

University of Southern Queensland
Faculty of Health, Engineering & Sciences

Drone Swarm Simulation for Tracking High Capability Malicious Drone

A dissertation submitted by

Joshua Carter

In fulfilment of the requirements of

ENG4111/ ENG4112 Research Project

Towards the degree of

Bachelor of Engineering (Honours)
(Electrical and Electronic)

Submitted: October 2021

Abstract

The availability of affordable ready-to-fly consumer, commercial, and industrial drones has exploded over the past ten to fifteen years and in turn so have the sales figures. Unprecedented technological advancements in component and material production have largely been credited with the increased affordability and capabilities of consumer drones. Common out-of-the-box features that are standard on many consumer drones present the opportunity for them to be used maliciously. Malicious use cases are wide and range, for example, from illegal surveillance of individuals, to smuggling of contraband into prisons and across borders. Continued breaches of restricted airspace around sensitive sites such as nuclear power plants and airports are especially concerning. Current mitigation methods are insufficient, often failing to identify the drone or its operator, there is a pressing need to track these malicious drones back to their point of origin, without the use of expensive terrestrially based radar systems. Off-the-shelf drones flown in a swarm have been shown to adequately detect and track a malicious drone. The efficacy of swarm detection can be increased through optimal initial flight formations of the swarm.

This research examined a ‘sunflower’ initial flight formation against benchmark formations identified within the literature; this evaluation was carried out through computer simulation. Two tracking methods were simulated for each formation: reactive tracking and reactive tracking with predictive pre-positioning. Multiple simulations for each formation were undertaken using both tracking methods at a variety of swarm sizes. The top speed of the drone swarm was then varied, and the simulations repeated. As the malicious drone is assumed to be of high capability, swarm top speed never exceeded the assumed malicious drone top speed. The output of the simulation was analysed to determine the optimum configuration that would provide the highest proportion of active tracking of the malicious drone while it was within the tracking area.

The simulation results show that the sunflower initial flight formation outperformed the benchmark formations for every configuration under test. As the swarm size increased to values over 500 drones a point of diminishing returns was observable across the board for all formation and tracking strategy configurations at all swarm speeds. Additionally, the performance of the sunflower formation, when coupled with reactive tracking and a more competitive swarm speed, was demonstrated to outperform the benchmark formations even when they had the perceived advantage of predictive pre-positioning.

University of Southern Queensland
Faculty of Health, Engineering and Sciences
ENG4111/ENG4112 Research Project

Limitations of Use

The Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled “Research Project” is to contribute to the overall education within the student’s chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

**University of Southern Queensland
Faculty of Health, Engineering and Sciences
ENG4111/ENG4112 Research Project**

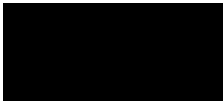
Certification of Dissertation

I certify that the ideas, designs and experimental work, results, analysis, and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Joshua Carter





14/10/2021

Acknowledgements

My partner, Dani, for her unwavering support over the past few years after I made the decision to tackle the degree fulltime. We welcomed our first child Ruben into the world in April and Dani has been instrumental in making sure I could still find the time for my studies and this project.

My supervisor, Dr Jason Brown, for his support throughout and for providing extremely useful and timely advice and feedback.

The University of Southern Queensland, for providing such a flexible online learning environment, I originally commenced this degree at another institution whilst working fulltime and had I not transferred to USQ I doubt I would have completed my studies.

Table of Contents

Abstract.....	i
Limitations of Use.....	ii
Certification of Dissertation.....	iii
Acknowledgements.....	iv
Table of Contents.....	v
List of Figures.....	viii
List of Tables.....	ix
Glossary of Terms.....	x
Chapter 1.....	1
1. Introduction.....	1
1.1 Project Overview.....	1
1.2 Project Aims.....	1
1.3 Project Objectives.....	2
1.4 Dissertation Overview.....	2
Chapter 2.....	4
2. Literature Review.....	4
2.1 History.....	4
2.1.1 Evolution of the Drone Industry.....	4
2.1.2 Civilian Drone Market Growth.....	5
2.2 Malicious Drones.....	7
2.2.1 Potential Threats.....	7
2.2.2 Prevalence of Malicious Use.....	8
2.3 Mitigation.....	10
2.3.1 Legislative and Regulatory Controls.....	10
2.3.2 Object Tracking via Drone Swarms.....	12
2.3.3 Tracking of Malicious Drones via Drone Swarms.....	13

2.3.4 Tracking of High Capability Malicious Drones.....	15
Chapter 3.....	17
3. Simulation Design.....	17
3.1 Simulation Environment	17
3.1.1 MATLAB.....	17
3.2 Simulation Implementation.....	17
3.2.1 Tracking Area and Malicious Drone Flight Path.....	17
3.2.2 Tracking Strategies	18
3.2.3 Implemented Initial Swarm Formations	21
3.2.4 Swarm Drone Movement Algorithm	26
3.3 Unimplemented Initial Swarm Formations.....	28
Chapter 4.....	30
4. Methodology	30
4.1 Methodological Approach.....	30
4.1.1 Assumptions.....	30
4.1.2 Simulation Characteristics and Variables	32
4.2 Methods Of Analysis	34
4.3 Data Collection	38
4.4 Methodology Justification.....	39
Chapter 5.....	40
5. Results and Analysis	40
5.1 Analysis Overview.....	40
5.2 Results At Different Swarm Speeds.....	40
5.2.1 Swarm Speed 20m/s.....	40
5.2.2 Swarm Speed 25m/s.....	42
5.2.3 Swarm Speed 29m/s.....	44
5.3 Results Summary	46
Chapter 6.....	48
6. Conclusions and Further Work	48

6.1 Conclusions.....	48
6.2 Further Work.....	49
References.....	51
Appendix A Project Specification.....	54
Appendix B Project Plan.....	55
Appendix C Project Resources	56
Appendix D Risk Assessment.....	57
Appendix E MATLAB Simulation Code.....	58
Appendix F Unimplemented Formation Codes	63

List of Figures

Figure 1. Timeline of military vs civilian drone applications (Giones & Brem 2017).	5
Figure 2. FAA Consumer Drone Registration Trends (Chavers 2018).	6
Figure 3. Point of Interest Flight Mode (DJI 2015).	7
Figure 4. Drone swarm utilising intermittent RF signals to track target drone (Koochifar et al. 2018). 14	
Figure 5. Malicious drone movement captured from MATLAB simulation animation	18
Figure 6. Reactive tracking of malicious drone (Brown & Raj 2021a).	19
Figure 7. Reactive Tracking + Predictive Pre-Positioning of malicious drone (Brown & Raj 2021a). 20	
Figure 8. Random swarm formation code.....	21
Figure 9. Code for variables related to swarm size.....	22
Figure 10. Circular swarm formation code	23
Figure 11. Sunflower swarm formation code.....	25
Figure 12. Implemented formation examples	26
Figure 13. Surveillance drone optimum bearing example (Brown and Raj 2021a).....	27
Figure 14. Unimplemented lattice formations	29
Figure 15. Circular and sunflower formation swarms shown with varied angular orientations.	34
Figure 16. Simulation configurations for each swarm speed.	35
Figure 17. Results for swarm speed $u = 20\text{m/s}$	41
Figure 18. Results for swarm speed $u = 25\text{m/s}$	43
Figure 19. Results for swarm speed $u = 29\text{m/s}$	45

List of Tables

Table 1: Summary of international regulatory authorities pertaining to drones.	11
Table 2. Maximum speeds of readily available consumer drones	33
Table 3. Summary of simulation specifications and variables.....	38
Table 4. Results of mean of 500 iterations used for plot generation where $u = 20\text{m/s}$	42
Table 5. Results of mean of 500 iterations used for plot generation where $u = 25\text{m/s}$	44
Table 6. Results of mean of 500 iterations used for plot generation where $u = 29\text{m/s}$	46
Table 7. Project Plan.	55
Table 8. Project Resources.....	56

Glossary of Terms

CASA – Civil Aviation Safety Authority

CUAS – Counter Unmanned Aircraft Systems

DJI – DJI Technology

DRN – Dynamic Radar Network

EO – Electro Optical

FAA – Federal Aviation Administration

FPV – First Person View

FRIA – FAA Recognised Identification Area

NAS – National Airspace System

PID – Proportional Integral Differential

PSO – Particle Swarm Optimization

Remote ID – Remote Identification

RePL – Remote Pilot License

RF – Radio Frequency

RPV – Remotely Piloted Vehicle

RSSI – Received Signal Strength Indicator

UAS – Unmanned Aircraft Systems

UAV – Unmanned Air Vehicle

Chapter 1

1. Introduction

1.1 Project Overview

The number of affordable ready-to-fly, consumer, commercial and industrial drones available to purchase has exploded over the last ten to fifteen years, with civilian drone sales figures skyrocketing in turn. Driven by unprecedented technological advancements in component and material production, the capabilities and affordability of consumer drones have increased substantially. Common out-of-the-box features that are standard on many consumer drones present the opportunity for the operator/s to use them nefariously. These features include ‘intelligent flight’ modes, high specification camera equipment, payload carrying capacity and long operational transmission ranges. Malicious drone use has been documented to be on the rise, notably in the United Kingdom, Australia, and the United States. Malicious use ranges from illegal surveillance of individuals, to smuggling of contraband into prisons and across borders, to potentially high-risk breaches of air space around nuclear power plants, airports, and other sensitive and restricted sites. Current malicious drone tracking strategies are expensive and often require the use of a terrestrial radar network. Research into tracking a malicious drone back to its origin using a swarm of surveillance drones has proved promising, even more so when combined with reactive tracking and predictive pre-positioning. Using MATLAB simulations this project sought to analyse and evaluate the effects of several different initial drone swarm formations on swarm tracking performance of a high capability malicious drone. Through repeated simulation with multiple formations and swarm sizes, it then sought to determine a more optimal swarm formation and size to those previously examined.

1.2 Project Aims

The principle aim of the project was to determine by simulation, the optimal drone placement, initial swarm size and formation required to achieve increased performance of tracking of a high capability malicious drone.

It sought to evaluate and determine:

- The effect on tracking performance of multiple different initial swarm formations and sizes.

- How simulation performance data compares with prior research.
- Recommendations regarding the most efficient and high performing swarm formation and size combination.

1.3 Project Objectives

The specific objectives of this project were:

1. Carry out background research on the history and increasing prevalence of consumer drones.
2. Undertake a comprehensive literature review into the potential threats posed by high capability malicious drones and the various tracking methodologies.
3. Develop a surveillance drone swarm simulation environment utilizing MATLAB.
4. Evaluate and compare via simulation a range of potential initial swarm formations.
5. Collate, assess, and compare data from the simulations against performance metric/s.
6. Make recommendations regarding the most efficient and high performing swarm formation, spacing and size configuration.

1.4 Dissertation Overview

Chapter 1 provides a summarised overview, including a clear statement of the broad aims and specific objectives of the project.

Chapter 2 is a literature review on prior research conducted on related topics. Including the evolution of the drone industry, drone market growth, malicious drone's potential threats and prevalence, object tracking, malicious drone tracking, and high capability malicious drone tracking.

Chapter 3 describes the design of the simulation used for the project. It provides details of the software being used for the simulation environment alongside explanations of key algorithms and sections of code.

Chapter 4 describes the methodology, including the data gathered and the method of analysis employed. The specific implementation of the simulation environment is also described.

Chapter 5 provides the simulation results and includes all of the analysis for each simulation configuration, including comments on anticipated and unexpected outcomes.

Chapter 6 contains the conclusions reached after project completion and assesses them against the objectives set out in Chapter 1. Potential further work in the field is suggested and discussed.

Chapter 2

2. Literature Review

2.1 History

2.1.1 Evolution of the Drone Industry

Unmanned air vehicles (UAVs), unmanned aircraft systems (UASs) and remotely piloted vehicles (RPVs) are closely related terms. UAVs usually possess the ability for partial or completely pre-programmed flight in addition to remote control, RPVs on the other hand function more like a standard aircraft but with the pilot and cockpit located remotely in a safe location. In a military application UAVs would carry out surveillance largely without oversight from a pilot, RPVs allow combat missions to be flown by humans whilst removing the risk to the pilot. UAVs and RPVs are both examples of components of a UAS, the term UAS encompasses all system components not just the aircraft, this can include the remote controllers, data links and any other supporting equipment.

UAVs, UASs and RPVs are all commonly known to the general public as drones. The ready-to-fly consumer drones and highly capable commercial/industrial drones available to purchase today are the culmination of a long and technical evolutionary process driven by a number of factors.

One of the key factors driving drone technology throughout history has been its use by militaries around the world, the development of drones for target practice was first noted in the early 1900's. In subsequent years the advantages of utilising unmanned vehicles for military operations became apparent, reconnaissance and surveillance missions and other high-risk activities could now be undertaken without personal risk to flight crew. Further technological developments lead to increased functionality and in turn increased emphasis on drone utilisation for military operations (Giones & Brem 2017).

Sprague and Perritt (2016) concur that the development of civilian drones was partly born out of the extensive coverage of the use of military drones during the 'war on terror', particularly in the conflicts in Kosovo, Iraq, and Afghanistan. The potential of repurposing the military technology in order to serve civilian uses was identified by entrepreneurs and engineers, and they set about achieving this goal. They also identified a second factor driving civilian drone development, model aircraft

hobbyists seeking to generate income by modifying their aircraft with camera equipment and offering their services for real-estate photography, events such as weddings, and other applications.

The subsequent introduction and uptake of civilian drones took place over a far shorter time period than that of military drones.

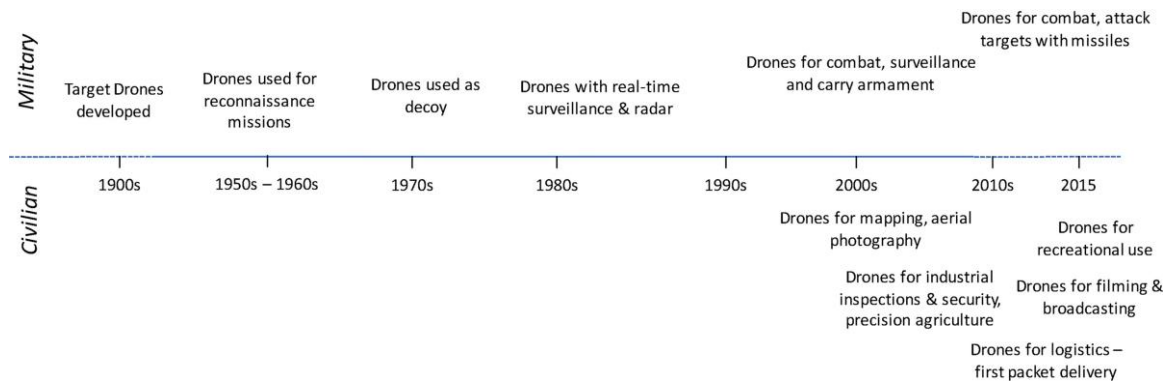


Figure 1. Timeline of military vs civilian drone applications (Giones & Brem 2017).

This accelerated adoption of civilian drone technology was made possible because of the unprecedented advances in many of the technological areas that were relevant to drone component production. Miniaturization of electronic components and imaging equipment, development of lighter state-of-the-art construction materials, and increasingly powerful processors have all contributed to the explosion of the market from the early 2000’s (Sprague & Perritt 2016; Giones & Brem 2017).

2.1.2 Civilian Drone Market Growth

Civilian drone sales were predicted to rise over the ten-year period from 2015 to 2025, from 80,000 units shipped to close to 2.7 million units shipped, representing an almost \$4 billion industry by 2025. The resultant service industries built around the adoption of these drones also stand to generate a predicted \$8.7 billion in 2025, a marked increase from the 2015 figure of \$170 million (Seitz 2015).

The increasing affordability of consumer drones has played a major role in this growth. For example, DJI technology (DJI) is a Chinese based drone manufacturer that in 2017 commanded 75% of the consumer market and in the same year launched a very affordable \$500 (USD) entry level model (Bateman 2017). Consumer drone sales within the United States can be quantified by looking to the Federal Aviation Administration’s (FAA) consumer drone registration numbers, with mandatory registration required from 2016 onwards. In January 2017, the number of registrations totalled 670,000 drones, this dramatically increased to over 770,000 drones by late March of the same year and during 2018 the number of registrations surpassed the 1,000,000 mark. It should be noted that although the FAA mandates registration, not all consumer drones are registered, so the number of registered drones cannot be assumed to account for all consumer drones within the US. In 2018 the FAA estimated that actual drone units were 500,000 higher than the official figure (Chavers 2018).

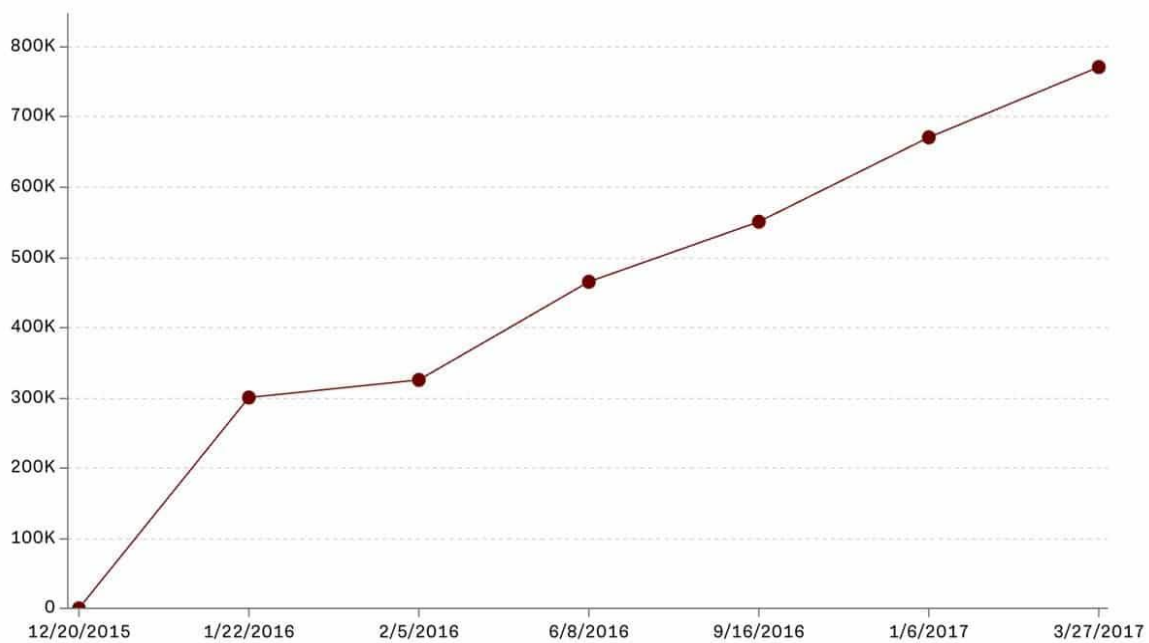


Figure 2. FAA Consumer Drone Registration Trends (Chavers 2018).

With the number of consumer drones within the US alone conservatively predicted to hit 3.55 million units in 2021, regulators and law makers worldwide have a tough task ahead of them in managing the appropriate operation of these increasingly affordable, portable, versatile, and easy to use consumer drones.

2.2 Malicious Drones

2.2.1 Potential Threats

The continuous expansion of commercial and consumer drone markets has led to the growth of a drone ecosystem large in scale and variety. Whilst it is accepted that the capabilities of these drones provide a range of positive and beneficial applications, Jackman (2019) asserts that the consumer drone will inevitably be associated with potential exploitation.

They further identify several developmental trends which present greater potential drone risk should they be utilised maliciously. The introduction of ‘intelligent flight’ modes by leading manufacturers, including DJI and Parrot in 2015 and 2016 respectively, is one of these trends. These flight modes greatly increase the manoeuvrability and capacity of the drones and are marketed as easy to use tools which enable the user to capture ‘expert’ shots and footage. Key ‘intelligent flight’ modes include the use of predetermined waypoints, the ability to track objects, people, or points of interest and either follow or survey them using a holding pattern (DJI 2015).



Figure 3. Point of Interest Flight Mode - Drone Automatically Revolves Around Designated Target (DJI 2015).

These flight modes mirror the capabilities of military drones and are able to track and target specific people, objects, and locations. This capability could be repurposed for malicious means, a ‘target’ could be tracked and surveyed whilst an operator waits for an ideal moment to ‘strike’, alternatively

the surveillance itself could be malicious. ‘Intelligent flight’ modes when coupled with ongoing advancements in obstacle detection and avoidance, and the capability of flight without a GPS signal, have increased the potential for malicious drones to operate in restricted environments whilst identifying and tracking a target. The potential to evade defences is also increased.

Another key developmental trend that lends itself to exploitation for malicious purposes is the increase in ease and amount of multimedia sharing, whether images or video are saved for later use or broadcast live. The potential for the invasion of corporate or personal privacy via drone surveillance is an ongoing issue within the industry, in its worst form surveillance flights over sensitive sites such as military bases or airports could compromise security and provide intelligence for a future physical attack.

Jackman (2019) also identifies the trend amongst enthusiasts and hobbyists to modify drones, these DIY modifications have opened the door to intentional weaponization of recreational consumer drones. Increased payload carrying capacity has created the potential for any item, tool, or weapon to be fitted to a drone and remotely released or operated. There are a wide range of examples ranging from the integration of paintball guns to fully functional firearms and flamethrowers. Modifications are not limited to the hardware side of the drone; software modifications are common among the online community as enthusiasts seek to disable geo-fencing and other software-imposed restrictions like maximum flight altitude in order to experiment with the operational limits of the drone. Ultimately the prevalence of these hardware and software modifications within the community, and the apparent ease with which an ordinary citizen can perform them, represents a significant additional threat for malicious use.

2.2.2 Prevalence of Malicious Use

The use of drones for both nuisance and more sinister activities has been widely documented over the years, including the reported smuggling of contraband into prisons in the United Kingdom, Australia, the United States, and elsewhere. Drones have also been used as part of public demonstrations, for example in April 2015 a payload of radioactive sand was deposited using a drone onto the roof of the Prime Minister’s office in Japan in protest of the governments nuclear policy. Likewise, to protest the German governments surveillance policy a drone was flown within metres of German Chancellor Angela Merkel in September 2013 (Friese et al. 2016).

Security breaches by unauthorised drones at critical infrastructure sites in the United Kingdom have been on the increase, with 37 reported incidents at nuclear power plants in 2014 alone. Similar

breaches also occurred in France during the same year, this is despite the law providing for harsh penalties for flying drones within a 5km exclusion zone around a power plant. In addition to the incidents at power plants within France, in February 2015 there were five occurrences of unauthorised drone flights over sensitive sites in Paris including the presidential palace and the American embassy. A common feature of all of the incidents in France was that, despite efforts to locate the drones in question and identify the operators, authorities were unable to accomplish either (Michaelides-Mateou 2016).

Similar activities have also been prevalent in the United States. In September 2019 a swarm of drones flew over restricted airspace at the Palo Verde Nuclear Power Plant prompting the implementation of new security measures. Despite these additional security measures, the Palo Verde plants airspace was again encroached in December 2019. These airspace infringements were a fraction of the 57 known drone incidents across 24 nuclear sites within the United States between 2015 – 2019. Similar to the incidents in Europe, often the drone and its operator/s are not identified and therefore neither are their intentions, at the time of reading 49 of the 57 incidents (constituting approximately 85% of the breaches) had been listed as ‘Closed Unresolved’ (Hambling 2020).

The financial implications of malicious drone flights, whether nuisance or nefarious, are evident in some key incidents that have occurred in recent years. The Gatwick Airport drone incident occurred in December 2018, with multiple drone sightings resulting in large scale disruptions to airport operations as flights were halted in accordance with safety protocols. The incident spanned three days and initially cost the airport £1.4m, however an additional £4m was spent in the aftermath on anti-drone technology. The airlines operating out of Gatwick suffered more significant losses, EasyJet alone reported compensation payments to passengers and lost revenue totalling £15m (Topham 2019).

The September 2019 drone attacks on the Saudi Arabian oil processing facilities in Abqaiq and Khurais had much wider financial ramifications, with the countries stock market opening 2.3% lower as a result. As the world’s largest oil processing facility, the attack also threatened to increase the price of crude futures by up to \$10 a barrel constituting an increase of 25¢ per gallon of petrol (Turak 2019).

2.3 Mitigation

2.3.1 Legislative and Regulatory Controls

Mitigation of malicious drone use through policies that apply to recreational and commercial drone flight is a difficult task, the rapidly evolving drone ecosystem means that policy makers are often reactive. In many countries there are either no established drone laws or existing laws are antiquated.

In the recreational space, the common restrictions applied to drone use are related to line of sight, maximum flight height, distances from objects and/or people, the size/weight of the drone, and the use of restricted or prohibited airspace. In Australia drone safety rules are set by the Civil Aviation Safety Authority (CASA), for recreationally flown drones weighing under 25kg there is no requirement for a license or flight approvals provided the following rules are also adhered to; flight height capped at 120m above ground level, flight area not within 5.5km of a controlled aerodrome or other restricted airspace, and not undertaking first person view (FPV) flight.

Commercial drone flights are governed by additional regulations with requirements existing for pilots to obtain operator accreditations and in some cases a remote pilot licence (RePL), additionally registration is now mandated for commercially flown drones. CASA has the ability to enforce these rules with sanctions that include imposing financial penalties, imposing operational restrictions and in extreme cases, breaches can result in criminal charges with financial and custodial sentences (CASA 2021).

Table 1, summarises the regulatory authorities associated with drone use as detailed by Sprague and Perritt (2016) for a number of major developed countries, all of which have active aviation industries.

Country	Regulatory Authority
Australia	Civil Aviation Safety Authority (CASA).
Brazil	National Agency for Civilian Aviation - Agência Nacional de Aviação Civil (ANAC).
Canada	Transport Canada via the Minister of Transport.
China	Civil Aviation Administration of China (CAAC).
European Union	European Aviation Safety Agency (EASA) in collaboration with member states national authorities.
France	Direction Générale de l'Aviation Civile (DGAC)
Germany	Luftfahrt-Bundesamt, "Federal Aviation Office" (LBA)
India	The Directorate General of Civilian Aviation (DGCA)
Italy	The Italian Civil Aviation Authority - Ente Nazionale per l'Aviazione Civile (ENAC)
Japan	Civil Aviation Bureau via the Ministry of Land, Infrastructure and Transport (MLIT)
United Kingdom	The UK Civil Aviation Authority (CAA)
United States	Federal Aviation Administration (FAA)

Table 1: Summary of international regulatory authorities pertaining to drones.

In the United States the FAA has taken steps beyond simply registering drones in an effort to integrate drone use safely and securely into the National Airspace System (NAS). The UAS remote identification (remote ID) initiative is a new rule being introduced that requires drones in flight to broadcast individual identification and location information. The information to be broadcast would include the drone's unique identifier, a time mark, the drone's velocity, latitude, longitude, and geometric altitude. Additionally, the latitude, longitude and altitude of the broadcast or control station would also be required to be broadcast.

The FAA will require all manufacturers to either manufacture drones with remote ID broadcast capability or to manufacture remote ID broadcast modules that can be used to retrofit existing craft, this requirement will be effective from September 16th, 2022. By September 16th, 2023, drone pilots will be required to only operate drones that are either fitted with remote ID as standard or have been retrofitted with a broadcast module. The only exception to this rule is if the drone is being operated at a FAA Recognised Identification Area (FRIA) (FAA 2021).

These mitigation methods rely largely on voluntary compliance by the operator and some compliance monitoring and enforcement by regulators. However, legislative and regulatory mitigation is less effective when the operator of a drone has malicious intentions. Likewise, the immobilisation of the drone may stop the immediate threat but without identifying the operator, the intentions of the flight will remain unknown, and the breach is at risk of being repeated.

Currently the majority of techniques used to detect and locate the drone operator involve the use of Radio Frequency (RF), acoustic, radar and Electro-Optical (EO) sensors, these sensors must be

distributed around the flight area. Often these systems are expensive and challenging to implement due to the presence of other signals in the airspace (Osborne 2020).

Additionally, as mentioned previously, drones operating using 'intelligent flight' modes may do so without any radio control signal being transmitted by the operator and therefore the sensors listed above are of little use in identifying operators. Accordingly, physically tracking the drone back to its point of origin provides a far more feasible method in a wider range of scenarios. This has resulted in a variety of research into malicious drone and object tracking using both single drones and drone swarms. The research literature in this regard is reviewed in the following sub-section.

2.3.2 Object Tracking via Drone Swarms

Earlier research carried out in this space focused on the tracking of ground-based targets using coordinated drone swarms. Cheng et al. (2013) sought to evaluate the performance of a decentralised controller against a centralised controller for a drone swarm undertaking a ground target engagement task. The decentralised control strategy governed the behaviour of the individual drones within the swarm through a set of rules, the individual drones operate without a supervisory drone and modify the task environment accordingly, the modified environment will then influence the future behaviour of the remainder of the swarm. The task simulated was the engagement of a moving ground-based target by a three-drone cooperative swarm, two of the drones continuously track the target while the third deploys an onboard weapon. The position of the target is triangulated via the tracking information from the two tracking drones and provides a targeting position for the weapon drone. The simulation found that the decentralised controller led to a very cooperative performance of the swarm without the need for a centralised controller. However, when the complexity of the task was increased the decentralised controller's performance declined compared to that of a centralised controller.

The algorithms deployed within the swarm by Ma'sum et al. (2013) differ to those mentioned above as each drone within the swarm has access to a global base rather than operating implicitly with each other through a pre-determined rule set. Similar to Cheng et al. (2013), the scenarios examined involved patrolling a defined area and the localization of both a stationary and a moving ground-based target. Again, a three-drone swarm was examined, object detection is achieved with the built-in cameras and an object detection algorithm, proportional integral differential (PID) control is used for the object tracking algorithm. A modified particle swarm optimization (PSO) algorithm was used for object localization and is evaluated through physical experimentation against a fully randomised moving algorithm. The results from the experiments demonstrated that the PSO algorithm outperformed the randomised algorithm in the stationary and moving target scenarios.

2.3.3 Tracking of Malicious Drones via Drone Swarms

Guerra et al. (2020) sought to provide an alternative to relying on ground-based radar systems to identify and track malicious drones. This would be achieved via the use of a dynamic radar network (DRN) made up of a swarm of drones capable of highly accurate real time tracking. This research concluded via simulation that the DRN created by the swarm was far more flexible and able to be customised than currently available terrestrial radar systems, and ultimately provided improved tracking of a passive target. It is important to note that in this work it appears that the malicious drone is of lower capability to that of the swarm, this may explain why there are no specific simulations carried out on set starting or operating flight formations, instead the swarm formation is optimized via a control algorithm.

The research carried out by Pozniak and Ranganathan (2019) into the hardware and software aspects of a counter unmanned aircraft system (CUAS) testbed yielded complimentary conclusions with regard to the efficacy of drone swarms, especially when compared to tracking via a single pursuit drone. In this work the swarm would utilise camera-based detection systems to identify their targets and then apply Dijkstra's algorithm in order to determine the fastest route for interception. The testbed proposed countermeasures and mitigation that largely revolved around encircling the malicious drone to restrict its movement or using fixed onboard nets in order to capture the drone. Whilst these mitigation techniques are efficient and perhaps necessary in immediately dangerous situations, they compromise the ability to identify the operator of the drone. There is no explicit clarification of the malicious drone's capabilities compared to that of the swarm in this research. However, the testbed is modular and highly scalable and could readily be applied to a scenario where the malicious drone is of higher capability than the swarm.

Encirclement to restrict movement of the malicious drone is a common mitigation technique described in the literature. The research undertaken by Brust et al. (2017), takes this a step further with the malicious drone being encircled and then escorted from the flight zone. This research examined a system that deploys an autonomous swarm of defence drones that progress through four phases of operation: clustering, formation, chasing and escorting. As a result of the extensive simulations carried out the defence swarm is shown to be resilient in the event of communication loss, and the encirclement and escort approach is concluded to be feasible. However, one of the assumptions included in the problem definition is that the malicious drone has a lower top speed than the swarm drones. Additionally, the proposed mitigation of escorting the drone from the flight zone once again removes any opportunity to identify the origin and operator of the malicious drone.

Koohifar et al. (2018) opted to investigate drone mounted radio frequency (RF) tracking as a malicious drone detection method in place of computer vision. Each drone is equipped with an omnidirectional received signal strength indicator (RSSI) and operates through a feedback loop of operational stages: Measurement of signal, estimation of target position, and path planning of swarm to reduce measurement errors. The key findings of the research concentrated on determining the optimum algorithms for the two main stages of the problem: estimation of the target position and path planning of the tracking swarm. In this regard the findings concluded that for the estimation or localization stage the recursive Bayesian estimator algorithm was the better performer and for the path planning stage the steepest descent algorithm was optimal. The capabilities of the malicious drone are never explicitly defined so the performance of the system with regard to a high capability malicious drone is unknown. The intention to track the malicious drone without attempting to restrict its movement or disable it does however allow for possible identification of the origin or operator of the drone.

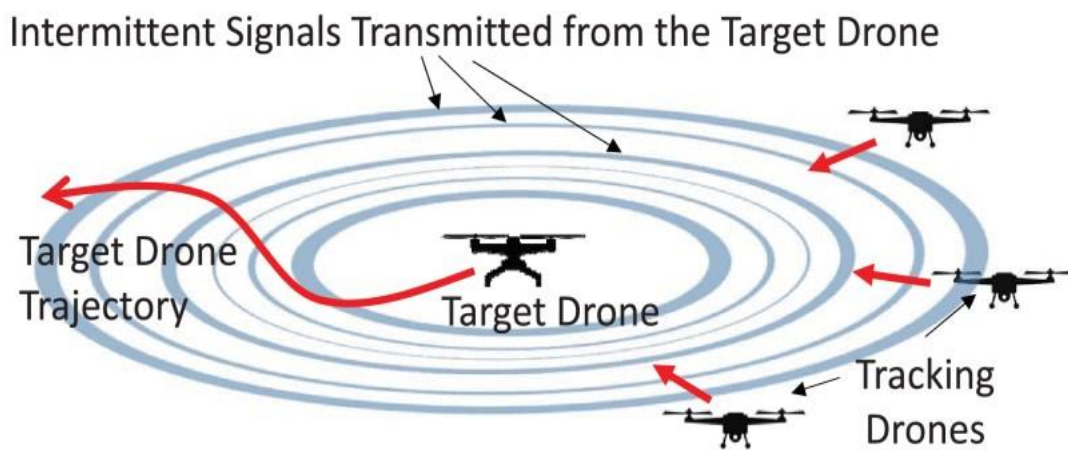


Figure 4. Drone swarm utilising intermittent RF signals to track target drone (Koohifar et al. 2018)

Wang et al. (2020) proposed an optimal guidance strategy and undertook simulation experiments to examine its efficacy. The strategy has been designed to be applied to a drone swarm specifically, which has distinctly different flight characteristics to the fixed wing aircraft and missiles that existing strategies were developed for. The foundation for the proposed strategy is the pure-pursuit guidance law integrated with the Kuhn-Munkres optimal matching algorithm, additional emphasis is placed on collision avoidance between both the drones within the swarm and the target. Ultimately the simulations demonstrate that the proposed strategy leads to the swarm successfully intercepting the moving target within 3D space whilst holding a reasonable formation. Malicious drones and birds are listed as potential targets for the swarm; however, it is explicitly stated in the problem formulation

chapter that the target in question must under all circumstances have a lower maximum speed than the swarm drones.

2.3.4 Tracking of High Capability Malicious Drones

The simulations undertaken by Arnold and Brown (2020) sought to determine the efficacy of three different drone swarm flight formations in tracking a target drone. These formations included, follow, surround, and cone. In contrast to the literature mentioned in the previous section the malicious drone in this case had three levels of flight capabilities, all of which were higher than that of the pursuing swarm drones. To ensure collation of adequate data the simulation was carried out multiple times using a mix of different parameters: three different malicious drone flight paths, three swarm formations, three levels of flight capability and a variable number of drones in the swarm. The simulations were carried out using OMNeT++ and determined that surround and cone formations were superior to the follow formation in effectively tracking the malicious drone, this was attributed to the encirclement characteristics present in these formations allowing for better reactions to changes in direction of the malicious drone. Suggested further research includes the investigation of additional drone swarm formations to determine if superior performance can be achieved.

Recognising that a high capability malicious drone has the potential to outrun a pursuing drone of lesser capability, Brown and Raj (2021a) sought to evaluate through simulation, any performance gain achieved by implementing predictive pre-positioning of the swarm alongside reactive tracking. Simulations were undertaken using MATLAB, where a circular area of interest was populated with randomly positioned surveillance drones to make up the swarm. The malicious drone travelled straight through the centre of the area in question at a set top speed that at all times was faster than the swarm drones, the size of the drone swarms as well as their top speed capabilities were variable, and a number of simulations were carried out and averaged for each variable configuration. The main metric used for the evaluation is the proportion of time that the malicious drone is actively tracked by one or more of the swarm drones (reduction in tracking voids), against this metric it was concluded that reactive tracking and predictive pre-positioning outperformed reactive tracking alone. It is important to note that the initial starting formation of the swarm is in this case randomised and further research into the possible performance effects of different initial formations is suggested.

The impacts of initial swarm formation on tracking of a high capability drone have recently been explored further by Brown and Raj (2021b) through a modification of their previous work. The simulations were repeated using the same parameters as before however this time the randomly positioned surveillance drones are evaluated against a circular formation consisting of uniformly

spaced concentric rings. The circular formation performed better than the randomised formation for both of the tracking strategies, with particular improvement shown for a predictive pre-positioning coupled with small swarm size scenario.

Further research into modifications of the circular formation, or entirely new initial formations, is the next logical challenge for further optimising the tracking ability of the swarm through the reduction of tracking voids.

Chapter 3

3. Simulation Design

3.1 Simulation Environment

3.1.1 MATLAB

The resources required to undertake real-world physical experiments are extensive and time consuming and as such the use of a simulated environment is necessary. A simulated environment provides for the adaptive adjustment of variables, and for a far wider range of variables to be tested. For example, drone swarm sizes in the hundreds or thousands. This project sought to expand upon the work completed by Brown and Raj (2021a) and Brown and Raj (2021b), where the simulation environment utilised was the MATLAB application. MATLAB is a numeric computing environment built around the MATLAB programming language, key features include manipulation of matrices, plotting of data and functions and algorithm implementation. Accordingly, this project also utilised MATLAB for all simulations with the specific implementation detailed within this chapter, additionally the entire simulation code is attached in Appendix D.

3.2 Simulation Implementation

3.2.1 Tracking Area and Malicious Drone Flight Path

A circular tracking area with a radius of 15km is utilised and is assumed to be centred around a point of interest that is susceptible to high capability malicious drone attacks (e.g., an aerodrome or power station). It would then be logical for the flight path of the malicious drone to pass through the centre of the tracking area, therefore during each iteration of the simulation the malicious drone traverses a diameter of the tracking area. Using the animation function built into the code the malicious drone's movement through the tracking area can be observed. Figure 5 is a frame captured from this animation where the tracking area is occupied by a circular formation, the red circle represents the malicious drone on its way across the x-axis whilst the blue crosses represent the surveillance drones comprising the swarm.

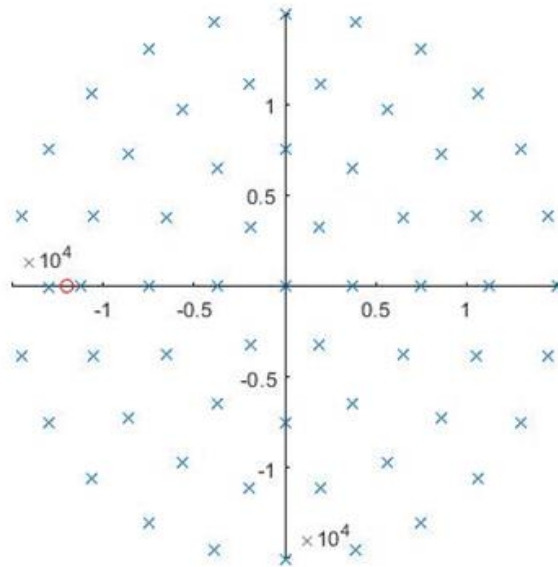


Figure 5. Malicious drone movement captured from MATLAB simulation animation

3.2.2 Tracking Strategies

Two different malicious drone tracking strategies will be simulated for each of the swarm formations under test, these strategies aim to reduce the duration of tracking voids and to compensate for the superior capability of the malicious drone by handing over tracking responsibility to better placed drones within the swarm. The algorithm pertaining to the movement of the swarm drones will be detailed in a later section within this chapter.

Reactive Tracking

The reactive tracking strategy involves individual drones within the surveillance swarm pursuing the malicious drone only when they have individually detected it and ceasing their pursuit once the malicious drone has left their detection range. This strategy assumes there is no communication between drones within the swarm regarding the malicious drone's position, this results in the remainder of the swarm hovering in formation with only individual drones commencing pursuit when they detect the malicious drone. Figure 6 depicts a basic application of the strategy, the malicious drone (M) travels in a straight-line trajectory, the swarm drone (S1) detects and then pursues M until it is inevitably outpaced. Swarm drone (S3) is positioned further down the flight path and upon detecting M will commence its own pursuit, the tracking void exists where swarm drone (S2) is positioned such that M never comes into detectable range and therefore S2 only ever hovers in place.

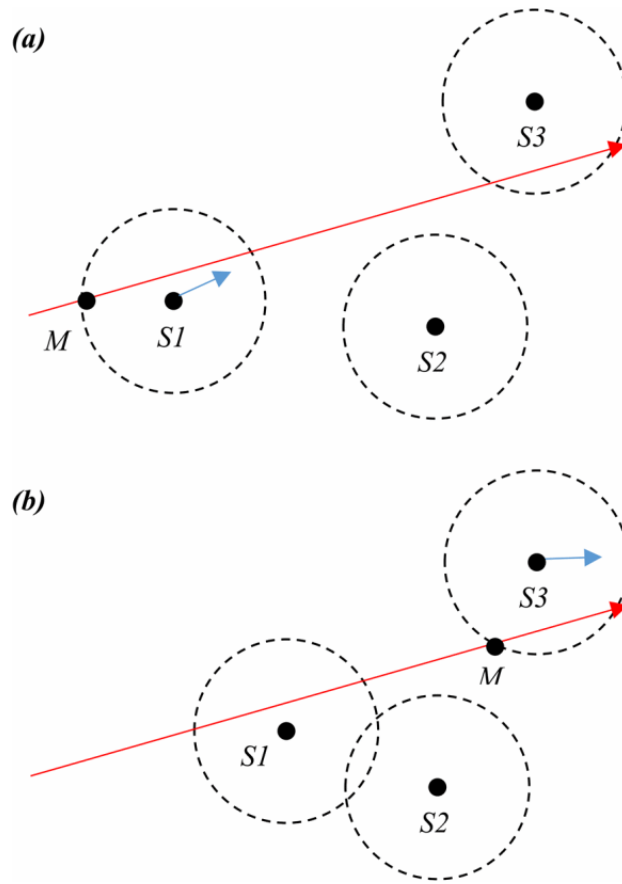


Figure 6. Reactive tracking of malicious drone (a) Surveillance drone S1 detects and pursues M. (b) M has outpaced S1 which has subsequently stopped pursuit, S3 has detected M and begun pursuit. S2 never detects M and never changes position (Brown & Raj 2021a).

Reactive Tracking with Predictive Pre-Positioning

Reactive tracking with predictive pre-positioning builds upon the previous strategy by incorporating intra swarm communications containing estimates about the malicious drone's position, speed and bearing. Once a malicious drone is detected by any of the surveillance drones in the swarm the shared data is then used by every other surveillance drone to set a course for a more optimum tracking position. This could in theory result in a string of surveillance drones positioned along the entirety of the malicious drone's flight path. Figure 7 demonstrates the implementation of this, once again S1 is first to come within detection range of M and begins its pursuit, however, in this scenario S1 has also communicated the estimated trajectory data of M to S2 and S3, both of which begin pre-positioning to an improved tracking position. The pre-positioning has completely removed the tracking void seen in Figure 6 as S2 is now within range of M and pursuit is handed over from S1. Once M has outpaced

S2, pursuit is handed over to S3 which has improved its starting position from the scenario in Figure 6 and will be able to maintain M within its detectable radius for a longer period as a result.

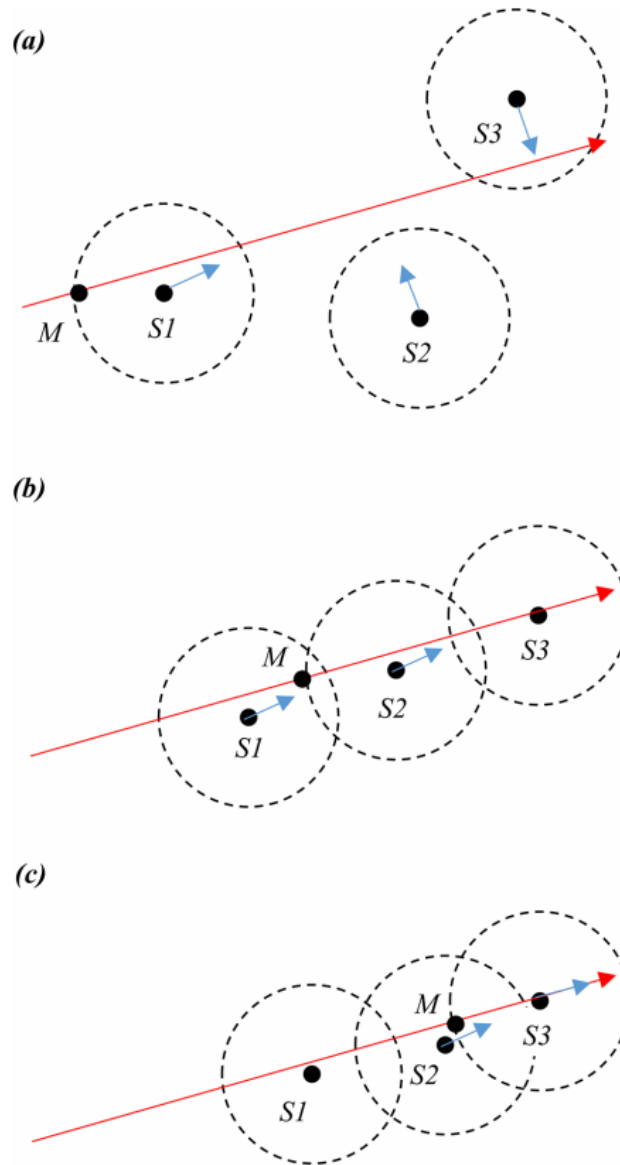


Figure 7. Reactive Tracking with Predictive Pre-Positioning of malicious drone (a) S1 detects M, begins pursuit, and relays M's estimated trajectory to S2 and S3, who begin pre-positioning. (b) S1, S2 and S3 are now positioned without tracking voids along M's trajectory. (c) S1 has handed over pursuit to S2 and S3 (Brown & Raj 2021a).

3.2.3 Implemented Initial Swarm Formations

As discussed in the literature review (Chapter 2), the basis for the work carried out by Brown and Raj (2021b) was the performance of the tracking strategies when applied to different initial flight formations of the swarm. In their work a randomly distributed swarm formation was evaluated against a circular formation, the results from this are replicated within this project and then utilized as a benchmark against which to evaluate new initial formations. The implementation of these formations within the code is discussed within this section.

Random Formation

The randomly positioned initial swarm formation was utilised by Brown and Raj (2021b) to provide a baseline comparison for their circular swarm formation. The construction of the circular formation was based on the principle that the distance between each swarm drone will be approximately the same across the test area, regardless of the swarm size. Therefore, for the random swarm formation and any subsequent formations under test, the same distribution principles should be implemented to allow meaningful direct comparison between formations.

The random swarm formation is constructed by selecting the radial and angular coordinates of each swarm drone from a continuous uniform probability distribution. This ensures a radial coordinate of an approximate value between 0 and R, where R is the radius of the swarm, and an angular coordinate of an approximate value between 0 and 2π . This approach was originally found to yield a formation that, although random in nature, did not meet the required swarm distribution principle as there was a disproportionate number of drones concentrated around the centre of the tracking area. In order to avoid this issue, the radial coordinate used for each drone is the product of R and the square root of a random variable in the range of 0 to 1 having a continuous uniform probability distribution. Figure 8 shows the section of the simulation code where the random formation is generated.

```
% random formation
swarmUAVPosMagnitude=FIELD_RADIUS*sqrt(rand...
    (numberOfSwarmUAVs(numberOfSwarmUAVsIndex),1));
swarmUAVPosAngle=2*pi*rand(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
swarmUAVPosX=swarmUAVPosMagnitude.*cos(swarmUAVPosAngle);
swarmUAVPosY=swarmUAVPosMagnitude.*sin(swarmUAVPosAngle);
```

Figure 8. Random swarm formation code.

Circular Formation

The circular formation is constructed using evenly spaced concentric rings of evenly spaced swarm drones, it is assumed that at least one drone, no matter the swarm size, would be positioned directly over the point of interest, that is, located in the centre of the tracking area. To achieve the uniform spacing required between each drone and each ring, the total number of drones in the swarm increases in line with the progression of centred hexagonal numbers as additional rings are added. The first ring is constructed using six drones which each represent a vertex of a hexagon, inclusive of the centralised drone this means a total of seven swarm drones for a single ringed circular formation. With each additional formation ring implemented, the number of drones in a given ring will increase linearly with radius, this ensures compliance with the uniform drone spacing principle of the formation.

Therefore, the inclusion of a second ring having twice the radius of the previous ring would require an additional $2 * 6 = 12$ drones, bringing the total to $1 + 6 + 12 = 19$, and a third ring would require an additional $3 * 6 = 18$ drones, bringing the total to $1 + 6 + 12 + 18 = 37$ and so on for n^{th} rings. The total drones within the formation can then be calculated via summation of the centre drone and each existing ring, this summation can be simplified via the formula:

$$N = 1 + 3n(n + 1) \text{ for } n \geq 1 \quad (1)$$

Where:

- N = Total drones within the swarm.
- n = Number of rings.

Figure 9 demonstrates how the input and output of the formula above has been utilised to create variables within the code which dictate the total number of rings and subsequently the total number of drones within the swarm. The 'numberOfSwarmUAVs' variable is utilised by all formations under test to ensure uniform swarm sizes, whilst the 'numberOfSwarmRings' variable is only called upon by the circular formation.

```
% Specify total number of UAV's in swarm formation
numberOfSwarmUAVs= [7, 19, 37, 61, 91, 127, 169, 217, 271, 331, 397,...
                   469, 547, 631, 721, 817, 919, 1027, 1141, 1261, 1387];
% Specify number of swarm rings (circular formation only)
numberOfSwarmRings=[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,...
                   12, 13, 14, 15, 16, 17, 18, 19, 20, 21];
```

Figure 9. Code for variables related to swarm size.

It is important to note that the malicious drone traverses the same path through the tracking area during each iteration of the simulation, to ensure an equitable comparison to the other formations under test it is necessary to randomise the angular position of the circular formation. This randomisation is accomplished with the addition of an angle within the range of 0 to 2π which is drawn from a continuous probability distribution. This method ensures that the formations response to the malicious drone is being simulated for a variety of different approach directions, Figure 10 demonstrates the section of code responsible for constructing the circular formation and the variable 'randPosAngle' can be seen to be instituting the necessary angular rotation on each loop through the code.

```

% circular formation
randPosAngle=2*pi*rand;
swarmUAVPosMagnitude = zeros(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
swarmUAVPosAngle = zeros(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
uavIndexAbsolute=2;
for ring=1:numberOfSwarmRings(numberOfSwarmUAVsIndex)
    NUMBER_OF_UAVS_IN_RING = (6*ring);
    for uavIndexInRing=1:NUMBER_OF_UAVS_IN_RING
        swarmUAVPosMagnitude(uavIndexAbsolute)=...
            FIELD_RADIUS*ring/numberOfSwarmRings...
            (numberOfSwarmUAVsIndex);
        swarmUAVPosAngle(uavIndexAbsolute)=randPosAngle...
            + 2*pi*uavIndexInRing/NUMBER_OF_UAVS_IN_RING;
        uavIndexAbsolute=uavIndexAbsolute+1;
    end
end

swarmUAVPosX=swarmUAVPosMagnitude.*cos(swarmUAVPosAngle);
swarmUAVPosY=swarmUAVPosMagnitude.*sin(swarmUAVPosAngle);

```

Figure 10. Circular swarm formation code

Sunflower Formation

The spiralling pattern seen in the arrangement of sunflower seeds is observed throughout the natural world, often influencing the manner in which flowers, leaves and branches are spaced around their stems or trunks. In the commonly recognised case of the sunflower, the seeds are positioned to make efficient use of the available space, providing maximum room for each seed whilst minimising wastage of space.

The goal here is to utilise such a pattern to uniformly distribute a predetermined set of points within a circle, or in the case of this project uniformly distribute surveillance drone swarms of varying sizes within the designated circular tracking area. The sunflower seed formation has already served as inspiration for other engineering endeavours, including the mirror arrangement in a solar concentrator array, an efficient showerhead design, and an efficient water mixer. It was anticipated that this formation would have the potential to reduce voids present in similar formations, such as the circular formation, due to the presence of multiple overlapping spirals which follow the Fibonacci sequence.

A basic mathematical formula exists for defining the sunflower formation:

$$\theta = \frac{2\pi}{\phi^2} n \quad \text{and} \quad r = c\sqrt{n} \quad (2)$$

Where:

- c is an arbitrary constant.
- n is the number of seeds/drones.
- ϕ = the golden ratio = $\frac{1+\sqrt{5}}{2}$.

The implementation of the sunflower formation within the code is shown in Figure 11 and required some additional adjustments in regard to the boundaries to ensure the formation was constrained within the designated tracking area. It should also be noted that the angular rotation applied to the circular formation is replicated here to ensure an equitable comparison in relation to random malicious drone flight paths. Additionally, similar to the circular formation, there is also provision to lock one surveillance drone to the centre of the tracking area, this can be toggled for each simulation run as desired.

```

% Sunflower formation
swarmUAVPosMagnitude = zeros(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
swarmUAVPosAngle = zeros(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
goldenratio = (1+sqrt(5))/2;
randPosAngle=2*pi*rand;
uavIndexAbsolute=2; % Change for UAV at center or not
for k=1:numberOfSwarmUAVs(numberOfSwarmUAVsIndex)- 1
    boundaryPoints = round(sqrt(k));
    swarmUAVPosMagnitude(uavIndexAbsolute) =...
        FIELD_RADIUS*(sqrt(k-1/2)/sqrt(numberOfSwarmUAVs...
            (numberOfSwarmUAVsIndex)-(boundaryPoints+1)/2));
    swarmUAVPosAngle(uavIndexAbsolute) = randPosAngle...
        + 2*pi*k/goldenratio^2;
    swarmUAVPosX=swarmUAVPosMagnitude.*cos...
        (swarmUAVPosAngle);
    swarmUAVPosY=swarmUAVPosMagnitude.*sin...
        (swarmUAVPosAngle);
    uavIndexAbsolute=uavIndexAbsolute+1;
end

```

Figure 11. Sunflower swarm formation code.

Initial Formation Plots

Figure 12 shows the three implemented initial formations generated during the simulation, they have each been captured at two swarm sizes, the first comprising 91 drones and the second comprising 1387 drones.

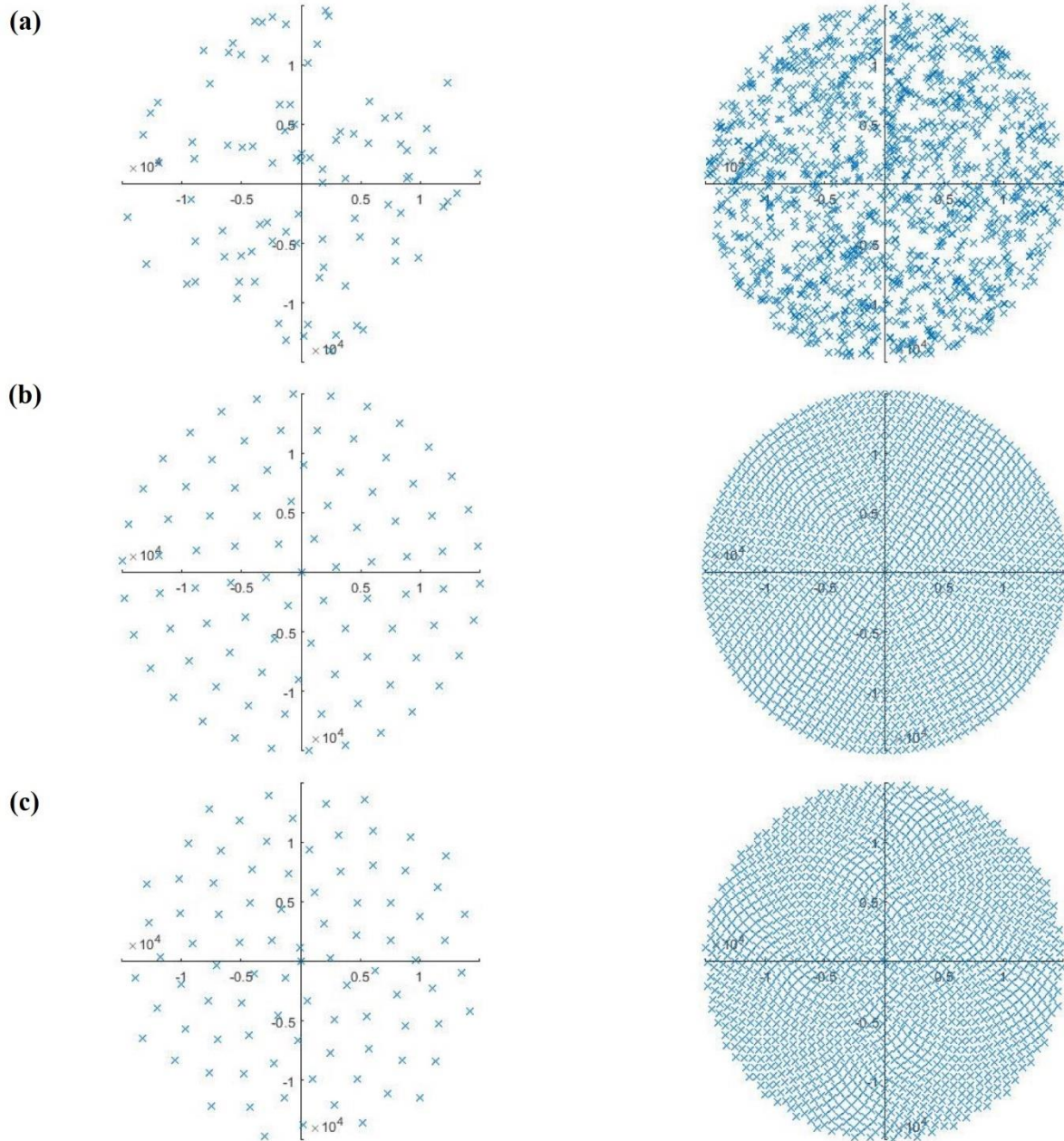


Figure 12. Implemented formation examples with 91 drone swarm on L and 1387 drone swarm on R (a) Random formation. (b) Circular formation. (c) Sunflower formation.

3.2.4 Swarm Drone Movement Algorithm

Irrespective of the tracking strategy or formation being implemented, movement of the individual surveillance drones within the swarm is dictated by the guidance law utilised by Brown and Raj (2021a) and Brown and Raj (2021b). The guidance law algorithm enables calculation of the optimum bearing that a swarm drone should use to track a high capability malicious drone in order to minimise tracking voids. That is, to maximize the tracking time.

The algorithm can best be described visually using Figure 13, where:

- r = the detection radius of the surveillance drone.
- u = the maximum speed of S.
- v = the set speed of M in the direction of the x-axis (v is always $> u$ as M is of higher capability).
- φ = the angle between the line joining M and S and the x-axis ($-\pi/2 \leq \varphi \leq +\pi/2$).
- θ = the angle relative to the x-axis in which S moves to track M ($-\pi/2 \leq \theta \leq +\pi/2$).

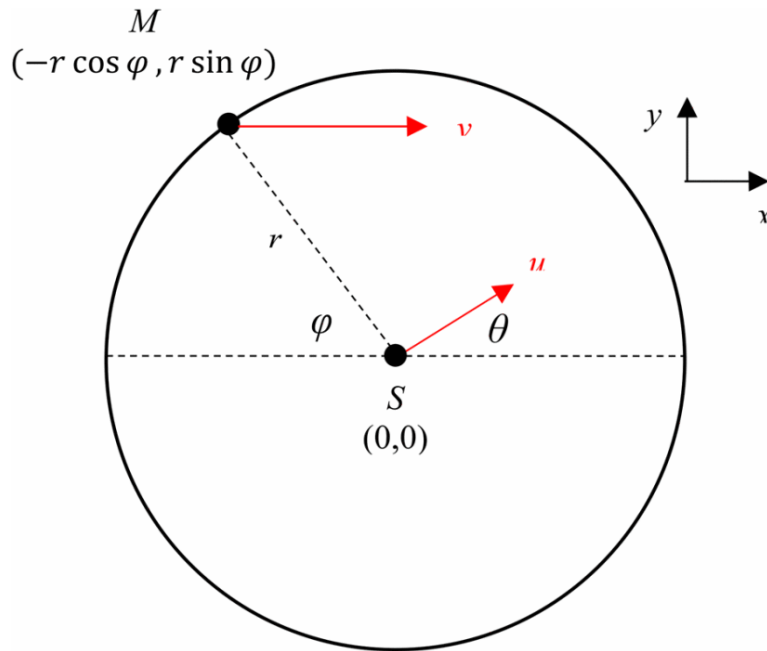


Figure 13. Surveillance drone optimum bearing example, surveillance drone (S) is detecting malicious drone (M) Brown and Raj (2021a).

The guidance law also provides the derivation of the following formula for calculating the optimal value of θ that minimises tracking voids i.e., maintains the distance between S and M at less than or equal to r for as long as possible.

$$\theta_{optimal} = \cos^{-1}\left(\frac{2uv \sin \varphi}{\sqrt{u^4 + v^4 - 2u^2v^2 \cos 2\varphi}}\right) - \tan^{-1}\left(\frac{v^2 - u^2}{[u^2 + v^2] \tan \varphi}\right) \quad (3)$$

This formula is implemented within the code to dictate the movement of each, and every swarm drone as required by the tracking strategy being utilised during that particular iteration.

3.3 Unimplemented Initial Swarm Formations

Three additional alternate initial swarm formations were proposed for evaluation and coded to some extent within MATLAB, however integration into the simulation did not eventuate. The adaptation of these formations to the radial and angular coordinate system utilised within the simulation environment proved to be more difficult than anticipated, this was in contrast to the sunflower formation, which due to its circular nature did lend itself to the coordinate system established by the benchmark formations. Ultimately excessive debugging in an attempt to implement these formations was beginning to encroach on the project timeline.

The additional alternate formations that were not further pursued in this project are all variations of Bravais lattice type structures, this type of structure is used to describe the geometric arrangement of the lattice points within the structure of a crystal. The lattice points themselves represent the vertices of a unit cell, which in crystallography is a space which fills the lattice space without any overlapping or voids. Therefore, it could be presumed that taking lattice type structures and placing individual swarm drones on the lattice points, could provide an efficient method with which to maximise malicious drone tracking time. Accordingly, these alternate formations should be considered in future research projects of this nature.

In the two-dimensional plane there exists five Bravais lattices: monoclinic, orthorhombic, tetragonal, and hexagonal. The unimplemented formations partially coded for this project were the tetragonal, hexagonal, and a special case of the hexagonal lattice. The tetragonal lattice is also known as a square lattice which is a fairly self-explanatory structure, the hexagonal lattice is also referred to as the triangular lattice and is a little more complex. The triangular lattice involves repeating equilateral triangles as the unit cells, if picking any one lattice point a hexagon can be seen to be surrounding said point. The final formation under consideration is a special case of the hexagonal/triangular lattice known as the honeycomb lattice, the honeycomb lattice could be viewed as the merging of two offset triangular lattices, the centres of the hexagons of the honeycomb structure form a hexagonal/triangular lattice. These formations are best visualised and examples of each can be seen below in Figure 14, with the code used attached in Appendix F.

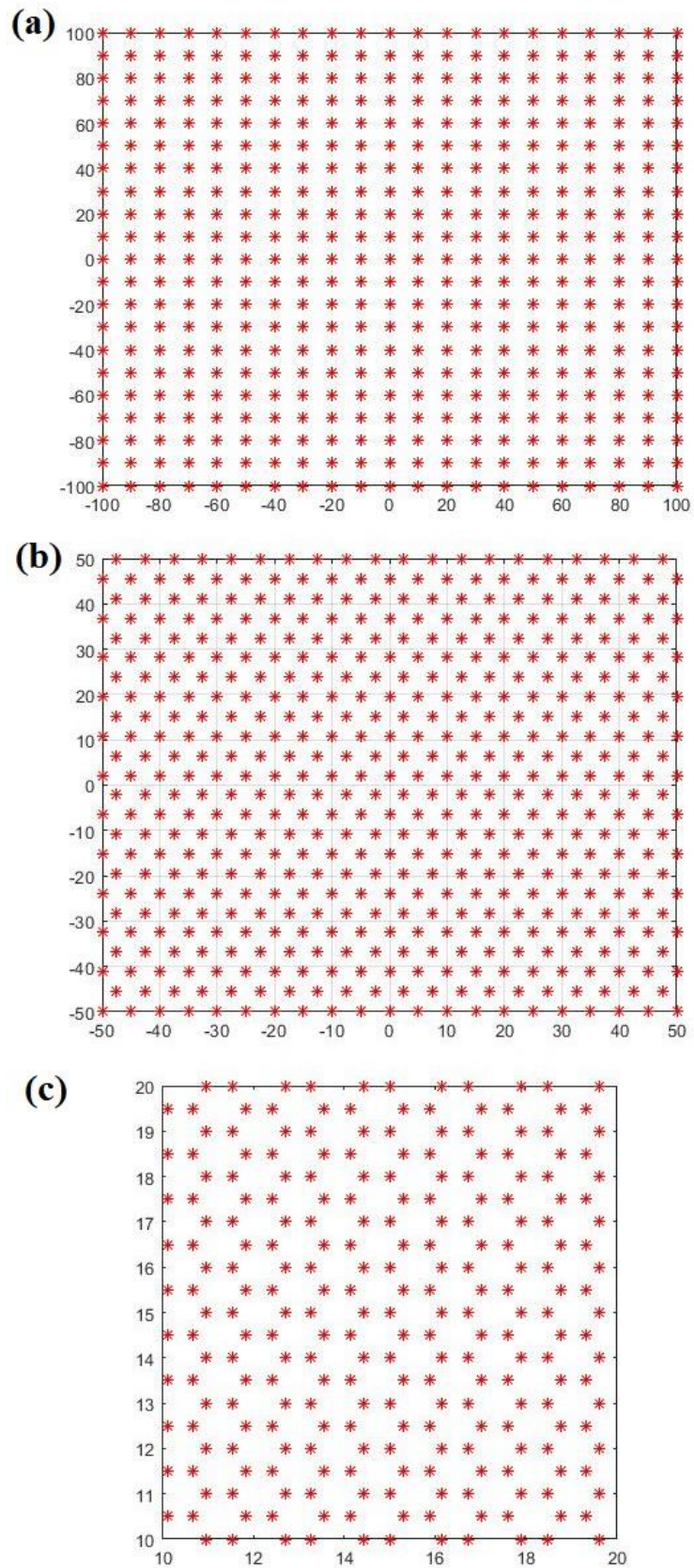


Figure 14. Unimplemented lattice formations. (a) Square Lattice. (b) Hexagonal/Triangular Lattice. (c) Honeycomb Lattice

Chapter 4

4. Methodology

4.1 Methodological Approach

This project seeks to examine the effectiveness of a variety of surveillance drone swarm initial flight formations in reducing tracking voids when tracking a high capability malicious drone. To achieve this objective, it is imperative that quantitative data can be obtained from multiple replications of the same experiment, with different configurations for each replication. These configurations are determined by adjustable independent variables and must be free from external interference that could compromise the data. As previously discussed, the extensive resources and time required for physical experimentation determined that this project would be best completed utilising simulation.

Although not a real-world representation, a simulated environment in this case provides many benefits including the elimination of external interference/s which could confound the results or delay the outcome of the experiment, such as inclement weather and equipment breakdowns. Additionally, as mentioned in previous chapters the use of a simulated environment allows for a far greater scope than that achievable in the real world with the resources and time frame available, for instance the largest simulated swarm size is to be 1387 drones, this scale is inconceivably large in financial requirements alone. Simulation also removes the health, safety and ethical risks that would accompany a real-world experiment of this form and by extension removes the need for risk assessments to be completed.

4.1.1 Assumptions

In order to keep the complexity of the project at a manageable level within the time frame provided, assumptions were made. An additional reason that these assumptions were made is that they largely mirror those made in the previous research highlighted within Chapter 2, this allows for a consistent and accurate replication of those results and by extension allows the project to meet the aim listed in Chapter 1 of enabling direct comparison to historical results. The assumptions that apply to this project include:

- Acceleration is not considered in the simulation.
- Turn speed of the drones is not considered.

- Intra swarm communication method is not specified.
- No collision avoidance between other drones or the environment is considered.
- All drones are at a constant altitude i.e., the simulation remains in the 2D plane.
- Malicious drone detection occurs 100% of the time once within swarm drone detection radius.
- There are no range limitations applied to the drones with regards to flight time, transmission distance or battery levels.

Acceleration and Turn Speed

In order to minimise the complexity of the code and to ensure a simulation environment which is consistent with that used in the previous research, drone acceleration is not considered. Instead, both the malicious and swarm drones within the simulation traverse the field at their set maximum speeds and move at these speeds instantaneously. Similarly, the orientation of the drones is never specified and therefore the drone turn speed is irrelevant as the drone is never required to ‘turn’. The omission of both acceleration and turn speed is not detrimental to the ultimate goal of characterising the potential increase in tracking efficiency brought about by implementing different initial swarm formations.

Intra Swarm Communication

The method of communication used within the drone swarm is not specified, intra swarm communication is however assumed to be present and is a key requirement for correct implementation of the predictive pre-positioning tracking strategy. Due to the tracking area being of a significant size (radius of 15km) it would be assumed that to maintain communication between all swarm drones, a terrestrial relay network would need to be utilised. However, for the purpose of evaluating initial flight formations it is not necessary to elaborate on the specific communication protocol being used.

Collision Avoidance and Constant Altitude

The flight altitude of both the swarm drones and the malicious drone is not specified and is considered to be a constant and equal value. This prevents a drastic increase in the complexity of the simulation coding by restricting the simulation to the 2D plane, and once again it enables an equitable comparison to historical results obtained in previous research. That being said, with appropriate time invested the existing code could be altered to operate in the 3D plane. Collision avoidance between

the individual drones in the swarm is not accounted for within the code, again this maintains the environmental assumptions made in prior research whilst reducing coding complexity. It is of note that many commercially available drones ship with collision avoidance sensors and software as standard. In a real-world scenario large swarm sizes such as that simulated within this project, would most likely require collision avoidance to be incorporated in the guidance law algorithm that was detailed in Chapter 3.

Detection Accuracy and Range Limitations

Detection of the malicious drone by a swarm drone is assumed to be 100% accurate as soon as the malicious drone encroaches the detection zone of the swarm drone. That is to say when the distance between the malicious drone and the swarm drone is less than or equal to 100m, it will be instantaneously detected, and tracking will be implemented as per the strategy being utilised at that time by the code. The method of malicious drone detection is also not specified, although examples are covered within Chapter 2, including the implementation of drone embedded radar and RF signal tracking. Ultimately this project is not attempting to evaluate different detection methods and although 100% accuracy is likely not achievable in a real-world setting, it is consistent across all simulations within this project and therefore appropriate for evaluating swarm formations. Similarly, the removal of all range limitations is not applicable to the real-world, however selecting any one specific drone model and its specifications as the basis for range limits within the simulation would pigeonhole the results obtained. The inclusion of range limitations would ultimately not provide any benefit in the comparison of flight formations in the general sense in which they are being evaluated within this project.

4.1.2 Simulation Characteristics and Variables

Swarm Drones

In order to ensure an equitable comparison with the benchmark results identified within the literature review, the maximum speed of the drones comprising the swarm will be set at one of three levels for each simulation run: 20 m/s, 25 m/s, or 29 m/s. As a point of interest, if these maximum speeds are compared to the specifications of a range of consumer and commercial drones readily available today, it can be observed that they are within the realm of possibility for a real-world scenario. Table 2 demonstrates the maximum speed specification of a range of drones currently available in the market as of October 2021. As identified within Chapter 2, DJI commands at least 75% of the industry market share and therefore is heavily represented within the table. Other performance specifications

with regard to flight range and acceleration are not considered as per the previous section and so are not provided within the table.

Manufacturer	Model	Top Speed
DJI	FPV	140 km/h – 38.89 m/s
	Inspire 2	94 km/h – 26.1 m/s
	Mavic 2 Pro	72 km/h – 20 m/s
	Phantom 4 Pro	72 km/h – 20m/s
Uvify	OOri	50 mph – 80.47 km/h – 22.35 m/s
Yuneec	Typhoon H3	72 km/h – 20 m/s
Autel	Evo II	72 km/h – 20 m/s

Table 2. Maximum speeds of readily available consumer drones DJI (2021), UVify (2018), Yuneec (2021), Autel (2017).

As covered in the preceding chapter, the initial position of the swarm drones will be dictated by whichever formation is currently under test in the simulation. In instances where the formation under test is not the ‘random formation’, a sufficient level of randomness for each iteration is still achieved via the angular rotation of the formation. Intra-swarm communication is invoked for simulation runs that utilise the predictive pre-positioning tracking strategy, however as previously stated the method is not specified and therefore there is no characteristics or variables associated.

Malicious Drone

The malicious drones speed is constant for all simulation scenarios and is always greater than the speed of the swarm drones pursuing it. It is imperative to again align with the benchmark research in order to allow an equitable comparison, therefore the maximum speed is set to 30 m/s. The drone flight path remains constant for each iteration and traverses the x-axis in one metre increments. To adequately simulate malicious drone approaches from random directions, the formations themselves are either randomly distributed by nature or as previously mentioned, randomly offset via angular manipulation for each iteration, this can be observed in Figure 15.

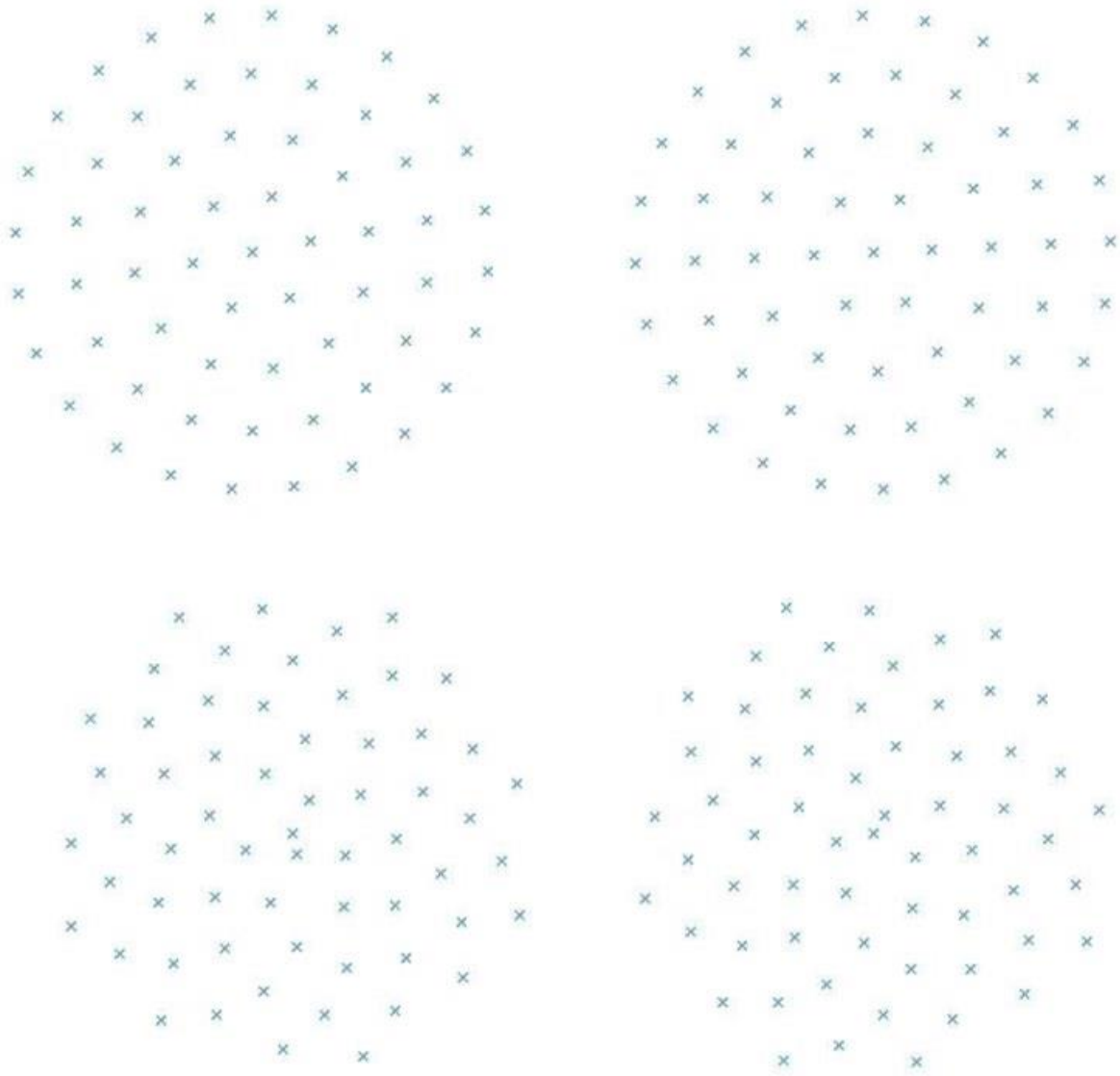


Figure 15. Circular and sunflower formation swarms comprising 61 drones, shown with varied angular orientations.

4.2 Methods Of Analysis

Each time the simulation is run it sequentially loops through six different formation and tracking strategy pairings:

- Reactive tracking (random formation)
- Reactive tracking (circular formation)
- Reactive tracking (sunflower formation)

- Reactive tracking with predictive pre-positioning (random formation)
- Reactive tracking with predictive pre-positioning (circular formation)
- Reactive tracking with predictive pre-positioning (sunflower formation)

Each pairing is simulated at 21 different swarm sizes, the swarm size increases in line with the progression of centred hexagonal numbers. This was previously detailed in Chapter 3, where swarm size is equal to the following subset of centred hexagonal numbers:

$$1 + 3n(n + 1) \text{ for } 1 \leq n \leq 21 \quad (4)$$

$$\equiv (7, 19, 37, 61, 91, \dots, 1141, 1261, 1387)$$

Each one of these configurations completes 500 unique iterations, resulting in 63,000 total iterations being completed for each simulation run, this translates to a simulation duration of approximately 16 hours per run and the simulation is completed at least three times, once for each maximum swarm speed. These simulation configurations allow for meaningful analysis of the independent variables under test and can be visualised with the aid of Figure 16.

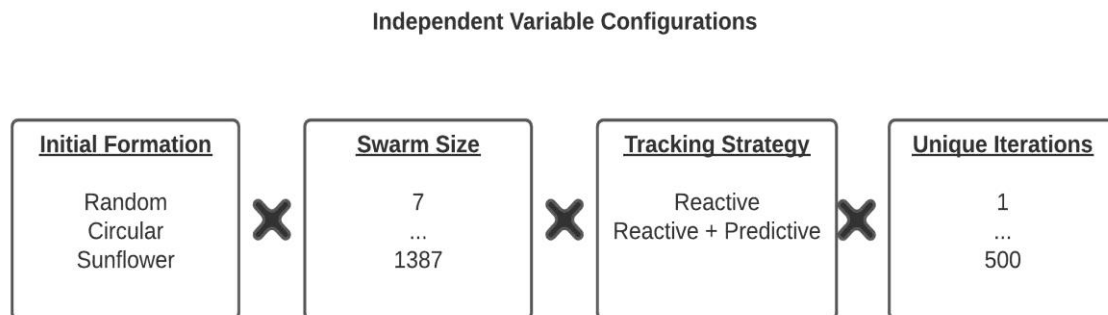


Figure 16. Simulation configurations for each swarm speed.

This simulation structure allows for the creation of quantitative data relevant to the following particular project objectives laid out in Chapter 1:

- Evaluation and comparison of the performance of initial swarm formations and sizes
- The replication of and evaluation against benchmark results identified in the literature.

The performance metric used to evaluate the benchmark tracking strategies and formations, was the proportion of time that any one or more surveillance drone/s were actively tracking the malicious drone whilst it traversed the tracking area. Using the simulation specifications detailed throughout this Chapter and in Chapter 3, this translates to the proportion of time that a malicious drone is within the 100m detection range of any of the drones comprising the swarm. To maintain an equitable comparison to the benchmark results, the same metric is adopted for this simulation.

As the malicious drone traverses the tracking area over the course of a single iteration, the distance between it and all of the drones comprising the swarm is calculated every simulation step using the standard formula for the distance between two coordinate points:

$$distance = \sqrt{[(x_{swarm} - x_{malicious})^2 + (y_{swarm})^2]} \quad (5)$$

Where the Y coordinate is only considered for the swarm position as the malicious drone traverses the X-axis exclusively. With a tracking area having a radius of 15,000m this translates to 30,000 calculations being performed per iteration. Once calculated for all swarm drones the closest drone is found by locating the minimum value and if that value is less than or equal to the detection range of the swarm drones, a count is incremented. At the completion of one iteration i.e., one traversal of the tracking area by the malicious drone, the count value is stored, and the count is reset for the next iteration. This detection is also the trigger for the tracking strategy code detailed within Chapter 3 to be implemented and attempt, in line with the strategy applicable to the current configuration, to manoeuvre the swarm toward the malicious drone.

At the completion of all iterations at a particular swarm size the mean is taken of all 500 count values, this value is then normalised by division by 30,000, stored and then subsequently plotted. This process repeats for all swarm sizes resulting in 21 data points for each of the tracking strategy and formation pairings under test. The resulting plots illustrate the proportion of time (Y-axis) that the malicious drone is actively tracked by any number of swarm drones, against the number of drones comprising the swarm (X-axis). At least three such plots are generated, one for each of the top speed pre-sets specified for the swarm drones.

This data flow as it occurs in MATLAB can be demonstrated via the following example using only five iterations for simplicity:

$$countInRangeForOneIteration = [6000; 6000; 15351; 15789; 15820]$$

For each of the five unique iterations the amount of simulation steps for which the malicious drone was being actively tracked are counted and stored, the mean is taken and then normalised prior to plotting:

$$\text{mean}(\text{countInRangeForOneIteration}) = 11,792$$

$$\text{normalised data (proportion of time with active tracking)} = 11,792 * \frac{1}{30000} = 0.393$$

This example was completed with the circular formation which by design will always provide some level of tracking due to the surveillance drone located at the centre, if the example were repeated with the random formation there would be a chance of count values equal to zero. For a low number of iterations this would create some large outliers that would greatly skew the plots, however the 500 iterations used ensure these zero values are smoothed out prior to plotting. A summary of the simulation specifications detailed in this section is viewable in Table 3.

Variable	Value
Tracking area shape and size	Circular area with a 15,000 m / 15 km radius
Malicious drone flight path	Diameter of the tracking area (the x-axis)
Malicious drone maximum speed	30 m/s
Simulation step size	Malicious drone steps in 1m increments (30,000 total)
Total number of drones comprising the swarm	Set to increment each loop as per: $1 + 3n(n + 1)$ for $1 \leq n \leq 21$ $\equiv (7, 19, 37, 61, 91, \dots, 1141, 1261, 1387)$
Initial flight formation of the swarm	Fixed for each simulation run as one of the following: Random formation Circular formation Sunflower formation See Chapter 3 for details.
Tracking strategy implemented by the swarm	Fixed for each simulation run as one of the following: Reactive tracking Reactive tracking with predictive pre-positioning See Chapter 3 for details
Swarm drones maximum speed	Fixed for each simulation run as one of the following: 20 m/s, 25 m/s, 29 m/s
Range of swarm drone/s when detecting malicious drone	100 m

Table 3. Summary of simulation specifications and variables.

4.3 Data Collection

The nature of the data collected as a result of the simulations has been touched on in the preceding section of this Chapter, it represents the proportion of time that the malicious drone is actively tracked whilst within the tracking area by one or more of the swarm drones. The data collected is numerical and represented by double-precision floating point numbers, which is the default format for numeric variables in MATLAB.

The code structure involves multiple nested loops as different configurations are cycled through, data is stored within MATLAB for the entirety of the simulation, the output data in question is stored for plotting and the global variables are reset at the completion of each configuration run. The plot is not visible until completion of the whole simulation which encompasses all six pairing configurations, upon completion of each run the data used to generate the plot could be exported to excel or interrogated further within MATLAB itself if required.

4.4 Methodology Justification

The research conducted by Brown and Raj (2021a, 2021b) is to be used as a benchmark and so the methodology must be replicated in part. Additionally, the research in Brust et al. (2017), Wang et al. (2020), Guerra et al. (2020), and Arnold and Brown (2020) all utilize computer simulation with numerical analysis when determining their research outcomes. Although earlier research into object tracking via drone swarms by Ma'sum et al. (2013) utilised real-world experiments, the drone swarm was limited to three drones and the test area was only six by eight metres in size. Therefore, to achieve the project aims and proposed scope, the methodology detailed within this chapter is in line with those used throughout the literature and is appropriate.

Chapter 5

5. Results and Analysis

5.1 Analysis Overview

The principle aims of this project as detailed in Chapter 1 were to determine by simulation, the optimal drone placement, initial swarm size and formation required to achieve increased performance of tracking of a high capability malicious drone. In order to demonstrate any increased performance, the benchmark results identified within the literature were replicated alongside a newly proposed formation. The simulation utilises independent variables including, swarm size, initial swarm formation, tracking strategy, and the maximum speed of the swarm drones. The malicious drone flight path and top speed specifications are fixed for all simulations. The performance defining dependent variable is the proportion of time that the malicious drone is actively tracked whilst within the tracking area. Randomisation of the initial formation placement acts to simulate different malicious drone approach angles, and this is repeated for 500 iterations to provide a significant sample size for analysis.

5.2 Results At Different Swarm Speeds

The nature of the code means that for each full simulation run the independent variables with regards to swarm size, initial formation, and tracking strategy are cycled through automatically. The input variable adjusted externally prior to each run is the maximum speed of the drones comprising the swarm. Therefore, the results in this section will be analysed according to the swarm speed variable for that particular simulation run. Analysis will be carried out on the proportion of time that the malicious drone is actively tracked, calculated as the mean result of 500 iterations per configuration as detailed in Section 4.2.

5.2.1 Swarm Speed 20m/s

With the maximum speed of the swarm drones set to 20m/s this simulation represents the greatest discrepancy in capability between the pursuing drones and the malicious drone. It would be expected that actively tracking the malicious drone under these conditions would be difficult. It can be observed in Figure 17 and Table 4 below that the reactive tracking strategy provides limited performance under these conditions, where the mismatch in ability is quite large. It can however be

seen that at these performance levels the circular formation outperforms the random formation, as in the literature, and that the newly proposed sunflower formation subsequently outperforms both, albeit not by a significant amount.

When considering reactive tracking with predictive pre-positioning, there is a clear gulf in performance almost immediately, this mirrors the results observed in the benchmarking studies. The circular formation can be seen to outperform the random formation for the duration of the simulation as expected, however once the swarm size hits approximately 400 drones the performance increase is less significant. The proposed sunflower formation outperforms both benchmark formations for the entirety of the simulation, but in contrast the largest difference in performance is within the 400 – 800 drone swarm section. The sunflower and circular formation are not too significantly different at smaller swarm sizes, perhaps due to both being guaranteed some level of success due to having a centred surveillance drone. The larger difference observed at the greater swarm sizes, could be down to the nature of the sunflower formation at making more efficient use of the tracking area for its distribution of the swarm drones, it could also be that the Fibonacci sequence swirls being cut by the malicious drone’s flight path are far more varied than the ring structure of the circular formation.

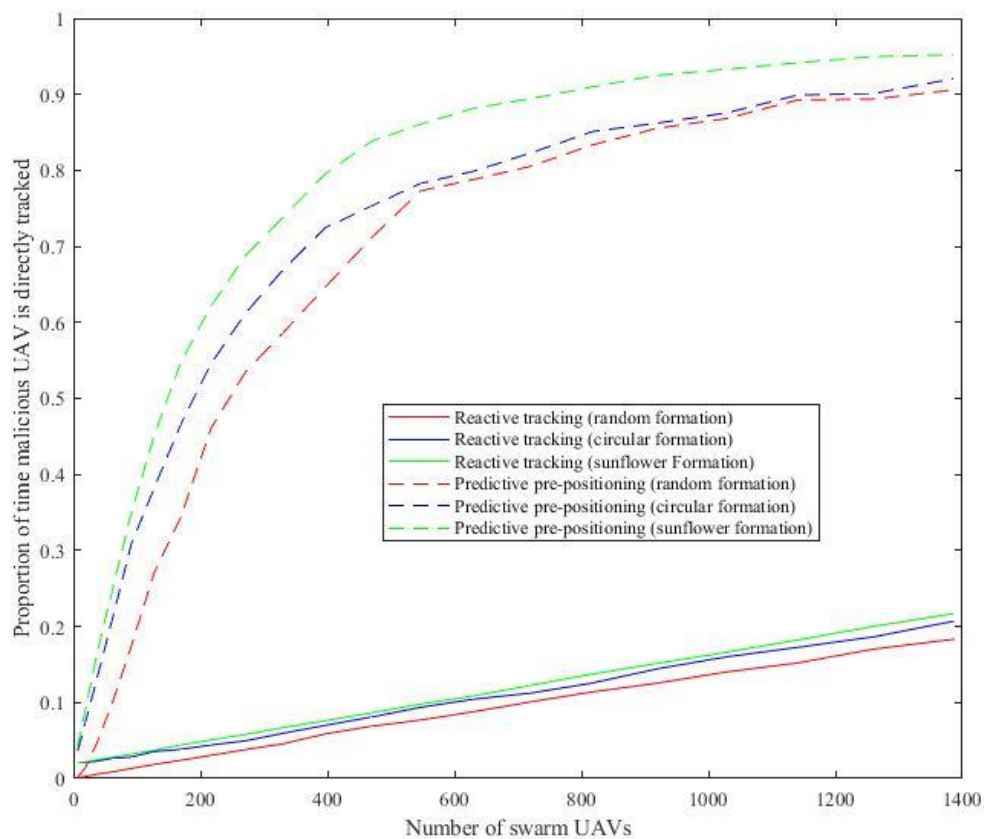


Figure 17. Results for swarm speed $u = 20m/s$.

Proportion Of Time Malicious Drone Is Actively Tracked (Swarm Speed 20m/s)						
Swarm Size	Reactive			Reactive + Predictive Pre-Positioning		
	Random	Circular	Sunflower	Random	Circular	Sunflower
7	0.0010	0.0201	0.0205	0.0023	0.0368	0.0434
19	0.0026	0.0211	0.0221	0.0143	0.0743	0.0905
37	0.0058	0.0229	0.0246	0.0465	0.1310	0.1638
61	0.0086	0.0265	0.0281	0.0985	0.2086	0.2467
91	0.0133	0.0283	0.0321	0.1737	0.3081	0.3489
127	0.0185	0.0355	0.0370	0.2704	0.3816	0.4505
169	0.0240	0.0384	0.0442	0.3434	0.4658	0.5474
217	0.0305	0.0442	0.0507	0.4613	0.5461	0.6218
271	0.0381	0.0496	0.0581	0.5348	0.6120	0.6876
331	0.0458	0.0598	0.0671	0.5870	0.6701	0.7391
397	0.0588	0.0699	0.0760	0.6467	0.7246	0.7956
469	0.0687	0.0808	0.0864	0.7110	0.7530	0.8381
547	0.0769	0.0937	0.0980	0.7731	0.7828	0.8608
631	0.0881	0.1044	0.1088	0.7882	0.7991	0.8819
721	0.1009	0.1124	0.1227	0.8055	0.8231	0.8945
817	0.1139	0.1256	0.1374	0.8334	0.8510	0.9097
919	0.1254	0.1442	0.1514	0.8554	0.8621	0.9251
1027	0.1401	0.1598	0.1659	0.8680	0.8753	0.9328
1171	0.1522	0.1762	0.1823	0.8926	0.8991	0.9416
1261	0.1703	0.1865	0.2003	0.8937	0.9013	0.9497
1387	0.1833	0.2071	0.2171	0.9060	0.9207	0.9522

Table 4. Results of mean of 500 iterations used for plot generation where $u = 20\text{m/s}$, colour coded based on performance.

5.2.2 Swarm Speed 25m/s

It is evident when inspecting Figure 18 and Table 5 that the performance of the reactive tracking strategy is dependent on the capability difference between the swarm drones and the malicious drone, although as expected it again performs poorly overall, there is however a substantial increase in performance than at the lower swarm speed. The random formation sees around an 80% increase at the largest swarm size from 0.1833 to 0.3302, the circular formation is similar with around an 82% increase from 0.2071 to 0.3768, and finally the sunflower formation sees a 95% increase from 0.2171 to 0.4234. Once again, the sunflower formation largely outperforms the benchmark formations, except for the case where the swarm size is equal to 271 drones where the circular formation performed slightly better with 0.1166 compared to 0.1139.

Reactive tracking with predictive pre-positioning again unsurprisingly greatly outperforms reactive tracking only, providing further replication of the benchmark results, the circular formation outperforms the random formation for all possible swarm sizes. The proposed sunflower formation

continues to achieve good results with increases in performance on both benchmark formations at all swarm sizes. The increased swarm speed seems to provide for the most improvement at smaller swarm sizes, with key performance thresholds being hit much earlier than the previous swarm speed setting. For instance, the random formation achieves ≥ 0.5 proportion of time tracked with a 217-drone swarm, for the preceding swarm speed, 271 drones were required. The circular formation utilised only 127 drones compared to the previous requirement of 217, and the sunflower formation reached the threshold with 91 drones, compared to 169. Performance increases at the larger swarm sizes are nowhere near as significant, the sunflower formation at the maximum swarm size of 1387 drones only improved to 0.9547 from 0.9522.

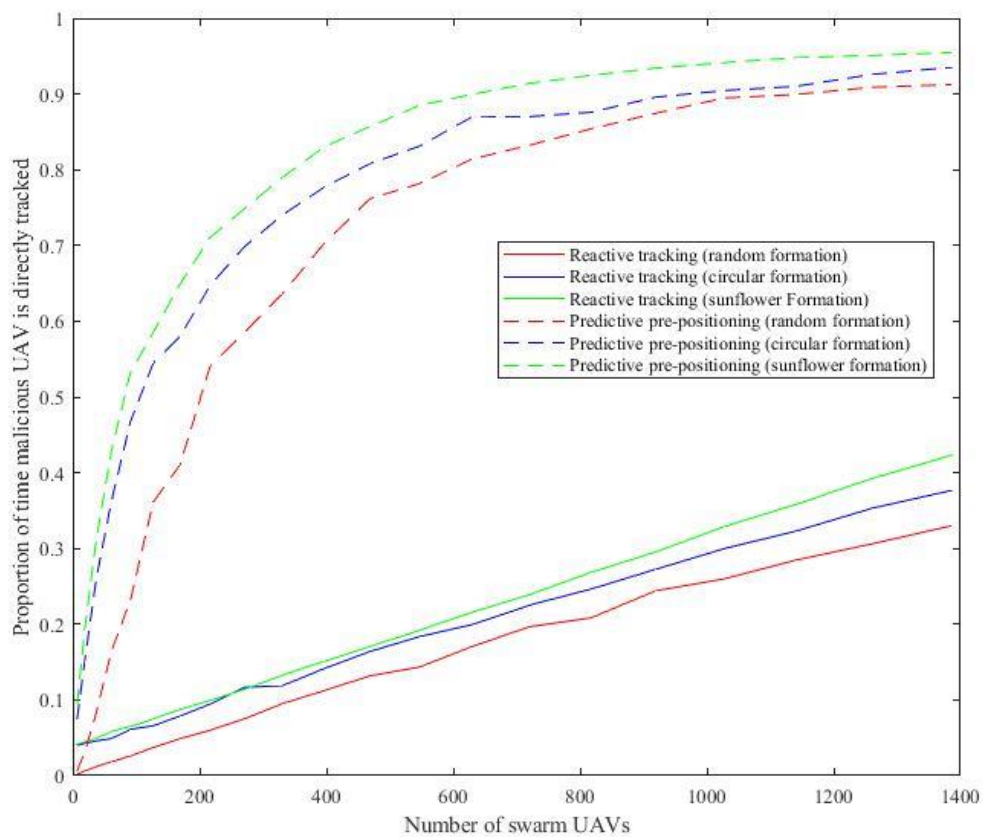


Figure 18. Results for swarm speed $u = 25\text{m/s}$.

Swarm Size	Proportion Of Time Malicious Drone Is Actively Tracked (Swarm Speed 25m/s)					
	Reactive			Reactive + Predictive Pre-Positioning		
	Random	Circular	Sunflower	Random	Circular	Sunflower
7	0.0021	0.0402	0.0414	0.0066	0.0750	0.0941
19	0.0061	0.0426	0.0448	0.0312	0.1518	0.1936
37	0.0119	0.0459	0.0492	0.0825	0.2595	0.3114
61	0.0183	0.0490	0.0584	0.1644	0.3620	0.4286
91	0.0260	0.0611	0.0650	0.2318	0.4675	0.5322
127	0.0372	0.0659	0.0750	0.3612	0.5446	0.5853
169	0.0488	0.0787	0.0873	0.4102	0.5797	0.6488
217	0.0600	0.0947	0.0995	0.5412	0.6476	0.7109
271	0.0752	0.1166	0.1139	0.5852	0.6986	0.7486
331	0.0951	0.1189	0.1327	0.6368	0.7405	0.7901
397	0.1125	0.1415	0.1511	0.7032	0.7772	0.8304
469	0.1319	0.1641	0.1705	0.7619	0.8082	0.8572
547	0.1434	0.1837	0.1921	0.7818	0.8312	0.8849
631	0.1710	0.1997	0.2161	0.8144	0.8704	0.8998
721	0.1967	0.2253	0.2392	0.8325	0.8702	0.9140
817	0.2082	0.2463	0.2684	0.8539	0.8758	0.9246
919	0.2440	0.2724	0.2952	0.8745	0.8957	0.9341
1027	0.2598	0.2996	0.3287	0.8947	0.9045	0.9414
1171	0.2847	0.3231	0.3583	0.8994	0.9102	0.9478
1261	0.3062	0.3531	0.3924	0.9090	0.9259	0.9510
1387	0.3302	0.3768	0.4234	0.9124	0.9353	0.9547

Table 5. Results of mean of 500 iterations used for plot generation where $u = 25\text{m/s}$, colour coded based on performance

5.2.3 Swarm Speed 29m/s

When the discrepancy between swarm and malicious drone capabilities is reduced even further the reactive only strategy starts to become a viable option. Having previously failed to achieve the 0.5 proportion of time actively tracking threshold, all three formations have now achieved the 0.8 threshold by the time swarm size hits 631 drones, this is observable in Figure 19 and Table 6. Once again, the benchmark formations perform as expected with the circular formation besting the random formation, the sunflower formation maintains its form and outperforms them both. The most noteworthy observation for this dataset is that the reactive only strategy coupled with the sunflower formation, outperforms the random and circular formations when they are implementing additional predictive pre-positioning and the swarm size is 817 or greater. This is unprecedented and could provide solutions to specific scenarios where the intra-swarm communication required to implement predictive pre-positioning is not feasible.

Reactive tracking with predictive pre-positioning sees even larger performance improvements at the smaller swarm sizes, with the circular and sunflower formations hitting the 0.5 proportion of time

tracked threshold at swarm sizes of 37 and 19 respectively. The sunflower formation outperforms the benchmark formations for all swarm sizes bar the 37-drone formation, where the circular formation narrowly edges it. It is worth noting that once the swarm size reaches 1027 or greater the sunflower formation almost converges with the reactive only iteration of itself. It is also noteworthy that once again at the larger swarm sizes the performance increases are not very significant over the preceding inferior swarm speeds. Achieving active tracking thresholds within proximity of 0.9 or greater requires similarly sized swarms regardless of the gap in capabilities between the swarm and the malicious drone.

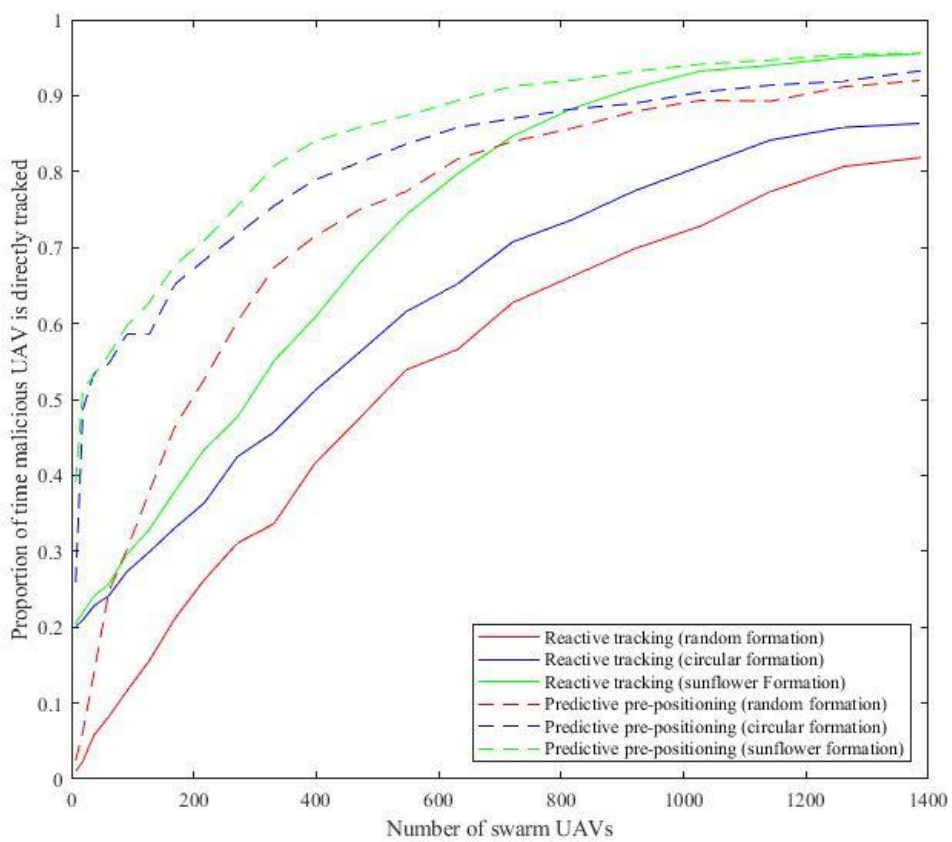


Figure 19. Results for swarm speed $u = 29\text{m/s}$.

Swarm Size	Proportion Of Time Malicious Drone Is Actively Tracked (Swarm Speed 29m/s)					
	Reactive			Reactive + Predictive Pre-Positioning		
	Random	Circular	Sunflower	Random	Circular	Sunflower
7	0.0098	0.2009	0.2056	0.0239	0.2595	0.3911
19	0.0237	0.2096	0.2191	0.0637	0.4871	0.5131
37	0.0579	0.2281	0.2413	0.1394	0.5342	0.5311
61	0.0821	0.2413	0.2565	0.2468	0.5470	0.5585
91	0.1164	0.2733	0.2964	0.3027	0.5862	0.5974
127	0.1554	0.2988	0.3282	0.3775	0.5852	0.6271
169	0.2113	0.3306	0.3791	0.4641	0.6515	0.6769
217	0.2622	0.3635	0.4339	0.5263	0.6831	0.7093
271	0.3106	0.4243	0.4765	0.6023	0.7172	0.7544
331	0.3364	0.4570	0.5507	0.6736	0.7549	0.8076
397	0.4149	0.5111	0.6069	0.7142	0.7887	0.8396
469	0.4738	0.5608	0.6777	0.7490	0.8116	0.8578
547	0.5390	0.6155	0.7433	0.7739	0.8362	0.8735
631	0.5658	0.6523	0.7973	0.8165	0.8582	0.8934
721	0.6275	0.7074	0.8469	0.8397	0.8699	0.9126
817	0.6618	0.7363	0.8825	0.8568	0.8822	0.9200
919	0.6981	0.7743	0.9103	0.8791	0.8896	0.9320
1027	0.7280	0.8069	0.9323	0.8937	0.9044	0.9413
1171	0.7733	0.8413	0.9397	0.8927	0.9137	0.9468
1261	0.8066	0.8582	0.9501	0.9116	0.9190	0.9542
1387	0.8183	0.8633	0.9554	0.9201	0.9327	0.9559

Table 6. Results of mean of 500 iterations used for plot generation where $u = 29\text{m/s}$, colour coded based on performance

5.3 Results Summary

These results have demonstrated a clear replication of the benchmark studies identified within the literature, the superiority of the reactive with predictive pre-positioning tracking strategy over the solely reactive strategy is reproduced, as is the increased performance of the circular formation over the random formation. The faithful reproduction of these results provides the benchmark for this project to evaluate the newly proposed sunflower formation against. The sunflower formation performs exceptionally well, providing increased performance over the benchmark formations for every simulation configuration under test.

The most unexpected result was the performance of the sunflower formation when coupled with reactive tracking only, and with minimal capability mismatch between swarm and malicious drones. For this configuration at certain larger swarm sizes, the reactive only strategy managed to greatly outperform the benchmark formations whilst they were utilising the historically higher performing reactive tracking with predictive pre-positioning strategy. This could present the opportunity to

implement the simpler tracking strategy in specific scenarios where intra-swarm communication is difficult to implement.

A common observation across all three simulation scenarios is that the reactive tracking with predictive pre-positioning strategy seems to generate a similarly shaped curve each time, for smaller swarm sizes there are huge performance gains made for each swarm size increase, this steep plot eventually reaches a knee point and then begins to plateau. This knee point in the data seems to occur at approximately the 0.85 proportion of time threshold, past this point large increases in swarm size are having minimal effect on the performance, perhaps representing a point of near constant returns or diminishing returns. This is easily observable when we look at Table 6, the sunflower formation achieves a performance value of approximately 0.75 with a swarm size of 271 drones, to achieve approximately 0.85 an additional 198 drones are required (469 drones total), however in order to achieve approximately 0.95 an additional 792 drones are required (1261 drones total) when compared to the 0.85 threshold. Additionally, none of the configurations tested or simulations run could produce a maximum performance value ≥ 0.96 , larger swarm sizes or better performing formations may be required to achieve or surpass this threshold.

It can then be determined based on the configurations tested and simulations run that the sunflower formation is the highest performing and most efficient initial flight formation for all applications. When determining the optimal swarm size, the characteristics mentioned above with regard to diminishing returns may play a part, if maximum tracking performance is an essential requirement, then the biggest swarm size should be selected. If there is flexibility on the minimum performance and a score of 0.85 is acceptable for the individual system, then swarm size can be greatly reduced. The capabilities of the swarm drones will also influence the optimal swarm size, designing for a worst-case scenario in relation to a capability mismatch between swarm and malicious drones may be the safest course of action. Applying this to the scenario simulated for this project would mean a system comprising 547 swarm drones, each with a maximum speed of 20m/s, distributed in accordance with the sunflower formation, and implementing reactive tracking with predictive pre-positioning. This would achieve a performance score of 0.85 whilst tracking a malicious drone with a top speed of 30m/s.

Chapter 6

6. Conclusions and Further Work

6.1 Conclusions

This project sought to further examine the optimal initial swarm size and formation required to achieve increased performance of tracking a high capability malicious drone. A performance benchmark was adopted from studies identified within the literature review, utilising the methodologies applied within these studies allowed for an equitable comparison. The results of this project would determine whether the flight formation proposed would outperform those used in the benchmarking studies, and therefore contribute to an improved benchmark for tracking performance. The swarm performance was tested for multiple iterations at multiple configurations in order to provide a sufficiently large sample size, the results of 500 unique iterations for each configuration are then averaged, providing the final output.

The performance of each configuration is determined via this output, which represents the proportion of time that the malicious drone is actively tracked by one or more swarm drones whilst within the tracking area. Multiple assumptions were made with regard to the simulation environment, this was partially to maintain the methodology of the benchmark research as well as to reduce complexity whilst increasing the scope of the project within the available time frame. These assumptions remove many real-world characteristics that may otherwise have been used to aid in selection of optimal system arrangements. However, when solely evaluating the performance of the flight formations at different swarm sizes, it is sufficient to mirror previously used methodologies to document performance increases.

The analysis of the simulation output at the three different maximum swarm speed values (20m/s, 25m/s, 29m/s) yielded several important results. Firstly, the benchmark results were replicated with reactive tracking with predictive pre-positioning outperforming reactive tracking on its own for the random and circular formations at all three swarm speeds. Secondly, the newly proposed sunflower formation was successfully evaluated against these benchmark results, where it was found to outperform both benchmark formations for all swarm speeds, at all swarm sizes, and with both tracking strategies being implemented. This is a significant result as any increase in active tracking time increases the chances that the malicious drone and/or its operator can be identified at its origin and therefore mitigate any further malicious incursions on the tracking area under surveillance.

These performance improvements are not limited strictly to the achieved tracking time values, but also affect some of the input variables, for instance at all swarm speeds the sunflower formation will hit performance thresholds whilst utilising smaller swarm sizes than the benchmark formations. These factors all contributed to the sunflower formation being deemed the highest performing and most efficient initial flight formation. Theoretically the optimal swarm size is as large as possible, however realistically the swarm size is dictated by the proposed performance of the system and the speed of the malicious drone, which is of course unknown prior to detection. The optimal swarm size in the simulation environment and results was found to be a 547-drone swarm, as detailed in Chapter 5.

Initially it appeared that the optimal tracking strategy was consistent with previous work, as in the literature reactive tracking with predictive pre-positioning had universally outperformed reactive tracking only. This was largely replicated until the final simulation run where the swarm drones' capabilities were much more closely matched to the malicious drone (29m/s to 30m/s). For these values the reactive strategy when coupled with the sunflower formation actually outperformed the benchmark formations for swarm sizes of 817 drones and above, where the benchmark formations were implementing the additional predictive pre-positioning tracking strategy. This unprecedented result means that reactive tracking could still provide a viable alternative in specific scenarios where intra-swarm communication may not be possible in order to facilitate predictive pre-positioning or where the hardware and software being used cannot implement the more complex code required.

This project has replicated historical results identified within the literature and successfully used them as a benchmark to evaluate a new initial formation. Consequently, this makes an important contribution to the research by establishing a new performance benchmark. An optimal configuration for the simulation environment is proposed and this is complemented by discussion of potentially optimal configurations for other simulation environments. In combination the project outcomes and discussion contribute to the development of tools to assist with developing specifications for any potential real-world implementation.

6.2 Further Work

There is a range of potential future works that could be based either directly or indirectly on this research. Three additional initial formations were considered for inclusion in this project, alongside the sunflower formation and the two benchmark formations, these proposed formations are detailed in Chapter 3 Section 3.3 and could be simulated using the sunflower formation as a benchmark to determine potentially further increases in performance.

The premise of expanding the scope from the 2D plane to the 3D plane is a necessary step for providing data that is more applicable to the real world, modification of the current simulation environment would most likely accommodate this, however the simulation environment as it stands already takes approximately 16 hours per run, so a more efficient test environment may need to be developed rather than retrofitting the existing test environment. Transitioning to a 3D simulation environment would allow some of the assumptions made for the project to be removed and collision avoidance and terrain could be introduced, bringing more real-world characteristics into the environment.

An example of further assumptions that could be removed would be if further research into malicious drone detection methods could provide for a more detailed implementation of malicious drone detection, removing the assumption of 100% accuracy and introducing some error will most likely provide a more realistic result. Investigation into removal of any of the assumptions made within Chapter 4 Sub-Section 4.1.1 of this project could provide important future work that help to create a more realistic and complete model.

In relation to the malicious drone, a more varied flight path and/or the implementation of evasive tactics presents a possible research area. The implementation of multiple malicious drones within the tracking area at one time would be another worthwhile variable to explore. A combination of any or all of these malicious drone characteristics would again help to increase the realism of the simulation and subsequently the results, whilst also increasing the scope.

The ultimate goal of these simulation configurations is to provide tools to assist in the development of real-world drone swarms to further assess performance, and ultimately, to allow drone swarms to be deployed effectively and efficiently to mitigate the real-world risks posed by malicious drones.

References

- Arnold, C & Brown, J 2020, 'Performance Evaluation for Tracking a Malicious UAV using an Autonomous UAV Swarm', *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0707-12.
- Autel 2017, *EVO II specification*, viewed 12/10/2021, <<https://auteldrones.com/pages/evo-ii-specification>>.
- Bateman, J 2017, *China drone maker DJI: Alone atop the unmanned skies*, CNBC, viewed 22/03/2021, <<https://www.cnbc.com/2017/09/01/in-race-to-dominate-drone-space-west-is-no-match-for-chinas-dji.html>>.
- Brown, J & Raj, N 2021a, 'Predictive Tracking of a High Capability Malicious UAV', *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0747-52.
- Brown, J & Raj, N 2021b, 'The Impact of Initial Swarm Formation for Tracking of a High Capability Malicious UAV', *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1-6.
- Brust, MR, Danoy, G, Bouvry, P, Gashi, D, Pathak, H & Gonçalves, MP 2017, 'Defending Against Intrusion of Malicious UAVs with Networked UAV Defense Swarms', *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 103-11.
- CASA 2021, *Drones*, viewed 28/07/2021, <<https://www.casa.gov.au/drones>>.
- Chavers, M 2018, *Consumer Drones By the Numbers in 2018 and Beyond*, Web Page, News Ledge, viewed 22/03/2021, <<https://www.newsledge.com/consumer-drones-2018-numbers/>>.
- Cheng, H, Page, J & Olsen, J 2013, 'Cooperative control of UAV swarm via information measures', *International Journal of Intelligent Unmanned Systems*, vol. 1, no. 3, pp. 256-75.
- DJI 2015, *New Phantom 3 and Inspire 1 Intelligent Flight Modes*, viewed 7/04/21, <<https://forum.dji.com/thread-30363-1-1.html>>.
- DJI 2021, *DJI - Official Website*, viewed 12/10/2021, <<https://www.dji.com/au>>.
- FAA 2021, *UAS Remote Identification Overview*, Web Page, viewed 28/07/2021, <https://www.faa.gov/uas/getting_started/remote_id/>.
- Friese, L, Jenzen-Jones, NR & Smallwood, M 2016, *Emerging Unmanned Threats: The use of commercially-available UAVs by armed non-state actors*, Armament Research Services, Perth, Australia, <<https://armamentresearch.com/wp-content/uploads/2016/02/ARES-Special-Report-No.-2-Emerging-Unmanned-Threats.pdf>>.
- Giones, F & Brem, A 2017, 'From toys to tools: The co-evolution of technological and entrepreneurial developments in the drone industry', *Business Horizons*, vol. 60, no. 6, pp. 875-84.

Guerra, A, Dardari, D & Djuric, PM 2020, 'Dynamic Radar Networks of UAVs: A Tutorial Overview and Tracking Performance Comparison With Terrestrial Radar Networks', *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 113-20.

Hambling, D 2020, *Dozens More Mystery Drone Incursions Over U.S. Nuclear Power Plants Revealed*, Forbes, Forbes, viewed 17/04/2021, <<https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/?sh=4fd013c26296>>.

Jackman, A 2019, 'Consumer drone evolutions: trends, spaces, temporalities, threats', *Defense & Security Analysis*, vol. 35, no. 4, pp. 362-83.

Koohifar, F, Guvenc, I & Sichitiu, ML 2018, 'Autonomous Tracking of Intermittent RF Source Using a UAV Swarm', *IEEE Access*, vol. 6, pp. 15884-97.

Ma'sum, MA, Jati, G, Arrofi, MK, Wibowo, A, Mursanto, P & Jatmiko, W 2013, 'Autonomous quadcopter swarm robots for object localization and tracking', *MHS2013*, pp. 1-6.

Michaelides-Mateou, S 2016, 'The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives', in B Custers (ed.), vol. 27, ch Chapter 8: Terrorism and National Security, pp. 159-60.

Osborne, C 2020, 'Researchers learn how to pinpoint malicious drone operators', *Zero Day*, 07/07/2020, viewed 20/04/2021, <<https://www.zdnet.com/article/researchers-learn-how-to-pinpoint-malicious-drone-operators/>>.

Pozniak, M & Ranganathan, P 2019, 'Counter UAS Solutions Through UAV Swarm Environments', *2019 IEEE International Conference on Electro Information Technology (EIT)*, pp. 351-6.

Seitz, P 2015, 'Commercial Drone Sales Set To Soar', *Investor's business daily*.

Sprague, EO & Perritt, HH, Jr. 2016, *Domesticating Drones : The Technology, Law, and Economics of Unmanned Aircraft : The Technology, Law, and Economics of Unmanned Aircraft*, CRC Press LLC, London, UNITED KINGDOM.

Topham, G 2019, *Gatwick drone disruption cost airport just £1.4m*, The Guardian, viewed 18/04/2021, <<https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m>>.

Turak, N 2019, *Saudi stock market dives, crude futures to jump after drone attack on oil plants*, CNBC, CNBC, viewed 19/04/2021, <<https://www.cnbc.com/2019/09/15/saudi-stock-market-dives-crude-to-jump-after-attack-on-oil-plants.html>>.

UVify 2018, *OOri - UVify Store*, viewed 12/10/2021, <<https://store.uvify.com/collections/oori/products/oori>>.

Wang, X, Tan, G, Dai, Y, Lu, F & Zhao, J 2020, 'An Optimal Guidance Strategy for Moving-Target Interception by a Multirotor Unmanned Aerial Vehicle Swarm', *IEEE Access*, vol. 8, pp. 121650-64.

Yuneeec 2021, *Typhoon H3 Info* – *Yuneeec*, viewed 12/10/2021, <<https://us.yuneeec.com/typhoon-h3/info/#specs>>.

Appendix A Project Specification

ENG4111/4112 Research Project

Project Specification

For: Joshua Carter
Title: Drone Swarm Simulation for Tracking High Capability Malicious Drone
Major: Electrical and Electronic Engineering
Supervisors: Dr. Jason Brown
Enrollment: ENG4111 – EXT S1, 2021
ENG4112 – EXT S2, 2021
Project Aim: To determine by simulation, the optimal drone placement and initial swarm formations to achieve increased high capability malicious drone tracking performance.

Programme: Version 1, 17th March 2021

1. Complete initial background research on the history and increasing prevalence of commercially available drones.
2. Conduct a comprehensive literature review into the threat posed by high capability malicious drones, passive tracking of high capability malicious drones using surveillance swarms, reactive tracking, predictive pre-positioning, initial swarm formations, drone placement and surveillance swarm simulations.
3. Develop a surveillance swarm simulation environment utilizing MATLAB.
4. Investigate and determine the optimal drone placement to ensure uniform spacing with regards to the high capability malicious drones predicted trajectory.
5. Investigate and determine the optimal swarm formation via simulation of a range of potential formations.
6. Collate, assess, and compare data from simulations to determine any improvements against performance criteria.
7. Make recommendations regarding the most efficient and high performing swarm formation, spacing and size combination.

If time and resource permit:

8. *Expand scope of simulations from the 2D plane into the 3D plane.*
9. *Expand scope of simulations to include multiple high capability malicious drones.*

Appendix C Project Resources

Required Resources

To ensure the project successfully achieves the proposed objectives a number of resources will be required. The largest resource requirement will be the investment of time, additional resources include access to various computer hardware and software.

In terms of student time resources, the specification for ENG4111/4112 lists a total student workload of approximately 310 hours, this will be assumed as the minimum amount of time required to undertake the project. This figure will encompass all phases of the project through planning and investigation, construction of computer simulations, running of simulations, analysing, and interpreting data, communicating with supervisors, and completing the preliminary and final dissertation reports.

This project will be completed alongside additional coursework being undertaken and the student will need to ensure proper allocation of time to ensure the project is completed satisfactorily.

Required software and equipment is detailed in the following table:

Item	Quantity	Source	Cost
Microsoft Word	1	Student	Owned
Microsoft Excel	1	Student	Owned
PC with Microsoft Windows	1	Student	Owned
MATLAB with appropriate toolboxes	1	Student	Owned
Miscellaneous stationery items	Various	Student	\$100 maximum

Table 8. Project Resources

Appendix D Risk Assessment

At the project specification stage, it was noted that no risk assessment or ethics application are required due to the nature of this project being entirely conducted through simulation. Instead, the risks to the project were related to the possibility of missed deadlines on the project timeline and the subsequent insufficient level of new research this may result in. An additional risk that was considered and mitigated was that of equipment failure and subsequent data loss or corruption.

To mitigate the instance where project timeline deadlines were missed one proposed formation was integrated into the simulation environment at a time, with full characterisation required before attempting to integrate another, ensuring some level of new research is obtained.

To mitigate equipment failure and data loss, the entire project folder including the MATLAB path folder were routinely copied to a second location on iCloud.

Appendix E MATLAB Simulation Code

```
% Drone Swarm Simulation for Tracking High Capability Malicious Drone
%
% Simulation code developed using sample code provided by Project
% Supervisor: Dr Jason Brown.
%
%
% 02/08/2021

% Reset Workspace
clc;
clear;

% Toggle Simulation Animation
ANIMATION=0;

% Set Simulation Variables
FIELD_RADIUS = 15000; % m
MAX_TRACK_DISTANCE = 100; % m
NUMBER_ITERATIONS = 500;
MUAV_STEP = 1; % Simulation Step Interval 1m
u=29; % Swarm UAV speed m/s
v=30; % Malicious UAV speed m/s

% Initialize random number generator
rng('shuffle');

% Specify total number of UAV's in swarm formation
numberOfSwarmUAVs= [7, 19, 37, 61, 91, 127, 169, 217, 271, 331, 397,...
    469, 547, 631, 721, 817, 919, 1027, 1141, 1261, 1387];
% Specify number of swarm rings (circular formation only)
numberOfSwarmRings=[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,...
    12, 13, 14, 15, 16, 17, 18, 19, 20, 21];

% Small data set for testing purposes
%numberOfSwarmUAVs= 61;
%numberOfSwarmRings=4;

% plotInstance 1: reactive mobility of individual swarm UAVs - random
% positioning
% plotInstance 2: reactive mobility of individual swarm UAVs - circular
% positioning
% plotInstance 3: reactive mobility of individual swarm UAVs + proactive
% mobility based upon networking - random positioning
% plotInstance 4: reactive mobility of individual swarm UAVs + proactive
% mobility based upon networking - circular positioning
% plotInstance 5: reactive mobility of individual swarm UAVs - sunflower
% positioning
% plotInstance 6: reactive mobility of individual swarm UAVs + proactive
% mobility based upon networking - sunflower positioning

% Begin Test loop
for plotInstance=1:6

    meanProportionInRangeOverAllIterations=zeros...
```

```

(length(numberOfSwarmUAVs),1);

for numberOfSwarmUAVsIndex=1:length(numberOfSwarmUAVs)

    countInRangeForOneIteration = zeros(NUMBER_ITERATIONS,1);

    for iteration=1:NUMBER_ITERATIONS

        % set up initial positions of swarm UAVs

        if plotInstance == 1 || plotInstance == 3
            % random formation
            swarmUAVPosMagnitude=FIELD_RADIUS*sqrt(rand...
                (numberOfSwarmUAVs(numberOfSwarmUAVsIndex),1));
            swarmUAVPosAngle=2*pi*rand(numberOfSwarmUAVs...
                (numberOfSwarmUAVsIndex),1);
            swarmUAVPosX=swarmUAVPosMagnitude.*cos(swarmUAVPosAngle);
            swarmUAVPosY=swarmUAVPosMagnitude.*sin(swarmUAVPosAngle);
        elseif plotInstance == 2 || plotInstance == 4
            % circular formation
            randPosAngle=2*pi*rand;
            swarmUAVPosMagnitude = zeros(numberOfSwarmUAVs...
                (numberOfSwarmUAVsIndex),1);
            swarmUAVPosAngle = zeros(numberOfSwarmUAVs...
                (numberOfSwarmUAVsIndex),1);
            uavIndexAbsolute=2;
            for ring=1:numberOfSwarmRings(numberOfSwarmUAVsIndex)
                NUMBER_OF_UAVS_IN_RING = (6*ring);
                for uavIndexInRing=1:NUMBER_OF_UAVS_IN_RING
                    swarmUAVPosMagnitude(uavIndexAbsolute)=...
                        FIELD_RADIUS*ring/numberOfSwarmRings...
                            (numberOfSwarmUAVsIndex);
                    swarmUAVPosAngle(uavIndexAbsolute)=randPosAngle...
                        + 2*pi*uavIndexInRing/NUMBER_OF_UAVS_IN_RING;
                    uavIndexAbsolute=uavIndexAbsolute+1;
                end
            end

            swarmUAVPosX=swarmUAVPosMagnitude.*cos(swarmUAVPosAngle);
            swarmUAVPosY=swarmUAVPosMagnitude.*sin(swarmUAVPosAngle);
        else
            % sunflower formation
            swarmUAVPosMagnitude = zeros(numberOfSwarmUAVs...
                (numberOfSwarmUAVsIndex),1);
            swarmUAVPosAngle = zeros(numberOfSwarmUAVs...
                (numberOfSwarmUAVsIndex),1);
            goldenratio = (sqrt(5)+1)/2;
            randPosAngle=2*pi*rand;
            uavIndexAbsolute=2; % Change for UAV at center or not
            for k=1:numberOfSwarmUAVs(numberOfSwarmUAVsIndex)- 1
                boundaryPoints = round(sqrt(k));
                swarmUAVPosMagnitude(uavIndexAbsolute) = ...
                    FIELD_RADIUS*(sqrt(k-1/2)/sqrt(numberOfSwarmUAVs...
                        (numberOfSwarmUAVsIndex)-(boundaryPoints+1)/2));
                swarmUAVPosAngle(uavIndexAbsolute) = randPosAngle...
                    + 2*pi*k/goldenratio^2;
                swarmUAVPosX=swarmUAVPosMagnitude.*cos...
                    (swarmUAVPosAngle);
                swarmUAVPosY=swarmUAVPosMagnitude.*sin...
                    (swarmUAVPosAngle);
            end
        end
    end
end

```

```

        uavIndexAbsolute=uavIndexAbsolute+1;
    end

end

oldSwarmUAVInRange = zeros(numberOfSwarmUAVs...
    (numberOfSwarmUAVsIndex),1);
theta = zeros(numberOfSwarmUAVs(numberOfSwarmUAVsIndex),1);
phi = zeros(numberOfSwarmUAVs(numberOfSwarmUAVsIndex),1);

mUAVDetected = false;

count=0;

% move malicious UAV across field
for mUAVPosX=-FIELD_RADIUS:MUAV_STEP:FIELD_RADIUS
    distance = sqrt((swarmUAVPosX - mUAVPosX).^2 +...
        swarmUAVPosY.^2);
    minDistance = min(distance);
    if min(distance) <= MAX_TRACK_DISTANCE
        count=count+1;
        mUAVDetected = true;
    end

% identify swarm UAVs that have just come into range and
% calculate their theta values

swarmUAVInRange = distance <= MAX_TRACK_DISTANCE;
newSwarmUAVInRange = swarmUAVInRange &...
    ~oldSwarmUAVInRange;
phi(newSwarmUAVInRange) = atan(-swarmUAVPosY...
    (newSwarmUAVInRange)./(swarmUAVPosX...
    (newSwarmUAVInRange) - mUAVPosX));

theta(newSwarmUAVInRange) = acos(2*u*v.*sin(phi...
    (newSwarmUAVInRange))./sqrt...
    (u^4+v^4-2*(u^2)*(v^2).*cos(2.*phi...
    (newSwarmUAVInRange)))-atan((v^2-u^2)./...
    ((u^2+v^2).*tan(phi(newSwarmUAVInRange)))));
%adjustment for negative phi angles
theta(theta > pi/2) = theta(theta > pi/2) - pi;

oldSwarmUAVInRange = swarmUAVInRange;

% move swarm UAVs that are in range of malicious UAV
swarmUAVPosX(swarmUAVInRange) = swarmUAVPosX...
    (swarmUAVInRange) +...
    (u/v)*MUAV_STEP.*cos(theta(swarmUAVInRange));
swarmUAVPosY(swarmUAVInRange) = swarmUAVPosY...
    (swarmUAVInRange) + (u/v)*MUAV_STEP.*sin...
    (theta(swarmUAVInRange));

if ANIMATION == 1 && mod(mUAVPosX, 1000) == 0
    scatter(swarmUAVPosX, swarmUAVPosY, 'x');
    xlim([-FIELD_RADIUS, FIELD_RADIUS]);
    ylim([-FIELD_RADIUS, FIELD_RADIUS]);
    set(gca, 'XAxisLocation', 'origin',...
        'YAxisLocation', 'origin');
    daspect([1 1 1]);
end

```

```

        hold on;
        plot(mUAVPosX,0,'ro');
        hold off;
        drawnow;
    end

    if plotInstance == 3 || plotInstance == 4 ||...
        plotInstance == 6
        % move other swarm UAVs towards the mUAV trajectory
        % unless they are already on it
        if mUAVDetected
            swarmUAVPositiveYAndNotInRange =...
                ~swarmUAVInRange & swarmUAVPosY > 0;
            swarmUAVPosY(swarmUAVPositiveYAndNotInRange) =...
                swarmUAVPosY(swarmUAVPositiveYAndNotInRange)...
                -(u/v)*MUAV_STEP;
            swarmUAVNegativeYAndNotInRange =...
                ~swarmUAVInRange & swarmUAVPosY < 0;
            swarmUAVPosY(swarmUAVNegativeYAndNotInRange) =...
                swarmUAVPosY(swarmUAVNegativeYAndNotInRange)...
                +(u/v)*MUAV_STEP;
        end
    end
end

countInRangeForOneIteration(iteration)=count;

end
meanProportionInRangeOverAllIterations(numberOfSwarmUAVsIndex)=...
    mean(countInRangeForOneIteration)*MUAV_STEP/(2*FIELD_RADIUS);

    %histogram(countInRange,'Normalization','probability','BinWidth',
2*MAX_TRACK_DISTANCE);

end
if plotInstance == 1
    plot1 = meanProportionInRangeOverAllIterations;
elseif plotInstance == 2
    plot2 = meanProportionInRangeOverAllIterations;
elseif plotInstance == 3
    plot3 = meanProportionInRangeOverAllIterations;
elseif plotInstance == 4
    plot4 = meanProportionInRangeOverAllIterations;
elseif plotInstance == 5
    plot5 = meanProportionInRangeOverAllIterations;
elseif plotInstance == 6
    plot6 = meanProportionInRangeOverAllIterations;
end

end

plot(numberOfSwarmUAVs', plot1,'-r', numberOfSwarmUAVs', plot2,'-b',...
    numberOfSwarmUAVs', plot5,'-g', numberOfSwarmUAVs', plot3,'--r',...
    numberOfSwarmUAVs', plot4,'--b',numberOfSwarmUAVs', plot6,'--g');
set(gca, 'FontName', 'Times New Roman')
xlabel('Number of swarm UAVs');
ylabel('Proportion of time malicious UAV is directly tracked');

```



```
ylim([0,1]);  
legend({'Reactive tracking (random formation)',...  
      'Reactive tracking (circular formation)',...  
      'Reactive tracking (sunflower Formation)',...  
      'Predictive pre-positioning (random formation)',...  
      'Predictive pre-positioning (circular formation)',...  
      'Predictive pre-positioning (sunflower formation)'},...  
      'Location', 'southeast')
```

Appendix F Unimplemented Formation Codes

```
% Generate square lattice

x = -100:10:100;
y = -100:10:100;

[X,Y] = meshgrid(x,y);

plot(X,Y, '*r');

% Triangular Lattice
% Equilateral Triangle

close all
clear;

horz = 5; % triangle base length
vert = sqrt(horz^2-(horz/2)^2); % triangle vertical height

% X,Y Limits
xlim = 100;
ylim = 100;

% Generate triangular lattice
trilattice = [];
previous_y = 0;
x = 0;
offset = 0;
while previous_y < ylim
    if offset == 0
        x = [0:horz:xlim]';
        y = ones(length(x), 1)*previous_y;
        offset = 1;
    else
        x = [horz/2:horz:xlim]';
        y = ones(length(x), 1)*previous_y;
        offset = 0;
    end
    trilattice = [trilattice; [x,y]];
    previous_y = previous_y + vert;
end
%centre about (0,0)
trilattice = bsxfun(@minus, trilattice, max(trilattice)./2);
% Plot
figure()
plot(trilattice(:,1), trilattice(:,2), '*r');
grid on;

% Generate hexagonal lattice

radius = 1;
apothem = radius*sqrt(3) / 2;

[x y] = meshgrid(0:1:41);
```

```
n = size(x,1);  
x = apothem * x;  
y = y + repmat([0 0.5],[n,n/2]);  
  
% Plot  
[xx yy] = voronoi(x(:),y(:)); plot(xx,yy,'*R')  
axis equal, axis([10 20 10 20]), zoom on
```