2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Pure Pursuit Strategy Enhanced with Defense Margin under Noisy Measurements for Protective Drone Missions

Minjun Sung, Christophe J. Hiltebrandt-McIntosh, Hunmin Kim, and Naira Hovakimyan

***Abstract*— This paper investigates the problem of protecting a *safe zone* against rogue drone intrusion when the defender has noisy observations. The conventional strategies were not sufficient to achieve high mission success rates, prompting the introduction of a concept called defense margin. The proposed strategy improves upon the Pure Pursuit (PP) strategy by incorporating the defense margin strategy, offering better performance compared to using either strategy alone. Simulation results demonstrate the effectiveness of the proposed strategy, resulting in higher mission success rates.**

I. Introduction

With the rapid growth of the drone market, incidents and concerns involving malicious drones have risen. These incidents range from flight disruptions to privacy violations and terror attacks [1], [2]. The need for measures to protect property and assets from unauthorized aerial intrusions has become increasingly important.

Jamming with Electromagnetic Pulse (EMP) is a widely studied method for neutralizing drones [3]. However, the use of EMPs can cause unintended harm to electronics and communication, leading to restrictions on their use at the consumer level in many countries. Physical interception using aerial capturing measures, such as net guns and birds, is, therefore, the preferred method of neutralization [4]. Of these methods, deploying a defender drone using a net gun is considered a scalable option due to its reliability and safety.

Guarding a safe zone against invasive drones is a challenging problem, especially considering the noise present in the measurements of the flying vehicles [5]. The defender faces a difficult decision between improving observation accuracy and interception by approaching the attacker or maintaining the security of the safe zone. This dilemma poses a challenge for the defender, making it tricky to protect the safe zone.

A. Related works

A protective mission against a rogue drone is a variant of the Pursuit-Evasion game in which the evader tries to enter the safe zone while avoiding interception by the pursuer [6]. Given the initial positions of both agents, the barrier curves that mark off the dominant regions of the defender and attacker can be found, which determines the outcome of the game. Then, a minimax optimization problem is formulated as in [7] (and references therein) to derive an optimal strategy for each agent via the Hamilton-Jacobi-Bellman-Isaacs (HJI) equation. This problem has been extended to multi-agent scenarios [8], [9].

In a typical Pursuit-Evasion game setup, the defender attempts to minimize the time to capture the evader. When the state of the attacker is known in the Euclidean space, the optimal strategy for the defender is given by a straight line which can be obtained by solving the HJI equation, assuming a smooth value function designed based on the distance to the evader [10]. Since the strategy is optimal, the game is guaranteed to become more favorable to the defender if the attacker deviates from its optimal behavior. Our work departs from the conventional problem setting by addressing a more practical scenario, where the attacker's state measurement is noisy, and its behavioral model is unknown. Additionally, our problem setting amplifies measurement noise with distance [5], presenting the defender with an added complication: it must approach closer to the attacker to obtain more precise observations, while not deviating too far away from the safe zone. This formulation deviates from the differential game approach, by instead focusing on balancing the possibly countering objectives of pursuing and defending under the presence of uncertainty.

A mission to track and defend a drone also resembles the close-in jamming problem introduced in [11]. This work addresses the problem of jamming a rogue drone with observational uncertainty. However, this work differs from ours in that it assumes only a limited number of possible control actions for agents and mainly focuses on controlling the jamming intensity instead of a protective mission.

B. Statement of Contributions

We propose a method to address the dilemma faced by the defender in the protective mission when observing the attacker subject to noise. Our main contributions are:

1) Novel problem formulation of a protective mission assuming a noisy observation and unknown strategy of the attacker;
2) Providing a metric that can be computed in a closed form to quantify defense performance for a protective mission in the presence of uncertainty;
3) Designing an adaptive defense strategy and proving its efficacy analytically and empirically.

C. Notations

We use $\|\cdot\|$ to represent the Euclidean norm and $\mathbb{E}[\cdot]$ to denote the expectation of a random variable. In Section III-B,

This work was supported by the NSF (CNS-1932529), NASA (NNH20ZEA001N-ULI, NNH21ZEA001N-USRC), and AFOSR.

Minjun Sung, Christophe J. Hiltebrandt-McIntosh, and Naira Hovakimyan are with the Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign, USA. {mjsung2, cjh11, nhovakim}@illinois.edu

Hunmin Kim is with the Department of Electrical and Computer Engineering, Mercer University, USA. kim_h@mercer.edu

we employ $\overline{z_a z_b}$ to indicate the line segment connecting the endpoints of vectors z_a and z_b. Finally, $z_a \perp z_b$ and $z_a \parallel z_b$ respectively denote perpendicular and parallel vectors.

II. Problem formulation

We investigate the task of protecting a designated safe zone using a single defending drone, referred to as the *defender*, against a single attacking drone, referred to as the *attacker*[1]. We focus on devising a defender strategy that can effectively counter an attacker with an unknown strategy and noisy observation. We present a fundamental framework for a one-on-one defender-attacker scenario, which can be directly extended to multi-agent scenarios as done in [12], [13].

A. State-space representation

The mission takes place in $\mathbb{R}^2$ space, where the zone of interest, denoted as $\Omega_I \subset \mathbb{R}^2$, defines the area where the observation of a drone is deemed to have a rogue intent. The safe zone, denoted as $\Omega_S \subset \Omega_I$, encompasses the area that the defender aims to protect. We approximate Ω_I and Ω_S with their respective minimal circular hulls, with radii R_{Ω_I} and R_{Ω_S} centered at the origin $\mathcal{O}$.

The attacker and the defender configurations at time t are expressed as $x_t^j \in \mathbb{R}^2$ for $j \in \{a, d\}$. The discrete-time dynamics of the attacker and the defender can be written as:

$$x_{t+1}^j = x_t^j + u_t^j, \quad j \in \{a, d\}.$$

Here $u_t^j \in \mathbb{U}_t^j \subset \mathbb{R}^2$ for $j \in \{a, d\}$ is the deterministic control input of each agent, and u_t^a is unknown to the defender at all times. Moreover, $\mathbb{U}_t^a$ and $\mathbb{U}_t^d$ denote a set of admissible controls of the attacker and the defender at time t. This is a commonly used discretized single integrator model in PE games [7]–[9], which differs from the more restrictive double-integrator dynamics assumption [14].

In this paper, we assume $\|u_t^a\| \leq \|u_t^d\| = 1$ for all t, such that the control input is normalized. This implies that an attacker can be as fast as a defender, which is a relaxed assumption compared to many other works that assume the defender to strictly outpace the attacker [15], [16].

The attacker is considered to be *intercepted* by the defender if the distance $\|e_t\| \triangleq \|x_t^a - x_t^d\|$ is less than the maximum capturing distance τ. Technically, the attacker is intercepted if $\|e_t\| \leq \tau$. The maximum capturing distance is determined by the net gun specifications.

B. Attacker detection model

When dealing with a noisy target, different models have been proposed, such as the Brownian motion model [17] and the ellipsoid model [18]. In this work, we adopt the uncertainty model from [19], where we assume to receive independent and noisy state observations of the attacker at each time step. Since we have no information about the attacker's behavioral model, commonly used filtering methods, such as the Kalman filter and its variations [20], cannot be employed to reduce the variance of the noise.

An observation of x_t^a at time t is denoted as $y_t \in \mathbb{R}^2$, and is subject to a zero-mean Gaussian noise with covariance matrix $\sigma_t^2 I_2$ as in [11], where $\sigma_t^2 \in \mathbb{R}_{\geq 0}$ represents a variance of a Gaussian distribution, and $I_2 \in \mathbb{R}^{2\times 2}$ represents an identity matrix. Formally, the following model is adopted to express the observational uncertainty:

$$\begin{aligned} y_t &= x_t^a + w_t \\ w_t &\sim \mathcal{N}(0, \sigma_t^2 I_2). \end{aligned} \tag{1}$$

Furthermore, σ_t is modeled by adopting the uncertainty model proposed in [19]:

$$\sigma_t^2 = \beta_b + \beta_d \|e_t\|^2 + \beta_v (1 - \nu_t).$$

Parameters $\beta_b, \beta_d, \beta_v$ are non-negative real values characterized by the sensor and the estimation model. Specifically, they represent the variance coefficient for baseline, distance, and visibility, respectively. Visibility $\nu_t \in [0, 1]$ relates the blockage of the sight to the variance of the uncertainty, such that $\nu_t = 0$ if the sight is fully blocked by an obstacle, and $\nu_t = 1$ if the sight is not blocked at all. Any values in-between represent partial blockage of the sight.

In this paper, we will consider an environment without any obstacles such that $\nu_t \equiv 1$, and zero baseline variance $\beta_b = 0$. Then, we can rewrite (1) as

$$\begin{aligned} y_t &= x_t^a + w_t \\ w_t &\sim \mathcal{N}(0, \beta \|e_t\|^2 I_2), \end{aligned} \tag{2}$$

where β is a short hand notation for β_d.

C. Joint defense and tracking problem

Formally, the defender's mission is to prevent the attacker from landing at the safe zone Ω_S for all time *or* to intercept the attacker before it reaches the safe zone. Specifically, the problem is to find a sequence of discrete control inputs u_t^d for all t such that it satisfies

$$\begin{aligned} x_t^a \notin \Omega_S \; \forall t \in [t_i, t_f] \text{ or} \\ \exists t_c \in [t_i, t_f] : (x_t^a \notin \Omega_S \; \forall t \in [t_i, t_c]) \wedge (\|e_{t_c}\| \leq \tau), \end{aligned} \tag{3}$$

subject to

$$\begin{aligned} & x_{t+1}^j = x_t^j + u_t^j, \quad j \in \{a, d\} \\ & \|u_t^a\| \leq \|u_t^d\| = 1 \quad \forall t \in [t_i, t_f] \\ & y_t = x_t^a + w_t \\ & w_t \sim \mathcal{N}(0, \beta \|e_t\|^2 I_2), \end{aligned} \tag{4}$$

where t_i, t_f, t_c respectively denote the initial time of observation, terminal time that can be chosen by the user, and the capturing time. Note that this problem is not limited to the interception problem, but extends to a more general class of a defense problem in which the defender can win by protecting the safe zone for a sufficiently long *runtime*.

[1]Defender and attacker are analogous to the pursuer and evader in the Pursuit-Evasion game setup. We intentionally used a distinct term to emphasize the different objectives of our problem setup.

III. METHOD

We propose a solution that enhances the PP strategy with the Defense Margin (DM) strategy to solve our problem. In Section III-A, we introduce and discuss the advantages and limitations of the PP strategy, along with other popular guidance laws. In Section III-B, we evaluate the DM strategy and its ability to complement the PP strategy. Finally, in Section III-C, we present our proposed Adaptive Defense Margin (ADM) strategy.

A. Pure Pursuit strategy

Popular strategies utilized in PE games are Constant Bearing (CB), Line of Sight (LoS), and PP guidance laws [21]. Having only access to the instantaneous positional estimate of the attacker, the PP strategy is a reasonable strategy to be considered among the above three. CB is not a suitable strategy because it assumes the knowledge of the attacker's instantaneous velocity as well as its position [22], whereas the defender only has access to the noisy observation of the attacker in our problem. On the other hand, LoS is known to be infeasible in missions with observational uncertainty unless there are external or additional measures to complement the noisy observation [23].

The idea of the PP strategy is to always steer the defender directly to the observation of the attacker (3). Formally, the defender's control input is designed by

$$u_t^d = \frac{y_t - x_t^d}{\|y_t - x_t^d\|}, \tag{5}$$

where u_t^d is normalized to meet the constraint (4).

In this work, we analyze the conditions under which the PP strategy is effective and determine when it becomes less reliable under uncertainty. The following definitions and theorems provide the necessary background to describe these conditions analytically.

Definition 1. *Consider the n-dimensional stochastic discrete-time system*

$$\zeta_{t+1} = f(\zeta_t, \chi_t, \chi), \quad \zeta(t_0) = \zeta_0. \tag{6}$$

The trivial solution of the system is said to be stochastically stable or stable in probability, if $\forall \epsilon, h > 0$, $\exists \delta = \delta(\epsilon, h, t_0) > 0$ *such that* $P\{|\zeta_t| < h\} \geq 1 - \epsilon$ *for* $t \geq t_0$ *when* $|\zeta_0| < \delta$. *Otherwise, it is stochastically unstable [24].*

Consider the Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}$, with $V(0) = 0$. Its discrete increment is expressed as follows:

$$\Delta V(\zeta_t) = V(\zeta_{t+1}) - V(\zeta_t). \tag{7}$$

Using this definition and discrete-time Lyapunov functions and their increments, the following theorems can be stated.

Theorem III.1. *If there exists a positive definite function* $V(\zeta_t) \in C^2(D_r)$, *such that*

$$E[\Delta V(\zeta_t)] \leq 0 \tag{8}$$

for all $\zeta_t \in D_r$, *then the trivial solution of* (6) *is stochastically stable in probability [24].*

In the following, we present the condition that ensures interception when using the PP strategy.

Theorem III.2. *Assume* $\|e_t\| > \sqrt{2}$ *and* $\|w_t\| < \|e_t\|$. *The error* e_t *is stochastically stable under the PP strategy* (5)*, if the following condition holds:*

$$\frac{e_t^\top u_t^a + 1}{\|e_t + u_t^a\|} \leq \mathbb{E}[\cos\alpha], \tag{9}$$

where

$$\cos\alpha \triangleq \frac{(e_t + w_t)^\top (e_t + u_t^a)}{\|e_t + w_t\| \, \|e_t + u_t^a\|}, \; \alpha \in (-\frac{\pi}{2}, \frac{\pi}{2}).$$

Proof. We use the Lyapunov function to provide a condition under which stability can be guaranteed.

Define a Lyapunov function $V(e_t)$ as

$$V(e_t) = e_t^\top e_t. \tag{10}$$

Plugging the uncertain observation model (2) into the PP control (5) yields

$$u_t^d = \frac{y_t - x_t^d}{\|y_t - x_t^d\|} = \frac{e_t + w_t}{\|e_t + w_t\|} \tag{11}$$

Plugging (11) into (7) and rearranging it yields

$$\begin{aligned}\Delta V(e_t) &= V(e_{t+1}) - V(e_t) \\ &= -2\frac{e_t^\top (e_t + w_t)}{\|e_t + w_t\|} + 2e_t^\top u_t^a + \frac{(e_t + w_t)^\top (e_t + w_t)}{\|e_t + w_t\|^2} \\ &\quad + u_t^{a\top} u_t^a - 2\frac{(e_t + w_t)^\top u_t^a}{\|e_t + w_t\|}\end{aligned}$$

Rearranging and taking expectation on both sides with $\|u_t^a\| \leq 1$, $\|e_t\| > \sqrt{2}$ and $\|w_t\| < \|e_t\|$ yields

$$\mathbb{E}[\Delta V(e_t)] \leq -2\|e_t + u_t^a\|\mathbb{E}[\cos\alpha] + 2e_t^\top u_t^a + 2.$$

Rearrange this to satisfy (8), and we obtain (9). □

Remark 1. *In practice, an actual capturing distance would ensure the fulfillment of the normalized constraint,* $\tau > \sqrt{2}$, *considering the update rate and speed limit of a vehicle [25].*

The theorem states that the PP strategy leads to an interception in expectation when the uncertainty w_t is small and the attacker is heading towards the defender. Therefore, to make effective use of the PP strategy, the defender should pursue a complementary strategy until it is close enough to the attacker and is positioned between the safe zone and the attacker, so the attacker cannot steer away from the defender and simultaneously advance toward the safe zone.

B. Defense Margin Strategy

Definition 2. *The safe reachable set* $L_{x_t^a}$ *is the set of positions reachable by the attacker before the defender [18].*

Following the assumption in (4) that the defender is equivalently fast as the attacker, we can express $L_{x_t^a}$ as $L_{x_t^a} = \{l \in \mathbb{R}^2 | \; \|l - x_t^a\| \leq \|l - x_t^d\|\}$.

We subsequently define $l_{x_t^a} \in L_{x_t^a}$ as the closest point in the reachable set to the safe zone: $l_{x_t^a} = \arg\inf_{l \in L_{x_t^a}} \|\Omega_S - l\|$, where $\|\Omega_S - l\| \triangleq \inf_{\omega_S \in \Omega_S} \|\omega_S - l\|$, for a given l. We

can follow the same notations to represent the estimation of $L_{x_t^a}$ and $l_{x_t^a}$ as L_{y_t} and l_{y_t}, respectively.

Definition 3. *Defense margin $\rho_{x_t^a}$ is the norm of $l_{x_t^a}$:*

$$\rho_{x_t^a} = \|l_{x_t^a}\|.$$

Note that if $\rho_{x_t^a} \leq R_{\Omega_S}$, there exists a strategy for the attacker to win regardless of the defender's strategy.

We define the *defense margin strategy (DM strategy)* as

$$u_t^d = \frac{l_y - x_t^d}{\|l_y - x_t^d\|}. \tag{12}$$

Note that the strategy is defined with respect to l_{y_t} instead of x_t^a. Intuitively, this strategy implicitly attempts to accomplish the first goal of (3) by forcing the attacker to take a detour to reach the safe zone. Technically, the probability of reducing an actual defense margin is optimal, due to the certainty equivalence of the model (2).

Lemma III.3. *The defense margin $\rho_{x_t^a}$ can be measured as:*

$$\rho_{x_t^a} = \frac{1}{2}\frac{\|x_t^a\|^2 - \|x_t^d\|^2}{\|x_t^a - x_t^d\|}.$$

Proof. By construction, $(\frac{x_t^d + x_t^a}{2}) \cdot (x_t^a - x_t^d) = l_{x_t^a} \cdot (x_t^a - x_t^d)$. Rearranging for $\|l_{x_t^a}\|$ yields the result. □

Next, we provide an analytical proof to explain that (12) outperforms (5) in terms of $\rho_{x_t^a}$, implying that the DM strategy can provide the defensive property whereas the PP strategy provides the interception property.

Theorem III.4. *Assume $\|e(t)\| > \sqrt{2}$ and $\|x_t^a\| > \|x_t^d\|$. For static attacker state vector $x_{t+1}^a = x_t^a$ with uncertainty $w_t = 0 \quad \forall t$, the following inequality holds for one step change of the defense margin:*

$$\Delta\rho_{x_t^a}|u_{DM}^d \geq \Delta\rho_{x_t^a}|u_{PP}^d, \tag{13}$$

where $\Delta\rho_{x_t^a}|u_{DM}^d$ and $\Delta\rho_{x_t^a}|u_{PP}^d$ respectively denote $\rho_{x_{t+1}^a} - \rho_{x_t^a}$ following (12) *and* (5)*.*

Proof. **Step 1) Coordinate Transformation** At time t, given x_t^a and x_t^d, we do a *rigid* coordinate transformation $\Phi : x \to \hat{x}$ such that $x_t^d \to \hat{x}_t^d = [0,0]^\top$, $x_t^a \to \hat{x}_t^a = [r,0]^\top$, where $r = \|e(t)\|$ and the center of the safe zone Ω_S will correspondingly be transformed to $[p,q]^\top$. The assumption $\|x_t^a\| > \|x_t^d\|$ is translated to $p < \frac{r}{2}$ in these coordinates.

Rigid transformation only allows rotation and is followed by translation, and therefore preserves the Euclidean distance between every pair of points. In these transformed coordinates, the two strategies are simplified as $u_{PP}^d = [1,0]^\top$, and $u_{DM}^d = [\cos\psi, \sin\psi]^\top$. Subsequently, $x_{t+1}^d = [1,0]^\top$ for PP strategy, and $x_{t+1}^d = [\cos\psi, \sin\psi]^\top$ for DM strategy.

Now $\rho_{\hat{x}_t^a}$ lies precisely on the perpendicular bisector of the line segment $\overline{\hat{x}_t^a \hat{x}_t^d}$. Consequently, $\angle\rho_{\hat{x}_t^a}\hat{x}_t^d\hat{x}_t^a = \angle\rho_{\hat{x}_t^a}\hat{x}_t^a\hat{x}_t^d = \psi$, where $\psi \in (-\frac{\pi}{2}, \frac{\pi}{2})$. Formally, $p = \frac{r}{2} - \rho_{\hat{x}_t^a} < \frac{r}{2}$ and $q = \frac{r}{2}\tan\psi$.

Step 2) Change in Defense Margin for PP strategy

For $x_{t+1}^d = [1,0]^\top$, we have $\rho_{\hat{x}_{t+1}^a} = \frac{r+1}{2} - p$. Thus,

$$\begin{aligned}\Delta\rho_{\hat{x}_t^a}|u_{PP}^d &= \rho_{\hat{x}_{t+1}^a} - \rho_{\hat{x}_t^a} \\ &= (\frac{r+1}{2} - p) - (\frac{r}{2} - p) = \frac{1}{2}.\end{aligned}$$

Step 3) Change in Defense Margin

Similarly, we have the line that bisects $\hat{x}_{t+1}^d$ and $[r,0]^\top$:

$$\frac{r - \cos\psi}{\sin\psi}(x - \frac{r + \cos\psi}{2}) - (y - \frac{\sin\psi}{2}) = 0.$$

Consequently, we have

$$\rho_{\hat{x}_{t+1}^a}|u_{DM}^d = \frac{|r^2 - 1 + 2q\sin\psi - 2p(r - \cos\psi)|}{2\sqrt{(r - \cos\psi)^2 + \sin^2\psi}}. \tag{14}$$

Here we will find the lower bound of $\rho_{\hat{x}_{t+1}^a}|u_{DM}^d$ and assert that it is greater or equal to $\frac{1}{2}$ to complete our proof.

First observe that we only need to consider for $\psi \in [0, \frac{\pi}{2})$, since $\rho_{\hat{x}_{t+1}^a}$ is symmetrical with respect to $\hat{x}$-axis. Every result we obtain can therefore be identically proved for $\psi \in (-\frac{\pi}{2}, 0]$. Subsequently, $q \geq 0$. Note that $q = 0$ or $\psi = 0$ is a trivial case which yields $u_{PP}^d \equiv u_{DM}^d$.

The numerator of (14) can be lower-bounded by the following:

$$\begin{aligned}r^2 - 1 + 2q\sin\psi - 2p(r - \cos\psi) \\ > r^2 - 1 + 2q\sin\psi - 2p(r - \cos\psi)|_{p=\frac{r}{2}} \\ = -1 + \frac{r}{\cos\psi} > 0 \quad \forall\psi \in [0, \frac{\pi}{2}).\end{aligned}$$

Here we used $\psi \in [0, \frac{\pi}{2})$, $r > \sqrt{2}$, $q = \tan\psi$, and $p < \frac{r}{2}$. Hence, we can ignore the absolute operator for the remainder of the proof.

Then, we have

$$\begin{aligned}\rho_{\hat{x}_{t+1}^a}|u_{DM}^d &> \frac{r^2 - 1 + 2q\sin\psi - r(r - \cos\psi)}{2\sqrt{(r - \cos\psi)^2 + \sin^2\psi}} \\ &= \frac{r - \cos\psi}{2\cos\psi\sqrt{(r - \cos\psi)^2 + \sin^2\psi}}.\end{aligned}$$

Here, the last equality again used $p < \frac{r}{2}$ and $q = \frac{r}{2}\tan\psi$. Furthermore,

$$\frac{r - \cos\psi}{2\cos\psi\sqrt{(r - \cos\psi)^2 + \sin^2\psi}} \geq \frac{1}{2}$$

holds whenever $r > \sqrt{2}$. Note that equality holds only when $\psi = 0$. Due to the rigidity of the transformation $\Phi(x,y)$, we can obtain $\rho_{x_{t+1}^a}|u_{DM}^d \geq \rho_{x_{t+1}^a}|u_{PP}^d$ directly from $\rho_{\hat{x}_{t+1}^a}|u_{DM}^d \geq \rho_{\hat{x}_{t+1}^a}|u_{PP}^d$. □

The DM strategy outperforms the PP strategy in terms of the actual defense margin when no uncertainty is present, as demonstrated by this theorem. The property under noisy conditions is empirically verified via neural network analysis in Section IV. It should be noted here that the defense margin may not always be non-decreasing under the presence of uncertain observations. Numerous cases, as demonstrated in

Section IV, highlight that the DM strategy fails to defend against an *intelligent* attacker due to its passivity and lack of interception attempts.

C. Adaptive Defense Margin Strategy

We discussed the limitations of using the PP and the DM strategy in Sections III-A and III-B. We next introduce an adaptive convex combination of both to solve our problem.

We introduce a weight parameter λ_t and define the *Adaptive Defense Margin (ADM) strategy* as follows:

$$u_t^d = c\lambda_t \frac{y - x_t^d}{\|y - x_t^d\|} + c(1-\lambda_t)\frac{l_\mu - x_t^d}{\|l_\mu - x_t^d\|}, \qquad (15)$$

where c is a normalizing constant that makes $\|u_t^d\| = 1$. Note that $\lambda_t \equiv 1$, and $\lambda_t \equiv 0$ restores the PP and the DM strategy.

The intuition is to follow the DM strategy until it gets to a favorable position to apply the PP strategy. The problem is to construct adequate λ_t that effectively balances DM and PP strategy in the evolving dynamics of the mission. We first define the reliability of an observation y_t, which we can measure without precise knowledge of x_t^a.

Definition 4. *Let $\hat{w}_t$ be an estimate of the uncertainty w_t, expressed as $\hat{w}_t \sim \mathcal{N}(0, \beta(\|y_t - x_t^d\|^2 I_2)$. The reliability of the observation y_t is denoted as P_t and is expressed as $P_t = F(k,k) + F(-k,-k) - F(-k,k) - F(k,-k)$. Here $F(\cdot,\cdot) : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ is the cumulative distribution function (CDF) of a multivariate Gaussian distribution $\hat{w}_t$, and k is the characterizing length of the reliability square.*

We propose the parameterization $\lambda_t = P_t$, which considers the reliability of each observation. Rewriting (15), we obtain

$$u_t^d = cP_t \frac{y - x_t^d}{\|y - x_t^d\|} + c(1-P_t)\frac{l_\mu - x_t^d}{\|l_\mu - x_t^d\|}. \qquad (16)$$

This strategy transitions from the PP approach as the attacker approaches the safe zone, shifting towards the DM method to prepare for worst-case scenarios when the attacker is further away. This continuous transition is governed by a reliability parameter that allows the defender to balance the risk of deviation from the safe zone with the need for accurate observations to optimize interception.

IV. Simulation and Results

Here we evaluate the effectiveness of three defense strategies (PP, DM, and ADM) against three attacker strategies: Linear, Spiral, and Intelligent. While the Linear and Spiral strategies follow pre-defined straight and curved paths, the Intelligent attacker mirrors the ADM strategy:

$$u_t^a = \frac{\xi d_1 + d_2}{\|\xi d_1 + d_2\|}, \quad d_1 = -(\hat{x}_t^d - x^a), \quad d_2 = -x_t^a,$$

where ξ is a tuning parameter. In all scenarios we fixed $\|u_t^a\| = 1$ for all t. Figure 1 provides a visual representation of the trajectories followed by the attackers under each behavior. The simulation parameters used in this work are: $t_f = \infty$, $R_{\Omega_I} = 50$, $R_{\Omega_S} = 10$, $\tau = 2$, $x_{t_i}^d \sim [\mathcal{U}[0,20], \mathcal{U}[-\pi,\pi]]^\top$, $x_{t_i}^a \sim [\mathcal{U}[45,50], \mathcal{U}[-\pi,\pi]]^\top$, $\beta = 0.05$, $\xi = 2$, and $k = 0.5$, where $\mathcal{U}[c_1, c_2]$ denotes a uniform distribution with support on the interval $[c_1, c_2]$.

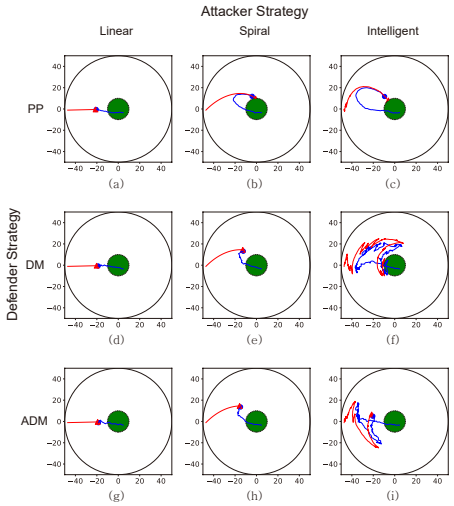

Fig. 1. This figure shows the trajectories of the attacker and defender under different behavior scenarios. The outer circle represents Ω_I, and the green circle represents Ω_S. Red and blue lines represent the attacker x_t^a and defender x_t^d trajectories, respectively, over time. Homogeneous initial positions of the attacker and defender are assumed. The defender successfully defends the safe zone in all cases except for (b), (c), and (f).

Figure 1 shows that the PP guidance law is ineffective in defending the safe zone against spiral (b) and intelligent (c) attacker behavior. The DM strategy also proved ineffective against an intelligent attacker (f), as demonstrated by a scenario in which the defense margin steadily decreases due to the lack of interception attempts. However, the ADM strategy successfully defended against all types of attackers.

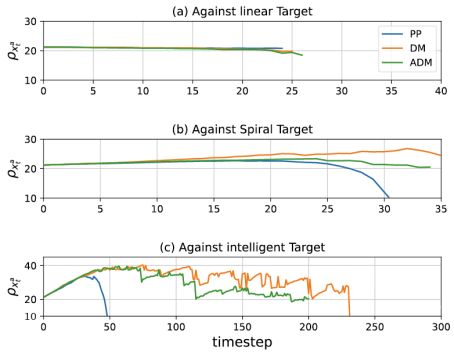

Fig. 2. Defense margin as a function of a timestep. The mission is considered to have failed if $\rho_{x_t^a} = R_{\Omega_S} = 10$. Trajectories that ended before failing imply that the defender has intercepted the attacker.

We can also interpret the results using $\rho_{x_t^a}$. The cases (b), (c), and (f) of Figure 1 for which the defender fails to defend the safe zone can be clearly observed in Figure 2. Noticeably for Figure 2 (b) and (c), $\Delta\rho_{x_t^a}|u_{DM}^d \geq \Delta\rho_{x_t^a}|u_{PP}^d$ as in (13). The failure in Figure 2 (c) can be attributed to the passive nature of the strategy. Concretely, the defender avoids taking proactive measures to intercept the attacker and instead retreats until the attacker enters the capturing radius.

Figure 3 depicts the defense performance from 1,000 trials for each scenario. As the attacker behavior complexity

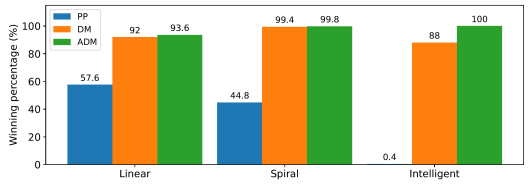

Fig. 3. Winning percentage of each strategy against different attacker strategies. Each percentage result is obtained by counting successful missions out of 1,000 randomly initialized scenarios.

increases, the PP strategy's performance declines, while the ADM strategy performs better. Some of the failure cases of the ADM strategy against non-intelligent attackers can be explained by the randomness of the initial conditions [7].

We extend Theorem III.4 by using a Neural Network to approximate $\Delta\rho_{x_t^a}$ and relaxing the assumption of the absence of uncertainty. We then analyze the results obtained.

Definition 5. *Assume* $u_t^a = -\frac{x_t^a}{\|x_t^a\|}$. *A strategy* u_A^d *is said to be safer than strategy* u_B^d *with respect to the noise* $w_t \sim \mathcal{N}(0, \beta\|e_t\|^2 I_2)$ *defined in* (2)*, if* $\Delta(\rho_{x_t^a})|_{u_A^d} \geq \Delta(\rho_{x_t^a})|_{u_B^d}$*, where* u_A^d *and* u_B^d *rely on uncertain observation of* x_t^a.

We trained two fully connected neural networks, $\Delta\rho_{\hat{x}_t^a}|u_{PP}^d$ and $\Delta\rho_{\hat{x}_t^a}|u_{DM}^d$, using training data collected from simulations of linear attacker behavior to obtain Figure 3. The networks take (x_t^a, x_t^d) as inputs and return predictions of $\Delta\rho_{x_t^a}|u_{PP}^d$ and $\Delta\rho_{x_t^a}|u_{DM}^d$, respectively. We used a two-layer neural network with 100 nodes in each layer, an Adam optimizer, and a learning rate of 0.001. To test the models, we randomly generated 100,000 test data samples (x_q^a, x_q^d) uniformly sampled from the same distribution of the training dataset. The result shows that

$$\Delta\rho_{x_t^a}|u_{PP}^d = -0.132 < \Delta\rho_{x_t^a}|u_{DM}^d = -0.028,$$

confirming that the DM strategy outperforms the PP strategy in terms of defense margin even in the presence of uncertainty w_t. Moreover, this result also highlights the possibility of the defense margin shrinking in some conditions, indicating the importance of having an adaptive defense strategy.

V. Conclusion

This work proposes a defense strategy for protective missions in the presence of uncertain measurements. The proposed strategy combines the PP and DM strategies based on the reliability of the observations, which is inversely correlated to the distance from the attacker. Analytical proof and empirical demonstration are provided.

Future research may expand upon the proposed methodology by integrating obstacle-present environments and investigating its implications against a variety of attacker behaviors. Additionally, conducting a more in-depth analysis including multi-agent scenarios can be analyzed.

References

[1] J. Loeb, "Exclusive: Anti-drone technology to be tested in UK amid terror fears," *Engineering & Technology*, vol. 12, no. 3, p. 9, 2017.

[2] A. Singh, D. Patil, and S. Omkar, "Eye in the sky: Real-time drone surveillance system (DSS) for violent individuals identification using ScatterNet Hybrid Deep Learning network," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1629–1637, 2018.

[3] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, 2018.

[4] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on anti-drone systems: Components, designs, and challenges," *IEEE Access*, vol. 9, pp. 42 635–42 659, 2021.

[5] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-art in research," *IEEE Access*, vol. 7, pp. 138 669–138 682, 2019.

[6] R. Isaacs, "Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization," 1999.

[7] Y. Lee and E. Bakolas, "Optimal strategies for guarding a compact and convex target set: A differential game approach," *IEEE Conference on Decision and Control*, pp. 4320–4325, 2021.

[8] H. Fu and H. H.-T. Liu, "Guarding a territory against an intelligent intruder: Strategy design and experimental verification," *IEEE/ASME Transactions on Mechatronics*, vol. 25, no. 4, pp. 1765–1772, 2020.

[9] E. Garcia, D. W. Casbeer, and M. Pachter, "Optimal strategies for a class of multi-player reach-avoid differential games in 3d space," *IEEE Robotics and Automation Letters*, vol. 5, no. 3, pp. 4257–4264, 2020.

[10] E. Garcia, Z. E. Fuchs, D. Milutinovic, D. W. Casbeer, and M. Pachter, "A geometric approach for the cooperative two-pursuer one-evader differential game," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 15 209–15 214, 2017.

[11] P. Valianti, S. Papaioannou, P. Kolios, and G. Ellinas, "Multi-agent coordinated close-in jamming for disabling a rogue drone," *IEEE Transactions on Mobile Computing*, 2021.

[12] A. Pierson, Z. Wang, and M. Schwager, "Intercepting rogue robots: An algorithm for capturing multiple evaders with multiple pursuers," *IEEE Robotics and Automation Letters*, vol. 2, no. 2, pp. 530–537, 2016.

[13] Z. E. Fuchs, P. P. Khargonekar, and J. Evers, "Cooperative defense within a single-pursuer, two-evader pursuit evasion differential game," *IEEE Conference on Decision and Control*, pp. 3091–3097, 2010.

[14] M. Coon and D. Panagou, "Control strategies for multiplayer target-attacker-defender differential games with double integrator dynamics," *IEEE Conference on Decision and Control*, pp. 1496–1502, 2017.

[15] V. R. Makkapati and P. Tsiotras, "Optimal evading strategies and task allocation in multi-player pursuit–evasion problems," *Dynamic Games and Applications*, vol. 9, no. 4, pp. 1168–1187, 2019.

[16] A. Von Moll, M. Pachter, E. Garcia, D. Casbeer, and D. Milutinović, "Robust policies for a multiple-pursuer single-evader differential game," *Dynamic Games and Applications*, vol. 10, no. 1, pp. 202–221, 2020.

[17] O. Basimanebotlhe and X. Xue, "Stochastic optimal control to a nonlinear differential game," *Advances in Difference Equations*, vol. 2014, no. 1, pp. 1–14, 2014.

[18] K. Shah and M. Schwager, "Multi-agent cooperative pursuit-evasion strategies under uncertainty," *Distributed Autonomous Robotic Systems*, pp. 451–468, 2019.

[19] B. Davis, I. Karamouzas, and S. J. Guy, "C-opt: Coverage-aware trajectory optimization under uncertainty," *IEEE Robotics and Automation Letters*, vol. 1, no. 2, pp. 1020–1027, 2016.

[20] F. Daum, "Nonlinear filters: beyond the kalman filter," *IEEE Aerospace and Electronic Systems Magazine*, vol. 20, no. 8, pp. 57–69, 2005.

[21] M. Breivik and T. I. Fossen, "Guidance laws for planar motion control," *IEEE Conference on Decision and Control*, pp. 570–577, 2008.

[22] V. R. Makkapati, W. Sun, and P. Tsiotras, "Pursuit-evasion problems involving two pursuers and one evader," *2018 AIAA Guidance, Navigation, and Control Conference*, p. 2107, 2018.

[23] A. Ratnoo and T. Shima, "Line-of-sight interceptor guidance for defending an aircraft," *Journal of Guidance, Control, and Dynamics*, vol. 34, no. 2, pp. 522–532, 2011.

[24] Y. Li, W. Zhang, and X. Liu, "Stability of nonlinear stochastic discrete-time systems," *Journal of Applied Mathematics*, vol. 2013, 2013.

[25] H. Yang, Y. Lee, S.-Y. Jeon, and D. Lee, "Multi-rotor drone tutorial: systems, mechanics, control and state estimation," *Intelligent Service Robotics*, vol. 10, pp. 79–93, 2017.