FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems

Shaoyuan Xie, Mohamad Habib Fakih, Junchi Lu, Fayzah Alshammari, Ningfei Wang, Takami Sato, Halima Bouzidi, Mohammad Abdullah Al Faruque, and Qi Alfred Chen

University of California, Irvine

Abstract

Autonomous Target Tracking (ATT) systems, especially ATT drones, are widely used in applications such as surveillance, border control, and law enforcement, while also being misused in stalking and destructive actions. Thus, the security of ATT is highly critical for real-world applications. Under the scope, we present a new type of attack: distance-pulling attacks (DPA) and a systematic study of it, which exploits vulnerabilities in ATT systems to dangerously reduce tracking distances, leading to drone capturing, increased susceptibility to sensor attacks, or even physical collisions. To achieve these goals, we present FlyTrap, a novel physical-world attack framework that employs an adversarial umbrella as a deployable and domain-specific attack vector. FlyTrap is specifically designed to meet key desired objectives in attacking ATT drones: physical deployability, closed-loop effectiveness, and spatial-temporal consistency. Through novel progressive distance-pulling strategy and controllable spatial-temporal consistency designs, FlyTrap manipulates ATT drones in real-world setups to achieve significant system-level impacts. Our evaluations include new datasets, metrics, and closed-loop experiments on real-world white-box and even commercial ATT drones, including DJI and HoverAir. Results demonstrate FlyTrap's ability to reduce tracking distances within the range to be captured, sensor attacked, or even directly crashed, highlighting urgent security risks and practical implications for the safe deployment of ATT systems.

Main Content

This work is published at Network and Distributed System Security (NDSS) Symposium 2026, and the assigned DOI is https://dx.doi.org/10.14722/ndss.2026.230904. The original abstract and author list are shown above. Since the work is not yet published, we are providing the paper link to the arXiv version: https://arxiv.org/abs/2509.20362.

FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems

Shaoyuan Xie, Mohamad Habib Fakih, Junchi Lu, Fayzah Alshammari, Ningfei Wang,
Takami Sato, Halima Bouzidi, Mohammad Al Faruque, Qi Alfred Chen

UC Irvine

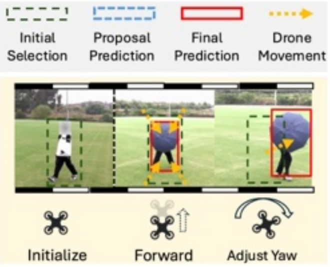
[Published at NDSS'26]

NDSS SYMPOSIUM

Background

Autonomous Target Tracking (ATT) systems are widely used in drones for surveillance and law enforcement but pose security and privacy risks. The ATT drones are used as:

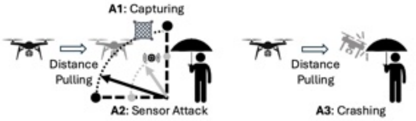
- **Security and Surveillance**: Widely used in border patrol, crowd monitoring, and private security to automatically track suspicious individuals or objects.
- **Law Enforcement**: Deployed by **police departments** for suspect tracking during operations.
- **Malicious Stalking**: Followed by unknown ATT drones.



Problem Formulation

Goal: We proposed **Distance-Pulling Attack (DPA),** a novel attack that manipulates tracking distance, bringing drones dangerously close to targets. DPA can lead to:

- Drone capture (net gun)
- Range-limited sensor attacks
- Physical collision



Threat Model:

- **White box assumption**:
  - Attacker knows the victim's Single Object Tracking (SOT) model (via drone identification and reverse engineering).
  - Attacker collects aerial videos of general tracking scenarios (not necessarily the same person or location) for attack optimization.
- **Black box assumption**:
  - No access to the exact model, but the attack relies on **transferability** across models.
  - Validated via successful black-box attacks on commercial drones.

Prior Works

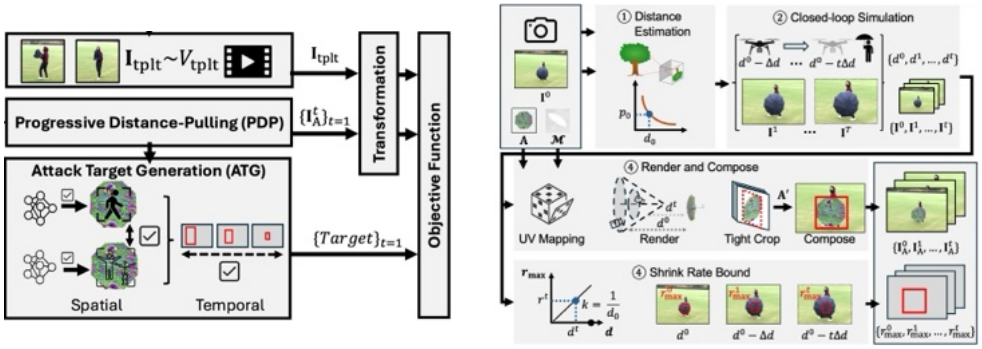
(CVPR 2020) Cooling-Shrink Attack

(CCS 2022) AttrackZone

(AAAI 2021) Universal Physical Attack

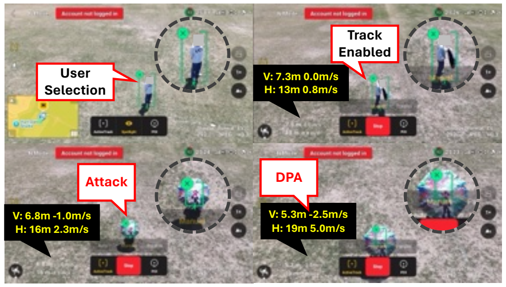
Previous works limitations: (1) not deployable for outdoor ATT use cases (e.g., pixel perturbation, projector, printed paper); (2) cannot achieve closed-loop DPA effecs; and (3) lack of spatio-temporal consistency and be already be defended by state-of-the-art spatio-temporal defenses.

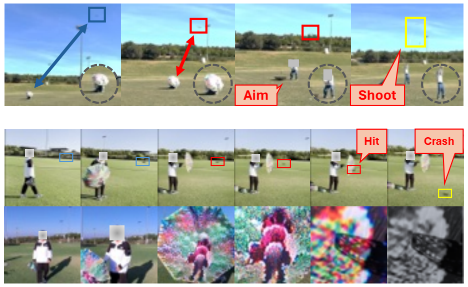
FlyTrap Attack


$\mathbf{I}_{\text{tplt}} \sim V_{\text{tplt}}$
$\mathbf{I}_{\text{tplt}}$
Progressive Distance-Pulling (PDP)
$\{\mathbf{I}_A^t\}_{t=1}$
Attack Target Generation (ATG)
Spatial
Temporal
$\{Target\}_{t=1}$
Transformation
Objective Function
$\mathbf{I}^0$
$\mathbf{A}$
$\mathcal{M}$
① Distance Estimation
p_0
d_0
② Closed-loop Simulation
$d^0 - \Delta d$ ... $d^0 - t\Delta d$
$\mathbf{I}^1$ ... $\mathbf{I}^T$
$\{d^0, d^1, \dots, d^t\}$
$\{\mathbf{I}^0, \mathbf{I}^1, \dots, \mathbf{I}^t\}$
④ Render and Compose
UV Mapping
d^t
d^0
Render
Tight Crop
$\mathbf{A}'$
Compose
$\{\mathbf{I}_A^0, \mathbf{I}_A^1, \dots, \mathbf{I}_A^t\}$
④ Shrink Rate Bound
$r_{\max}$
r^t
$k = \frac{1}{d_0}$
d^t
d
$r_{\max}^0$
$r_{\max}^1$
$r_{\max}^t$
d^0
$d^0 - \Delta d$
$d^0 - t\Delta d$
$\{r_{\max}^0, r_{\max}^1, \dots, r_{\max}^t\}$

- **Adversarial Umbrella**: A physically deployable, domain-specific attack vector.
- **Progressive Distance-Pulling (PDP)**: Simulates closed-loop system response as the drone gets closer and maintains attack effectiveness across distances using a gradually shrinking bounding box design. Leverage computer graphics modeling to ensure high physical fidelity.
- **Attack Target Generator (ATG)**: Ensures spatial-temporal consistency.
- **Objective Function**: $\mathcal{L}_{\text{loc}} = \frac{1}{NMT} \sum_{i=1}^{N} \sum_{j=1}^{M} \sum_{t=1}^{T} \left\| \mathcal{P}_{i,j}^t \ominus \mathcal{P}_a^t \right\|$, $\mathcal{L}_{\text{cls}} = \frac{1}{NMT} \sum_{i=1}^{N} \sum_{j=1}^{M} \sum_{t=1}^{T} [-\log(score_{i,j}^t)]$.

Experiments





We collect an evaluation dataset, print physical umbrellas, build full-stack white-box ATT drones, and purchase three commercial drones for the experiment:

- **Effectiveness**: We achieve much better attack effectiveness with the PDP design.
- **Universality**: FlyTrap can be used by different individuals from different locations.
- **Physical experiment**: One of the physical umbrellas can successfully attack full-stack ATT and three commercial drones, including DJI Mini 4 Pro, HoverAir-X1, and DJI Neo.

Future Plans

- **Defense**: Advancing defense techniques against DPA.
- **Effectiveness on real-world systems**: Further understanding and improving the black-box transferability, especially to commercial drones.

***Disclaimer**: All drone data and experiments presented in this work were completed before December 22, 2025.*