International Journal of Aviation, Aeronautics, and Aerospace

Volume 7 | Issue 2 Article 2

2020

Agent Based Modeling for Low-cost Counter UAS Protocol in Prisons

Travis L. Cline
Purdue University, cline40@purdue.edu
J. Eric Dietz
Purdue, jedietz@purdue.edu

INTRODUCTION

Threat background

As technology advances and computing power continues to become more and more miniaturized, commercial small unmanned aerial systems (sUAS), more commonly known as "drones," are becoming more prevalent. These systems are defined by the Federal Aviation Administration (FAA) in Title 14 of the Code of Federal Regulations (C.F.R.) § 107.3 as a small unmanned aircraft and its associated elements. While there are many beneficial uses of sUAS including photography, building and tower surveys, search and rescue applications, and geospatial uses, there are more nefarious uses that are concerning from a physical security standpoint. Drones have been used to attack the Venezuelan president, land undetected on the property of the White House, and to deliver crude explosives to troops in the Middle East (Gramer, 2017; Grossman, 2018; Wallace & Loffi, 2015). Indeed, current physical security protocols are proving too costly or ineffective to stop unwanted sUAS activity.

Within the United States, an alarming number of prisons have reported use sUAS to drop contraband to inmates. Reports from Maryland, Ohio, Oklahoma, Tennessee, South Carolina, and other states have described the use of these systems to air-drop heroin, cell phones, and blades to prisoners ("United States," 2016). In California, 45 "unauthorized drone intrusions" were recorded between July 2017 and May 2018, some of which were found to have successfully smuggled cell phones, drugs, and saw blades putting correctional officers and other inmates at risk (Harvey, 2018; Kotowski, 2018). In South Carolina, a drone was used to give personnel locations and deliver wire-cutters to assist a convict in a prison break. After a manhunt, the criminal was re-apprehended ("Dedrone," 2019).

Challenge

Many prisons struggle to implement an effective counter unmanned aerial systems (C-UAS) detection program tailored to the typical UAS threat they encounter and do not have enough funding for a robust C-UAS protocol (Otte, 2017). Additionally, even well-funded organizations are finding effective C-UAS solutions for fixed sites a challenge, as evidenced by a March 2019 solicitation by the Department of Defense admitting, "It has proven difficult to identify and mitigate threats," in regard to its bases, installations, and facilities (NC DefTech, 2019). Common characteristics of UAS intrusions to prisons include using minimally modified commercial off-the-shelf platforms from manufacturers such as DJI and Yuneec. This gives threat sUAS some unique characteristics that can be used to develop tailored and low-cost solutions that are specific to this problem.

Modeling and UAS Security

Currently, the ability to interdict drones is illegal outside of certain Federal entities. Agent-based modeling may serve as an appropriate venue to test counter

UAS policies and techniques without legal consequences. Technical data can be programmed into a model to represent a geographical space, a sensor, an interdiction device, a threat UAS, and a facility footprint. Modeling may be an appropriate method to provide data to guide policy revisions involving counter UAS operations. Once a model is built, it can be used to validate the security procedures of a fixed site, while different scenarios can be used to test and refine the security policy and implementation. This data may provide lawmakers with insights to make legal revisions necessary for corporations and non-federal entities to protect themselves with C-UAS technology currently restricted from use.

Research Question

Given a hypothetical C-UAS sensor performance data and fixed C-UAS interdiction characteristics, what are the effects of a threat unmanned aerial vehicle's speed on detection and interdiction of a C-UAS designed to protect a 40-acre facility from threat UAS overflights?

LITERATURE REVIEW

Threat UAS Characteristics

FAA sUAS guidelines affecting manufacture.

Current threats to U.S. prison systems involve 'low-tech' offenders using commercially available sUAS from manufacturers such as DJI, Yuneec, and Parrot and minimally modifying them for the purposes of intrusive overflight and contraband smuggling. Manufacturers adhere to FAA regulations regarding the use of and operation of sUAS, which gives these threats several common characteristics that can be used in detecting, tracking, and integrating interdiction methods.

Title 14 C.F.R §107.31 requires that a remote pilot is within visual line of sight of the sUAS at all times and able to re-direct the aircraft (e-CFR, 2019). Typically this will place the remote pilot no further than one mile from the aircraft where visual tracking and obstacle avoidance becomes very challenging (UAV Coach, 2020). The control channel for DJI offerings, such as the Phantom 4, typically send control inputs from the radio control module on the 2.4 GHz wavelength, and image transmission is broadcast back from the aircraft to the control station over the 5.8 GHz wavelength (DJI, 2019). DJI reports the controllable signal strength of this UAS to be just over four miles. A similar Yuneec offering, the Typhoon 4K, transmits control inputs over the 2.4 GHz bandwidth and sends video signals back to the control system over the 5.8 GHz range as well (Yuneec, 2018). This control transmission architecture is not uncommon for commercial offerings and may be used to interdict trespassing sUAS. This also excludes the possibility of legal autonomous flight and requires that a remote controller can control the aircraft, as opposed to the capability of 'high-tech'

offenders to use pre-programmed GPS waypoints and flight routes for autonomous flight.

Title 14 C.F.R. §107.29 restricts sUAS operation during night hours. While the flight performance characteristics are not different at night, most of the control systems for commercial sUAS involve visual sensors for flight orientation and obstacle navigation. Night flight is therefore difficult without upgrading to expensive night visual optics and possible aircraft modifications, which would push the offender into the 'high-tech' category as well. For the purposes of this paper, 'low-tech' threats will be considered and modeled, as they are the primary sUAS threat encountered by prisons.

Popular sUAS performance characteristics.

The primary threat and common thread in the reviewed cases of unwanted UAS intrusions involving prisons is using commercial-off-the-shelf platforms with slight modifications for accepting and jettisoning a payload. The DJI Phantom 4 Pro is a popular UAS and can fly up to a maximum of 45 mph in ideal atmospheric conditions and in a clean configuration with no payload (DJI, 2019). This UAS has a retail price of approximately $1,700 and requires an Apple iPhone or iPad to operate. Additionally, DJI offers a robust and powerful flight control software that is intuitive and ideal for low experience sUAS pilots. This aircraft is consistent with the price point, power and specifications of reported prison intrusions and will be used as an initial basis from which to model flight behavior (Rubens, 2018).

C-UAS Sensor Types and Characteristics

As of December of 2019 a report highlighted that there are 537 C-UAS products and systems offered by over 277 different companies (Michel, 2019). The products range from detection only, interdiction only, or a mix of both. Detection methods include radar, radio-frequency tracking, electro-optical, infrared, acoustic, and mixed sensors. No single detection method has proven to be without fault, so often integrated systems use a mix of detection sensors. Interdiction methods can include radio-frequency jamming, global positioning system (GPS) jamming, spoofing, laser, nets, and projectiles (Michel, 2019). Table 1 represents a brief summary of UAS detection sensors.

Table 1
Types of Detection Sensors and Descriptions

Sensor Type	Description
Radar	Detects radar signature by emitting radio wave pulses and analyzing return energy to determine the range, angle, and velocity
Radio-Frequency	Detect UAS presence by scanning commonly used UAS bands such as 2.4 GHz and 5.8 GHz, may be able to determine location with complex antennas and multiple sensor locations
Electro-Optical	Detect UAS based on the visual signature of the UAS aircraft
Infrared	Detect UAS based on the infrared signature emitted by the UAS aircraft
Acoustic	Detect changes in sound by using microphones and software filters to match data from a database UAS audio signatures

Note. Descriptions are adapted from Michel (2018, p. 4).

For the purposes of this study, the hypothetical sensor used in modeling will be largely based on integrated acoustic UAS sensors since there is very limited data available with other sensors that can be used for simulation modeling, and this sensor type is typically lower in cost than other sensor types.

Acoustic sensor characteristics.

Acoustic means of sUAS detection typically rely on microphone arrays that are coupled with audio analysis software. Simply stated, a microphone array consists of several microphones positioned at a single site with positional offsets that allow for bearing and azimuth estimations based on the slight differences between the timing and intensity of the sound reaching each microphone. The detection range of these systems can be affected by multiple elements such as microphone quality and sensitivity, ambient noise, weather conditions, and software packages.

French-German Research Institute of Saint-Louis (ISL) conducted audio drone detection testing using four Brüel & Kjaer type 4189 metrological microphones (Christnacher et al., 2016). The research team was only able to accurately detect (in azimuth and elevation) a customized drone 20 seconds away from the sensors when the drone was directly traveling towards the sensor. However, the sensor array was able to continuously track the drone for 45 seconds when it was flying away. In ISL's 2016 experiment, the audio sensor array reached the longest detection range of up to 300 meters when testing against the DJI Phantom 2 at an altitude ranging from 120 to 150 feet. While there is no acoustic data specifically on the Phantom 4, the Phantom 2 is a close alternative.

Additionally, from data gathered by Guvenc, Koohifar, Singh, Sichitiu, & Matolak (2018), the detection range of different acoustic sensors ranges from 20 meters to 600 meters, mainly depending on drone types and sensor arrangement. According to Bernardini et al. (2017), their acoustic detection algorithms have accuracy ratings ranging from 0.964 to 0.992 when distinguishing UAS noises from different environmental noises. The lowest accuracy being in a crowd and street with traffic, while the highest rating was in natural daytime. These algorithms, however, do not account for limitations encountered by distance, ambient conditions and specifications of microphones.

The hypothetical sensor characteristics used for this study will be modeled largely after acoustic sensors as there is more available operational data for this sensor type than others, and it meets the intent for developing a low-cost solution for identifying threat sUAS.

Interdiction Agent Characteristics

UAS interdiction involves the disruption of the threat sUAS flight path by one or more methods, with a goal of threat mitigation or minimizing perceived risk from the unwanted activity. Table 2 represents a summary of different interdiction methods currently employed (Michel, 2018). It is important to note that currently UAS interdiction operations are illegal in the U.S. outside of the Department of Defense, Department of Energy, Department of Homeland Security, and Department of Justice.

Table 2
Types of Interdiction Methods Currently Employed

Sensor Type	Description
Radio Frequency (RF) Jamming	Interrupts the RF link between UAV and operator by generating large amounts of RF output. Once the RF link is disturbed, the UAV will land or return to the operator.
GNSS Jamming	Interrupts the satellite link used for navigating. Once the satellite link is lost, UAV will hover, land, or return to the operator.
Spoof	Taking control of the UAV by hijacking the communications link
Kinetic	Destroys portions of the airframe with directed energy, causing a crash
Net	Entangles the UAV or its rotors
Projectile	Employs ammunition to destroy UAV
Combination	Several C-UAS methods employed – commonly tandem RF and GNSS jamming

Note. Descriptions are adapted from Michel (2018, p. 4)

In 2016, a Michigan Tech research team demonstrated the effectiveness of a proof-of-concept anti-UAS net-launcher mounted on what appears to be a DJI Matrice 600 (Goodrich, 2016). This team later filed for and received a patent for their system which is able to aim the net projectile and carry the intruding UAS to a safe location for handling, mitigating human risk due to explosives or other potentially hazardous cargo (Aagaah et al., 2018).

In 2017, another research team from Purdue University demonstrated the effectiveness of a completely autonomous C-UAS detection and interdiction system involving a radar tracking system and autonomous hunter drone equipped with an ultra-light carbon-framed conical net (Goppert et al., 2017). The net design was selected to allow multiple attempts at interdiction of a threat in the event the autonomous positional data was too imprecise for a launched-net entanglement. The threat UAS was flown at a set altitude over a set path toward a protected object. The radar in use was described as a "high-precision" and "military" radar (Goppert et al., 2017, pp. 236, 238). This high-fidelity radar would be excellent for proving autonomous interdiction is possible but is largely outside of the budget and manpower available to prisons and other fixed facilities. Hunter type drone characteristics will be modeled for the interdiction agent in this study.

Prison Characteristics for Modeling Consideration

Like many other prisons across the country, there have been reports drones have been used to smuggle contraband within the security perimeter of the Indiana State Prison (J. E. Dietz, personal communication, September 20, 2018). Indiana State prison is a level four maximum-security prison located in Michigan City, Indiana which houses approximately 2,400 inmates (State of Indiana, 2019). The walled area spans 24 acres and the adjacent field is approximately another 18 acres (see Figure 1). These dimensions will be used to geographically represent the protected facility within the simulation model.

Figure 1. Indiana State Prison footprint of approximately 40 acres (Google Maps, 2020)

METHOD

This section discusses the research framework, approach, tools of measurement, variables, and assumptions used in this article.

Research Framework

This research paper explores the usefulness of agent-based modeling software for adjusting and determining parameters that could lead to a successful C-UAS detection system. Simulation modeling software has the unique ability to quickly adjust parameters and gather data and should provide insights that should transfer over to real-world systems, and bypass current legal restrictions on testing and implementation of C-UAS interdiction. Later iterations are intended to refine threat, sensor, and system behaviors. This will be done with a goal of identifying parameters for recommending system specifications for a comprehensive detection, tracking, and interdiction system for common commercially manufactured threats. AnyLogic modeling software will be used to replicate the geometric space, threat UAS, hypothetical C-UAS sensors, and an interdiction agent.

This study is designed to test an abstracted fixed counter unmanned aerial system that is designed to prevent overflight of a fixed facility representing an abstracted prison or compound. Parameters for agents will be discussed in later

sections and are designed to replicate probable integrations of equipment that may be purchased for these purposes. Data will be collected for 50 iterations of each varying threat speed, while all other C-UAS behaviors remain the same between iterations.

Model Characteristics

Threat UAS characteristics.

The DJI Phantom 4 Pro specifications will be used to model the threat aircraft characteristics. This UAS is capable of speeds up to 45 mph under ideal conditions with no other payload other than the integrated camera on-board. Adding a payload will lower the top speed and affect the center of gravity and other flight controllability characteristics. The modeled threat UAS was spawned .75 miles away from the protected facility outside of sensor detection range, and at the far end of feasible line-of-sight tracking (UAV Coach, 2020). The threat UAS was flown in a pattern as dictated by 100 “attractors” selected randomly, one after the other, as depicted in Figure 2. There were 50 attractors placed evenly within the bounds of the protected facility, and an additional 50 attractors spanning the remaining space surrounding the facility. The simulation was run with threat speeds set at 25, 27.5 30, 32.5, 35, 36, 37.5, and 40 mph to collect sample data in each speed category.

Facility characteristics.

The simulation model contains a .25 x .25-mile (40 acres) square that will be used to indicate the footprint of the protected facility. A ‘failure’ within an iteration is defined as the threat UAS overflying the footprint of the protected facility, regardless of the duration of overflight.

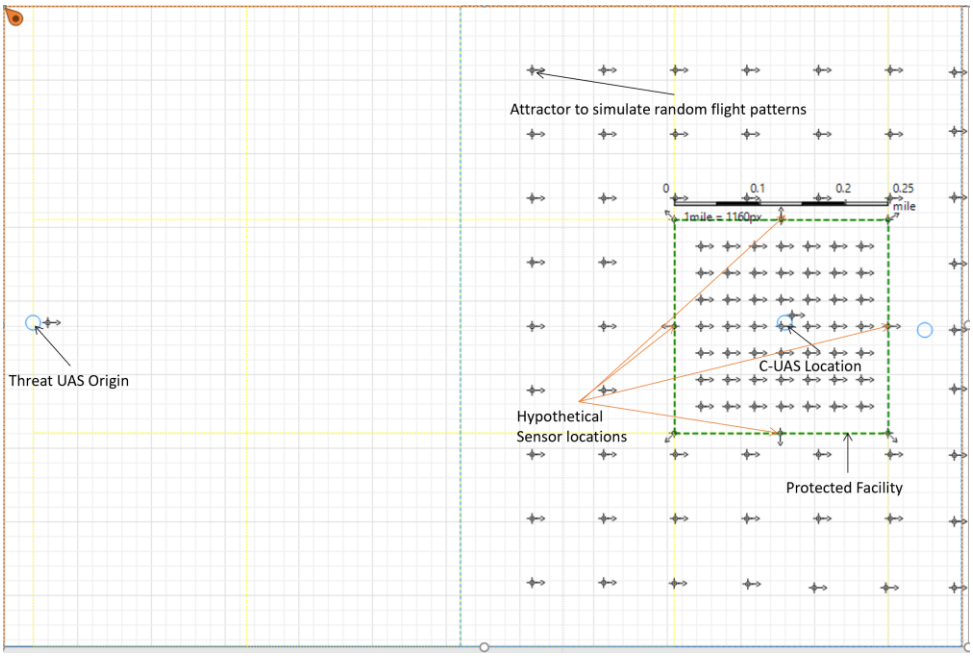

Figure 2. The physical representation of the model space used in the experiment

Hypothetical sensor model characteristics.

A hypothetical sensor will be used for modeling based on an average of performance characteristics of Bernardini et al. (2017) and listed specifications of DroneSheild as reported by Birch et al. (2015) for ranging and success probability. The hypothetical sensor will be assumed to provide cueing to a higher fidelity electro-optical sensor. For the purposes of this study cueing and additional functionality will be abstracted into the specifications listed in Table 3.

Table 3
Hypothetical sensor model parameters and values.

Sensor Type:	Omni-directional	Parabolic dish	Hypothetical
Effective Range	150 m / 495 ft	1000 m / 3280 ft	575 m / 1890 ft
Detection Angle	300°	30°	165°
Analysis Time Frame	-	-	5 second frames
SVM Success Rate	-	-	96.4%

Note. Analysis time and success rate derived from works by Bernardini et al. (2017, p. 63) and range and angle adapted from Birch et al. (2015, p. 27).

Interdiction agent model characteristics.

The DJI Matrice 600 Pro specifications will be used to model the interdiction aircraft characteristics. This UAS is capable of speeds up to 40 mph, no wind or excess payload (DJI, 2020). The simulation model will be using this as the fixed C-UAS interdiction speed. The model assumes that there will be an attached ultra-light net similar to the one used in a 2017 study by Goppert et al., in which a conical net and carbon-fiber housing were attached to a similar platform for the purposes of entangling threat UAS. The effects on top speed, the center of gravity, and other flight controllability characteristics have not been considered with the net attached for the purposes of this study. The C-UAS will be placed in the center of the protected facility and will track to the threat 10 seconds after the sensor detects the threat UAS. This will be the assumed time for cueing from the sensor to the interdiction agent.

RESULTS AND ANALYSIS

The model was built based on an abstracted facility footprint, hypothetical C-UAS sensor performance data and fixed C-UAS interdiction characteristics. After this framework was established and the agent behaviors set, the only variable manipulated in the model for each set of samples collected was the sUAS threat speed, which was set at the beginning of each iteration. These individual fixed-speed simulations were allowed 50 iterations of each run. The runs were documented and the threat UAS fixed speed was adjusted for the next set of simulations. Eight fixed-speed simulation sets were run, altering the threat UAS speed at 25 mph, 27.5 mph, 30 mph, 32.5 mph, 35 mph, 36 mph (added to explore the critical failure speed for this hypothetical system), 37.5 mph, and 40 mph and recorded each time. The results are recorded in Table 5.

Table 5
Model Simulation Results

Threat Speed (MPH)	Avg I - D Time (s)	Std. Dev. (s)	Overflights	Avg overflight time (s)
40.0	59.2	30.4	72%	18.2
37.5	50.8	23.4	54%	14.0
36.0	*48.8*	*19.2*	*56%*	*13.0*
35.0	35.5	9.9	4%	1.5
32.5	32.0	5.9	0%	0
30.0	33.9	5.7	0%	0
27.5	33.0	4.4	0%	0
25.0	34.6	3.8	0%	0

Note. I-D Time represents the interdiction time minus the detection time in seconds. 36 MPH was added to further explore the relationship between speed and system failure.

Predictably, the amount of 'failures' or overflights of the protected facility increase as the threat speed increases. Interestingly, however, the overflights increase rapidly between 35 mph and 37.5 mph. Another 50 trials were run to determine if there was a linear relationship between the threat speed and failures of the system. From 35 mph to 36 mph the overflights increased from 4% to 56% of the trials respectively.

This is interesting in that there is a large jump in system "failures" within a very small increase in speed. Subsequent research may be needed to identify the critical speed delta between the interdiction agent and the threat UAS to better determine the point at which the system's effectiveness is degraded.

The data from this experiment suggest that a 5 MPH or greater speed delta is required between the expected threat UAS and a hypothetical system designed as outlined in this study. Figure 3 displays the large increase in variance present when the difference in speed changes from 5 mph to 4 mph to 2.5 mph and 0 mph between the threat sUAS and interdiction UAS respectively.

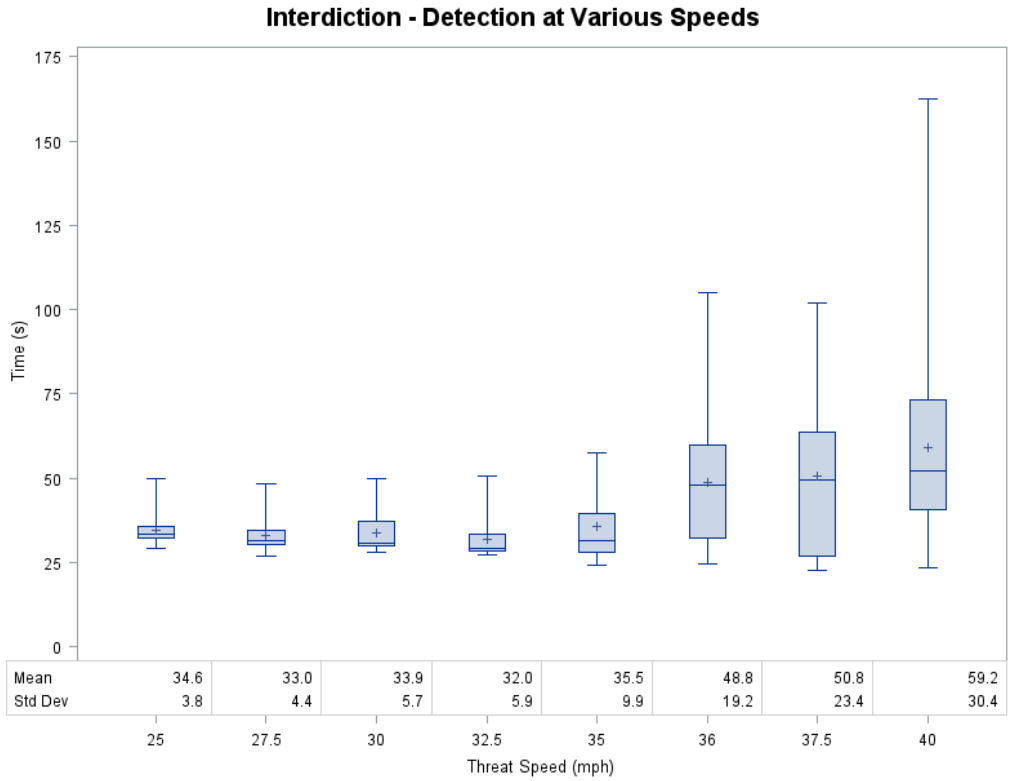

Figure 3. Interdiction time - Detection time at Various Speeds

The distributions in each category are generally right skewed with very close lower limits. This is due to the high success rates of the hypothetical C-UAS system for threats that follow a straight flight path toward the protected facility. Since half of the attractor points were located within the protected facility, this type of flight pattern was common. As the threat speed increases, the variance increases, as can be seen by larger box areas in the graph for each speed category. The higher tail grows drastically larger in the categories that have less than a 5-mph difference between the interdiction or 'hunter' UAS and the threat UAS.

DISCUSSION

The purpose of this study was to explore the relationship threat UAS speed has on a set C-UAS system that might be typical for a fixed facility such as a prison. Additionally, the second goal of this study was to explore the usefulness of agent-based modeling software as a future tool for adjusting and determining parameters that could ultimately lead to a cost-effective C-UAS detection and interdiction system for fixed facilities. Data was gathered that provide insights that may apply to real-world systems.

This study suggests that there is a critical threat speed in which the variance between detection to interdiction times drastically increases along with subsequent system failures. The critical threat speed will depend on sensor performance, the geographic position of the sensors in relation to the protected facility, and interdiction characteristics. The goal of a fixed facility C-UAS system is to mitigate the threat, or in this case, prevent overflights of the facility. Agent-based simulation modeling may be a useful tool for establishing system parameters when careful consideration is applied in replicating the environment, threat, and parts of the whole C-UAS system.

The threat agent was given behavior based on commands to fly to a random sequence of attractors around the protected facility with the largest concentration within the facility. Further investigation will be conducted prior to future research if there are better methods to model this threat behavior. Threat speed was set initially at the start of each simulation. Future works may add in a speed variability into the behavior of the agent to replicate more real-world threats. The simulation took place primarily in a two-dimensional plane. The third dimension was replicated with a changing variable that was not fully accounted for within the interdiction behavior. Future research will try to integrate the third dimension more natively, which will have an added benefit of providing more visually appealing simulations. Additionally, although the threat UAS was given semi-random behavior based on attractors distributed around the facility, there was only one spawn point for the threat UAS, which will likely be addressed in further iterations.

Sensor data was based on a hypothetical sensor, since there is a general lack of real-world performance characteristics of C-UAS sensors. As better data becomes available, more realistic sensor data will be modeled in future works. A 96.4% probability seems rather high for an SVM accuracy rating, and perhaps a distance tiered probability would be appropriate for such sensors if data is available.

Interdiction ‘warm-up’ time may need to be lengthened past ten seconds to replicate more real-world conditions. Further investigation will be conducted on similar integrated systems as data becomes available. As system complexity increases, communication delays due to cueing and data transmission may be added into the model logic.

CONCLUSION

This study suggests that there is a critical threat speed for a hypothetical C-UAS system in which the variance of possible detection to interdiction sequences becomes so great that system failure becomes prevalent. This critical speed will be based on the geographic location and layout of the protected facility, the parameters of the sensor network, and the interdiction agents that make up the counter unmanned aerial system. Additionally, this study suggests that simulation modeling may be a useful tool for determining the system parameters required for the desired

level of protection (i.e. notification of an overflight vs. prevention of an overflight) for a fixed facility, or can alternately suggest the appropriate makeup and placement of sensors and interdiction methods from tested and well-documented elements of a system. Simulation modeling may also be able to provide data to influence policy currently restricting UAS interdiction at the federal level.

References

Aagaah, M. R., Fleanha, E. M., & Mahmoudian, N. (2018). *Drone having drone-catching feature* (Patent No. US 10,005,556 B2).

Bernardini, A., Mangiatordi, F., Pallotti, E., & Capodiferro, L. (2017). Drone detection by acoustic signature identification. *Electronic Imaging*, *2017*(10), 60–64. https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168

Birch, G. C., Griffin, J. C., & Erdman, M. K. (2015). *UAS detection classification and neutralization: Market survey 2015. - SAND2015-6365*. https://doi.org/10.2172/1222445

Christnacher, F., Hengy, S., Laurenzis, M., Matwyshuck, A., Naz, P., Schertzer, S., & Schmitt, G. (2016). Optical and acoustical UAV detection. *SPIE*, *9988*(99880B). https://doi.org/10.1117/12.2240752

Dedrone. *(2019). Dedrone corrections airspace security study*. http://web-assets.dedrone.com/collateral/Dedrone_Corrections_Airspace_Security_Study2019.pdf

DJI. (2019). *DJI phantom 4 pro – Specs, tutorials & guides – DJI*. https://www.dji.com/phantom-4-pro/info

DJI. (2020). *Matrice 600 specifications*. https://www.dji.com/matrice600-pro/info

Goodrich, M. (2016, January 7). *Drone catcher: "Robotic falcon" can capture, retrieve renegade drones*. Michigan Technological University. https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

Google Maps. (2020). Google Maps. https://www.google.com/maps/place/Indiana+State+Prison/@41.7036668,-86.9196084,835m/data=!3m1!1e3!4m5!3m4!1s0x8811a7eb3f091ba7:0x74a24ce0965df5b9!8m2!3d41.7036647!4d-86.9177619

Goppert, J. M., Wagoner, A. R., Schrader, D. K., Ghose, S., Kim, Y., Park, S., . . . Hopmeier, M. J. (2017). Realization of an autonomous, air-to-air counter unmanned aerial system (CUAS). *2017 First IEEE International Conference on Robotic Computing (IRC)*, 235–240. https://doi.org/10.1109/IRC.2017.10

Gramer, R. (2017, January). *Afghan insurgents use drones in fight against U.S. – Foreign Policy*. Foreign Policy. https://foreignpolicy.com/2017/01/31/afghanistan-insurgents-use-drones-in-fight-against-u-s-nato-coalition-forces-unmanned-aerial-vehicles-future-warfare/

Grossman, N. (2018, August). *Analysis | Are drones the new terrorist weapon? Someone tried to kill Venezuela's president with one.* Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/10/are-drones-the-new-terrorist-weapon-someone-just-tried-to-kill-venezuelas-president-with-a-drone/

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. https://doi.org/10.1109/MCOM.2018.1700455

Harvey, K. (2018, May 18). *State invests $35k on pilot program to keep unwanted drones out of prisons | KBAK*. https://bakersfieldnow.com/news/investigations/state-invests-35k-on-pilot-program-to-keep-unwanted-drones-out-of-prisons

Kotowski, J. (2018). Drones used to deliver drugs, cellphones and other contraband to Delano prison, documents say. *TCA Regional News*. http://search.proquest.com/docview/2015026811/

Michel, A. H. (2018). *Counter-drone systems* (p. 23). Bard College. https://dronecenter.bard.edu/publications/

Michel, A. H. (2019). *Counter-drone systems* (2nd ed). Bard College. https://dronecenter.bard.edu/publications/

Otte, J. (2017, November 7). *Drones dropping drugs into prisons; Ohio fights back.* Daytondailynews. https://www.daytondailynews.com/news/drones-dropping-drugs-into-prisons-ohio-fights-back/GSB3jLP3sy9VMVWiaO31KM/

Rubens, T. (2018, February 8). *Drug-smuggling drones: How prisons are responding to the airborne security threat*. IFSEC Global. https://www.ifsecglobal.com/drones/drug-smuggling-drones-prisons-airborne-security-threat/

Small Unmanned Aircraft Systems, 14 C.F.R.§ 107 (2019)., Electronic Code of Federal Regulations § Part 107—Small Unmanned Aircraft Systems (2019), Source: Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, unless otherwise noted. https://www.ecfr.gov/cgi-bin/text-idx?SID=3f50729cff2b56a549c4515c703eda34&mc=true&node=pt14.2.107&rgn=div5

State of Indiana. (2019). *Indiana state prison fact sheet*. https://www.in.gov/idoc/2413.htm

NC Def Tech. (2019, March 11). *Tech area of interest: Installation counter unmanned aerial systems (CUAS)*. https://deftech.nc.gov/ opportunities/ 2019-04-30/tech-area-interest-installation-counter-unmanned-aerial-systems-cuas

UAV Coach. *(2020). Is there a specific distance implied when the FAA says "visual line-of-sight"?* https://www.dronepilotgroundschool.com/ kb/is-there-a-specific-distance-implied-when-the-faa-says-visual-line-of-sight/

United States: Drones pose new contraband, smuggling challenge for prisons. (2016). *Asia News Monitor*.

Wallace, R., & Loffi, J. (2015). Examining unmanned aerial system threats & defenses: A conceptual analysis. *International Journal of Aviation, Aeronautics, and Aerospace*. https://doi.org/10.15394/ijaaa.2015.1084

Yuneec. (2018). *Typhoon 4K specs*. http://us.yuneec.com/typhoon-4k-specs