Drone Swarm Case Study

Nancy R. Mead

Forrest Shull

Krishnamurthy Vemuru, University of Virginia

Ole Villadsen, Carnegie Mellon University

April 2021

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

Drown Swarm Case Study

Background

Unmanned aerial vehicles—commonly known as drones—are ideal for many rescue and emergency situations: they can fly into dangerous or uncertain conditions and go where manned vehicles cannot. We wish to design and develop fleets (or swarms, as we call them) of drones to be used in situations such as

- surveying and monitoring the extent of forest fires
- surveying the extent of earthquake damage and locating survivors
- delivering medical supplies and equipment to survivors or isolated people

Having human beings manually controlling individual drones not only requires a large number of trained personnel, but often is not even technically possible because of erratic radio communications around mountains and other terrain. As a result, each swarm must be able to act autonomously to achieve its objectives. Swarms should be capable of both national and international use.

Student Instructions

High-Level Requirements

Figure 1 shows a deployment example of two swarms, both sent out on search and rescue missions beyond a large fire. Each swarm consists of the following:

- One "leader": this drone contains radio equipment that attempts to maintain communication with a base station. The leader is the only drone that has this equipment; the other drones can communicate with each other and the leader but are not able to reliably reach the base. As a result, if the leader fails, the entire mission fails. Leaders aren't generally customized for the particular mission.

- One or more "followers": these drones usually have customized equipment for the mission—video cameras, medical-equipment payload carriers, and so on. They are in radio communication with the leader, but not the base. Depending on the mission, one or more followers may be required to successfully complete an assigned task, but in general, missions can succeed even when one or more followers fail. Followers don't have the equipment necessary to be "promoted" to leader mid-mission.

Upon deployment, the leader gives the swarm a list of physical coordinates (checkpoints), received from the base. Each coordinate must be reached by a given time. The leader alerts the base when each checkpoint is reached. The leader tracks time via an onboard clock; if any checkpoint is not reached in time, the mission is aborted, and the drones return to the base. This list of checkpoints may be changed mid-mission by the base. The leader alerts the base if the swarm is running low on fuel and may not be able to achieve its mission as a result. Naturally, reaching checkpoints on time isn't the only criterion for mission success: performing the survey, dropping medical supplies, and so on, are the ultimate success criteria. The mission checkpoints merely ensure that if flying conditions are much worse than anticipated, the drones won't vainly struggle to get to a location too late to be useful or become unable to return.

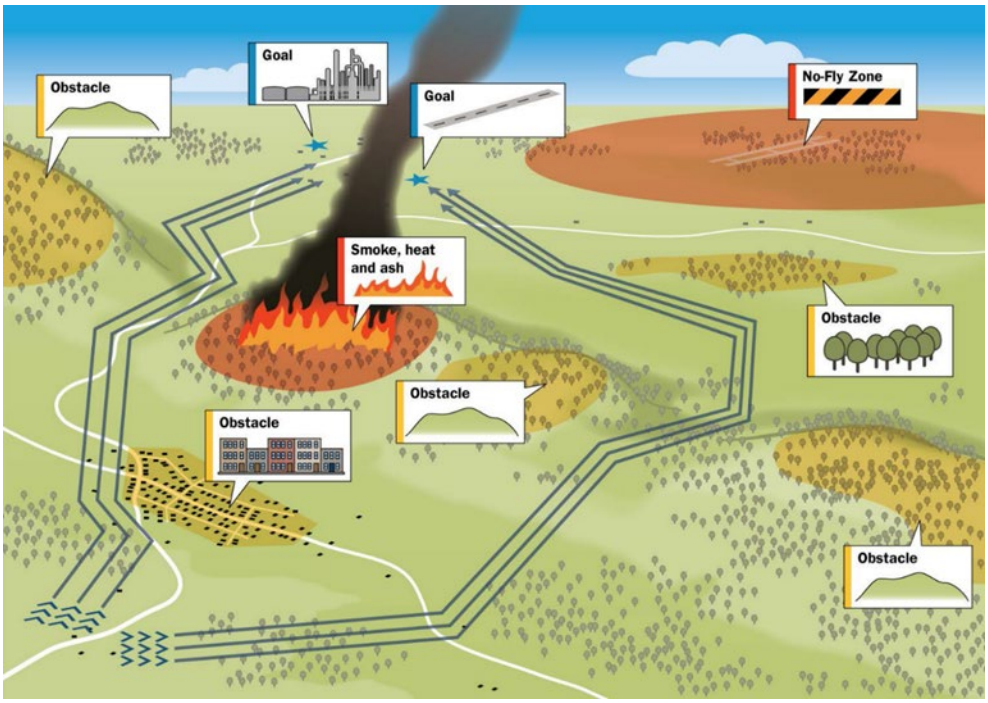

Figure 1: Deployment Example of Two Swarms

The drones should not collide with each other or with the ground. To avoid collisions, all drones are equipped with altimeters (to determine their height) and GPS; all of this information is periodically communicated to other drones in the swarm as well as to the base. If contact with the base is lost, the leader attempts to re-establish communication while the swarm continues to perform based on the most recent information.

Environmental Constraints

Because swarms may fly in areas containing smoke and debris, drones are expected to operate even when they are in imperfect physical condition or become damaged during the mission.

The follower drones should fly in formations that protect the leader from bird impacts and debris as much as possible. Also, poachers and frightened observers have been known to try to shoot drones. The swarm is given a map of "dangerous flying" areas. Because flying conditions are expected to be poor in these areas, the swarm should fly slower and the followers should stick closer to the leader to protect it from harm. The flying formation and logic for preventing collisions is managed by an algorithm running onboard the drones themselves; the base does not determine the formation.

Political borders and no-fly zones (such as around buildings in Washington, DC) must be observed, and the swarm must not fly into these areas.

The drones themselves, and their low-level software, will be built and supplied by a third-party company.

Instructor notes

Example solution

Threat Modeling with Secure Cards for Drone Deliveries

We consider a drone or drone swarm that is on its way to deliver emergency supplies to the flood-affected populations after it is dispatched by the team consisting of local government authorities and their drone technology contractors. See Figure 2 for an example. The drones face several potential threats, both physical and cyber in nature. We consider a few scenarios of drone attack and how those attacks affect the drones and the people who depend on them.

Figure 1: Example of a Drone Swarm
(*Source: http://www.ioti.com/security/drones-are-coming-take-cover*)

Part 1: Ranks within each category with reason it is considered a potential threat

A Ranked Overview

Human Impact Cards:

1. Emotional well-being (those suffering from the disaster are deprived of basic commodities and get depressed—the primary subject of the threat)
2. Physical well-being (health is affected due to lack of timely food supplies and medicine—the primary subject of the threat)

3. Relationships (the relations between the people, local authorities, and government is at stake if the rescue mission fails—a secondary subject)
4. Unusual impacts (loss of property, loss of life, loss of trust in local government, loss of businesses—a secondary or ternary subject)

Adversary's Motivations:

1. Money (the goods stolen from the drones and the drones/components can be resold to make money—the profitable nature makes this rank 1!)
2. Warfare (some local troublemakers may see this as a route and non-violent means of attack—allowing ease of attack, i.e., without having to face other humans in the operations makes this rank above the rest)
3. Politics (oppositions and opposition groups may intrude to bring bad name to local government—can lead to change of power, so it becomes attractive)
4. Unusual motivations (hack the drones and use them for other unauthorized purposes such as flying in restricted zones or delivery of harmful goods or simply to destroy)

Adversary's Resources:

1. Expertise (the attacker has all the expertise to hack the brand of drones used in the mission)
2. Inside knowledge (access to inside knowledge makes the attack viable)
3. Money (money flowing in for political reasons to bring down the local government's reputation)
4. Inside capabilities (an insider who turns attacker can do a lot of damage to the drones)

Adversary's Methods:

1. Physical attack (shoot the drone with a drone gun)
2. Technological attack (jam the GPS or the rotors)
3. Multiphase attack (damage partially—perhaps damage one rotor and partially disable the drone to take control)
4. Manipulation or coercion (hack the drone information system and its GPS, then change the destination or send it back to the origin or make it lose its sense of direction)

Part 2: In-depth analysis of all the potential threats: Threat Insights

Human Impact Cards:

1. Emotional well-being (those suffering from the disaster are deprived of basic commodities and get depressed—the primary subject of the threat)
2. Physical well-being (health is affected due to lack of timely food supplies and medicine—the primary subject of the threat)
3. Relationships (the relations between the people, local authorities, and government is at stake if the rescue mission fails—a secondary subject)

4. Unusual impacts (loss of life, loss of trust in local government, loss of businesses—a secondary or ternary subject)

Type	Actor	Action	Target	Purpose	Result	Impact
Denial	Attacker	Attack Methods 1-4	Drone (Physical, Cyber)	Motivations 1-4	Human Impacts 1-4	1-High 2-High 3-Low 4-Low

Adversary's Motivations:

1. Money (the goods stolen from the drones and the drones/components can be resold to make money—the profitable nature makes this rank 1!)
2. Warfare (some local troublemakers may see this as a route and non-violent means of attack—allowing ease of attack, i.e., not having to face other humans in the operations makes this an above the rest)
3. Politics (oppositions and opposition groups may intrude to bring bad name to local government—can lead to change of power, so it becomes attractive)
4. Unusual motivations (hack the drones and use them for other unauthorized purposes such as flying in restricted zones or delivery of harmful goods or simply to destroy)

Type	Actor	Action	Target	Purpose	Result	Impact
1-Capture 2,3,4-Hack	Attacker	Intrusion	Drone	Misuse Drone	Adversary's Motivations 1-4	1-High 2,3,4-Low

Adversary's Resources:

1. Expertise (the attacker has all the expertise to hack the brand of drones that are used in the mission)
2. Inside knowledge (access to inside knowledge makes the attack viable)

3. Money (money flowing in for political reasons to bring down local government reputation)
4. Inside capabilities (an insider who turns attacker can do a lot of damage to the drones)

Type	Actor	Action	Target	Purpose	Result	Impact
Denial, Spoofing, Jamming, Screening	Attacker	Physical, Cyber Attacks	Drone, Physical, GPS, Accelerometer, Computer	Adversary's Motivations 1-4	Human Impacts 1-4	1,2,3,4 High

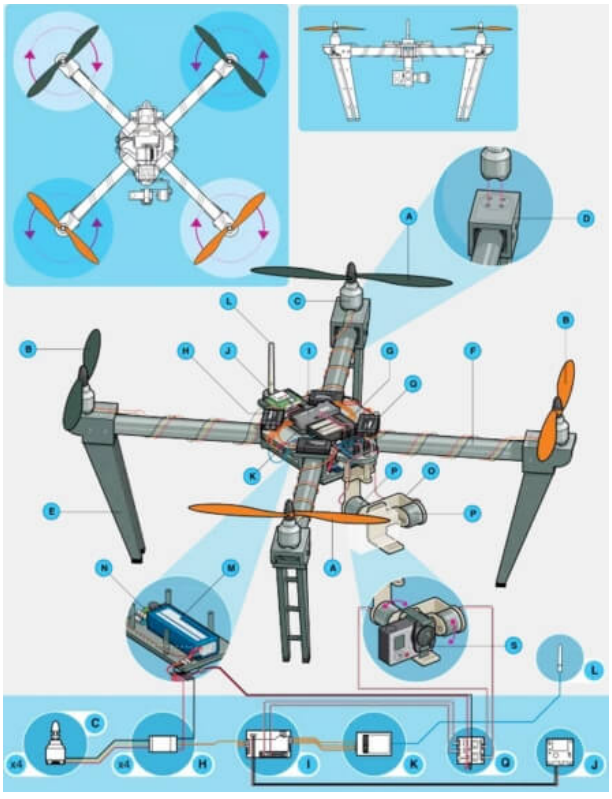

Figure 2: Example of Drone Components
(*Source: https://www.dronezon.com*)

Adversary's Methods:

To analyze how a drone can be subjected to an attack, let us consider an example. Figure 3 shows typical drone parts: Propellers, Brushless Motors, Motor Mount, Landing Gear, Boom, Drone Body Part, Electronic Speed Controllers, Flight Controller, GPS Module, Receiver, Antenna, Battery, Battery Monitor, Gimbal, Gimbal Motor, Gimbal Control Unit, Camera, Sensors, and Collision Avoidance Sensors. The attack can in principle be on any of the components. We consider a few most likely cases.

1. Physical attack (shoot the drone with a drone gun, direct objects, or spray a dark paint on drone's camera to blind the drone)
1. Technological attack (jam the GPS or the propellers)
2. Multiphase attack (damage partially, e.g., damage one propeller and partially disable the drone to take control)
3. Manipulation or coercion (hack the drone information system and its GPS, then change the destination or send it back to the origin or make it lose its sense of direction)

Type	**Actor**	**Action**	**Target**	**Purpose**	**Result**	**Impact**
Damaging, Capturing, Redirecting	Attacker	Shooting, Hacking, Modifying, Parameters	Drone, Physical, GPS, Accelerometer, Computer	Adversary's Motivations 1-4	Human Impacts 1-4	1,2,3,4 High

References

Mead, N. R., Shull, F., Vemuru, K., and Villadsen, O. 2018. A Hybrid Threat Modeling Method. Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf