Identifying UAV Swarm Command Methods and Individual Craft Roles Using Only Passive Sensing

Jonathan Meredith
Department of Mathmatics and Computer Science
Ashland University
Ashland, OH, USA
jmeredit@ashland.edu

Jeremy Straub, Benjamin Bernard
Department of Computer Science
North Dakota State University
Fargo, ND, USA
jeremy.straub@ndsu.edu,
ben.bernard@ndsu.edu

***Abstract*—Anti-drone technologies that attack drone clusters or swarms autonomous command technologies may need to identify the type of command system being utilized and the various roles of particular UAVs within the system. This paper presents a set of algorithms to identify what swarm command method is being used and the role of particular drones within a swarm or cluster of UAVs utilizing only passive sensing techniques (which cannot be detected). A testing configuration for validating the algorithms is also discussed.**

Keywords—UAV swarm control, UAV command, anti-drone, drone, swarm role detection, passive sensing, unmanned aerial vehicle, unmanned aerial system

I. Introduction

In recent years, small unmanned vehicles have become a competitive alternative to other vehicles for both civilian and military uses [1]. While unmanned aerial vehicles (UAVs) – commonly known as drones – are perhaps the best known, unmanned vehicles come in many different shapes and sizes. These unmanned vehicles can be used in a multitude of different applications. Communicating with these unmanned vehicles has remained a challenge due to the high-speed, low-latency connection that is needed to allow the vehicle to be controlled remotely. This includes fast communications for both commands from the ground station to the UAV as well as video and other telemetry from the UAV that is needed for decision-making.

One of the largest limitations to present-day UAV systems has been the requirement of having at least one operator per unmanned vehicle [2] which limits the number of vehicles that can be deployed, particularly when data connections available for command are limited. An alternative to this method is to use autonomous systems made up of large numbers of UAVs deployed as a cluster or swarm [3]. A cluster or swarm has the advantage of one operator having command over many unmanned autonomous vehicles (UAV) at one time. While this allows for resiliency, a distributed method of sensing obstacles and a reduction in the amount of labor needed per drone, there are numerous technical and logistical considerations and impediment to wholly autonomous drone systems and questions about what the appropriate human to drone oversight ratio remain to be answered [2]. However, the clear human time savings, particularly for large groups of UAVs with a similar or coordinated mission, makes it very likely that higher drone to operator ratios will become the future norm. The technology required to support these operations is a key area of current work.

In this paper, we discuss algorithms that have been developed to identify the command techniques utilized by a cluster or swarm of UAVs and to identify the different roles of particular UAVs within that system. A particular focus has been determining what UAV is serving as the master, and which UAVs are serving as slaves, within a master/slave configuration swarm, as the master represents a target of particular interest within the swarm. With this knowledge, an attacker can better focus their resources on more efficiently impairing, disabling or destroying the cluster or swarm. It is highly desirable for an attacker to focus on one, or a small number of UAVs, and to be able to compromise or bring down an entire swarm.

II. Background

This paper draws on prior work from several areas which are discussed in this section. First, swarm communications are discussed. Then, methods of UAV swarm communications are presented. Then, the process of detecting radio signals is considered. Finally, trilateration techniques are briefly presented.

A. Swarm Communication

There are multiple ways that a swarm or cluster of UAVs can communicate. Each method has its own advantages and disadvantages. The intended use and flight configuration of the UAV swarm dictates the selection of one method over another.

One of the traditional ways that swarms communicate is that every single drone has a link back to the main command station that receives sensor information from the UAV and then sends commands back to the UAV [1], [4]. This approach is based off of the one operator, one drone paradigm. For autonomous clusters, a benefit to this method is that calculations can be done faster on the command station's higher performance hardware which is shared across the UAV swarm. The drawback of this method is that the hardware needed to enable long-distance communication with the main command station can be problematic, given the small payload capacities of the UAVs. Additionally, if there was a failure of or an attack on the main command station, there is no redundancy built into the swarm resulting in the operability of the swarm being compromised.

c Under this model, the processing of the sensor data is all done within the swarm itself [1]. The local network is established between one or more members of the group so that all of the members can communicate with each other [5].

To eliminate all UAVs having to have long-distance communications hardware, a master UAV can be designated within the local network. This UAV has the ability to reach the main command station to provide updates and telemetry and receive communications regarding the swarm and its mission. The master UAV can also have superior computational processing hardware and, if it does, it can perform a majority of the group's processing, eliminating much of the needed computations on the command station and the data transmission requirements to support this [4]. The local network method also allows for faster communication between the different members of the swarm due to a shorter signal path from the master to the slave UAVs, as opposed to communications being relayed through a command station. Only one UAV needs the capability to communication back to the command station [5]. Of course, the downside to this method is that all communication is passed through a single member of the swarm which can be targeted and destroyed. Thus, a redundant stand-by master unit may be included for redundancy and resiliency.

A third method of communication builds upon the previous local network method. Each slave UAV is connected to one or more other slave UAVs which then connect back to the master UAV [1]. Each slave UAV relays the information from the other slaves back to the master [4]. This method increases the range of the swarm from the previous method, without requiring greater communications capabilities on each drone, because each UAV can relay to other UAVs in its range. Additionally, this method has some redundancy benefits, within the cluster.

B. Methods of Swarm Communication

Members of a swarm can communicate using multiple methods and the method selection will depend on whether a traditional link back to the command station or a master-slave link back to the command station is used [4].

The traditional method can be depicted as a star graph with the command station as the vertex. If one UAV senses a problem that it needs to share with another UAV (such as an approaching object), it requires at least two hops to communicate it. This communication also has a time delay.

In a master-slave configuration, the UAVs still communicate in a star configuration with the command station serving as a node and the master UAV as the vertex. The time to communicate between all nodes, except for the command station, is reduced due to proximity. Communication between nodes still requires two hops, as does communication of slave nodes to the command station.

The third type of configuration, a highly interconnected local network, is a complete graph between the UAVs with an additional link from one UAV to the command station. Only one hop is needed to communicate between any two nodes, except the command station. However, for all but one UAV, two hops are required for command station communications.

A wide variety of technologies can be used for local communications. For inexpensive drones, WiFi, ZigBee, and XBee – Pro are the go-to standards for communicating between UAVs. These methods are typically chosen due to the low latency and power capabilities that small UAVs typically have [6]. Larger drones use other communications standards.

C. Detecting Radio Signals & Trilateration

Radio signals are broadcast from a location and the signal radiates out from that point with decreasing levels of strength, as distance increases [7]. When a radio signal is detected, a likely origin direction can be determined by analyzing the strength of the radio signal in different directions from a radio detector [8]. The stronger the received signal is in one direction, the more likely that the signal is initially coming from that direction.

When a second radio detector is added, a likely position can be obtained by plotting where the strongest signals are in relation to the detectors [8]. With two signals, the overlap section can be very large. Three or more detectors, that can receive the radio signal, improve the accuracy of the origin location and decrease the possible locations that the radio wave is emitting from [7].

Trilateration is a way to determine the position of a radio emitter based on simultaneous measurements from three or more different receivers [9], [10]. Position determination of emitters is essential to correlate the logical determination of what drone is serving in a particular role with a physical drone.

III. Proposed System

This section discusses the components of the proposed system. First, it begins with a discussion for the process of determining what configuration of communication is being used. Next, role determination techniques are considered. Finally, UAV position determination techniques are presented.

A. UAV Communication Configuration Determination

For swarms with a single point of relay to a remote command station, the identification of this master node is a key objective. In order to determine which UAV is the master in the swarm, the system first has to determine what method of communication that the swarm is using. In order to determine the method of communication that the swarm is using, each receiver records and processes packets that have been sent over the air. At least three antenna receivers were set up in a triangle pattern and the distances between them were measured and recorded to allow this information to be used in finding the distance the emitter is from the receiver.

For capturing data packets out of the air, several open-source tools available on Linux systems were used. All of the tools used to pull the packets out of the air, such as tshark (the command line version of Wireshark) and Airomon are typically used by commercial penetration testers.

For the test system implementation, which is described in more detail in the subsequent section, TCP/IP communications over WiFi were utilized. However, the basic techniques used will work with a variety of communications technologies. The client computers were running the latest version of Kali Linux which allowed easy access to these tools.

WiFi transceivers supporting monitor mode, where all traffic can be captured, were used. Typically, all of the packets not destined for a given computer are rejected by the transceiver; however, in monitor mode they are passed to the computer. Being in monitor mode also allows the computer to access additional information about the Wi-Fi packets that is normally handled and discarded at the hardware level. The program on the computer can access this information and pass it into tshark, resulting in tshark being able to decode basic information about each packet. All the information that was decoded, such as the source and destination mac addresses, the SSID, frequency, channel, and what the source and destination addresses resolve to was sent to a central server for later processing.

The actual packet data (the information that was being sent from the source to the destination), does not need to be accessed (meaning that a target's encryption would not need to be broken for system functionality) and it was discarded after a hash was made. Hashing the packet data allowed packets to be compared without needing to store the actual packet. Additional information from the transceiver was also collected (such as the time the packet was received, strength of the signal, the interface it was collected on, and host identification information). This data is sent to the server machine.

This information was converted to a byte encoded string and sent over the ethernet connection to the server where it is stored in a database for later analysis. Data stored included the ID, frame interface name, time, the resolved names of the destination and source, SSID, IP and port of the client listening machine that was used. The hash of the packet included several fields that were not deemed necessary to store but helped to reduce hash collisions.

The hash is formed by taking the packet, that was sent by the client computers, and removing data that is unique to the client computer (such as the time the packet was captured and the signal strength). The md5 hash algorithm was used for hash generation.

B. Determining UAV Roles Within a Swarm or Cluster

Inside the database, the data is processed and correlated. The number (and other characteristics) of packets transmitted between each destination and source MAC address is identified. Analyzing the number of packets transferred between different MAC addresses allows a conclusion to be made about what form of command and which communication approach is being used. If the majority of the network traffic is coming from or going toward one machine, it can be concluded that the system is using a centralized swarm approach. Alternately, if the number of connections significantly exceeds the number of the UAVs, it is assumed that it is using a distributed swarm configuration. Lots of high signal strength communications, in one direction, and low signal strength communications in the reciprocal direction indicate command from a remote station.

When the determination of what type of communication the swarm is using is completed, the relevant packets are then identified in the database. The exact protocol used at this point will depend on specific objectives. For testing purposes, if it is a centralized swarm, the host that had the most packets (traffic) coming and going from it becomes the target of interest. Otherwise, multiple nodes, that had packets going back and forth between them are selected.

All of the packets that have the same hash and the same IP address are identified. For each group, the first packet is saved and the rest are discarded. Packets that that do not have a hash that matches another packet hash from a different IP address are thrown out. This data is now used for position and flight configuration determination.

C. UAV Position and Flight Configuration Determination

Now the system determines the distance to the emitter for each packet. All of the packets that have the same hash have the time extracted from them and the time with the earliest date is subtracted from the other times to get a time differential that can be used to determine distance, using the following formula:

Distance = speed x time
where speed is equal to 300,000 km/s.

Having the comparative distance away from each receiver allows a distance radius away from each transceiver to be plotted. The point (or points) that is/are the correct distance from each transceiver can then be located. If a set of candidate points are identified, the system must identify the most likely location of the UAV.

IV. Testing Configuration

To validate the efficacy of the proposed algorithms, a limited-scope demonstration and testing system was developed. A deployment of this system is shown in Figure 1.

Fig. 1. Testing Configuration Setup.

This system was comprised of five stations, with the ability for expansion to facilitate additional testing. Three stations detect transmissions and utilize this data for position and role determination. A fourth station coordinates between these three stations. Finally, for initial testing, a single emitter station (simulating the role of a UAV) was deployed. For future testing, this station could be augmented with additional emitter stations.

The initial testing configuration is depicted in Figure 2 and the positions of the stations have been marked in Figure 3, to facilitate easier identification.

Fig. 2. Testing Configuration.

Fig 3. Testing Configuration with Locations Identified.

Each detection station, as shown in Figure 4, was comprised of an Acer laptop, a Panda Wireless USB WiFi adapter and a stand. Each station had a hard-wired ethernet connection to the central coordinator station, such as to not interfere with signal reception.

The Panda external USB Wi-Fi transceivers were used to capture packets out of the air for several reasons. The first is that the larger external antenna allows the system to capture from a greater distance, therefore encompassing a greater area. Another reason for the external units is that most internal Wi-Fi cards tend to be WiFi Alliance certified. This certification does not allow the card to capture packets that are not destined for it and most of these cards discard these packets at the hardware level. To use an internal card and save the typically discarded packets, would have required a modification to the card at the hardware level. It was decided that external USB Wi-Fi transceivers would work the best due to the low cost of the transceivers and the rich set of features that some transceiver options included.

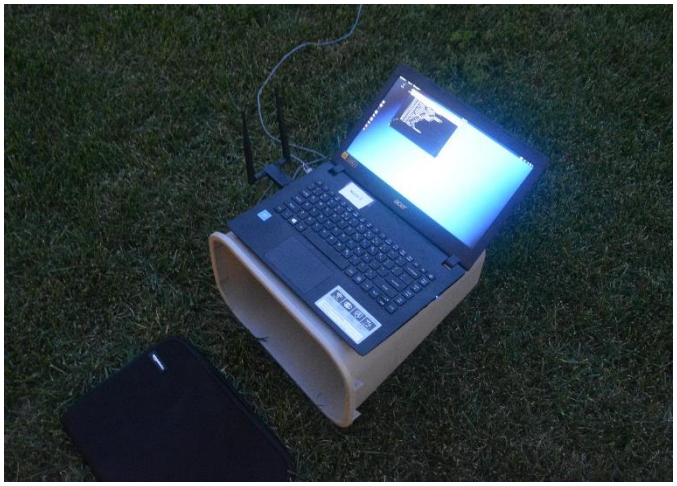

Fig 4. Testing Station.

After looking at the requirements, it was determined that a dual band transceiver (2.5 and 5 GHz) with support for the ac, b, g, and n channels and external antennas was needed. The selected transceiver, that met the above requirements, was the Panda Wireless PAU09 N600 Dual Band Wireless USB adaptor.

V. Conclusions and Future Work

This paper has presented an overview of algorithms for identifying a UAV swarm or cluster's command technique and the role of particular UAVs within the cluster or swarm. The proposed techniques could be useful in a variety of different ways, ranging from providing situational awareness to facilitating the kinetic targeting of particular drones (either due to their command role or capabilities or equipment associated with a given role) to providing critical information needed for launching an anti-autonomy anti-drone attack.

Future planned work includes additional work on the proposed system to facilitate its use in increasingly realistic scenarios. Additional testing of system efficacy and, in particular, efficacy under various conditions and for multiple drone physical and command configurations is also planned.

Acknowledgment

This work was supported by the U.S. National Science Foundation (award # 1757659). Facilities and some equipment were provided by the NDSU Institute for Cyber Security Education and Research.

References

[1] M. Campion, P. Ranganathan, and S. Faruque, "A Review and Future Directions of UAV Swarm Communication Architectures," 2018 IEEE Int. Conf. Electro/Information Technol., pp. 903–908, 2018.

[2] D. Liu, R. Wasson, and D. A. Vincenzi, "Effects of System Automation Management Strategies and Multi-mission Operator-to-vehicle Ratio on Operator Performance in UAV Systems," J. Intell. Robot. Syst., vol. 54, no. 5, pp. 795–810, May 2009.

[3] P. Chandhar, D. Danev, and E. G. Larsson, "Massive MIMO for Communications With Drone Swarms," IEEE Trans. Wirel. Commun., vol. 17, no. 3, pp. 1604–1629, 2018.

[4] L. N. A. Lakshmi Narashiman Aswin, "Design and Structural Analysis for an Autonomous UAV System Consisting of Slave MAVs with Obstacle Detection Capability Guided by a Master UAV Using Swarm Control," IOSR J. Electron. Commun. Eng., vol. 6, no. 2, pp. 1–10, 2013.

[5] A. L. Christensen et al., "Design of Communication and Control for Swarms of Aquatic Surface Drones," no. i, 2013.

[6] B. Olivieri, M. R. Junior, and M. Endler, "Controlling Swarms of Unmanned Aerial Vehicles using Smartphones and Mobile Networks ; an evaluation of the Latency requirements," XXXIV Simpósio Bras. Redes Comput. e Sist. Distrib. Salvador. Bahia, Brazil, p. 14, 2016.

[7] W. Society, "Some Sources of Bias and Sampling Error in Radio Triangulation Author (s): Joseph Tucker Springer Source : The Journal of Wildlife Management , Vol . 43 , No . 4 (Oct ., 1979), pp . 926-935 Published by : Wiley on behalf of the Wildlife Society Stable," vol. 43, no. 4, pp. 926–935, 2019.

[8] K. Connelly, Yong Liu, D. Bulwinkle, A. Miller, and I. Bobbitt, "A toolkit for automatically constructing outdoor radio maps," pp. 248-253 Vol. 2, 2008.

[9] Zheng Yang, Yunhao Liu, and Xiang-Yang Li, "Beyond Trilateration: On the Localizability of Wireless Ad Hoc Networks," IEEE/ACM Trans. Netw., vol. 18, no. 6, pp. 1806–1814, 2010.

[10] D. E. Manolakis, "Efficient solution and performance analysis of 3-D position estimation by trilateration," IEEE Trans. Aerosp. Electron. Syst., 1996.