Target Tracking with Signal Spoofing: Some Negative Results

Zhongshun Zhang, Lifeng Zhou and Pratap Tokekar

***Abstract*— The paper focuses on a pursuit-evasion game in probabilistic scenario, where both pursuer and evader positions are inexact and represented by the Gaussian distribution updated by a Kalman filter. The objective for the pursuer is to design the control command to capture the evader, i.e., keeps the inter target-robot distance bounded. Here, in order to escape from the pursuer, the evader uses spoofing strategy to mislead the purser.**

I. Introduction

II. Related Work

Inspired by the predator-prey behaviors in nature, pursuit-evasion games have been extensively studied in robotics [12]. In terms of differential games, pursuit-evasion problems have been formulated and studied in [6] and [3]. For a single pursuer and a single evader game [14], sufficient conditions are proposed for guaranteeing successful capture if both agents have the same equal maximum speeds and move within the non-negative quadrant of the plane with certain initial conditions. If both agents are restricted to moving with in a circular environment, upper and lower bounds of capture time have been calculated by assuming both agents can move optimally [2]. As an extension and generalization work, a pursuit-evasion game involved with multiple pursers and a single evader has been proposed in [9] where the capture is guaranteed if the evader is initially located inside a convex hull formulated by pursuers.

A common theme of the works mentioned above is assuming a perfect geometry, i.e., the locations of both purser and evader are known. Here, we focus on the pursuit-evasion game problem where the exact positions of evader is unknown to the pursuer, i.e., only the maximum motion ability of evader or noisy position measurement can be acquired [1], [5], [7], [11], [13], [15]. The task for pursuer is to design a control strategy to eventually captures the evader. There are various ways of defining the "successful capture". Typically, in terms of uncertainty scenario, the objective for pursuer is to maintain a finite or pre-defined distance between the evader [7]. A game between two persons, a sheriff and thief has been presented in [13] where the sheriff only knows the approximate location of the thief, and the capture is due to the speed constraints of two players. Consider the uncertainty in bearing measurement, two classical pursuit-evasion games have been proposed in [15]. First, if two player are in the open plane, for any purser strategy, the evader can increase the distance with rate α(linear in time) to the purser by an adversarial sensing model. Second, if the game is played inside a bounded circle area, the evader can escape from capture for any $\alpha > 0$ when sensing uncertainty is considered. Pursuit-evasion game with a probabilistic model has been proposed in [7] where both purser and evader positions are unknown and represented as a normal distribution evolving by a Kalman filter. And the boundedness of a distance of distributions between two players are guaranteed by resorting to sensor measurements only.

KF tracking estimation, distribution

Signal spoofing A common theme in the mentioned works is how to design a pursuer's control strategy for successful capture. Here, we focus on a problem where evader formulates its escaping strategy to arbitrarily enlarge the distance between the purser and itself. Since only measurement of evader's position can be used by pursuer, the evader can adversarially add the spoofing signal on the measurement to mislead the purser. Thus, we propose an evader's spoofing strategy

The authors are with the Department of Electrical & Computer Engineering, Virginia Tech, USA. {zszhang, lfzhou, tokekar}@vt.edu.

This material is based upon work supported by the National Science Foundation under Grant #1566247.

III. Problem Formulation

We assume that the position of the robot is known accurately using on-board sensors. The motion model of the target is given by:

$$x_{t+1} = Fx_t + Bu_t + \omega_t \tag{1}$$

where $x_t \in \mathbb{R}^2$ is the position of the target at step t, u_t is the of control inputs at step t and $w_t \sim \mathbb{N}(0, R_t)$ is the Gaussian process noise at time t.

The robot was sensors to estimate the target's position. The measurement equation is:

$$z_t = Hx_t + v_t \tag{2}$$

where $v(t) \sim \mathcal{N}(0, Q_t)$.

The target can interference with the robot's sensor by adding spoofing signal to mislead the robot's estimate of the target's state. That is, $\tilde{z}_t$ is the actual measurement received by the robot, where z_t would have been the measurement without spoofing. The spoofing signal ϵ increases the measurement error directly.

$$\tilde{z}_t = z_t + \epsilon_t \tag{3}$$

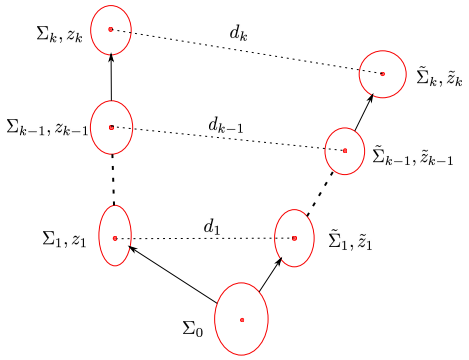

Fig. 1. Distance

We assume the robot was using a Kalman filter to estimate the target's position and the robot was not aware of the signal spoofing component ϵ_t. To avoid detection, the spoofing signal cannot be too large. Otherwise, the robot may detect abnormality and be aware the target is trying to mislead it.

We consider three problems in this paper, depending on whether the initial information available to the target or not.

Problem 1 (Off-Line with Known Initial Condition): Given a detectable and stabilized system $\{F, H, B, Q, R\}$ from (1), an known initial position and covariance (x_0, Σ_0), desired separation to avoid detection $d_1, d_2, \cdots, d_T$, discount factor $\gamma_0, \cdots, \gamma_T$. Find a sequence of spoofing signal input, $\epsilon_1, \epsilon_2, \cdots, \epsilon_T$ from time $t = 0$ to $t = T$ to maximize the sum of total norm of the spoofing signal from time $t = 0$ to $t = T$. That is,

$$\text{minimize} \quad \sum_{t=1}^{t=T} \gamma_t \cdot \|\epsilon_t\|_p^p \tag{4}$$

suject to,

$$\|m_T - \tilde{m}_T\|_p \geq d_T. \tag{5}$$

where $\rho_t(\cdot)$ is the algebraic Riccati equation [10].

When the initial condition of (m_0, Σ_0) used by the Kalman filter are not know to the target, who wants to design the spoofing signal. It can be shown that the condition $\|m_T - \tilde{m}_T\|_p \geq d_T$ can no longer be guaranteed since the measurement $z_1, \cdots, z_T$ are all with random noise. Instead of formulate the constrain condition as $\|m_T - \tilde{m}_T\| \geq d_T$, when the initial condition $m_0 \neq \tilde{m}$ and $\tilde{\Sigma}_0 \neq \tilde{\Sigma}_0$. Instead of formulating the constrain condition as deterministic, problem 2 formulates the constrain condition with the expectation.

Problem 2 (Off-line with Unknown Initial Condition): Given a initial position $[\tilde{x}_0, \tilde{\Sigma}_0]$, $\|m_0 - \tilde{m}_0\| = M_0$ and desired separation d_T, discount factor $\gamma_0, \cdots, \gamma_T$. Find a sequence of spoofing signal input, $\epsilon_1, \epsilon_2, \cdots, \epsilon_T$ from time $t = 0$ to $t = T$ to maximize the sum of total norm of the spoofing signal from time $t = 0$ to $t = T$. That is,

$$\text{minimize} \quad \sum_{t=1}^{t=T} \gamma_t \cdot \|\epsilon_t\|_p^p \tag{6}$$

subject to,

$$\|\mathbb{E}(m_T - \tilde{m}_T)\|_p \geq d_T. \tag{7}$$

In problem 2, we assume $\|\mathbb{E}(m_0 - \tilde{m}_0)\|_p = M_0$, which indicates the expected initial bias is greater or equal than a negative value M_0. As shown in theorem 1, $m_T - \tilde{m}_T$ depends on the measurement from time 0 to time T $(z_1, z_2, \cdots, z_T)$ with Gaussian noise v_t.

Problem 2 describes an off-line problem with unknown initial condition, the off-line optimal problem is to find the spoofing sequence $\{\epsilon_1, \epsilon_2, \cdots, \epsilon_T\}$ at time $t = 0$. One immediate work is to extend the off-line problem to an on-line algorithm. Problem 3 formulates an on-line problem.

Problem 3 (On-line with Unknown Initial Condition): Given a detectable and stabilized system $\{F, H, B, Q, R\}$ from (1), an bias initial position $[\tilde{x}_0, \tilde{\Sigma}_0]$, current time t, desired separation $d_1, d_2, \cdots, d_T$, a series of measurements $\{z_1^{real}, z_2^{real}, \cdots, z_t^{real}\}$ from time 0 to current time t, discount factor $\gamma_0, \cdots, \gamma_T$. Find the spoof signal input from time $t+1$ to T, $\epsilon = u_{t+1}, \epsilon_1, \cdots, \epsilon_T$. To maximize the sum of spoofing signal input form time 0 to t.

$$\text{minimize} \quad \sum_{t=1}^{t=T} \gamma_t \cdot \|\epsilon_t\|_p^p \tag{8}$$

subject to,

$$\|m_T - \tilde{m}_T\|_p \geq d_T. \tag{9}$$

IV. Signal Spoofing Strategies

Theorem 1: Given a detectable and stabilized system $\{F, H, B, Q, R\}$ from (1) (2) as the set of model parameters, the evolution of the Kalman filter gives the distributions (m_t, Σ_t) and $(\tilde{m}_t, \tilde{\Sigma}_t)$. The distance $m_t - \tilde{m}_t$ follows,

$$\begin{aligned} m_t - \tilde{m}_t = &\prod_{i=1}^{k} A_i \cdot (m_0 - \tilde{m}_0) + \\ &\sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1}(B_i + C_i) \right] + B_t + C_t \end{aligned} \tag{10}$$

Where, $A_t = F - \tilde{t}_t H F$, $B_t = (K_t - \tilde{K}_t)\left[z_t - H(F m_{t-1} + B u_{t-1})\right]$, $C_t = -\tilde{K}_t \epsilon_t$.

Theorem 1 shows that the distance of the two estimation mean at time t depends on: 1) The initial knowledge about m_0 and $\tilde{m}_0$. 2) The initial covariance matrix Σ_0 and $\tilde{\Sigma}_0$.

If we know the initial condition, as $m_0 = \tilde{m}_0$ and $\Sigma_0 = \tilde{\Sigma}_0$, since the covariance matrix updates through the same Ricatti equation (20), we have $\Sigma_t = \tilde{\Sigma}_t$ for all t. Thus, $B_t = 0$. Equation (10) can be simplified as:

$$m_t - \tilde{m}_t = \sum_{i=0}^{k-1} \left(\prod_{j=i}^{k-1} A_{j+1} C_i \right) + C_t$$

As a result, $m_t - \tilde{m}_t$ is independent of the measurements $z_1, z_2, \cdots, z_t$ if the estimator's initial condition is $m_0 = \tilde{m}_0$ and $\Sigma_0 = \tilde{\Sigma}_0$.

Consequently, Problem 1 can be solved off-line. Problem 1 and Problem 2 are generally two nonlinear programming problems for available norm p. However, when the norm is 1-norm. This section shows Problem 1 can both be formulated as a linear programming problem. Linear programming can be solved in polynomial time [8]. On the other hand, when 2-

norm is used, problem becomes a QCQP(Quadratically constrained quadratic program), which can be solved optimally. The following shows how to formulate the LP and QCQP solutions.

Theorem 2: Problem 1 and Problem 2 are linear programming problem when the norm is 1-norm($p = 1$). And Problem 1 and Problem 2 are QCQP when the norm is 2-norm($p = 2$).

A. Linear Programming Formulation $p = 1$

In Problem 1, let $\epsilon_i = [\epsilon_i^x, \epsilon_i^y]^T$. The constraint condition $\|m_t - \tilde{m}_t\|_1$ follows:

$$\begin{aligned}\|m_t - \tilde{m}_t\|_1 &= \left\| \sum_{i=0}^{t-1} \left(\prod_{j=i}^{t-1} A_{j+1} C_i \right) + C_t \right\|_1 \\ &= \left\| \sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1} \cdot \tilde{K}_i \cdot \epsilon_i \right] + \tilde{K}_t \epsilon_t \right\|_1 \end{aligned} \tag{11}$$

Where, $k = 1, 2, \cdots, T$. Since $\prod_{j=i}^{t-1} A_{t-j-1} \cdot K_i$ is constant 2×2 matrix which can be calculated from the initial covariance Σ_0 and the Riccati equation. And the 1-norm is simply the sum of the absolute values of the columns, (5) in Problem 1 is a linear combination of $\|\epsilon_i^x\|_1$ and $\|\epsilon_i^y\|_1$

Thus, Problem 1 can be relaxed as a linear programming problem.

Similarly, the constraint condition (7) in Problem 2 follows,

$$\begin{aligned}&\|\mathbb{E}\left(m_t - \tilde{m}_t\right)\|_1 \\ &= \left\| \mathbb{E}\left(\sum_{i=0}^{t-1} \prod_{j=i}^{t-1} A_{j+1} \cdot B_i + B_t \right) + \right. \\ &\left. \prod_{i=0}^{t-1} A_{t-i} \mathbb{E}(m_0 - \tilde{m}_0) + \sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1} \tilde{K}_i \epsilon_i \right] + \tilde{K}_t \epsilon_t \right\|_1 \end{aligned} \tag{12}$$

The real measurement $z_i = H(Fm_{i-1} + Bu_{i-1} + w_i) + v_i$, Where w_i and v_i are Gaussian noise. The expected measurement value of $\mathbb{E}(z_i) = H(Fm_{i-1} + Bu_{i-1})$ for all i, thus $\mathbb{E}[z_i - H(Fm_{i-1} + Bu_{i-1})] = 0$. Since $\|\mathbb{E}(m_0 - \tilde{m}_0)\|_1 = M_0$ and $\mathbb{E}[B_i] = 0$, then

$$\begin{aligned}&\|\mathbb{E}\left(m_t - \tilde{m}_t\right\|_1) \\ &= \left\| M_0 \prod_{i=0}^{t-1} A_{t-i} + \sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1} \tilde{K}_i \epsilon_i \right] + \tilde{K}_t \epsilon_t \right\|_1 \end{aligned} \tag{13}$$

As a result, the inequality constraint condition (7) can be formulated as a linear combination of $\|\epsilon_i\|_1$:

$$\left\| M_0 \prod_{i=0}^{t-1} A_{t-i} + \sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1} \tilde{K}_i \epsilon_i \right] + \tilde{K}_t \epsilon_t \right\|_1 \geq d_t \tag{14}$$

B. Quadratically Constrained Quadratic Program Formulation $p = 2$

If we consider the distance as Euclidean distance, the norm would be 2-norm. It can be shown that the problem is a Quadratically Constrained Quadratic Program(QCQP) [4], a problem closely related to quadratic programming. The standard from of QCQP is:

$$\begin{aligned} \text{minimize} \quad & \frac{1}{2} X^T P_0 X + q_0^T X + r_0 \\ \text{subject to:} \quad & \frac{1}{2} X^T P_i X + q_i^T X + r_i, \quad i = 1, \ldots, T \\ & Lx = g \end{aligned} \tag{15}$$

Where $X \in \mathbb{R}^n$ is the optimization variable, $A_i \in \mathbb{R}^{n_i \times n}$, $F \in \mathbb{R}^{p \times n}$.

Thus, in problem 1, let $X = [\epsilon_1^x, \epsilon_1^y, \cdots, \epsilon_T^x, \epsilon_T^y] \in \mathbb{R}^{2T}$. The objective function $\sum_{i=1}^{T} \|\epsilon_i\|_2^2$ follows a quadratic function and $\beta, L, g = 0$. Matrix P_T and q_T could be obtained from a transformation from the following matrix:

$$\left[\prod_{j=0}^{T-1} A_{j+1} \tilde{K}_0, \cdots, \prod_{j=T-1}^{T-1} A_{j+1} \tilde{K}_{T-1}, K_T \right]$$

since $\|Ax - b\|_2 = x^T A^T A x - 2b^T A x + b^T b$.

As shown above, when $p = 2$. Problem 1 is equivalent to QCQP.

In problem 2. The only difference is $M_0 \prod_{i=0}^{t-1} A_{t-i}$ is added. Similarly, it is also a QCQP.

V. Simulations

Consider a system:

$$x_{t+1} = \begin{bmatrix} 0.9 & 0.2 \\ 0.3 & 0.85 \end{bmatrix} x_t + u_t + \omega_t, \omega_t \sim (0, 0.1)$$

VI. Conclusion

Appendix

A. Kalman filter and Ricatti equation

Suppose the true measurement is $z(t)$, the Kalman filter estimation is:

$$\hat{x}_{t|t-1} = F x_{t-1|t-1} + B u_t \tag{16}$$

$$\hat{x}_{t|t} = F \hat{x}_{t|t-1} + K_t (z_t - H \hat{x}_{t|t-1} \tag{17}$$

$$\hat{\Sigma}_{t|t} = (I - K_t H_t)(F \hat{\Sigma}_{t|t-1} F' + R_t) \tag{18}$$

Where K_t is the Kalman gain and is given by:

$$K_t = (F \hat{\Sigma}_{t|t-1} F' + R_t) H' (H \Sigma_{t|t-1} H' + Q_t)^{-1} \tag{19}$$

From the Kalman gain update equation (19), the evolution covariance matrix at step t, and Σ_t only depends on the state model parameters and the initial condition of the covariance matrix Σ_0. And the Kalman gain at step t, K_t depends on the covariance matrix Σ_t. They do not depend on the control input series $\{u_t\}_{t=1,\cdots,k}$, measurement $\{z_t\}_{t=1,\cdots,k}$. Thus, the covariance matrix and the Kalman gain can be predict from the discrete Riccati difference equation [10].

$$\begin{aligned}\hat{\Sigma}_{t+1} =& F \hat{\Sigma}_t F^T - F \hat{\Sigma}_t H_t^T (H \hat{\Sigma}_t H^T + Q_t)^{-1} H \hat{\Sigma}_t F^T \\ &+ R_t\end{aligned}$$

B. Proof of theorem 1

Statement of theorem 1:

Proof: From the update of Kalman filter, we have

$$\begin{aligned} m_t &= m_{t|t-1} + K_t(z_t - Hm_{t|t-1}) \\ &= (I - K_tH)m_{t|t-1} + K_tz_t \\ &= (I - K_tH)(Fm_{t-1} + Bu_{u-1}) + K_tz_t \end{aligned} \tag{20}$$

And

$$\tilde{m}_t = (I - K_tH)(Fm_{t-1} + Bu_{u-1}) + K_t(z_t + \epsilon_t)$$

Induction on this yields:

$$\begin{aligned} & m_t - \tilde{m}_t \\ =&(I - K_tH)(Fm_{t-1} + Bu_{u-1}) + K_tz_t \\ &- [(I - \tilde{K}_tH)(F\tilde{m}_{t-1} + Bu_{u-1}) + \tilde{K}_t(z_t + \epsilon_t)] \\ =&(F - K_tHF)m_{t-1} - (F - \tilde{K}_tHF)\tilde{m}_{t-1} \\ &- (K_t - \tilde{K}_t)HBu_{t-1} + [K_tz_t - \tilde{K}_t(z_t + \epsilon_t)] \\ =&(F - \tilde{K}_tHF)m_{t-1} - (F - \tilde{K}_tHF)m_{t-1} \\ &- (K_t - \tilde{K}_t)HBu_{t-1} + (K_t - \tilde{K}_t)z_t - \tilde{K}_t\epsilon_t \\ &- (K_t - \tilde{K}_t)HFm_{t-1} \\ =&(F - \tilde{K}_tHF)(m_{t-1} - \tilde{m}_{t-1}) \\ &+ (K_t - \tilde{K}_t)[z_t - H(Fm_{t-1} + Bu_{t-1})] - \tilde{K}_t\epsilon_t \end{aligned} \tag{21}$$

Let,

$$A_t = F - \tilde{K}_tHF$$

$$B_t = (K_t - \tilde{K}_t)[z_t - H(Fm_{t-1} + Bu_{t-1})]$$

$$C_t = -\tilde{K}_t\epsilon_t$$

Then,

$$\begin{aligned} & m_t - \tilde{m}_t \\ =&A_t(m_{t-1} - \tilde{m}_{t-1}) + B_t + C_t \\ =&A_t[A_{t-1}(m_{t-1} - \tilde{m}_{t-1}) + B_{t-1} + C_{t-1}] \\ &\vdots \\ =&\prod_{i=t}^{t} A_i \cdot (m_0 - \tilde{m}_0) + \\ &(B_t + C_t) + A_t(B_{t-1} + C_{t-1}) \\ &+ A_tA_{t-1}(B_{t-2} + C_{t-2}) \cdots \\ &+ A_t \cdots A_3A_2A_1(B_0 + C_0) \\ =&\prod_{i=t}^{t} A_i \cdot (m_0 - \tilde{m}_0) + \\ &\sum_{i=0}^{t-1} \left[\prod_{j=i}^{t-1} A_{j+1}(B_i + C_i) \right] + B_t + C_t \end{aligned} \tag{22}$$

REFERENCES

[1] Saad A Aleem, Cameron Nowzari, and George J Pappas. Self-triggered pursuit of a single evader with uncertain information. *arXiv preprint arXiv:1512.06184*, 2015.

[2] Laurent Alonso, Arthur S Goldstein, and Edward M Reingold. lion and man: Upper and lower bounds. *ORSA Journal on Computing*, 4(4):447–452, 1992.

[3] Tamer Basar and Geert J Olsder. Dynamic noncooperative game theory (classics in applied mathematics). 1999.

[4] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[5] Leonidas J Guibas, Jean-Claude Latombe, Steven M LaValle, David Lin, and Rajeev Motwani. A visibility-based pursuit-evasion problem. *International Journal of Computational Geometry & Applications*, 9(04n05):471–493, 1999.

[6] Rufus Isaacs. *Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization*. Courier Corporation, 1999.

[7] Chanyoung Jun, Subhrajit Bhattacharya, and Robert Ghrist. Pursuit-evasion game for normal distributions. In *Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on*, pages 83–88. IEEE, 2014.

[8] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*, pages 302–311. ACM, 1984.

[9] Swastik Kopparty and Chinya V Ravishankar. A framework for pursuit evasion games in rn. *Information Processing Letters*, 96(3):114–122, 2005.

[10] Panqanamala Ramana Kumar and Pravin Varaiya. *Stochastic systems: Estimation, identification, and adaptive control*, volume 986. Prentice Hall Englewood Cliffs, NJ, 1986.

[11] Steven M LaValle. *Planning algorithms*. Cambridge university press, 2006.

[12] Darren Pais and Naomi E Leonard. Pursuit and evasion: evolutionary dynamics and collective motion. In *AIAA Guidance, Navigation and Control Conference*, pages 1–14, 2010.

[13] Günter Rote. Pursuit-evasion with imprecise target location. In *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 747–753. Society for Industrial and Applied Mathematics, 2003.

[14] Jiří Sgall. Solution of david gale's lion and man problem. *Theoretical Computer Science*, 259(1):663–670, 2001.

[15] Joshua Vander Hook and Volkan Isler. Pursuit and evasion with uncertain bearing measurements. In *CCCG*, 2014.