DRONES DETECTION USING SMART SENSORS

by

Aishah Moafa

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cybersecurity Engineering
at Embry-Riddle Aeronautical University

Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach, Florida
April 2020

DRONES DETECTION USING SMART SENSORS

by Aishah Moafa

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Radu F. Babiceanu, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.

Radu F. Babiceanu, Ph.D.
Committee Chair

Ilteris Demirkiran, Ph.D.
Committee Member

Shafagh Jafer, Ph.D.
Committee Member

Timothy A. Wilson, Sc.D.
Chair, Electrical Engineering and Computer Science

Maj Mirmirani, Ph.D.
Dean, College of Engineering

Christopher Grant, Ph.D.
Associate Provost of Academic Support

4/17/2020
Date

Acknowledgments

I would like to express my sincere gratitude to Professor Radu Babiceanu, for allowing me to undertake this work, for his continuous support, and encouragement. I would also like to thank my friends, especially Abdulrahman Alanazi for his valuable advice, support, and encouragement. Finally, the most grateful and thankful goes to my family, to my aunt who provided me with strength and handled me during this journey. To my kids, Danah and Talal who give me the reason to be happy. To my husband for being beside me all lift days and trying to keep me positive. To my mom who passed away when I was younger. Despite this, she still managed to teach me how to be persistent with school and everyday life. She left me with good memories that guided me through the bad days which I will always cherish. Last but not least, thank you to those who were the reason for every good thing that happened to me.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ATM - Air traffic management

SVM - Support Vector Machine

DNN - deep neural networks

CNN - convolutional neural network

RNN - repetitive neural network

RCS - RADAR cross-section

MIMO - multiple-input multiple-output

RF - Radio Frequency

SDR - Software Defined Radio

FPV - First Person View

OUI - Organizationally Unique Identifier

HPM - High power microwave

Abstract

Drones are modern and sophisticated technology that have been used in numerous fields. Nowadays, many countries use them in exploration, reconnaissance operations, and espionage in military operations. Drones also have many uses that are not limited to only daily life. For example, drones are used for home delivery, safety monitoring, and others. However, the use of drones is a double-edged sword. Drones can be used for positive purposes to improve the quality of human lives, but they can also be used for criminal purposes and other detrimental purposes. In fact, many countries have been attacked by terrorists using smart drones. Hence, drone detection is an active area of research and it receives the attention of many scholars.

Advanced drones are, many times, difficult to detect, and hence they, sometimes, can be life threatening. Currently, most detection methods are based on video, sound, radar, temperature, radio frequency (RF), or Wi-Fi techniques. However, each detection method has several flaws that make them imperfect choices for drone detection in sensitive areas. Our aim is to overcome the challenges that most existing drone detection techniques face. In this thesis, we propose two modeling techniques and compare them to produce an efficient system for drone detection. Specifically, we compare the two proposed models by investigating the risk assessments and the probability of success for each model.

Chapter 1

Introduction

Drones recently positioned themselves as an effective multi-task weapon in warfare, and nation states and armed groups have sought to possess them for their capabilities to deliver painful blows to enemies at low cost.

Drones are complex technical systems that do not need a pilot inside. But they are operated through a pilot located at the guidance station that controls the drone remotely. The ground pilot is responsible for controlling it remotely, ensuring that it does not get into any accidents, or interfering in emergency situations. The pilot must determine the drone's route points, and then the drone directs itself according to these coordinates under the guidance of its automatic flight system.

Drones are predicted to play main roles in future smart cities, through their use in surveillance and protection systems, and for maintaining security. Although drones can be used to improve daily lives, malicious organizations can use them to perform physical and cyber-attacks on infrastructure, private/public property, and individuals. Air traffic management (ATM) for unmanned systems (UTM) are essential for ensuring secure and collision-free activity for all drone flight use-cases. Consequently, different methods of identifying, monitoring and preventing potentially unwanted drone missions are of paramount importance for monitoring and ATM systems.

Problem Statement

The high availability of small drones has raised the interest of different societal actors, as remotely controlled drones can be used in various projects. The widespread use of these technologies has generated several privacy/security and protection issues which need be resolved through proper monitoring systems capable of dealing with these risks (Bisio, Garibotto, Lavagetto, Sciarrone, and Zappatore, 2018). In the current days, drones are becoming more hazardous and anyone could become a direct or indirect target. In order to prevent these potential hazardous situations, this thesis proposes solutions to overcome these issues.

Drones can perform their missions based on different technologies. Hence, the drone detection systems have to be comprehensive enough to detect drones of any kind. However, the current systems often have limitations in their ability to detect the several types of drones with malicious missions. To exemplify this, we consider a radar system. In such a system, any object that flies within the radar field is detected. Radiation is sent to hit the object body and then the signal is returned to the source of the radar to determine the object's location. However, many drones are hard to detect and made up of materials such as fiber that make signal reflection very difficult or impossible. Moreover, every object that flies over a low range is difficult to detect through radar-based techniques. Also, sometimes, it is hard to differentiate between birds and drones. Therefore, in the case of a drone attack, our aim is to design a system to defend against the attacker drone.

Research Motivation

Malicious actors out there seek to develop drones so that they are difficult to detect, disable and neutralize their threat. To build a safer world, the good actors must work on improving the techniques to detect, counter, and destroy the malicious-built drones.

Research Objectives

In order to achieve the goals of this research and address the identified problem, we use a descriptive approach that includes a review of previous studies found in the literature and the methods that relate to the topic of the research. Our research objective is to develop detection systems that reduce the research problems and provide feasible ways to address them. More specifically, we adopt some recent and powerful techniques in machine learning such as deep neural networks (DNN). Moreover, we combine a classic detection method that is based on radar with DNN to reduce false alarms as well as avoid miss-detection. To this end, later we show the advantages of each system with comparison between them to produce an optimal detection system.

Literature Review

Bisio et al. (2018) submitted a proposal for a Wi-Fi-based statistical fingerprint method to drone identification, capable of detecting nearby drone malicious mission risks even in the midst of hacking attempts. An observational efficiency test is provided and shows that the approach could achieve strong outcomes of detection accuracy in several real-life situations, with a significant real positive peak rate of 96%.

Loke (2015) presented a study focused on the services and applications presented by airborne computing infrastructure to mobile users. The study discusses many concepts, for example drones-as-a-service and flying, fly-out infrastructure, as well as focuses on data controlling and system configuration problems that are on an increasing growth. The surveyed paper clarifies the behavior of large data sets emerging from these applications, optimizing the design of airborne and ground infrastructure to provide the best Quality of Service (QoS) and Quality of Experience (QoE), situation knowledge, usability, performance routing, user interaction, and physical analysis drones (Loke, 2015).

Guvenc et al. (2020) studied technologies that rely on ambient radio frequency (RF) signals generated from drones, radar systems, acoustic sensors, and computer vision methods for recognition of malicious drone systems. Some experimental and early simulation outcomes are presented on radar-based range approximation of drones, and receding horizon tracking of drones. In addition, the study provided an overview of corporate methods that are measured for exclusion of drones (Guvenc, Ozdemir, Yapici, Mehrpouyan and Matolak, 2020).

According to Kaleem and Rehmani (2018) new suggested solutions coming from research and development arena advocate for the introduction of onboard drone detection systems. These solutions could make a link between the Monitoring Drone (MDr) and Intruder Drone (IDr) concepts.

Drone Detection Methods

The surveyed literature identified different techniques for detecting and tracking intruding drones, such as RF sensing (Nguyen et al., 2018), Wi-Fi sniffing (Bisio et al.,

2019), acoustic sensors (Guvenc et al., 2017), video surveillance (Sturdivant and Chong, 2017), and radar systems (Birch, Griffin, and Erdman, 2015). The following sections focus on the latest methods used to detect drones in larger detail.

Video-Based Detection

Video-based detection uses both graphical and electrical camera sensors to recognize moveable objects in the monitored environment. Generally, advertisement cameras can achieve an operating range of approximately 350 ft., which leads to a quiet desirable neighborhood of monitoring. This method uses characteristics like color, contour lines, shapes, and edges to categorize a typical drone's object as compared to other things (Zhang et al., 2016).

Remote monitoring algorithms can also be used for evaluating elements over consecutive frames (Ganti and Kim, 2016). This can help identify different objects with identical shapes through their usual gestures, like drones and birds (for example, differentiating between artificial drone motions vs. natural bird motions). Cameras mounted on these systems are also very sensitive to the lighting conditions and require that the target is in their line of sight to be able to detect flying objects. Furthermore, numerous studies and research have contributed to the development of a system for the detection and identification of drones from surveillance videos (Ganti and Kim, 2016; Wu et al., 2018).

Sound-Based Detection

Many recent studies and research have focused on the use of the voice detection method to detect and identify drones through tools such as correlation analysis (Mezei and

Molnar, 2016; Mezei, Fiaska, and Molnar, 2015). One of the leading methods that can be used in detecting, recognizing acoustics, and distinguishing between drones and other objects is the learning algorithm utilized in support vector machines (SVM) (Bernardini, Mangiatordi, Pallotti, and Capodiferro, 2017). Nijim and Mantrawadi (2016) presented a study to detect drones through their emission sounds. Other works used sound cameras and direction of arrival (DOA) rating for classification and tracking of drones (Chang et al., 2018; Busset et al., 2015; Yang et al., 2018).

Radar-Based Detection

Radar-based detection uses the electromagnetic principle of backscattering theory for drone identification. The conventional radar method is based on the observation that aircraft or flying objects typically show a broad radar cross-section (RCS). However, as it was observed through the literature survey, most modern drones are mechanical quadcopters, with a low RCS (Ritchie, Fioranelli, Griffiths, and Torvik, 2015). The main disadvantage of this method depends on the construction materials, some of them having dielectric characteristics close to air and resulting in little reflection back to the transmitter. Therefore, the new studies employ updated forms of radar detectors that harness the power backscattered from propellers and rotors.

To compensate for these limitations, many studies and researches have attempted to use multi-static radars to analyze the signature of micro doppler of drones, and classify drones with various payload size (Fioranelli, Ritchie, Griffiths, and Borrion, 2015). Additionally, Drozdowicz et al. (2016) used frequency-modulated continuous-wave (FMCW) radar to extract data on the scope, kind, range, and radial velocity of drones. In

addition, other methods were identified in the literature studied. Klare, Biallawons, and Cerutti-Maori (2016) introduced a multiple-input multiple-output (MIMO) radar to create 256 virtual components to identify and track drones. The device can be used to determine whether drones reside within a given range of angular cells. This radar-based method can be implemented in a rather portable format, so a motion detection radar (MDR) can also be deployed onboard (Moses, Rutherford, and Valavanis, 2011).

Moses, Rutherford, and Valavanis (2011), proposed a model for a lightweight X-Band radar system for identify drones via their Doppler signatures. Moreover, Mendis, Randeny, Wei and Madanayake (2016) suggested a model to automatically detect and classify three drones in a laboratory environment based on a radar sensor. Solomitckii, Gapeyenko, Semkin, Andreev, and Koucheryavy (2018), designed a system for detecting drones by exploiting 5G millimeter bands as radars. Lastly, Saqib, Khan, Sharma, and Blumenstein (2017), and Unlu, Zenou, and Riviere (2018), relied on computer vision detection approaches to detect drones in the vicinity of birds.

Radio Frequency Detection

The radio frequency (RF) based detection systems rely on the fact that drones use RF signals to connect with the ground station. Drone networking protocols typically are carried by the same also used for Wi-Fi communications, especially in the range 2.4 and 5 GHz. In addition, drones fitted with cameras typically relay a video stream during the same wireless channel to their control system.

According to Witschi et al. (2016), morphological frequency-domain filtering is used to formulate an algorithm for the identification of UMTS, LTE, and drone contact

signals in detrimental conditions. RF identification has a very long operational range covering more than 1400 ft. An identified limitation of this method is that the target detection rate is highly dependent on the transmission energy and response of the detector. More recently, novel methods that depend on software-defined radio (SDR) solutions have been suggested. A different approach is proposed in (Yue et al., 2018), where authors recommend a distributed system for tracking the location and estimated direction of unwelcomed drones through combining SDR transmitters and wireless acoustic sensors.

An overall summary of passive drone monitoring is presented in (Fu et al., 2015), where authors also establish a portable universal radio minor software design depending on SDR to simulate drones in various scenarios. Nguyen et al. (2018), considered a passive cost-effective RF sensing drone detection system. In addition, Zhang et al. (2018) suggested a drone detection based on RF sensing. Nguyen et al. (2016) described a preliminary investigation of active/passive RF methods for the recognition of drones. In the last two works surveyed here (Abeywickrama, Jayasinghe, Fu, and Yuen, 2017; and Azari et al., 2018), DOA approximation and surveillance drones established RF-based methods for drone optimization.

Wi-Fi-Based Detection

Many operational drones are designed and developed to be piloted via the Wi-Fi connection, allowing professionals to monitor the drone using their own intelligent devices. These types of systems often typically include a First-Person View (FPV) video capability to transmit the feed directly to the intelligent device monitor from their integrated camera. In previous studies, the concept of using the Wi-Fi signal to detect the presence of

unauthorized drones is explored by few submissions. The basic idea is to catch drone power and video transfer packet streams using a Wi-Fi channel network packet capture. This method is incorporated in specific drones designed to identify specific types of nearby equipment (Liu et al., 2015).

Nonetheless, these strategies are generally based on prior knowledge of the remotely controlled aircraft, such a as data about the Organizationally Unique Identifier (OUI) vendor used to classify the sender/receiver of unique packets (Kamkar, 2017). In this context, Bisio et al. (2018) proposed a novel method, where they suggest a model based on the study of the Wi-Fi traffic's statistical fingerprints to classify drones' position in the monitored environment. The same lead author, in two newer publications (Bisio, Garibotto, and Lavagetto, 2018; Bisio et al., 2019), conducted research on the Wi-Fi sniffing dependent drone identification through statistically analyzing Wi-Fi traffic for drone fingerprints. Other works such as Peacock and Johnstone (2013) and Terron (2017), carried out studies on the identification and disarming of drones relying on Wi-Fi signals. Last public work reviewed here is Sun et al. (2017), where a power-efficient system was implemented. The system is capable of identifying and removing video feeds from Wi-Fi-based drones, which could be an efficient mitigation solution for privacy-aware systems.

Models of Drones

This section discusses different drone types that were identified through the review of the literature and have been used in the past for a variety of missions.

1- Global Hawk RQ-4A

Schelp, Corea, and Jeffries (2003) mention that these flying objects were used during the American operations in Afghanistan and Iraq to expand the coverage area of the Jstars fleet. This aircraft flew for the first time in the year 1998 at a high altitude for a long time Baizert et al. (2006). The drone can take off with a payload of 11,600 kg.

Figure 1.1 Global Hawk RQ-4A Kvint (2012)

A heavyweight fighter, the RQ-4A is equipped with a single turbine fan and was designed to operate in a remote monitoring fashion from a low to medium threat environment. It is 31.5 meters long, its wingspan has 35.4 meters, its back and forth range is 25,000 km, has lasted 36 hours at an altitude of 65,000 feet, and has a beneficial load of 910 kg. This unmanned plane can take high-resolution pictures of large areas, works in all climatic conditions, day and night, and flies with its own capabilities or underground control. The

plane can provide 24-hour observation with a radius of 1,200 nautical miles and can conveniently hold sensors weighing up to 900 kg. These aircraft collect data with electronic optical cameras and infrared cameras for stationary, not video, imaging and radar with image detailing, at an effective range of more than 100 nautical miles.

2- Boeing X-45

Fulghum (2003) provided the information that this plane flew for the first time in May 2002 and was scheduled to enter service in 2008. The plane is 39 feet long and has a full load weight of 2.45 kg. Its flight speed reaches 0.85 Macs, a ceiling height of 4,000 feet, and a maximum range of 1,300 nautical miles.

The aircraft can be armed with multiple types of smart bombs. This plane is characterized by invisibility, and its wingspan is 10.3 meters, its length is 8.08 meters, its height is 2.94 meters, and has a complete balance of 5528 kg and a range of 600 km. A newer model of this aircraft is currently undergoing a comprehensive development under the name X-45c, which is about five meters wider than the first model and is intended to accommodate a tonnage of approximately two tons, with the possibility of providing additional fuel tanks that raise its range to 2400 km. The aircraft and its flying control equipment exhibit the latest high-tech being one of the most advanced aircraft models.

Figure 1.2 Boeing X-45 Pike, J. (2014)

Wise (2003) discusses the possibility of providing the aircraft with fuel during the desalination, which would push its advantages to be closer to those of traditional combat aircraft. Boeing intends to make the aircraft capable of carrying eight small ordnance, each weighing 113 kg, that can be loaded with the entire set of GPS target coordinates. The X-45c program has recently been expanded to also include the possibility of conducting electronic warfare and airspace operations.

3- Predator

The RQ-1 Predator drone flew for the first time in 1994. With a maximum resisting time of 40 hours, it was able to keep in contact with the ground station within a radius of 750 km for a period of 24 hours. Its main technical specifications are: its length is 8.23 meters, its wing span is 14.84 meters, its useful payload is 200 kg, and it includes electronic

sensors, two color video cameras, a forward looking infrared (FLIR) system, an artificial aperture radar SAR, and a GPS satellite data link. The aircraft can fly at altitudes up to 25,000 feet and can be equipped with laser mapping devices and two surface-to-surface missiles (the armed aircraft model is called the MQ-1 code).

Predator aircrafts connect to the ground guidance station through a ground-based information transfer link, or via a satellite link that is used when the aircraft is out of line of sight. Using these connections, the remote pilots of the aircraft can monitor the missions from ground-based locations and can perform up to 4-hour assignments from these remote locations. Predator systems were used in the Afghanistan theatre of operations and have been modified to be able to send target images directly to armed aircraft (Williams, 2013).

4- Gnat 750

Figure 1.3 Gnat, Leidy (2019)

This drone flew for the first time in 1989 and can carry electro-optical or thermal sensors. The drone can also be equipped with a SAR system. In 1994, United States intelligence used it on several missions in its operations in the former Yugoslavia theatre of operations. The drone weighs 520 kg and carries a useful load of 150 kg, can fly for 40 hours, and has an upper ceiling of 7600 meters (Ernst, 1994; Petrescu and Petrescu, 2012).

5- Neuron

Figure 1.4 Neuron, Donald, D. (2019)

The development of this French drone started in 2009 and was designed to be pilotless and it must demonstrate the ability to perform the most demanding tasks in the most severe conditions. The drone is fully integrated within the environment of the network hubs warfare, as it must reach its target with the greatest degree of concealment through the lowest radar fingerprint with infrared detection. The drone approaches the designated

target from another source of information at subsonic speeds and can deliver its mission in good conditions (Harris, Pfeiffer, Rubin, and Truman, 2015; and Kihlman and Engstrom, 2010).

6- Hunter RQ-5A

Figure 1.5 Hunter RQ-5A, Mons, de. (2017)

In 2005 the United States Army conducted its first experimental RQ-5A Hunter pilotless drone called the Endurance Hunter. The range, usefulness, and carrying capacity of the drone have been significantly expanded. This system combines a fixed-wing and double-wing hull to form a new tail and a longer middle wing to form a drone that can carry out missions of up to 30 hours at an altitude of more than 20,000 feet. The system can carry various external sensors, communication systems and useful loads of weapons.

The wing was provided with harsh points capable of carrying loads such as weaponry and also up to 110 liters of fuel to increase the drone's missions for an additional six hours.

Chapter 2

Drone Detection and Monitoring Methods

Drone Monitoring Equipment

Typically, there are four types of drone monitoring equipment:

1- Radio Frequency (RF) Analyzers

2- Acoustic Sensors (Microphones)

3- Optical Sensors (Cameras)

4- Radar

These types of monitoring equipment will be discussed in detail in the subsequent sections.

Radio Frequency (RF) Analyzers

Figure 2.1 Radio frequency (RF), Rohde & Schwarz, (2017)

Radio Frequency (RF) is one of the forms of electromagnetic energy, which includes also gamma rays, X-rays, and light. The frequency number is the number of waves that pass through a certain point in one second of any electromagnetic wave and is usually expressed in measuring units called Hertz (Fernandes, 1989).

RF energy is used in communications, radio broadcasts, television, wireless phones, pagers, police radio, space administration, and point-to-point links. Other uses of radio frequency energy include microwave ovens, radar, industrial heaters, medical treatments, military applications, and manufacturing plastic material (Fernandes, 1989).

Usually, radio frequency interference occurs, naturally or not. The interference is the effect of unwanted wireless signals as a result of one or several factors, which affects the receiving systems of communication devices, and leads to a decay in the specifications of the required signal or the loss of information about the signal that is present if the signal disappears other than when usually desirable. The interference radio frequency types can result from any of the below phenomena or actions.

1- Natural phenomena that adversely affect the electromagnetic waves (Van Der Togt, et al., 2008)
    - Lightning
    - Static electricity
    - Thermal energy
    - Solar sunspot
    - Tornadoes

2- Electrical and mechanical devices (Van Der Togt, et al., 2008)

- The effect of some components of electric lighting lamps (fluorescent). When the components of the electric lamps do not work efficiently, they emit a spark that results in a negative impact on the communications equipment.
- The effect of rotating motors emits spinning electromagnetic waves of random frequencies that cause interference events on communication devices.

3- Wireless devices (Mehrabanzad, et al., 2010)

- Pictures of some devices violating the communication system.
- Interference as a result of using one channel from more than one user in the same area.
- Interference from adjacent channels due to failure to observe the technical standards.
- Interference due to inter-modulation due to failure to observe the technical standards.
- Interference due to malfunctions of wireless devices.
- Overlap result overrun.
- Receiver overload.
- Wireless broadcast accompanying the original broadcast.
- Radio interference noise.

There are also some common types of radio interference:

1- Receiver overload.

- If a receiver is located near strong radiation transmission systems, the wireless transmission issued by these systems negatively affects the specifications of the zoom circuits in the receiver and thus leads to weak sensitivity and causes harmful interference due to the arrival of intermodulation vehicles.
- For transmitter signals to receiver antennas, there are ways to avoid this type of interference (Nanni, 2003).

2- Wireless transmission accompanying the original broadcast (out of band).

- All transmitters emit a transmitting power of the original frequency to be broadcasted in addition to transmitting a capacity for the accompanying frequencies of the original frequency, where the accompanying frequencies are known to be outside the band.
- Causes harmful interference to the receiver but can be reduced by using filters or removing the transmitters causing these interferences to distant locations. (Ru, Moseley, Klumperink, and Nauta, 2009).

3- Inter modulation product interference

- If more than one communication system is installed on one antenna, or if there are high-power communication systems close to each other, then the frequencies of these systems will mix with each other; or the frequencies of some of these systems will mix with the frequencies of the mixing circuits in the nearby receivers creating new frequencies that can cause harmful interference to the receiving systems.
- There are ways to avoid this type of interference (Babcock, 1953).

Acoustic Sensors (Microphones)

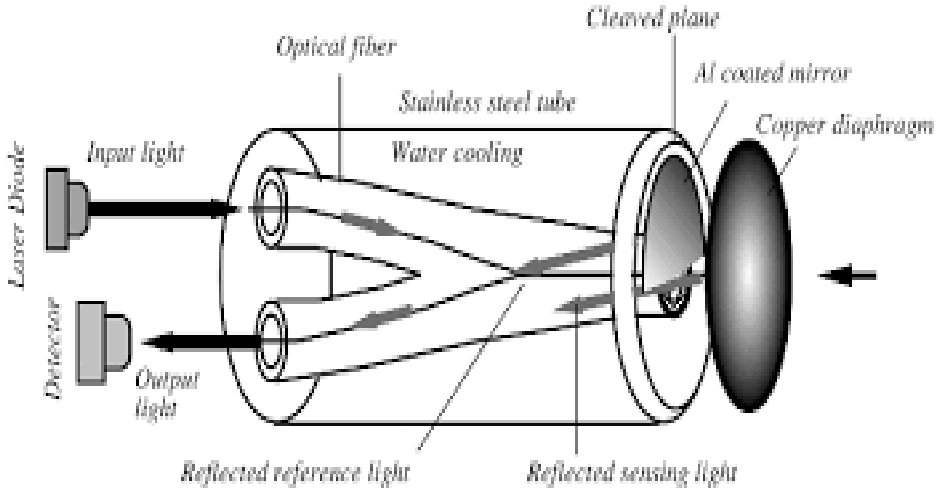

Figure 2.2 Acoustic Sensors, Sahni (2014)

Acoustic sensors (microphones) capture ultrasound waves that exceed the frequency of human-made sounds, and which are below the 20,000 Hz range. Ultrasound waves are studied by a branch of physics known as ultrasonic. Acoustic sensors have many applications in the fields of physics, chemistry, technology and medicine. They have many and varied uses, as they are used in physics to determine the properties of materials such as compressibility, elasticity, and specific heat ratios. They are also used in chemistry to produce homogeneous emulsions as used in making photographic films, as well as for the detection of cracks in plates and others.

Modern ultrasound generators generate waves with a frequency of up to a few gigahertz, by converting high-frequency alternating currents into mechanical vibrations.

These waves are usually detected using piezoelectric crystals or by light means, as the diffraction of light can benefit by making these waves visible (Sessler, 1991).

The pickup picks up the ultrasound and converts it to electrical vibrations. Then the Q1 and Q2 transistors amplify it, and it is moved to the integral circuit U1 and enters it through the terminal 14. The integral circuit compares the phase between the captured signal and the signal generated by the integral circuit whose frequency can be controlled by the C9 fractionator and gives the circuit a frequency at junction 2. The transistor Q3 amplifies the difference signal, and the signal is transmitted through the transducer T1 to the loudspeaker at the same frequency. (Ko, et al., 2009).

Ultrasound has been used for a long time to provide communications underwater and to detect submersible objects beneath it, such as submarines, in so-called sonar devices, which are radar-like devices, but they use ultrasound to perform their mission. Sonar devices are essential devices to provide safety of marine navigation. (Blumstein, et al., 2011). Sound acoustic sensors whose frequency is in the GHz field have been used to create an audio "microscope" that can distinguish dimensions from the micron rank. Surface waves whose frequency is in the ultrasound field known as Surface Acoustic Waves (SAW) play an important role in electronic control equipment (Brandstein, and Ward, 2013).

Ultrasounds are distinguished from other waves by many characteristics, the most important of which are (Lundgaard, 1992).

1- The inability of a person to distinguish them because they are beyond the human auditory range.
2- They are characterized by high frequency without other waves.

3- They are one of the shortest waves in wavelength.

4- They have the ability to travel at a high speed.

5- Some animal species can easily recognize and benefit from them.

6- They carry a medium cost in development.

7- They can provide drone direction.

Optical Sensors (Cameras)

Figure 2.3 Optical Sensors Hinkle, S., et al. (2019)

Optical sensors (cameras) are a type of digital sensor. The optical sensors use light to sense things. In the past, optical sensors were unreliable, because they used ordinary light, and therefore they were affected by ambient light. This behavior can cause many

problems, which could lead to unreliable data. The new optical sensors have been improved and became more reliable.

All optical sensors work in almost the same way, as they use a light source (transmitter) and a light detector (receiver) to sense the presence or absence of light (Narayanaswamy and Wolfbeis, 2013). Typically, optical sensors use light-emitting diodes as a type of light source. These diodes are used because of their small size, high strength and efficiency, and because they can also be turned on and off at high speed and operate at a narrow wavelength with good reliability. Optical diodes are also used in sensors in a pulse style, by sending them to vibrations (ignition and extinguishing quickly). The ignition time is very small compared to the extinguishing time, and therefore fluctuate for these two reasons. The sensor will not be affected by the surrounding light, as it increases the lifespan of the light source (Santos and Farahi, 2014).

The oscillating light is sensed by the light detector, and thus the detector captures all the surrounding light rays and searches for the oscillating light. The selected light sources are invisible to the human eye. Wavelengths are chosen so that the sensors are not affected by the light in the environment, as the use of different wavelengths is allowed by some sensors. Those are called directed color sensors to distinguish between colors. The pulse mode of the selected wavelengths makes the optical sensors more reliable. Moreover, all types of optical sensors work in the same simple manner and the differences are only in the way that the light source and the optical receiver are classified (Santos and Farahi, 2014).

There are many advantages to optical sensors (cameras) for drone detection, which are listed below (Busset, 2015).

1- Provides visuals on the drone
2- High quality
3- Fast to record
4- Potential payload can record images as forensic evidence.

At the same time, there are many disadvantages of the optical sensors (cameras) for drone detection (Müller, 2017).

1- Difficult to use for detection by itself
2- High false-alarm rates
3- Affected by surrounding factors.
4- Mostly poor performance in dark, fog, and other uncertain environments.

Radar

Figure 2.4 Radar, Techbriefs Media Group (2019)

A radar is an electromagnetic sensor used for tracking, locating, and recognizing various objects from far distances. The radar may be able to determine the size and shape of these objects as well. Radar devices' performance depend on the transmission of electromagnetic energy towards specific targets, and on the monitoring of the echoes returning from them. These targets can be aircraft, ships, spacecraft, cars, or birds. Radar devices are distinguished by optical sensors and infrared devices in their ability to accurately detect distant objects even in difficult weather conditions (Cook, 2012).

Radar systems use radio waves instead of sound waves because of their ability to reach more distances and ability to perform the work even when the signal is weak. To understand the way radar systems work, the radar detector can be used as an example. Radar systems operate the device that launches high-frequency radio waves for a microsecond period. Then the device that transmits the waves is closed, and the receiving echo device is activated, as it measures the time taken for the echo to arrive. For example, based on the radio wave speed, the distance to the plane can be measured accurately. In the case of a special equipment, by adjusting the signals, the radar system can accurately determine the aircraft speed (Skolnik, 2001). Below, several types of radars that differ according to their use, are presented.

1- Marine radar devices: used to determine the direction of the ships, the distance between them to avoid collision, and to locate them at sea based on fixed references such as islands (Harman, 2008).

2- Air radar devices: aircraft are equipped with radar equipment, in order to avoid obstruction of their path, and to determine air altitude readings accurately (Wang, et al., 2015).
3- Radar devices in missile guidance systems: used in military aircraft to determine missile destinations (Manoogian, 1999).
4- Radar devices in biological research: used to track animal and bird migration patterns. They are used in combination with weather radars to increase the accuracy of weather forecasting (Rotkovska, et al., 1993).

There are many advantages of radar systems, some of which are outlined in the below list (Baizert, et al., 2006).

1- Discovery of distant fixed objects moving from them, even if they are under the surface of the earth.
2- Identification of objects by specifying their shape on the radar screen.
3- Identification of speed of objects.
4- Assistance in mapping accurate topographic maps of planets and moons.
5- Long range accuracy.
6- Constant tracking in the monitored environment.
7- Highly accurate localization of the tracked object.
8- Handling of hundreds of targets simultaneously.
9- Tracking all drones regardless of autonomous flight characteristics.
10- Mission carried out independent of visual conditions (day, night, fog, etc.).

Drone Countermeasures Equipment

RF Jammers

Due to the rapid development of civilian drone in urban areas, many industries now look at drones as an aid for several processes such as, enhance productivity, aerial photography, geographical mapping, forest fire prevention, and agricultural pest control (Desai, et al., 2015).

The outdoor low-flying aircraft defense system is a specialized interfering and suppressing common drone used to counter malicious mission drones. The system shoots down harmful drone, by using RF frequency and GPS signal. It uses dual control, remote control signal and navigation signal, which makes the malicious drone unable to enter the defense zone, outside the emergency landing zone (Desai, et al., 2015).

GPS Spoofers

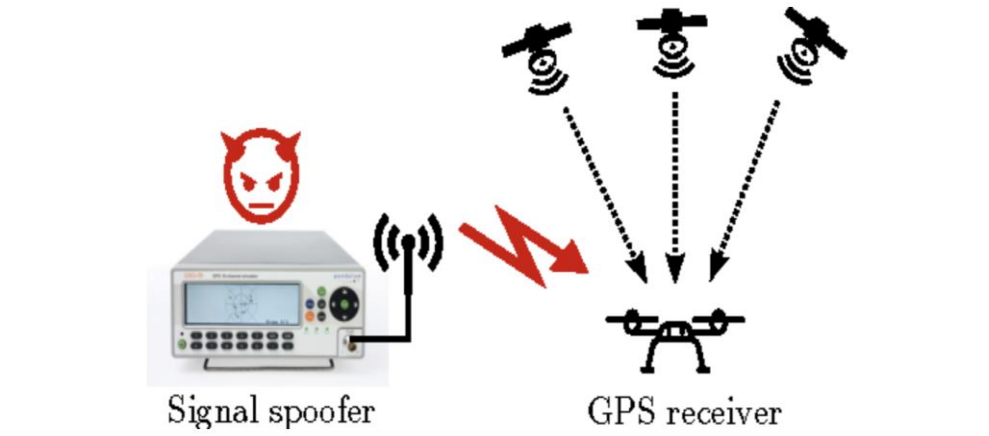

Figure 2.5 GPS Spoofers, Ranganathan, A., et al. (1970)

GPS spoofers are systems used to jam the drones' GPS signals making them unable to receive data from ground control. They are advanced systems where the jamming is

obtained with GPS systems on the system layer side, that carry the wrong information. Spoofers are characterized by a medium cost, non-kinetic neutralization, and a short range, which can affect other radio communications (McDowell, 2007).

High Power Microwave (HPM) Device

This high-power device is one of the systems used for current high-voltage applications such as diode. These high-power devices are used in ships, unmanned aircraft, power and railway stations, and large power sources that require very high-quality products. When used for drone detection, the high-power microwave systems carry out their mission with high reliability, so that the attacker drones can be stopped effectively using non-kinetic neutralization.

Figure 2.6 HPM Device, Diehl Defence (2019)

The drawback of these systems come from the risk of unintentionally disrupting communications and their high cost. Also, the neutralized drone switches off instantly, falling uncontrolled to the ground (Zhang, Zhong, and Luo, 2004).

Nets & Net Guns

Guns are weapons used during specific defend and attack scenarios. Poorly designed or manufactured guns often can lead to unsuccessful missions. In the world of gunsmithing, there are many memories of rifles that were especially bad, many of which ending of the life of brave soldiers. The rapid pace of the development of firearms in the nineteenth and twentieth centuries successfully led to avoiding the repeat of manufacturing errors, but the memories of these weapons, some of them with deadly consequences for their owner, remained and their bad reputation continues (Dizard, et al., 1999).

Figure 2.7 Nets & Net Guns, McFadden, C. (2019)

The net gun is a non-lethal weapon designed to fire shots from networks designed to obstruct and foil target movement. It is used for drone detection, to sway away birds from aircrafts, and, sometimes to save wild birds. The net gun system detects drone and physically captures them, enhancing forensics and prosecution. They have a high accuracy of mission success, a low risk of collateral damage, and exhibit a long range for the deployed nets (White and Bartmann, 1994).

High-Energy Laser

Figure 2.8 High-Energy Laser, Kautilya (2020)

The military forces around the world desire to develop small, but highly effective, laser weapon systems that can destroy enemy missiles and drones from a safe distance. However, the current weapon systems that have been designed so far are large and heavy and cannot be installed on motorized vehicles or combat aircraft. This prompted the major

players in the defense industries to look into fiber laser weapons to find alternate solutions (Apollonov, 2020)

Defense systems for manned and unmanned aircraft are experiencing unprecedented stages of development, which requires an increasing need to achieve a rapid and effective response to address these threats to aircraft of all kinds. High-power laser weapons meet these requirements, and provide a solution to this challenge, because high-power liquid laser weapons systems provide the speed and power of light to meet multiple threats. Laser weapons systems have additional offensive mission capabilities, as well as precision targeting with low potential for side effects (Guisado-Pintado, Jackson, and Rogers, 2019).

Birds of Prey

Figure 2.9 Birds of Prey, Krone (2017)

Birds of prey are all birds that feed on prey, such as animals. They are scientifically called Accipitriformes and are famous for their sharp vision and high speed, as well as their flowing wings that help them fly quickly. They have large sizes and are characterized by sharp beaks and strong claws that can tear the prey. There most known birds of prey are eagles and falcons (Redpath and Thirgood, 1997).

These characteristics need to be mimicked in the design and development of drones to obtain speed and accuracy in dealing with events, especially with a reduced risk of side damage.

Chapter 3

Proposed Drones Detection Systems

In the design and development of unmanned systems, there is always a needed trade-off between drone detection and false alarm. In this thesis, our aim is to build an optimal model for drone detection and neuralization. Hence, we propose two models, a camera-based model and a combined camera and radar-based model. After defining the models, we will study the probability of success for each of the two models. Then, a comparison among the two models will be provided in order to select the one exhibiting better characteristics.

Model 1: Camera Based Model

Figure 3.1 shows the first proposed model. This camera-based model has three main components: Sensing, Detection, and Destroying. The first component is a camera with night vision to record the scene. Then, any drones flying in the field of view will be detected by a deep learning algorithm. The results will be sent to a decision-making tool to manage the operation of the destroying system.

Unfortunately, Model 1 has some potential problems including lack of data, false alarms, and the inability to detect bird-like drones. Note that a potential solution to lack of data can use what is so-called *augmentation* or use the method proposed in Aker & Kalkan

(2017). Our second proposed model is able to overcome the false alarms and inability to detect bird-like drones.

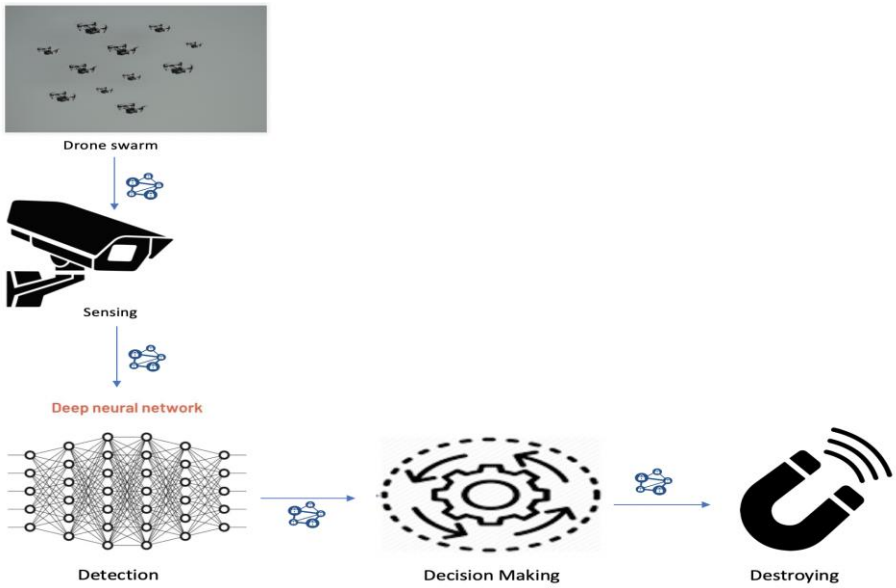

Figure 3.1 Model 1: Camera Based Model

Risk Assessment

Each method has its own risks of either miss-detect a drone or give a false alarm. Hence, this section investigates the risks associated with Model 1. Generally, weather hazards, failure to cover required places, quality issues, vision blocking, and some of the other risks can lead to miss detection of a malicious drone. However, the camera-based Model 1 has some important advantages such as:

- Ability to distinguish birds from drones
- Ability to track malicious drone and do surveillance using machine learning
- Ability to destroy a swarm of drones even though they are self-autonomous

Camera Hazard

Hazard	Hazard causes	Hazard effects
Weather hazards (heavy rain, snow, storm)	Nature	The image is not clear, or it is not taken at all
Interference	Interference with another object	
Low battery	Charging problem	Sensing component does not work
Small field of view	Not enough converge	Not able to detect drone
Quality issues	Lens accuracy	
Vision blocking	Human intervention	
Getting the camera stolen or lost	Human intervention	Not able to detect drone
Camera does not work	Technical failure	

Table 3.1 Camera Hazard

Deep Learning Hazard

Hazard	Hazard causes	Hazard effects
Expensive	Many hardware requirements	High cost
	Experts (highly paid)	
Miss detection	Lack of data	Drone reaches a target
	Bird-like drones	
	Drones have different characteristics	
	Drone and background are alike	
	Swarm of drones	

Table 3.2 Deep Learning Hazard

High Power Microwave Hazard

Hazard	Hazard causes	Hazard effects
Does not be in right location	Problem in tracking drone	Drone will not be destroyed or destroying other things
Did not go in the right time	Problem in decision making	
Device does not work	Damaged, not connected to power, or technical failure	Drone will not be destroyed
High power microwave is not connected to the system	Problem with software	

Table 3.3 High Power Microwave Hazard

The likelihood of occurrence of the camera hazards, deep learning hazards, and high-power microwave hazards causes of Tables 3.1, 3.2, and 3.3 are obtained using the rating levels described in Table 3.4. Similarly, the severity of the camera hazards, deep learning hazards, and high-power microwave hazards effects of the same Tables 3.1, 3.2, and 3.3 are obtained using the rating levels of Table 3.5. Both quantitative evaluations are measured on a 1-10 scale.

Rating	Qualitative Evaluation	Quantitative Evaluation
A	Unlikely occurrence	1-2
B	Remote occurrence	3-4
C	Occasional occurrence	5-6
D	Repeated occurrence	7-8
E	Frequent occurrence	9-10

Table 3.4 Hazard Causes Evaluation Model

Rating	Qualitative Evaluation	Quantitative Evaluation
I	No relevant effect on drone detection, analysis, and neutralizing	1-2
II	Very minor effect on drone detection, analysis, and neutralizing	3-4
III	Minor effect on drone detection, analysis, and neutralizing	5-6
IV	Major effect on drone detection, analysis, and neutralizing	7-8
V	Catastrophic effect on drone detection, analysis, and neutralizing	9-10

Table 3.5 Hazard Effects Evaluation Model

The risk assessment is obtained by multiplying the likelihood of hazard causes with the severity of hazard effects for each of the three categories of hazards: camera, deep learning, and high-power microwave. The qualitative risk assessment is obtained using the risk matrix of Table 3.6, while the quantitative risk assessment is obtained through normalization of the quantitative results of risk, such that they can be measured on a 0-1 risk scale. The low risk cells in the Risk Assessment Matrix of Table 3.6 denote a low risk of drone non-detection, incorrect analysis, and inability to neutralize the malicious drone. Consequently, as the risk increases to moderate, high, and very high, it means that there is an increased risk of non-detection, incorrect analysis, and inability to neutralize the malicious drone.

	A	B	C	D	E
I	Low	Low	Low	Moderate	High
II	Low	Low	Moderate	High	High
III	Low	Moderate	Moderate	High	Very high
IV	Low	Moderate	High	Very high	Very high
V	Moderate	High	Very high	Very high	Very high

Table 3.6 Hazard Risk Assessment Matrix

In other words, if our proposed camera-based and camera and radar-based models are successful in their missions, the mission risk assessment will be placed towards the upper left corner. If our proposed camera-based and camera and radar-based models are struggling in their missions, the mission risk assessment will be placed towards the lower right corner, with almost certainty of mission failure given by the “very high” labels.

Since there are many unknown performance metrics that compose the hazard causes and effects, an actual calculation of risk is not possible at the time of writing of this thesis. Estimating the unknown values may be not accurate and could result in the assignment of subjective risk assessment values.

Model 2: Camera and Radar Based Model

Fig. 3.2 shows our proposed camera and radar-based model. This second model includes also three main components: Sensing, Detection, and Destroying. The first component is a camera with night vision to record the scene. Then, any drones flying in the field of view are detected through the use of a deep learning algorithm. To reduce the false alarms identified in Model 1, we propose to add a radar system in parallel with our camera sensor. Figure 3.2 demonstrates the mechanisms of our second model, which has an added radar as an extra sensor to our first component. It is expected that adding a radar will reduce the false alarms, and hence significantly increase the probability of mission success. Once a drone flying in the monitored environment is detected, then the proposed system will identify it and it will be destroyed by our last component.

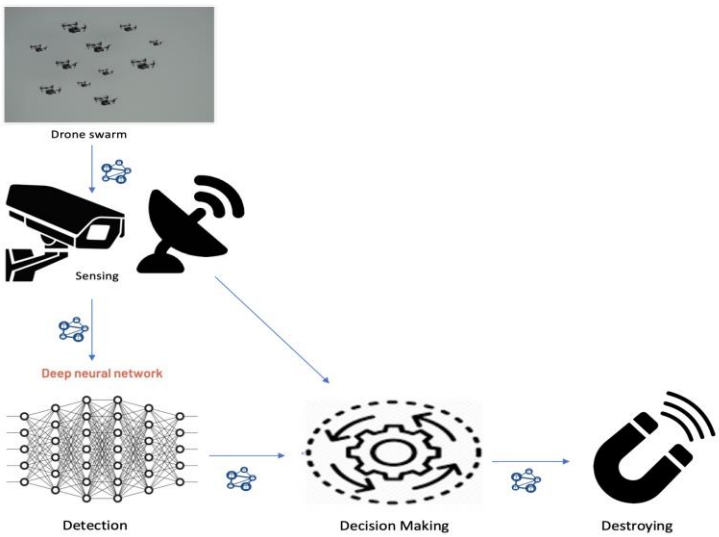

Figure 3.2 Model 2 Camera and Radar Based Model

Algorithm 1: Decision Maker Algorithm
1. While sensing 2. if {a drone is detected by DNN} 3. {Destroy} 4. elseif {a flying object is detected by Radar} 5. {Destroy} 6. elseif {a drone detected by DNN || Radar} 7. {Destroy} 8. end 9. end

Risk Assessment

Risk assessment is also performed for our camera and radar-based system, which form our second model. Model 2 considers the radar hazard in addition to already defined camera, deep learning, and high-power microwave hazards. As it can be seen from the radar hazard components, inference or radar does not work instances and some of the other risks can lead to drone non-detection.

It can be inferred that the camera and radar-based solution of Model 2 has the same features of Model 1, but in addition it helps in increasing the chances of detection under bad weather.

Radar Hazard

Hazard	Hazard causes	Hazard effects
Weather hazards (heavy rain, snow, storm)	Nature	A drone cannot be detected
Interference	Other devices	
Drone fly in low altitude	A drone designed to not be detected by radar	
Rader does not work	Damaged	Technical fault

Table 3.7 Radar Hazard

The likelihood of occurrence of the camera, deep learning, and high-power microwave hazards causes and effects of Tables 3.1, 3.2, and 3.3 are obtained on the same manner as above. Model 2 adds an extra evaluation for the radar hazard causes and effects using the same models in Tables 3.4 and 3.5. The risk assessment of Model 2 is obtained by multiplying the likelihood of hazard causes with the severity of hazard effects for each of the four categories of hazards: camera, deep learning, high power microwave, and radar. The qualitative risk assessment is obtained using the risk matrix of Table 3.6, while the quantitative risk assessment is obtained through normalization of the quantitative results of risk, such that they can be measured on a 0-1 risk scale.

Since there are many unknown performance metrics that compose the hazard causes and effects for the four hazard categories, an actual calculation of risk is not currently possible. Estimating the unknown values may be not accurate and could result in the

assignment of subjective risk assessment values that could invalidate one or both of our solution models.

Comparison

According to the rationale of the previous sections, an actual quantitative comparison of the two models is not computed. From the qualitative evaluation perspective, though, we can state that the second model that adds the radar sensor is more performant for drone detection, analysis, and neutralizing (destroying) than the first model. Many of the limitations of the first model, which can increase the risk of drone detection, analysis, and neutralizing are reduced or potentially eliminated by the second model. Therefore, for the same drone detection and neutralizing mission, the placement of Model 2 in the risk assessment matrix of Table 3.6 is most likely towards the upper left corner in comparison with the placement of Model 1 in the same risk assessment matrix.

Generally, if our proposed camera-based and camera and radar-based models are carrying out successfully their mission tasks, the mission risk assessment will be placed towards the upper left corner in the matrix of Table 3.6. But, if our proposed camera-based and camera and radar-based models are not carrying out their missions successfully, then the mission risk assessment will be placed towards the lower right corner, with almost certainty of mission failure given by the “very high” table cells.

Chapter 4

Conclusion and Future Research

Conclusion

In this thesis, we have studied malicious unmanned aircraft systems that, if left unchecked, may result in high risk, and can destroy vital assets. At the beginning of this study, we presented different models of unmanned aircraft systems that were used in the past. We also covered the solutions used for drone detection and destroying, along with outlining the advantages and disadvantages of each of the studied sensor-type.

The main threat in defense activities lies in the difficulty of detecting malicious drones. To address this threat, we proposed two counter-drone models based on smart sensors. The first model, a camera-based model, utilizes the advantage of machine learning for the detection step by using deep neural network modeling and decision-making. F utilizes the advantage of machine learning for the detection step by using deep neural network modeling and decision-making. or the second model, a camera and radar-based model, we added a radar sensor to reduce the risks of miss-detection identified for the first model. The second model also utilizes the advantage of machine learning for the detection step by using deep neural network modeling and decision-making. After that, we proposed a method to compare the mission risk assessment of the two models and inferred through

qualitative evaluation that the second model would provide an increased mission achievement evaluation in terms of malicious drone detection, correct parameter analysis, and successful drone neutralization. Thus, the second model is expected to outperform the first one in terms of drone detection and neutralizing efficiency.

Future Research

Future research can be performed on implementing the two models, which this thesis could not cover. The difficulty of implementing these models comes from the high cost, large sizes, and lack of an appropriate environment. It is possible in the future to implement these systems practically and collect actual data to validate their effectiveness. Another research direction could potentially look into adding another sensor to the system or increase the effectiveness of the previous ones. The risk assessment analysis performed in this thesis could be used for any future implementation or re-development research.

References

Kvint, P. O. (2012). Ekspert om droner til forsvaret: logik for burhøns. Retrieved March 25, 2020, from https://ing.dk/artikel/ekspert-om-droner-til-forsvaret-logik-burhoens-130492.

Pike, J. (2014). Military. Retrieved March 23, 2020, from https://www.globalsecurity.org/military/systems/aircraft/x-45-pics.htm.

Leidy, L. (2019). 10 Best Military Weapons Through History: From the AK-47 to the PrSM. Retrieved March 25, 2020, from https://www.ourmilitary.com/best-military-weapons/

Donald, D. (2019). Neuron Passes 150-flight Milestone. Retrieved February 26, 2020, from https://www.ainonline.com/aviation-news/defense/2019-01-07/neuron-passes-150-flight-milestone.

Mons, de. (2017). L'armée belge ne dispose plus que de onze drones B-Hunter. Retrieved February 20, 2020, from https://www.laprovince.be/159823/article/2017-11-29/larmee-belge-ne-dispose-plus-que-de-onze-drones-b-hunter.

Rohde & Schwarz. (2017) Retrieved February 27, 2020, from https://vipress.net/analyseur-de-reseau-analyseur-de-spectre-portables-rohde-schwarz/.

Sahni, S. (2014). Acoustic sensors. Retrieved February 26, 2020, from https://www.slideshare.net/shankarsahni2011/acoustic-sensors.

Hinkle, S., Hinkle, S., Hinkle, S., Jerry, MissusB, & Paul. (2019). Drones With Thermal Imaging - Amazing Tools Helping Advance Drone Adoption Across The Board. Retrieved March 27, 2020, from https://mavicmaniacs.com/drones-with-thermal-imaging.

Techbriefs Media Group. (2019). An Integrated Framework for Complex Radar System Design. Retrieved March 15, 2020, from: https://www.aerodefensetech.com/component/content/article/adt/features/articles/34122.

Ranganathan, A., Ólafsdóttir, H., & Capkun, S. (1970). Figure 3 from SPREE: a spoofing resistant GPS receiver: Semantic Scholar. Retrieved March 23, 2020, from https://www.semanticscholar.org/paper/SPREE:-a-spoofing-resistant-GPS-receiver-Ranganathan-Ólafsdóttir/d7a420aba8199d4aab3db1806d91dbee336e9393/figure/3.

Diehl Defence, Supercars Drone Incursion. (2019). Retrieved March 12, 2020, from https://newcastleonhunter.com/2019/11/26/supercars-drone-incursion/.

McFadden, C. (2019). 7 Examples of Anti-drone Weapons from Around the World. Retrieved March 23, 2020, from https://interestingengineering.com/7-anti-drone-weapons-used-by-the-military-and-law-enforcement-around-the-world.

Kautilya. (2020). Anti-Drone Tech Used for First Time to Guard VVIPs at Parade: Dharmakshethra - India Unabridged. Retrieved March 23, 2020, from https://dharmakshethra.com/anti-drone-tech-used-for-first-time-to-guard-vvips-at-parade/.

Krone.at. (2017). Adler: Gefiederte Räuber im Kampf gegen Drohnen. Retrieved February 26, 2020, from https://www.krone.at/555208.

S. Kamkar, “Skyjack: autonomous drone hacking w/ Raspberry Pi, aircrack&Javascript,” http://www.samy.pl/skyjack/, Accessed on: 18/ 04/2017.

Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, K. Ren, “Rise of minidrones: Applications and issues,” in Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing. New York, NY, USA: ACM, 2015, pp. 7–12

Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, K. Ren, “Rise of minidrones: Applications and issues,” in Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing. New York, NY, USA: ACM, 2015, pp. 7–12

X. Yue, Y. Liu, J. Wang, H. Song, H. Cao, “Software defined radio and wireless acoustic networking for amateur drone surveillance,” IEEE Communications Magazine, vol. 56, no. 4, pp. 90–97, APRIL 2018.

Z. Zhang, Y. Cao, M. Ding, L. Zhuang, W. Yao, “An intruder detection algorithm for vision-based sense and avoid system,” in 2016 International Conference on Unmanned Aircraft Systems, June 2016, pp. 550–556.

S. R. Ganti and Y. Kim, “Implementation of detection and tracking mechanism for small uas,” in 2016 International Conference on Unmanned Aircraft Systems, June 2016, pp. 1254–1260.

R. Stolkin, D. Rees, M. Talha, I. Florescu, “Bayesian fusion of thermal and visible spectra camera data for mean shift tracking with rapid background adaptation,” in 2012 IEEE Sensors, Oct 2012, pp. 1– 4.

M. Ritchie, F. Fioranelli, H. Griffiths, B. Torvik, “Micro-drone rcs analysis,” in 2015 IEEE Radar Conference, Oct 2015, pp. 452–456.

F. Fioranelli, M. Ritchie, H. Griffiths, H. Borrion, “Classification of loaded/unloaded micro-drones using multistatic radar,” Electronics Letters, vol. 51, pp. 1813–1815(2), October 2015.

J. Drozdowicz, M. Wielgo, P. Samczynski, K. Kulpa, J. Krzonkalla, M. Mordzonek, M. Bryl, Z. Jakielaszek, “35 GHz FMCW drone detection system,” in 2016 17th International Radar Symposium (IRS), May 2016, pp. 1–4.

J. Klare, O. Biallawons, D. Cerutti-Maori, “Detection of UAVs using the MIMO radar MIRA-CLE Ka,” in Proceedings of EUSAR 2016: 11th European Conference on Synthetic Aperture Radar, June 2016, pp. 1–4.

A. Moses, M. J. Rutherford, K. P. Valavanis, “Radar-based detection and identification for miniature air vehicles,” in 2011 IEEE International Conference on Control Applications (CCA), Sept 2011, pp. 933–940.

M. Witschi, J. Schild, B. Nyffenegger, C. Stoller, M. Berger, R. Vetter, G. Stirnimann, P. Schwab, F. Dellsperger, “Detection of modern communication signals using frequency domain morphological filtering,” in 2016 24th European Signal Processing Conference (EUSIPCO), Aug 2016, pp. 1413–1417.

Z. Kaleem, M. H. Rehmani, “Amateur drone monitoring: State-of-the-art architectures, key enabling technologies, and future research directions,” IEEE Wireless Communications, vol. 25, no. 2, pp. 150–159, April 2018.

I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, “Unauthorized amateur UAV detection based on Wi-Fi statistical fingerprint analysis,” IEEE Communications Magazine, vol. 56, no. 4, pp. 106–111, 2018.

I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, Blind detection: Advanced techniques for Wi-Fi-based drone surveillance, IEEE Trans. Veh. Technol. 68 (1) (2019) 938–946, http://dx.doi.org/10.1109/TVT.2018. 2884767.

P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, T. Vu, Cost-effective and passive RF-based drone presence detection and characterization, GetMobile: Mobile Comp. Comm. 21 (4) (2018) 30–34.
http: //dx.doi.org/10.1145/3191789.3191800.

A. Moses, M. J. Rutherford, K. P. Valavanis, Radar-based detection and identification for miniature air vehicles, in: 2011 IEEE International Conference on Control Applications (CCA), 2011, pp. 933–940.
http://dx.doi.org/10. 1109/CCA.2011.6044363.

G. J. Mendis, T. Randeny, J. Wei, A. Madanayake, Deep learning based doppler radar for micro UAS detection and classification, in: MILCOM 2016-2016 IEEE Military Communications Conference, pp. 924–929.
http: //dx.doi.org/10.1109/MILCOM.2016.7795448.

D. Solomitckii, M. Gapeyenko, V. Semkin, S. Andreev, Y. Koucheryavy, Technologies for efficient amateur drone detection in 5G millimeter-wave cellular infrastructure, IEEE Commun. Mag. 56 (1) (2018) 43–50.
http: //dx.doi.org/10.1109/MCOM.2017.1700450.

M. Saqib, S. D. Khan, N. Sharma, M. Blumenstein, A study on detecting drones using deep convolutional neural networks, in: 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance, AVSS, 2017, pp. 1–5 http://dx.doi.org/10.1109/AVSS.2017.8078541.

E. Unlu, E. Zenou, N. Riviere, Using shape descriptors for UAV detection, Electron. Imaging 2018 (9) (2018) 128–1–128–5, http://dx.doi.org/10.2352/ ISSN.2470-1173.2018.09.SRV-128.

M. Wu, W. Xie, X. Shi, P. Shao, Z. Shi, Real-time drone detection using deep learning approach, in: L. Meng, Y. Zhang (Eds.), Machine Learning and Intelligent Communications, Springer International Publishing, Cham, 2018, pp. 22–32, http://dx.doi.org/10.1007/978-3-030-00557-3_3.

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

M. Nijim, N. Mantrawadi, Drone classification and identification system by phenome analysis using data mining techniques, in: 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1–5 http://dx.doi. org/10.1109/THS.2016.7568949.

X. Chang, C. Yang, J. Wu, X. Shi, Z. Shi, A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays, in: 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2018, pp. 573–577 http://dx.doi.org/10.1109/SAM.2018.8448409.

J. Busset, F. Perrodin, P. Wellig, B. Ott, K. Heutschi, T. Rühl, T. Nussbaumer, Detection and tracking of drones using advanced acoustic cameras, Proc. SPIE Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications 9647 (2015) pp. 9647–9647–8. http://dx.doi.org/10.1117/12.2194309.

C. Yang, Z. Wu, X. Chang, X. Shi, J. Wo, Z. Shi, DOA Estimation Using Amateur Drones Harmonic Acoustic Signals, in: 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop, SAM, 2018, pp. 587–591 http://dx.doi.org/10.1109/SAM.2018.8448797.

J. Mezei, A. Molnar, Drone sound detection by correlation, in: 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics, SACI, 2016, pp. 509–518 http://dx.doi.org/10.1109/SACI.2016. 7507430.

J. Mezei, V. Fiaska, A. Molnar, Drone sound detection, in: 2015 16th IEEE International Symposium on Computational Intelligence and Informatics, CINTI, 2015, pp. 333–338 http://dx.doi.org/10.1109/CINTI.2015.7382945.

I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, Unauthorized amateur UAV detection based on Wi-Fi statistical fingerprint analysis, IEEE Commun. Mag. 56 (4) (2018) 106–111, http://dx.doi.org/10.1109/MCOM. 2018.1700340.

M. Peacock, M. N. Johnstone, Towards detection and control of civilian unmanned aerial vehicles, Proceedings of the 14th Australian Information Warfare Conference. http://dx.doi.org/10.4225/75/57a847dfbefb5.

L. Val Terron, Design, development and assessment of techniques for neutralizing drones, (Ph.D. Thesis), Galician Research and Development Center in Advanced Telecommunications, 2017, URL: http://castor.det. uvigo.es:8080/xmlui/handle/123456789/96.

A. Sun, W. Gong, R. Shea, J. Liu, X.S. Liu, Q. Wang, Drone privacy shield: A Wi-Fi based defense, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, Mobile Radio Commun., PIMRC 2017, pp. 1–5. http: //dx.doi.org/10.1109/PIMRC.2017.8292780.

H. Zhang, C. Cao, L. Xu, T.A. Gulliver, A UAV detection algorithm based on an artificial neural network, IEEE Access 6 (2018) 24720–24728. http: //dx.doi.org/10.1109/ACCESS.2018.2831911.

P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, T. Vu, Investigating cost-effective RF-based detection of drones, in: Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, DroNet '16, ACM, New York, NY, USA, 2016, pp. 17–22. https://dl.acm.org/doi/10.1145/2935620.2935632.

S. Abeywickrama, L. Jayasinghe, H. Fu, C. Yuen, RF-based direction finding of UAVs using DNN, arXiv preprint arXiv:1712.01154.

M. M. Azari, H. Sallouha, A. Chiumento, S. Rajendran, E. Vinogradov, S. Pollin, Key technologies and system trade-offs for detection and localization of amateur drones, IEEE Commun. Mag. 56 (1) (2018) 51–57. http://dx.doi.org/10.1109/MCOM.2017.1700442.

S. R. Ganti, Y. Kim, Implementation of detection and tracking mechanism for small UAS, in: 2016 International Conference on Unmanned Aircraft Systems (ICUAS), 2016, pp. 1254–1260 http://dx.doi.org/10.1109/ICUAS. 2016.7502513.

R. A. Fernandes (1989). U.S. Patent No. 4,818,990. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US4818990A/en

R. Van Der Togt, E. J. van Lieshout, R. Hensbroek, E. Beinat, J. M. Binnekade, and P. J. M. Bakker, (2008). Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. Jama, 299(24), 2884-2890. https://jamanetwork.com/journals/jama/article-abstract/182113

S. Mehrabanzad, S. Ananthaiyer, P. A. Humblet (2010). U.S. Patent No. 7,801,487. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US7801487B2/en

P. Nanni, (2003). U.S. Patent No. 6,614,806. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US6614806B1/en

Z. Ru, N. A. Moseley, E. A. Klumperink, B. Nauta (2009). Digitally enhanced software-defined radio receiver robust to out-of-band interference. IEEE journal of solid-state circuits, 44(12), 3359-3375. https://ieeexplore.ieee.org/abstract/document/5342340/

W. C. Babcock, (1953). Intermodulation interference in radio systems frequency of occurrence and control by channel selection. The Bell System Technical Journal, 32(1), 63-73. https://ieeexplore.ieee.org/abstract/document/6768265/

G. M. Sessler, (1991). Acoustic sensors. Sensors and Actuators A: Physical, 26(1-3), 323-330. https://www.sciencedirect.com/science/article/pii/092442479187011Q

W. H. Ko, R. Zhang, P. Huang, J. Guo, X. Ye, D.J. Young, C. A. Megerian, (2009). Studies of MEMS acoustic sensors as implantable microphones for totally implantable hearing-aid systems. IEEE Transactions on Biomedical Circuits and Systems, 3(5), 277-285. https://ieeexplore.ieee.org/abstract/document/5259709/

D. T. Blumstein, D. J. Mennill, P. Clemins, L. Girod, K. Yao, G. Patricelli, S. F. Hanser, (2011). Acoustic monitoring in terrestrial environments using microphone arrays: applications, technological considerations and prospectus. Journal of Applied Ecology, 48(3), 758-767. https://besjournals.onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2664.2011.01993.x

M. Brandstein, D. Ward, (Eds.). (2013). Microphone arrays: signal processing techniques and applications. Springer Science & Business Media. https://books.google.com/books?hl=en&lr=&id=JinrCAAAQBAJ&oi=fnd&pg=PA3&dq=applications+Acoustic+sensors+(microphones)&ots=UjmMRaStox&sig=15CytvUF2vzDDx_OQUSLqpiO2i0

L. E. Lundgaard, (1992). Partial discharge. XIV. Acoustic partial discharge detection-practical application. IEEE Electrical Insulation Magazine, 8(5), 34-43. https://ieeexplore.ieee.org/abstract/document/156943/

R. Narayanaswamy, O. S. Wolfbeis, (2013). Optical sensors: industrial environmental and diagnostic applications (Vol. 1). Springer Science & Business Media.

https://books.google.com/books?hl=en&lr=&id=Bs7sCAAAQBAJ&oi=fnd&pg=PA1&dq=R.Narayanaswamy,+%26+O.S.Wolfbeis,+O.+S.+(2013).+Optical+sensors:+industrial+environmental+and+diagnostic+applications+(Vol.+1).+Springer+Science+%26+Business+Media.&ots=9Ph_9sHSLf&sig=_CJh5Y_PZFIc9QtMUbT59IcGLws.

J. L. Santos, F. Farahi, (Eds.). (2014). Handbook of optical sensors. CRC Press. https://books.google.com/books?hl=en&lr=&id=yY7aBAAAQBAJ&oi=fnd&pg=PP1&dq=work+of+Optical+Sensors++&ots=VyBbDp1xak&sig=5UGIWl9lryv0g8uODMtjVdRBSIA

J. Busset, F. Perrodin, P. Wellig, B. Ott, K. Heutschi, T. Rühl, T. Nussbaumer, (2015). Detection and tracking of drones using advanced acoustic cameras. In Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications (Vol. 9647, p. 96470F). International Society for Optics and Photonics. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9647/96470F/Detection-and-tracking-of-drones-using-advanced-acoustic-cameras/10.1117/12.2194309.short

T. Muller, (2017). Robust drone detection for day/night counter-UAV with static VIS and SWIR cameras. In Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII (Vol. 10190, p. 1019018). International Society for Optics and Photonics.

https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10190/1019018/Robust-drone-detection-for-day-night-counter-UAV-with-static/10.1117/12.2262575.short

C. Cook, (2012). Radar signals: An introduction to theory and application. Elsevier. https://books.google.com/books?hl=en&lr=&id=hB3CQQ7jBckC&oi=fnd&pg=PP1&dq=radar+introduction&ots=imE-YzazFb&sig=ij7lCT11mbtDfNjevSpG8YgEw-M

M. I. Skolnik, (2001). RADAR systems. McGraw-Hill, NY. https://pdfs.semanticscholar.org/2a47/4223090a15445faae325bdedd3691af2b649.pdf

S. Harman, (2008). The performance of a novel three-pulse radar waveform for marine radar systems. In 2008 European Radar Conference (pp. 160-163). IEEE. https://ieeexplore.ieee.org/abstract/document/4760826/

H. Wang, J. Johnson, C. Baker, L. Ye, C. Zhang, (2015). On spectrum sharing between communications and air traffic control radar systems. In 2015 IEEE Radar Conference (RadarCon) (pp. 1545-1550). https://ieeexplore.ieee.org/abstract/document/7131242/

D. V. Manoogian, (1999). U.S. Patent No. 5,917,442. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US5917442A/en

D. Rotkovská, J. Moc, J. Kautská, A. Bartonícková, J. Keprtová, M. Hofer, (1993). Evaluation of the biological effects of police radar RAMER 7F. Environmental health perspectives, 101(2), 134-136.

https://ehp.niehs.nih.gov/doi/abs/10.1289/ehp.101-1519743

P. Baizert, T. B. Hale, M. A. Temple, M. C. Wicks, (2006). Forward-looking radar GMTI benefits using a linear frequency diverse array. Electronics Letters, 42(22), 1311-1312. https://digital-library.theiet.org/content/journals/10.1049/el_20062791

P. Desai, G. Desjardins, V. Roussel, (2015). U.S. Patent No. 9,197,332. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US9197332B2/en

C. E. McDowell, (2007). U.S. Patent No. 7,250,903. Washington, DC: U.S. Patent and Trademark Office. https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.19

J. Zhang, H. H. Zhong, L. Luo, (2004). A novel overmoded slow-wave high-power microwave (HPM) generator. IEEE transactions on plasma science, 32(6), 2236-2242. https://ieeexplore.ieee.org/abstract/document/1366516/

J. E. Dizard, R. Muth, R. Merrrill, S. P. Andrews, (Eds.). (1999). Guns in America: a reader. NYU Press. https://books.google.com/books?hl=en&lr=&id=ZyYTCgAAQBAJ&oi=fnd&pg=PR9&dq=Guns+introduction+&ots=hSa-hZcIgH&sig=IWzelBdcSpKH6MxJszRpKRuD4zU

G. C. White, R.M. Bartmann, (1994). Drop nets versus helicopter net guns for capturing mule deer fawns. Wildlife Society Bulletin (1973-2006), 22(2), 248-252. https://www.jstor.org/stable/3783253

V. Apollonov (2020). High Energy Ecologically Safe HF/DF Lasers: Physics of Self Initiated Volume Discharge based HF/DF Lasers.

https://www.taylorfrancis.com/books/9781003041962

E. Guisado-Pintado, D. W. Jackson, D. Rogers, (2019). 3D mapping efficacy of a drone and terrestrial laser scanner over a temperate beach-dune zone. Geomorphology, 328, 157-172. https://www.sciencedirect.com/science/article/pii/S0169555X1830504X

S. M. Redpath, S. J. Thirgood, (1997). Birds of prey and red grouse. Stationery Office. http://nora.nerc.ac.uk/id/eprint/5029/1/Birds_of_prey.pdf

D. D. Berger, H. C. Mueller, (1959). The bal-chatri: a trap for the birds of prey. Bird-banding, 30(1), 18-26. https://www.jstor.org/stable/4510726\

D. Canal, J. J. Negro, (2018). Use of drones for research and conservation of birds of prey. In Birds of Prey (pp. 325-337). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-73745-4_14

T. Schelp, V. Corea, J. Jeffries, (2003). Development of the RQ-4A Global Hawk propulsion system. In 39th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit (p. 4680). https://arc.aiaa.org/doi/pdf/10.2514/6.2003-4680

D. A. Fulghum, (2003). Boeing Redesigns X-45 At the orders of Darpa, the unmanned X-45C strike aircraft will offer increased size, range and payload. Aviation Week & Space Technology, 158(18), 38-38. https://elibrary.ru/item.asp?id=6167452

K. Wise (2003). X-45 program overview and flight test status. In 2nd AIAA" Unmanned Unlimited" Conf. and Workshop & Exhibit (p. 6645). https://arc.aiaa.org/doi/pdf/10.2514/6.2003-6645

P. P. Saratchandran, K. C. Ajithprasad, K. P. Harikrishnan, (2015). Numerical exploration of the parameter plane in a discrete predator–prey model. Ecological complexity, 21, 112-119. https://www.sciencedirect.com/science/article/pii/S1476945X14001536

B. G. Williams, (2013). Predators: The CIA's drone war on al Qaeda. Potomac Books, Inc https://books.google.com/books?hl=en&lr=&id=9UtQeSKJRUQC&oi=fnd&pg=PP2&dq=predator+is+the+only+plane+in+the+United+States+of+America+&ots=U9diB6xxew&sig=BG1BAkYFZ4Hg0R-ICZx_CDxBg4o

L. L. Ernst (1994) Medium Altitude Endurance Unmanned Air Vehicle. In Airborne Reconnaissance XVIII (Vol. 2272, pp. 103-112). International Society for Optics and Photonics. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/2272/0000/Medium-Altitude-Endurance-Unmanned-Air-Vehicle/10.1117/12.191909.short

F. I. Petrescu, R. V. Petrescu, (2012). New Aircraft II. BoD–Books on Demand. https://books.google.com/books?hl=en&lr=&id=cwjd0K8NCucC&oi=fnd&pg=PA3&dq=A+US+drone+flew+for+the+first+time+in+1989.+It+can+carry+electro optical+or+thermal+sensors,+and+it+can+also+be+equipped+with+a+SAR+system.+In+1994,+US+intelligence+used+it+on+several+missions+in+its+operations+in+the+former+Yugoslavia.+It+weighs+520+kg+an&ots=7B0keFkDs2&sig=funp883nI5yo07QeZITu3OuTI84

R. M. Harris, B. D. Pfeiffer, G. M. Rubin, J. M. Truman, (2015). Neuron hemilineages provide the functional ground plan for the Drosophila ventral nervous system. elife, 4. https://elifesciences.org/articles/04493

H. Kihlman, M. Engstrom, (2010). Flexapods-Flexible tooling at SAAB for building the NEURON Aircraft (No. 2010-01-1871). SAE Technical Paper. https://www.sae.org/publications/technical-papers/content/2010-01-1871/

J. Kosmatka, A. Valdes (2006). Accurate structural dynamic modeling of the Hunter UAV using ground vibration testing. In 47th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 14th AIAA/ASME/AHS Adaptive Structures Conference 7th (p. 1744). https://arc.aiaa.org/doi/pdf/10.2514/6.2006-1744

C. Aker and S. Kalkan, "Using deep networks for drone detection," 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Lecce, 2017, pp. 1-6.