Aerial Swarms as Asymmetric Threats

Stephen Wilkerson, Christopher Korpela, Kevin Chang, Andrew Lee, Andrew Gadsden

***Abstract*— Despite being unmatched on the battlefield or at home, low-cost, asymmetric threats have proven dangerous for U.S. military forces and homeland security. The proliferation of improvised explosive devices of all types in the Iraqi and Afghan theaters has demonstrated that inexpensive, commercial off-the-shelf technology and some electronics knowledge can be combined to significantly impact high-tech operations. Autonomous GPS-guided and semi-autonomous unmanned aerial vehicles will change the paradigm in their employment in the very near future. While a single attack might be insignificant, a swarm of robotic devices could prove a credible threat. In this paper we discuss the impact and limitations of commercially off-the-shelf drones and what measures might be used to counter these devices. We back up our findings with flight tests and observations on systems commonly used for research but also easily available to adversaries and bad actors. Finally, we present some speculation on the potential implementation of swarms using these vehicles as a continuation to the discussion.**

I. Introduction

Radio controlled aerial vehicle usage among hobbyists, researchers, and commercial entities have grown substantially in the last decade due to improvements in the cost, weight, and performance of the components used to construct them. In particular, there has been an explosion of improvements in motor technology, lightweight high-energy batteries, and microelectronics. These advancements have led to radio controlled aerial vehicles capable of speeds greater than 60mph and a variety of every size. Brushless motors have several advantages over brushed DC motors. These motors include higher torque to weight ratios, increased efficiency, increased longevity, and better reliability. Furthermore, since the motors windings are supported by the housing, they can be cooled by conduction. This configuration requires only airflow over the motor housing for cooling. Therefore, the internal parts can be isolated from dust and moisture. The cost of these motors, in particular smaller systems, has been drastically reduced in the past 10-15 years [1].

Battery technologies have also been increasingly improving during this same period primarily due to the need for extended life and performance of cell phones and mobile devices. Lithium-based batteries have shown the greatest improvement. Lithium is the lightest of all metals, has the greatest electrochemical potential, and provides the largest specific energy per weight. From iron phosphate to nickel manganese cobalt oxide, there are many types of lithium ion batteries in use today. They are one of the most popular types of rechargeable batteries for portable electronics, due to their high energy density, small memory effect, and slow loss of charge. Furthermore, lithium-based batteries are being used heavily by the military. Due to their popularity and demand in numerous industries, lithium-based batteries have dropped in cost and increased in capacity by an order of magnitude in the past 10 years [2].

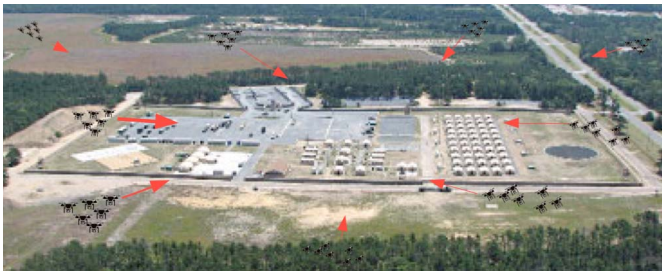


Fig. 1: Concept showing an aerial swarm attack on a fixed installation.

Finally, microelectronics and the software controlling them has drastically changed in recent years. The open source software community continues to expand rapidly. The nature of the open source software and maker communities has produced software and electronic components that can be easily combined creating new capabilities. Control algorithms, GPS way-point navigation techniques, path planning, feature detection, obstacle and collision avoidance methods are easily downloaded and implemented on commercial off-the-shelf (COTS) aerial vehicles [3], [4].

The combination of these critical new technologies has led to a boom of recreational hobby, research, and private industry vehicles at extremely low prices. Open source and open architecture software can now readily be found on the Internet allowing sophisticated control of these devices beyond tele-operation. Moreover, these devices can be controlled beyond the line of sight and without direct human input through simple point and click programming operations and the use of GPS devices. Another interesting development has been in the use of First Person View (FPV) capabilities that enable a relatively untrained pilot or operator to control devices as though they were actually on board flying them. These new capabilities have led to concerns by the FAA

Manuscript received May 5, 2016. This work was supported in part by the Army Research Laboratory and the U.S. Army Tank Automotive Research, Development and Engineering Center (TARDEC). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government, ARL, or TARDEC.

S. Wilkerson is with the Army Research Laboratory, Aberdeen, MD 21005 USA stephen.a.wilkerson.civ@mail.mil

C. Korpela is with the United States Military Academy at West Point, NY 10996 USA christopher.korpela@usma.edu

K. Chang, A. Lee, and S. A. Gadsden are with the University of Maryland Baltimore County, Catonsville, MD 21250 USA gadsden@umbc.edu

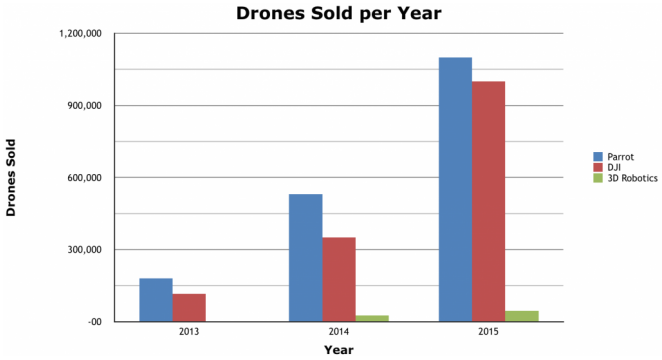


Fig. 2: Estimated sales of popular drones (i.e. quadcopters) [7].

and other organizations restricting flying zones and areas of use. Additionally, the FAA is now requiring licensing of unmanned aerial vehicles weighting more than a half pound with strict penalties and fines to enforce the regulation. For example, the airspace near the Washington, DC corridor currently has a restriction of 30 nautical miles where unmanned aerial vehicles cannot be used. Not surprisingly, there are similar restrictions near airports and other key installations in the United States. Quadcopters crashing into the lawn of the White House or harassing commercial aviation pilots at airports are just a few recent examples [5], [6].

The U.S. military already has a suite of unmanned vehicles that have been taking advantage of some of these new capabilities. However, most of these military hardened vehicles are hugely expensive while having some of the same limitations of their inexpensive counterparts. Moreover, some of these systems require extensive training to operate and train personnel to maintain them. Whereas, many of the commercially available systems can be operated by the novice and repaired by untrained personnel. The proliferation of drones (a typical designation used to describe unmanned aerial vehicles and can often be a polarizing word) in the United States has grown significantly in the past three years. It was estimated in a recent article that several million drones have been sold by the leading manufacturers, DJI, Parrot and 3D Robotics in 2015 (Fig. 2) [7].

What we hope to do in this paper is to examine some of the drone capabilities and limitations now available to our adversaries and further the discussion of how we might prepare for the use of these devices in ways unintended by their manufacturers. Wired magazine reported that the Department of Homeland Security pitted $5,000 worth of drones against a convoy of armored vehicles and the drones won. The article further reported that Syrian rebels are importing consumer-grade drones to launch attacks [8]. We begin with various scenarios on how an aerial swarm attack may occur. Next, we introduce some possible countermeasures in defending fixed or moving assets. For this particular work we will focus on two inexpensive multi-rotor systems widely used by hobbyists and in research, namely the DJI Flamewheel 450 and the 3D Robotics DIY X4. By examining these

Fig. 3: Intel Drone 100 record breaking aerial swarm.

systems from a research perspective where implementations are readily available on-line, we can estimate the potential capabilities an adversary would possess to carry out an attack. For the purposes of this discussion, a number of flight experiments were performed and the data from these experiments is presented.

II. State of the Art in Aerial Swarms

The field of aerial swarms has seen great advances just in the past few years with movement from out of the laboratory environment to outdoor experiments with tens of vehicles. In January 2016 at the Consumer Electronics Show in Las Vegas, NV, Intel set the Guinness World Record for most UAVs airborne simultaneously when it debuted its Drone 100 accomplishment. Each pilot (a total of 4) controlled 25 UAVs that lifted off from a soccer field. Engineers created custom software to coordinate the flight paths, synchronize the lighting, and move in formation with the orchestra music (Fig. 3) [9]. The Naval Postgraduate School successfully launched 50 simultaneous fixed-wing UAVs. The Navy is currently testing launching drones out of a tube-based launcher where up to 30 drones could be deployed in one minute. The program is called LOCUST (Low-cost UAV Swarming Technology) and will include armed and unarmed versions that can join together, break apart, and conduct missions individually, collaboratively, and spontaneously [10].

Drones 100, the NPS ARSENL demonstration, and the Navy LOCUST project represent a few examples in the state of the art in swarm autonomy. And we are just at the beginning in developing swarms. These same factors that allow almost anyone to build a flying camera for under $100 will enable 1000s and tens of 1000s small to medium sized drones simultaneously controlled by a single operator in the next 10 to 20 years. The commercial sector is already poised to leverage these technologies to provide goods in under 30 minutes (probably most famously is Amazon's desire to deliver goods using UAVs). We are only a year or two away from a user clicking on an item and then having it delivered on their back porch without a single human involved in the process.

III. Aerial Swarm Attack

One aim of this paper is to further the discussion of the threat posed by COTS hobbyist aerial vehicles by investigating what risks these devices pose and how might

we counter these concerns using the technology that exists without forbidding the continued development of unmanned systems. So what risk does a swarm of small inexpensive drones pose now and in the future? So let us speculate that with the current state of the art of 100 simultaneously-controlled drones, each armed with a small explosive device, were all converging on a location from just over a mile away. Could such a coordinated attack be repelled? Certainly GPS jamming would eliminate the threat in this case, but it would also need to be active and have a perimeter large enough to deny access to the entire area. It would also deny GPS to users within that area. Moreover, who determines where GPS jamming is used and not used and what areas are then secure and what areas are left unprotected.

For the military, this scenario poses a real problem in the near future. Would a low-tech enemy be able to coordinate such an attack using store bought drones? From our experiments here and knowledge of the market and technology, we believe the answer is absolutely yes. For completeness, we examine two potential scenarios involving a Forward Operation Base (FOB): one with GPS-guided drones and a second scenario with FPV tele-operated drones. Another aspect of this issue is if the adversary could conduct such an attack with impunity. In other words, is it possible to engineer an operation where retaliation is not only unlikely, but unrealistic.

A. Scenario 1: FOB under attack from 25 or more GPS-guided COTS drones

Piloting small, traditional RC fixed-wing or rotary-wing aircraft is no simple task. Typically, most RC pilots will tell you that it takes a season to become competent with an RC aircraft. An unseasoned pilot will find frequent crashes, repairs, and frustration while learning to fly. However, drones and in particular quadcopters offer a new capability. The autopilots that have been incorporated into these small drones make it possible for almost anyone pilot these aircraft with less of a chance of crashing. Moreover, with the use of GPS, the pilot is taken out of the loop with the chance of crashing becoming less likely. RC drones typically have a fair amount of excess lift capability allowing them to be loaded up with additional payload. Be that as it may, as these drones become heavier they tend to lumber rather than flying quickly and nimbly. A single drone flying at 5 mph is unlikely to pose a large risk to a facility. In order for these drones to fly faster they need to remain light which will restrict their range and payload. This trade-off will, in the near future, limit the utility of purchasing an off the shelf ready to fly drone capable of delivering a large explosive payload. For our scenario we are not concerned as much with the single drone but rather a swarm of drones that might arrive at a location at the same time. While most of these COTS drones contain point and click capabilities on a map, coordinating multiple drones from multiple locations will prove to be technically more difficult. Despite these limitations it is not difficult to envision multiple drones being launched simultaneously and arriving at a location relatively quickly at about the same time. The overarching restrictions for someone launching this type of attack will be the speed at which they fly, the distance from which they are launched, and the payload that they will be capable of carrying.

B. Scenario 2: FPV Attack using pilots to manually fly vehicles

Flying into a location using the first-person view offers a number of advantages and disadvantages over a GPS-guided attack. For instance, the pilot or pilots can fly to whatever target they choose. Likewise, they can fly slowly to the target conserving power and then use all the reserves with a high speed sprint to the target. This scenario offers a new set of technical and personnel challenges, namely training a pilot or pilots to accomplish the task. The technical challenges will be coordinating frequencies, video channels, and ranges for the FPV camera and goggles. Currently, only a couple of FPV pilots can fly at a time with commercially available FPV frequencies. This limitation is why FPV racing typically only allows 3 to 5 racers at the time. With the available frequencies it is easy to interfere with someone else's frequency with a video transmitter thereby rendering the pilot blind in mid-flight. Furthermore, training multiple pilots requires significant time and investment. During a recent series of STEM events, we attempted to train pilots to fly small drones in FPV mode. This exercise was conducted over an eight-week period with five different groups of approximately 30 students. While some success was obtained, by and large most of the pilots were incapable of consistently controlling the drones after a week of training and flight simulation. Moreover, when flying the actual drones numerous crashes were recorded. Just the same, in every control group there always seem to be several students with superior capabilities who were capable of flying the drones by the end of the week. Therefore, this scenario is possible, but probably unlikely for coordinating swarms of vehicles at this time.

IV. Swarm Countermeasures

Key to any countermeasures will be the ability to detect any UAV system within a given perimeter. This detection is particularly difficult for terrain nap of the earth type vehicles like a drone. However, The Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System, (JLENS) has shown the ability to track boats, ground vehicles, cruise missiles, manned and unmanned aircraft with some success. Nonetheless, these systems need to be deployed. For ground based systems the task is made more difficult if the vehicle is flying slow and low. Distinguishing this vehicle from a bird may prove to be very difficult, but electronic noise signatures may provide the key. In the near term and with COTS hardware, the systems mode of attack will be very limited (as discussed, GPS-guided or flown in by remote control). In the former mode, one needs only to detect the aircraft at a reasonable range and jam the GPS signal. In the later, there are only a number of frequencies commercially available that can be used to pilot a system. These frequencies can easily be detected and jammed as well. Most systems available to the

commercial public are broadcasting at a low output power (0.1 to 1 watt) and have a limited range (1-3 miles). There are also only a couple of frequencies that need to be considered for COTS hardware. Moreover, beyond line of sight or over the next hill will drastically reduce the range. Such systems will give off a signal that is easily detected and could be countered. It will be important for the military to put in place devices that can detect and counter these low flying systems before they arrive undetected. In doing so the complexity of using them effectively will greatly reduce the threat from a low-tech terrorist [11], [12].

V. Experimental Results

It would virtually be impossible to write a report that accurately addressed every variable in any given drone. What we attempt to do here is to provide a baseline set of tests from which to build additional tests to look at individual parameters governing specific drone baseline performance, characteristics, and capabilities. Clearly when we add additional batteries we can extend the mission of the drone in terms of time in the air and distance traveled. However, in doing so we reduce the effective payload of the drone while also increasing the energy demands from the batteries. Additionally, the added weight will effect the speed at which the drone can fly. We choose as our two test drones standard do it yourself (DIY) systems from 3D Robotics and DJI. Both are of similar size (~500 mm) and we use the Pixhawk flight control unit to navigate under GPS control during the tests. The 3D Robotics system has a sturdy metal frame and slightly larger motors leading to slightly greater demands on battery power and less performance in terms of time in the air. Our two baseline systems are shown in Fig. 4. Both are capable of carrying several pounds of additional weight without over burdening their respective power plants.

Widely popular with a large user community, the Pixhawk is an advanced autopilot system designed by the PX4 open-hardware project and manufactured by 3D Robotics. It includes an advanced processor and sensor technology from ST Microelectronics and a NuttX real-time operating system. The Pixhawk offers the flexibility and reliability for controlling any autonomous vehicle for the applications in this work. The Pixhawk system includes integrated multithreading, a Unix/Linux-like programming environment, completely new autopilot functions such as Lua scripting of missions and flight behavior, and a custom PX4 driver layer ensuring tight timing across all processes [13]. These features allow for the flexibility needed to conduct surveillance and reconnaissance experiments in a GPS environment as well as GPS denied ones.

Other parameters within our control effecting the quadcopter's performance are listed here as well. There are numerous parameters that affect the overall performance of these two quadcopters. In fact they are too numerous to mention them all, nonetheless, we will discuss a few. The pitch and size of the propellers are related to the amount lift, motor speed, overall speed, and amount of energy it will use. Many of these parameters are understood well enough that they can be estimated without testing. Additionally, the motor size and speed control size coupled with these parameters will determine some of the performance characteristics of a particular system. However, one of the parameters that is not fully understood for any given system is the overall time limitations imposed by speed, transitional lift characteristics, and wind speed. Therefore, in our baseline test we examine both of these quadcopters flying the exact same mission at different speeds with little or no wind speed. Furthermore, we conduct these tests with a stripped-down version of the quadcopter eliminating energy use from video transmitters cameras and other devices that might skew our results.

Fig. 4: A common COTS quadcopter widely used in research and by hobbyists.

Fig. 5: 1500 feet long flight path plan to maintain speed and altitude.

A. Multi-rotor Experiments

For our initial experiments we examine a standard 3D Robotics quadcopter that uses the Pixhawk autopilot system and ArduCopter/APM firmware. The quadcopter was stripped of excess weight and power drains like cameras, telemetry, and video transmitters. The flight body weighed 1.875kg and the 4000mA batteries used in the experiments weighed an additional 420g. As with any system there are numerous choices for propellers, motors, and speed controllers that all have some effect on efficiency, duration of flight, and energy use. For these experiments we use the baseline 3D Robotics system with 11-4.7 APC propellers (shown in Fig. 4). Experiments were conducted at each condition to include: hover, 1-3-6-9-12-15 m/s, and 20 m/s. Each of these tests was repeated three times to assure repeatability of the results. The flight path was approximately 1500 feet long allowing the aircraft to maintain speed and altitude for an extended period (see Fig. 5).

For this initial estimate of power consumption, 23 flight tests in all were conducted ranging in time from ~10 minutes to under 3 minutes. During these tests the wind was gusting between 3 and 9 mph leading to some transitional lift

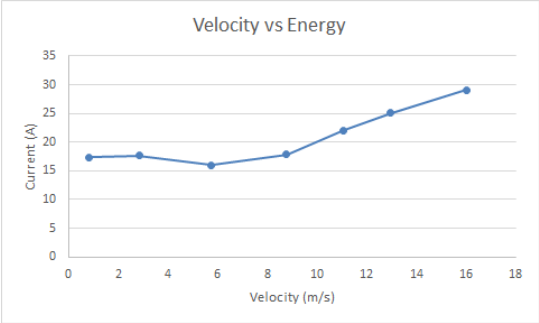


Fig. 6: Transitional lift experiments on 3D Robotics quadcopter baseline system.

during the hover condition. Nonetheless, throughout most of the testing the steady wind speed were near zero. Tests were done at 40m altitude above a flat and level field with temperatures varying between 40 and 48 degrees Fahrenheit. The results are summarized in Figs. 6 and 7. The first, Fig. 7a, shows a typical velocity profile for 12 m/s as the drone traversed its course. In particular, the flight would have an up leg portion where it would fly to the head of the field and position itself at the proper altitude. Afterwards, it would turn and fly at constant velocity and altitude for just over a quarter of a mile. This allowed us the opportunity to have consistent data taken at a specific altitude and speed for a period of time. As can be seen in Fig. 7a, a circle indicates the portion of the flight where the data was analyzed from. Additionally, we duplicated each flight and path on three separate occasions to show repeatability of the data. Fig. 7b shows the flight path for two flights at 3 m/s and is obvious that the data is near identical in each flight. Fig. 7c shows the same for 12 m/s and once again the data where the data taken was extremely consistent. In all of these figures, time of start might be shifted slightly due to start times and ending times, one can easily pick out the areas where we were taking data from. Furthermore, the data was taken from numerous parameters, one of which was altitude and in Fig. 7d it can once again be seen that the aircraft holds the near perfect altitude of approximately 40m above the surface. For comparison the velocity plot from the same flight is shown underneath in Fig. 7d as well. Finally, we show the current draw during the flight for that same 12 m/s flight. Since the wind velocity was all but zero with light gusts during the flight the data across all the parameters was extremely consistent. This will enable us to examine other parameters of the flight and their effects on battery life, mission length, and other items of interest as influenced by some of the quadcopter's design parameters.

The results indicate that we will be using a quadcopter with a range of energy needs between 16 and 30 amp hours. The drain on the battery will ultimately affect the overall time the quadcopter could spend in the air and it is well know that drain rates also effect the overall energy available from a lithium polymer battery. At slower speeds these quadcopters will be seen and heard well before they arrive at a location. At the higher speeds they are less likely to be detected and more difficult to counter. For both of these quadcopter speeds, it is quite conceivable that they could travel several miles under GPS control to a target and deliver a substantial payload. Moreover, with the inclusion of FPV technologies, these systems could also deliver a payload under tele-operation control from out of direct line of sight.

VI. Conclusions

It is important for the Army to recognize an aerial swarm attack vector and to develop countermeasures to protect against it. Hardware for these attacks is readily available and the software is easy to find in the open-source community. Together, these elements create an opportunity for future opponents to attack us at home and aboard despite our technological advantage. To understand the threat and prepare for it, it is necessary to survey the threat devices and software and then develop a plan to mitigate them.

VII. Acknowledgments

The authors would like thank the students at the University of Maryland Baltimore County for their work on conducting the flight tests.

References

[1] R. E. Mahony, V. Kumar, and P. Corke, "Multirotor aerial vehicles: Modeling, estimation, and control of quadrotor," *IEEE Robot. Automat. Mag.*, pp. 20–32, 2012.

[2] B. A. Johnson and R. E. White, "Characterization of commercially available lithium-ion batteries," *Journal of Power Sources*, vol. 70, no. 1, pp. 48–54, 1998.

[3] H. Chao, Y. Cao, and Y. Chen, "Autopilots for small unmanned aerial vehicles: a survey," *International Journal of Control, Automation and Systems*, vol. 8, no. 1, pp. 36–44, 2010.

[4] H. Lim, J. Park, D. Lee, and H. J. Kim, "Build your own quadrotor: Open-source projects on unmanned aerial vehicles," *Robotics & Automation Magazine, IEEE*, vol. 19, no. 3, pp. 33–45, 2012.

[5] S. Maddox and D. Stuckenberg, "Drones in the us national airspace system: A safety and security assessment," *Harvard Law School National Security Journal, Online: http://harvardnsj.org/2015/02/drones-in-the-us-national-airspace-system-a-safety-andsecurity-assessment*, 2015.

[6] D. Sathyamoorthy, "A review of security threats of unmanned aerial vehicles and mitigation steps."

[7] A. Amato. (2015, April) Drone sales numbers: Nobody knows, so we venture a guess. Online. Dronelife. [Online]. Available: http://dronelife.com/2015/04/16/drone-sales-numbers-nobody-knows-so-we-venture-a-guess/

[8] K. Poulsen. (2015, February) Why the us government is terrified of hobbyist drones. Online. Wired. [Online]. Available: http://www.wired.com/2015/02/white-house-drone/

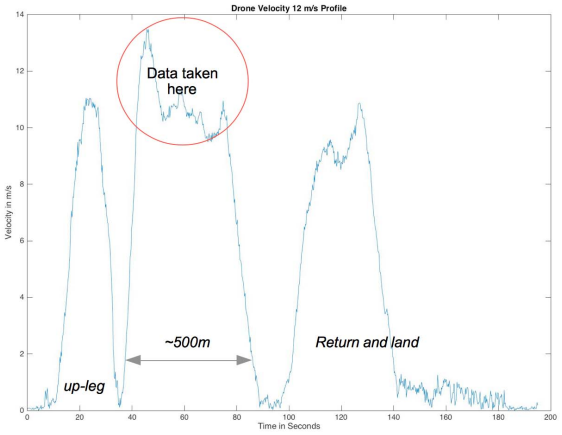
[9] A. Justice, "Ces 2016: Intel set new world record for synchronising 100 drones with live orchestra playing beethoven's fifth," *International Business Times*, 2016.

[10] P. Tucker. (2015, April). [Online]. Available: http://www.defenseone.com/technology/2015/04/navy-preparing-launch-swarm-bots-out-cannons/110167/

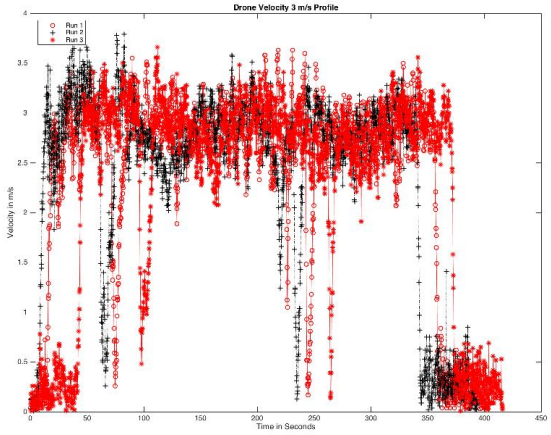
[11] C. Bolkcom, "Potential military use of airships and aerostats." DTIC Document, 2004.

[12] W. L. Myrick, M. D. Zoltowski, and J. S. Goldstein, "Low-sample performance of reduced-rank power minimization based jammer suppression for gps," in *Spread Spectrum Techniques and Applications, 2000 IEEE Sixth International Symposium on*, vol. 1. IEEE, 2000, pp. 93–97.

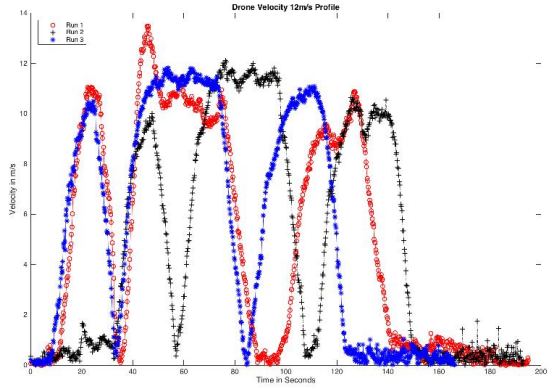
[13] www.3drobotics.com.



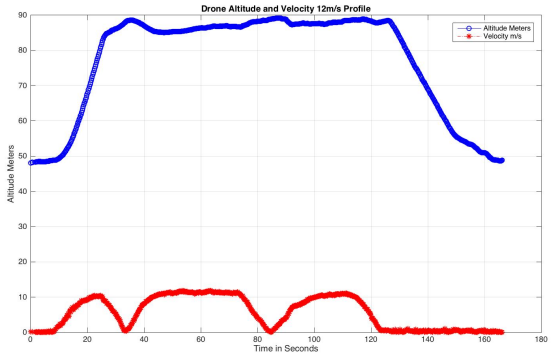
(a) Drone velocity at 12 m/s.



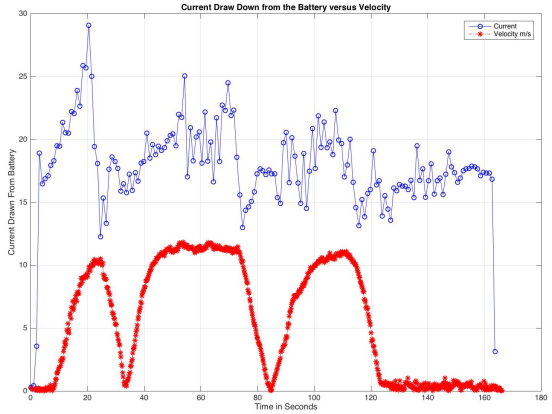
(b) Drone velocity at 3 m/s.



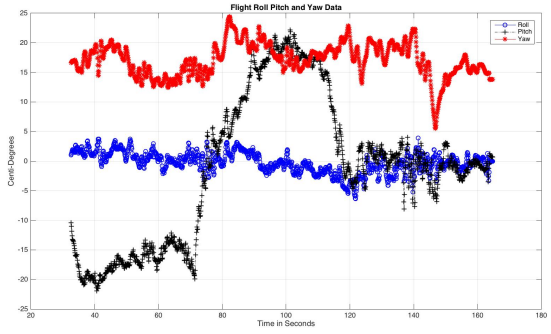
(c) Drone velocity at 12 m/s.



(d) Drone velocity at 12 m/s.



(e) Current draw down from the battery versus velocity.



(f) Flight roll, pitch, yaw data.

Fig. 7: Flight results.