Small Unmanned Aerial Vehicle Identification using Radar

Master Thesis for the Delft University of Technology

by

M.G. Bezema

Student number:	4248252
Project duration:	May 1, 2021 – September 30, 2022
TU Delft supervisor:	Prof. M. Conti
Daily supervisor:	Dr. A. Brighente
Military supervisor:	Cpt. B. van der Ven

TU Delft

Abstract

Attacks using drones are increasing, war zones see more and more use of drones and civilian areas are threatened by cheap commercial drones. In order to prevent drone attacks, they have to be detected; identified and neutralized. Faster identification results in more time to respond, making identification vital. This thesis uses radar to identify drone threats using behavioral history. The basis for identification is created by flying experiments around critical infrastructure whilst recording the movement using radar. Subsequently multiple identification algorithms are compared to determine the fastest and most accurate way of identification. We determined distance to critical infrastructure and degrees scouted around critical infrastructure are the most important features. Next to that, the random forest achieves 96% accuracy, decreasing to 86% when challenged. The decision tree scores 94% accuracy, but due to its explanatory nature it becomes the desired algorithm. Understanding the basis for action is essential in neutralizing drone threats, making decision trees the preferred method of identification.

Contents

1 Introduction

This chapter provides an introduction into the thesis. It first introduces the field and relevance of this thesis in **Section 1.1**. **Section 1.2** introduces the subject. Followed by an explanation of the research question in **Section 1.3** and ending in an overview of the structure of the thesis in **Section 1.4**.

1.1. Relevance

With the advent of widespread use of cheap commercial Unmanned Aerial Vehicles (UAVs) or Drones[1] comes an array of potential security issues, such as delivering contraband to secured locations [71], performing acts of terror [22] or committing privacy violations [21]. These issues are becoming increasingly dangerous and prevalent, due to the low cost of attaining and arming a drone. Cheap drones create a big economical asymmetry in war zones, insurgents build and operate drones for around 2000 euros. The drone can subsequently fly into an air base and take out a $300m fighter jet, providing a 'profit' of $299.999.998 [22]. Conversely, protection against a single drone is the use of specially fitted stinger-missiles costing around $175.000 each, a loss of $173.200. In other words, if the decision is made to deactivate a drone, it has to be correct. In order to combat drone security threats Solomitckii et al. [63] define 5 stages and issues in preventing a drone attack, the 4^{th} step is expanded with identification. The 6 steps are shown in **Figure 1.1**. Classification step is further subdivided into Classification and Identification for clarification.

Figure 1.1: Drone attack prevention process

The first step, Detection, is becoming aware of objects entering an area that is safeguarded. After detecting an object entering an area we want to find out where exactly it is located, i.e. Localization. When the location is determined we want to keep on determining the location over time, i.e. Tracking. Following Tracking comes classification, determining the type of object we are tracking. Types like birds or trees are not relevant, types like fixed-wing drones or quad-copters are. Knowing the presence, location, movements and type of an object does not provide sufficient grounds for action. To determine the ground, the next step is identification, more specifically identification of a threat or no threat. Identification is the topic of this thesis, designing an algorithm for identifying drones based on tracking information. We perform valuation of and identification algorithm by running it against real-world simulations. Deactivation is the final step in the drone attack prevention process, this is currently another major problem in the process and a whole field of research in its own right. With scoping in mind, only Identification is addressed extensively in this thesis. For the other steps, the state of the art is discussed in **Related Work**.

[1] For the rest of the thesis the term drone will be used.

1.2. Subject

The primary subject of this thesis is use of radar data to perform identification of drones. With the rapid technological advances in drone sophistication, radar is the preferred method of detection. Additionally it is robust at detection in changing environments. Identification is chosen because it is a complex, urgent and little researched part of the literature surrounding drones.

This thesis is written in cooperation with the military. The military provides access to radar and flies experiments to generate data. In return we perform research that aids the military in the identification process. The military currently uses a combination of radar and camera to identify drones. Radar uses electromagnetic waves that reflect off the surfaces on the drone to detect, localize and track it [35]. The signature created by the reflection is used by the radar to classify it. Identification is performed entirely by an operator with the assistance of a very high resolution camera. This method is effective in short range, clear weather environments with a small amount of drones, extrapolation to more difficult environments or a multitude of drones becomes problematic.

The aim of this thesis is augmenting the identification process of the military operators. The question posed by the military is: "is it possible to use radar data to improve identification by a radar-operator?". In practice this translates to: is it possible to add a threat level to drones classified by the radar to identify their intent? The operator can then use the added information to make better decisions. In layman's terms: the monitor with radar data changes color for drones representing threat.

Due to the nature of the subject and the repercussions of deactivation, an important component in the recommendation towards the military is comprehensibility. The imperfect nature of the real world and chances of freak occurrences, requires the basis for action to be clear. The operator needs to justify deactivating a drone using comprehensible information. A clear example of this is the story of Stanislav Petrov: in September 1983 Stanislav prevented global nuclear war when the sensors on his radar system told him the United States were launching multiple nuclear warhead. Because he could see the basis for the warhead launch warning and determined they were highly unlikely he decided not to take action and saved our world as we know it today [31]. For this research it translates into a preference for a sufficient and clear basis of information for the operator. Enriching the information basis and preferring white box or "explainable" algorithms as solutions[2].

1.3. Research Question

The aim of this thesis is to use data extracted from a radar system to perform identification of unmanned aerial vehicles. The research question is: "How accurately can we identify Intelligence, Surveillance, Reconnaissance (ISR) from non-ISR behavior in drones using data collected by radar? ". The central hypothesis this thesis answers is "there is no significant difference in behavior, as detected by radar, between ISR drones and other types of drones.". The solution accepts or rejects this hypothesis and uses it to answer the research question.

To answer the research question, time series data is gathered using radar. Due to the lack of available data it is generated by flying experiments. During these experiments a radar collects flight information. After collecting the data it is converted to a flight path. Using these flight paths a comparison is made to check for a significant difference in behavior within flight paths. If there is a significant difference in behavior this difference is used to build a model which identifies the actors.

This thesis will not focus on detection, localization, tracking, classification or deactivation of drones. A lot of research is done on these topics and there is still a lot more to be done. However the scope of this thesis is to initiate the literature on drone identification.

[2] White box algorithms are defined further in **Section 5.3.2**

1.4. Structure of the Thesis

The first chapter of the report is the **Introduction**, where the relevance of the subject is argued and the research question posed. The second chapter is the **Related Work**, this chapter provides an overview of the current research in this field and positions this thesis within the current state of the art. Chapter 3, **System Model**, presents the system within which this research will take place. The system model discusses the preliminary information needed in order to understand the system used to identify drones. In the **Threat Model**, an overview of threat actors their resources, capabilities and common behavior is given. Following the threat model the 5^{th} chapter **Solution** expands on the previous chapters by proposing a solution to the threats of the system. It discusses the general method and algorithms proposed to provide a mitigation of the stated threat. The **Evaluation**, goes deeper into the solution and explains how the solution is tested, it then explores the data and provide numerical results. With the 7^{th} chapter, **Future Work**, the recommendations for improvement of the provided solution is given. Ultimately chapter 8, **Conclusion**, will summarize the work done and provide an answer to the hypothesis and the research question. Additionally it will contain a recommendation for the military based on the results of this thesis.

2

Related Work

This chapter provides an overview of the state of the art in drone attack prevention. The chapter is divided into the steps of the drone attack prevention process. Starting off with the literature surrounding detection, localization and tracking in **Section 2.1**. Followed by a foray into the deactivation literature in **Section 2.2**. **Section 2.3** then provides an overview of classification literature. The central focus of this thesis will then be discussed in **Section 2.3.2**. Finally the knowledge gap which this thesis fills is given in **Section 2.4**. A very extensive and fascinating literature review of counter-drone systems around airports is provided by Lykou et al. [39]. This literature review has a similar focus and expands on their work.

2.1. Detection, localization and tracking literature

A large amount of literature is being produced in the field of detection [3, 7, 18, 59, 60, 63, 65, 88][1]. The literature of drone detection can be divided into two major methods: detection of air vibration (sound) or detection of electromagnetic radiation (visible light, WiFi, Bluetooth, etc.). In both methods a receiver is used to receive the signals sent by another object[2]. The limiting factors in detection of signals are the strength of the signal as well as the amount of similar signals (or noise). With drone attack prevention comes another dimension to signal detection: adversarial behavior. A malicious operator will try to diminish a signal, avoid an active signal or even try to flood a receiver with signals so that it is very difficult to detect the malicious drone. Alternatively he might try to alter the signal, to try and confuse a receiver.

The adversarial factor produces a preference for passive detection methods, where the detector only receives incoming signals. Imagine standing on a field and watching for something to approach, you wait for light to come from the sun and bounce of the object (some other examples are SONAR, Camera, WiFi receivers). As opposed to active methods where a signal is sent and the time taken to return to the sender is measured. Imagine standing in the same field but there is no sun to provide a signal, you now need to use a flashlight to bounce light of an object to see it approaching (other examples include Radar, Echolocation, Identification Friend or Foe). In the passive method, if the object is adversarial, it does not know that you are looking for it. In the active method you are standing there with a flashlight so it is easy for the adversary to know that you are looking for him. The rest of this section is dedicated to providing a short overview of the main methods used in detection.

2.1.1. Air vibration

First of all, detection of air vibration. This method involves the implementation of an acoustic array (an array of microphones) to listen for sound produced by drones. The literature on this method is improving but still not impervious to the limitations of signals mentioned before [4, 11, 13, 57]. An environment with a lot of noise such as urban area's will severely limit the effectiveness of this method. On top of that the effective

[1] This whole section will be focused on detection, even though localization and tracking are distinct activities it is assumed that they are possible with detection for purpose of brevity.

[2] some methods, often called active, like radar and echolocation first send a signal towards an object and record the return of the signal bouncing of the object. The active part referring to the active sending of a signal.

range is just around 300m, which is short if a drone is flying at top speed towards an objective it wants to attack [11, 57]. Another downside is that acoustic sensors use a database of know drone sounds, an unknown sounds from a new or adjusted model will go undetected [39]. All in all this method will likely be developed further in the future, but currently does not look promising.

2.1.2. Electromagnetic radiation

The second major detection method is the detection of electromagnetic radiation. Electromagnetic radiation "refers to the waves (or their quanta, photons) of the electromagnetic field, propagating through space, carrying electromagnetic radiant energy" [49, 73]. The difference in the frequency of the wave defines its name, some examples ordered from low to high frequency: radio, microwave, Bluetooth, WiFi, visible light and X-rays. The main electromagnetic waves used in detection of drones are visible light or optical based methods, radio frequency detection and radar based detection.

Visible light or optical based detection is a promising method of detection, localization, tracking. Proposed systems include using camera's attached to cars or drones [53, 58] or the use of a wide-angle stationary camera to perform broad range detection [70]. The limitations of optical methods are their sensitivity to low-visibility environments (lots of other objects to bounce the reflections off) as well as a limitation on range, depending on the camera used. Optical methods in the right environment are however a very promising method in the detection of drones.

Passive Radio Frequency (RF) detection is a good example of a passive detection method that is slowly becoming obsolete. As mentioned in **the introduction to this chapter** some drones require a constant connection with its operator in order to receive orders. This connection between a drone and its operator requires both parties to send radio waves in order to communicate. Radio frequency is the most popular method but WiFi or Bluetooth based methods work in the same way, a WiFi or Bluetooth receiver could also be used to detect if a drone is present (and communicates via that medium) [23, 45]. The limitation of this method is the increasing technological advancement of drones, such that they can fly without a connection to its operator (i.e. navigation based on GPS coordinates or even solely on an inertial measurement unit (IMU) or lasers as used in GPS deprived environments [20]) making it impossible to passively detect them. Another downside of RF based detection, accurate till 600m [45], is that in environments with a lot of RF use (for Wi-Fi, mobile data, etc.) detection of RF can be limited to just 100m [56].

An active way of using the radio frequency for detection is commonly referred to as radar. Radar consists of an electromagnetic wave transmitter and receiver. Waves are sent by the transmitter and upon encountering an object bounced back towards the receiver. The returning waves towards the receiver provide information on it's size and distance. The main challenge of using radar in the detection of drones is the choice of frequency used. High frequency radar is very accurate but only up to several tens of meters. Whereas low frequency radar has a very large range but has difficulty detecting smaller objects such as drones [44, 61]. The downsides of radar based detection are the costs, interference by obstacles, lower detection rates in crowded air spaces and the difficulty of classification or identification [39]. Interference by obstacles is a problem suffered by all detection methods, a possible solution is usage of multiple radar systems placed at different locations to maximize coverage. Lower detection rates in crowded air spaces can be prevented by higher frequencies and usage of multiple radar systems.

An interesting development in the field of drone attack prevention is the utilization of drones to mitigate the limitations of detection methods. A system of smaller drones that is communicating with a control station is deployed in an area. When an unidentified drone enters the area the relay drones perform the act of detection, tracking and localization by flying towards and following the unidentified drone [3, 12]. Use of smaller drones is limited by the speed of the used drones (packed with sensors and deactivation methods to perform its task), the weather conditions (smaller drones are more susceptible to bad weather) and the cost of designing and implementing a large system of drones like this.

In conclusion, detection is a big field of study which is constantly evolving and improving. It consists of a variety of different methods for detection each having its challenges. Based on the nature of the adversary and the environment in which to operate a choice has to be made for a specific method. Before exploring the literature of classification, the next section provides a short discussion of the current deactivation literature.

2.2. Deactivation literature

Deactivation of drones as explained in the introduction can be a very expensive and difficult process. With deactivation the goal is to make sure that a drone is not able to continue it's mission. In order to perform it's mission the drone has to receive an objective, navigate towards it and execute a task (possibly returning to it's operator afterwards). Deactivation is aimed at preventing the drone from receiving an objective, making navigation towards it impossible or by simply destroying or immobilizing the drone.

The first step is the receiving of an objective, simply put: if a drone has no objective it can not execute it. The simplest way that a drone receives and executes objectives is by having an active connection to it's operator. The operator continuously receives a video feed and sends commands toward the drone in real-time. Deactivating a drone with an active connection can be as simple as flooding the medium with which it communicates so that it is unable to receive other commands (jamming). A major drawback of jamming, however, is that it also interrupts surrounding actors using the same medium (airplanes, friendly drones or even radar systems). The solution being the use of rifle-like jammers that jam only a small beam (in busy area's this is still to blunt an instrument) [47]. Conversely the connection could be hijacked, giving control of the drone to the defenders. There are even examples of counter-drones being able to hijack a drone mid-air [54].

An alternative to an active connection is the use of a more abstract set of commands (follow a specific object). Allowing the drone to temporarily lose connection to its operator while still being able to execute its objective. This connection is still open to jamming and could be hijacked by a defender.

Finally drones can circumvent these defenses and be pre-programmed with an objective before being deployed (follow magnetic direction for x minutes). Allowing its operator to drop the drone off, drive far away and let it execute it's task. Making it very difficult to deactivate this drone. Jamming is not possible on most frequencies, however the drone could still be GPS based. Hijacking the "session" existing between the drone and it's operator is no longer possible. Supply chain attacks are however still possible.

An alternative to changing the objective of a drone is the interruption of it's navigation module. A fully autonomous drone, without a connection to its operator, can still execute objectives. Instead of navigating via the operator it uses methods like an IMU sensor, LiDAR, microphones, GPS, camera or heat sensors [20]. Navigating using solely these sensors is often complicated and can be performed by swarms of drones communicating together [14, 84]. Fully autonomous drones are still very sophisticated so it is unlikely to be used by most actors, but it will become easier in the future. In the case of a fully autonomous drone the attacker will have to determine its means of navigation and then attack it accordingly or resort to the final method of deactivation.

The main method of taking down drones is often referred to as the "kinetic approach", where the drone is taken down by using kinetic force. The first example was created in the Netherlands and involves the use of birds of prey [39]. The drawback of this is the training required, but also the need for the birds to be in a constant state of hunger in order to be willing to attack a drone. The second example, already alluded to in the introduction is the use of rockets. This is a very expensive method, especially when considering the cheap cost of building a drone. Additionally this method has the potential for collateral damage as well as the spreading of fear when used in urban environments. Alternatively, companies proposed the use of drones carrying nets which they can deploy on malicious drones [39]. Finally the use of hunter drones carrying means to deactivate a malicious drone could still be considered. Limiting factor being its requirement to be fast to get near to a malicious drone as well as being capable of carrying a payload useful in taking down said drone.

Finally, depending on influence and resources of the defender, a supply chain attack could be performed. Supply chain attacks assume the defender has access to part of the supply chain of the attacker. This allows the defender to build in a kill-switch into the drone without the knowledge of the attacker. The ability to build your own drone from scratch makes this kind of deactivation a lot more difficult (even then the hard- and software could still contain a kill-switch).

In the end the deactivation of drones is not a straightforward process and research will have to be done. The taking down of a single drone is difficult and often expensive. Combined with the low cost of producing

a drone and with that the opportunity to create multiple attacking drones is a serious threat. Before deactivation can happen though, classification must still be performed. Lest a non-malicious drone is taken down accidentally. The next section will go deeper into the known classification methods.

2.3. Classification literature

The central subject of this thesis is the classification and more specifically the identification step in drone attack prevention. This section provides an overview of the main strategies used in classification. Starting off with a deep dive in the classification literature in **section 2.3.1**, zooming in on identification specific literature in **section 2.3.2**. Finising with zooming in on, and justifying behavior based identification methods in **section 2.3.3**.

2.3.1. Classification

Classification or the determining of the type of drone detected is a challenging subject. It involves distinction between any type of material in the air, birds and drones (as well as type of drone).

Acoustic based detection method look attractive at short ranges (less than 300m [57]). A positive aspect is that they can differentiate between models and even load of a drone, providing basis for classification and more specifically identification. However acoustic fingerprints vary based on weather conditions. A hot, zero wind day at an open plain has different fingerprints than a cold, high wind day in the forest [42]. However in environments with high amounts of noise the arrays are not effective [39].

Optical based methods are also seen as a realistic method of classification. Proposed systems include the use of a wide-angle camera to perform broad range and general detection and is then supported with a higher resolution camera to perform classification [66, 70]. The paper suggests using it as a primary filter in the classification task and backing it up with a more precise method. Classification distances are not mentioned. The limitations of optical methods are their sensitivity to low-visibility environments as well as a limitation on range, depending on the camera used. Optical methods in the right environment are a very promising method in the classification of drones. Currently the main focus has been on classification of Persons or animals [82], but drone classification is increasingly performed [66]. A good supplementation to optical detection is the use of radars, Chadwick et al. [10] proposes the use of camera in combination with radar to perform small object detection. They show that radar classification can be improved by use of camera. This expands upon the longer range provided by radar for detection. But still suffers from the drawbacks of environmental effects like clouds and rain.

Classification based on radar is attractive due to it being unaffected by low visibility, fog or haze, unlike optical methods [32]. It is also resistant to the use of camouflage. The most prevalent radar based classification method is the use of a micro-Doppler to distinguish between birds, planes or drones is. Statistically describing the micro-Doppler signature of an object [15, 26, 43, 52]. However drones which have a smaller Radar Cross Section (RCS) can still be difficult to detect. [32, 80].

An interesting radar based classification method is the use of range profiles. One of the first attempts at this has been done by Zyweck and Bogner [89], classifying between Boeing 727 and Boeing 737 aircraft. This is done using High Range Resolution Profiles, they achieve high accuracy with simple classifiers. Zhang et al. [87] has shown that using high frequency radar and neural networks it is possible to use bi-spectra to classify targets. Mentioning that the range profile "which is the projection of a target's back-scattering on the radar line of sight" is a suitable identification vector. However these range profiles are sensitive to time shift and aspect angle change. The limitation here being the large size of the objects on which classification has been performed. Another limitation compared to our research is the use of raw signal data. The radar systems used by our research will not provide this kind of data. In conclusion, this method look promising and will have to be performed on smaller objects but this is not within the possibilities of our research.

2.3.2. Identification

In the identification step the aim is to determine intent of an object classified as a drone. Identifying it as a friend or foe.

The first strategy comes from commercial air traffic control. Commercial air traffic is a mature and related field, it uses a system of Identification Friend or Foe (IFF), which consists of a transponder fitted to aircraft and a radar-based system for identification. The traffic controller sends an interrogation signal to an unidentified object. The responder on the unidentified object then sends a response, identifying itself [72]. One limitation of IFF is the occurrence of spoofing or the presence of a malfunctioning transponder, resulting in miss-identification.

A very crude but effective method is a simple no-fly zone: define a zone within which every object is considered to be malicious and will thus be deactivated. In some situations this will be sufficient. However in events where friendly drones are used for patrolling or where media drones are present for recording this can be undesirable. Additionally the no-fly zone only starts identification once it is entered, decreasing the response time to threats by operators. No-fly zones can be augmented by an IFF system to create a very robust identification method. If a drone cannot identify itself and is within a no-fly zone, it is considered hostile and will be deactivated.

Another alternative to radar is the use of relay/surveillance drones to perform in-flight IFF. A system of smaller drones that is communicating with a control station is deployed in an area. One of the smaller drones is fitted with a camera and a pre-trained machine learning algorithm that is used to perform identification for speeds up to 1.5 m/s, achieving a detection accuracy of 77% [3, 12, 83]. Additionally this vision-based system can be used in GPS-deprived environments [20]. This method is limited by the speed of the used drones (becoming heavy when packed with sensors and deactivation methods to perform its task), the weather conditions (optical recognition and navigation does not work well in low visibility conditions such as fog, haze or the night) and the cost of designing and implementing a large system of drones like this.

A proposed radar based identification method is the use of micro-Doppler. The current research into the use of micro-Doppler in identification is vast and ever expanding [6, 50, 85, 86]. Zhang et al. [85] uses 2 radar sensors which are 1 meter apart and 1.2 meters away from the drone in a quiet environment. They are able to classify between different types of drones using the radar data and a state vector machine. Our use case requires longer distances containing more noise, making this method less viable. This method could however be used by having a network of stationary or drone-mounted radars capable of doing short range identification.

Finally Caris et al. [8, 9] performs identification of small drones using W-band radar. Their results look promising as they require very small amounts of power however their range is very small, current results are only accurate up to around 100 meters with a possibility of going up to 300 meters. In order for this research to be useful an increase in detection range will have to be achieved. W-band radar can be considered an expansion of a detection system, placing multiple radars to validate data gathered by longer range radar.

Conclusively, these identification based on raw signals look promising but all have their limitations. Which is why the choice has been made to zoom out and look at behavior-based identification. The only data needed is the x, y, z-coordinates over time and to perform identification. The subsequent section covers an exploration into the behavior based identification methods.

2.3.3. Behavior based identification

Because radar cross-section based methods do not look viable the remaining method is the use of behavior based classification. Simply put: using x, y, z -coordinates over time (flight paths) to classify behavior. Research into flight paths of drones is currently limited, which is why alternative fields are also considered.

Andersson and Luong [2] performs classifications of birds and UAV's using flights paths obtained by radar. They achieve 90% accuracy in classification of birds and drones using only coordinates over time. This result is achieved using filter based classification on a Recurrent Neural Network using Gated Recurrent Units. Their thesis is promising because they show that it is possible to perform classification on drones and birds using

detection history. Their method of classification can possibly be extrapolated to the identification step. However their use of a neural network is undesirable in the context of this thesis as explained in **section 1.2**.

The field of driver classification looks promising. With the huge influx of money and interest into autonomous vehicles also comes an increase in research done into classification. For example, Bouhoute et al. [5] looks at building graphical models to represent driver behavior. This is done using probabilistic hybrid automata and labeled directed graphs. This method is interesting because it uses transitions of states to define behavior. In the case of drones the states can be a simplistic way of representing threat. From the point of detection the different states keep track of behavior and when behavior changes significantly the drone can be classified as malicious. An alternative is lane changing prediction as performed in Kim et al. [29]. They use multi-class support vector machines to predict lane changing. This method sounds promising in detecting behavior changes.

Crowd classification is another alternative field which tries to analyze behavior, however the focus here is in large and dense data [33]. The data is subsequently used for crowd counting, violent behaviour detection and density level classification [41]. Violent behavior detection is done by looking at instant entropy and temporal occupancy variation in crowds to estimate changes in the "mood" of a crowd [48]. Whereas our aim is more akin to detecting the intentions of multiple actors in a crowd. Computer vision is effectively used in detection of animal behavior, recognizing behaviors which can be used as features. In the case of hens they detect moving or resting with close to 100% accuracy, however exploration only shows 54% accuracy [34]. Exploration detection is useful, however radar data is not fine-grained enough to extract the same features. Another paper looks at the behavior of sows, they define different postures: standing, sitting, lying left and lying right. And use a deep learning based feature extractor to extract these postures from images. Subsequently a convolutional neural network (CNN) is used to estimate the heat stress experienced by the sows [28]. The extraction of features using computer vision differs from my case as the features in radar data are easier to extract. The extraction of an entropy feature can be used to signal changes in behavior also present in radar data.

By basing identification on radar behavior, identification ranges can be increased from just no-fly or warning zones to the maximum range of a radar system. Providing an early warning system. A possible limitation lies in the high granularity of radar data, providing a small basis to base identification on. As well as the limitations discussed in **section 2.1**: susceptibility to noise and obstacles. Because no research has been performed on radar based behavior identification yet, it offers an important learning opportunity to the field of drone identification.

2.4. Knowledge Gap

In conclusion, adversarial behavior is the main challenge of the drone attack prevention process. With a risk of catastrophic consequences reliance on standards and compliance is insufficient. Requiring robustness against adversarial behavior in every step of the drone attack prevention process. Based on the current state-of-the-art radar based detection, localization, tracking and classification looks promising in terms of robustness. However, improvements and augmentation are still needed. Due to it's robustness against adversarial behavior, we decided to utilize radar for identification.

The problem of identification currently has little research and no solution. Limitations by range, noise or weather conditions make current solutions undesirable. A radar behavior based solution offers the opportunity to diminish range and noise, as well as solve weather problems. Next to that the lack of research in radar and behavior based identification provides a chance for exciting new research.

3

System Model

This chapter presents the preliminary knowledge needed to understand the current system in which identification takes place. **Section 3.1** elaborates on the set-up on the side of the military, the equipment used and the classification strategy used. **Section 3.2** discusses the anatomy of a drone and the components most commonly found in a drone. Finally **Section 3.3** covers the main types of actors and uses of drones and explains their aim, behavior and characteristics.

3.1. Field set up by the military

The set up used by the military consists of a sensor group which controls the radar equipment. Within the sensor group a small team controls the individual radar units and another team sits in a control room that receives the signals from the radars and displays it on a screen. The control room group also has access to a high resolution camera which includes a range finder. On localization of a drone the camera is used to better classify the target. The primary goal of the sensor group is to increase the time to react to threats. Faster detection, localization, tracking, classification and identification equates to increased time for deactivation. The operator in the control room receives information from the radar concerning a drone in the vicinity, the operator then uses the camera to perform a classification of the target, finally a decision for deactivation is made by the operator.

3.1.1. Radar

The objective of the radar within the system is detection, localization, tracking and initial classification of drones. Performed by sending and receiving electromagnetic waves. The radar is positioned close to the control room and is aimed at critical infrastructure. The radar classifies drones from other objects and connects coordinates of drones to create tracks that are unique to a drone. **Figure 3.1** shows a very simplistic overview of the basic components of a sensor group. The radar is deployed facing critical infrastructure and its radar beam covers a specific area. It is linked to a laptop that displays and records the objects captured by the data. **Figure 3.2** shows an actual picture of the radar position. The radar is indicated with a white 1 and the truck containing the laptop is indicated by a white 2.

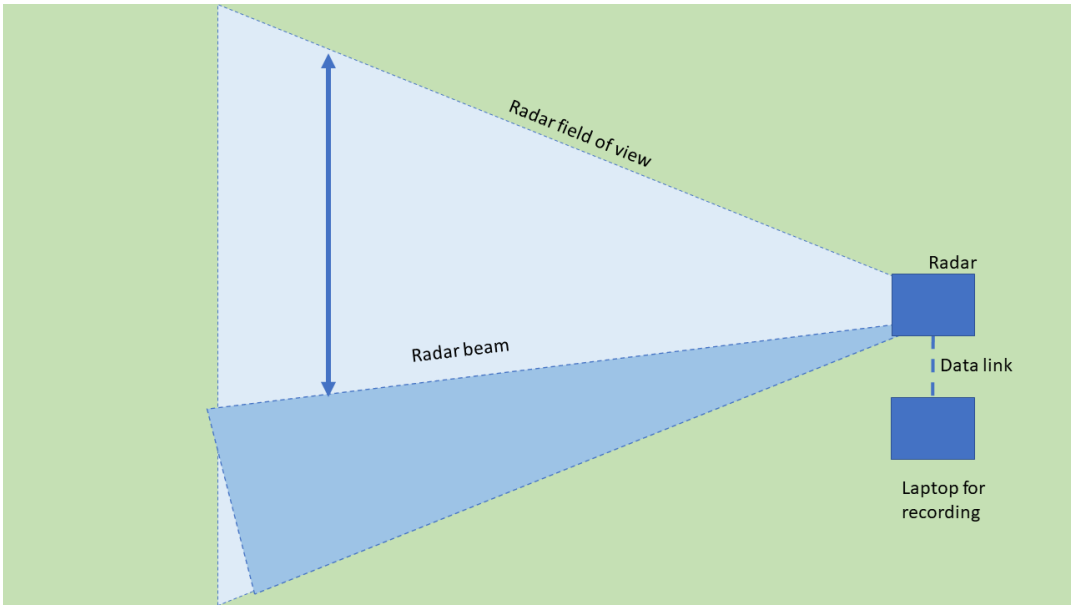


Figure 3.1: Experimental Setup

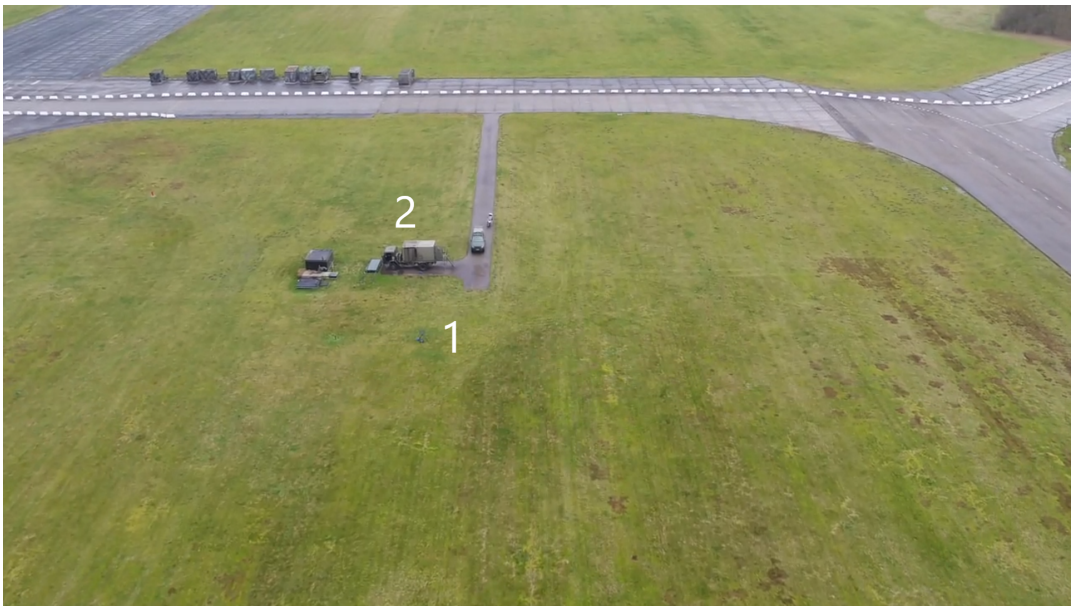


Figure 3.2: Aerial picture of the radar set-up

3.2. Drone

The central target in the system is the drone, a drone is an Unmanned Aerial Vehicle (UAV). It's most common commercial form is the quad-copter or fixed wing variant. The basic components of a drone are shown in **Figure 3.3**.

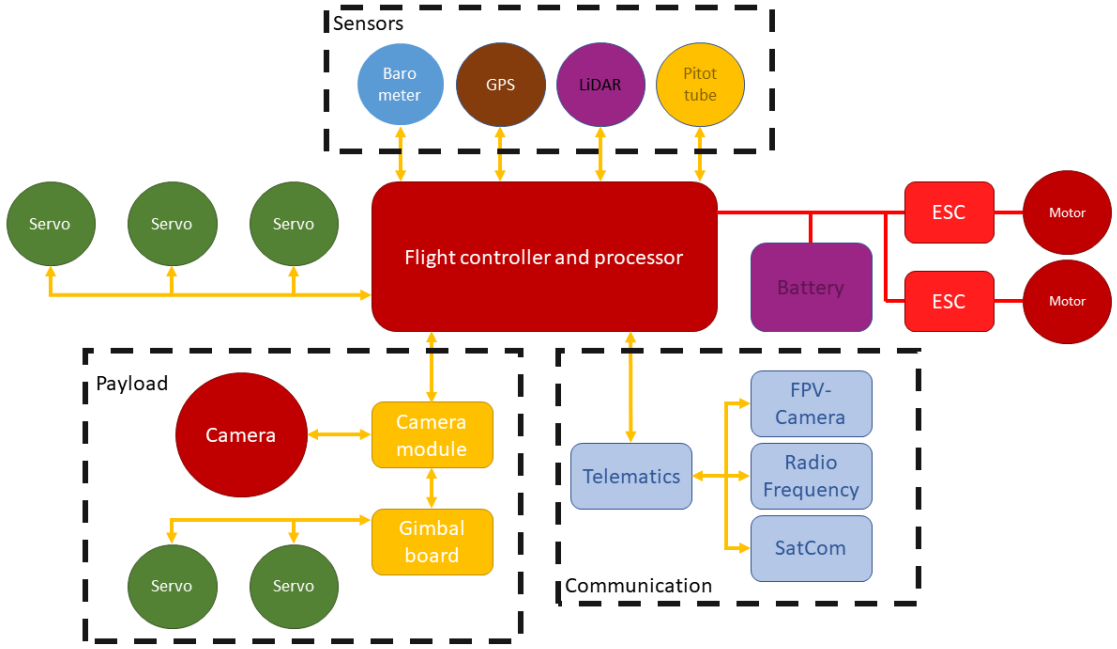


Figure 3.3: Composition/Technology – Typical drone (quad or fixed wing) [24]

The 'brain' of the drone is the flight controller and processor, they process signals and convert it into actions related to flying or executing one of its capabilities. The battery powers the drone and is connected to Electronic Speed Controllers (ESC), the ESC controls and adjusts the speed of the attached motors. Drones that receive instructions from an operator use telematics to receive said orders and relay information. Depending on the medium used the telematics uses a radio frequency or SatCom connection and possibly relays a live-feed captured by a First Person View (FPV) camera. The drone can be enhanced by adding different types of sensors, some examples are: Barometer for height data, GPS for receiving GPS positions, LiDAR to navigate or make images using radar or a pitot tube for measuring speed. Next to that drones often have a gimbal board to which a camera or servo's carrying other kinds of payloads can be attached. Finally drones can have extra servo's to operate wings in the case of fixed wing drones.

The drone represents the central actor of the system, it operates in 3-D centering on the critical infrastructure. It is often controlled by an operator in direct control of the drone and navigating by video feed. However other navigational methods do exist as discussed in **section 2.1**

3.3. Common drone actors and behaviors

Due to it's low operating cost and large range of capabilities drones are used in a wide variety of purposes, the most common uses of drones are currently:

1. Media drones.
2. Transportation, i.e. first-aid drones, drones used by postal/food services;
3. Communication, i.e. mobile hot spots;
4. Hobby drones;
5. Race drones;
6. Inspection drones.

For each type of drone a short description of its aim, behavior and operating characteristics is defined. These attributes are used to distinguish between different actors and in practise are used as a starting point in mapping out actors present in an environment. The aim of an actor describes what goal that actor is trying to achieve. The behavior provides a general description of the behaviors used to achieve the aim. The characteristics make the behaviors concrete the characteristics used are the following.

- Control: either manual control or automatic control, this influences the movement of the drone;
- Flight-path: either direct or indirect, if the drone flies in a very direct fashion towards an 'objective' or flies more indirect without a purpose;
- Distance to object: the distance with regards to a critical infrastructure as defined by the guarding actor;
- Speed: the speeds used by the drone to perform it's aim;
- Altitude: the heights most commonly used while executing the drone's aim.

3.3.1. Media

Aim: Taking pictures, making video's or using a live video feed to capture current events,
Behavior: The drone stays close to objects of interest for as long as possible, to gather more images. Once in place it will be still or moving slowly, often manually, to get good quality images. In order to swap batteries or drop off data the drone will have to return to a drop-off location. In order to record longer, the drone can be deployed nearby. The drone will not fly too high in order to maintain image quality.
Table 3.1 shows the main characteristics of this drone actor.

Characteristics of media drones	
Control	Manual
Flight-path	Indirect
Distance to object	1000-2000 meters
Speed	5-60 kmh
Altitude	200-100 meters

Table 3.1: Characteristics of media drones

3.3.2. Transportation

Aim: Transportation of goods between two or more locations.
Behavior: The drone spends a short time at the drop-off location. It flies in straight lines straight towards drop-off locations. It might be used to make multiple flights to and from a location. The drone can come from a large distance and has a low speed to provide longer range and a bigger payload.
Table 4.2 shows the main characteristics of this drone actor.

Characteristics of transportation drones	
Control	Manual/automatic
Flight-path	Direct
Distance to object	2000-3000 meters
Speed	40km/h
Altitude	50-100 meters

Table 3.2: Characteristics of transportation drones

3.3.3. Communication

Aim: Provide connection services in crowded area's. Often done to "relieve" the more permanent network infrastructure.
Behavior: The drone will stay on location for a longer time, possibly landing while the access point is active. It might return to recharge the drone and hub. To save energy the drone can take off from a nearby location. A high altitude could be used to increase connection distance.
Table 3.3 shows the main characteristics of this drone actor.

Characteristics of communication drones	
Control	Manual/automatic
Flight-path	Direct
Distance to object	0-2000 meters
Speed	40km/h
Altitude	50-100 meters

Table 3.3: Characteristics of communication drones

3.3.4. Hobby

Aim: Practise of drone flying.
Behavior: The drone performs erratic behavior centered on a location often within view of it's operator. It shows large changes in speed and altitude.
Table 3.4 shows the main characteristics of this drone actor.

Characteristics of hobby drones	
Control	Manual
Flight-path	Indirect
Distance to object	2000-3000 meters
Speed	20-80 km/h
Altitude	50-100 meters

Table 3.4: Characteristics of hobby drones

3.3.5. Race

Aim: Training for drone racing.
Behavior: The drone moves at fast speeds and performs short turns. It can move further away from it's operator and moves in an indirect manner.
Table 3.5 shows the main characteristics of this drone actor.

Characteristics of race drones	
Control	Manual
Flight-path	Direct
Distance to object	2000-3000 meters
Speed	80km/h
Altitude	50-100 meters

Table 3.5: Characteristics of race drones

3.3.6. Inspection

Aim: Creating images or LiDAR scans of an object in order to determine its status.
Behavior: The drone flies towards an object, then makes a calibration flight to set up it's sensors. Then it flies in a pattern around the object while performing a scan. It repeats the calibration and scan phases multiple times at different angles to create a complete image.
Table 3.6 shows the main characteristics of this drone actor.

Characteristics of inspection drones	
Control	Manual
Flight-path	Direct
Distance to object	2000-3000 meters
Speed	5-10km/h
Altitude	50-100 meters

Table 3.6: Characteristics of inspection drones

4

Threat Model

This chapter describes the threats to the system model. A short overview of all possible threat actors their aims, behavior and characteristics is given in **Section 4.1**.

4.1. Standard Threat Scenario's

The military uses 6 main Standard Threat Scenarios. These scenarios outline behaviors of actors. When approached to secure an environment the possible threats are divided in these categories. They function as a starting point in defining a new environment, providing a general description of behavior. The definitions are by not exhaustive and actors can deviate from the defined behavior. The Threat Scenario's used are:

1. Intelligence, Surveillance and Reconnaissance (ISR);
2. Transportation;
3. Man-in-the-middle (MITM);
4. Air Disruption;
5. Harassment;
6. Attack.

The first two scenario's are similar to scenario's in the **System Model**, however as a threat they have different characteristics. Each scenario is discussed shortly, it's aim, the associated behavior and characteristics are discussed.

4.1.1. Intelligence, Surveillance and Reconnaissance (ISR)

Aim: Gathering of information by taking pictures, making video's or using a live video feed. The information can be used to plan successive action or sold to media outlets.
Behavior: The drone stays close to the critical infrastructure for as long as possible, to gather more data. Once in place it will be still or moving slowly, often manually, to get good quality images. In order to swap batteries or drop off data the drone will have to return to a drop-off location. In order to record the critical infrastructure longer the drone can be deployed nearby. The drone will not fly too high in order to maintain image quality.
Table 4.1 shows the main characteristics of this drone actor.

Characteristics of ISR drones	
Control	Manual
Flight-path	Indirect
Distance to object	1000-2000 meters
Speed	40-60 kmh
Altitude	200-100 meters

Table 4.1: Characteristics of ISR drones

4.1.2. Transportation

Aim: Transportation of (illegal) goods between two or more locations.
Behavior: The drone spends a short time at the drop-off location. It might be used to make multiple flights to and from a location. The drone can come from a large distance and has a low speed to provide longer range and a bigger payload.
Table 4.2 shows the main characteristics of this drone actor.

Characteristics of transportation drones	
Control	Manual/automatic
Flight-path	Direct
Distance to object	2000-3000 meters
Speed	40km/h
Altitude	50-100 meters

Table 4.2: Characteristics of transportation drones

4.1.3. Man-in-the-middle

Aim: Transportation of a WiFi-hub to provide a rogue access point at a remote location. The access point can be used to sniff traffic, relay a signal or hack into a device.
Behavior: The drone will stay on location for a longer time, possibly landing while the access point is active. It might return to recharge the drone and hub. To save energy the drone can take off from a nearby location. A high altitude could be used to avoid detection.
Table 4.3 shows the main characteristics of this drone actor.

Characteristics of MITM drones	
Control	Manual/automatic
Flight-path	Direct
Distance to object	1000-2000 meters
Speed	40km/h
Altitude	50-100 meters

Table 4.3: Characteristics of MITM drones

4.1.4. Air Disruption

Aim: Disrupt take-off and landing routes of air traffic without causing physical damage.
Behavior: The drone needs a short time on location to cause disruption. It might make return flights to be used more frequently. High altitude and high speeds are used for avoidance against countermeasures.
Table 4.4 shows the main characteristics of this drone actor.

Characteristics of air disruption drones	
Control	Manual
Flight-path	Indirect
Distance to object	2000-3000 meters
Speed	60-80km/h
Altitude	200+ meters

Table 4.4: Characteristics of air disruption drones

4.1.5. Harassment

Aim: Causing panic or disruption without physical damage, at airports, urban areas, mass crowds or specific people.
Behavior: Drone follows a specific target. Flies at a low altitude and speed varies depending on the target.
Table 4.5 shows the main characteristics of this drone actor.

Characteristics of harassment drones	
Control	Manual
Flight-path	Indirect
Distance to object	2000-3000 meters
Speed	40-60 km/h
Altitude	10-100 meters

Table 4.5: Characteristics of harassment drones

4.1.6. Attack

Aim: Modifying a drone so that it can be used as a weapon. The drone can then be used as a means or platform for direct attacks. Targeting resources, personnel or infrastructure.
Behavior: Drone only needs to be on target for a short time. Drone makes a single flight to a target. Without a return flight or long time on target the drone can take off at a larger distance. High speeds are used to approach a target faster. Low altitude is used to increase accuracy.
Table 4.6 shows the main characteristics of this drone actor.

Characteristics of attack drones	
Control	Manual or autonomously
Flight-path	Direct
Distance to object	2000-3000 meters
Speed	80+ km/h
Altitude	10-100 meters

Table 4.6: Characteristics of attack drones

5

Solution

In **Section 5.1** the target behavior of this thesis is discussed. Then in **Section 5.2** the features that are used by the model to classify the target behavior are explored. Finally in **Section 5.3** the approach used to classify the target behavior using the designed features is discussed.

5.1. Target Behavior

The system and threat models describe possible behaviors that are encountered in the field. From the profiles available, the identification of ISR drones is picked as the main behavior for answering the research question of this thesis. The identification of ISR drones requires the recognizing of: "Gathering of information by taking pictures, making video's or using a live video feed. The information can be used to plan successive action or sold to media outlets". The key behavior to identify is the ability to make accurate videos or provide a live video feed. This behavior is chosen for its ambiguity and loose definition, providing a challenging behavior for classification.

The most common environment encountered is a deployment of the sensor group in a compound which has a nearby village. Based on that environment the most common actors are non-professional or hobby drones. Data for identification is generated by simulating this environment in experiments. The experiments simulate ISR behavior, the pilot approaches an object defined as critical infrastructure and attempts to get a clear view. During the flight the radar system captures the movement of the drone and sends it to a laptop that records the capture data.

Non ISR-behavior is generated in two ways. Firstly the ISR tracks that are flown with respect to a specific critical infrastructure location, are rotated. This affects the distance and angle based features but does not change the other features. Making it more difficult for a model to distinguish rotated from actual ISR behavior. Secondly, recordings of drones performing normal test flights for the radar are added to the dataset to provide normal behavior independent of critical infrastructure.

5.2. Feature design

To start identify ISR behavior, a set of features is defined. This set is used in the next step to define the boundaries of ISR behavior. As described in the **System Model**, the raw data contains x,y,z-coordinates over time. We define artificial features to increase the basis of information for identification. The goal of the feature design phase is to increase the information extracted from the raw radar data. The full list of features with elaborate explanations is shown in Appendix A. A short breakdown of the used features is provided below.

5.2.1. General features

These features are based on the characteristics of actors defined in **System Model** and **Threat Model**. The characteristics are: *Control (Manual/Automatic), Flight-path: (Direct/Indirect), distance to object, Speed and Altitude*. Detecting control and flight paths is difficult due to the large-grained nature of the data. It is defined by using three features: *Degrees of operation, speed variance and altitude variance*. The features describe erratic behavior, hinting at automated behavior as well as how focused the behavior of a drone is. The other three features are directly implemented from the **System Model**.

5.2.2. ISR specific features

These features are designed specifically for ISR-behavior, with a focus on camera accuracy. The first feature is *degrees of operation* and captures the totality of the view created by a drone. *Time within accurate zone* is based on the effective range of the camera on a drone and captures the time spent in that zone.

Non-moving time and *covering of precious trajectories* aim at detecting superresolution imaging. The supperresolution method takes advantage of statistics in combining information from different images. By aligning pictures of a setting taken from slightly different angles the information gathered is combined into a higher resolution image [16, 46]. This method requires shots of a critical infrastructure taken from the same position, which can be detected by tracking *non-moving time*. New methods are being developed to create superresolution for video-feeds, in the future this becomes a bigger problem [36]. The *covering of precious trajectories* captures video feed superresolution. Next to that it is used to detect scouting over time to map troop movements.

5.2.3. Extra features

To augment the feature space further, we add four additional features. First of all *movement towards critical infrastructure*, this captures the focus of a drone on the critical infrastructure. *Point of detection/loss* detects take-off and landing locations which creates an understanding of the environment and locations of actors. *Area of operation* is a meta-feature that distinguishes less hostile actors, hobbyists operate in much smaller area's than bigger actors. Finally, *weather conditions* adds crucial information about the environment. Sunny conditions indicate higher accuracy of camera's at bigger distances. A full breakdown of each feature and its calculation is given in **Appendix A**.

5.3. Approach

We want to answer the following research question: "How accurately can we Identify Intelligence, Surveillance, Reconnaissance (ISR) from non ISR behavior in drones using data collected by radar?". Will be answered in two steps. First of all a theoretical model explaining ISR behavior is built. We build this model to provide insight into the most important features. The model itself provides a novel way of discussing ISR behavior and a starting point for discussing drone behavior in general. In step two we compare strengths of multiple algorithms for predicting ISR behavior.

Before the theoretical model or the prediction algorithms are tested, data is generated. This is done by flying ISR missions using a drone and capturing the movements using radar. During the capturing a laptop is connected to the radar and parses the data stream containing the radar information packets[1]. Next to the flown missions, some non-ISR captures from training sessions are captured and added to the data set. The data set is then processed: removing perfect predictors, removing redundant features, performing normalization. Finally a theoretical model is built and the prediction algorithms are tested.

5.3.1. Theoretical model

In order to identify ISR behavior we perform an exploration of the feature space. To understand the importance of individual features in explaining behavior feature importance is calculated. The feature importance of a variable is a measure that describes how powerful that variable is in predicting a target variable [55]. Feature importance for each individual feature is calculated, using univariate as well as multivariate measures. Information on feature importance forms the basis of a theoretical model for drone behavior. The information on feature importance is used in exploring different machine learning algorithms for identification.

5.3.2. Prediction algorithms

Data is put into different algorithms to show underlying patterns. The algorithms produce separations within the features based on ISR-behavior. Finally the separation of data found by the algorithm is examined to gain further insight into ISR-behavior.

We use two types of algorithms: white box and black box algorithms. White box algorithms have simple inner-workings and because of that can be understood and explained (e.g. decision tree, linear regression). Black box algorithms are more complex and often have a higher accuracy but are difficult to understand and explain (e.g. neural networks). White box algorithms are very useful as they provide a good insight into the data and form a basis on which to talk to experts about results. Black box algorithms are useful because if they provide a good separation of data that separation can be used in the final model, however the separation is often too complex to be reasoned about with experts.

[1] EXPLAIN PACKETS?

6

Evaluation

This chapter describes how the solution are evaluated. The first section, **Section 6.1**, explains the experimental setup used to test the solution. Consequently the experiments that are executed are discussed in **Section 6.2**. The third section, **Section 6.3**, summarizes the most important results found in the experiments. **Section 6.4**, provides a brief overview of the evaluated algorithms. The numerical results found by the algorithms are given and discussed in **Section 6.5**. Lastly, **Section 6.6** explores the robustness of the algorithms to changes in features and data.

6.1. Experimental setup

The actual equipment used to create the system model is explained in this section.

6.1.1. SQUIRE Radar system

The radar used in this thesis is the Signal Quiet Universal Intruder Recognition Equipment (SQUIRE) radar system as produced by Thales. The SQUIRE is a portable radar system which can be carried by 2 operators (in backpacks weighing 23kgs). It uses Frequency Modulated Continuous Wave (FMCW) technology and is the preferred radar for quick and temporary deployments [67, 81]. The SQUIRE performs filtering such as on Clutter, i.e. non moving objects and birds which are filtered using micro-Doppler data. The effective classification range of UAV's is up to 6km depending on weather conditions [51]. The SQUIRE is attached to a laptop running a Graphical User Interface (GUI)[1] that shows the received data . An operator uses this GUI to coordinate troop movements as well as communicate with the radar.

The operational azimuth[2] of the SQUIRE is 360 degrees, however it is most often operated in 1200mils, which allows a group of 3 SQUIRE's to cover a half circle . The opening angle of the radar is 8 degrees or 142 mills. Which is why the SQUIRE is limited in the height of its detection area at shorter ranges (at 250 meters the scanning height is 35 meters, at 3000 meters the scanning height is 420 meters).

The SQUIRE produces a binary stream of data in a custom protocol designed by Thales, a parser is built to convert this data stream into (Python) objects usable for further analysis. The SQUIRE converts the data points into x, y, z coordinates relative to it's position. Next to that the SQUIRE connects related data points to create tracks as well as perform a classification of the objects. Discerning between drones and other objects.

Connected to the SQUIRE is a laptop that receives the radar data and displays it on a map. That laptop has a listening function duplicating the received data stream for connected systems. We connect to the listening port and receive the same stream of data as the Operators' laptop. Combining the coordinates per track with information on the location of critical infrastructure, the data is enriched with extra features. A detailed explanation per feature is provided in **Appendix A**. In order to simulate lack of information the received

[1] The graphical user interface is a form of user interface that allows users to interact with electronic devices through graphical icons and audio indicator such as primary notation, instead of text-based UIs, typed command labels or text navigation [78].

[2] The azimuth is an angular measurement in a spherical coordinate system [74]

data tracks (consisting of up to 80 data points) are subdivided into tracks of 10 data points each. During the evaluation the increase of data points per track is explored, increasing to 20 and 30 data points.

6.1.2. DJI Inspire 2

Due to the large variety in drone models and different qualities in camera, the choice is made for a single drone and camera model. By showing the correct identification of behavior for a single make and model the results can be extrapolated to a wider range of drones, camera and even behaviors in further research.

The chosen drone is the DJI Inspire 2, frequently used by armies and private actors across the world to perform operations. The top speed is $94\frac{k}{h}$, it ascends at $9\frac{m}{s}$ and descends at $6\frac{m}{s}$. It can operate to a height of 2500-5000m above sea level depending on the propellers and up to (-20°C). It can fly up to 27 minutes or up to 7km before needing a recharge. It is connected to an operator using a radio frequency between 2.4 and 5.8 GHz. It has a camera capable of recording video in 6K at $4.44\frac{Gb}{s}$. The live video feed provides 1080p as well as 720p. It has the possibility to approach and track a designated object. The camera is attached to a gimbal allowing the operator to perform movement while the camera stays centered [19].

6.2. Experiments run

Generating ISR behavior requires actual flight recordings using radar. To reproduce ISR behavior for the radar, different flight patterns are flown and recorded. Using a variety of altitudes and perspectives. The flights create video images of the critical infrastructure, but also show behavior of an ISR pilot before the critical infrastructure is within clear sight. **Figure 6.1** shows the position used as critical infrastructure, the drone approaches the critical infrastructure from a distance and creates a video feed.

Figure 6.1: Aerial picture of the critical infrastructure scouted.

1. Flying around the critical infrastructure at 700 meter distances, while circling around the infrastructure to get a clear view. Altitude used is 50 meters.
2. Flying around the critical infrastructure at 300 and 500 meter distances, while circling around the infrastructure to get a clear view. Altitudes used are 70 and 50 meters.
3. Approaching the critical infrastructure in a straight line at an altitude of 50 meters. Then flying back in a straight line.
4. Approaching the critical infrastructure in a straight line at an altitude of 10 meters. Then flying back in a straight line.
5. Approaching the critical infrastructure in a straight line, then performing manoeuvres to distort the video feed.

6.3. Feature Exploration

The dataset generated by flying experiments, extracting features and adding additional features is explored in this section. The feature set contains both dependent and independent variables[3]. The independent variables are continuous and the dependent variable is categorical. For data exploration a track length of 10 data points is used. The dataset contains 2529 data points on non-ISR behavior and 1588 data points on ISR behavior.

First of all Pearson's correlation is used to find statistical relationships between the independent variables [75]. To strengthen the feature set all columns which show a correlation above 0.8 are removed. Comparing time, max time and percentage spent in rings a direct correlation is seen between time and max time in **Figure 6.2**. Justifying the removal of max time [4].

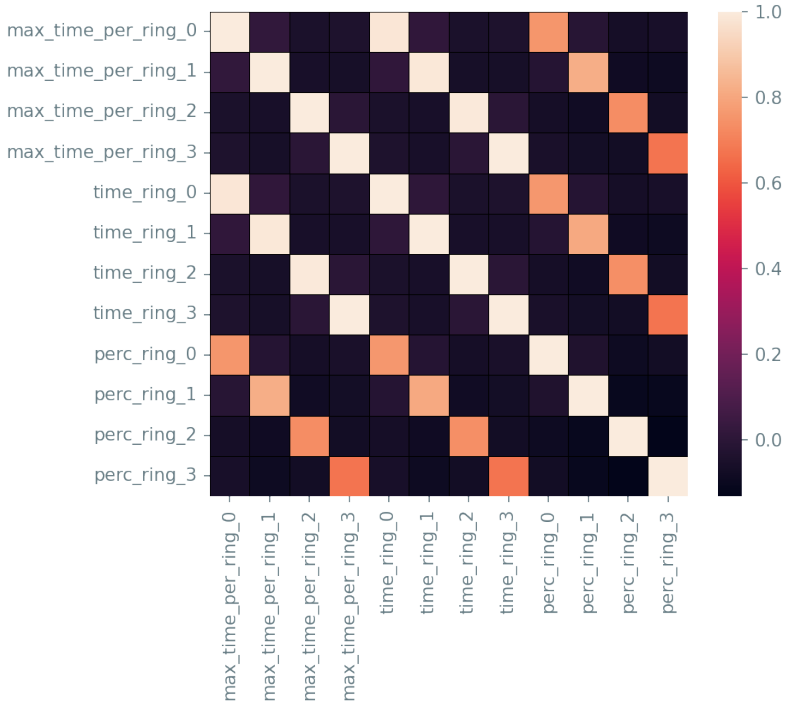


Figure 6.2: Heat map containing correlations for different ring based features

6.3.1. Feature Importance

Following the removal of these columns a range of measures is used to explore the feature importance. Both univariate and multivariate feature importance are explored, a complete list of the used measures their definitions and results is given in **Appendix B.2**. The main indicators are discussed in this section.

The first measure is the Maximal Information Coefficient (MIC), which measures uncertainty reduction about a random variable by knowledge of another variable [30]. The second measure is the absolute importance, representing how far a specific feature influences the final prediction of the test set [27].

The 10 best scoring features are shown in **Figure 6.3**. Distance to critical infrastructure scores best on both measures, followed by the z-value or altitude and the average height.

[3] "Dependent and Independent variables are variables in mathematical modeling, statistical modeling and experimental sciences. Dependent variables receive this name because, in an experiment, their values are studied under the supposition or demand that they depend, by some law or rule (e.g., by a mathematical function), on the values of other variables. Independent variables, in turn, are not seen as depending on any other variable in the scope of the experiment in question."[76]

[4] The same relation can be seen in sectors **Appendix B.1**

	MIC	Absolute importance	Total Normalized [%]
dist_to_crit_infra	1.00	1.00	26.34
z	0.24	0.15	5.19
height_average	0.22	0.15	4.89
max_time_any_zone	0.24	0.02	3.38
time_sector_4	0.18	0.01	2.48
time_sector_7	0.08	0.11	2.45
max_time_per_ring_1	0.19	0.00	2.44
perc_ring_1	0.19	0.00	2.44
time_ring_1	0.19	0.00	2.44
speed_average	0.05	0.14	2.44

Figure 6.3: Strongest predictors

In order to see the decrease in feature importance on removal of distance to critical infrastructure the tests were executed without this feature. Resulting in **Figure 6.4**. The removal clearly shows the impact of distance to critical infrastructure, where z and max time in any zones are only 0.24 for the univariate measure with it. Removing the distance to critical infrastructure makes both max time and z the new 1 and scales the rest accordingly. This makes degrees of operation very important where it was not as important before. However the normalized % of importance is 7.13 compared to the 26.34 of the distance to critical infrastructure. Removing distance to critical infrastructure evens out the other feature and shows a more uniform distribution of features.

	MIC	Absolute importance	Total Normalized [%]
degrees_of_operation	0.68	1.00	7.13
height_average	0.92	0.39	5.59
z	1.00	0.19	5.08
max_time_any_zone	0.99	0.00	4.23
perc_same_traj	0.76	0.15	3.85
max_time_per_ring_1	0.77	0.00	3.28
perc_ring_1	0.77	0.00	3.28
time_ring_1	0.77	0.00	3.28
max_time_per_sector_4	0.73	0.00	3.12
time_sector_4	0.73	0.00	3.10

Figure 6.4: Strongest predictors without distance

Taking a closer look at distance to critical infrastructure, multiple boxplots are created. One with ISR tracks, one with rotated scouting tracks and one with non ISR tracks. As **figure 6.5** clearly shows, the distances for the ISR tracks are a lot nearer to the critical infrastructure than the distances for non ISR and rotated tracks. Showing clearly that the distance to the critical infrastructure is a very good predictor.

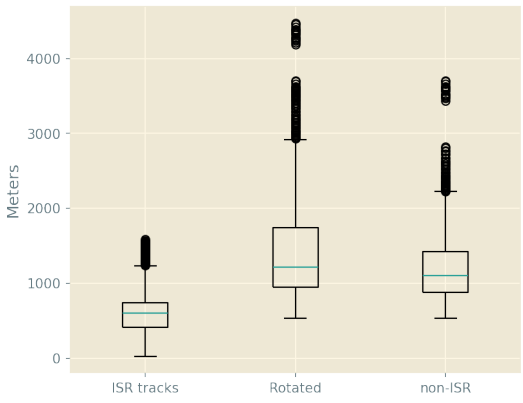


Figure 6.5: Boxplot of distance to critical infrastructure

6.3.2. Theoretical model

From the data exploration we can build a theoretical model of drone behavior. The model used in the **System Model** and **Threat Model** uses control, flight-path, distance to critical infrastructure, speed and altitude. For ISR behavior these characteristics can be improved. Due to the lack of fine-grained data it is difficult to distinguish control and flight-path characteristics, standard deviation metrics might indicate control and flight path but have low feature importance. Distance to critical infrastructure and altitude are good indicators as proven by their feature importance. Speed is not a good predictor of ISR behavior as it has a low importance. Features that explain movement are better predictors. First of all max time in any zone, an indicator for how much an actor moves scores high on univariate measures but on multivariate measures it scores very poor. Indicating that it might not be an ideal predictor. Subsequently, degrees of operation, an indicator for the aspects of an object that have been seen is an important predictor. Percentage covering of the same trajectory is an indicator for repetitive patterns, corresponding to winning information on a target. This feature scores high on univariate and multivariate measures.

Using this information we can conclude that the following features should be used in discussing ISR behavior:

- Distance to critical infrastructure;
- Degrees of operation around critical infrastructure;
- Z-coordinate or altitude;
- Percentage covering of the same trajectory.

Finally the addition of rings sectors and zones is too specific for a general theoretical model but they are not insignificant and can be used when discussing specific scenarios.

6.4. Description of Algorithms

This section gives a short overview of the classification algorithms that were considered, how they work and how they can be tweaked.

6.4.1. Decision tree

The first white box classification algorithm is the decision tree. The algorithm explores data and attempts to find single independent variables that explain the dependent variable. Per independent variable it find the maximum separation for the dependent variable and creates a decision node on that separation boundary (split). Continuing till a maximum separation of data is achieved. The tree consists of internal nodes or branches with splits and external nodes or leaf nodes which have no children. **Figure 6.6** shows a small decision tree, we can see the decision points in the graphs. it also shows a single data point and what path is taken to reach its classification.

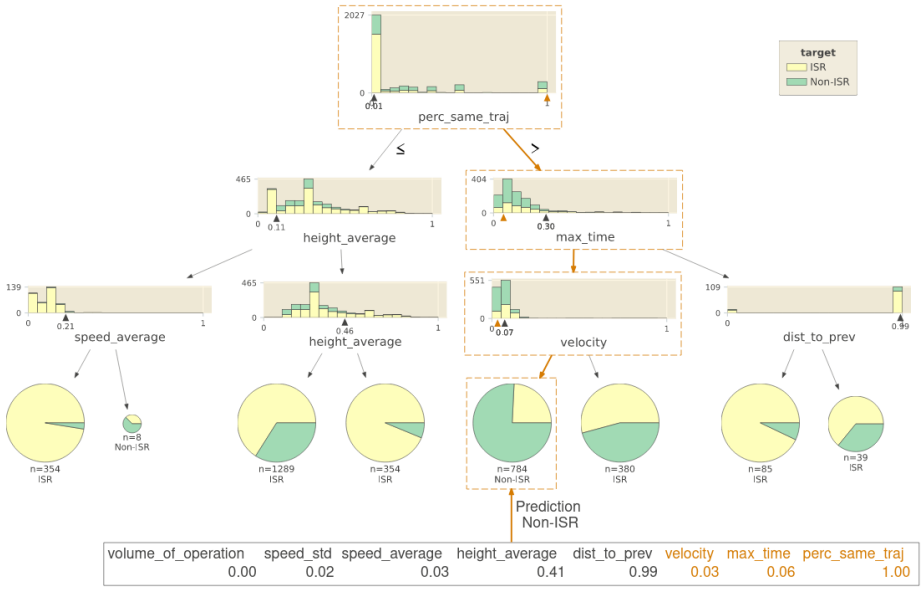


Figure 6.6: Decision tree with pathing

We explore the parameters listed below[5]:

- Minimum samples in leaf: *"The minimum number of samples required to be at a leaf node. A split point at any depth will only be considered if it leaves at least min_samples_leaf training samples in each of the left and right branches."*
- Minimum samples in split: *"is a fraction and ceil(min_samples_split * n_samples) are the minimum number of samples for each split."* The min samples split refers to inner nodes in the tree and the minimal amount of dependent variable classes required per branch. The ideal value is often found between 1 and 40 [40].
- Max depth: *"The maximum depth of the tree. If None, then nodes are expanded until all leaves are pure or until all leaves contain less than min_samples_split samples."*. A higher depth results in a better fit on the training data and a higher possibility of overfitting.

6.4.2. Random forest

The black box classifier is a random forest algorithm. The random forest uses multiple decision tree classifiers, which are fitted to subsets of the dataset. It averages the results of the individual decision tree's to create an extensive decision structure. It expands the decision tree algorithm with one paramater. The number of trees used in the forest. Next to that it uses all the decision tree parameters as seen in **section 6.4.1**.

[5]explanations are taken from sklearn [62]

6.4.3. Support Vector Machine

The other white box classifier is the Support Vector Machine (SVM). An “SVM maps training examples to points in space so as to maximise the width of the gap between the two categories. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall” [79]. The two parameters used to tune the SVM are discussed below.

- C value: regularization parameter, the higher the value the smaller the margin used by the SVM.
- Gamma: the amount of support vectors used, a high gamma has a "linear decision boundary", a lower gamma provides a "non-linear decision boundary".

6.5. Numerical results

The algorithms used are compared on their performance for track lengths of 10, 20 and 30 data points. The length of the track corresponds to the amount of previous data points used in determining features. An example of the calculation of x-coordinate for generic track lengths is given in **equation 6.1**. Where x_n represents the n^{th} data point and x_{total} represents the summation of the past n datapoints.

$$\mathrm{x}_{total} = \sum_{n=0}^{n_{tracklength}} x_n \tag{6.1}$$

Per track length, accuracy, precision and recall is calculated. All of them are aggregated into a generalized score for performance [68]. For identification of ISR behavior, every positive requires an action, so if a track is classified positively it should be correctly classified. Making recall the most important metric. Missing of ISR behavior limits the preparation time for possible attacks, if a track is positive it should be correctly identified making precision important. Accuracy provides an overall indication of performance, high accuracy is desirable. Prior to comparing classifiers, the individual classifiers are calibrated for optimal results. Using 5 fold cross validation, optimal parameters are found for each algorithm. This is done by calculating accuracy over 5 folds.

Finally a statistical test is used to compare differences in results between different algorithms. a “5x2 Cross-Validation Test” is used to compare statistical significance between algorithms [17]. The assumption for the “5x2 Cross-Validation Test” is that the results follow a Gaussian distribution [6], to check this a Shapiro-Wilk test is performed on the results. If the results follow a Gaussian, we can use the “5x2 Cross-Validation Test”. The “5x2 Cross-Validation Test” is picked over the commonly used Student’s T-test as the key assumption of the Student t-test does not hold, independence of observations. Independence of observation equates to the train set and test set being independent sets, sampling the train and test set from the same data set removes independence. This results in an incorrect interpretation of the t-statistic and p value for the Student’s T-test [17]. If the results do not follow a Gaussian distribution, a less powerful[7] non-parametric test is used to compare difference: the Wilcoxon signed rank test. The result of a test is a calculated t-statistic representing how the test scored, followed by a p-value indicating the likeliness of a result if the null-hypothesis is true. If the results of two classifiers are significantly different the p-value is higher than 0.05. A value lower than 0.05 indicates no significant difference between classifiers.

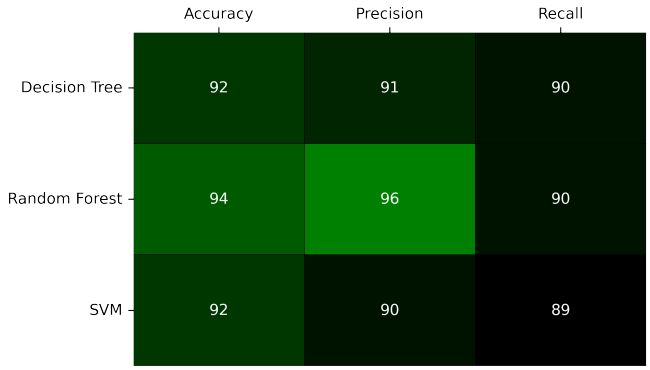
[6] A Gaussian distribution is a type of continuous probability distribution for a real-valued random variable. A Gaussian distribution is said to be normally distributed, and is called a normal deviate. [77]

[7] Power is the probability of wrongly concluding that two classifiers are or are not distinct. Hence a higher power reduces this probability and is preferred.

6.5.1. Track length 10

Figure 6.7 shows a summary of the most important metrics. In **a**, the accuracy, precision and recall for each classifier is shown in a heatmap, the green color indicating performance on the metric. Next to that in **b** the statistical comparison on the results for the classifiers is shown. The first column explains which classifiers are compared, the second column show the statistical test used, the third column covers the t-statistic and the final column is the p-value.

Classification of tracks at length 10 is very good, the "worst" classifier is the decision tree, which still achieves 92% accuracy. The random forest performs is the most accurate classifier. The results of all classifiers are statistically distinct: the decision tree and the random forest results do not follow a Gaussian and Wilcoxon signed rank test provides a p-value of 0.125, which is larger than 0.05 resulting in a rejection of the null hypothesis (the results of both classifiers are equal). The results of the decision tree and SVM follow a Gaussian and the 5x2 Cross-Validation Test provides a p-value of 0.8, resulting in rejection of the null hypothesis. Finally the random forest and SVM show a p-value of 1.8. Due to the p-values, all classifiers are distinct.



(a) Results

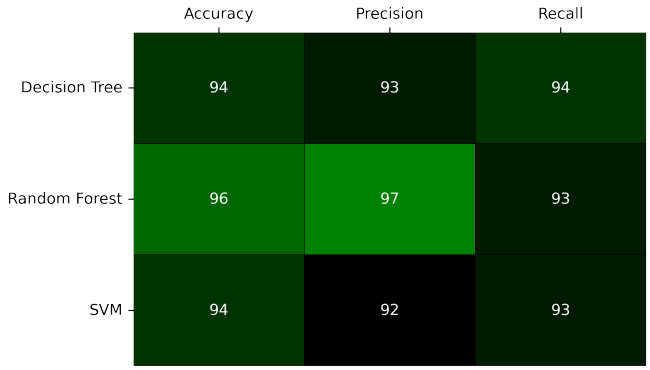
Classifiers compared	Test	T-statistic	p-value
Decision tree x Random forest	Wilcoxon	1.000000	0.125000
Decision tree x SVM	5x2 Cross-Validation Test	0.263654	0.802568
Random forest x SVM	5x2 Cross-Validation Test	-1.476489	1.800155

(b) Statistical comparison

Figure 6.7: Track length 10 results

6.5.2. Track length 20

Figure 6.8 shows the results for a track length of 20. As expected, classification using more information becomes better, resulting in higher accuracy, precision and recall scores for all classification algorithms. The increase is around 2% for each metric. The decision tree is now closer in results to the other classifiers, the SVM is the worst classifier for a track length of 20. The p-values are above 0.05, resulting in distinct results.



(a) Results

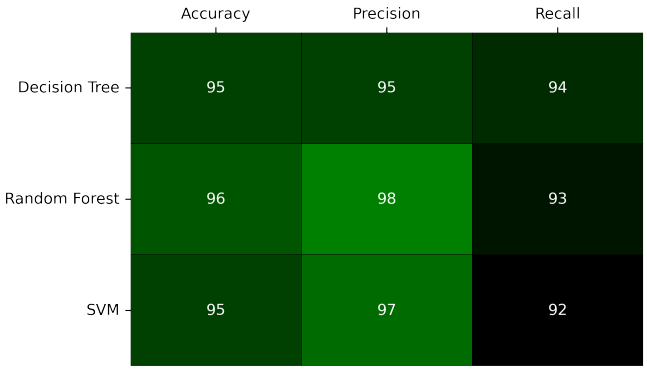
Classifiers compared	Test	T-statistic	p-value
Decision tree x Random forest	5x2 Cross-Validation Test	-1.139257	1.693784
Decision tree x SVM	5x2 Cross-Validation Test	0.132649	0.899644
Random forest x SVM	5x2 Cross-Validation Test	-1.774818	1.863900

(b) Statistical comparison

Figure 6.8: Track length 20 results

6.5.3. Track length 30

Figure 6.9 shows the results for a track length of 20. At a track length of 30 precision is the most improved metric. The decision tree becomes slightly worse than the others. The results are still statistically significant.



(a) Results

Classifiers compared	Test	T-statistic	p-value
Decision tree x Random forest	5x2 Cross-Validation Test	-1.353523	1.766142
Decision tree x SVM	5x2 Cross-Validation Test	-0.993063	1.633724
Random forest x SVM	5x2 Cross-Validation Test	-1.313686	1.754003

(b) Statistical comparison

Figure 6.9: Track length 30 results

At a track length of 30 precision is the most improved metric. The decision tree becomes slightly worse than the others. The results are still statistically significant.

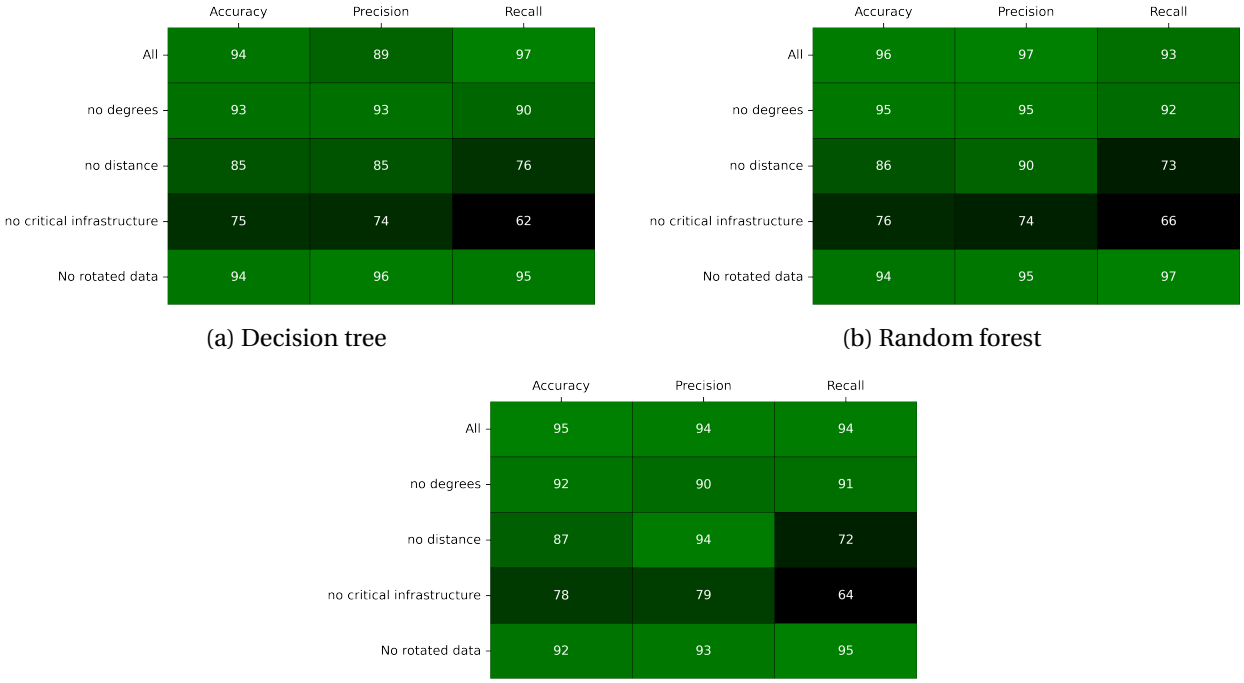
6.6. Challenging the models

Next to regular comparisons, a change in features is used to compare classification algorithms. The goal is to explore changes in performance when information is missing. Track lengths of 10 are used, as they show the worst results for all classifiers, amplifying distinctions. 5 different experiments are run:

- All, this experiment contains all the features as used previously.
- No degrees, this experiment removes all angle-based features.
- No distance, this experiment removes all distance based features.
- No critical infrastructure, this experiment removes all critical infrastructure related features[8].
- No rotated data, due to rotated data being identical to ISR tracks we explore the results without rotated tracks, using all features.

The results are shown for all metrics, for each experiment and per classifier in **Figure 6.10**. The conclusions in **feature exploration** are confirmed by all classifiers. The distance to critical infrastructure is the best predictor, removing that removes a significant amount of accuracy. Removing all critical infrastructure related features makes rotated and normal ISR-features inseparable and impossible to distinguish. Which explains the difference between the no critical infrastructure experiments and the no rotated data experiments. Another interesting trend is that recall suffers relatively more from a decrease in features. In other words: non-ISR behavior is more often miss-classified as ISR behavior with a lack of features.

The random forest scores highest with removal of features, with the decision tree and SVM being close but significantly worse. It is interesting to see that the recall for the SVM becomes very bad if more features are removed.



(a) Decision tree

(b) Random forest

(c) SVM

Figure 6.10: Robustness in features per classifier

[8]This makes rotated data indistinguishable from non rotated data. As angle and distance based features are calculated with respect to critical infrastructure

6.6.1. Explaining effects with decision trees

The decision tree classifier being a white box classifier provides a lot of insight into the changes occurring with less features present. Because it is fully white box, it is possible to visualize the final decision tree. The visualized trees are shown with a max depth of 3, making it easier to visualize[9]. The trees with all features and the tree without critical infrastructure related features are shown, the trees for no angle based features and the tree for no distance based features are shown in **Appendix C**.

Figure 6.11 shows a decision tree using all features. The first 2 nodes contain *distance to critical infrastructure*, showing it's importance. Next to that only *speed average* is not critically infrastructure related. Confirming the strength of adding critical infrastructure to classification.

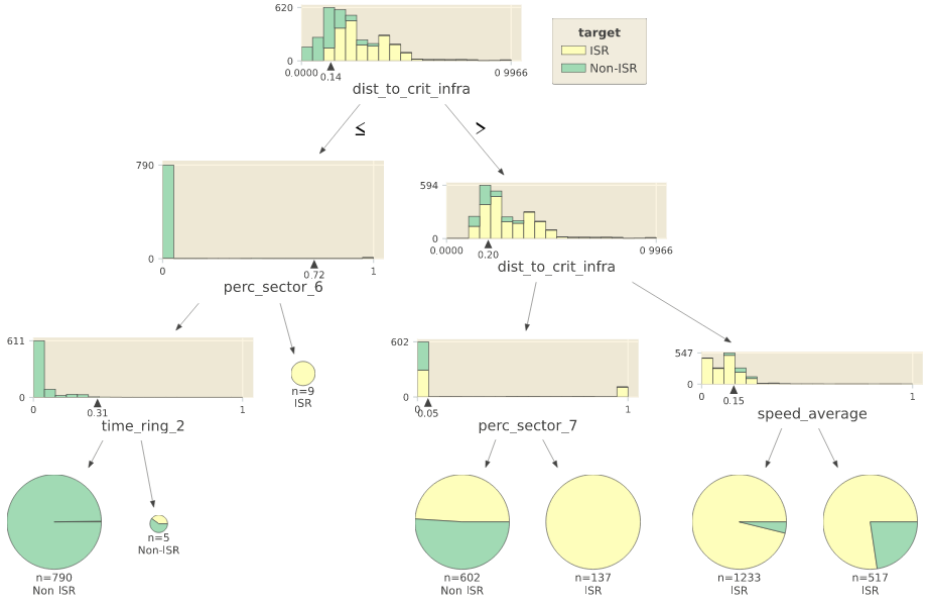


Figure 6.11: Decision tree with all features

Figure 6.12 shows a decision tree where all critical infrastructure related features are removed. With no critical infrastructure related features, the covering of the same trajectory becomes the best divider reflecting the multivariate test performed in **feature exploration**. Speed average is still present as a divisor in this tree. The visualization clearly shows the ambiguity in classification, where the all features tree has pie charts showing large single classes. The no critical infrastructure tree showing larger minority classes in the pie chart.

[9] optimal depths are between 11 and 14 nodes deep.

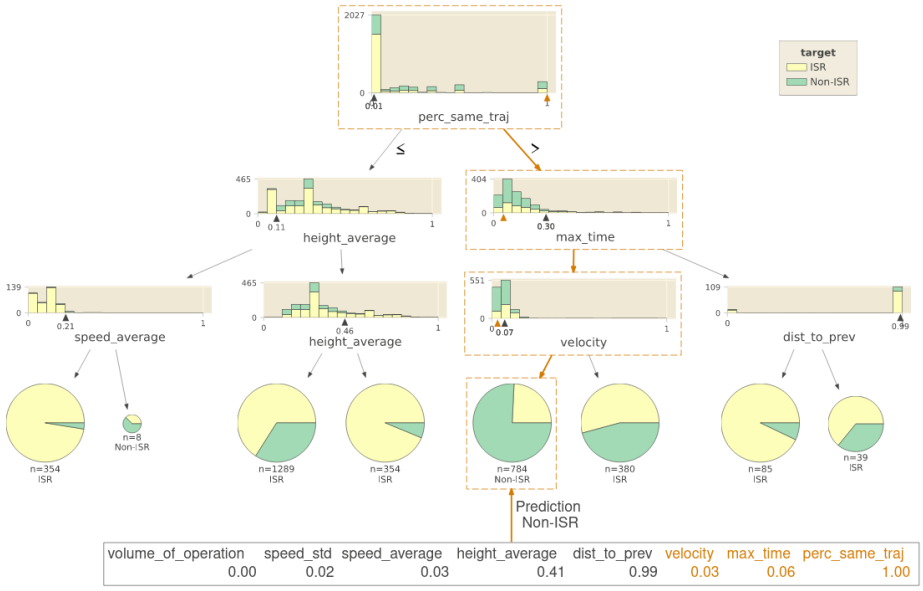


Figure 6.12: Decision tree without critical infrastructure based features

In summary, the Random forest is the best performing classifier, in terms of accuracy and robustness. The decision tree and SVM perform very well too, making them good alternatives.

7

Future work

This chapter covers improvements recommendations for future work. There are a number of improvements to the solution. The first section, **Section 7.1**, is a discussion of improvements to the dataset. **Section 7.2** covers improvements to the theoretical model. And **Section 7.3** goes into the identification process and its improvements.

7.1. Improvements to the dataset

One of the main challenges of this thesis is the lack of "in the wild" recordings of behavior. Future work can aim to get recordings from war zones as well as civilian identification missions. Next to that a new iteration of ISR flights can be performed with the knowledge and models provided by this thesis. Knowing the boundaries of classification, flying adversarial missions that avoid known ISR patterns will challenge and improve the current models. Next to flying ISR data, other benign and malicious (as defined in **System Model** and **Threat Model**) flights can be added to the dataset.

Additionally changing the equipment and environments used improve the dataset: flying with other drone models, changing the camera used by the drone, flying missions with different operators, using different radar systems or settings and flying missions in other environments (different weather and/or locations).

Addition of more features is another improvement for the future. Incorporating the weather and changes in visibility into the dataset for example. Rings, sectors and zones are a big improvement in implementing terrain features, however altitude based layers are another extra step to make. Allowing a more precise allocation of importance to layers.

7.2. Improvements to the theoretical model

The theoretical model derived from the dataset removes the control and flight path characteristics as stated in **System Model** and **Threat Model** are removed in our solution. In the future a good proxy for these characteristics should be found, the best predictors for control are: "standard deviation of each of acceleration, jerk, roll velocity, roll acceleration and pitch velocity"[69]. These were determined with computer simulation programs. Increase in accuracy of radar and validation of these factors in the field would be an interesting expansion to this thesis. Due to the precision of the SQUIRE radar system it is not possible to accurately detect the features in our dataset. A higher frequency could solve this problem, at the cost of range. Finally, validation of the theoretical model with subject matter experts should be performed, a discussion on its parameters would be very valuable.

7.3. Improvements to the algorithms

Due to the performance of the used algorithms, improvement is currently not a high priority. The main improvement to the algorithms is the prevention of overfitting our notion of ISR behavior. Actual ISR behavior might be different to our definition, strict adherence to the solution might make one blind to adversarial ISR behavior. Because of that the solution should be used as an accessory to decision making and not as a sole basis of decision making as explained in **section 1.2**. As **section 1.2** explains and due to the sufficient performance of the current algorithms, more complex black box algorithms are not explored in this thesis. In the future our classifiers could decrease in performance and justify exploration of more complex black box algorithms such as neural networks.

8

Conclusion

The final chapter, Conclusion, reiterates the research question of this thesis and answers it in **Section 8.1**. Based on the answer a recommendation for the military is provided in **Section 8.2**.

8.1. Research question

The research question of this thesis is: "How accurately can we identify Intelligence, Surveillance, Reconnaissance (ISR) from non ISR behavior in drones using data collected by radar." In order to answer the resaerch question the central hypothesis will first be answered: "there is no significant difference in behavior, as detected by radar, between ISR drones and other types of drones.".

The evaluation chapter clearly shows that there is a distinction in behavior between ISR and other drones. Decision trees, random forest as well as an SVM are able to distinguish ISR from non ISR behavior. Hence the null-hypothesis is rejected. This rejection enables identification of ISR behavior. To answer the research question: the accuracy achieved varies between 85% and 96% based on the features used and track lengths. The longer the track length available the better the classification and random forest classifier is the best classifier by a small margin. Removing features continues to provide an accuracy of 86%.

8.2. Recommendation Military

The question posed by the military is: "is it possible to use radar data to improve identification by a radar-operator?". The simple answer is: Yes, to a high degree our conception of ISR behavior can be distinguished from other behavior.

In achieving this answer we discovered new features which are useful in talking about ISR behavior: the distance to critical infrastructure, total amount of degrees of operation around critical infrastructure, altitude and the percentage covering of the same trajectory. In discussing drone behavior these features should be used. Next to that we recommend the addition of important rings, sectors and zones in observing environments. This research provides a starting point for a more complex understanding and discussion of drone behavior. Improving the teaching process of drone and radar operators.

The addition of identification algorithms to the decision making process of radar operators looks very promising. In environments with a high drone-density the algorithms assist in making preliminary identifications. Removing work load of the operators. In lower drone-density environments the algorithms can help in identifying behavior at a longer distance, providing more time to react. Three algorithms were compared, all three identify in a negligible amount of time because they are calibrated before deployment. Due to the nature of operations the recommendation is to use a decision tree classifier. The decision tree classifier allows a tracing of the identification process, providing operators a clear explanation of the achieved identification. Because the decision tree classifier is only slightly worse than a random forest the loss in accuracy is acceptable. The consequences of deactivation of drones and the dangers of miss-identification call for verification by a human operator.

In conclusion, radar and behavior based identification of drone intention are a continuously evolving field of research. These results look promising. With the challenging of the current algorithms and discussions about the theoretical model, the identification process will grow stronger.

A

Feature list

This appendix provides an overview of all the explored and implemented features. Providing a short title followed by the unit it is measured in and subsequently a short definition of the feature.

- Distance to objective [meters]: the main feature used for identification, this feature will be enriched by combining it with other features to get better threat levels.
- Degrees of operation [degrees]: the amount of degrees that a drone has flown around the sensitive object, a larger amount of degrees corresponds to a more complete view.
- Changes in direction [count]: the changes in direction bigger than X degrees made by the drone. A large amount of changes might correspond to more erratic and less of a focus on a clear objective
- Speed variance [kilometers per hour]: the changes in speed a drone performs with respect to its average. If a drone comes in flying fast and then slows down its movement that might indicate a switch to ISR behavior.
- Height variance [meters]: this feature can correspond to a change in perspective, the drone can attempt to get an overview of the sensitive object and its surroundings. A low height at bigger distance might correspond to having a bad view of the object.
- Average speed [kilometers per hour]: the average speed of a drone since the moment of detection. A faster drone has a different objective than a slow flying drone, as defined in the **Threat Model**.
- Average Height [meters]: the average height of a drone since the moment of detection. A higher flying drone has a different objective than a low flying drone, as defined in the **Threat Model**.
- Time within accurate zone [seconds]: the amount of seconds spent within ISR range, the longer a drone is within this range, the more information can be gathered.
- Non moving time [seconds]: the amount of seconds that the drone has not changed position. By being more stable more images from the same perspective are gathered. Using interpolation these images can be merged to get a more detailed view.
- Covering of previous trajectory [% covered]: this is an indicator for automated behavior, useful in gathering information at multiple points in time to build up a profile of a location.
- Max time spent in zone, ring or sector [s]: an indicator of what the longest time between 2 data points in an area is. [1]
- Time spent in zone or sector [s]: the total amount of time spent by a track within an area.
- Percentage of time spent in zone, ring or sector [%]: the percentage of the total amount of time spent by the track within each area.[1]

[1] The definition of sectors, rings and zones is given in **Section A.1**

- Movement towards sensitive object [percentage]: the amount of movement the drone has performed towards the objective. This feature is subdivided into movement in a 45 and a 90 foot cone, further definition of this feature is found in **Section A.2**
- Volume of operation [m^3]: the volume covered by all the data points provided with a track.
- Point of detection/loss [x,y,z coordinate]: is a useful feature for finding rogue access points or creating a map of possible bad actor locations. This feature is not explored in this thesis.
- Weather conditions [type of weather]: a feature that adds information about the current weather conditions. A change in weather could affect other indicators. This feature is not explored in this thesis.

A.1. Sectors, Rings and zones

In order to quantify location information with regards to critical infrastructure the area surrounding the critical infrastructure is subdivided into zones. Instead of relying solely on distance or angle regarding the critical infrastructure a more abstract approach is made. Making reasoning about distance and angle easier. As shown in **Figure A.1**, the area surrounding the critical infrastructure is subdivided into rings as well as sectors. The rings start at the critical infrastructure and are subdivided based on radius (250 meters, 500, 750 and 1000 meters). The sectors originate from the critical infrastructure and begin at unit vector (1, 0). The sectors divide the 360 degrees around the object into 45 degree sectors. Based on preference the rings and sectors can be changed at will. Zones are created by the combination of rings and sectors, so a zone would be sector 0 (0-45 degrees) and ring 0 (0-250 meters).

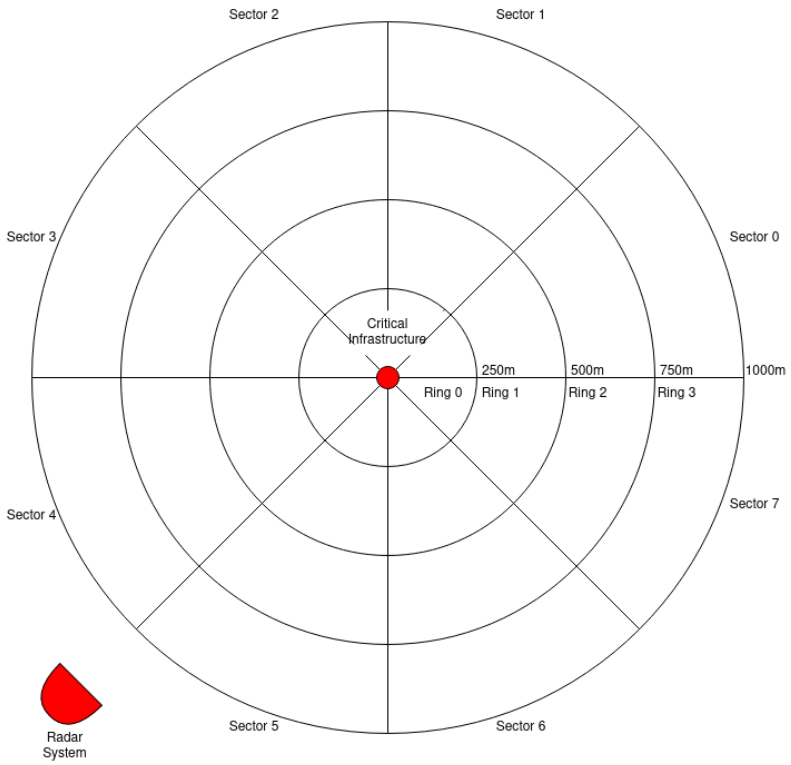


Figure A.1: Sectors and Rings surrounding critical infrastructure

Using the defined zones and sectors, features can be subdivided into features per zone or sector. The

A.2. Time in cone

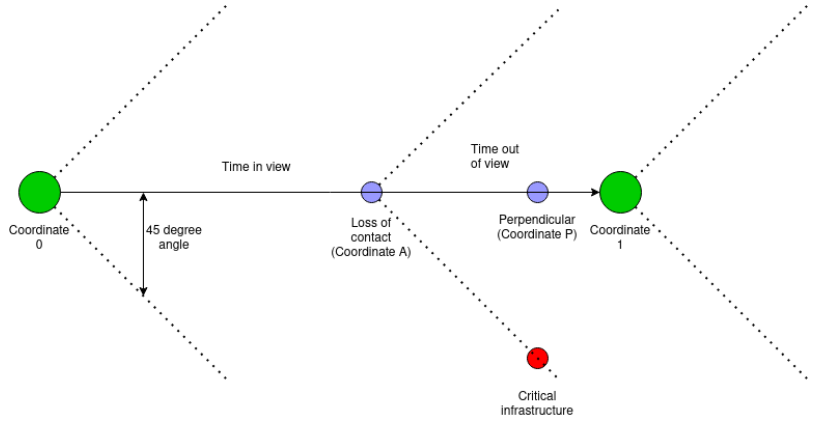


Figure A.2: Time in cone (45 degrees)

The time in cone feature creates a cone or "view" based on the direction the drone has moved in the last 2 coordinates (coordinate 0 and coordinate 1). Using this cone it calculates if the position of the critical infrastructure (coordinate c) is inside this cone or not as well as how long the critical infrastructure was inside the cone on the previous time interval. This is done by calculating the perpendicular intersection of the critical infrastructure on the line between coordinate 0 and 1 (coordinate I). Coordinate I represents the division of the distance between coordinate 0 and 1 if the cone is 90 degrees. At the time in cone at 90 degrees the time spent between coordinate 0 and 1 is thus divided by the ratio of the distance till coordinate I and the distance after coordinate I. For time in cone at other degrees the distance from coordinate c to coordinate I is divided by the tangent of the angle to provide the distance between coordinate A and I. Using that distance the position of a on the distance between coordinate 0 and 1 is found and can be used to calculate the proportion within view of any angle. The algorithm used is supplied below.

```
"""
          so
         /|
        / |
c0-----a--i--------c1
so = sensitive object
a = point where angle hits sensitive object
i = point of intersect
"""
c0 = np.array(c0)
c1 = np.array(c1)
sens_obj = np.array(self.sensitive_object)

# calc a - so - i triangle distances
# calc distance from sens_obj to the line between c0 and c1
"""
source: https://stackoverflow.com/questions/39840030/distance-between-point-and-a-line-f
"""
d_so_i = norm(np.cross(c1 - c0, c0 - sens_obj)) / norm(c1 - c0)

# calc point at which the sens obj goes out of view
d_a_i = d_so_i / math.tan(math.radians(angle))

# calculate distances from c0
# calc distance sens obj and c0
d_so_c0 = norm(c0 - sens_obj)
```

```
# calc distance i and c0
d_i_c0 = math.sqrt(math.pow(d_so_c0, 2) - math.pow(d_so_i, 2))

# calc distance c0 and a
d_c0_a = d_i_c0 - d_a_i
# find point a along the line between c0 and c1
# calculate unit vector from c0 to c1
v_c0_c1 = c1 - c0
norm_c0_c1 = math.sqrt(v_c0_c1[0] ** 2 + v_c0_c1[1] ** 2)
unit_vector_c0_c1 = [v_c0_c1[0] / norm_c0_c1, v_c0_c1[1] / norm_c0_c1]

# find point a which is d_c0_a along unit vector c0_c1
a_x = d_c0_a * unit_vector_c0_c1[0] + c0[0]
a_y = d_c0_a * unit_vector_c0_c1[1] + c0[1]
a = [a_x, a_y]

# check whether point a is on the line between c0 and c1
# calculate distance c1 and a
d_c1_a = norm(c1 - a)

# calc distance c1 and c0
d_c0_c1 = norm(c0 - c1)

if d_c0_a + d_c1_a != d_c0_c1:
    return 1.0
else:
    return d_c0_a / d_c0_c1
```

B

Data exploration

B.1. Sector Heat Map

The regular text shows the heat map for rings. **Figure B.1** shows the heat map for sectors.

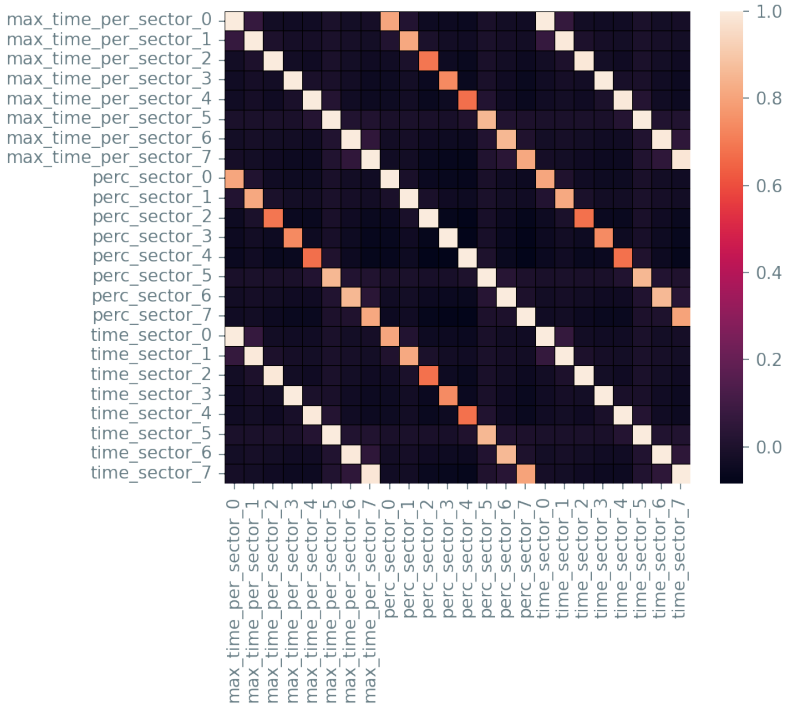


Figure B.1: Sector Heat Map

B.2. Feature importance

In order to compare individual features, two kinds of measures are used: univariate and multivariate. univariate measures consider individual features whereas multivariate measures measure the contribution of a feature conditionally on every other feature.

B.2.1. Univariate measures

The first univariate measure is the F-statistic which amounts to a Pearson correlation which addresses linear relationships only [64, 75]. The second measure is the Maximal Information Coefficient (MIC), which measures uncertainty reduction about a random variable by knowledge of another variable [30].

B.2.2. Multivariate measures

The first multivariate measures are determined in fit time, they reflect what a model learnt from training data. The caveat for fit-time measures is that it may assign a high importance to features that do not work well on unseen data. Starting off with impurity reduction, determined on decision trees, it measures the decrease in mean impurity of all nodes that split on the measured feature [25]. The second fit-time measure is split count, counting the amount of times a feature has been used for a split [37]. The number of splits is an ambiguous measure as some splits contain just a small number of observations. Weighting splits by the coverage they achieve bypasses this and provides the coverage metric [38].

The final measures regard predict-time measures, these measures are model independent. These measures are calculated after training is completed and measure how good a feature classifies unseen data. The first feature is the permutation importance, it measures the performance of a classifier with or without a certain feature [1]. The final measure is the absolute importance, representing how far a specific feature influences the final prediction [27].

The 10 best scoring features are shown in **Figure :10**$_b est_p redictors$. The distance to critical infrastructure is by far the best predictor on both univariate and multivariate measures. Only on Coverage it scores less than other features, meaning the splits created by it do not cover a lot of dependent cases. It is interesting to see that max time per sector scores well on split-time measures but bad on predict-time measures.

	f-statistic	MIC	Impurity Reduction	Split count	Coverage	Permutation importance	Absolute importance	Total Normalized [%]
dist_to_crit_infra	1.00	1.00	1.00	1.00	0.21	1.00	1.00	21.07
height_average	0.02	0.22	0.17	0.60	0.14	0.20	0.15	5.09
z	0.02	0.24	0.17	0.50	0.08	0.21	0.15	4.66
max_time_per_sector_2	0.02	0.12	0.02	0.00	1.00	0.00	0.00	3.95
max_time_per_sector_7	0.04	0.08	0.03	0.04	0.77	0.00	0.00	3.24
speed_average	0.00	0.05	0.12	0.36	0.09	0.17	0.14	3.17
max_time_per_sector_6	0.03	0.04	0.05	0.02	0.71	0.00	0.00	2.86
perc_sector_2	0.11	0.09	0.03	0.00	0.57	0.00	0.00	2.72
perc_sector_6	0.03	0.04	0.04	0.03	0.50	0.06	0.09	2.71
perc_sector_7	0.07	0.08	0.05	0.01	0.56	0.01	0.01	2.65

Figure B.2: Strongest predictors

In order to see the decrease in feature importance on removal of distance to critical infrastructure the tests were executed without this feature. Resulting in **Figure B.3**. Removing the distance results in a shift in most importance features, degrees of operation becoming very important where it was not important before.

	f-statistic	MIC	Impurity Reduction	Split count	Coverage	Permutation importance	Absolute importance	Total Normalized [%]
degrees_of_operation	0.83	0.68	0.30	0.15	0.18	1.00	1.00	5.83
height_average	0.07	0.92	1.00	1.00	0.15	0.42	0.39	5.56
z	0.07	1.00	1.00	0.86	0.22	0.20	0.19	4.98
max_time_per_ring_1	0.66	0.77	0.31	0.08	1.00	0.00	0.00	3.97
speed_std	0.01	0.21	0.59	0.94	0.13	0.24	0.26	3.37
dist_to_prev	0.25	0.33	0.73	0.52	0.18	0.20	0.15	3.32
no_fly_zone_entered	0.53	0.40	0.35	0.11	0.72	0.10	0.11	3.26
speed_average	0.01	0.19	0.68	0.93	0.07	0.23	0.18	3.23
perc_same_traj	0.53	0.76	0.30	0.08	0.27	0.19	0.15	3.21
perc_to_crit_infra_90	0.26	0.52	0.45	0.48	0.16	0.16	0.14	3.05

Figure B.3: Strongest predictors without distance

C

Decision tree visualization

Further visualization of the decision tree classifier, without the use of angle based features and without the use of distance based features.

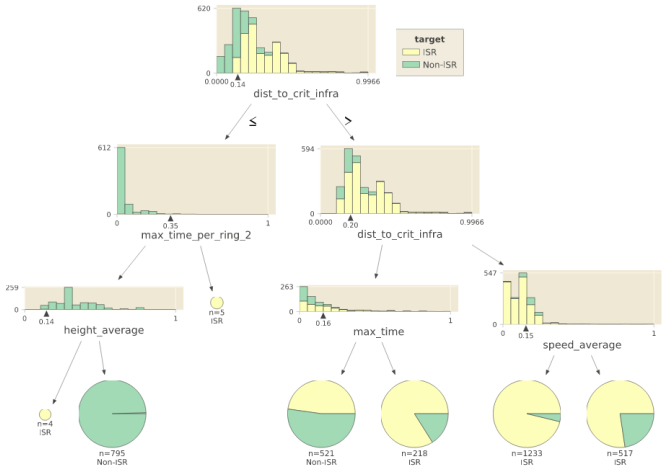


Figure C.1: Decision tree without angle based features

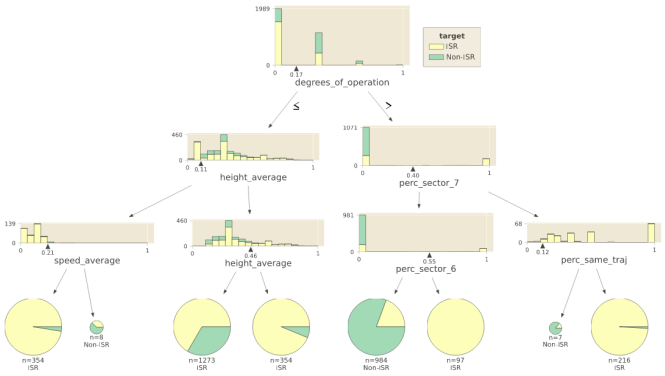


Figure C.2: Decision tree without distance based features

Bibliography

[1] André Altmann, Laura Toloşi, Oliver Sander, and Thomas Lengauer. Permutation importance: a corrected feature importance measure. *Bioinformatics*, 26(10):1340–1347, 2010.

[2] Henrik Andersson and Chi Thong Luong. Classification between birds and uavs using recurrent neural networks. 11 2020. URL `https://hdl.handle.net/20.500.12380/302030`.

[3] Mohammad Mahdi Azari, Hazem Sallouha, Alessandro Chiumento, Sreeraj Rajendran, Evgenii Vinogradov, and Sofie Pollin. Key technologies and system trade-offs for detection and localization of amateur drones. *IEEE Communications Magazine*, 56(1):51–57, 2018.

[4] Andrea Bernardini, Federica Mangiatordi, Emiliano Pallotti, and Licia Capodiferro. Drone detection by acoustic signature identification. *Electronic Imaging*, 2017(10):60–64, 2017.

[5] Afaf Bouhoute, Rachid Oucheikh, Karim Boubouh, and Ismail Berrada. Advanced driving behavior analytics for an improved safety assessment and driver fingerprinting. *IEEE Transactions on Intelligent Transportation Systems*, 20(6):2171–2184, 2019. doi: 10.1109/TITS.2018.2864637.

[6] Daniel A. Brooks, Olivier Schwander, Frederic Barbaresco, Jean-Yves Schneider, and Matthieu Cord. Temporal deep learning for drone micro-doppler classification. In *2018 19th International Radar Symposium (IRS)*, pages 1–10, 2018. doi: 10.23919/IRS.2018.8447963.

[7] Joël Busset, Florian Perrodin, Peter Wellig, Beat Ott, Kurt Heutschi, Torben Rühl, and Thomas Nussbaumer. 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*, volume 9647, page 96470F. International Society for Optics and Photonics, 2015.

[8] M. Caris, S. Stanko, W. Johannes, S. Sieger, and N. Pohl. Detection and tracking of micro aerial vehicles with millimeter wave radar. *2016 46th European Microwave Conference (EuMC)*, pages 1553–1555, 2016.

[9] M. Caris, W. Johannes, S. Sieger, V. Port, and S. Stanko. Detection of small uas with w-band radar. In *2017 18th International Radar Symposium (IRS)*, pages 1–6, 2017. doi: 10.23919/IRS.2017.8008143.

[10] Simon Chadwick, Will Maddern, and Paul Newman. Distant vehicle detection using radar and vision. In *2019 International Conference on Robotics and Automation (ICRA)*, pages 8311–8317, 2019. doi: 10.1109/ICRA.2019.8794312.

[11] Xianyu Chang, Chaoqun Yang, Junfeng Wu, Xiufang Shi, and Zhiguo Shi. A surveillance system for drone localization and tracking using acoustic arrays. In *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pages 573–577, 2018. doi: 10.1109/SAM.2018.8448409.

[12] Yunseok Chang. A drone iff and tracking algorithm with the relay drone and the beacon system. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 7:199–203, 2019.

[13] Frank Christnacher, Sébastien Hengy, Martin Laurenzis, Alexis Matwyschuk, Pierre Naz, Stéphane Schertzer, and Gwenael Schmitt. Optical and acoustical uav detection. In *Electro-Optical Remote Sensing X*, volume 9988, page 99880B. International Society for Optics and Photonics, 2016.

[14] Mario Coppola, Kimberly N McGuire, Christophe De Wagter, and Guido CHE de Croon. A survey on swarming with micro air vehicles: Fundamental challenges and constraints. *Frontiers in Robotics and AI*, 7:18, 2020.

[15] JJ M de Wit, RIA Harmanny, and G Premel-Cabic. Micro-doppler analysis of small uavs. In *2012 9th European Radar Conference*, pages 210–213. IEEE, 2012.

[16] J. Delgado-Centeno, P.J. Sanchez-Cuevas, Carol Martinez, and M.A. Olivares-Mendez. Enhancing lunar reconnaissance orbiter images via multi-frame super resolution for future robotic space missions. *IEEE Robotics and Automation Letters*, 6:7729–7735, 10 2021. doi: 10.1109/LRA.2021.3097510.

[17] Thomas G. Dietterich. Approximate Statistical Tests for Comparing Supervised Classification Learning Algorithms. *Neural Computation*, 10(7):1895–1923, 10 1998. ISSN 0899-7667. doi: 10.1162/089976698300017197. URL https://doi.org/10.1162/089976698300017197.

[18] Guoru Ding, Qihui Wu, Linyuan Zhang, Yun Lin, Theodoros A Tsiftsis, and Yu-Dong Yao. An amateur drone surveillance system based on the cognitive internet of things. *IEEE Communications Magazine*, 56(1):29–35, 2018.

[19] DJI. Inspire 2, power beyond imagination. https://www.dji.com/nl/inspire-2, 2022. [Online; accessed 24-July-2022].

[20] Bardienus P. Duisterhof, Shushuai Li, Javier Burgués, Vijay Janapa Reddi, and Guido C. H. E. de Croon. Sniffy bug: A fully autonomous swarm of gas-seeking nano quadcopters in cluttered environments, 2021.

[21] The Economist. A looming threat, 2018. URL https://www.economist.com/democracy-in-america/2015/03/19/a-looming-threat.

[22] The Economist. Home-made drones now threaten conventional armed forces, 2018. URL https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces.

[23] Martins Ezuma, Fatih Erden, Chethan Kumar Anjinappa, Ozgur Ozdemir, and Ismail Guvenc. Detection and classification of uavs using rf fingerprints in the presence of wi-fi and bluetooth interference. *IEEE Open Journal of the Communications Society*, 1:60–76, 2020. doi: 10.1109/OJCOMS.2019.2955889.

[24] Matt Gaffney. Aerospace village - uav research series - ep1, 2021. URL https://youtu.be/V5M_aE7Z0SA?t=1623.

[25] Ulrike Grömping. Variable importance assessment in regression: linear regression versus random forest. *The American Statistician*, 63(4):308–319, 2009.

[26] RIA Harmanny, JJM De Wit, and G Prémel Cabic. Radar micro-doppler feature extraction using the spectrogram and the cepstrogram. In *2014 11th European Radar Conference*, pages 165–168. IEEE, 2014.

[27] Hilary J Holz and Murray H Loew. Relative feature importance: A classifier-independent approach to feature selection. In *Machine intelligence and pattern recognition*, volume 16, pages 473–487. Elsevier, 1994.

[28] Kasani Payam Hosseinzadeh, Oh Seung Min, Choi Yo Han, Ha Sang Hun, Jun Hyungmin" ark Kyu Hyun, Ko Han Seo, Kim Jo Eun, Choi Jung Woo, Cho Eun Seok, and Kim Jin Soo. A computer vision-based approach for behavior recognition of gestating sows fed different fiber levels during high ambient temperature. *Journal of animal science and technology*, 63:367–379, 2021. doi: 10.5187/jast.2021.e35. URL https://www.sciencedirect.com/science/article/pii/S1077314215002052.

[29] Dae Jung Kim, Jin Sung Kim, Jin Ho Yang, Seok Cheol Kee, and Chung Choo Chung. Lane change intention classification of surrounding vehicles utilizing open set recognition. *IEEE Access*, 9:57589–57602, 2021. doi: 10.1109/ACCESS.2021.3072413.

[30] Justin B Kinney and Gurinder S Atwal. Equitability, mutual information, and the maximal information coefficient. *Proceedings of the National Academy of Sciences*, 111(9):3354–3359, 2014.

[31] Michael T Klare. 'skynet'revisited. *Arms Control Today*, 50(3):10–15, 2020.

[32] Eugene F Knott, John F Schaeffer, and Michael T Tulley. *Radar cross section*. SciTech Publishing, 2004.

[33] Sonu Lamba and Neeta Nain. Crowd monitoring and classification: A survey. In Sanjiv K. Bhatia, Krishn K. Mishra, Shailesh Tiwari, and Vivek Kumar Singh, editors, *Advances in Computer and Computational Sciences*, pages 21–31, Singapore, 2017. Springer Singapore. ISBN 978-981-10-3770-2.

[34] Fengdan Lao, Guanghui Teng, Jun Li, Ligen Yu, and Zhuo Li. Behavior recognition method for individual laying hen based on computer vision. *Transactions of the Chinese Society of Agricultural Engineering*, 28 (24):157–163, 2012.

[35] Nadav Levanon. Radar principles. *New York*, 1988.

[36] Dingyi Li and Zengfu Wang. Video superresolution via motion compensation and deep residual learning. *IEEE Transactions on Computational Imaging*, 3(4):749–762, 2017. doi: 10.1109/TCI.2017.2671360.

[37] Xiao Li, Yu Wang, Sumanta Basu, Karl Kumbier, and Bin Yu. A debiased mdi feature importance measure for random forests. *Advances in Neural Information Processing Systems*, 32, 2019.

[38] Lingyi Liu, David Sheridan, William Tuohy, and Shobha Vasudevan. A technique for test coverage closure using goldmine. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 31(5): 790–803, 2012.

[39] Georgia Lykou, Dimitrios Moustakas, and Dimitris Gritzalis. Defending airports from uas: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors*, 20(12), 2020. ISSN 1424-8220. doi: 10.3390/s20123537. URL `https://www.mdpi.com/1424-8220/20/12/3537`.

[40] Rafael Gomes Mantovani, Tomáš Horváth, Ricardo Cerri, Sylvio Barbon Junior, Joaquin Vanschoren, and André Carlos Ponce de Leon Ferreira de Carvalho. An empirical study on hyperparameter tuning of decision trees, 2018. URL `https://arxiv.org/abs/1812.02207`.

[41] Mark Marsden, Kevin McGuinness, Suzanne Little, and Noel E. O'Connor. Resnetcrowd: A residual deep learning architecture for crowd counting, violent behaviour detection and crowd density level classification. In *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 1–7, 2017. doi: 10.1109/AVSS.2017.8078482.

[42] Vincent Mirelli, Stephen Tenney, Yoshua Bengio, Nicolas Chapados, and Olivier Delalleau. Statistical machine learning algorithms for target classification from acoustic signature. In *Proc. MSS Battlespace Acoust. Magn. Sensors*, pages 1–18. Citeseer, 2009.

[43] Pavlo Molchanov, Ronny IA Harmanny, Jaco JM de Wit, Karen Egiazarian, and Jaakko Astola. Classification of small uavs and birds by micro-doppler signatures. *International Journal of Microwave and Wireless Technologies*, 6(3-4):435–444, 2014.

[44] Thomas Multerer, Alexander Ganis, Ulrich Prechtel, Enric Miralles, Askold Meusling, Jan Mietzner, Martin Vossiek, Mirko Loghi, and Volker Ziegler. Low-cost jamming system against small drones using a 3d mimo radar based tracking. In *2017 European Radar Conference (EURAD)*, pages 299–302. IEEE, 2017.

[45] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu. Matthan: Drone presence detection by identifying physical signatures in the drone's rf communication. In *Proceedings of the 15th annual international conference on mobile systems, applications, and services*, pages 211–224, 2017.

[46] Ian Norman. A practical guide to creating superresolution photos with photoshop, 2015. URL `https://petapixel.com/2015/02/21/a-practical-guide-to-creating-superresolution-photos-with-photoshop/`.

[47] James O'Malley. The no drone zone. *Engineering Technology*, 14(2):34–38, 2019. doi: 10.1049/et.2019.0201.

[48] Andrea Pennisi, Domenico D. Bloisi, and Luca Iocchi. Online real-time crowd behavior detection in video sequences. *Computer Vision and Image Understanding*, 144:166–176, 2016. ISSN 1077-3142. doi: https://doi.org/10.1016/j.cviu.2015.09.010. URL `https://www.sciencedirect.com/science/article/pii/S1077314215002052`. Individual and Group Activities in Video Event Analysis.

[49] Edward M Purcell, Edward Mills Purcell, Edward Mills Purcell, and Edward Mills Purcell. *Electricity and magnetism*, volume 2. McGraw-Hill New York, 1965.

[50] Samiur Rahman and Duncan A Robertson. Classification of drones and birds using convolutional neural networks applied to radar micro-doppler spectrogram images. *IET Radar, Sonar & Navigation*, 14(5): 653–661, 2020.

[51] redimec. Squire man-portable-surveillance radar, 2021. URL `https://www.redimec.com.ar/contenido/productos/pdf/1432630805_1.pdf`.

[52] Matthew Ritchie, Francesco Fioranelli, Hugh Griffiths, and Borge Torvik. Micro-drone rcs analysis. In *2015 IEEE Radar Conference*, pages 452–456. IEEE, 2015.

[53] Artem Rozantsev, Vincent Lepetit, and Pascal Fua. Detecting flying objects using a single moving camera. *IEEE transactions on pattern analysis and machine intelligence*, 39(5):879–892, 2016.

[54] Sam Kamkar. Skyjack: autonomous drone hacking, 2013. URL `http://samy.pl/skyjack/`. [Online; accessed 2-August-2021].

[55] Samuele Mazzanti. 6 types of feature importance any data scientist should master. `https://towardsdatascience.com/6-types-of-feature-importance-any-data-scientist-should-master-1bfd566f2` 2022. [Online; accessed 24-July-2022].

[56] Waylon D Scheller. *Detecting drones using machine learning*. PhD thesis, Iowa State University, 2017.

[57] Alexander Sedunov, Alexander Sutin, Nikolay Sedunov, Hady Salloum, Alexander Yakubovskiy, and David Masters. Passive acoustic system for tracking low-flying aircraft. *IET Radar, Sonar & Navigation*, 10(9):1561–1568, 2016.

[58] Hakki Erhan Sevil, Atilla Dogan, Kamesh Subbarao, and Brian Huff. Evaluation of extant computer vision techniques for detecting intruder suas. In *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 929–938. IEEE, 2017.

[59] Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Communications Magazine*, 56(4):68–74, 2018.

[60] Zhiguo Shi, Chengwei Zhou, Yujie Gu, Nathan A Goodman, and Fengzhong Qu. Source estimation using coprime array: A sparse reconstruction perspective. *IEEE Sensors Journal*, 17(3):755–765, 2016.

[61] Dong-Hun Shin, Dae-Hwan Jung, Dong-Chan Kim, Jong-Wook Ham, and Seong-Ook Park. A distributed fmcw radar system based on fiber-optic links for small drone detection. *IEEE Transactions on Instrumentation and Measurement*, 66(2):340–347, 2016.

[62] sklearn. sklearn.tree.decisiontreeclassifier. `https://scikit-learn.org/stable/modules/generated/sklearn.tree.DecisionTreeClassifier.html`, 2022. [Online; accessed 02-August-2022].

[63] Dmitrii Solomitckii, Margarita Gapeyenko, Vasilii Semkin, Sergey Andreev, and Yevgeni Koucheryavy. Technologies for efficient amateur drone detection in 5g millimeter-wave cellular infrastructure. *IEEE Communications Magazine*, 56(1):43–50, 2018. doi: 10.1109/MCOM.2017.1700450.

[64] Lars St, Svante Wold, et al. Analysis of variance (anova). *Chemometrics and intelligent laboratory systems*, 6(4):259–272, 1989.

[65] Rick L Sturdivant and Edwin KP Chong. Systems engineering baseline concept of a multispectral drone detection solution for airports. *IEEE Access*, 5:7123–7138, 2017.

[66] Van-Phat Thai, Weixian Zhong, Thinh Pham, Sameer Alam, and Vu Duong. Detection, tracking and classification of aircraft and drones in digital towers using machine learning on motion patterns. In *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pages 1–8, 2019. doi: 10.1109/ICNSURV.2019.8735240.

[67] THALES. Squire ground surveillance radar, 2021. URL `https://www.thalesgroup.com/en/squire-ground-surveillance-radar`.

[68] Tommy Dang. Guide to accuracy, precision, and recall. https://www.mage.ai/blog/definitive-guide-to-accuracy-precision-recall-for-product-developers, 2022. [Online; accessed 24-July-2022].

[69] Ahmad Traboulsi. *Quadcopter Behaviour Identification*. PhD thesis, Carleton University, 2022.

[70] Eren Unlu, Emmanuel Zenou, Nicolas Riviere, and Paul-Edouard Dupouy. Deep learning-based strategies for the detection and tracking of drones using several cameras. *IPSJ Transactions on Computer Vision and Applications*, 11(1):1–13, 2019.

[71] L. Watkins, Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, W. H. Robinson, and A. Rubin. Defending against consumer drone privacy attacks: A blueprint for a counter autonomous drone tool. 2020.

[72] Wikipedia contributors. Identification friend or foe — Wikipedia, the free encyclopedia, 2021. URL https://en.wikipedia.org/w/index.php?title=Identification_friend_or_foe&oldid=1028434033. [Online; accessed 2-August-2021].

[73] Wikipedia contributors. Electromagnetic radiation — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Electromagnetic_radiation&oldid=1037259666, 2021. [Online; accessed 19-August-2021].

[74] Wikipedia contributors. Azimuth — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Azimuth&oldid=1096996820, 2022. [Online; accessed 24-July-2022].

[75] Wikipedia contributors. Correlation — Wikipedia, the free encyclopedia, 2022. URL https://en.wikipedia.org/w/index.php?title=Correlation&oldid=1099281285. [Online; accessed 22-July-2022].

[76] Wikipedia contributors. Dependent and independent variables — Wikipedia, the free encyclopedia, 2022. URL https://en.wikipedia.org/w/index.php?title=Dependent_and_independent_variables&oldid=1096272389. [Online; accessed 22-July-2022].

[77] Wikipedia contributors. Normal distribution — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Normal_distribution&oldid=1103405874, 2022. [Online; accessed 11-August-2022].

[78] Wikipedia contributors. Graphical user interface — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Graphical_user_interface&oldid=1098150200, 2022. [Online; accessed 24-July-2022].

[79] Wikipedia contributors. Support-vector machine — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Support-vector_machine&oldid=1102839221, 2022. [Online; accessed 8-August-2022].

[80] Thomas Withington. Scanning for trouble. *Asian Military Review*, 01 2020. URL https://asianmilitaryreview.com/2020/01/scanning-for-trouble/. [Online; accessed 2-August-2021].

[81] Christian Wolff. Frequency-modulated continuous-wave radar (fmcw radar). https://www.radartutorial.eu/02.basics/Frequency%20Modulated%20Continuous%20Wave%20Radar.en.html, 2022. [Online; accessed 24-July-2022].

[82] Yu Wu, Yutian Lin, Xuanyi Dong, Yan Yan, Wei Bian, and Yi Yang. Progressive learning for person re-identification with one example. *IEEE Transactions on Image Processing*, 28(6):2872–2881, 2019. doi: 10.1109/TIP.2019.2891895.

[83] Philippe Martin Wyder, Yan-Song Chen, Adrian J Lasrado, Rafael J Pelles, Robert Kwiatkowski, Edith OA Comas, Richard Kennedy, Arjun Mangla, Zixi Huang, Xiaotian Hu, et al. Autonomous drone hunter operating by deep learning and all-onboard computations in gps-denied environments. *PloS one*, 14 (11):e0225092, 2019.

[84] Hao Xu, Luqi Wang, Yichen Zhang, Kejie Qiu, and Shaojie Shen. Decentralized visual-inertial-uwb fusion for relative state estimation of aerial swarm. In *2020 IEEE International Conference on Robotics and Automation (ICRA)*, pages 8776–8782. IEEE, 2020.

[85] Pengfei Zhang, Le Yang, Gao Chen, and Gang Li. Classification of drones based on micro-doppler signatures with dual-band radar sensors. In *2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL)*, pages 638–643, 2017. doi: 10.1109/PIERS-FALL.2017.8293214.

[86] Renyuan Zhang and Siyang Cao. Real-time human motion behavior detection via cnn using mmwave radar. *IEEE Sensors Letters*, 3(2):1–4, 2019. doi: 10.1109/LSENS.2018.2889060.

[87] Xian-Da Zhang, Yu Shi, and Zheng Bao. A new feature vector using selected bispectra for signal classification with application in radar target recognition. *IEEE Transactions on Signal Processing*, 49(9): 1875–1885, 2001. doi: 10.1109/78.942617.

[88] Chengwei Zhou, Yujie Gu, Shibo He, and Zhiguo Shi. A robust and efficient algorithm for coprime array adaptive beamforming. *IEEE Transactions on Vehicular Technology*, 67(2):1099–1112, 2017.

[89] A. Zyweck and R.E. Bogner. Radar target recognition using range profiles. In *Proceedings of ICASSP '94. IEEE International Conference on Acoustics, Speech and Signal Processing*, volume ii, pages II/373–II/376 vol.2, 1994. doi: 10.1109/ICASSP.1994.389643.