Finding Probable Drone Launch Points Using Counter Battery Radar and Radio Detectors

Connor Leavesley

Rochester Institute of Technology

Abstract

Drone technology is a large and pervasive threat to critical infrastructure. Drones are being used increasingly by both civilians in private applications and by threat actors looking to spy and attack important facilities. While much research has been done in the detection, capture, and destruction of these infiltration drones, very little has been done in attributing a drone to an operator's location. In this paper we proposed a method of attributing a drone to a specific launch location using counter battery radar and radio detection. These methods will aid in the apprehension of threat actors by local law enforcement and stop drone infiltrations at the source.

Finding Probable Drone Launch Points Using Counter Battery Radar and Radio Detectors

Introduction

The night of 29 September 2019, several drones infiltrated the Palo Verde Nuclear Power Plant in Arizona. Security forces were helpless to stop the drones as they circled the protected area of the power plant for a little under an hour. The drones returned the next night and performed the same actions. No person or group was attributed for the infiltration (Hambling, 2020a). Unfortunately, drone incursions are fact of life for our nation's crucial infrastructure. Drones and other unmanned aerial vehicles have become a major threat in recent years to both public and private facilities. While research has been done in the areas of drone detection and defense, little has been done to attribute a drone to an operator.

This paper proposed a system to attribute a drone back to a probable launch point using counter battery radar, radio detectors, and a centralized command and control server to hasten the response of law enforcement. This system will be able to devise a probable operator location based on gathered information and known terrain data, and alert an operator in the case of an incident. First, we will discuss the background and significance of this research. Second, we will discuss related work that has been done in the field of drone attribution and drone sensing technologies. Third, we will discuss the research design and methodology for the proposed research. Fourth, we will discuss preliminary theoretical and practical implications that may arise. Finally, we will end with the expected outcomes of the experiment.

Background

Drones are quickly becoming a primary threat to many public and private installations. According to the FAA's UAS Sightings Report, there were 409 drone incidents reported by individuals between the months of April 2020 and June 2020 (Federal

Aviation Administration, 2020). Many of the incidents involved drones around airfields, putting aircraft and ground personnel at risk. In almost all of the incidents, the drone was visual identified. Further, in almost all of the incidents the drones was never attributed to an operator. Other pieces of critical infrastructure are also at risk. In 2014, France's minister of the interior vowed to neutralize drones after drones had flow over thirteen of France's nuclear power plants. The drones were spotted by guards on the ground. The people flying the drones were never identified (de la Baume, 2014). France is not the only nation having issues. According to a Freedom of Information Act request, between 2015 and 2019, 57 drone incursions occurred at 24 nuclear power plants in the United States. Of the incidents, 49 of the 57 were marked as "Closed Unresolved" as of 2020 (Hambling, 2020b). The Stars and Stripes reported that 70 drones flew over US bases in Japan in 2018 (Robson & Kusumoto, 2019). As can be seen, many of the cases reported over the past few years have had little to no attribution to the operator, resulting in many incidents being closed unresolved. Security forces were helpless to stop the drones or the operator due to inadequate policy and a technological inability to track the drone and it's operator.

Current drone policy is both inadequate and restrictive. For one, currently it is a federal crime to shoot down a drone. The FAA considers drones aircraft under 49 U.S.C. § 40102(a)(6) (U.S. House of Representatives, n.d.-b), where aircraft are defined as "any contrivance invented, used, or designed to navigate or fly in the air." Under 18 U.S.C. 32, it is a felony to damage, destroy, or disable aircraft in US airspace or used for foreign commerce (U.S. House of Representatives, n.d.-a). These two laws make it extremely difficult for security forces to deal with infiltrating drones in the continental United States. In addition, according to Chris Copeland, a base defense operations controller for the United States Air Force, Posse Comitatus limits the ability to use federal troops on US soil. Often troops have no jurisdiction outside the wire of the their base and have to hand off base policing duties to local law enforcement. This makes policing difficult as no action can be taken until a threat crosses the wire (2020). Security forces are unable to take down

a drone before it enters a facility, and they must rely on local law enforcement take any enforcement action outside the perimeter of the infrastructure. Systems that speed up law enforcement response and direct their action are direly needed.

Worldwide, militaries have been rushing to develop and field effective counter battery radar systems. These systems are designed to pick up incoming artillery rounds and calculate a probable location of origin for precise counter battery fire (United States Navy, n.d.). With shells being small and quite fast, theses systems are extremely potent at object tracking.

Related Work

Drone detection is a well researched field. Much research has been done in the way of utilizing different bands and types of radar and radio frequencies to detect and classify drones. These two detection methods have shown themselves to be potent sensors in detection systems. Used together, they can detect most drones thrown at them.

In "Drone Detection by Ku-Band Battlefield Radar", the authors explore the use of the Ku-band, a radio band between 12 to 18 GHz. The radar was able to detect non-moving and slow moving drones at a height of 20 meters from up to two kilometers away in optimal conditions. The terrains constituted of shrubs and small trees (Ochodnický et al., 2017). Other bands exist that would be a suitable fit for drone detection. In "Pursuing Drones With Drones Using Millimeter Wave Radar", Dogru and Marques use a Texas Instruments AWR1443 3D radar, but this system was not able to consistently detect the target drone. Instead, a Texas Instruments AWR1642 2D radar was used on a band between 76 and 81 GHz, which had a far better detection rate. To get 3D positions from the radar, the authors maneuvered the purser drone around the target drone, allowing for estimations of the missing axis (Dogru & Marques, 2020). Millimeter band radars have high resolutions due to their large bandwidths. This leads to a highly accurate radar for detection, classification, and tracking. In fact, they are so accurate they

can be used to tell the type of the drone and its payload. However, these high resolution radars suffer at range. The resolution can only be used at ranges up to a couple hundred meters. High resolution radar would struggle to detect fast moving drones at long range (Guvenc et al., 2018). In addition, frequency modulated continuous wave and continuous wave radars would be the best solution for drone detection due to the continuous wave. Other radars such as pulse radars are not ideal as they can not always provide full coverage at all times (Coluccia et al., 2020). Jarabo-Amores et al. explore the use of passive radar in drone detection. Active radar requires more power for broadcasting and retrieving returned signals in comparison. Passive radar also does not require the operator to cooperate with other radar users in the area in terms of band usage. However, active radar is more sensitive and more likely to detect drones at range. The passive radar was placed close to the drone launch point, 250 meters, and was successful in getting a clear image of the drones. However, it was found that drones made of plastic were more difficult to detect. The authors claim that their system could work up to eight kilometers, but was a technical estimation (Jarabo-Amores et al., 2018). Using the right radar band is important. Many drones are quite small, less than one meter across, resulting in a small radar cross section. This means that detection methods will have to use a high frequency radar for any meaningful detection. However, high frequency radar also has shorter range, meaning any system looking to detect small objects must find a balance between detail and range.

In order to tell a target from the background, a "Moving Target Indicator" can be used. Essentially, radar can be used to filter out objects that do not move over a period of time, leaving only moving objects (Coluccia et al., 2020). Using this, radar can be used to find drones in high clutter backgrounds, which can be smoothed out using radio detectors.

Radio detection has long been used as a passive detection method due to the ability to triangulate the location of a signal. While triangulation relies on being within line of sight of the source or destination of the transmission, it has been used to some effect for detection, classification, and localization in research. Nguyen et al. explored the localizing

a drone and its controller via radio frequency triangulation. In their system, there were two stations made up of a omnidirectional and directional antenna. The directional antennas would actively search for radio communications from a drone. Once a drone was found, the two omnidirectional antennas would be used in conjunction with the directional antenna to triangulate the position of the drone. A similar action can be done to find the drone controller on the same frequency. The system was able to localize the drone with an error between 10 and 15 meters while the drones were flying at around 70 to 150 meters away (Nguyen et al., 2019). While not extremely accurate, this system provides a glimpse of future localization efforts.

In "Radio Frequency Toolbox for Drone Detection and Classification", Abdulkabir uses features of RF transmissions such as modulation scheme and signal energy to detect and classify drones. To detect the drone, a module searched for RF energy. At greater than 50 meters, 56 percent of drones were detected. Only under excellent signal to noise ratio conditions would the drone be detected. To classify the drone, radio frequency data was fed to a machine learning algorithm. However, the classifier struggled to accurately classify certain brands of drones (Bello, 2019). Radio frequency signals are hard to detect at range and are highly dependent on the strength of the transmitter. A low powered transmitter will not have super far range, but will also be harder to detect. In general, consumer drones' transmissions will be able to be detected accurately at up to 50m (Guvenc et al., 2018). With higher signal strengths, this distance will increase. In order to triangulate the signal of a drone and it's operator, a system will need to have line of sight. Without it, the system would have to follow radio reflections which is a complicated and inaccurate process.

There are a number of shortcomings in the current literature. For one, there is a severe lack of research done in attribution. Of the papers listed above, only one explores localization methods to any extent. Two, there is a strong dependence on radio frequency for drone detection. In high RF environments, these approaches will struggle.

Research Design and Methodology

This research sought to localize a drone operator in a real world environment. As such, the research design follows a experimental structure. First, we will describe the design and overall structure of the system. Second, we will cover data measurement and paths for analysis of that data. Third, we will discuss the procedures of the experiment.

Design

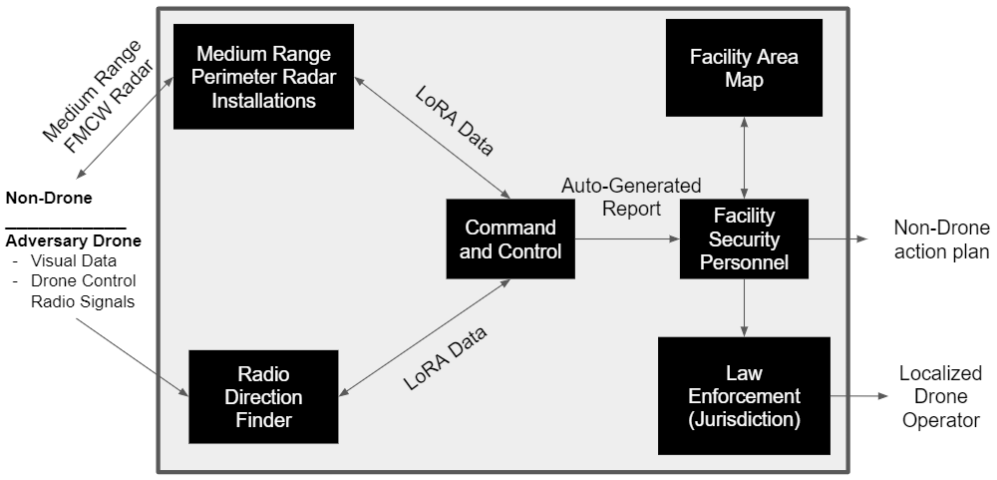
This system is designed to localize the operator of a drone. To do this, there are three main parts of the system that are crucial to its success: radar and radio direction finder arrays and a central command and control server.

The radar array will take the form of several arrays of frequency modulated continuous wave (FMCW) radar. This allows for accuracy and detail over longer ranges while still keeping costs relatively low, as well as allowing for radar to be used in a mix of different weather conditions. These radar arrays will be placed equidistant from each other with minimal coverage overlap. They will be used to detect airborne drones and will relay that location information back to a central command and control (C2) server via long range networking protocol (LoRa).

Radio direction finders will be placed with enough density to allow for triangulation of a radio signal, but far enough apart to allow for minimal coverage overlap. Triangulation will allow the system to get a location for different radio transmissions, regardless of whether or not the channel is encrypted. The radio detectors send radio frequency, modulation, and triangulation data back to the C2 over LoRa.

Figure 1

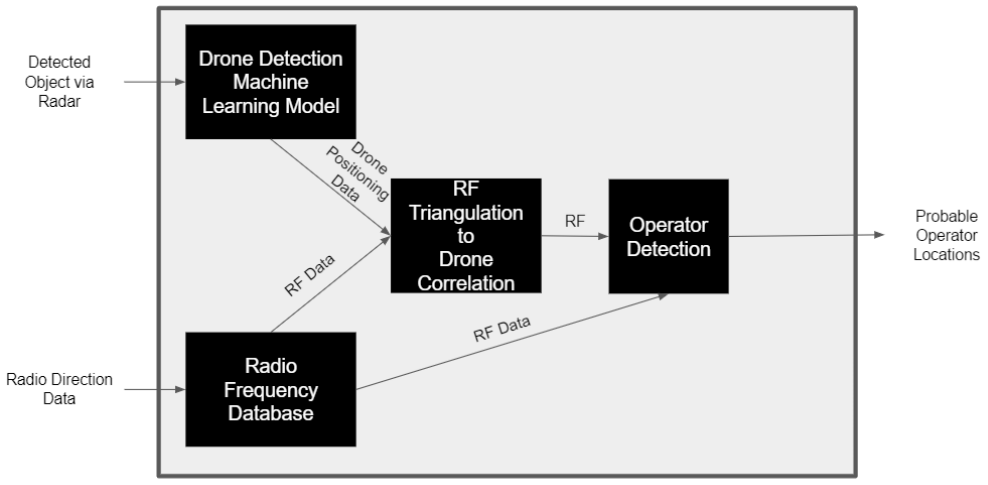
Layer 2 of the S.O.D.A. Black Box



The C2 in an integral part of the system. It will process all the data collected by the sensors, and forms the core of the system. As radar data is collected by the C2, it will use a machine learning model to detect drones. This eliminates the need for a human radar operator. The RF triangulation data is sent to a central RF database. When a drone is detected, its position is continuously sent to a "RF Triangulation to Drone Correlation" algorithm. The algorithm will query the RF triangulation database for location data that is close to where the drone is located. This is done to attribute a radio frequency to the drone. As the drone moves, the database query is done multiple times, confirming the frequency and also uncovering patterns of frequency hopping if applicable. The algorithm has now discovered what frequency the drone is on. The RF database is then queried again on that specific frequency. The list of frequencies returned provided probable locations of the drone operator. By using a map of the surrounding area, facility security can further reduce the likely locations and send law enforcement.

Figure 2

Layer 3 of the S.O.D.A. Black Box



Data Measurement & Analysis

There are a several quantitative metrics of note in each part of the system. Radar metrics are the maximum effective range, the number of objects that can be simultaneously tracked, and the minimum size of tracked objects. The maximum effective range of the radar, measured in meters, is the range at which the radar can effectively detect drone sized objects. This is important as sensors need to be spread out far enough to reduce over lap, but close enough that there are no gaps in the radar screen. The number of objects that can be tracked simultaneously will be measured in units. Due to the future threat of drone swarms, new tracking systems must be capable of tracking multiple objects at once. The size of the trackable drone will be measured in centimeters. Radar has difficulty tracking small objects. As drones get smaller, they will become increasingly harder to detect and track. In terms of the machine learning model for the radar, accuracy, recall, and precision will be measured. These are the standard units of measurement for machine learning models, and offer a glimpse of how good the model is. RF direction finders metrics are the maximum and minimum ranges for detection and triangulation. Reflections of radio signals are not useful to this system. As such, RF direction finders need to have line of sight with the source of the signal. This puts an upper bound on the range of triangulation, measured in meters. The RF location to drone location correlation will be

measured by its accuracy, recall, and precision.

Procedures

The testing performed for the system would fall into four categories: radar, the machine learning model, radio detection and triangulation, and RF location to drone location correlation.

Radar should work in a multitude of different conditions from sunshine to any form of inclement weather. Each test for radar will be done in sunshine, rain, fog, and snow. Using several types of drones, radar detection will be tested at ranges incremented by 250m starting at it's theoretical maximum range and moving downwards. The lower bound of detection will be the assumed max range of the radar system. During this testing, small, commercially available drones will be included in the line up to determine the minimum size of drone that can be tracked at distance. Multiple drones, starting with 3 and moving up to N, will be flown at once in both randomized flight paths and tight formation to ascertain the radar's ability to track multiple objects. Once all this information is collected, it will be split up by scenario and fed into the machine learning model, resulting in the accuracy, recall, and precision for the different scenarios.

Radio direction finders should also work in a multitude of different weather conditions. Similar to radar, the RF direction finders will be tested in sunshine, rain, fog, and snow. Drones and drone controllers have varying transmission power, meaning several different drones will have to be tested against the detectors. In each test, the maximum range of detection will be calculated in three rounds, with the average being taken of the ranges. The lowest average will be the assumed maximum range of radio detection.

As a test of a the entire system, using the maximum ranges found in the previous tests, two sets of tests will be performed against the system to ascertain the accuracy, recall, and precision of the RF location to done location correlation. The first test set will involve a single drone of varying type that will fly into the sensor net and the operator

location will be guessed by the system. In the second test set, a multitude of drones will be flown into the sensor net and the operator(s) locations will be guessed by the system.

Timeline

The timeline for this project is 54 weeks. The first 40 weeks will involve further research and development into the system. Different radar and radio direction finders will require a cost benefit analysis to find the best for the system. A drone radar signature data set will either have to be found or created. The command and control code will need to be developed, as well as the code for integrating with the sensor arrays and the database. The last 14 weeks will be split up into four sections. The first section is four weeks and is dedicated to testing the radar system. The second section is four weeks and will be dedicated to testing the radio direction finders. The third section will also be four weeks and is dedicated to testing the systems as a whole. The final section is two weeks and is dedicated to writing the final report on the system.

Preliminary Suppositions and Implications

This research expanded and refine on the current work available on drone operator localization. While there are several papers on drone detection, tracking, and classification (Bello, 2019)(Coluccia et al., 2020)(Guvenc et al., 2018)(Jarabo-Amores et al., 2018)(Ochodnický et al., 2017), there was only one paper done on the localization of the operator (Nguyen et al., 2019). There is an opportunity to add insight on how to properly localize an operator given a tracked drone.

Theoretical Implications

Existing knowledge about ranges that drones can be reliably tracked and located will be reinforced with both radar and RF. These systems (Guvenc et al., 2018)(Ochodnický et al., 2017) have been seen already. These processes and procedures can

be laid out and refined in this research adding to the duplication of research and refinement of the processes.

Practical Implications

Finally, this system will allow for law enforcement and critical infrastructure security to localize a drone operator and stop repeated drone incursions. Law enforcement will benefit from the ability to stop drone operators at the source and offer a non-drone take down option. In addition, this research will yield a radar data set of drone detection, something that is severely lacking in this field.

Expected Outcomes

We suspect the development and testing of the described system to provide a state of the art drone operator localization system, opening up the area of research for further refinement. In addition, this research would outline how to detect and track drones via radar and RF direction finders.

Conclusion

Throughout this paper, we have discussed how to design and test system for localizing a drone operator. We listed out different technologies needed for such a system: radar, radio direction finders, and a central command and control system. For each part, we went into detail on how to design and develop the part to integrate with the rest of the design. Finally, we detailed how to test the system to learn the optimum ranges and effectiveness of the system.

Drones are becoming more and more popular with the general populace and our adversaries by the day. In addition, drone operator localization is a new area of research with little work being put in thus far. It is heavily important to research ways to localize the operator to stop illegal drone flights in their tracks.

References

Copeland, C. Interview Szafran, D. 2020, September 30.

Bello, A. (2019). *Radio frequency toolbox for drone detection and classification* (Master's thesis). Old Dominion University.

Coluccia, A., Parisi, G., & Fascista, A. (2020). Detection and classification of multirotor drones in radar sensor networks: A review. *Sensors*, *20*(15), 4172. https://doi.org/10.3390/s20154172

de la Baume, M. (2014). Unidentified drones are seen above french nuclear plants. *New York Times*. https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html

Dogru, S., & Marques, L. (2020). Pursuing drones with drones using millimeter wave radar. *IEEE Robotics and Automation Letters*, *5*(3), 4156–4163.

Federal Aviation Administration. (2020). *Uas sightings report*. Retrieved October 12, 2020, from https://www.faa.gov/uas/resources/public_records/uas_sightings_report/

Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine*, *56*(4), 75–81.

Hambling, D. (2020a).

drone swarm' invaded palo verde nuclear power plant last september — twice. *Forbes*. https://www.forbes.com/sites/davidhambling/2020/07/30/drone-swarm-invaded-palo-verde-nuclear-power-plant/

Hambling, D. (2020b). Dozens more mystery drone incursions over u.s. nuclear power plants revealed. *Forbes*. https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/

Jarabo-Amores, M. P., Mata-Moya, D., Gómez-del-Hoyo, P. J., Bárcena-Humanes, J. L., Rosado-Sanz, J., Rey-Maestre, N., & Rosa-Zurera, M. (2018). Drone detection

feasibility with passive radars. *2018 15th European Radar Conference (EuRAD)*, 313–316.

Nguyen, P., Taeho, K., Miao, J., Hesselius, D., Kennelly, E., Massey, D., Frew, E., Han, R., & Vu, T. (2019). *Towards rf-based localization of a drone and its controller.* Retrieved October 12, 2020, from https://www.cs.colorado.edu/~rhan/Papers/2019_DRONET_RF-based_Localization.pdf

Ochodnický, J., Matousek, Z., Babjak, M., & Kurty, J. (2017). Drone detection by ku-band battlefield radar. *2017 International Conference on Military Technologies (ICMT)*, 613–616.

Robson, S., & Kusumoto, H. (2019). Drones buzzed us bases in japan 70 times last year, military says. *Stars and Stripes*. https://www.stripes.com/news/drones-buzzed-us-bases-in-japan-70-times-last-year-military-says-1.571691

United States Navy. (n.d.). Ground/air task oriented radar (g/ator) [https://www.dote.osd.mil/Portals/97/pub/reports/FY2013/navy/2013gator.pdf?ver=2019-08-22-111215-033].

U.S. House of Representatives. (n.d.-a). 18 u.s.c. 32 [https://www.law.cornell.edu/uscode/text/18/32].

U.S. House of Representatives. (n.d.-b). 49 u.s.c. § 40102(a)(6) [https://www.law.cornell.edu/uscode/text/49/40102].