Vision-based Perimeter Defense via Multiview Pose Estimation

Elijah S. Lee\textsuperscript{1}, Giuseppe Loianno\textsuperscript{2}, Dinesh Jayaraman\textsuperscript{1}, and Vijay Kumar\textsuperscript{1}

\textbf{Abstract}—Previous studies in the perimeter defense game have largely focused on the fully observable setting where the true player states are known to all players. However, this is unrealistic for practical implementation since defenders may have to perceive the intruders and estimate their states. In this work, we study the perimeter defense game in a photo-realistic simulator and the real world, requiring defenders to estimate intruder states from vision. We train a deep machine learning-based system for intruder pose detection with domain randomization that aggregates multiple views to reduce state estimation errors and adapt the defensive strategy to account for this. We newly introduce performance metrics to evaluate the vision-based perimeter defense. Through extensive experiments, we show that our approach improves state estimation, and eventually, perimeter defense performance in both 1-defender-vs-1-intruder games, and 2-defenders-vs-1-intruder games.

\section{I. INTRODUCTION}

In a perimeter defense game, defenders aim to intercept intruders by moving along the perimeter while intruders try to reach the perimeter without being captured by defenders \cite{1}. As shown in Fig. 1, we study Unmanned Aerial Vehicles (UAVs) equipped with cameras as defenders. A dynamic defender aims to capture an intruder based on its perception while a static defender enables multiview perception. Vision-based UAVs have been well studied in various settings such as power plant \cite{2}, penstock \cite{3}, forest \cite{4}, or disaster sites \cite{5}, and all these settings can be real-world use-cases for perimeter defense; for instance, an intruder tries to attack a military base in the forest and a defender aims to capture the intruder.

In large, there are three modules in end-to-end perimeter defense: perception, planning, and control. In this work, the planning module is theoretically derived from our previous work \cite{6} that the defenders aim to move to the optimal breaching point to maximize their probability to win the game. Since the optimality of the game is given as a Nash equilibrium, we executed the controller to follow the trajectories from the planner.

A number of previous works solve the perimeter defense problem assuming perfect state estimation \cite{6, 7, 8}; however, this is unrealistic for real-world implementations of perimeter defense because defenders may have to perceive the intruders and estimate their states (i.e., positions and velocities) to execute the optimal defense strategies. We newly add a vision-based perception module to predict intruder pose based on domain randomization \cite{9} that runs a lightweight network for scalability.

Our work introduces performance metrics to evaluate the vision-based defense and demonstrates that combining camera views from multiple defenders improves defense performance. In short, our main contributions are:

\begin{itemize}
  \item Realization of vision-based perimeter defense. To the best of our knowledge, we are the first to relax the assumption that all states are known to all players and instead employ vision sensors to acquire necessary state information in a perimeter defense game.
  \item Improvement of perimeter defense algorithm performance by incorporating pose estimation by aggregating multiple views with one dynamic and one static defender.
\end{itemize}

\section{II. RELATED WORK}

\subsection{A. Perimeter defense}

In the perimeter defense game, defenders are tasked to protect a region from intruders. The intruder aims to reach the target without being captured by the defender, while the defender tries to capture the intruder. We refer to \cite{1} for a detailed survey. In particular, a cooperative multiplayer perimeter-defense game is solved on a planar game space in \cite{7}, and Yan et al. \cite{8} solve a reach-avoid differential game in three-dimensional space. Optimal
A. The hemisphere coordinate system

Fig. 2(a) shows the defender $D$, the intruder $A$, and the hemisphere $O$ with radius $R$. The positions of the players in spherical coordinates are: $z_D = [\psi_D, \phi_D, R]$ and $z_A = [\psi_A, 0, R]$, where $\psi$ and $\phi$ are the azimuth and elevation angles, which gives the relative position as: $z = [\psi, \phi, R]$, where $\psi = \psi_A - \psi_D$ and $\phi = \phi_D$. At a given time, the speed of defender and intruder are $v_D$ and $v_A$, respectively, and the ratio is defined as $v = v_A/v_D \leq 1$. Given $z_D$, $z_A$, we call breaching point as a point on the perimeter at which the intruder aims to reach the target, as shown $B$ in Fig. 2(a). It is proved in [6] that given the current positions of $z_D$ and $z_A$, there exists a unique breaching point such that the optimal strategy for both defender and intruder is to move towards it, known as optimal breaching point.

B. Intruder pose

We assume that a camera is mounted on defender to perceive intruder and define the intruder pose as $(u,v,y_c)$, which is a 3-tuple combining $u,v$ intruder position in the image coordinates and $y_c$, which indicates $Y_c$ direction in the camera coordinates (i.e., $y_c = y'^*_c$), as shown in Fig. 2(b). This selection is intuitive in that it is easier to infer the intruder’s center position $u,v$ than to infer $(x'^*_A, y'^*_A, z'^*_A)$ from an image, and the $Y_c$ direction is correlated with the known size of the intruder.

C. Performance metrics

In theory, we assume perfect state estimation without noise, and thus moving towards the optimal breaching point would preserve a Nash equilibrium. However, vision-based perimeter defense may be responsible for uncertainty and noise in estimating intruder pose. Accordingly, we define the performance metrics $\Delta d$ at any time to evaluate the perimeter defense performance as follows:

$$\Delta d = |\overline{DB}| - |AB|$$

(1)

If the intruder wins, it reaches the target before the defender does, and $\Delta d$ indicates the geodesic between the defender $D$ and some breaching point $B$. If the defender wins, it is located at some point on the base plane at the end, and $\Delta d$ indicates the negative value of the distance between $D$ and $A$. In both cases, the defender aims to minimize $\Delta d$ while the intruder aims to maximize it.

---

III. PROBLEM FORMULATION

We consider a hemisphere defense game where the defender operates on the surface $S$ of the hemisphere while the intruder approaches on the ground plane $\mathbb{R}^2$. For instance, a perimeter of a building that defenders aim to protect can be enclosed by a hemisphere. Since defenders cannot pass through the building, they are employed to move along the surface of the dome, which leads to the hemisphere perimeter defense game.

Although there exist optimal strategies for both players in theory [6], it can be inferred that the theoretical model (e.g. perfect state estimation) may not be realistic for a real-world implementation [16]. In this work, we extend our previous work [6] to incorporate the perception module in the hemisphere perimeter defense game to bridge the gap between theory and practice. This work differs from the previous work in that the dynamics of the UAVs, uncertainty in state estimation, and multiple viewpoints of defenders are newly introduced. Furthermore, we realize the vision-based perimeter defense and test the proposed system in hardware experiments. We also improve vision-based perimeter defense performance by incorporating pose estimation by aggregating multiple views. This section addresses the problem formulation relevant to the vision-based defense.
IV. Methods

In this work, we build a framework for vision-based perimeter defense by estimating the intruder pose. We propose a pose estimation by aggregating multiple views for perimeter defense with the framework shown in Fig. 3. Our motivation is to close the perception-action loop for the dynamic defender to maneuver with a strategy comparable to the optimal strategy from theory, which is moving towards the breaching point. The end goal is to minimize the performance metrics $\Delta d$, expressed in (1). We aim to show that the multiview perception improves perimeter defense performance.

A. Pose estimation using multiple aggregated views

In our defense application, we prepare defenders with two roles: dynamic defender and static defender. These roles enable different capabilities of defenders - dynamic defender operates on a hemisphere surface and aims to capture the intruder by estimating the intruder pose with an on-board camera, and static defender stays in the same position observing the intruder. The multiple views of the scene available from these roles allow multiple data points, which improves the overall perception. We perform an ablation study by combining multiple intruder poses by parameterizing each camera coordinate with weights $\alpha, \delta, \gamma$ (see Section V-D for more details). It is worth noting that the static defender does not try to capture the intruder in the scope of this work, but working with multiple vision-based dynamic defenders will be interesting for future work.

B. Network architecture

As shown in Fig. 3(b), we trained an end-to-end deep neural network for estimating intruder pose. We prefer deep learning over traditional methods for its scalability. The network input is $640 \times 360$ image, and the output is $\{u, v, y_c\}$. We employ ShuffleNet [17] as the backbone for its efficiency, followed by a linear layer to output the pose. The loss function is MSE loss with a weight factor of $\epsilon$ on $u$ and $v$.

C. Perception-action loop

To close the perception-action loop, the output from multiview pose estimation is given to the dynamic defender’s defender strategy module in Fig. 3(a), which outputs the position command towards the direction of the optimal breaching point. The SO(3) command [18] that consists of thrust and moment to control the robot is then passed to the dynamic defender for control. In this loop, we evaluate the performance metrics $\Delta d$ and aim to show that the proposed approach using multiview perception improves perimeter defense performance.

V. Experiments

In large, we run experiments with a realistic simulator and quadrotor platforms. We first set up the simulator environments (Section V-A) and collect training data (Section V-B) to train the proposed pose estimation networks (Section V-C). Once the parameters are selected by ablation analysis (Section V-D), we further evaluate perimeter defense performance by observing the improvement from the multiview perception in diverse scenarios (Section V-E). Finally, we run hardware experiments by employing quadrotor platforms with on-board cameras to validate that vision-based perimeter defense performance improves with multiview perception (Section V-F).

A. Experimental setup in simulation

We run the simulation in Flightmare [19], a modular simulator composed of a rendering engine built on Unity and a physics engine for dynamics simulation. We consider the defense game based on a 1 vs. 1 (a dynamic defender vs. an intruder) and a 2 vs. 1 (a dynamic defender and a static defender vs. an intruder) game. When the game starts, the position of the intruder relative to the dynamic defender is set to desired $z = [\psi, \phi, r]$ in the hemisphere coordinate. The position of the static defender is set to desired $[x_w, y_w, z_w]$ in the world coordinate. The parameters used for the camera and image coordinates are: $W = 640, H = 360$, FOV= 90, $f = 180$, $t_0 = 320$, and $t_0 = 180$. 

Fig. 3. (a) Overall framework for vision-based perimeter defense. The dynamic defender may communicate with the static defender to perform multiview pose estimation, and the defender strategy is computed to give position commands to the controller to close the loop. (b) Pose estimation network architecture with ShuffleNet [17] as the backbone.
B. Data collection and domain randomization

Domain randomization [9] utilizes irrelevant variability to learn the relevant features for real-world problems. Practical applications include autonomous vehicles [20], drone racing [21], and robot manipulation [15].

As displayed in Fig. 4, we vary the visual domain in collecting the training set. To reach better generalization, we regularize the pose estimation network using data augmentation. The used randomization factors [20] are:

- Brightness: brightness factor is drawn from (0.6, 1.4)
- Contrast: contrast factor is drawn from (0.6, 1.4)
- Saturation: saturation factor is chosen from (0.6, 1.4)
- Hue: hue factor is chosen from (−0.2, 0.2)

C. Training for intruder pose estimation

We implemented all networks in Pytorch [22] and used the Adam optimizer [23]. A total of 4168 images were captured in the Unity scene with a dynamic defender. We set the initial learning rate to 5e-4, which was reduced by a factor of 2 every 5 epochs from epoch 10 until epoch 30. The final epoch of 40, a batch size of 4, and $\epsilon = 0.02$ for the loss function were used.

We consider a number of backbones as possible alternatives to our model: MobileNet [24], SqueezeNet [25], and MnasNet [26], and training curves of the four backbones are shown in Fig. 5. These are all lightweight networks that would enable real-time perimeter defense. We perform further training with domain randomization, which was applied to one-tenth of the training images, and split the training and validation sets with an 8 : 2 ratio. We find that our model with the backbone as ShuffleNet [17] with domain randomization performs the best.

The quantitative results for intruder pose prediction are detailed in Table I. For comparison, we also run YOLOv3 detector [27] that has been widely used for real-time object detection [13], [14], [28]. Since YOLOv3 outputs a bounding box for detection, the UV prediction takes the center of the produced bounding box, and the $y_c$ prediction is estimated by looking at the size of the bounding box given that we assume the size of the intruder is known and fixed. In predicting the true pose of $(u, v)$, ShuffleNet with domain randomization achieves the lowest average UV error at 6.25 pixels. The $y_c$ prediction errors seem almost the same for all the methods (e.g. $0.55 \pm 0.1m$), and this may be due to the fact that it is challenging to estimate the exact depth from an image since even a single pixel can represent a long distance. One exception is YOLOv3, which shows a much larger error in the $y_c$ prediction. This large error could be due to the fact that the size of the bounding box may not correctly represent the actual size of the intruder in case of occlusion.

Fig. 6 shows the qualitative results for intruder pose prediction. The true and predicted intruder poses are marked by red and green circles, respectively. The pose estimator is robust against challenging environments considering occlusion, shadow, or different camera viewpoints.

D. Ablation analysis on vision-based perimeter defense

From the pose estimation results, we simulate the full defense system to close the perception-action loop. Fig. 7 shows the overview of the vision-based perimeter defense. Fig. 7(a)-(c) are the camera views from the dynamic defender, static defender, and intruder. Fig. 7(d) shows the schematic view of agents and perimeter corresponding to the Flightmare simulator. Fig. 7(e) describes the overall Flightmare simulation [19].

### Table I

| Average Error   | UV (pixel) | Y (m) |
|-----------------|-----------|-------|
| YOLOv3 [27]     | 13.94     | 2.81  |
| MobileNet [24]  | 11.06     | 0.52  |
| SqueezeNet [25] | 11.39     | 0.66  |
| MnasNet [26]    | 9.27      | 0.45  |
| ShuffleNet [17] | 8.48      | 0.59  |
| MobileNet + Domain randomization | 9.83 | 0.50 |
| SqueezeNet + Domain randomization | 10.36 | 0.64 |
| MnasNet + Domain randomization | 7.90 | 0.44 |
| ShuffleNet + Domain randomization | **6.25** | 0.46 |

Fig. 6. True intruder pose (red) and prediction results (green) under occlusion, shadow, and different viewpoints.
As shown in Fig. 7(a), the \((x_s, y_s, z_s)\) output from the multiview pose estimation is transmitted to the defender strategy module that computes the optimal breaching point based on agent positions. The control command for the defender is fed back into the Unity simulator to close the perception-action loop and render the moving agents.

In the ablation analysis, we take an advantage of the static defender whose camera view has a different perspective from the dynamic defender’s camera view. In particular, we assume that the dynamic defender’s optical axis of its camera is perpendicular to the static defender’s optical axis. Let \(\{I_d, \bar{P}_d\}\) and \(\{I_s, \bar{P}_s\}\) denote the true image and intruder pose pairs for the dynamic defender and static defender, respectively. Our goal is to learn the domain randomization mapping \(f\) so that we can estimate the intruder pose given an image as \(f(I_d) = \bar{P}_d\) and \(f(I_s) = \bar{P}_s\). The prediction \(P_d\) and \(P_s\) are the estimates of \(\bar{P}_d\) and \(\bar{P}_s\). We assume no errors in state estimation so that we can estimate the transformation \(T\) between the dynamic and static defenders are known, i.e., \(T(P_d) = P_s\). Then, we can collect multiple data points \(P_{d,k}\) from both defenders by

\[
f(I_d) = P_{d,1} \cdot T^{-1}(f(I_s)) = P_{d,2}.
\]

While a previous work predicted the final pose as the sample average [15], we combine \(P_{d,1}\) and \(P_{d,2}\) by parameterizing each camera coordinate as

\[
x_c = x_{c,1} \alpha + x_{c,2}(1 - \alpha),
\]

\[
y_c = y_{c,1} \delta + y_{c,2}(1 - \delta),
\]

\[
z_c = z_{c,1} \gamma + z_{c,2}(1 - \gamma),
\]

where \((x_{c,k}, y_{c,k}, z_{c,k})\) are the camera coordinates corresponding to \(P_{d,k}\), and \(\alpha, \delta, \gamma\) are parameters used for ablation study.

Table II shows the relationship between the choice of parameters \(\alpha, \delta, \gamma\) and performance metrics \(\Delta d\). We set up the initial conditions in the experiments so that performance metrics should be zero if we assume the pose estimation was perfect. Trial 1 uses \(\alpha = 1.0, \delta = 1.0, \gamma = 1.0\), which represents the 1 vs. 1 defense where we only utilize the dynamic defender’s perception module. Next, we give a high weight (e.g. 0.9) to a parameter in Trial 2 and give high weights to two parameters in Trial 3. Trial 4 shows various parameter choices with increasing weight on \(\gamma\).

It can be inferred from Trials 2 and 3 that high weight on \(\alpha\) would help minimize \(\Delta d\). This indicates that it would be better to trust the dynamic defender than to trust the static defender in estimating the x-coordinate of the intruder in camera coordinates. This may be due to the fact that the dynamic defender estimates the x-coordinate as a lateral position while the static defender estimates it as longitudinal information. In general, the camera is known to obtain lateral information better than longitudinal information [29], [30]. It seems that the z-coordinate of the intruder is estimated the best if trusting both dynamic and static defenders with equal weight.

In all trials, the choice of \(\alpha = 0.7, \delta = 0.3, \gamma = 0.5\) achieves the best performance, which results in \(\Delta d = 4.03\). It is worth noting that this result outperforms the choice of \(\alpha = 0.5, \delta = 0.5, \gamma = 0.5\), which represents the sample average method [15] in computing the final pose. As mentioned before, this ablation study validates that multiview perception improves the perimeter defense algorithm.

E. Multiview perception on vision-based perimeter defense

This section validates that multiview perception improves vision-based perimeter defense. Fig. 8(a) shows the intruder pose estimation error with three different choices for the perception component. For multiview perception, we use the parameters \(\alpha = 0.7, \delta = 0.3, \gamma = 0.5\) to achieve the best performance. In all cases, we assume that the intruder follows its optimal strategy so that we can equally compare a different set of defenses. We take the \(L_2\) norm of intruder position error along the trajectories, and the

\[
\text{Table II: Ablation Analysis on Defense Algorithm}
\]

| Trial | \(\alpha\) | \(\delta\) | \(\gamma\) | \(\Delta d\) |
|-------|-----------|-----------|-----------|-------------|
| 1     | 1.0       | 1.0       | 1.0       | 4.91        |
| 2(a)  | 0.1       | 0.1       | 0.9       | 4.33        |
| 2(b)  | 0.1       | 0.9       | 0.1       | 4.32        |
| 2(c)  | 0.9       | 0.1       | 0.1       | **4.14**    |
| 3(a)  | 0.1       | 0.9       | 0.9       | 4.44        |
| 3(b)  | 0.9       | 0.1       | 0.9       | 4.38        |
| 3(c)  | 0.9       | 0.9       | 0.1       | **4.17**    |

**Fig. 8.** (a) The average of \(L_2\) norm of intruder position error with different perception methods. (b) Perimeter defense performance \(\Delta d\) for representative scenarios.
average of $L_2$ norm position error in a trajectory is shown for a number of trials with different initialization. It can be seen that the static defender has less perception error than the dynamic defender does since the static defender is initially placed so that its perception can closely monitor the entire trajectory of the intruder. All trials verify that multiview perception lowers the $L_2$ norm of intruder position error from both defender viewpoints and thus improves the vision-based perimeter defense.

We evaluate the perimeter defense performance measured by $\Delta d$ using the three choices for the perception component, as shown in Fig. 9(b). We test the performance in representative scenarios: for "simple," both defender and intruder start with the same azimuth angles; for "general," defender moves on a geodesic path while intruder moves in a straight line towards the optimal breaching point; and for "degenerate," the initial position of the defender is on the base plane of the hemisphere. We run multiple trials with different initialization and confirm that multiview perception outperforms single-view perceptions in all scenarios. In the degenerate case, dynamic defender perception outperforms static defender perception since both agents are on the base plane.

**E. Hardware experiments**

To further validate our proposed framework, we employ quadrotors as the defender and the intruder. The quadrotor platform is based on the quadrotor used in [31]. As shown in Fig. 9(a), it is a 0.16 m diameter, 256 g quadrotor using a Qualcomm Snapdragon™ board with a 7.4 V LiPo battery. The platform is equipped with a downward-facing camera and an on-board VIO state estimator. In the experiments, a dynamic defender hovers around a designed perimeter shown in Fig. 9(b) to prevent an intruder from reaching the perimeter, and a static defender on the side allows multiview perception (Fig. 9).

The robots’ software stack is built on the Robot Operating System (ROS). All quadrotors run separate ROS masters and can communicate with the VICON Motion Capture system to obtain the ground truth pose. Due to the computing limit of the lightweight quadrotor platform, we perform the image processing on a base station but the image transmission and our full system are implemented in real-time. We utilize the same networks and parameters as the simulator to evaluate our proposed system.

![Fig. 9. Setup for hardware experiments. (a) The Snapdragon platform with a downward-facing camera. (b) Designed perimeter.](image)

**VI. Conclusion**

This paper realizes vision-based perimeter defense and incorporates the pose estimation by aggregating multiple views. The multiview perception improves perimeter performance in simulation and real-world experiments. The future work will focus on working with multiple dynamic defenders with communication and consider an end-to-end perimeter defense approach.
