gamma L))$ is marginally stable, and $\Delta^\ell X \in \mathbb{R}^N$ is given by $\Delta^\ell X = -\gamma_i \sum_{j \in N_i} a_{ij}(\Delta_j^1 - \hat{\Delta_j}).$ Then, we obtain

$$X^\ell((k+1)T) = T_{c}\sum_{j=0}^{N-1} (I - T_c(\Gamma L))^N_{j} \theta^\ell(kT+jT_k).$$

where $G = (I - T_c(\Gamma L))^N_{j}$ is stable and $H = T_c\sum_{j=0}^{N-1} (I - T_c(\Gamma L))^N_{j} \theta^\ell(kT+jT_k).$
Let $d_{w_i} = \sum_{j=1}^{N} w_{ij}$ and $D_w = \text{diag}(d_{w_1}, \ldots, d_{w_N})$. At time $kT$, the formation convergence level $J_{f_0}$ is calculated by

$$J_{f_0} = \left( \frac{1}{2} m^T Q m^1 + r^T m^1 + s \right) + \left( \frac{1}{2} m^2 T Q m^2 + r T m^2 + s \right),$$

where $Q = D_w - [w_{ij}] = D_w - W$. We have $\lim_{k \to +\infty} J_{f_0} = 0$, i.e., the expected formation is formed.

### C. Performance Degradation with Stochastic Input

Next, we consider the formation control with stochastic input. Then, the global dynamics of (19) is reformulated as

$$X^f((k+1)T) = T_e \sum_{j=0}^{N_T-1} (I - T_e \Gamma L)^{N_T-j-1} \nu^0_j (kT+jT_e) \cdot 1$$

$$+ G X^f(kT) + H \Delta X^f + H \Theta (kT).$$

Since $E(\Theta(kT)) = 0$, we have $X^f(k) \sim (m^f(k), P^f(k))$ with unknown distribution. The evolutions of the mean and covariance are

$$\begin{cases} m^f(k+1) = G m^f(k) + H \Delta_x^f, \\ P^f(k+1) = G P^f(k) G^T + H \Sigma H^T, \end{cases}$$

where $\Delta_x^f = \text{diag}((\sigma^2_1^f, \ldots, \sigma^2_N^f))$.

Similar to the proof in [16], we have

$$J_{f_1} = \left( \frac{1}{2} m^T Q m^1 + r^T m^1 + s \right) + \frac{1}{2} \text{tr}(Q P^1(k))$$

$$+ \left( \frac{1}{2} m^2 T Q m^2 + r T m^2 + s \right) + \frac{1}{2} \text{tr}(Q P^2(k)).$$

Then, $\Delta J_f$ is given by

$$\Delta J_f = J_{f_1} - J_{f_0} = \frac{1}{2} \text{tr}(QP^1(k) + QP^2(k)).$$

Since $G \geq 0$, the $P^f$ in (22) is convergent, i.e., $\lim_{k \to +\infty} P^f = P^f_{*}$, and we have

$$\Delta J_f = \lim_{k \to +\infty} \Delta J_f = \frac{1}{2} \text{tr}(QP^1_{*} + QP^2_{*}).$$

In terms of how to design the variances for each agent, there are mainly three factors that need to be taken into consideration, i.e., formation convergence performance, extra energy consumption and security improvement. The extra energy consumption $J_e$ by adding random input is directly proportional to variances. And we take $\min_{\hat{u}(k,k+1)} E(S)$ to describe security improvement, which is expressed analytically. Let $\sigma_1^i = [\sigma_1^i, \sigma_2^i]^T$ and $c_1, c_2$ be weights. Then, the variances is determined by

$$\min_{\sigma_1, \ldots, \sigma_N} \Delta J_f^* + c_1 J_e - c_2 \min_{\hat{u}(k,k+1)} E(S),$$

where $\Delta J_f^* = \frac{1}{2} \text{tr}(QP^1_{*} + QP^2_{*})$. The curve fluctuation is due to random motion. It is alleviated when larger $\tau$ or average value of $S$ in a fixed time window is considered.
Performance Value

The values of convergence level (b) Performance degradations when and performance degradation when the variance of whole formation $\sigma^2 = \left(\frac{\sigma}{3}\right)^2$, takes different values.

Fig. 4: Performance degradation with random inputs.

the optimal for both problems. Moreover, we reveal that the estimate errors by attacker will not decrease safety indexes. Furthermore, we extend our results to formation control of multiple agents, where the performance degradation of formation convergence is quantified and the stochastic control is redesigned to obtain trade-off between cooperation and security. Finally, simulations are conducted to illustrate and verify the effectiveness.

REFERENCES


