Article

Research Trends in Collaborative Drones

Michel Barbeau [1,†] [ID]**, Joaquin Garcia-Alfaro** [2,*] [ID] **and Evangelos Kranakis** [1,†] [ID]

1. School of Computer Science, Carleton University, Ottawa, ON K1S 5B6, Canada; barbeau@scs.carleton.ca (M.B.); kranakis@scs.carleton.ca (E.K.)
2. Télécom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France
*   Correspondence: jgalfaro@ieee.org; Tel.: +33-160-76-47-22
†   All authors contributed equally to this work.

Abstract: The last decade has seen an explosion of interest in drones—introducing new networking technologies, such as 5G wireless connectivity and cloud computing. The resulting advancements in communication capabilities are already expanding the ubiquitous role of drones as primary solution enablers, from search and rescue missions to information gathering and parcel delivery. Their numerous applications encompass all aspects of everyday life. Our focus is on networked and collaborative drones. The available research literature on this topic is vast. No single survey article could do justice to all critical issues. Our goal in this article is not to cover everything and include everybody but rather to offer a personal perspective on a few selected research topics that might lead to fruitful future investigations that could play an essential role in developing drone technologies. The topics we address include distributed computing with drones for the management of anonymity, countering threats posed by drones, target recognition, navigation under uncertainty, risk avoidance, and cellular technologies. Our approach is selective. Every topic includes an explanation of the problem, a discussion of a potential research methodology, and ideas for future research.

Keywords: drone; distributed computing; countering drone threats; target recognition; navigation; risk avoidance; cellular technologies; management of anonymity

1. Introduction

Drones have already demonstrated their potential. Their agility allows them to navigate and accomplish tasks in various indoor and outdoor environments. Application examples are the shipping and delivery of essential supplies to remote locations, safe contactless delivery or information gathering for disaster management, geographic mapping of inaccessible terrains, aid in thermal scanning for search and rescue operations, aid farmers for precision land monitoring, law enforcement and border control surveillance, storm tracking, forecasting hurricanes and tornadoes, military surveillance, parcel delivery, and sewer inspection [1–7].

Drone research is well established [8,9]. Key research areas include drone dynamics, navigation, path planning, and formation control. In this article, rather than cover everything, we offer a personal perspective on a few selected research topics that we envision might lead to fruitful future investigations. Each of the topics that we cover will play an essential role in developing future drone technologies. For every subject, we describe the main challenges, discuss potential approaches and methodology, and develop ideas for further research. More specifically, we explore the six specific problems listed in the sequel.

The first problem deals with collaborative drone applications, in which we assume services that are delegated to cloud services. We provide a representative scenario of distributed computing for the generation, management, and distribution of pseudonyms. The second problem relates to the issue of countering drone threats. Indeed, drones are a perfect example of dual-use technology. They can be used for beneficial as well as malicious purposes. While the adoption of drones simplifies unauthorized video and

photo recordings of protected areas, it can also lead to the release of dangerous materials in the proximity of critical infrastructures. Examples include attacks carried out in military missions and flying drones in proximity to airport areas. According to [10], only in 2017, there were more than 300 reported incidents involving small drones. Similar issues are even more popular in the public media [11]. While specific drone applications have countless benefits, others may be a real threat to safety and security. There is a need to develop a science for countering drone threats.

The following three problems we address relate to specific algorithms for collaborative drone applications. First, we explore algorithms for target recognition from the air at a certain altitude. We establish the foundations of a probabilistic framework. Ideas for future work building on this framework are discussed. Second, we establish foundations for drone navigation in GPS-denied environments in the face of decision-making uncertainties. We discuss how these foundations can lead to future research. We complement the previous approach by exploring a formal framework for risk avoidance by flying drones. Within this framework, we introduce ideas for further investigation.

The final problem that we address relates to cellular technologies in networked collaborative drone applications. While early generations of drones required line-of-sight communications with a ground station to maintain control and push data, such as a video stream, the latest drone generations may benefit from the use of Beyond Visual Line of Sight (BVLOS). BVLOS lifts the pilot-drone line-of-sight constraint [12]. It expands the range of operation of drones and types of applications considerably. However, for safe operation, BVLOS requires reliable and real-time command and control. Connections may also serve other purposes, such as data communication and collaboration between drones. Various questions deserve attention, such as the use of cellular technology to network drones, making drones integral parts of the network infrastructure, such as base station-drone or relay, drones pushing information to the cloud, such as location-related signal strength data, or drones pulling information from the cloud, such as flight awareness data. Networking elevates drones' capabilities to another level.

The outline of this article is as follows. The management of anonymity in the context of distributed computing is explored in Section 2. Countering drone threats is investigated in Section 3. Target recognition, navigation under uncertainty, and risk avoidance problems are covered in Sections 4–6. Trends on networked drones using cellular technologies are discussed in detail in Section 7. Section 8 concludes the paper.

2. Distributed Computing with Drones

We start with collaborative drone applications in which services are delegated to edge nodes connected to cloud services. This aims at addressing situations in which cooperative drones may not have enough computational resources. They outsource part of their workload to remote resources using the distributed computing paradigm. We provide as a representative scenario the use of cloud services for the generation, management, and distribution of pseudonyms. The use case can be easily adapted to address other similar distributed computing problems.

2.1. Problem Description

Network operators may require that drones broadcast messages announcing their identity and location while executing a given mission. Reasons can include identifying and isolating faulty drones, e.g., drones misbehaving due to failures or errors. Privacy issues deriving from the broadcast of unprotected identifiers on a wireless channel have been extensively reported in the literature. This calls for the use of the distributed computing paradigm to delegate the management of pseudonyms while guaranteeing anonymity [13]. Similar privacy-preserving authentication frameworks for Internet-connected vehicles have been proposed. Trends suggest that networked drones may interact with cloud services to generate, distribute, and report results. In such scenarios, edge cloud nodes connected to the cloud service and within the wireless range of collaborative drones

assure the mapping of pseudonyms to real identities. These nodes also correlate the collected information and communicate to the cooperative drones new findings, e.g., lists of misbehaving faulty drones.

2.2. Approach and Methodology

As a representative example, we indicate how cloud services can be used to handle the anonymous reporting of faulty drones combining outsourced cloud services with machine-to-machine (short range) communications. Figure 1 offers a centralized approach to generating and broadcasting lists of ephemeral identifiers (e.g., pseudonymous tokens) to collaborative drones using cloud services associated with 5G communications. Later, the drones would exchange those identifiers with other drones hovering nearby, e.g., using machine-to-machine contacts, to report drones showing faulty behavior. The use of either edge or cloud services is assumed for both handling the generation and distribution of ephemeral identifiers as well as to help local drones to report faulty drones to other swarms of collaborative drones.
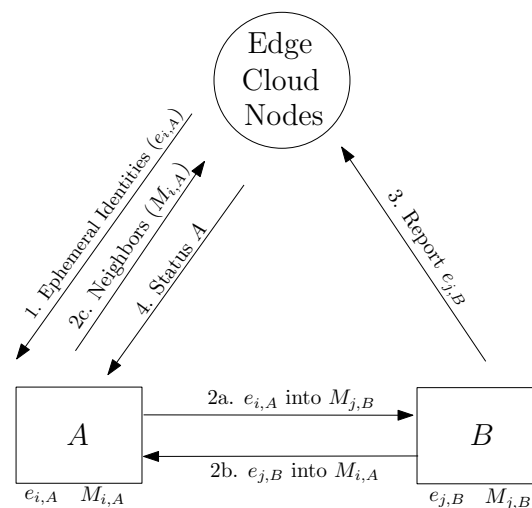

Figure 1. Use of edge cloud nodes to report faulty drones using (anonymous) ephemeral identifiers. Step 1 represents the broadcasting of ephemeral identities to drones *A* and *B*. In steps 2a and 2b, the drone *A*'s data are stored in the memory of drone *B*. In Step 3, drone *B* reports a malfunction to the central service. In Step 4, the central service updates the neighboring drones (e.g., drone *A*, for instance).

Step 1 in Figure 1 represents an operation in which a cloud service is broadcasting an ephemeral identity $e_{i,A}$ to drone *A*. This ephemeral identity becomes associated to drone *A* at time *i*. We assume that the cloud service has also generated and broadcasted an ephemeral identity, i.e., $e_{j,B}$ for drone *B* at time *j*.

Notice that the ephemeral identities are time-sensitive. Regularly, they expire, and drones need to request the cloud service to generate and broadcast their new identities to them. We also assume that drones *A* and *B* move around a given terrain in which 5G communications are possible to connect and use those cloud services required to create and distribute new ephemeral identities.

Drones in this scenario are expected to periodically receive and store the ephemeral identities of nearby drones in their local memories. Each drone is expected to receive the identity of other drones via machine-to-machine communications, e.g., using short-range communications such as Bluetooth or IEEE 802.11.

Step 2a in Figure 1 represents an operation in which drone *B* stores the ephemeral identity of drone *A* at time *i* in its local memory. $M_{j,B}$ represents the action of storing those ephemeral identities received by user *B* at time *j*. Similarly, Step 2b represents drone *A* storing the ephemeral identity of drone *B* at time *i* into its local memory. Action $M_{i,A}$ represents the action of storing those ephemeral identities received by drone *A* at time *i*.

Periodically, drones report to a central cloud service the lists of ephemeral identities they received via machine-to-machine communications, which they temporarily stored in their local memories. This is represented in Step 2c of Figure 1, in which drone A shares the list $M_{i,A}$ with the central server.

Now, let us assume that drone B is reported as faulty at time j to get blacklisted in the swarm. This situation is depicted in Figure 1 as Step 3, i.e., reporting the ephemeral identity of drone B at time j to the central server. The central server that holds all the information collected by all the drones can now warn other drones in the same swarm or other swarms in proximity to drone B. This is depicted in Figure 1 as Step 4. The central cloud service sends a new status to drone A, since this drone may be affected by the faulty behavior reported for drone B.

2.3. Future Research

The presented approach requires a dedicated infrastructure, which may not be possible in all drone scenarios and applications. For instance, cloud services and edge nodes to assure the mapping of pseudonyms to real identities may not fit amateur drone applications, i.e., mini-quadcopter drones without an Internet connection. Similar issues have been reported in the anonymity literature related to, e.g., Vehicular Ad-hoc Networks (VANET)s [14]).

In such VANET scenarios, privacy-preserving strategies leverage mix-network ideas that could also be implemented in collaborative drone applications. The use of group schemes [15,16] can be complemented with the help of privacy zones, in which entry and exit from a zone can force the update of pseudonyms. The approach can also be extended to crowd area scenarios [17], in which swap pseudonym strategies [18] and obfuscation techniques can help increase the level of anonymity between groups of drones. The main limitation of those approaches is the necessity of dedicated infrastructure and human-operator assistance.

We envision machine-to-machine communication solutions without the necessity of deploying a cloud infrastructure to access edge computing services. Such future trends can benefit from alternative schemes considered in avionic and maritime contexts. For instance, the authors in [19] propose secure pseudonym schemes for aircraft in which dedicated entities, referred to as trusted registration authorities, oversee assisting aircraft to generate pseudonyms that are evolving. The generation process guarantees irreversible procedures with respect to tracing back a pseudonym to its real identity. Continuous interaction with the operators associated with the trusted authorities may be an important limitation for drone applications. Moreover, data exfiltration from such trusted authorities may reveal the correspondence between pseudonyms and real identities. Future trends can also be inspired by applications in the maritime domain, in which pseudonym strategies have been enforced over marine vessels via traditionally trusted authorities [20]. The main difference is using an infrastructure-free approach, although a persistent connection to the registration authority is still required. Methods such as those proposed in [21] for the secure and anonymous broadcast of identifiers assume a secure communication channel among mobile vehicles.

Inspired by the previous ideas, we envision some alternative methodologies to conduct the anonymous collection and dissemination of information reported in this section, but limiting as much as possible the dependence of drones to cloud infrastructure services as those referred to in Figure 1. A decentralized version of the previous approach is depicted in Figure 2. In this new approach, drones create the list of ephemeral identities by themselves. This way, now both drones A and B manage their lists of ephemeral identities, broadcasting and expiring them at regular time intervals. When drones such as B are reported as faulty, they can be sensed and reported to other drones in the neighborhood by using the list of ephemeral identities previously exchanged when they were still behaving correctly.
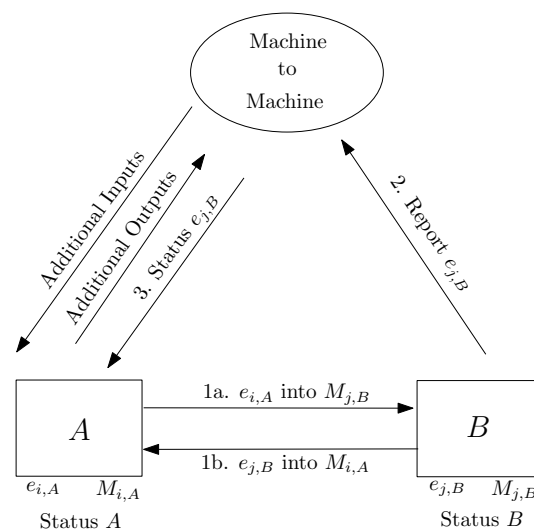
Figure 2. Distributed architecture to report faulty drones using anonymous ephemeral identifiers. In contrast to the approach depicted in Figure 1, drones exchange lists of ephemeral identities and locally update their status without the necessity of central intermediary services. The main differences with respect to the centralized version are in Steps 2 and 3, which are conducted now in a machine-to-machine mode.

In contrast to the approach illustrated in Figure 1, drones can now request and obtain lists of ephemeral identities and locally check whether or not their neighbors are potentially faulty. Remote cloud and edge services can be used as a redundant resource to store, forward, and broadcast lists of potentially defective drones identified by their ephemeral identities. In some mission-specific applications, a delegation of distributed processing to edge nodes and cloud services leads to assumptions and issues, which are not always possible to solve—for example, in situations where the deployment of dedicated infrastructure and centralization is not possible. At the same time, the use of distributed computing with collaborative drones may lead to more complex scenarios when managing, e.g., fault diagnosis, which is a promising future research field in collaborative drone scenarios with well-established foundations from cooperative multi-agent systems [22,23]. We consider that further work remains to address such additional scenarios.

3. Countering Drone Threats

Drones can be used in illicit activities. Several cases have been documented lately. In Saudi Arabia, terrorists used drones to attack oil pumping stations [24]. A Turkish company has developed an autonomous suicide drone [25]. Drones flying close to airports, business centers, and elsewhere in densely populated areas pose a direct danger to critical infrastructure and humans. There are numerous incidents involving rogue drones violating airspace. Drones have also been used to smuggle drugs into the walls of jails [10]. These incidents call for technology to protect infrastructures and populations from harmful activities perpetrated leveraging drones.

3.1. Problem Description

The problem is threefold:

1. *Spotting and Following.* When do drones enter a given airspace? Are they friends or adversaries? What tasks are drones specially fitted for? Are they armed? Loaded? What is their kind? How many rotors do they have? Are they small? Micro? Are they equipped with infrared cameras? Are drones autonomous or under the command and control of a human pilot? What are the whereabouts of spotted drones?
2. *Intention determination.* What is the drones' mission? Are they looking around infrastructures? Searching? Are they preparing for a strike? What is their target? Are they

taking pictures? Shooting videos? What strategies or algorithms are they following to achieve their mission?

3. *Riposte.* How to respond to the presence of adversarial drones? What are the effective countermeasures?

The swarm dimension, drones acting in a collaborative group to achieve their goal, and the increasing degree of elaborateness of drones compound the problem. The environmental conditions are also challenging, since drones are equipped with sensors of various types and have onboard computing resources that enable embedding advanced algorithms and artificial intelligence, rendering them reactive and adaptable.

3.2. Approach and Methodology

The sub-problems can be approached either passively or actively. Table 1 lists the countering drone threat tasks together with various ideas that exist and sometimes have been investigated in the research community. Conventional radar technology is not practical for spotting and following drones, especially for micro-drones flying at slow speed and low altitudes and for areas such as urban environments. Luckily, spotting and following can be achieved passively using audio, video, and radio frequency observations [26–28]. The use of artificial intelligence and Machine Learning (ML) for solving problems related to countering drone threats has grown considerably. Agents learn and exploit what they have learned to spot and follow drones. Al-Sa et al. have created a Data Base (DB) of drone Radio Frequency (RF) signals. Together with the use of neural networks, the database can be used to detect drone presence, their type, and kind of flight [29]. Wit et al. use micro-Doppler signatures for drone rotary-wing determination, i.e., helicopter, bi-rotor, quadcopter, hexacopter, or octocopter [30]. Research has also been completed to determine the load carried by a drone. Using micro-Doppler signatures, Fioranelli developed an approach to determine whether a drone carries a load or not [31]. Traboulsi and Barbeau further investigated this question and developed a method to determine the weight of the payload of a drone [32]. Schumann et al. [33] use deep learning to build classifiers to discriminate drones from birds. The approaches considered have limited success due to the weaknesses of the classifiers to adversarial learning attacks, as demonstrated by Shamir et al. [34] and Eykholt et al. [35].

Table 1. Tackling the countering drone threats. The first column lists the tasks. The second column provides passive solutions based solely on observations. The third column indicates active solutions, acting on threatening drone behavior.

	Passive	**Active**
Spotting and following	Audio, video and RF observations and ML RF signal DB Micro-Doppler signatures	Autonomy rev. Turing test
Intention determination	Maneuvers recognition w. RL Formation prediction w. SL	
Riposte		RF jamming Counterattack drones

On the intention determination front, drone maneuvers recognition has also been investigated, such as the work of Bartak and Vemlelova using Reinforcement Learning (RL) [36]. Using telemetry data, a Supervised Learning (SL) model to predict the formation of a drone swarm aims has been proposed by Traboulsi and Barbeau [37].

Ideas for riposte in response to detecting malicious drone behavior have been quite limited. Attempts to jam the signals of autonomous drones may not be applicable. Shooting flying drones may have their risk.

3.3. Future Research

In summary, attention has been given mainly to drone spotting and following. Intention determination and riposte have received little if any attention. More research is needed on all aspects of countering drone threats. Table 1 highlights the lack or absence of solutions to several sub-problems related to the countering of drone threats.

4. Target Recognition

In this section, we focus on ways to recognize physical targets using one or more drones, possibly either cloud connected or wirelessly with each other, and which are traveling at a certain speed either away from or toward a (moving) target.

4.1. Problem Description

Drones are being used to explore terrestrial regions to discover specific or sought after features and characteristics, such as carrying out human or animal counts, diagnosing specific environmental situations, recognizing a given landmark or sign, or searching for a particular mammal, cf. [38,39]. Additional technical studies also include [40–42].

Tasks with low bandwidth requirements can be performed offline by participating ground stations interacting with drones using a cellular network. However, appropriate network bandwidth may not be available. It is more likely that a drone (or swarm of drones) would need to explore the environment, interpret the data collected, and make decisions based on its own online diagnosis. In this section, we ask the question:

How can we accurately detect a (possibly) mobile target from a distance?

We consider only altitude-based detection (see [43–46]). Considerations could also be extended to speed-based detection (e.g., speed of data sampling) or a combination of altitude and speed.

4.2. Approach and Methodology

Consider a drone flying over a certain highway represented as a line segment L of length $\ell = |L|$. During the flight, the drone retains a given altitude x. The speed $v(x)$ of the drone may be decided by prevailing regulations on the drone's flying territory and is a function of x (see Figure 3, left picture).
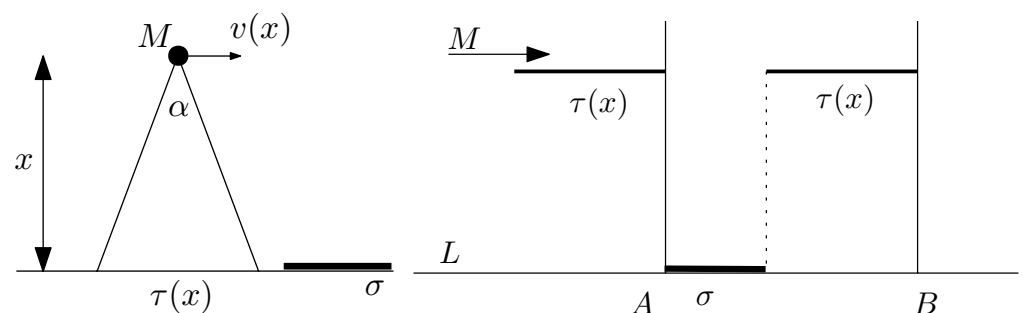

Figure 3. Drone M is flying over a line segment L of length ℓ and a certain object of length σ. At height x, the drone flies with speed $v(x)$ which depends on the altitude x. The picture in the righthand side indicates that the drone's camera has a sliding window effect of width $\tau(x)$ within which it can detect an object of length σ.

The drone's camera has a field of view (or visibility angle) α. When flying at height x, the drone's visibility angle α subtends a subsegment of the line of length $\tau(x)$; this is the portion of the line ℓ on which the drone's camera can detect objects. Since the field of view of the camera is α and the drone is flying at altitude x, we must have that $\tau(x) = 2x \tan(\alpha/2)$ degrees.

First, we determine the target object density as a fraction of the total length ℓ of the segment L. As the drone is moving, it is detecting objects located on the line segment.

The drone's camera at altitude x has a sliding window of width $\tau(x)$. This is moving with speed $v(x)$, thus yielding a time of possible observation equal to $\tau(x)/v(x)$.

The following analysis is inspired from [38,40]. An object of length σ is placed on the line L. As indicated in Figure 3 (right picture), assuming it is moving left to right, the drone starts observing the object at its leftmost endpoint A. It stops observing when at the point B, thus yielding a total distance of observation equal to $\sigma + \tau(x)$. The total duration of observation is equal to $\frac{\sigma+\tau(x)}{v(x)}$. It follows that the drone is observing the target object a fraction $f(x)$, where

$$f(x) = \frac{(\sigma + \tau(x))/v(x)}{(\ell - \tau(x))/v(x)} = \frac{\sigma + \tau(x)}{\ell - \tau(x)}, \tag{1}$$

of its total flying time over the segment of length ℓ, assuming that the rightmost point of the target object is at a distance at most $\tau(x)$ from the rightmost point of the segment of length ℓ. In a way, the righthand side of Equation (1) represents the target object density.

Next, we look at distributions for the probability that the object is detected by the drone. Using distance sampling statistics, one could use the exponential distribution

$$p(x) = \frac{1}{\ln(1 + 1/k)} \cdot \frac{e^{-x}}{k + e^{-x}}, \tag{2}$$

as the probability that a drone flying at altitude $x \geq 0$ detects the target object when its camera is directed toward it.

The parameter k appearing in Equation (2) is chosen so as to indicate the probability that an autonomous ground vehicle detects the target when traveling at ground level (altitude $x = 0$), e.g., $p(0) = \frac{1}{k\ln(1+1/k)}$. The term $\frac{1}{\ln(1+1/k)}$ is the normalizing coefficient and is derived as follows. Observe that $\int \frac{e^{-x}}{e^{-x}+k}dx = x - \ln(ke^x + 1)$ and for $x \geq 0$, this yields the formula

$$\int_0^\infty \frac{e^{-x}}{e^{-x} + k}dx = \ln\left(1 + \frac{1}{k}\right)$$

Note that the (exponential) probability distribution above is one of several potential choices; others may be considered depending on the situation.

Using the target object density calculations in the previous subsection, we conclude that the probability $P_\sigma(x)$ that the drone detects a target object of length σ is equal to

$$P_\sigma(x) := p(x) \cdot f(x) = \frac{1}{\ln(1 + k)} \cdot \frac{e^{-x}}{k + e^{-x}} \cdot \frac{\sigma + \tau(x)}{\ell - \tau(x)},$$

where $f(x)$ is the fraction of its total flying time that the drone will be observing a fixed object of length σ over the segment of length ℓ.

4.3. Future Research

There are several directions for additional research. In case of a searching swarm consisting of n drones acting independently of each other, the probability that the target object is detected by at least one of the drones is easily seen to be equal to $1 - (1 - P_\sigma(x))^n$. One could also consider more general settings by employing $p(v, h)$ as the error probability of image interpretation, namely the probability that the image is interpreted wrongly given that the drone is moving with speed v and is at altitude h from the target. It should be noted that a similar analysis could be applied if the object itself is mobile. Moreover, one could also explore machine learning techniques to improve target recognition for swarms of cooperating drones.

5. Navigating under Uncertainty

This section considers drone navigation under conditions that may cause decision uncertainty in path selection. These may affect the signal's quality as received or processed by the drone. To this end, we take into account recognition and advice errors.

5.1. Problem Description

When drones are navigating an unknown environment, they may have to find a flight path from a source to a destination in a GPS-denied environment using only clues obtained from landmarks visited. In particular, when hovering over an area, they can acquire data through their camera(s) and other sensors, which may be visual, acoustic, etc. Data collected are being used to interpret landmarks. A priori, drones may be given clues and specific characteristics about landmarks that they can use throughout their route discovery. For example, they may be seeking a green door or a tall building. Our main question here is the following:

> How can drones navigate through an environment of landmarks without using GPS information?

5.2. Approach and Methodology

In the sequel, we outline a technique notivated from the work of [47] and first employed in [48,49] in order to navigate such a terrain.

Consider a terrain with available landmarks, e.g., road signs, monuments, or even other terrestrial indicators. The landmarks encountered may provide information whose interpretation by the drone may be prone to various types of errors. One can distinguish two types of errors, namely, recognition and advice.

- Recognition errors may be due to misinterpretation of sensed data or confusion of objects. For example, a drone has found a green door which in fact is not a door but rather a window leading to an incorrectly recognized object. We assume that for some real number $p \in [0, 1]$, the value p is the probability that a drone performs recognition erroneously and $1 - p$ that it is correct.
- Advice errors could be about landmarks because the information they provide is either not up to date or even outright wrong. For example, upon finding a landmark, a drone is advised to traverse a certain distance within the terrain in direction north where it will find the next landmark, say a restaurant, but this information is wrong because the restaurant is no longer there. Again, we may assume that for some real number $q \in [0, 1]$, the value q is the probability that the advice provided to a drone about a landmark is erroneously interpreted and $1 - q$ that it is correctly interpreted.

The next step concerns mathematical assumptions of the model above. To facilitate calculations, one may assume that recognition errors are independent and identically distributed and advice errors are also independent and identically distributed. In other words, the drones are acting independently of each other. In addition, the outcome of the recognition process is random with a probability of success that depends on the parameter p. A similar observation applies to the advice process. We can use this methodology to our advantage so as to improve the recognition and advice mechanisms for swarms of drones.

There is an underlying graph determined by the terrain of landmarks. Landmarks are vertices of a graph $G = (V, E)$ whose edges are discovered online by the recognition and/or advice process. In a typical setting, we start with a source node s and end with a target node t. The drones are seeking a flight path connecting $m + 1$ vertices $s := v_0, v_1, \ldots, v_i, v_{i+1}, \ldots, v_m := t$, see Figure 4.
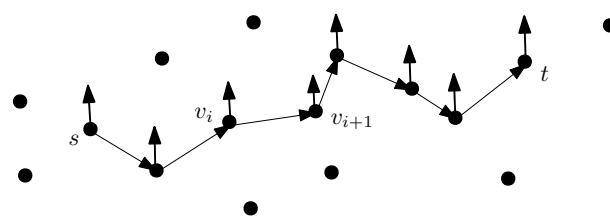

Figure 4. Flight path from source s to destination t. Edge (v_i, v_{i+1}) is an intermediate segment connecting landmarks v_i and v_{i+1}. The vertical (thicker) arrows represent the landmarks encountered by the drones.

A possible flight path, denoted as P, consists of a number of vertices $v_0 := s, v_1, \ldots, v_i,$ $v_{i+1}, \ldots, v_m := t$ from s to t. An edge $\{v_i, v_{i+1}\}$ corresponds to a segment of the flight path P. It is said to be correctly traversed if and only if the advice provided about the landmark associated with vertex v_i is valid and correctly interpreted and the landmark associated with vertex v_{i+1} is correctly recognized. For $i = 0, \ldots, m - 1$, the flight path P is correctly traversed if and only if each of its segments defined by edges $\{v_i, v_{i+1}\}$ are correctly traversed.

At the start, a drone is given a flight plan. The flight plan defines the flight path P. For each vertex v_i, $i = 0, \ldots, m - 1$, the flight plan comprises advice for searching for the next landmark, such as directional data. For each vertex v_{i+1}, the flight plan contains recognition data, such as landmark characteristics. A flight plan is correctly performed solely if every single segment is correctly traversed.

The next important step is for the swarm of drones to fuse information collected so to reach an optimal decision. The basic method is to employ error amplification. Namely, we amplify errors by employing the majority rule and using statistical sampling in order to make decisions on how to navigate the environment (e.g., choose a direction along the ones recommended, accept a certain advice but discard others, and in general improve recognition, etc). Thus, at each landmark being explored, the drones first collect information and make individual decisions on how to interpret the information. Second, they exchange their individual interpretations and decide based on the majority rule by communicating the common decision. Additional details of this can be found in [48,49]. Such an approach turns out to be useful and may lead to improved navigation that may supplement existing navigation techniques.

5.3. Future Research

The methodology proposed offers potential for additional research and testing more sophisticated majority strategies based on probability distributions that are realistic in that they are sensitive, for example to geographic location, proximity to base station, and/or landmarks and available energy of drones. Additionally, one could make use of a database (DB) of landmarks and employ machine learning approaches on drone swarms that could improve the overall decision-making process. For example, contextual bandits could be a natural framework for routing and decision making in such a terrestrial environment, cf. [50] for further details.

6. Risk and Obstacle Avoidance

This section considers approaches to risk and obstacle avoidance when drones are traveling through a possibly unknown environment. The drones themselves may be equipped with sensors to analyze collected data locally or in the cloud.

6.1. Problem Description

When a drone is traversing a given terrain, it is exposed to risks arising from the spatial density of a particular factor being taken into account, e.g., concentration of chemicals, disturbing weather phenomena and/or patterns, environmental pollution, population density, and even the viral load (for a given virus) in a constrained space. Our main question is the following:

> How can a drone navigate a risky terrain so as to minimize the impact of hazardous factors?

6.2. Approach and Methodology

There are many ways to measure the risk when a given region is traversed by the drone. For example, when the source of the risk is not known, it could be measured by the length of the portion of the path traversed by the drone that is inside the given region (see Figure 5), which we also refer to as the exposure. In general, the hazardous region will be enclosed by the perimeter of a complicated domain (represented as oval in Figure 5).

However, if the source of the risk is also known (something we refer to as hotspot), then sometimes, it may be possible to measure the risk from either the distance from the hotspot or an area covered by the drone during the traversal (e.g., see Figure 6.) This is of course an idealized scenario, but it can be useful for making computational estimates on the complexity of the problem.
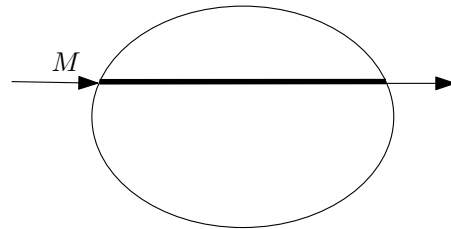

Figure 5. A drone M is traversing a straight line trajectory. Its exposure during the trajectory may be measured by the length of the path inside the risky region.

More generally, consider regions in the plane representing risky areas, which were initiated from various sources (which may or may not be known) of pollution, viral infection, population density, etc. As depicted in Figure 6, a drone M is traversing a straight-line trajectory in a given terrain. The goal of the drone is to navigate the terrain so as to find a path that minimizes its risk of exposure. In many instances, one might be able to measure this quantity precisely.
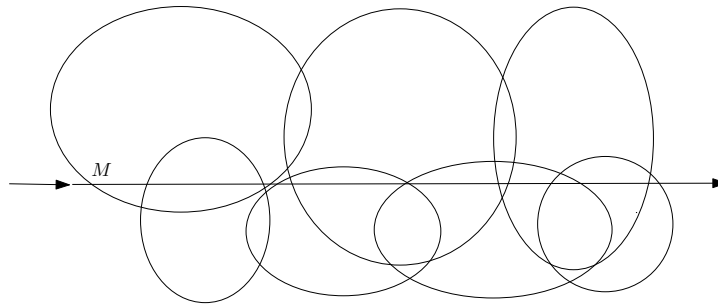

Figure 6. A drone M is traversing a straight lime trajectory. Its exposure during the trajectory is measured by the sum of the exposures from each of the regions (depicted as ovals) within its range.

Measurements can be done in various ways. For example, associated to each region, the authors of [51] consider only disks which are generated by hotspots located at the respective centers of the disks. The critical parameter is a distance $r > 0$ that represents how far the hotspots can reach. The value of r depends on the hotspot's intensity to cause harm, so that the bigger the r, the higher the degree of harm that the hotspot can cause. Moreover, beyond r, no harm is possible. A drone in proximity to the hotspot may get harmed depending on its distance from it. The amount and intensity of harm depends on the distance between the drone and the hotspot (see [51] for additional details). More specifically, the metric introduced in [51] is defined by the area of the circular sector delimited by the points A, E, B, D; it is easy to see that this satisfies $Area(AEBD) = \arccos\left(\frac{h}{r}\right) \cdot r^2 - h \cdot \sqrt{r^2 - h^2}$ (see Figure 7).
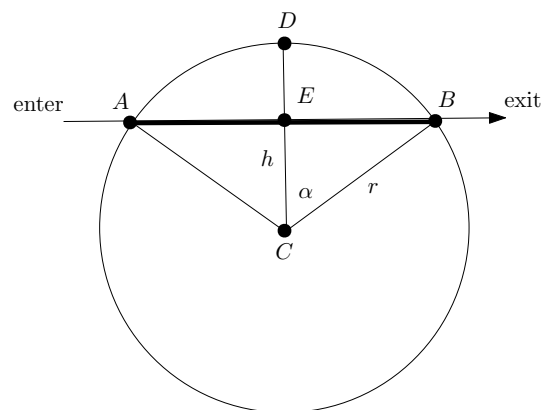
Figure 7. A drone M is traversing a straight line trajectory from A (entrance) to B (exit) at distance h from the point C. Its path inside the circle is depicted by the thick segment AB.

For the metric of harm proposed here, one may consider the length of the portion of the trajectory of the mobile inside the disk. For this metric, we observe the following. Assume a drone is traversing a straight line trajectory at distance h from a hotspot (e.g., an infected station) with critical distance r, where $r \geq h \geq 0$. The total amount $H(r,h)$ of harm that the drone M incurs for its entire trajectory within the hotspot's range is equal to

$$H(r,h) = 2r\sqrt{1 - h^2/r^2} \tag{3}$$

(see Figure 7 where a drone M is traversing a straight lime trajectory at distance h from the source C entering at A and exiting at B). Similar estimates may also be possible to derive for other types of regions. There are various kinds of hotspots, for example, for the case of an infection, the function $H(\cdot, \cdot)$ may be the well-known viral load which is studied in epidemics, but in general, it does not have to be limited to this.

More generally, if a drone traverses a path P consisting of $k + 1$ vertices $u_0, u_1, \ldots, u_k$ with respective sensitivity distances $r_0, r_1, \ldots, r_k$, then the total harm accumulated will be equal to

$$\sum_{i=0}^{k} H(r_i, h_i), \tag{4}$$

where h_i is the distance of the drone from node u_i. The summands in Formula (4) as given by Equation (3) are for all the hotspots encountered. Moreover, a drone may be within more than one region at the same time and hence under the influence of more than one hotspot. More generally, different hotspots may cause different types of harm $H_i(\cdot, \cdot)$, for $i = 0, \ldots, k$. We can develop navigation strategies using this metric that are similar to those developed in [51]. Similar obstacle avoidance navigation algorithms can also be found in [52,53].

6.3. Future Research

In our discussion and analysis, we proposed a simple additive model for measuring the viral load accumulated thus leading to a technique for risk avoidance. Additional metrics for complex regions (e.g., polygonal, etc.) could also be explored using algorithmic and optimization techniques inspired from computational geometry. An interesting question would be to give algorithms to determine (or even prevent taking) a path given that a certain threshold cannot be exceeded. For example, if the critical value of harm is T, one might assume that a harm occurs if

$$\sum_{i=0}^{k} H(r, h_i) \geq T, \tag{5}$$

i.e., the total amount of harm is at least T, a threshold value that may well depend on risk and safety considerations as well as sensitivity of the measuring equipment. The models proposed and studied so far are in 2D space; another important case would be to look at more realistic models in 3D space. It would also be interesting to explore other metrics as well as incorporate techniques from Bandit routing, cf. [50], and study machine learning approaches to improve risk avoidance and maintain a safe routing path.

7. Networked Drones Using Cellular Technologies

The classical pilot-to-drone connection is assured using Visual Line of Sight (VLOS) communications. A direct link is used between a pilot and a drone. The pilot–drone distance is limited by the capability of maintaining eye contact with a drone, such as 500 m. To go far off VLOS, it has been proposed that cellular network infrastructures be used for pilot-to-drone command and control and more. This concept is called BVLOS communications. Pilots maintain communications with drones across arbitrarily long distances over cellular networks. BVLOS enables the piloting of drones outside the line of sight of pilots. Drone traveling distances become limited solely by cellular network coverage. Drones may be guided in complex structures involving buildings, electric poles, and wiring. Because communications are maintained, pilots can always intervene if something goes wrong. Applications of BVLOS include inspection of infrastructures, such as pipelines, and delivery of parcels, food, and medical supplies in urban or rural areas. BVLOS communications are expected to be one of the important applications of upcoming generations of cellular networks. This realization of this concept enables drone applications requiring wide geographical area coverage.

7.1. Problem Description

Research issues that stem from BVLOS include:

1. Low latency connections for drone command-and-control.
2. Interference mitigation due to altitudes of drones.
3. Cooperative drone group communications.

7.2. Approach and Methodology

The BVLOS concept has been explored with 4G cellular networks [12]. The 4G cellular networks made possible multimedia applications such as music and video streaming. The latency of 4G networks, in the order of 50 to 200 ms, does not address the real-time needs for drone command and control, which are in the order of a few milliseconds. Furthermore, 4G cellular networks have been designed for serving ground User Equipment (UE). In contrast, flying drones operate at altitudes. It has been observed that 4G cellular communications of flying drones are prone to high interference levels [12]. The resulting low Signal to Interference Ratio (SINR) values are causing degradation and loss of connectivity [2].

Low network latency is a requirement for safe drone command and control. The 5G networks are aiming at network latency in the order of a few milliseconds. The 5G technology being deployed addresses the needs of drone communications. BVLOS is a use case of 5G networks [54–56]. BVLOS communications require reliable connections between pilots and drones for aspects such as command and control, telemetry and first-person camera video [57,58]. The 5G network BVLOS communications build upon the Ultra Reliable Low Latency Communication (URLLC) use case [59]. It aims at a latency of a few milliseconds. Another goal is reliability, that is, less than a 10^{-5} packet drop rate and less than 10^{-9} bit error rate. Pilots can safely operate drones unhindered within these parameters by network traffic load and latency.

7.3. Future Research

Drone communications are different from traditional cellular communications due to the tight closed-loop requirements of uplink and downlink communications and the mixed traffic types communicated, such as command and control signals, sensor measurements,

and bandwidth-hungry high-definition video and liDAR. Future research should ideally be conducted in the 5G network environment, which aims to overcome the drawbacks of 4G networks concerning the support of drone communications. The 5G networks make drones capable of operating across long non-line-of-sight distances. The wide 5G bandwidth enables more considerable data traffic. The BVLOS concept paves the way for new applications. For example, drones can communicate with each other and ground stations to combine their efforts to achieve a search and rescue mission. The 5G BVLOS communications with drones have their challenges, including propagation channel modeling, 3D trajectory planning, energy-efficient design, and network and radio resource allocation.

An exciting idea is the use of drones to physically carry core network elements [60–65]. They can play the role of relay or Base Station (BS). They can be untethered or tethered. The battery's capacity limits the time of operation of an untethered drone, such as one hour. A tethered drone is powered and linked by a cable. Fly time is not limited by battery capacity. It can last for days. The wired link can provide wider bandwidth than a wireless link. However, being attached to the ground, the range of operation of a drone is limited to a particular zone, typically a truncated hemisphere. Benefits of flying relays or BSs include easy relocation and installation concerning ground relays and BSs. Their lifetime is, of course, limited, especially for untethered BS, which are dependent on the energy reserve of their battery. Research challenges include air-to-ground and air-to-air channel modeling and optimal placement of flying relays or BS. Past research has investigated the quality of ground user connections served by a flying BS and achieving the best possible data rates using machine learning approaches to determine the best location for flying relays.

A challenge in the BVLOS connected drone use cases is ensuring drone connectivity and Quality of Service (QoS) support throughout a drone mission. Ensuring predictable coverage and low communication delays is a non-trivial task due to the phenomenon of scattered cell associations where different altitudes result in varying patterns of received signal power [66]. Classical drone navigation strategies tend to focus on reducing the travel time and energy consumption of drones. However, the optimal navigation path does not likely provide the uplink and downlink QoS requirements of a drone or may unnecessarily consume a large amount of network resources. Minimizing travel time and energy usage while maximizing connectivity and reducing cellular network resources are conflicting requirements that need novel algorithms and approaches to enable widespread connected drone use-case adoption. Another challenge within this domain is drone re-connectivity upon connection disruption. Even with connectivity-aware path planning, a drone may often lose connectivity due to propagation errors or changes in network deployment and increased load. To mitigate this, novel algorithms that can re-route the drone to alternative routes with the required QoS connectivity are needed.

8. Conclusions

Collaborative drones use new networking technologies, such as 5G networks and cloud computing. The goal is to expand traditional applications and their horizon from search and rescue to more ambitious scenarios encompassing new aspects of everyday life. The available research literature on the topic is vast. No single survey article could ever cover all the relevant issues. We have presented a personal collection of research themes covering a few selected areas that we consider worth pursuing in future research. We chose a few research trends on networked, collaborative drones, highlighting target recognition, navigation, risk avoidance, use of cellular technologies, anonymity, and countering drone threats. We introduced each topic by including the problem definition, discussion of a potential research approach, and ideas for future research. Each topic represents just one promising solution w.r.t. the applications domains reported in our work. For example, the use of distributed computing with collaborative drones presents clear advantages for the management of communications in a decentralized manner, for instance, to deal with anonymity issues in situations where the deployment of dedicated infrastructure and centralization is not possible. At the same time, the use of distributed computing

with collaborative drones may lead to more complex scenarios when managing, e.g., fault diagnosis in cooperative tasks. Further work remains to be done to address such issues.

References

1. Clarke, R. Understanding the drone epidemic. *Comput. Law Secur. Rev.* **2014**, *30*, 230–246. [CrossRef]
2. de Amorim, R.M.; Wigard, J.; Kovacs, I.Z.; Sorensen, T.B.; Mogensen, P.E. Enabling cellular communication for aerial vehicles: Providing reliability for future applications. *IEEE Veh. Technol. Mag.* **2020**, *15*, 129–135. [CrossRef]
3. Zhang, J. Occlusion-aware uav path planning for reconnaissance and surveillance in complex environments. In Proceedings of the 2019 IEEE International Conference on Robotics and Biomimetics (ROBIO), Dali, China, 6–8 December 2019; pp. 1435–1440.
4. Guerrero-Sánchez, M.E.; Lozano, R.; Castillo, P.; Hernández-González, O.; García-Beltrán, C.; Valencia-Palomo, G. Nonlinear control strategies for a UAV carrying a load with swing attenuation. *Appl. Math. Model.* **2021**, *91*, 709–722. [CrossRef]
5. Shahmoradi, J.; Talebi, E.; Roghanchi, P.; Hassanalian, M. A comprehensive review of applications of drone technology in the mining industry. *Drones* **2020**, *4*, 34. [CrossRef]
6. Burgués, J.; Marco, S. Environmental chemical sensing using small drones: A review. *Sci. Total Environ.* **2020**, *748*, 141172. [CrossRef]
7. Chmaj, G.; Selvaraj, H. Distributed processing applications for UAV/drones: A survey. In *Progress in Systems Engineering*; Springer: Cham, Switzerland, 2015; pp. 449–454.
8. Popescu, D.; Stoican, F.; Stamatescu, G.; Chenaru, O.; Ichim, L. A survey of collaborative UAV–WSN systems for efficient monitoring. *Sensors* **2019**, *19*, 4690. [CrossRef]
9. Li, X.; Savkin, A.V. Networked Unmanned Aerial Vehicles for Surveillance and Monitoring: A Survey. *Future Internet* **2021**, *13*, 174. [CrossRef]
10. Di Pietro, R.; Raponi, S.; Caprolu, M.; Cresci, S. *New Dimensions of Information Warfare*; Advances in Information Security; Springer International Publishing: Cham, Switzerland, 2020.
11. SeedScientific. Electrifying Drone Statistic; Technical Report. 2021. Available online: https://seedscientific.com/drone-statistics/ (accessed on 19 January 2022).
12. Ivancic, W.D.; Kerczewski, R.J.; Murawski, R.W.; Matheou, K.; Downey, A.N. Flying drones beyond visual line of sight using 4G LTE: Issues and concerns. In Proceedings of the 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 9–11 April 2019; pp. 1–13.
13. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. *J. Inf. Secur. Appl.* **2019**, *48*, 102354. [CrossRef]
14. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. In Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, Montreal, QC, Canada, 10 September 2007; pp. 19–28.
15. Boualouache, A.; Moussaoui, S. S2si: A practical pseudonym changing strategy for location privacy in vanets. In Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 17–19 June 2014; pp. 70–75.
16. Boualouache, A.; Senouci, S.M.; Moussaoui, S. PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 3209–3218. [CrossRef]
17. Benarous, L.; Kadri, B.; Boudjit, S. Alloyed pseudonym change strategy for location privacy in vanets. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6.
18. Li, X.; Zhang, H.; Ren, Y.; Ma, S.; Luo, B.; Weng, J.; Ma, J.; Huang, X. PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs. *IEEE Internet Things J.* **2020**, *7*, 11789–11802. [CrossRef]
19. Asari, A.; Alagheband, M.R.; Bayat, M.; Asaar, M.R. A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. *Comput. Netw.* **2021**, *185*, 107599. [CrossRef]

20. Goudossis, A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *J. Mar. Sci. Technol.* **2019**, *24*, 410–423. [CrossRef]

21. Zamani, M.; Saia, J.; Movahedi, M.; Khoury, J. Towards provably-secure scalable anonymous broadcast. In Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13), Washington, DC, USA, 13 August 2013.

22. Niu, G.; Han, T.; Yang, B.S.; Tan, A.C.C. Multi-agent decision fusion for motor fault diagnosis. *Mech. Syst. Signal Process.* **2007**, *21*, 1285–1299. [CrossRef]

23. Jennings, N. *Cooperation in Industrial Multi-Agent Systems*; World Scientific: Singapore, 1994; Volume 43.

24. Raghavan, S. Saudis say oil pipeline was attacked by drones, possibly from Yemen. *The Washington Post*, May 15, 2019.

25. Zitser, J. A rogue killer drone 'hunted down' a human target without being instructed to, UN report says. *Bus. Insid.* **2021**. Available online: https://www.businessinsider.com/killer-drone-hunted-down-human-target-without-being-told-un-2021-5 (accessed on 19 January 2022).

26. Shi, X.; Yang, C.; Xie, W.; Liang, C.; Shi, Z.; Chen, J. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Commun. Mag.* **2018**, *56*, 68–74. [CrossRef]

27. Shi, L.; Ahmad, I.; He, Y.; Chang, K. Hidden Markov model based drone sound recognition using MFCC technique in practical noisy environments. *J. Commun. Netw.* **2018**, *20*, 509–518. [CrossRef]

28. Anwar, M.Z.; Kaleem, Z.; Jamalipour, A. Machine learning inspired sound-based amateur drone detection for public safety applications. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2526–2534. [CrossRef]

29. Al-Sa'd, M.F.; Al-Ali, A.; Mohamed, A.; Khattab, T.; Erbad, A. RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database. *Future Gener. Comput. Syst.* **2019**, *100*, 86–97. [CrossRef]

30. de Wit, J.M.; Harmanny, R.; Premel-Cabic, G. Micro-Doppler analysis of small UAVs. In Proceedings of the 2012 9th European Radar Conference, Amsterdam, The Netherlands, 31 October–2 November 2012; pp. 210–213.

31. Fioranelli, F.; Ritchie, M.; Griffiths, H.; Borrion, H. Classification of loaded/unloaded micro-drones using multistatic radar. *Electron. Lett.* **2015**, *51*, 1813–1815. [CrossRef]

32. Traboulsi, A.; Barbeau, M. Identification of Drone Payload Using Mel-Frequency Cepstral Coefficients and LSTM Neural Networks. In *Proceedings of the Future Technologies Conference*; Springer: Cham, Switzerland, 2020; pp. 402–412.

33. Schumann, A.; Sommer, L.; Müller, T.; Voth, S. An image processing pipeline for long range UAV detection. In *Emerging Imaging and Sensing Technologies for Security and Defence III; and Unmanned Sensors, Systems, and Countermeasures*; International Society for Optics and Photonics: Bellingham, WA, USA, 2018; Volume 10799, p. 107990T.

34. Shamir, A.; Safran, I.; Ronen, E.; Dunkelman, O. A simple explanation for the existence of adversarial examples with small hamming distance. *arXiv* **2019**, arXiv:1901.10861.

35. Eykholt, K.; Evtimov, I.; Fernandes, E.; Li, B.; Rahmati, A.; Xiao, C.; Prakash, A.; Kohno, T.; Song, D. Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–22 June 2018; pp. 1625–1634.

36. Barták, R.; Vomlelová, M. Using machine learning to identify activities of a flying drone from sensor readings. In Proceedings of the Thirtieth International Flairs Conference, Marco Island, FL, USA, 22–24 May 2017.

37. Traboulsi, A.; Barbeau, M. Recognition of drone formation intentions using supervised machine learning. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 408–411.

38. McLaren, I.A. Methods of determining the numbers and availability of ringed seals in the eastern Canadian Arctic. *Arctic* **1961**, *14*, 162–175. [CrossRef]

39. van Gemert, J.C.; Verschoor, C.R.; Mettes, P.; Epema, K.; Koh, L.P.; Wich, S. Nature conservation drones for automatic localization and counting of animals. In *European Conference on Computer Vision*; Springer: Cham, Switzerland, 2014; pp. 255–270.

40. Laake, J.L.; Calambokidis, J.; Osmek, S.D.; Rugh, D.J. Probability of detecting harbor porpoise from aerial surveys: Estimating g (0). *J. Wildl. Manag.* **1997**, *61*, 63–75. [CrossRef]

41. Hodgson, A.; Kelly, N.; Peel, D. Unmanned aerial vehicles (UAVs) for surveying marine fauna: A dugong case study. *PLoS ONE* **2013**, *8*, e79556. [CrossRef] [PubMed]

42. Chittka, L.; Dyer, A.G.; Bock, F.; Dornhaus, A. Psychophysics: Bees trade off foraging speed for accuracy. *Nature* **2003**, *424*, 388. [CrossRef] [PubMed]

43. Chen, B.; Perona, P. Speed versus accuracy in visual search: Optimal performance and neural architecture. *J. Vis.* **2015**, *15*, 9. [CrossRef]

44. Chen, B.; Perona, P. Speed Versus Accuracy in Visual Search: Optimal Performance and Neural Implementations. In *Computational and Cognitive Neuroscience of Vision*; Springer: Singapore, 2017; pp. 105–140.

45. Ha, I.K.; Cho, Y.Z. A probabilistic target search algorithm based on hierarchical collaboration for improving rapidity of drones. *Sensors* **2018**, *18*, 2535. [CrossRef]

46. Yonas, A.; Pittenger, J. Searching for many targets: An analysis of speed and accuracy. *Percept. Psychophys.* **1973**, *13*, 513–516. [CrossRef]

47. Kranakis, E.; Krizanc, D. Searching with Uncertainty. In Proceedings of the SIROCCO'99, 6th International Colloquium on Structural Information & Communication Complexity, Lacanau-Ocean, France, 1–3 July 1999; pp. 194–203.

48.   Barbeau, M.; Garcia-Alfaro, J.; Kranakis, E. Geocaching-Inspired Navigation for Micro Aerial Vehicles with Fallible Place Recognition. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, Bari, Italy, 19–21 October 2020; Springer: Cham, Switzerland, 2020; pp. 55–70.

49.   Barbeau, M.; Garcia-Alfaro, J.; Kranakis, E.; Santos, F. GPS-Free, Error Tolerant Path Planning for Swarms of Micro Aerial Vehicles with Quality Amplification. *Sensors* **2021**, *21*, 4731. [CrossRef]

50.   Lattimore, T.; Szepesvári, C. *Bandit Algorithms*; Cambridge University Press: Cambridge, UK, 2020.

51.   Barbeau, M.; Garcia-Alfaro, J.; Kranakis, E. Risky Zone Avoidance Strategies for Drones. In Proceedings of the 2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Virtually, 12–17 September 2021; pp. 1–6.

52.   Olfati-Saber, R.; Murray, R.M. Distributed cooperative control of multiple vehicle formations using structural potential functions. *IFAC Proc. Vol.* **2002**, *35*, 495–500. [CrossRef]

53.   Vásárhelyi, G.; Virágh, C.; Somorjai, G.; Nepusz, T.; Eiben, A.E.; Vicsek, T. Optimized flocking of autonomous drones in confined environments. *Sci. Robot.* **2018**, *3*, eaat3536. [CrossRef]

54.   The 3rd Generation Partnership Project (3GPP). 3GPP TR 36.777, Enhanced LTE Support for Aerial Vehicles. 2017. Available online: ftp://www.3gpp.org/specs/archive/36_series/36.777 (accessed on 18 January 2022).

55.   The 3rd Generation Partnership Project (3GPP). UAS-UAV. 2019. Available online: https://www.3gpp.org/uas-uav (accessed on 18 January 2022).

56.   The 3rd Generation Partnership Project (3GPP). Unmanned Aerial System (UAS) Support in 3GPP, Technical Specification (TS). 2020. Available online: https://www.3gpp.org/ftp//Specs/archive/22_series/22.125 (accessed on 18 January 2022).

57.   Ullah, H.; Nair, N.G.; Moore, A.; Nugent, C.; Muschamp, P.; Cuevas, M. 5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases. *IEEE Access* **2019**, *7*, 37251–37268. [CrossRef]

58.   Mozaffari, M.; Kasgari, A.T.Z.; Saad, W.; Bennis, M.; Debbah, M. 3D cellular network architecture with drones for beyond 5G. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.

59.   Bennis, M.; Debbah, M.; Poor, H.V. Ultrareliable and low-latency wireless communication: Tail, risk, and scale. *Proc. IEEE* **2018**, *106*, 1834–1853. [CrossRef]

60.   Kishk, M.; Bader, A.; Alouini, M.S. Aerial base station deployment in 6G cellular networks using tethered drones: The mobility and endurance tradeoff. *IEEE Veh. Technol. Mag.* **2020**, *15*, 103–111. [CrossRef]

61.   Kishk, M.A.; Bader, A.; Alouini, M.S. On the 3-D placement of airborne base stations using tethered UAVs. *IEEE Trans. Commun.* **2020**, *68*, 5202–5215. [CrossRef]

62.   Pourbaba, P.; Ali, S.; Manosha, K.S.; Rajatheva, N. Multi-Armed Bandit Learning for Full-Duplex UAV Relay Positioning for Vehicular Communications. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 188–192.

63.   Fotouhi, A.; Ding, M.; Hassan, M. DroneCells: Improving spectral efficiency using drone-mounted flying base stations. *J. Netw. Comput. Appl.* **2021**, *174*, 102895. [CrossRef]

64.   Fotouhi, A.; Ding, M.; Hassan, M. Flying Drone Base Stations for Macro Hotspots. *IEEE Access* **2018**, *6*, 19530–19539. [CrossRef]

65.   Fotouhi, A.; Ding, M.; Hassan, M. Dynamic base station repositioning to improve spectral efficiency of drone small cells. In Proceedings of the 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Macau, China, 12–15 June 2017; pp. 1–9.

66.   Lin, X.; Wiren, R.; Euler, S.; Sadam, A.; Määttänen, H.L.; Muruganathan, S.; Gao, S.; Wang, Y.P.E.; Kauppi, J.; Zou, Z.; et al. Mobile network-connected drones: Field trials, simulations, and design insights. *IEEE Veh. Technol. Mag.* **2019**, *14*, 115–125. [CrossRef]