Unpredictable Trajectory Design for Mobile Agents

Jialun Li, Jianping He, Yushan Li and Xinping Guan

Email: jialunli@sjtu.edu.cn

Shanghai Jiao Tong University
Outline

- Problem Raised
- Problem Formulation
- Main Results
- Future Work
Problem Raised

- Consider a mobile agent moving on 2-D plane with kinematic equation
  \[ x((l + 1)T_c) = x(lT_c) + u_c(lT_c)T_c \]
  \[ x = [x^1, x^2]^T \in \mathbb{R}^2 : \text{position vector} \]
  \[ u_c = [u^1_c, u^2_c]^T \in \mathbb{R}^2 : \text{control input} \]
  \[ T_c : \text{control period} \]

- An example: \( u_c = \text{const} \)

  The trajectory is a line (the blue line in fig.)
Problem Raised

- **Leakage of future position information**

  An attacker who wants to intercept the mobile agent can predict the position \( x(l + \tau) \) of it by

  \[
  \hat{x}(l + \tau) = x(l) + \tau (x(l) - x(l-1))
  \]

  if the trajectory data obtained at \( t = lT_c \) is \( \mathcal{I}_{1l} = \{ x(1), \ldots, x(l) \} \)

  \[
  \hat{x}(l + \tau) = x(l + \tau)
  \]

  The position of agent can be predicted exactly!

- To make the trajectories of mobile agents unpredictable (red line), let

  \[
  x((l + 1)T_c) = x(lT_c) + u_c(lT_c) + \theta(lT_c)T_c.
  \]

  extra input for unpredictability

  Q: How to design the optimal \( \theta \) ?
The importance of this problem

- anti-predator behaviors in biology [1]
- pursuit-evasion games [2]
- Interceptions and latest security problem of CPS systems [3]


[3] Delay-Predictability tradeoffs in reaching a secret goal J. N. Tsitsiklis and K. Xu, Operations Research, 2018
Challenges & Novelty

- Critically lacking researches: How to design an optimal unpredictable path?

- Aspects of challenges
  - Unknown prediction algorithms
  - Unknown estimation accuracy
  - Unknown time instant and period of observation

- Novelties
  - Formulating the problems universal for various prediction methods.
  - Obtain the optimal control for secure movement
  - Extending the method to multiple agents in formation and achieve a trade-off between the degradation of formation convergence and the improvement of safety level
Problem Formulation

- Form of input $\theta$
  - A bounded function of time $\times$
  - A random vector sequence $\checkmark$

PDF: $f_{\theta}(y) = [f_{\theta^1}(y), f_{\theta^2}(y)]^T$

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

The motion during time slot $[kT, (k+1)T]$, 

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

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

- An attacker aims to predict future positions of the agent by observing
  its position every period $T_o$. We take $T = T_o$.

Unknown time instant and period of observation are not considered!
Problem Formulation

The trajectory update from k-th to (k+1)-th observation of the attacker:

\[ x(k + 1) = x(k) + \sum_{l=0}^{N_T-1} u_c (k + l \frac{T_c}{T}) + \theta(k)T \]

\[ = x(k) + \bar{u}(k, k+1)T + \theta(k)T \]

\[ = x(k) + u(k, k+1)T, \]

where \( u(k, k+1) = [u^1, u^2]^T \) and \( E(u^\ell) = \bar{u}^\ell, D(u^\ell) \leq (\sigma^\ell)^2 \).

- The trajectory data obtained at \( t = kT \) is \( \mathcal{I}_{1:k} = \{ z(1), \ldots, z(k) \} \).
- Based on \( \mathcal{I}_{1:k} \), prediction of \( u(k, k+1) \) is \( \hat{u}(k, k+1) \)
  and the posteriori estimate of \( x(k) \) is \( \hat{x}(k) \).
Problem Formulation

\[ \varepsilon(k) = x(k) - \hat{x}(k) = [\varepsilon^1(k), \varepsilon^2(k)]^T \]

- **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):
  1. \( E(\varepsilon) = [0, 0]^T \)
  2. \( \varepsilon(k) \) and \( u(k, k+1) - \hat{u}(k, k+1) \) are independent.
  3. unknown PDF and variance

The position prediction \( \hat{x}(k+1 \mid k) \) is given by

\[ \hat{x}(k+1 \mid k) = \hat{x}(k) + \hat{u}(k, k+1)T. \]

The prediction accuracy of attacker:

\[ S = \| x(k + \tau) - \hat{x}(k + \tau \mid k) \|_2^2. \]
Problem Formulation

We first take the case of $\tau = 1$ as basis and $S = \| x(k+1) - \hat{x}(k+1|k) \|_2^2$.

In order to determine the optimal $\theta$, the problems are formulated as:

**P1:** \[
\max_{f_{\theta}(y)} \min_{\hat{u}(k,k+1)} E(S) \\
\text{s.t. } E(\theta^\ell) = 0, \ D(\theta^\ell) \leq (\sigma^\ell)^2,
\]

and

**P2:** \[
\min_{f_{\theta}(y)} \max_{\hat{u}(k,k+1)} \Pr(S \leq \alpha^2) \\
\text{s.t. } E(\theta^\ell) = 0, \ D(\theta^\ell) \leq (\sigma^\ell)^2, \ \alpha \in \mathbb{R}^+.
\]

- 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, and we need to make the prediction less reliable.
- A game between the agent and attacker
Main Results

- Optimal Distribution of $P1$

**Definition 1**

**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**

**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.
Main Results

- Optimal Distribution of $P_1$

### Theorem 1

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

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

**Remark 1:** Theorem 1 indicates that the larger the variances are, the harder the attacker makes precise predictions, which is consistent with our intuitions.

**Case 2:** We are able to come to the same conclusion qualitatively.
Main Results

- Optimal Distribution of $P1$

**Lemma 1**

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

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

**Case 2:** According to Lemma 1, $\min_{\hat{u}(k,k+1)} J = [D(u^1) + D(u^2)]T^2 + \sigma_{\epsilon_1}^2 + \sigma_{\epsilon_2}^2$.

Note $\hat{x}(k)$ is calculated by fusing $\hat{x}(k | k-1)$ and $z(k)$ at $kT$.

- For $\hat{x}(k | k-1)$, larger random input variances will increase the prediction error, which lead to higher $\sigma_{\epsilon_1}^2 + \sigma_{\epsilon_2}^2$ and $E(S)$.
- As for $z(k)$, an extreme case is that the attacker takes $\hat{x}(k) = z(k)$.

$D(x(k) - z(k))$ is only relevant to the sensing accuracy and $\sigma_{\epsilon_1}^2 + \sigma_{\epsilon_2}^2$ becomes constant.
Main Results

- Optimal Distribution of P2

**Definition 3**

**Definition 3.** (Optimal input prediction) For \( J = P_r(S \leq \alpha^2) \), 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**

**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.
Main Results

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 $P1$ and $P2$ have the same results in variances, but solution of $P2$ gives the specific form for the PDF of $\theta$. 

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.,

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

• Note the distribution of $\varepsilon(k)$ is unknown in practice, making it hard to obtain minimum $\max_{\hat{u}(k,k+1)} J$.
• But in Case 2, $\varepsilon(k)$ will not increase probability $Pr(S \leq \alpha^2)$.

Theorem 3

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. \(\exists \alpha_1 \in \mathbb{R}, \forall \alpha \in (0, \alpha_1],\)

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

• $f_\theta^U$ is the optimal distribution for P1 and Case 1 in P2.
• For Case 2 in P2, when $E(\varepsilon(k)) \ll E(\theta(k)T)$ and $D(\varepsilon(k)) \ll D(\theta(k)T)$, $f_\theta^U$ is the approximately optimal. $\varepsilon(k)$ will not degrade the performance of random input.

We take $f_\theta = f_\theta^U$!
Simulations

- Simulations on one mobile agents with security consideration.

**Fig. 1:** Original and stochastic path of agent.

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

- Simulations on one mobile agents with security consideration.

Table 1: Contrast of input with three different distributions and no random input.

<table>
<thead>
<tr>
<th></th>
<th>$E(S)$</th>
<th>$D(S)$</th>
<th>$Pr(S \leq 0.05^2)$</th>
<th>$Pr(S \leq 0.1^2)$</th>
<th>$Pr(S \leq 0.15^2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform</td>
<td>0.1104</td>
<td>0.0062</td>
<td>0.2549</td>
<td>0.4783</td>
<td>0.7263</td>
</tr>
<tr>
<td>Gaussian</td>
<td>0.1041</td>
<td>0.0114</td>
<td>0.3824</td>
<td>0.6255</td>
<td>0.7747</td>
</tr>
<tr>
<td>Laplace</td>
<td>0.1145</td>
<td>0.0354</td>
<td>0.4734</td>
<td>0.6759</td>
<td>0.7816</td>
</tr>
<tr>
<td>No input</td>
<td>0.0</td>
<td>0.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

- The mean of $S$ is almost identical for three distributions which is close to $\{(\sigma^1)^2 + (\sigma^2)^2\} T^2 = 0.1067$.
- The uniform distribution has minimum $Pr(S \leq \alpha^2)$ when $\alpha$ is sufficiently small.
- $D(S)$ corresponding to uniform distribution is the lowest.
- Table 1 reflects advantage of formulated $P2$ and best performance of random input with uniform distribution.
Main Results

- Stochastic control for formation control
  - Their trajectories are hard to be predicted accurately.
  - The performance of formation convergence is degraded inevitably.
  - How to choose variances to make a trade-off between security and cooperation?

- Cooperation method
  \[ g_i(x_1, \cdots, x_N) = \gamma_i \sum_{j \in N_i} a_{ij} ((x_j(Ic(T_j)) - \Delta_j) - (x_i(Ic(T_i)) - \Delta_i)). \]

- Convergence level \( E(J_f) \)
  \[ J_f = \frac{1}{4} \sum_{i=1}^{N} \sum_{j=1}^{N} w_{ij} \left\| (x_i - x_0 - (x_j - x_0) - (\Delta_i - \Delta_j) \right\|_2^2 \]
Main Results

- Performance Degradation
  1) $\theta_i = 0$, $J_{f_0} = E(J_f)$.
  2) $\theta_i$ is added, $J_{f_1} = E(J_f)$.

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

\[
\Delta J_f^* = \lim_{k \to +\infty} \Delta J_f = \frac{1}{2}tr(QP^1*, QP^2*)
\]

- Design of $\theta_i$
  - Variance: $\min_{\sigma_1, \cdots, \sigma_N} \Delta J_f^* + c_1 J_c - c_2 \min_{\hat{u}(k, k+1)} E(S)$.
  - Distribution: $H\Theta$ subjects to uniform distribution
Conclusions & Future Work

- **Conclusions**
  - Input with uniform distribution and maximum variance is the optimal against predictions.
  - Decrease in performance by stochastic input is quantified.

- **Future work**
  - Relationship between control and observation period.
  - Unpredictability analysis by other formulated methods, e.g. path complexity.
Thank you!

Q&A