Demo: One Shot All Kill: Building Optimal Attack on Swarm Drones

Minki Lee, Gangmin Kim, Jonghyun Kang, Hyunwoo Kim, Jangwon Lee, Hongjun Choi
DGIST, Daegu, Republic of Korea
{leeminki, kjkj0513, yuri7579, gudens0823, dlwkddnjs53, hongjun}@dgist.ac.kr

Introduction

With the growing attention to Cyber-Physical Systems (CPS) and drone systems, research on the security and various attack methods against drone swarms are coming up. The most effective way to attack a swarm is to comprehensively target all drones within the swarm. However, since not all drones in a swarm may be of the same type or situation, the attack method may not be universally fatal to all drones. This study aims to demonstrate the potential to cause catastrophic consequences for the entire drone swarm by attacking a single drone within the swarm. Following this, the goal is to provide an interim report on identifying the optimization methods for finding the most effective attack approach through simulations and experiments in a real-world environment.

Attack Explanation

Assumptions. This study focuses on identifying effective attack strategies against a drone swarm, where each drone independently operates and dynamically communicates within the network. The reliance of drones on real-time data for navigation makes the network vulnerable to attacks. The aim is to find an optimal attack approach that threatens the entire swarm's mission with minimal intervention.

Attack Method. For our approach, we identified each drone's position numerically and executed an attack using the Intentional Electromagnetic Interference (IEMI) [1] method. This attack utilizes electromagnetic waves to disrupt or destroy various sensors in the drone's system, including the IMU sensor, which is fundamental to its operation. To determine the optimal attack, we varied the mission maps, target drone, attack frequency, attack launch time, and the phase shift of the sine wave during the attacks.

Target System. The attack was carried out on the widely utilized Adaptive Swarm algorithm [2], a representative algorithm to support collision avoidance in swarm robotics. During the attacks, following the principles of IEMI attacks, we analyzed the effectiveness of different attacks by distinguishing them based on the phase difference of sine waves and the selected victim drone. We experimented on three target systems: Crazyflie 2.1-based real-world swarm drones, simple Python Adaptive Swarm Simulator, and PX4/gazebo-based simulation system as in Fig. 1.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25008
www.ndss-symposium.org

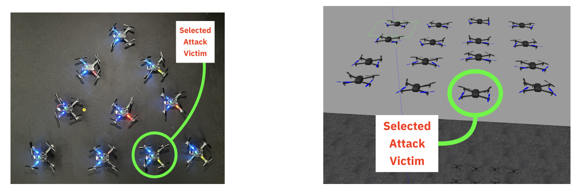
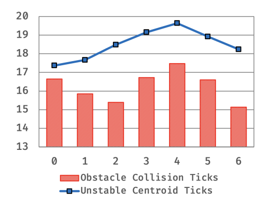
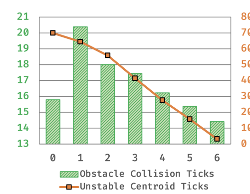


Fig. 1: Target Swarm System (Real-world, Simulation)

Evaluation Rules. We evaluated the severity of the attack based on five criteria: *Collision Tick Count*, *Centroid Low Stability Count*, *Path Length*, *Average Velocity*, and *Mean Formation Area*. These metrics were instrumental in assessing the attack's impact on the swarm's performance. Mainly, we used *Collision Tick Count* and *Centroid Low Stability Count* to check the resilience of the overall algorithm after the attack, as shown in Figure 2. Details about the results and demos are available at https://sites.google.com/view/controlattack.



(a) x-y Phase difference



(b) Attack Launch Time

Fig. 2: Criticality changes according to attack variables

Future Works

The concept of executing a minimal attack to maximize its impact on dynamic swarm control presents intriguing possibilities for future research. The planned full paper will delve deeper into these areas, focusing on: expanding attack repertoire, formalizing attack models and real-world implications, maximizing attack consequences, automatically searching for variables for the optimal attack, and providing defense techniques.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2023-00209836) and DGIST Start-up (2023010056)

References

[1] Kim, S. G., Lee, E., Hong, I. P., & Yook, J. G. (2022). Review of intentional electromagnetic interference on UAV sensor modules and experimental study. Sensors, 22(6), 2384.

[2] Agishev, R. (2019). Adaptive Control of Swarm of Drones for Obstacle Avoidance (Doctoral dissertation, Master's thesis, Skolkovo Institute of Science and Technology).