Realization of an Autonomous, Air-to-Air Counter Unmanned Aerial System (CUAS)

James M. Goppert[1], Amy R. Wagoner[2], Daniel K. Schrader[2], Shiva Ghose[2], Yongho Kim[2]
Seongha Park[2], Mauricio Gomez[2], Eric T. Matson[2], and Michael J. Hopmeier[3]

***Abstract*— The proliferation of small Unmanned Aerial Systems (UASs) has led to a security gap in the defense of strategic installations and at public events. One of the most proven and low-regret methods employed by Counter Unmanned Aerial Systems (CUASs) is entanglement of the hostile UAS in a net carried by a hunter UAS. Typically these hunter UASs are controlled by a human pilot. We employ a ground based RADAR system for tracking the target UAS and command the hunter UAS to follow the target UAS, using the Robot Operating System (ROS), the MAVLink protocol, and the PX4 autopilot. This system is fully autonomous, which reduces cost and response time when compared to human-in-the-loop systems. In addition, a novel cylindrical net design is presented. We demonstrate the system's effectiveness through field testing.**

I. Introduction

In the last few years, several high profile events have been interrupted by small scale Unmanned Aerial Systems (UASs), commonly referred to as drones. In September of 2013, a man flew a UAS in front of the German chancellor during a campaign event [1]. Two years later, in January 2015, a hobbyist unwittingly flew his DJI Phantom over the highly restricted airspace near the White House and crashed it on the ground [2].

Fortunately, there were no personal injuries or damage in either of those cases. However, as a direct result of those incidents and more, world governments realized that there are a lack of security protocols in place for such small, yet potentially dangerous, threats. In both of the aforementioned cases, the UAS operators had no ill-intent. Yet, as UASs become more innovative, so too might the threats. The fear that UASs will be used for more nefarious purposes, causing severe risk to life and property, is legitimate.

Most of the threat of UASs being used for malicious purposes stems from the fact that these small systems are very difficult to detect. Small UASs are nearly impossible to see with a naked eye from long distances. Anti-aircraft systems that are built specifically for detecting objects in the sky are typically specialized to detect much larger objects or smaller objects moving at much faster speeds. These detection systems, similar to the ones used by the White House, cannot detect small, slow moving UASs [3]. Smaller detection systems have difficulty distinguishing UASs from small birds or other small, slow moving objects in the sky. Furthermore, small UASs are typically flown at much lower altitudes than standard aircraft. Anti-aircraft weaponry pointed at such low altitudes is not only ineffective at countering very small UASs, but also becomes an immediate danger to any people in the area. Similarly, if the UAS has a volatile payload, any destructive counter-measure may cause the UAS and its payload to drop into an undesirable area. An ideal solution to the threat of UASs must be low-regret, meaning that as few people as possible are alarmed or put in harm's way when taking down the threat.

A. Regulatory Reaction

In February 2015, the Federal Aviation Administration (FAA) in the United States established new regulations and policies for UASs [4] in an effort to reduce the number of negative incidents involving UASs. The regulations require UAS pilots to remain within visual line of sight of a UAS and under a ceiling of 500 feet. In addition, the Department of Transportation and the FAA require UAS registration [5], which mandates that UAS operators obtain an electronic certificate of registration and personal universal registration number for use on all UASs. However, these regulations are controversial as they do little to directly prevent the malicious use of UASs, and they disallow many legitimate UAS applications (i.e. long range autonomous package delivery).

The U.S. Department of Defense (DoD) categorizes UASs into five groups [6]. The threats we are attempting to mitigate with this research are limited to Group 1, which contains vehicles analogous to radio-controlled model aircraft (low cost, low weight, and low speed). Since most people only have access to vehicles belonging in Group 1, current counter UAS efforts are focused on countering threats of this type and magnitude.

II. Related Work

Academic and industry professionals have worked simultaneously in an attempt to address the CUAS problem [7], [8]. The maker of the most popular commercially available UAS, DJI, has developed proprietary software for their on-board autopilots that prevents (with unproven reliability)

[1]James M. Goppert is President of JMG Robotics, LLC, is a member of the M2M Lab in Computer and Information Technology at Purdue University, and with the School of Aeronautics and Astronautics, Purdue University, West Lafayette, IN 47907, USA. jgoppert@purdue.edu

[2] Amy R. Wagoner, Daniel K. Schrader, Shiva Ghose, Yongho Kim, Seongha Park, Mauricio Gomez, and Eric T. Matson are members of the M2M Lab in the Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47907, USA. {arwagone, dkschrad, shivaghose, kim1681, park708, mgomezmo, ematson}@purdue.edu

[3]Michael J. Hopmeier is President of Unconventional Concepts, Inc., Mary Esther, FL 32569, USA. hopmeier@unconventional-inc.com

978-1-5090-6724-4/17 $31.00 © 2017 IEEE
DOI 10.1109/IRC.2017.10

their UASs from flying into restricted air space, such as airports and government facilities [9]. However, such software can easily be disabled or hacked into, rendering these safety protocols useless. Furthermore, there are several open-source autopilots available, which enables users to disable or ignore any safety features, making reliance on known safety protocols a poor security solution.

In response, several companies have begun developing CUAS solutions [10]. However, some of these offerings are only one piece of what needs to be an end-to-end solution. Boeing released footage of a high energy laser destroying a UAS [11]. While very effective in destroying the threat, a focused energy beam is not low-regret. To be effective, such a device would need to be "laser-accurate." Aiming the device too low may result in property damage, or worse, human injury or death. Aiming the device skyward presents the risk of the beam unintentionally striking a manned aircraft. Even if the beam struck only the UAS, any hazardous cargo may be ignited or dispersed, or the beam could reflect off the UAS in an unpredictable direction.

DroneShield has developed a sophisticated acoustic sensor that detects several of the most common UASs, based on their expected sound signature (which may be different if the UAS is carrying a payload [12]). Due to the nature of acoustic detection, noisy environments or tree covet can significantly reduce the detection accuracy. When a UAS is detected, DroneShield only notifies authorities and does not engage the UAS with any counter measures [13]. The flaw with this approach is that by the time authorities can react, a malicious UAS has likely already completed its mission.

Airbus recently announced an autonomous CUAS solution that uses RADAR, infrared cameras, and directional sensors to detect small UASs [14]. Once the UAS has been detected, the countermeasure, which is a radio and GPS signal jammer capable of operating up to 10 kilometers away, attempts to disable the UAS. The weakness of this approach is the assumption that any incoming UAS will be radio controlled or on a GPS-reliant autopilot mode. While those may be valid assumptions most of the time, signal jamming alone will not stop many UASs from entering restricted space. Jamming radio signals only stops UASs that are manually controlled. Jamming GPS signals, aside from being problematic at locations like the White House, will force only some UASs to stop and/or return to the original location. Other UASs, when GPS signal is lost, will simply continue on the course they were on before the signal was interrupted [15]. In addition to these issues, the FAA does not allow any sort of signal jamming in the US [10].

Academia is also contributing pieces to the UAS defense puzzle. RADAR is emerging as one of the primary methods of UAS detection [16]. The authors of this paper have developed a very low-cost, low-power RADAR that is capable of detecting UASs at short range (around 10 meters) [12]. Additionally, air-to-air combat for neutralization of undesired UASs is an active area of research. While some researchers are focusing on autonomous maneuvering of the UASs [17], [18], most of the work is focused on human-in-the-loop air-to-air combat solutions, specifically countering UASs with nets. Kaist University in South Korea has developed a human-in-the-loop solution that employs a small team of UASs that attempt to catch the target UAS in a small, circular net [19]. Once the target UAV is on the ground, an Unmanned Ground Vehicle is released from an additional UAS with explosives to neutralize the target, which is not low-regret. Michigan University has released footage of their DroneCatcher, which is a manually controlled UAS with a one-shot net gun attached [20]. Delft Dynamics has also released a similar system [21].

The research presented in this paper attempts to overcome these limitations by:

- Using a cylindrical net with a large cross-section at any angle of approach.
- Using open-source hardware and software to make the system simple to implement and adapt.
- Making the system fully autonomous from detection to neutralization.
- Developing a simple predictive control law for air-to-air interception.

III. System Description

In early 2015, the USA Federal Government immediately identified a direct threat after a UAS landed easily on the lawn of the White House. After this incident, a challenge was put forward for a limited number of research groups to solve the problem of dangerous drones. This research is a direct result of this challenge to develop and demonstrate the first end-to-end, autonomous, low regret, cooperative counter-UAS (CUAS) ever. The system was designed to detect, track, and kill UAS-sized targets at ranges up to 500 meters, and do so without relying on easily defeated or unreliable approaches, such as RF detection or signal jamming. The system, designed, developed, and fielded for operational assessment, was completed in 90 days. It consisted of a high-precision RADAR, a purpose designed net entanglement system, and an air-to-air attack UAS, and a ground station, all functioning as components of the CUAS.

The hunter UAS used in this experiment was a 3DR Iris+ UAS, equipped with a Pixhawk flight controller running the open-source PX4 autopilot firmware [15]. The Iris+ is an inexpensive, consumer-grade UAS that is powerful enough to overtake many of the most common consumer UASs, even while carrying the large net seen in Fig. 2. The Pixhawk is an open-source hardware platform that is capable of running several different flight stacks (i.e. firmware).

An overview of the CUAS is shown in Fig. 1. Robot Operating System, or ROS [22], was used as a message broker to facilitate communication between the subsystems. The RADAR tracked the target UAS and continuously published the position data via its ROS node. As new data was published, the ground station transformed the position coordinates using a ROS transformation server, filtered the data to reduce noise, and published the new target coordinates to the hunter UAS at 10 Hz using MAVLink/MAVROS [23]. The position of the target UAS was interpreted by the hunter as

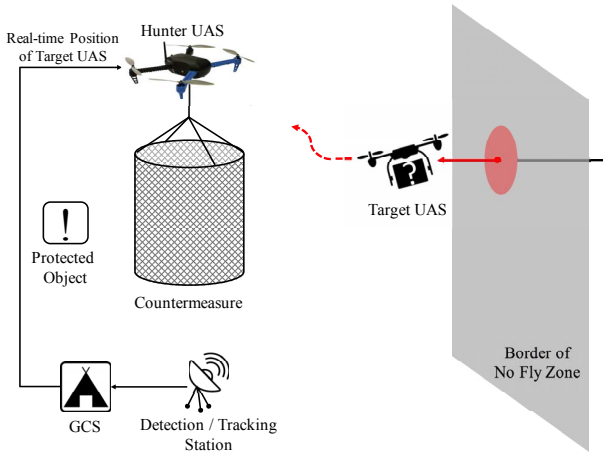

Fig. 1. Overview of the CUAS

a local position command ("LOCAL_POSITION_NED") in the PX4 [15] firmware. The hunter then adjusted its heading and speed in an attempt to intercept the incoming UAS.

A. Net Design

The net design went through several iterations before reaching the final design used to take down the target UAS. Each iteration solved problems that were discovered in previous designs. The final design was comprised of mono-filament netting held together with two carbon-fiber rings at the top and bottom. The cylindrical shape allowed the net to have the same cross section from any direction, giving the hunter UAS the best chance of intercepting the target UAS. The top of the net had a dome made of carbon fiber that attached the net to the hunter UAS. The dome shape distributed the tension of the load to prevent the net from twisting and tangling in on itself or the hunter.

B. Controller Design

For estimation of the target UAS state, $\mathbf{x}$, we assume a constant velocity model, as defined below, and employ a hybrid Kalman filter with a continuous prediction step and a discrete update step. RADAR measurements, $\mathbf{z}_k$, are used to correct the estimate and are received at 10 Hz.

$$\mathbf{x} = \begin{bmatrix} p_x & p_y & p_z & v_x & v_y & v_z \end{bmatrix}^T \tag{1}$$

$$\mathbf{f}(\mathbf{x}) = \begin{bmatrix} v_x & v_y & v_z & 0 & 0 & 0 \end{bmatrix}^T \tag{2}$$

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{f}(\mathbf{x}(t)) + \mathbf{w}(t) \tag{3}$$

$$\mathbf{g}(\mathbf{x}) = \begin{bmatrix} p_x & p_y & p_z \end{bmatrix}^T \tag{4}$$

$$\mathbf{z}_k = \mathbf{g}(\mathbf{x}_k) + \mathbf{v}_k \tag{5}$$

where p_i are the position components in the north-east-down frame, v_i are the velocity components in the north-east-down frame, the state at step k is defined as $\mathbf{x}_k = \mathbf{x}(t_k)$, the RADAR measurement at step k is defined as $\mathbf{z}_k = \mathbf{z}(t_k)$, the process noise at time t, $\mathbf{w}(t)$, is normally distributed with mean $\mathbf{0}$ and covariance matrix Q, $\mathbf{w}(t) \sim \mathcal{N}(\mathbf{0}, Q)$, and the RADAR measurement noise at step k, v_k, is normally distributed with mean $\mathbf{0}$ and covariance matrix R, $\mathbf{v}_k \sim \mathcal{N}(\mathbf{0}, R)$.

Fig. 2. The hunter UAS with the countermeasure

In order to increase the rate of successful engagement, we command the hunter position set-point $\mathbf{x}_{sp}$ to lead the trajectory of the target by $\Delta_l = 0.6$ seconds. This accounts for both the net trailing the hunter UAS, due to drag at high velocities, as well as latencies in the system. This prediction is achieved using the constant velocity model defined below.

$$\mathbf{x}_{sp} = \hat{\mathbf{x}}(t) + \mathbf{f}(\hat{\mathbf{x}}(t))\Delta_l \tag{6}$$

A PID controller is then used to regulate the error ($\mathbf{x_e} = \mathbf{x}_{sp} - \hat{\mathbf{x}}$) in the system and send a velocity command to the lower level control laws. This velocity command must be saturated using the norm of the velocity, instead of component-wise for the x and y components, to ensure that the heading to the target is preserved. Since the target vehicle is approaching from a distance, the velocity command will be saturated during a significant portion of the flight. It is therefore important that the saturated velocity vector point toward the target. This simple approach proved effective. If the hunter overshoots the target on the first pass, it turns around and then continues trying to intercept while following where the relative speed is reduced and the tracking is more accurate.

If the commanded velocity in the x-y plane exceeds the

maximum, V_{xy}, it is saturated by:

$$sat_{xy}(v_x) = V_{xy}\left(v_x/\sqrt{v_x^2+v_y^2}\right) \quad (7)$$

$$sat_{xy}(v_y) = V_{xy}\left(v_y/\sqrt{v_x^2+v_y^2}\right) \quad (8)$$

Similarly, if the commanded z velocity exceeds the maximum, V_z, it is saturated by:

$$sat_z(v_z) = V_z\left(v_z/\sqrt{v_z^2}\right) \quad (9)$$

The original PX4 firmware did not employ saturation for the local position setpoint command sent via MAVLink [23], so a modification to the firmware was required. The hunter UAS reached speeds of 20 m/s without velocity saturation, which reached the target quickly, but lead to excessive overshoot.

IV. Experiments and Results

Field testing was conducted over a five day period in June 2015, due to limited availability of the military RADAR equipment, to evaluate the performance of the prototype CUAS. The experiments revealed issues with the control of the system, as discussed previously, but finally concluded with successful engagements of the target UAS by the hunter. As a result of our limited test time, there were a limited number of complete field test flights with the complete software and system configuration. In the end, the system was successful in detecting, tracking and remediation of an enemy UAS. A photo of a successful engagement is shown in Fig. 3. After the successful engagement with the RADAR-based system, the experiment was repeated with a LIDAR as the primary sensor. Results of those experiments will be discussed in an upcoming further works.

A. Test Setup

The tests were performed at an abandoned airport with a 500 meter asphalt runway. The aerial view of the airport is shown in Fig. 4. To make the test as realistic as possible, we used a DJI Phantom 2 as the target UAS, due to its popularity in the market. The target UAS flew in a straight line from the end of the runway toward the protected area at 4 m/s.

B. Results

The overall results are plotted in Fig. 5. Notice that when RADAR data is not present, the prediction of the target UAS continues in a straight line. The hunter UAS approaches the target and makes the first pass around 100 meters from the protected location. The hunter then continues engagement attempts over the next 13 seconds and 52 meters. The final engagement occurs at approximately 40 meters from the protected location.

The time history of the target and hunter trajectories can be seen in Fig. 6. The initial pass of the target by the hunter occurs at 15 seconds. As the measurements become more accurate, the hunter continues making engagement attempts with the net until it captures the target UAS at 28 seconds.

The altitude time history is shown in Fig. 7. The RADAR elevation angle data is degraded when compared to the

Fig. 3. Engagement of target by hunter

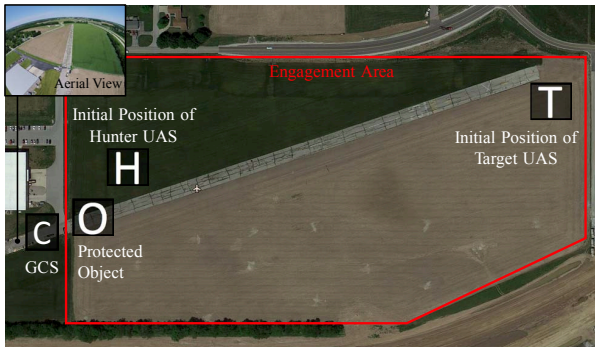

Fig. 4. Aerial view of the test site

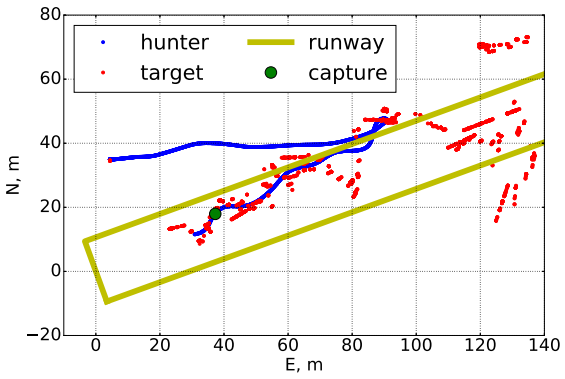

Fig. 5. Interception of target by hunter with RADAR based tracking

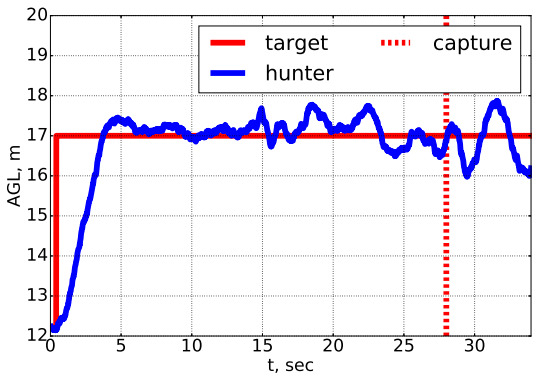

Fig. 7. Altitude tracking

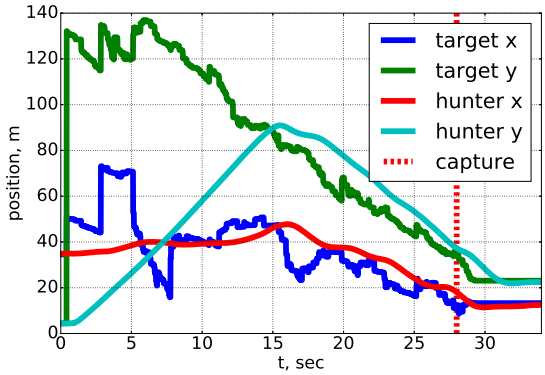

Fig. 6. Position tracking

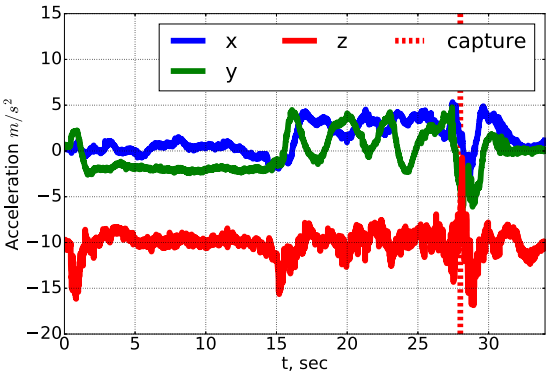

Fig. 8. Measured IMU accelerations of the hunter

azimuth, so we compensated by having the hunter vehicle fly at a set height of 17 meters and increasing the length of the net to account for the uncertainty in the target altitude. The hunter altitude tracking performance error remains below 1 meter from the estimated altitude during the entire flight.

The engagement is visible on the plot of the measured IMU data at 28 seconds. There is a 1 g spike in the z acceleration as the vehicle stops after the engagement, but in this case, the target UAS was a DJI Phantom 2 and the props stopped after hitting the carbon fiber supports on the net, which caused it to fall to the ground instead of becoming tangled. This caused little disturbance to the hunter as shown in Fig. 8.

Fig. 9 shows the two phases of flight where the hunter approaches the target UAS and reaches the commanded velocity of $7m/s$. After missing the first high velocity pass, the hunter turns around to pursue the target with the net and engages it at 28 seconds. The ability of this system to continue engagement attempts makes it more robust than single-fire systems, such as net guns, where you cannot retry after the first attempt.

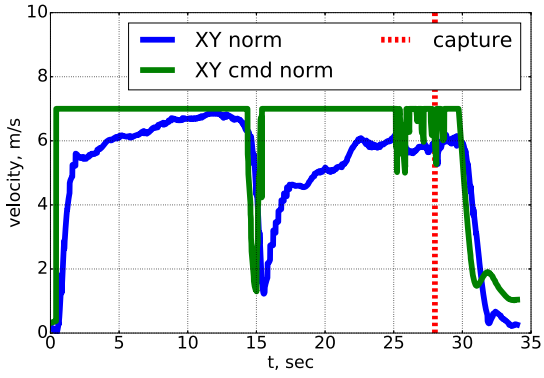

Fig. 9. Velocity magnitude (xy components) of the hunter

V. Conclusion

The experimental field test has shown that a RADAR-based, fully autonomous, air-to-air Counter Unmanned Aerial Systems (CUASs) are possible with existing technologies. The major challenges were distinguishing between the target and hunter UASs when they were in close proximity, to each other, the altitude and accuracy of the RADAR measurements, and the initial recognition and track development of the dubious UAV. The cylindrical net design that enabled a single hunter UAS to make repeated engagement attempts at various angles and with full autonomy greatly improved the reliability of the system.

For future work, we plan to improve the reliability of the system with several methods. The size of both the net and the hunter UAS can be increased. Also, the commanded approach trajectory could employ game theory, instead of saturated PID control. Finally, we plan to investigate fusion of several types of sensor information, such as RADAR, LIDAR, and acoustic data.

Acknowledgments

We want to thank and acknowledge the various agencies, partners and groups that supported and participated directly in this effort, as well as the project sponsor, UCI. We also acknowledge support personnel such as Junhan Bae and Sangjun Lee.

References

[1] S. Gallagher, "German chancellors drone attack shows the threat of weaponized uavs," 2013. [Online]. Available: http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of\-weaponized-uavs/

[2] H. Abdullah, "Man detained for flying drone near white house," 2015. [Online]. Available: http://www.nbcnews.com/news/us-news/man-detained-trying-fly-drone-near-white-house-n359011

[3] M. S. Schmidt and M. D. Shear, "A drone, too small for radar to detect, rattles the white house," 2015. [Online]. Available: http://www.nytimes.com/2015/01/27/us/white-house-drone.html

[4] Federal Aviation Administration, "Operation and certification of small unmanned aircraft systems," Feb 2016. [Online]. Available: http://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf

[5] ——, "Registration and marking requirements for small unmanned aircraft interim final rule," Dec 2015. [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2015-12-16/pdf/2015-31750.pdf

[6] Department of Defense, "Unmanned aircraft system airspace integration plan," March 2011. [Online]. Available: http://www.acq.osd.mil/sts/docs/DoD_UAS_Airspace_Integ_Plan_v2_(signed).pdf

[7] D. Sathyamoorthy, "A review of security threats of unmanned aerial vehicles and mitigation steps," *The Journal of Defence and Security(In press)*, vol. 6(2), Oct 2015.

[8] T. Humphreys, "Statement on the security threat posed by unmanned aerial systems and possible countermeasures," 2015. [Online]. Available: http://docs.house.gov/meetings/HM/HM09/20150318/103136/HHRG-114-HM09-Wstate-HumphreysT-20150318.pdf

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

[10] A. Levin, "Drone-chasers tinker with defeat devices in tiny war for skies," February 2016. [Online]. Available: http://www.bloomberg.com/news/articles/2016-02-16/drone-chasers-tinker-with-defeat-devices-in-tiny-war-for-skies

[11] Boeing, "Boeing's compact laser weapons system tracks and disables uavs," 2015. [Online]. Available: http://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page

[12] S. Park, S. Shin, Y. Kim, E. T. Matson, K. Lee, P. J. Kolodzy, J. C. Slater, M. Scherreik, M. Sam, J. C. Gallagher *et al.*, "Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles (uavs)," in *SENSORS, 2015 IEEE*. IEEE, 2015, pp. 1–4.

[13] DroneShield, 2016. [Online]. Available: https://www.droneshield.com/

[14] L. Belz, "Counter-uav system from airbus defence and space protects large installations and events from illicit intrusion," 2015. [Online]. Available: https://airbusdefenceandspace.com/newsroom/news-and-features/counter-uav-system-from-airbus-defence-and-space-protects-large\-installations-and-events-from-illicit-intrusion/

[15] L. Meier, D. Honegger, and M. Pollefeys, "Px4: A node-based multithreaded open source robotics framework for deeply embedded platforms," in *Robotics and Automation (ICRA), 2015 IEEE International Conference on*. IEEE, 2015, pp. 6235–6240.

[16] M. Kratky and L. Fuxa, "Mini uavs detection by radar," in *Military Technologies (ICMT), 2015 International Conference on*. IEEE, 2015, pp. 1–5.

[17] J. S. McGrew, "Real-time maneuvering decisions for autonomous air combat," Ph.D. dissertation, Massachusetts Institute of Technology, 2008.

[18] J. S. McGrew, J. P. How, B. Williams, and N. Roy, "Air-combat strategy using approximate dynamic programming," *Journal of guidance, control, and dynamics*, vol. 33, no. 5, pp. 1641–1654, 2010.

[19] E. Ackerman, "South korea prepares for drone vs. drone combat," 2015. [Online]. Available: http://spectrum.ieee.org/automaton/robotics/aerial-robots/south-korea-drone-vs-drone

[20] M. Goodrich, "Drone catcher: Robotic falcon can capture, retrieve renegade drones," 2016. [Online]. Available: http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

[21] Delft Dynamics, "Dronecatcher catches drone," 2015. [Online]. Available: http://www.delftdynamics.nl/index.php/en/news-en/117-dronecatcher-catches-drone

[22] M. Quigley, K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler, and A. Y. Ng, "Ros: an open-source robot operating system," in *ICRA workshop on open source software*, vol. 3, no. 3.2, 2009, p. 5.

[23] L. Meier, J. Camacho, B. Godbolt, J. Goppert, L. Heng, M. Lizarraga *et al.*, "Mavlink: Micro air vehicle communication protocol," *Online]. Tillgänglig: http://qgroundcontrol. org/mavlink/start.[Hämtad 2014-05-22]*, 2013.