# Unpredictable Trajectory Design for Mobile Agents

Jialun Li, Jianping He, Yushan Li and Xinping Guan

***Abstract*— Mobile agents have attracted considerable attentions 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

The authors are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China. E-mail: {jialunli, jphe, yushan_li, xpguan}@sjtu.edu.cn. This research work is partially sponsored by the National Key R&D Program of China 2017YFE0114600, NSFC 61973218, 6163301 and 61933009.

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.

- 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.
- 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.
- 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

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

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

$$u_{c,i} = g_i(x_1, \cdots, x_N) + v_i, \quad (2)$$

where $g_i(x_1, \cdots, x_N)$ is a function of $\{x_1, \cdots, x_N\}$ 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 $\theta_i = [\theta_i^1, \theta_i^2]^T$ is added to $u_{c,i}$, i.e.,

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

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

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

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

$$x(kT + (l+1)T_c) = x(kT + lT_c) + (u_c(kT + lT_c) + \theta(kT))T_c, \quad (5)$$

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

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 lossing 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

$$\begin{aligned} x(k+1) =& x(k) + \sum_{l=0}^{N_T-1} u_c(k + l\frac{T_c}{T})T_c + \theta(k)T \\ =& x(k) + \overline{u}(k, k+1)T + \theta(k)T \\ =& x(k) + u(k, k+1)T, \end{aligned} \quad (6)$$

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

$$E(u^\ell) = \overline{u}^\ell, D(u^\ell) \leq (\sigma^\ell)^2. \quad (7)$$

In order to design unpredictable trajectory, prediction model is given here. The trajectory data obtained at $t = kT$ by attacker is denoted by $\mathcal{I}_{1:k} = \{z(1), \cdots, z(k)\}$, and it can be used for further prediction or information fusion, e.g., Kalman Filter. Based on $\mathcal{I}_{1:k}$, 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 $D(\varepsilon) = [\sigma_{\varepsilon^1}^2, \sigma_{\varepsilon^2}^2]^T$.

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

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

### 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

$$S = \|x(k+\tau) - \hat{x}(k+\tau|k)\|_2^2. \quad (9)$$

[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 $f_\theta(y)$. The problems are formulated as

$$\begin{aligned} \mathbf{P1}: \quad & \max_{f_\theta(y)} \min_{\hat{u}(k,k+1)} E(S) \\ & \text{s.t. } E(\theta^\ell) = 0, D(\theta^\ell) \leq (\sigma^\ell)^2, \end{aligned} \tag{10}$$

and

$$\begin{aligned} \mathbf{P2}: \quad & \min_{f_\theta(y)} \max_{\hat{u}(k,k+1)} Pr(S \leq \alpha^2) \\ & \text{s.t. } E(\theta^\ell) = 0, D(\theta^\ell) \leq (\sigma^\ell)^2, \alpha \in \mathbb{R}^+. \end{aligned} \tag{11}$$

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 predict accuracy satisfies the preset range. The modeling method of $\mathbf{P1}$ and $\mathbf{P2}$ 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 $\mathbf{P1}$ and $\mathbf{P2}$ to make the trajectory of one agent unpredictable.

### A. *Optimal Distribution of* $\mathbf{P1}$

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

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

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

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

***Definition** 2: (Optimal distribution)* In the sense of expectation, if arbitrary $f_\theta(y)$ satisfies

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

$f_\theta^*(y)$ is the optimal distribution.

***Theorem** 1:* For **Case 1**, $f_\theta(y)$ is the optimal distribution for $\mathbf{P_1}$ iff

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

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

$$\begin{aligned} J =& E\left[\|x(k) + u(k,k+1)T - \hat{x}^*(k) - \hat{u}(k,k+1)T\|_2^2\right] \\ =& E\left[\left(u^1 - \hat{u}^1\right)^2\right] T^2 + E\left[\left(u^2 - \hat{u}^2\right)^2\right] T^2 \\ =& [(\hat{u}^1)^2 - 2E(u^1)\hat{u}^1 + (\hat{u}^2)^2 - 2E(u^2)\hat{u}^2 \\ & + E(u^1)^2 + E(u^2)^2] T^2. \end{aligned} \tag{12}$$

Then, the optimal input prediction and index satisfy

$$\begin{aligned} \hat{u}^*(k,k+1) =& \arg\min_{\hat{u}(k,k+1)} J = \left[E(u^1), E(u^2)\right]^T, \\ \min_{\hat{u}(k,k+1)} J =& \left\{D(u^1) + D(u^2)\right\} T^2. \end{aligned} \tag{13}$$

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

***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.

***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

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

Compared with the cost $J$ of **Case 1** given by (13), there are two more terms $\sigma_{\varepsilon^1}^2, \sigma_{\varepsilon^2}^2$ in (14). Since the method to estimate $\hat{x}(k)$ is unknown, it is impossible to give analytical expression about $f_\theta(y)$ 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, $\varepsilon(k)$ is dependent with them. For $\hat{x}(k|k-1)$, larger random input variances will increase the prediction error, which leads to higher $\sigma_{\varepsilon^1}^2, \sigma_{\varepsilon^2}^2$ 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 $\sigma_{\varepsilon^1}^2 + \sigma_{\varepsilon^2}^2$ 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 $f_\theta(y)$ cannot be determined. Therefore, we leverage the probability measure as $J(S)$ and formulate problem $\mathbf{P2}$.

### B. *Optimal Distribution of* $\mathbf{P2}$

***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 $\alpha \in (0, \alpha_1]$,

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

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

***Definition** 4: (Optimal distribution)* In the sense of probability, if arbitrary PDF vector $f_\theta$ satisfies

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

then, $f_\theta^*(y)$ 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.,

$$f^*_{\theta^\ell}(y)=f^U_{\theta^\ell}(y)=\begin{cases}\dfrac{1}{2\sqrt{3}\sigma^\ell}, & \text{if } y\in[-\sqrt{3}\sigma^\ell,\sqrt{3}\sigma^\ell].\\ 0, & \text{otherwise.}\end{cases} \tag{15}$$

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 $\mathbf{P1}$ and $\mathbf{P2}$ have the same results in variances, but solution of $\mathbf{P2}$ 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 $\max\limits_{\hat{u}(k,k+1)} J$. But in **Case 2**, $\varepsilon(k)$ will not make probability $Pr(S\le\alpha^2)$ 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 $\hat{x}(k)\neq x^*(k)$ and $\hat{x}^*(k)$, respectively. $\exists\,\alpha_1\in\mathbb{R}$, we have $\forall\,\alpha\in(0,\alpha_1]$,

$$J(f_\theta(y),\hat{u}_1^*(k,k+1),\hat{x}(k),\alpha)\le J(f_\theta(y),\hat{u}_2^*(k,k+1),\hat{x}^*(k),\alpha).$$

*Proof:* Let the PDF of $\varepsilon(k)=x(k)-\hat{x}(k)$ be $f_\varepsilon=[f_{\varepsilon_p},f_{\varepsilon_q}]^T$. Suppose $\Omega=\{(x,y)|(x-\hat{u}_p)^2+(y-\hat{u}_q)^2\le\alpha_T^2\},\alpha_T=\frac{\alpha}{T}$ and $\Omega_1=\{(x,y,w,v):(\frac{w}{T}+x-\hat{u}_p)^2+(\frac{v}{T}+y-\hat{u}_q)\le\alpha_T^2\}$. Choose arbitrary $\alpha_1>0$ and for $\forall\,\alpha\in(0,\alpha_1]$, $\hat{u}_1(k,k+1)\in\mathbb{R}^2$, it follows that

$$\begin{aligned}
&J(f_\theta(y),\hat{u}_1(k,k+1),\hat{x}(k),\alpha)\\
=&Pr\{\|\frac{1}{T}(x(k)-\hat{x}(k))+u(k,k+1)-\hat{u}(k,k+1)\|_2^2\le\alpha_T^2\}\\
=&\iint\limits_{\mathbb{R}^2} f_{\varepsilon_p}(w)f_{\varepsilon_q}(v)(\iint\limits_{\Omega_1} f_p(x)f_q(y)\,\mathrm{d}x\mathrm{d}y)\,\mathrm{d}w\mathrm{d}v\\
\le&\max_{\hat{u}(k,k+1)}\iint\limits_{\Omega} f_p(x)f_q(y)\,\mathrm{d}x\mathrm{d}y\cdot\iint\limits_{\mathbb{R}^2} f_{\varepsilon_p}(w)f_{\varepsilon_q}(v)\,\mathrm{d}w\mathrm{d}v\\
=&\max_{\hat{u}(k,k+1)}\iint\limits_{\Omega} f_p(x)f_q(y)\,\mathrm{d}x\mathrm{d}y\\
=&J(f_\theta(y),\hat{u}_2^*(k,k+1),\hat{x}^*(k),\alpha).
\end{aligned}$$

The equations above also holds for $\hat{u}_1^*(k,k+1)$ and Theorem 3 has been proved. ■

By combining the results of $\mathbf{P1}$ and $\mathbf{P2}$, we choose $f_\theta=f_\theta^U$, given by (15). The reasons are as follows: i) $f_\theta^U$ is the optimal distribution for $\mathbf{P1}$ and **Case 1** in $\mathbf{P2}$. ii) For **Case 2** in $\mathbf{P2}$, the PDF of $\varepsilon(k)$ is unknown and the optimal distribution cannot be achieved. When $E(\varepsilon(k))\ll E(\theta(k)T)$ and $D(\varepsilon(k))\ll D(\theta(k)T)$, which is reasonable in practice, $f_\theta^U$ is the approximately optimal. Besides, $\varepsilon(k)$ will not degrade the performance of random input with $f_\theta^U$.

*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 $\mathbf{P1}$. And for $\mathbf{P2}$, it is straightforward to induce in the best distribution is given by $\sum\limits_{n=0}^{\tau-1}\theta^\ell((k+n)T)\sim U[-\sqrt{3\tau}\sigma^\ell,\sqrt{3\tau}\sigma^\ell]$. Note that $f_\theta(y)$ is not uniform and should be redesigned if $\tau$ is estimable, or we take $\theta^\ell((k+n)T)\sim U[-\sqrt{3}\sigma^\ell,\sqrt{3}\sigma^\ell](n\in N)$ otherwise. Then, the random control sequence is not optimal for **Case 1** whose performance will degrade. An extreme example is that when $\tau$ is large enough, $\sum\limits_{n=0}^{\tau-1}\theta^\ell((k+n)T)$ obeys the normal distribution $\mathcal{N}(0,\tau(\sigma^\ell)^2)$ 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 convergence 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

$$g_i(x_1,\cdots,x_N)=\gamma_i\sum_{j\in N_i}a_{ij}((x_j(lT_c)-\Delta_j)-(x_i(lT_c)-\Delta_i)). \tag{16}$$

When $\theta_i=0$, $\mathcal{G}$ must have at least one spanning tree and $T_c\gamma_i d_i<1$ 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

$$J_f=\frac{1}{4}\sum_{i=1}^N\sum_{j=1}^N w_{ij}\|(x_i-x_0)-(x_j-x_0)-(\Delta_i-\Delta_j)\|_2^2, \tag{17}$$

where $w_{ij}=w_{ji}\ge0$ and $w_{ii}=0$.

Suppose the convergence level for $\theta_i=0$ is $J_{f_0}$. When $\theta_i$ 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

$$X^\ell((k+1)T_c)=(I-T_c\Gamma L)X^\ell(kT_c)+v_0^\ell(kT_c)T_c\,\mathbf{1}+T_c\Delta_X^\ell, \tag{18}$$

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

$$\begin{aligned}X^\ell((k+1)T)=&T_c\sum_{j=0}^{N_T-1}(I-T_c\Gamma L)^{N_T-j-1}v_0^\ell(kT+jT_c)\cdot\mathbf{1}\\&+GX^\ell(kT)+H\Delta_X^\ell,\end{aligned} \tag{19}$$

where $G=(I-T_c\Gamma L)^{N_T}$ is stable and $H=T_c\sum\limits_{j=0}^{N_T-1}(I-T_c\Gamma L)^{N_T-j-1}$.

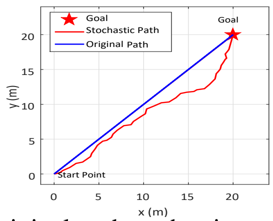



Fig. 1: Original and stochastic path of agent.

Let $d_{w_i} = \sum_{j=1}^{N} w_{ij}$ and $D_w = \text{diag}(d_{w_1}, \cdots, d_{w_N})$. At time $kT$, the formation convergence level $J_{f_0}$ is calculated by

$$J_{f_0} = (\frac{1}{2}{m^1}^T Q m^1 + r^T m^1 + s) + (\frac{1}{2}{m^2}^T Q m^2 + r^T m^2 + s), \tag{20}$$

where $Q = D_w - [w_{ij}] = D_w - W$. We have $\lim_{k\to+\infty} J_{f_0} = J_{f_0}^* = 0$, 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

$$\begin{aligned} X^\ell((k+1)T) =& T_c \sum_{j=0}^{N_T-1} (I - T_c \Gamma L)^{N_T-j-1} v_0^\ell(kT + jT_c) \cdot \mathbf{1} \\ &+ GX^\ell(kT) + H\Delta_X^\ell + H\Theta(kT). \end{aligned} \tag{21}$$

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

$$\begin{cases} m^\ell(k+1) = Gm^\ell(k) + H\Delta_X^\ell, \\ P^\ell(k+1) = GP^\ell(k)G^T + H\Lambda^\ell H^T, \end{cases} \tag{22}$$

where $\Lambda^\ell = \text{diag}((\sigma_1^\ell)^2, \cdots, (\sigma_N^\ell)^2)$.

Similar to the proof in [16], we have

$$\begin{aligned} J_{f_1} =& (\frac{1}{2}{m^1}^T Q m^1 + r^T m^1 + s) + \frac{1}{2} tr(QP^1(k)) \\ &+ (\frac{1}{2}{m^2}^T Q m^2 + r^T m^2 + s) + \frac{1}{2} tr(QP^2(k)). \end{aligned} \tag{23}$$

Then, $\Delta J_f$ is given by

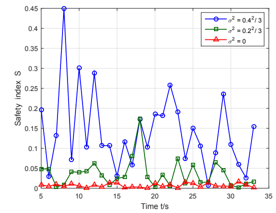
$$\Delta J_f = J_{f_1} - J_{f_0} = \frac{1}{2} tr(QP^1(k) + QP^2(k)). \tag{24}$$

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

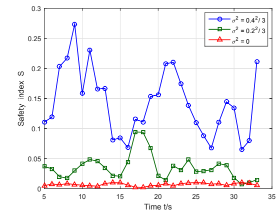
$$\Delta J_f^* = \lim_{k\to+\infty} \Delta J_f = \frac{1}{2} tr(QP^{1,*} + QP^{2,*}). \tag{25}$$

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 $J_c$ 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 $\sigma_i = [\sigma_i^1, \sigma_i^2]^T$ and $c_1, c_2$ be weights. Then, the variances is determined by

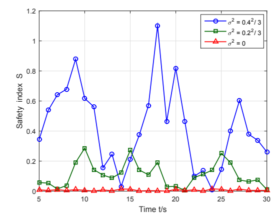
$$\min_{\sigma_1, \cdots, \sigma_N} \Delta J_f^* + c_1 J_c - c_2 \min_{\hat{u}(k,k+1)} E(S), \tag{26}$$



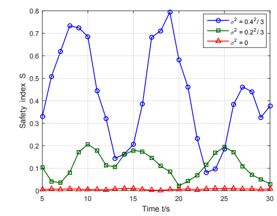
(a) Safe index values when $\tau = 1$ without smoothing processing.



(b) Safe index values when $\tau = 1$ with smoothing processing.



(c) Safe index values when $\tau = 4$ without smoothing processing.



(d) Safe index values when $\tau = 4$ with smoothing processing.

Fig. 2: Safe index corresponding to uniform distribution inputs with different variances.

In addition to variances, the distribution form of $\theta$ also needs to be reconsidered. By (21), $f_{\theta_i}$ $(i = 1, 2, \cdots, N)$ should be designed such that $H\Theta$ subjects to uniform distribution. Based on the variances and distribution, the unpredictable trajectory design for multiple agents is obtained.

## V. Simulation

### A. One Agent with Stochastic Input

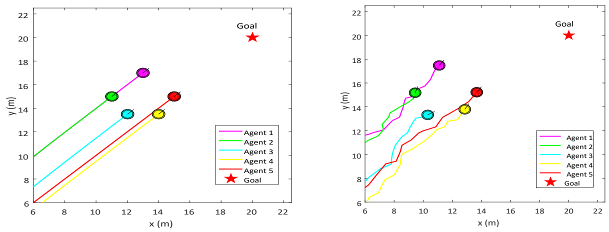
Consider an agent moves from the starting point (0,0) towards the target (20,20). Its velocities along two axes are both 0.5 units/s and velocity thresholds are 1 unit/s. Control period is $T_c = 0.1s$ and $T = T_o = 1s$ for the random input.

Figure 1 illustrates path complexity of agent motion with stochastic input. Random input $\theta$ subjects to uniform distribution with mean 0 and variance $(\sigma^\ell)^2 = (\frac{0.4}{\sqrt{3}})^2$, and the trajectory of the agent becomes irregular after adding $\theta$. The original path and target region is extremely hard to be inferred from the historical trajectory data even if the attacker has prior knowledge of uniform distribution.

Figure 2 displays relationship between values of random variable $S$ during agent motions and variances of stochastic inputs, which verifies the theorem 1. The random inputs for agent are all uniform and variances are set to be $(\sigma^\ell)^2 = 0, (\frac{0.2}{\sqrt{3}})^2$ and $(\frac{0.4}{\sqrt{3}})^2$, which verifies the theorem 1. Figure 2(b), 2(d) are achieved by smoothing data in Figure 2(a), 2(c) by $\overline{S}(k) = \frac{1}{3}(S(k-1) + S(k) + S(k+1))$. We suppose the measurement of attacker satisfies $x(k) - z(k) \sim \mathcal{N}(0, 0.01)$. Besides, the attacker uses Kalman filter algorithm to obtain agent position. In the algorithm, variances of process noise and observation noise are set to be $[(\frac{0.4}{\sqrt{3}})^2, (\frac{0.4}{\sqrt{3}})^2]^T, [0.01, 0.01]^T$ respectively. For prediction, the attacker achieves the the optimal input prediction $\hat{u}^*(k, k+1) = 0.5$. 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.

TABLE I: Contrast of input with different distributions

| | $E(S)$ | $D(S)$ | $Pr(S \leq 0.05^2)$ | $Pr(S \leq 0.1^2)$ | $Pr(S \leq 0.15^2)$ |
|---|---|---|---|---|---|
| Uniform | 0.1104 | 0.0062 | 0.2549 | 0.4783 | 0.7263 |
| Gaussian | 0.1041 | 0.0114 | 0.3824 | 0.6255 | 0.7747 |
| Laplace | 0.1145 | 0.0354 | 0.4734 | 0.6759 | 0.7816 |
| No input | 0.0 | 0.0 | 1.0 | 1.0 | 1.0 |




(a) $t = 30s$, formation control without security consideration. (b) $t = 30s$, formation control with security consideration.

Fig. 3: Illustration of $N = 5$ agents in formation.

Table I contrasts indexes of $S$ when the agent is added by stochastic control with the same variance $(\sigma^\ell)^2 = (\frac{0.4}{\sqrt{3}})^2$ but three kinds of distributions or not. We let agent keep moving and total observation time of the attacker is $500s$ which is long enough. The position estimation and input prediction are the optimal here. From the table, the mean of $S$ is almost identical for three distributions which is close to $\left\{(\sigma^1)^2 + (\sigma^2)^2\right\} T^2 = 0.1067$. But the uniform distribution has minimum $Pr(S \leq \alpha^2)$ when $\alpha$ is in suitable range, which verifies the Theorem 2. Moreover, although $Pr(S \leq \alpha^2)$ is taken as index, $D(S)$ corresponding to uniform distribution is the lowest. When $E(S)$ values are the same, smaller fluctuations will lead to higher safety levels. These results reflects advantage of formulated $\mathbf{P2}$ and best performance of random input with uniform distribution.

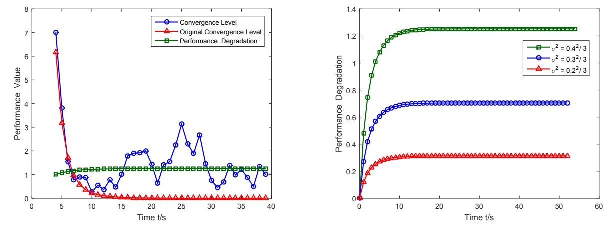
### *B. Agents in Formation with Stochastic Input*

Suppose that each agent in formation satisfy the condition for single agent above. The formation is form in a consensus-based method given by (16) with $\gamma_i = \frac{1}{2(1+d_i)}$ and $N = 5$. The initial positions of five agents are (2,1), (-5,3), (-4,-3), (1,-3) and (0,0). The desired formation is described by $\Delta^1 = [-2, -4, -3, -1, 0]^T$ and $\Delta^2 = [2, 0, -1.5, -1.5, 0]^T$. We set the same variances $\sigma$ along two axes for all agents.

Figure 3 shows the formation of five agents. In figure 4(a), the performance degradation $\Delta J_f$ is converged to $\Delta J_f^*$ with time. Under random inputs, the error relative to desired formation $J_f$ fluctuates and performance degradation equals to deviation between expectation of $J_f$ and original $J_{f_0}$. Figure 4(b) demonstrates$\Delta J_f$ increase with $\sigma^2$, serving as the criterion for choosing the variance for the formation.

## VI. Conclusion

In this paper, we investigate unpredictable trajectory design for mobile agents against malicious attacker. We start with the situation for one agent, by adding an extra input to guarantee the unpredictability. Then, two objective functions insensitive to prediction algorithms are proposed as safety indexes to achieve the optimal control. We prove that the input with uniform distribution and maximum variance is




(a) The values of convergence level and performance degradation when $\sigma^2 = (\frac{0.4}{\sqrt{3}})^2$. (b) Performance degradations when the variance of whole formation 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


[1] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE TAC*, vol. 58, no. 11, pp. 2715–2729, 2013.

[2] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *IEEE Allerton*, 2009.

[3] C. Zhao, J. He, and Q.-G. Wang, "Resilient distributed optimization algorithm against adversarial attacks," *IEEE TAC*, 2019.

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[5] S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, "Guaranteeing spoof-resilient multi-robot networks," *Autonomous Robots*, vol. 41, no. 6, pp. 1383–1400, 2017.

[6] C. Irvene, D. Formby, S. Litchfield, and R. Beyah, "Honeybot: A honeypot for robotic systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 61–70, 2017.

[7] B. Schlotfeldt, V. Tzoumas, D. Thakur, and G. J. Pappas, "Resilient active information gathering with mobile robots," in *IROS*, 2018.

[8] A. Tsiamis, A. B. Alexandru, and G. J. Pappas, "Motion planning with secrecy," in *ACC*, 2019.

[9] Y. Li, J. He, C. Chen, and X. Guan, "Learning-based intelligent attack against formation control with obstacle-avoidance," in *ACC*, 2019.

[10] G. Bianchin, Y.-C. Liu, and F. Pasqualetti, "Secure navigation of robots in adversarial environments," *IEEE Control Systems Letters*, vol. 4, no. 1, pp. 1–6, 2019.

[11] S. Roberts, T. Guilford, I. Rezek, and D. Biro, "Positional entropy during pigeon homing i: application of bayesian latent state modelling," *Journal of Theoretical Biology*, vol. 227, no. 1, pp. 39–50, 2004.

[12] J. E. Herbert-Read, A. J. Ward, D. J. Sumpter, and R. P. Mann, "Escape path complexity and its context dependency in pacific blue-eyes (pseudomugil signifer)," *Journal of Experimental Biology*, vol. 220, no. 11, pp. 2076–2081, 2017.

[13] V. G. L. Mejia, F. L. Lewis, Y. Wan, E. N. Sanchez, and L. Fan, "Solutions for multiagent pursuit-evasion games on communication graphs: Finite-time capture and asymptotic behaviors," *IEEE TAC*, 2019.

[14] L. Lennart, "System identification: theory for the user," *PTR Prentice Hall, Upper Saddle River, NJ*, pp. 1–14, 1999.

[15] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan, "Privacy-preserving average consensus: privacy analysis and algorithm design," *IEEE Trans. on Signal and Information Processing over Networks*, vol. 5, no. 1, pp. 127–138, 2018.

[16] V. Katewa, F. Pasqualetti, and V. Gupta, "On privacy vs. cooperation in multi-agent systems," *International Journal of Control*, vol. 91, no. 7, pp. 1693–1707, 2018.