Machine Learning Based Spectrum Fingerprinting of Drones for Defensive Cyber Operations

Citation

Permanent link
https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374978

Terms of Use
This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story
The Harvard community has made this article openly available. Please share how this access benefits you. Submit a story.

Accessibility
Machine Learning Based Spectrum Fingerprinting of Drones for Defensive Cyber Operations

Abir Ray

A Thesis in the Field of Software Engineering for the Degree of Master of Liberal Arts

Harvard University

May 2023
Abstract

The rapid development of unmanned aerial vehicle (UAV) or drone capabilities in the past decade has significantly expanded the commercial, military, and consumer applications for these innovative airborne devices. Characterized by fixed wings or multiple rotors, drones are valued for their long-range flight, their lightweight design, and their imaging and sensory capabilities. Traditionally operated by radio controllers on dedicated channels, modern drones are evolving towards autonomous, machine-controlled swarms of tactical UAVs that are capable of fulfilling an array of complex purposes. However, due to the size and relatively limited battery power of these devices, the computing capabilities and onboard software embedded in these functional tools remain extremely limited. As a growing number of malicious actors seek to disrupt, hijack, and misdirect drone flight paths, the challenge of securing drones is an important academic problem. From drone hijacking to denial of service (DoS) to signal interference, the common techniques for affecting drone flight reliability are simple, high-powered, and widely available to the general public. The current study analyzes the relationship between drone risk management capabilities and the opportunities afforded by trained machine learning models. This study demonstrates
the viability of algorithmic in-flight data monitoring and security threat detection for future onboard applications by applying a Python-based semi-supervised training set to several machine learning solutions. Further extension of these findings to swarm-based, multi-drone fingerprinting and flight monitoring demonstrates the potential for networked threat identification and security management. Ultimately, these findings propose a novel model that incorporates both onboard and offline machine learning capabilities into a shield-based software solution that can detect and respond to flight anomalies and changing threat patterns of malicious actors.
Acknowledgements

I would like to thank my partner, Danielle Letourneau, who’s support and encouragement were essential for the completion of this thesis. And a special thanks to my thesis advisor, Dr. Hongming Wang, who aided me substantially in the direction and creation of this research.
Contents

Chapter I: Introduction

1.1 Research Background .............................................. 1
1.2 Research Rationale ............................................... 5
1.3 Research Objectives ............................................. 8
1.4 Research Questions ............................................... 9
1.5 Definition of Key Terms ......................................... 10

Chapter II: Related Works

2.1 Drone Flight Management ......................................... 13
2.2 Swarms and Flocking for UAVs ................................. 16
2.3 Risk Assessment and Drone Operations ......................... 19
2.4 Denial of Service (DoS) Attacks ............................... 25
2.5 Hijacking and GPS Spoofing .................................... 28
2.6 Intrusion Detection Systems for Drone Monitoring ........... 32
2.7 Machine Learning and Drone Flight Continuity Analysis .... 36
2.8 Conceptual Framework ........................................... 43
2.9 Summary .......................................................... 47
Chapter III: Methodology

3.1 Introduction ............................................. 48
3.2 Experimental Design ..................................... 48
3.3 Algorithms, Models and Computing ...................... 51
3.4 Data Analysis ............................................ 57
3.5 Limitations and Challenges ............................ 61
3.6 Summary ............................................... 62

Chapter IV: Results

4.1 Introduction ............................................ 63
4.2 Dataset ................................................ 64
  4.2.1 Time Series and State Signal ..................... 64
4.3 Drone Flight Logs Analysis ............................ 69
4.4 Model Design Stages and Classifier Selection .......... 80
4.5 Machine Learning Analysis ............................ 88
4.6 Swarm Modeling and Drone Fingerprinting ............ 93
4.7 Summary ............................................... 100

Chapter V: Discussion and Analysis

5.1 Introduction ............................................ 101
5.2 Findings and Practical Implications .................. 102
5.3 Risk Assessment and Drone Security .................. 108
5.4 DoS and UAV Hijacking ............................... 113
# List of Figures

1. Reynolds Flocking in Action (Source: Hambling, 2021) .................. 18
2. Three-Dimensional Risk Modeling for Drone Operations (Adapted From: Tubis et al., 2021) ................................................................. 21
3. Breakdown of the TXT File Structure (Source: Clark et al., 2017, S8) 24
4. Example of a Drone Hijacking Attack (Source: Feng et al., 2020, 2) 30
5. Conceptual Framework ................................................................. 46
6. Breakdown of a DJI DAT File Structure (Source: Clark et al., 2017, S9) 52
7. Various Gaussian Distributions with a Difference in Mean and Variance (Source: Singh, 2019, 1) ................................................................. 55
8. DatCon User Interface (Source: DatCon, 2020) ........................... 65
9. Fields Included in Drone Flight Log Output .................................... 69
10. Flight Nave Health 05 ................................................................. 70
11. Multivariate Representation of Normative Patterns in Flight 05 ...... 71
12. Flight Nav Health 28 ................................................................. 72
13. Multivariate Representation of Aberrant Patterns in Flight 28 ...... 73
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Overlay of Flight Nav Health and Motor Speed</td>
<td>74</td>
</tr>
<tr>
<td>15</td>
<td>Overlay of Flight Nav Health and Motor Speed</td>
<td>75</td>
</tr>
<tr>
<td>16</td>
<td>Nav Health, Height, Lat, Long, and GPS Dirsuption Flight</td>
<td>76</td>
</tr>
<tr>
<td>17</td>
<td>Geolocation Route for Drone Flight</td>
<td>77</td>
</tr>
<tr>
<td>18</td>
<td>Flight Disruption Model Flight</td>
<td>78</td>
</tr>
<tr>
<td>19</td>
<td>DoS Attack and Flight Disruption Flight</td>
<td>79</td>
</tr>
<tr>
<td>20</td>
<td>Key Variation Report Data from Flight</td>
<td>80</td>
</tr>
<tr>
<td>21</td>
<td>Procedural Design of GMM and Machine Learning Analysis</td>
<td>82</td>
</tr>
<tr>
<td>22</td>
<td>K-Means Flight Path Clustering by Distance Traveled</td>
<td>83</td>
</tr>
<tr>
<td>23</td>
<td>K-Means Pitch vs Controller Throttle Analysis</td>
<td>84</td>
</tr>
<tr>
<td>24</td>
<td>GMM Pitch vs Controller Throttle Analysis</td>
<td>85</td>
</tr>
<tr>
<td>25</td>
<td>Pitch vs Roll In-Flight Trajectory Clusters K-Means</td>
<td>86</td>
</tr>
<tr>
<td>26</td>
<td>Pitch vs Roll in-Flight Trajectory Clusters GMM</td>
<td>87</td>
</tr>
<tr>
<td>27</td>
<td>Core Flight Path Classifiers</td>
<td>88</td>
</tr>
<tr>
<td>28</td>
<td>Comparison of Machine Learning Classifiers (Detection)</td>
<td>90</td>
</tr>
<tr>
<td>29</td>
<td>Comparison of Machine Learning Classifiers (Combined Execution)</td>
<td>91</td>
</tr>
<tr>
<td>30</td>
<td>Max Depth Effects in RF Classifier</td>
<td>92</td>
</tr>
<tr>
<td>31</td>
<td>Estimator Effects in RF Classifier</td>
<td>93</td>
</tr>
<tr>
<td>32</td>
<td>DJI Phantom 4 Underside Interior (Source: Watson, 2022, p.13)</td>
<td>95</td>
</tr>
<tr>
<td>33</td>
<td>Swarm Flocking Optimisation Model with Machine Learning Integration</td>
<td>99</td>
</tr>
<tr>
<td>34</td>
<td>DoS Attack</td>
<td>104</td>
</tr>
</tbody>
</table>
Chapter I.

Introduction

1.1. Research Background

In today’s digitally connected world, various industries and applications are integrating into their service provisions. Due to their relatively low cost, speed, dexterity, and flexibility, the applications for drones are diversifying exponentially. Drones, or Unmanned Aerial Vehicles (UAVs), are even being considered for use in a variety of e-commerce and critical service deliveries. In their current lifecycle phase, drones are commonly deployed to conduct aerial video surveillance, monitor wide swaths of geographic territory, and observe naturally occurring environmental phenomena (Feng et al., 2015). As innovative applications such as medical, military, and social services are considered, the critical role of drone functionality and continuity in service deliveries influences their fulfillment of exacting and consistent service objectives (Zibaei et al., 2018). Alternatively, as defense-based applications are developed, various military and defense agencies are using drones for Electromagnetic Battle Management (EMBM) purposes, covering communications (Spectrum Management), jamming (Electronic Warfare) and signal collections (Intelligence) (Vacca and Onishi,
Therefore, drones are broadly considered by both governmental and commercial sectors as normalized occupiers of a densely populated collective airspace. With applications across critical governmental and commercial services, the future of drones is inexorably linked to the security and stability of the networks in which they operate. As a result of remote, autonomous, and wireless control solutions, both individual and drone swarms are vulnerable to a variety of cybersecurity threats including malicious hacking, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, exploitation, and performance modification (Gabrielsson, 2021). Where some attacks threaten the continuity of drone operations, others pose severe threats to public safety due to remote access and manipulation of service provision. Global positioning system (GPS) spoofing attacks, for example, allow external actors to assume control over drone navigation, misdirecting flight paths or reducing performance during critical maneuvers (Zhu et al., 2019) even though most drones feature a return to home (RTH) program (Doyle et al., 2021). With these increasingly complex systems, the disruption of flight reliability can be catastrophic for drone swarms and for pilots’ control during mission critical exercises.

Whereas traditional drone operations have relied upon manned UAV navigation, more recent operations leverage AI-supported flight management to enable autonomous, semi-autonomous, and remotely piloted flight capabilities. Actors who use GPS spoofing to hijack drone location awareness with GPS spoofing may upload home coordinates, replacing those originally assigned by the drone operation team.
Such attacks utilize a Software Defined Radio (SDR) such as BladeRE, a power amplifier, and a transmission antenna to relay the signal to the target drone or swarm. Most drones are programmed to accept unencrypted GPS signals, resulting in widely exploitable systems that can be counterfeited to redirect flights to desired locations (Zheng and Sun, 2020). In many cases, the delay between hijack and detection may be too long to allow operator recovery, potentially resulting in a severe event such as drone loss or misdirection of onboard payload (e.g. missiles, packages, data) (Feng et al., 2020). Whilst behavioral models, inertial monitoring, and real-time flight path monitoring are frequently used to identify potential exploits, the rate and effectiveness of existing countermeasures may result in a loss of flight control (Zhu et al., 2019; Yaacoub et al., 2020). Malicious attacks, spoofing, and hijacking can have significant consequences for both civilian and drone operators. A drone undergoing a DoS attack, for example, is likely to engage its RTH function or land immediately, leading to device loss or mission failure (Feng and Tornert, 2021). Hijacked drones can become small scale missiles or be used to interfere with air traffic operations, target civilians, or damage property and equipment (Yaacoub et al., 2020). Though operators may believe they are returning the drone to their home landing spot, location spoofing can communicate false GPS coordinates and trigger fly-off behavior, resulting in vehicle loss or other system disruptions (Pardhasaradhi and Cenkeramaddi, 2022). Considering that these threats and others are continuously present during drone flights, the relationship be-
tween onboard security features and system protection and stability is an important condition of operational continuity and flight performance.

Within the conceptual foundations of systems security, there is a risk management protocol based upon a common series of responsibilities including risk identification (pre- and case-based), risk analysis (likelihood, severity), and risk evaluation (consequence, mitigation strategy) (Tubis et al., 2021). In their current iteration, drones are vulnerable to a variety of risks, many of which have been identified by trial and error, thereby leading to a potentially vulnerable profile that requires security hardening and operational protection (Yaacoub et al., 2020). An array of regulatory controls and legislative standards have been implemented in recent years to increase the accountability of drone operators for flight behavior and air traffic responsibility (Vacca et al., 2017). Yet, losing control remains one of the most significant risks facing drone operators, potentially resulting in unavailable or unresponsive aircraft that could violate any series of legal standards and platform expectations (Singh and Verma, 2017). Despite a growing body of research in this field to develop improved risk identification and mitigation measures, additional research was needed to identify techniques for fingerprinting compromised drones and determining the data and informational needs to inform and support operators in future recovery initiatives. This study has extended the field of research by contributing new evidence regarding several advanced, machine learning techniques that can be applied to this form of risk-averse, control-driven approach.
1.2. Research Rationale

The core research problem addressed in this study is the vulnerability of unmanned aerial vehicles (UAVs) or drones to cyber attacks. In general, drones are increasingly being used in commercial, defense, and consumer applications across vast geographies and for a wide range of purposes. Operational standards require ground control units to trigger drone behavior and establish the parameters of in-air activities including flying, sensing, videoing, and engagement. As such operational capabilities have improved over the past decade, and the scope of drone services has expanded to include commercial and civil use cases such as taking aerial photographs, performing live and recorded video surveillance, performing public announcements and limited policing, delivering products delivery, and observing environmental phenomena. Drones also have practical military applications for surveillance and ground attack purposes, missile transportation, and direct, kamikaze attack capabilities using onboard explosive devices. The rapid and global proliferation of drones is being accelerated by an array of capabilities. However, alongside popularity and increased usage, the threats and vulnerabilities affecting drone continuity and service operations is increasing exponentially. Therefore, the need to secure drones and data networks against malicious actors is an industry imperative.

Despite efforts to establish localized or general security standards for drone operations, limited onboard computing power means that most commercial drones cannot be described as secured end-to-end. Instead of investing resources to enhance
system security, manufacturing and software development initiatives are typically geared toward cost reduction, functionality, and ease of user operation. Therefore, several gaps are frequently observable in commercial drone offerings including: (1) firmware that can be manipulated, (2) unencrypted transmission data, and (3) lack of unencrypted onboard data (Siddiqi et al., 2022). To detect such threats, operators are largely dependent upon the critical assessment of data indicators related to key sources including communication channels, flight paths and navigation, and network continuity (e.g. between drone operations). Due to malicious agents' subversive efforts, the availability of such information might be delayed, potentially leading to an escalated threat vector that could compromise entire UAV networks (Singh and Verma, 2017). Recent research in this field has emerged to identify the possible relationship between onboard monitoring capabilities and anomaly detection during routine or normalized drone operations. Lu et al. (2017), for example, designed

As commercial and military applications of drone technology evolve, drone swarm capabilities is an innovation that has the potential to diversify and extend operational capabilities. For example, drone swarms have been used in recent military conflicts for reconnaissance over large areas through linked geographical quadrants and waypoints (Hambling, 2021). Within a given swarm, drone fingerprinting is typically performed autonomously, with onboard media access control (MAC) addresses providing the call sign or indicator of a drone in relation to other swarm members (Li et al., 2017). However, as the complexity of swarm flight paths increases, au-
tonomous drone murmuration capabilities are being recognized as essential functions of autonomous and adaptive UAV flocks (Hambling, 2021). Security profiling of a network of autonomous drones is significantly more complex than single drone monitoring. Therefore, an array of interrelated capabilities that predict in-flight behavior based upon traditional Reynolds flocking theory (separation, alignment, cohesion) is being integrated into a new model for security management, flight tracking, and operations control (Jia et al., 2019). Additional research is needed, however, to determine optimal solutions for monitoring security threats in swarm operations and developing drone fingerprinting solutions to quickly single out specific aircrafts that have been compromised or are under attack.

This study develops and presents a machine learning classification model to detect compromised or infected drones on a network. Specifically, the proposed model can analyze swarm and network datasets to quickly identify drones that are compromised and at risk of disruption. With increased awareness of such exploits, drone operators can implement an appropriate threat response, such as removing the drone from use, forcing a return to base (RTB) or destroying the drone to ensure safety. The machine learning model developed in this study, coupled with the data set used, will secure drones against an array of future security threats. To achieve this goal, this study has identified an efficient, machine learning algorithm that uses indicators of compromise (IOC) detection to identify compromised drones. The underlying data signatures have been used to normalize swarm activity and establish operational pa-
parameters that enable AI-supported systems to identify drones quickly and accurately by variant and aberrational behavioral indicators.

1.3. Research Objectives

The primary aim of this investigation was to develop an efficient machine learning algorithm that identifies compromised drones within a swarm quickly, autonomously, and consistently to implement immediate recovery steps and maintain operational continuity. Accordingly, this research assesses the array of security risks and vulnerabilities threatening drone swarm reliability, develops a practical intervention strategy, and tests that strategy via real world applications to assess its validity. Over the course of these multiple stages of exploratory research, the following primary research objectives have been accomplished:

i. To critically evaluate the available methods and techniques for identifying compromised drone data within a wider set of healthy data.

ii. To develop and deploy a machine learning model to scan for and detect normative and aberrational flight behavior across drone swarms on a large scale.

iii. To evaluate the optimal size of the drone dataset required to ensure that most indicators of compromise can be identified consistently and accurately.

iv. To recommend the form of machine learning that optimizes detection of compromised signatures based upon both real-time and post-flight data analysis.
1.4. Research Questions

These research aims highlight the method-based focus of this study, outlining the targeted approach to designing, experimenting, and reporting system specifications and procedural opportunities in machine learning security analysis. By not only recognizing the current deficiencies in drone security, but also identifying a means of overcoming such limitations through advanced machine learning techniques, the results of this study will contribute new evidence to a field in which systemic discipline and tactical designs must be cohesive to mitigate rising threats. For drone operators, the effectiveness and reliability of real-time security monitoring and drone recovery predicts the future of flight continuity. Therefore, the current study focuses on the probabilistic techniques and analytical resources needed to identify anomalies reliably and consistently by using flight path data to train and classify machine learning capabilities. This study answers the following questions to address the core research aim and associated research objectives:

i. How can one best analyze compromised drone and uninfected drone datasets to develop a collection of indicators of compromise (IOCs) so as to create robust signatures of infection?

ii. How can one deploy the machine learning model in a real-life environment to scan for and detect compromised drones on a large scale?

iii. What is the optimal size of the drone dataset to ensure that most IOCs are covered?
iv. What is the most unobtrusive way to deploy infected drone detection algorithms, and which form of machine learning will detect signatures most efficiently and effectively?

1.5. Definition of Key Terms

Many key terms in drone flight management and securitization theory must be clearly defined to ensure they are clearly understood in this context. The following section defines several central concepts repeated in this study:

Classifier model – The rules and systems used by machines and computers to classify data for machine learning purposes.

Cyber attack – A deliberate and malicious intent to breach the security of an information system for which the attacker does not possess user authorization.

Drone – An Unmanned Aerial Vehicle (UAV) which flies and operates via remote control, with no human pilot on board.

Drone dataset – The set of data provided by several drones to their operators, based on commands received, operations undertaken, and sensor input from the environment.

Swarm – A network of interconnected drones working under control or autonomously to achieve a specific objective across extended ranges and varied environmental conditions.

Electromagnetic battle management – The monitoring and management of
parts of the electromagnetic spectrum for military and combat purposes.

Inertial Navigation and Measurement – An onboard system capable of detecting changes in inertial patterns during drone flight to report deviations and aberrations to operators or management systems.

Machine learning – Computer systems which are designed to learn using algorithms and statistical models, to improve their performance over time.

Spectrum signature identification – The process of identifying material and objects by analyzing their specific signature from the electromagnetic spectrum.

Software Defined Radio (SDR) – A simple GPS-based exploit solution which transmits a counterfeit GPS signal or civil aviation warning (e.g., no-fly zone) to force drone recipients to actively respond (e.g. change course, land).
Chapter II.

Related Works

For much of the early research on drone design and swarm configurations, most investigators primarily focused on system functionality. However, as the technical complexity of this research has increased, the operational nature of drone theory has evolved beyond swarm- and location-based analyses and towards security-related priorities and operational continuity. The following sections begin with a theoretical overview of drone flight management technologies and swarm-based operational capabilities. Subsequent insights regarding current threats and security risks are presented to outline the central problem of flight security and operational continuity. Finally, technological insights related to spectrum fingerprinting and machine learning capabilities are introduced to establish the foundations of the theoretical model. A focused, system of systems model is presented to narrow the conceptual framework into those key components needed to realize techno-systemic functionality in drone applications.
2.1. Drone Flight Management

Although ubiquitous in terms of applications and widespread recognition, drones or UAVs are a relatively new technology that are classified into one of six interrelated groups (Mekala and Baig, 2019, 173):

i. Civil and Commercial: Deployed by various civilian operators, these drones are typically used for photography or data collection across an array of settings and applications.

ii. Research and Development: Drones for technological development, site assessment, and active visual-spatial research.

iii. Logistics: Drones for cargo delivery and resource transport in rural or hard to access areas.

iv. Target and Decoy: Typically used for military purposes. The controller is able to take a clear shot on the target by providing both ground and aerial views of the surroundings.

v. Reconnaissance: Often used in military operations to collect battlefield intelligence, assess localized conditions, and remotely analyze potential tactical advantages.

vi. Combat: A weaponized version of UAVs that is used on military battlefields to carry missiles, facilitate drone strikes, or perform kamikaze operations.

Drones are subject to routinizing of operations, whereby flight predictability is essential from both an operational and a practical perspective (Baig et al., 2022). As
aviation-based resources, drones and their operators must comply with a variety of aviation safety rules such as the 1944 UN Convention on International Civil Aviation and the 2015 European Union (EU) Riga declaration on remotely piloted aircraft. Explicitly, the drone operator assumes responsibility and liability for drone usage, thereby requiring that drones not only adhere to regional aviation rules and guidelines, but that drones are used responsibly, which preserves and protects other local rights (e.g., right to privacy, lack of interference) (EU, 2015). With emerging data protection laws, legal precedence, and national legal standards establishing the basis for drone operator accountability, Vacca et al. (2017) recognize that drone-based risk analysis and systems management is increasingly essential to framing the security protocol for both civil and military operations.

Many of the technological and operational benefits of drones can also create security risks and liabilities. One significant asset is the remote nature of drones because it allows operators to pilot these highly adaptable resources across broad distances without direct contact with the intended target (e.g., ground coverage monitoring, enemy targeting, home roof inspections). However, Yaacoub et al. (2020) observe that such remote capabilities make drones vulnerable to an array of external forces, including signal jamming, spoofing, and drone hijacking. For example, a drone expected to fly over a specific target might receive inaccurate GPS coordinates (spoofing) and instead target a different region or location, potentially undermining the mission or threatening target security (e.g., air-to-ground missile, kamikaze attack). Other as-
sets of drones are its lightweight software design and onboard features which optimize battery life for operations. Unfortunately, this efficient design limits the ability to embed security capabilities which increases the risk of drone exploitation by outside agents with more powerful and more capable computing and broadcasting technologies (Yaacoub et al., 2020). The categorical threat to drone flight management can be characterized according to the relative severity and operational impacts of the attack or disruptive event. Singh and Verma (2017) propose seven key operational threats that drone operators must manage:

i. Unavailability or unresponsiveness of UAV  
ii. Disruption of UAV operations and/or functionality  
iii. Degradation of ground-to-flight communication  
iv. Inaccurate GPS coordinates  
v. Unauthorized access or exposure of confidential information  
vi. Damage to infrastructure  
vii. Compromised or exploited UAV

For drone operators, GPS provides the basis of several central operational needs including route navigation, location detection, and telemetric analysis and data modeling. Zheng and Sun (2020, 2730) define GPS as a ‘global navigation system that utilizes satellites to provide precise three-dimensional position, velocity, and time information.’ It uses 24 satellites that are distributed across six different orbits and broadcast on two different signals including the civilian, unencrypted signal at the L1 band (1575.24 MHz) and the military, encrypted signal at the L2 band (1227.60 MHz) (Zheng and Sun, 2020). Due to their reliability and unencrypted vulnerability, civilian GPS signals are at risk for spoofing or disruption by a software defined radio.
(SDR) that is able to mimic the same frequency, signals, and information as GPS satellites.

As the military increases capability development, drones are outfitted with autonomous weapons systems including air-to-surface or air-to-air missiles which significantly increase the risk profile of drones to the localized public and surrounding properties (Johnson, 2020). For larger force solutions, AI-supported drone swarms are being developed featuring onboard loitering attack munitions (LAMs) that allow individual UAVs to function as suicide drones once enemy targets such as radar arrays or weapon caches have been identified (Johnson, 2020). Although such solutions present a novel, advanced perspective on modern warfare, Johnson (2020) argues that the efforts to remove human decision-making from the AI-supported drone equation require a degree of delegated authority dependent upon the accuracy and consistency of machine learning capabilities and intelligence systems.

2.2. Swarms and Flocking for UAVs

Drone swarm behavior is predicated upon flocking specifications which prior researchers such as Watson et al. (2003) have based upon telemetry coordination, whereby zone relationships determine the specifications of UAV flight paths both relative to the target position and the other linked drones. Based on Reynolds flocking theorem, flight path continuity requires three interrelated attributes including separation, alignment, and cohesion (Pyke and Stark, 2021). Relying upon short-range
communication capabilities, Hauert et al. (2011) suggest that such omnidirectional motion controls are affected by two primary domains: the proximity signals from within the flock and the longer-range guidance signals distributed via control modules over dedicated radio frequency (RF) channels. Extending this generalization of flight flocking to quantitative domains, Jia et al. (2019) subdivided the input signals received by individual drones within a given flock according to the various coordinates required to maintain continuity in flight (e.g., roll, pitch, yaw, speed, torque, and acceleration). Due to the multi-axis behavior of drone flights under swarm conditions, however, deviance from pre-defined flight paths can have a significant impact on flock continuity. Therefore, Jia et al.’s (2019) algorithmic solution includes multiple protective dimensions including collision avoidance, connectivity preservation, velocity alignment, and defines the coordinated, full-scale flight path, as a flocking center or rotation point.

For modern applications of drone flocking capabilities, operators have developed coordinate-based systems which control drones according to explicit flight paths that are pre-programmed with various telemetry indicators to minimize the likelihood of in-air collisions (Hambling, 2021). However, when drone swarms, such as those used by military operations, are expected to swarm in space and navigate over extended distances, there is a need for a naturalistic swarming capability that uses system autonomy, event responsiveness, and coordinated murmuration (Hambling, 2021). Although this paradigm still derives its rules from the Reynolds separation,
alignment, and cohesion theorem, the centralized control structure transitions away from a ground control system or direct UAV link protocol to an intra-swarm flight path solution as depicted in Figure 1. This model highlights a spatial relationship between drones that is center-proximal, thereby allowing models to assess the degree of intra-swarm consistency relative to each of these three operational dimensions. If a drone veers beyond established tolerances, it then separates from the swarm, becomes unaligned, and damages the swarm’s intragroup cohesion. Such modeling can be highly effective for analyzing aberrations in geographically distributed swarm networks, particularly when drones are traveling at high speeds or over long distances from the control unit (Hambling, 2021).

![Figure 1: Reynolds Flocking in Action (Source: Hambling, 2021)](image)

One of the problems with drone swarm cohesion is the vulnerability of individual drones to sensor interference and/or signal degradation during contact-critical missions (Johnson, 2020). AI technologies provide drones with coordinative solutions that not only maximize the efficiency of the Reynolds flocking behavior, but create tactical opportunities for operators such as remote sensing, facial recognition capa-
bilities, signal interference, and attack vectoring (Johnson, 2020). For drone swarms to operate efficiently and safely, Ahn et al. (2019) propose that technologies must be developed to detect anomalies in the behavioral patterns and activities of drones and explicitly consider sudden changes in network health and/or performance. Within the swarm capabilities, fault detection, identification, and recovery (FDIR) technologies utilize a cooperative virtual sensor (CVS) system to interpret onboard signals and identify potential variations in both individual drone and swarm performance (34). However, despite the potential benefit of such technologies to complex operational systems, Ahn et al. (2019) caution that they are dependent upon known or predictable behavioral profiles, thereby restricting their usefulness to scenarios where environmental variables or malicious actors disrupt the routinization of the drone flight paths.

2.3. Risk Assessment and Drone Operations

Continuity of any interconnected digital system depends on network security and the ability to establish, monitor, and maintain the confidentiality, integrity, and availability of the expected information and services (Vasconcelos et al., 2016). Risk assessment in drone operations is typically characterized by one of two dominant approaches including (1) the occurrence or probability of adverse events and (2) the scale or severity of negative (disruptive) or positive (opportunity) effects on drone operations and performance (Tubis et al., 2021). From a quantitative perspective,
the collection and inventorying of risks associated with drone operations involves a critical review of a variety of factors which Tubis et al. (2021, 7-8) have identified as follows:

i. Descriptions of the primary conditions of the UAV system operating environment during service/transportation.

ii. Identification of disturbances or anomalous events that have occurred during drone operations. Frequency analysis of the disturbance(s).

iii. Cause or attribution of the disturbance(s), including the conditions allowing the event to occur.

iv. The consequences of the disturbance for the UAV, the mission, and the underlying data or technology.

More formal risk assessment techniques such as ISO 31000 (2018) have been developed for commercial purposes and include a simplified procedure of risk identification, risk analysis, and risk evaluation. Although the profile of such risks is often obscured by operational assumptions (e.g., device hardness, lack of accessibility, remoteness, lack of interest), the procedures surrounding this three-stage protocol are critically important to creating a formal risk register that can evolve and adapt with the range of operational activities. (Tubis et al., 2021). Figure 2 summarizes the three-dimensional risk assessment model for drone operations, adopting a commercial perspective for modeling, weighing, and interpreting risks relative to a flight plan or operational objective. As risks are profiled according to their probability, severity,
and frequency, the relative likelihood of an adverse event increases or decreases according to the drone flight path and its vulnerability to exposure and/or an adverse environmental scenario (Tubis et al., 2021). For example, military operators in a high-volatility zone are more likely to encounter hackers and malicious actors than a farmer surveying land on his own property. Drone operators flying near restricted airspace such as an airport are more likely to face risks of law enforcement detection and interference than drone operators surveying mountain caverns or canyons.

<table>
<thead>
<tr>
<th>Risk Identification (Qualitative Analysis)</th>
<th>Risk Analysis (Quantitative Analysis)</th>
<th>Risk Evaluation (Deductive/Inductive Reasoning)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis of historical data and observations regarding known risks, threats, and operational concerns.</td>
<td>Expert opinion and observations regarding risk probability</td>
<td>Weighted determination of the acceptable level of risk.</td>
</tr>
<tr>
<td>Identification and description of anomalies and adverse event scenarios</td>
<td>Assessment of probabilities based on flight plan and/or risk parameters</td>
<td>Comparison of the risk profile (probability vs severity) with level of acceptability</td>
</tr>
<tr>
<td>Prioritization of mitigation or avoidance tactics</td>
<td>Fuzzy quantification and analysis of risk parameters and scenario framing</td>
<td>Selection of routes and scenarios in which risk profile is reduced</td>
</tr>
<tr>
<td>Development of monitoring and/or tracking capabilities for risk profiling</td>
<td>Implementation of automatic or responsive risk avoidance and mitigation solutions</td>
<td>Post-event performance analysis and modeling.</td>
</tr>
</tbody>
</table>

Figure 2: Three-Dimensional Risk Modeling for Drone Operations (Adapted From: Tubis et al., 2021)

To effectively weigh and analyze the risks to drone operations, Singh and Verma (2017) propose a five-factor model that includes the threat identification, estimated severity of impact, probability or likelihood of attack, ranking of the range of attacks, and formal modeling of the end risk scores. Although this approach may
allow researchers detail the potential threats against drone operators, the method is deficient in its ability to detect ongoing threats that may be masked as a similar phenomenon (e.g., disruption of radio signal). Evidence captured by Hsieh et al. (2021) using onboard sensor data revealed that performance variation can be used as a proxy for anomalous drone behavior, allowing researchers and operators to monitor variations in drone flight operations by selectively tracking key criteria. Although drones maintain onboard datasets, that researchers are unable to access in real-time, researchers can still use onboard behavioral monitoring such as signal strength tracking and accelerometer data to identify potential changes in drone flight status (Hsieh et al., 2021). The problem with this approach is that it is contingent upon the accuracy and speed of event recognition by the device being used for onboard readings, a delay which Hsieh et al. (2021) suggested might lead to more serious performance effects during drone operations (e.g., loss, unable to recover).

One of the most important operational objectives in drone flight management, particularly when flying swarms of multiple UAVs, is fingerprinting or accurately identifying the drones and their operational behavior. Li et al. (2017) explain that many law enforcement agencies are seeking remote sensing resources to identify drones according to key indicators such as their serial numbers, which are recorded and reported for flight authorization purposes in some jurisdictions. However, in many cases, drone or operator cooperation is limited, meaning that drones are fingerprinted through various communication protocols such as signal tracking, WiFi analysis, and
onboard indicators such as frame header fields (Li et al., 2017). Drone fingerprinting can also defend against exploitation, as it can be used to monitor variations in flight navigation as well as changing signal strength patterns which indicate directional changes or distances between drone/controller or drone/swarm relationships. Through the deployment of a remote 802.11 packet header extractor, Li et al. (2017) were able to capture field values that revealed various fingerprint characteristics such as the NIC manufacture (first three bytes of the MAC address) which further reveals the default communication channel (e.g. 2447 MHz—Channel 8 for 3DR Solo drones).

Forensic data from exploratory analysis is being deployed to assess the specific traits and/or characteristics of individual UAVs, with the potential for remote fingerprinting and monitoring. Clark et al. (2017) were able to download text (TXT) files from a DJI drone within the flight record subdirectory of a captive aircraft. Within the k.class flight record file, they obtained around 190 bytes of data that included the drone’s name (operator-defined) and four individual serial or identification numbers related to the IMU, the camera, the primary circuit board, and the battery. As visualized in Figure 3, this TXT file structure includes a variety of non-important data before positioning critical flight data (e.g., GPS, battery, flight status) in packets within the second to last position in the file. The remaining bytes are dedicated to the drone identity and offer investigators the best opportunity for capturing and tracing the identifying features of a drone, even if only the TXT file can be recovered (Clark et al., 2017).
The onboard DAT logs, which are recorded during drone flights for popular brands like Parrot and DJI, are systemically encrypted which reduce direct access to the datasets. However, they can be bypassed using an open source software solution like DatCon (Kumar and Agrawal, 2021). Through a comparative analysis of the 268 different parameters recorded during a sample DJI drone flight, Kumar and Agrawal (2021) determined only 8 indicators had direct implications for forensic security analysis. From those 8 dimensions they were able to not only convert the evidence into comma-separated values (CSV) format for virtual analysis, but were able to chart the drone’s flight path, analyze variations in drone flight behavior such as motor speed and altitude, and characterize control systems such as RC frequency and operator distance (signal strength) (Kumar and Agrawal, 2021). As a form of reverse charting solution, criminal investigators can use this approach to drone forensics analyze adverse activities by drone operators and model patterns that might relate to a specific event or criminal action (e.g., dropping drugs into a prison, surveilling a home for theft opportunities, crashing into a glass window).
Whilst onboard data might provide forensic analysts with critical insights that could be used for predictably monitoring ongoing and past events, it can also fingerprint and identify drone-specific traits using real-time data analysis. Medaiyese et al. (2021) suggests that drone detection under various environmental conditions may yield important commercial or military advantages, allowing individuals to identify variations in the localized signal field and thereby identify possible threats and/or unauthorized UAVs. Although not specific to onboard security threat detection, the model demonstrates the direct relationship between drone operations and drone control modules via the RF control signal (Medaiyese et al., 2021). Through advanced packet extraction techniques such as wavelet transformation and signal decomposition, it becomes possible to apply statistical parameters (e.g., algorithmic constraints) to the assessment of input data, thereby identifying aberrant signals which lie outside of the normative bandwidth (Medaiyese et al., 2021). This same approach could be reversed for onboard threat detection, as drones utilize RC signal mapping and AI-supported signal analysis to determine which control signals are expected or legitimate and which control signals are classified as aberrant or outside of the normative signal ranges.

2.4. Denial of Service (DoS) Attacks

The research on drone operations typically focuses on the relationship between normative and abnormal performance outcomes. Feng and Tornert (2021) evaluated
the effects of a targeted DoS attack on the Parrot ANAFI drone, a device that was locally connected to a WiFi access point to facilitate control remotely from ground operations. Due to the dedicated flow of traffic across the WiFi network, the experiment identified several traffic-based vulnerabilities that threatened communications protocols and network continuity. For example, consistent communications with the in-air drone can be disrupted by manipulating the network traffic data and flooding the communication channel (e.g., WiFi bandwidth, TCP flooding) with bots and high-volume traffic, resulting in both a loss of continuity and threat to airborne operations (Feng and Tornert, 2021).

In developing DoS countermeasures, early experimentation by Vasconcelos et al. (2016) observed that when routing cloud services through Transmission Control Protocol (TCP), command-line software using the Hping3 can be used to execute a TCP SYN (SYNchronize) flood attack known as a Low-Orbit Ion Cannon (LOIC). The LOIC is recognized as a user-friendly DoS attack protocol that simply requires the user to enter the target address and trigger the ‘IMMA CHAGIN MAH LAZER’ button after optimizing in-software settings such as TCP, User Datagram Protocol (UDP), and/or Hypertext Transfer Protocol (HTTP) (Vasconcelos et al., 2016, p.2). Hping3 is an open-source tool used as a packet generator or analyzer for TCP/Internet Protocol (IP), that can send multiple, spurious packets of data to the drone’s network address using the-fast-flood command (Vasconcelos et al., 2016). Observable impacts compared operational data under non-DoS conditions to the intra-DoS at-
tacks, resulting in a significant decrease in frame rate exchanged between pilot and drone. Where onboard communication ports were left unencrypted, the experiments demonstrated that the test drone could be consistently powered off using a simple command (Poweroff Application) and the open, onboard telenet port (Vasconcellos et al., 2016). Such findings not only illuminate the vulnerability of drones to disruptive exploits, but the potential threats associated with unencrypted data and static, channel-dependent network communications.

Researchers recognize the threat of DoS attacks and have developed countermeasures to circumvent attempts to hijack or contravene network operations and reduce their impact. For example, techniques adopted by Chibi et al. (2021) revealed that onboard data analysis for swarm-based telemetry can be used to analyze the receiver signal strength indicator (RSSI) and triangulate in-air readings of member drones to reduce the likelihood of successful DoS attacks. By acknowledging telemetry data relative to the active agents within a given network (e.g., drone 1, 2, 3 + ground station), the estimated distance (d) between the transmitter (t), and the receiver (r) can be calculated relative to the strength of the incoming signal, thereby predicting the reliability of the signal/data packets (Chibi et al., 2021). By triangulating such signal data from multiple drones in a swarm, Chibi et al. (2021) proposed an algorithmic RSSI tool that could identify threats to drone activities and either deploy effective countermeasures or return the UAVs home. The problem with these emergent capabilities is that they lack fidelity and are typically used for a large broadcast
area which reduces precision.

2.5. Hijacking and GPS Spoofing

In addition to service interruption and DoS attacks, drone vulnerabilities within communication links can also be exploited using various smart devices and hardware. Malicious actors can adapt these methods across domains, often hacking and interfering with drone operations, resulting in theft, destruction, and/or risks to human life (Yaacoub et al., 2020). Due to a drone’s system vulnerabilities and the range of remote software exploits, drone hijacking through software modification and rerouting can be particularly disruptive to flight operations. For example, in wayfinding and waypoint navigation, UAVs typically utilize a return to home (RTH) function that external actors can manipulate remotely, interfering with mission critical operations or causing incomplete reporting (Baig et al., 2022). Malicious actors may also hijack communication channels to alter drone sensor images and change attack vectors, both of which could lead to catastrophic failure or drone loss (Doyle et al., 2021). Doyle et al., 2021 identify additional tactics including communications jamming or interference, sensor mirroring or duplication, and tracker alterations or misdirection.

GPS spoofing, although similar to hijacking, may not involve onboard intervention or manipulation of the drone software and mission objectives. Instead, geolocation coordinates can be spoofed to redirect in-flight UAVs towards the at-
tacker’s target or waypoint. (Pardhasaradhi and Cenkermaddi, 2022). Attackers may also use amplified signals across RF antennas to refocus the drone’s onboard location systems towards a new target (Pardhasaradhi and Cenkermaddi, 2022). Due to technological limitations, most commercial drones have been pre-programmed to accept unencrypted GPS signals, thereby allowing individuals bad intentions to tamper with the original destinations and redirect flight pathways (Baig et al., 2022). A recent study by Yaacoub et al. (2020), collected evidence of the potential severity of spoofing consequences for an array of targets including humans, smart city resources, vehicles, and other ground-based locations.

Despite drone operators’ best efforts to maintain accurate information about onboard flight direction, telemetry, and GPS position, the range of spoofing and hijacking exploits developed by malicious actors is creating various reliability challenges. Figure 4 provides a visual representation of the effects of a drone hacking attack upon a UAV’s planned trajectory. Whilst this linear model assumes a steady-state flight path for the drone, it highlights the potential risks associated with a flight path that uses triangulated GPS data to artificially append the horizon, thereby gradually redirecting the drone away from its target (Feng et al., 2020). Using machine learning analysis to simplify detection capabilities of drones, Feng et al. (2020) were able to reduce the number of criteria to just four primary datasets including GPS (longitude and latitude) and IMU data (angle velocity and acceleration). The model is tuned and trained to recognize variations in-flight path performance according to onboard
sensor data, allowing hijacked drones to self-identify external influences during the supervised training session. However, Feng et al. (2020) also observed that without such supervision, autonomous hijack detection accuracy fell significantly, requiring future research to address specific criteria and evolve the detection capabilities of the individual drones towards a more accurate standard. As drones inherently depend upon their telemetry data and the inputs provided by dedicated GPS location modeling, the threat of spoofing to operational displacement is significant; signals mirroring those sent by the control unit are able to fool onboard systems into misidentifying GPS coordinates (Carson et al., 2016). Hack RF One, for example, is an open-source, GPS spoofing hardware system that broadcasts across a range of frequencies from 1MHz to 6GHz, covering the frequency band of GPS signals and can potentially reroute or disrupt the GPS data received by UAVs within a given range (2020).

Figure 4: Example of a Drone Hijacking Attack (Source: Feng et al., 2020, 2)

Although the internal oscillator is inadequate for long range spoofing, Zheng and Sun (2020) upgraded this component using a temperature compensated crystal oscillator (TCXO) to transmit pre-generated GPS data (e.g., coordinates of a no-fly...
zone) to affect drone flight patterns and telemetry. The following three GPS spoofing exploits were tested to affect drone position and flight behavior (Zheng and Sun, 2020):

Forced Landing: Despite their commercial availability, drones are robust machines that pose risks to public safety, particularly in restricted airspace (e.g., airports, over national buildings). Spoofing onboard GPS coordinates can cause a drone to self-identify as being within a no-fly zone and force it to engage embedded security protocols like landing immediately.

False Direction Guiding: During hovering exercises, drones are programmed to fly in a fixed location in space defined by GPS coordinates. The drone can modify its position during periods of high winds or if it encounters an obstacle by shifting to an alternative location. If the spoofer can report inaccurate GPS data to the drone during hovering activities, the drone will automatically amend its position, attempting to regain its localized hovering status. This can significantly alter the drone’s flight path and misdirect it to a target position or zone.

Landing in False Area: This two-part spoofing attack involves jamming drone communications to trigger a go-home function. Once the drone begins its return, the onboard GPS coordinates will direct the flight path towards the originating location. The spoofing module can prescribe a false direction, guiding the drone to a new ‘home’ that is artificially defined by the hacking agent.

However, many of these solutions were based on cryptographic techniques,
making them highly computationally extensive, increasing the cost and complexity of drone usage (Gupta et al. 2020). As such, the potential exists to use artificial AI techniques, including machine learning, to focus on the detecting these attacks, rather than just relying on cryptographic prevention, thus facilitating the secure usage of drones as they are increasingly relied on.

Pardhasaradhi and Cenkermaddi (2022) observe that drones, particularly those in swarm operations lack the ability to reconcile anomalies within their immediate proximity due to the relative inefficiency and inconsistent performance of onboard IMU sensors. This means that drone spoofing attacks where other in-air targets are generated through virtual projections are likely to be highly disruptive to onboard flight systems. To overcome this challenge, Pardhasaradhi and Cenkermaddi (2022) proposed a localized, control-based radar tracking solution that maintains a filtering capability to identify not only real, in-air targets or threats, but those that are being fabricated by malicious actors. The consequences of noise during flight such as rain, fog, or electromagnetic interference can be significant; however, when combined with ground-based support systems, coordinated swarm operations can be supported and guided.

2.6. Intrusion Detection Systems for Drone Monitoring

Intrusion detection systems (IDS) originated in traditional software and systems design and focus on two pathways to the detection of malicious or unauthorized
activities including anomaly-based and signature-based (Yaacoub et al., 2020). In a signature-based output, the IDS utilizes existing information about security threats to match the signature of incoming traffic or in-network behaviors to deviant or threat-based behavior. By monitoring the drone data, the live information connects the signature feedback from the drone with the ground controller, either validating or rejecting the attempts to access network nodes. Alternatively, anomaly-based detection is based upon an established routinization of data packetization and exchange between the drone, ground controllers, and edge nodes (e.g., other UAVs). Each of these core approaches to drone operational monitoring and security management are defined below:

Rule-Based Intrusion Detection: A detection-based model capable of identifying false attacks and/or communications that are based upon explicit behavior and communication rules (Mitchell and Chen, 2013; Strohmeir et al., 2015).

Signature-Based Intrusion Detection: Drone fingerprinting or signature detection involves identifying drones according to their specific traits and/or identities such as their GPS signal or their communication characteristics (e.g., MAC address, signal channel) (Casals et al., 2013; Kacem et al., 2016).

Anomaly-Based Detection: Designed to prevent anomalous signals and interference via DoS or signal interference, anomaly-based detection involves monitoring network traffic to identify possible external actors and/or malicious agents who are attempting to gain access to drone communications (Sedjelmaci et al., 2017; Con-
domines et al., 2019).

One of the problems with detecting abnormal or anomalous behavior is that drone computing capabilities are limited to a simple set of onboard signals and commands that are guided by ground-based information and feedback. Therefore, operating an onboard IDS would require significantly greater computing power than what is available on the drone itself, particularly if the device were loaded with malicious signatures and abnormal cues. However, by applying machine learning technologies and AI-supported controls to drone capabilities, the overall efficiency of the IDS can be improved without requiring a much greater and more significant computing solution (Baig et al., 2022). Sailpoint (2022) recognizes that AI-supported cybersecurity measures can be used to detect an attack before it disrupts or destabilizes a drone and its control network. By drawing upon trained datasets extracted from known attack vectors, machine learning techniques increase the ability to detect threats before critical disruptive events manifest into more serious consequences for the operator or the UAV (Sailpoint, 2022).

An array of operational and environmental forces reduces the likelihood of reliably detecting anomalies. Lu et al. (2017) developed an innovative anomaly detection methodology that focused on an onboard sensor affixed to a DJI drone that could record variations in flight characteristics such as motor temperature, motor sounds, and communication anomalies. Gyroscopic capabilities also alerted the operator to abnormal rotation, benchmarking expected rotation against the actual real-world
outcomes according to a 70 percent normalization standard (Lu et al., 2017). When applied to future drone applications, Lu et al. (2017) hypothesized that a similar sensor-based analytical solution could be used to systematically monitor drone operations criteria, alerting the operator to potential problems as time-based records were generated during the flight path. Although this approach required an external sensor (e.g., raspberry Pi and software), it demonstrated how data collected during drone operations could be used as a security alert mechanism to not only ensure that the operator responded rapidly and effectively, but to detail the causes and underlying effects of any anomalies.

As remote vehicles with extensive capabilities that often require autonomous or onboard control decisions, UAVs are evolving beyond the traditional point-to-point flight concept. Sindhwani et al. (2020), for example, introduced a 12-rotor, unsupervised delivery UAV model that is capable of delivering weight-controlled packages across multiple delivery points in a single flight vector. By selectively disabling key components such as one of the 12 hover motors or positioning the drone in high wind conditions, the researchers demonstrated how onboard sensing capabilities and craft recovery solutions could be used to autonomously overcome obstacles, whilst recording data for future machine learning training and analysis (Sindhwani et al., 2020).
2.7. Machine Learning and Drone Flight Continuity Analysis

In detecting variations in drone flight behavior, researchers such as Syed et al. (2022) have shown that digital forensic investigation from flight logs can be used to model specific events or chart past variations in drone behavior according to potential aberrations and malicious attacks. Where probabilistic estimates of drone flight behavior, particularly in autonomous, waypoint flights (e.g., directional, set path), predict a direct, normative flight pattern, changes in status such as interference with RC signals or disruption of GPS data can be recorded in onboard datasets as aberrant behavior (Syed et al., 2022). To model this phenomenon, Syed et al. (2022) applied a similar analytical approach to Baig et al. (2022), processing flight data logs using DAT-converted CSV files and unsupervised, machine learning clustering algorithms including K-Means and Gaussian Mixture Model (GMM). The output suggested a viable application for both post hoc and real-time flight data analysis, and made recommendations for future complexity and innovation in machine learning and data classifier modeling (Syed et al., 2022).

In systematizing the characteristics of machine learning classifiers, Baig et al. (2022, 6) identified three primary domains that can be used to streamline IDS capabilities:

Supervised Learning: Data presented to the machine learning classifier is labeled according to its class definition (e.g., drone attack = rows of data representing attack vectors). Routine flight data can then be classified as normal or optimal.
Once the machine has learned the distinctions between attack and normal, onboard
responses to varying data packets can be assessed via testing, thereby determining
the accuracy of the response.

Unsupervised Learning: Data presented to the classifier is unlabeled. The
procedure involves clustering similar data samples into explicit cluster headings based
upon analytic differentiation of the inter-cluster behaviors or levels.

Reinforcement Learning: Also initially driven by unsupervised learning, re-
warding functions are included to assist the AI identify the optimal or near-optimal
classification of the data samples. Often employing Markov decision models, the
primary objective of the data processing is to attain the highest cumulative reward
during classification.

Although there are a variety of machine learning classifiers, given the rou-
tinization of drone operations, several common solutions have been adopted in recent
studies including Naïve Bayes, support vector machines (SVMs), and random (for-
est) classifiers. Feng et al. (2015) applied the random forest classifier to assist in
remote sensing of vegetation traits captured via flyover data from drone images. By
bootstrapping the initial dataset according to its characteristics (e.g., agricultural,
forestry, rock formations, structures), a decision tree is defined which can then be ap-
plied to the remaining dataset to confirm the accuracy of the machine learning model
(Feng et al., 2015). These ensemble-based classifiers are known for their robustness in
image classification and negotiating multiple dimensions or identifying variables (Feng
et al, 2015). In addition to this analytical approach, researchers have also adopted supervised learning techniques to support operational continuity and identify cyber threats to a drone and its control network. For example, Baig et al (2022) presented a framework for supervised learning which can classify drone data into its normative or aberrative domains. Such post hoc analysis involves downloading datasets, training machine learning systems, and applying these analytical tools to identify particular gaps and/or inconsistencies in the operational data (Baig et al., 2022).

As machine learning continues evolving towards improved probabilistic models, researchers are exploring additional techniques to address the threat of more technologically advanced attacks on manned and autonomous drones and swarms. For example, Shafique et al (2021, 1) propose the SVM algorithm for identifying signal spoofing and GPS-related attacks. By targeting variations in the dataset, the researchers employed a K-fold analysis to assess the effectiveness of the SVM findings, demonstrating the potential application of a deeper, machine learning solution for identifying variations in drone flight and signal behavior. Similarly, Arthur (2019) proposed a deep learning-based, adaptive IDS, which drones could apply to identify intruders and ensure a safe RTH; drones would follow the original flight path rather than relying on a spoofed GPS. This approach used the Deep-Q Network learning algorithm to support dynamic route learning, thereby allowing drone operators to monitor expected versus flow routes and identify variations in real-time (Arthur, 2019). This form of on-demand threat tracking solution is an important evolution of machine
learning capabilities as it enables operators to respond quickly and strategically to recover the drone or prevent harm to person or property.

SVMs are a valuable resource for distinguishing between normal and abnormal drone behaviors as machine learning algorithms develop a ‘hyperplane in an N-dimension of space that maximizes the margins between two classes of data’ (Baig et al., 2022, 6). Similar to grouping the data into competing subsets, these hyperplane models clearly differentiate between the classifications of data according to their assigned membership. Novel research by Karimibiuki et al. (2019) applies the SVM algorithm to the analysis of drone flight data in IoT-supported autonomous flight environments to determine the appropriate and targeted pathway for flight and mission success. Critical to drone authentication within the network, the SVM separates data into either normative or anomalous behavior, using criteria based-analytics to classify drone flight variations. By applying a one-class SVM, Karimibiuki et al. (2019) recognize that every column of drone operational data (e.g., yaw, pitch, roll, motor speed) is independent from the other columns, establishing normalization within columns through multiple real and fake data training sets to indicate malicious threats or system attacks. As an authentication mechanism, the researchers confirmed that SVM does offer a valuable resource that can be combined with other algorithms such as the K-Nearest Neighbor (KNN) classification of flight data and distance variables.

The Naïve Bayes classifier is a probabilistic model based on the Bayes theorem to classify and subdivide attributes and address the randomness and complexity
of drone security management. Ho et al. (2018), for example, developed a Naïve Bayes classifier that calculated the criteria-based performance threshold for drone flight performance, establishing a binary pass-fail solution for defining recovery behavior. When events such as a high headwind are recorded, the Naïve Bayes classifier provided compensatory directions to drone navigation that could improve overall route performance and ensure that drones could fulfill their operational priority (goal achievement) rather than return home mid-air or fall. (Ho et al., 2018). Despite the advantages of this binary solution, as evidenced by Majeed et al. (2021), the Naïve Bayes classifier assumes independence between information criteria, thereby increasing the number of false positive relationships despite a 95 percent classification outcome. Due to miscalculations and a lack of model precision, such inconsistencies may threaten the relative effectiveness of this algorithmic solution, encouraging researchers to explore alternative approaches to increase the efficiency and performance (Majeed et al., 2021).

The multiple linear regression approach to machine learning seeks to ‘estimate the parameters of the model that describes the relationship between two or more independent variables and a response variable by fitting a linear equation to the observed data, often using the least squares method’ (Oliveira et al., 2020, 8). In remote sensing studies, Oliveira et al. (2020) have shown that multiple linear regression can be used to compare hyperspectral images and their relationship to vegetation and canopy height models and predict the effects of climate change, climatological events,
or anthropomorphic influences on vegetal health and yield. Jensen et al. (2021) similarly applied this approach to ground cover modeling, selectively identifying arboreal features and classifying the regression models (linear, logarithmic, and exponential) according to the pretrained images and field settings. As a predictive solution to drone route definition and management, Majd et al. (2018) highlighted the combi-native role of various clustering algorithms, such as (KNN), with linear regression predictive modeling to demonstrate the optimal flight planning of drone swarms. Despite valuable programmatic findings for designing swarm-optimized flocking capabilities, the regression solution is supplementary, framing the quantitative output rather than identifying the intra-variable relationship (Majd et al., 2018).

As a clear leader amongst researchers in this field, the random forest classifier is defined as an ‘ensemble learning technique that uses decision trees or estimators to classify data.’ Probabilistic ranking of the underlying solutions combines the results of various trees, bagging and training tree structures via bootstrapped samples that result in error-defined outcomes (Aldaej et al., 2022). Ultimately, it is the decision tree with the lowest error rate that is given the highest priority, requiring that researchers determine the optimized number of estimators and the max depth of the tree branch structure to maximize effectiveness and reliability of the results (Aldaej et al., 2022). Although this form of decision analysis model is valuable for detecting and analyzing variations in datasets, the ability to differentiate between variations in drone behavior is complicated by the relatively binary representation of attack
or normalization (Guerber et al. (2021). In designing network models that can be effectively classified using Random Forest algorithms, Guerber et al. (2021) propose that differenting between traffic patterns (e.g. inside versus outside) is essential not only to restrict flow from unauthorized sources, but to determine whether variance in drone flight behavior is based upon normal flight-based activities or is indicative of a malicious actor or outside event.

The applications of supervised learning in identifying drone cybersecurity threats are myriad and continuing to evolve with researchers including Baig et al. (2022) utilizing event data and post-incident reports to classify in-flight experiences into normal and abnormal behavior for future digital forensic models and analysis. With a novel multi-dimensional methodology, Ahn et al. (2019), applied a variety of machine learning solutions to the factor-based modeling of drone cluster anomaly data, highlighting the ability to identify particular anomalies in drone performance probability. Whereas normal behavioral likelihood could be expressed consistently across multiple drones within a given swarm, the researchers’ findings suggest that probabilistic quantification of the variations in flight behavior and underlying kinematic values indicated significant departure from the collective norm by one specific drone (Ahn et al., 2019). By labeling onboard datasets and adopting various algorithmic solutions, including a deep neural network for training and verifying real flight data anomaly detection, Ahn et al. (2019) confirmed the viability of machine learning applications for online monitoring of system variations in real-time drone swarm
operations.

This chapter provided an in-depth review of the spectrum of literature on drone operations, security challenges, and machine learning solutions. This field continues to evolve as many researchers recognize the intrinsic value of an autonomous or unsupervised machine learning system to detect anomalies in drone behavior or sensor data. Within these varied approaches, researchers have adopted common techniques focused on specific themes related to the reliability of quantitative models, the accuracy of security monitoring, and the portability and lightweight value of an on-board threat detection system. Such considerations are magnified for drone swarm behavior monitoring, and therefore, reflect a deeper level of complexity that must be resolved through some degree of structural modification and systems control.

2.8. Conceptual Framework

The findings in this chapter demonstrate that it is possible to extrapolate a conceptual framework to shape and focus the experimental tests introduced in subsequent chapters to explore swarm behavior monitoring with reference to specific, real-world datasets and drone reporting insights. Figure 5 provides a visual representation of the following core concepts and their relationship to drone security monitoring and management.

Security Protocol: To secure drone operations, operators are expected to follow a reliable protocol that involves monitoring threats, recognizing variations or
inconsistencies in flight patterns, applying intervention methods or restrictions, and recovering assets.

Fingerprinting and Identification: Within a given drone swarm, identifying features such as the MAC address can be used to fingerprint drones, whilst in-flight signaling such as separation, alignment, and cohesion can be used to frame the continuity and consistency of the flight path (Li et al., 2017; Medaiyese et al., 2021).

Attack Vectors: The spectrum of in-flight attack vectors is diverse and technology-limited; however, it generally involves DoS attacks, hijacking, spoofing, or interference (Singh and Verma, 2017; Johnson, 2020). Narrowing attack risk profiles is a critical antecedent to the targeted identification and analysis of operational risk profiles as they relate to drone flight paths and regional environmental assessment.

Monitoring and Detection: Key features of the drone dataset are required to identify security threats and aberrations including operational variables (e.g., motor speed, flight direction, behavioral consistency) and communication variables (e.g., GPS strength, RC strength, proximity signals) (Chibi et al., 2021; Hsieh et al., 2021; Kumar and Agrawal, 2021).

Analytical Tools: The range of machine learning capabilities identified within the literature review includes a variety of highly effective classifiers that can be used in real-time to evaluate the relationship between expected and realized operational outcomes (Naïve Bayes, Random Forest, SVM, Linear Regression) (Feng et al., 2020; Baig et al., 2022; Syed et al., 2022) Swarm Sensing and Coordination: The flocking
protocol for swarm flight operations is based upon an optimized, central solution through which operators can map normative and aberrant behaviors over time to determine the likelihood of threat to the broader swarm objective (Hauert et al., 2011; Ahn et al., 2019; Jia et al., 2019).

Drawing upon these core conceptual considerations, Figure 5 provides a visual representation of the multi-dimensional relationship between drone operations and security threat identification and mitigation. The initial phase of this framework establishes the normative dimensions of drone identity and operational tolerances, integrating known vectors such as flight plan information, GPS data, and baseline signal strength into the threat assessment procedure. Downstream behavioral monitoring and threat detection recognizes the risk profile of various threat vectors including DoS, hijacking, spoofing, and signal interference. Although these threats may be recognized, they cannot be actively monitored by using standard drone data and control-drone communication channels. Instead, an advanced, machine learning solution is required that draws upon one or more of the four algorithmic models including Naïve Bayes, Random Forest, SVM, and Linear Regression.
Figure 5: Conceptual Framework
2.9. Summary

This chapter has provided an in-depth review of a broad spectrum of literature on drone operations, network security risks, data mining and analysis, and machine learning. As researchers expand their focus to include defensive capabilities, the role of real-time drone security monitoring in supporting operational continuity and reliability is increasingly critical. In large scale systems such as drone swarms or long-distance coordinated flight networks, the consequences of in-flight disruption can be severe and range from lost assets to catastrophic crashes. Therefore, additional research is needed to develop a real time drone fingerprinting and security monitoring capability that can be applied to the systematic analysis of onboard flight information. The following chapter outlines the methods that were adopted for this study, highlighting the comparative approach to supervised machine learning and drone data analysis that was developed to realize a long-term goal of security and operator support.
Chapter III.

Methodology

3.1. Introduction

The array of methods and data collection techniques outlined in the preceding chapter highlights the breadth and scope of the field of study in drone operations and security management. By comparing several experimental methodologies with the primary aim and objectives of this study, the following sections provide a critical evaluation of research design and methodological techniques. These sections use an exploratory, experiment-based design to discuss the resources, technologies, and software solutions developed for this study. Finally, key limitations and potential technological hurdles of the targeted approach developed for this study are presented.

3.2. Experimental Design

The research design has focused on detecting anomalies in drone flight paths through the analysis of on-device data to ensure safe drone utilization and prevent compromised drones from being actively used. Due to data collection and scope difficulties, labeled and effectively classified flight datasets for UAVs are restricted.
Therefore, operators lack the information and capabilities to detect flight anomalies in real-time (or even post hoc), limiting their ability to mitigate malicious attacks. Whilst Baig et al. (2022) and Syed et al. (2022) have demonstrated the validity of more advanced data analysis techniques, this study extends such findings and demonstrates the classification-oriented, factor-based insights needed to fingerprint and monitor drone behavior in more complex, swarm-based systems. There are several recent studies that discuss the detection of anomalous data-points in drone flight data (e.g. Bronz et al., 2020; Medaiyese et al., 2021; Baig et al., 2022; Syed et al., 2022). Other investigations have targeted specific indicators related to variations in drone flight behavior, such as Liu et al. (2017) who modeled abnormal patterns in drone motor temperatures and Zibaei et al (2018), who present detection of drone in-flight faults caused by software, sensor, and actuator failures. Such techniques require a machine learning solution capable of distinguishing between normative and aberrational in-flight behaviors.

For the purpose of detecting and classifying or defining such aberrational events, this investigation focuses on steady-state variables such as drone motor speeds and telemetry models to identify potentially unusual events recorded in drone logs. Drone log analysis techniques described in Syed et al. (2022) and Siddiqi et al (2022) illustrate that flight logs may help detect such faults. The approach developed for this study combines these techniques and makes extensive use of the parsed data delivered from the drone motor, accelerometer, and altitude datasets, to detect a crash
or an attempt to crash a drone. By applying post hoc, machine learning techniques to the multivariate analysis of drone datasets, it was possible to effectively train AI programs to not only detect anomalies, but to reliably analyze targeted data in future flight events to show similar patterns and identify specific records that point to malicious attacks, interference, or drone hijacking. In fact, by dividing the onboard risk profile of drone classifier data into key subsets, this study was able to utilize the fingerprinting approach to further typify the risk profile of various events according to their attack vector including DoS, hijack, or interference.

This study also considers the nature of intra-swarm drone operations when assessing the implications of the quantitative analysis procedures developed for this machine learning experiment. Although the datasets presented in this study are based upon individual drone flights and a single operational mission (e.g., point to point behavior), when extrapolated across multiple drones in a single swarm, it was possible to weigh the Reynolds flocking protocol and its three-tiered paradigm of separation, alignment, and cohesion when recommending an optimized, machine learning model to support future security protocol. Research conducted by Johnson (2020) and Hambling (2021) has provided critical insights into the range of threats confronting swarm activities and the technological imperative of a signal-based standard that leverages the swarm flocking behavior and signal communication to secure against outside actors. Methods developed by Ahn et al. (2019) and Johnson (2020) provide critical insights into the multivariate structure of drone data analysis within swarm
domains and the critical role of real-time flight tracking along the central domain as targets or routes are pursued. Ultimately, the machine learning criteria developed for single drone analysis is extended to include a signal-based assessment of in-swarm radio signals that can be applied to future security system design.

3.3. Algorithms, Models and Computing

The first stage of this exploratory procedure was to obtain the DJI Phantom 4 flight logs in DAT format from VTO labs drone data set online (VTO Labs, 2022). Once downloaded and unzipped, a similar procedure to those used by Mekala et al. (2019), Baig et al. (2022) and Syed et al. (2022) was performed to convert the DAT format files into CSV format using DatCon and CSVView. Once converted, each individual file was analyzed to ensure complete and properly formatted datasets. Subsequently, the findings were analyzed using Python as the primary programming language (as well Extract-Transform-Loading). The drone dataset comprised pre-classified information captured by the main recording parts of the drone including the gyro stabilizer, on-board flight computer communication system, flight controller, power supply, GPS modules and similar data sources. Categories of data fields available in these flight logs are listed as follows: Air Speed, Battery Status, Battery Info, Clock, Compass Filter, Controller, ATTI_MINI (Attitude Mode), Motor and Motor Control, GPS, IMU_ATT (inertial measurement unit), RC_info (radio controller information), OSD Data (on screen display) in addition to State Signals (which are
fields indicating the state of the drone) (Siddiqi et al., 2022).

Figure 6 breaks down the standard DJI drone file structure, highlighting several critical datasets including packetized representations of flight behavior, radio frequency stability, and operational status.

![Diagram of DJI DAT File Structure]

Figure 6: Breakdown of a DJI DAT File Structure (Source: Clark et al., 2017, S9)

The primary aim of this study is to test a machine learning-based approach and produce a two-tier anomaly detection framework for detecting compromised or infected drones. The methods applied in this study can detect the following forms of compromise: hijacking of a drone to change controllers; signal jamming of the drone’s navigation system to change flight path or cause mission failure; and Denial of Service
(DoS) attacks that send too many packets to a drone and cause malfunction. As the flight data logs include full flight path information and associated onboard responses from start to finish, the output model represented both normative and aberrant behaviors, requiring targeted pre-processing to facilitate deeper anomaly detection and analysis (Kumar et al., 2021). Once the data had been normalized, grouped, and classified, datasets could then be analyzed for various unusual data points that match the attack scenarios listed above. The simulations and machine learning-based data clustering tasks were performed using Python Scikit-learn libraries (Pegregosa et al., 2011). The following section details these approaches and their specific software resources.

Due to the breadth of academic research on drone data and security-related considerations, analytical organizations such as VTO Labs (2022) have captured and compressed extensive, anonymized databases into downloadable Zip files on public portals. This study uses a specific dataset from this public portal to analyze DJI Phantom 4 flight behavior. The public pathway to the specific file adopted for this study is identified as follows:

```
\Drone_Forensics > DJI_phantom_4 > df005_DJI_Phantom_4 >2018_June
> flight_logs> flight_logs.zip
```

The procedure for data extraction and analysis was derived from several prior studies in this field including those by Kumar and Agrawal (2021) and Baig et al. (2022). The structured and systematized guidelines introduced by these researchers
highlight the ease of access associated with UAV datasets, particularly if they are publicly accessible. The 4.8GB zipped DAT file was downloaded and extracted from the VTO (2022) database. Despite a robust spectrum of data, much of the report was incomplete or failed to provide a comparable range of drone readings. This required distilling the evidence to only those data files that reported the full set of 288 features related to state signals within the flight logs. Once the data subsets were selected, they were converted into CSV files to facilitate viewing and analysis. The exclusive DatCon tool was used to extract the underlying data in sequence at 10 Hz, a low but sufficient sampling rate to achieve a high degree of consistency and analytical insight. The output was loaded into the machine learning tool and transformed using state signals, or those categorical fields that indicate the state of the drone during flight. Only time series categorical fields were extracted to reduce the scope of evidence trained and analyzed, thereby increasing the predictability of the machine learning algorithm.

Once the data had been converted, the analysis and machine learning required an appropriate training procedure that could identify anomalies in the dataset. As the drone’s flight path is normalized according to an array of multi-dimensional indicators (e.g., latitude, longitude, motor speed), the study predicts that applying the appropriate analytical tool can expose abnormal patterns.

The gaussian mixture model (GMM) is defined as a ‘probabilistic model that assumes that the given data points are samples generated from a mixture of a finite
number of Gaussian densities’ (Arora et al., 2021, 262). The Gaussian densities suggest that normal densities can be represented by the intra-group mean and associated variance. By applying this soft clustering approach to the data distribution, each of the different points are characterized by the conformity to this normative distribution, as visualized in Figure 7. This model demonstrates various mean distributions and variance levels on a single dimensional plane.

![Various Gaussian Distributions](image)

**Figure 7: Various Gaussian Distributions with a Difference in Mean and Variance**
(Source: Singh, 2019, 1)

Following this initial clustering approach, the study adopted and explored an array of supervised learning algorithms including Naïve Bayes, SVMs, K-Means, and
Random Forests models. A key challenge for anomaly detection is the severely imbalanced class distribution, i.e., anomalous examples being extremely rare compared to normal examples. One state-of-the-art solution is to apply one-class classification algorithms (Seliya et al, 2021) which train a generative model for the normal class based on only normal examples and apply the model to classify a new example as normal or anomalous, for example, simple, lightweight one-class SVM (Manevitz & Yousef 2001), and deep learning based Deep Support Vector Data Description (Ruff et al, 2018) and one-class LSTM (Li et al, 2022). The study subsequently adapted a bootstrapping strategy to process the bulk of the training data (about 2/3rd) samples and test the model’s accuracy. This approach ensured that the classifier would have ample data to train on and produce a model that could be applied to the remaining dataset. This remaining (1/3) data was set aside for later model testing and confirmation. The machine learning model was pre-trained using the training data to produce a decision tree, and the remaining data was used to validate the trained random forest decision tree model, and thus ensure accuracy. This tree was pre-trained using each supervised learning algorithm, to determine which provided the best results and learning outcomes for the analysis going forward. The outputs could then be critically compared across the various machine learning solutions to determine the best fit in terms of accuracy, precision, recall, and training time.
3.4. Data Analysis

To accomplish the central research aim, the investigative process first utilized a common clustering technique, GMM for cluster and outlier analysis. K-Means cluster model was also deployed to provide additional depth and comparability of the techniques used to analyze the flight expectation distribution of the underlying clustered flight data (Singh, 2019). This procedure was undertaken to identify anomalous points in the dataset and used data from a subset of the flight logs prepared. Rather than using Euclidean distances, the GMM, which utilizes probability distribution of various data points (primarily the feature-value tuples present in my dataset), was adopted (Singh, 2019; Syed et al., 2022). This approach ensured that the appropriate and relevant data distributions in the dataset could be measured. One of the primary advantages of utilizing GMM is its ability to analyze data points that belong to the same cluster and fall within a Gaussian distribution. Hence, each distribution is defined as a unique cluster, allowing further analysis of the flight path data for this data subset (Syed et al., 2022).

The purpose of the GMM approach was to predict the probability of normalization with accuracy, whereby data points fall within a given density function or curve based upon multiple 3-dimensional comparisons (e.g., multi-vector) (Singh, 2019). Whereas alternative methods such as K-Means clustering uses an iterative interoperation of the mean value to link and cluster multiple data points, it fails to consider the broader distribution of the distributions and their associated variance.
levels (Singh, 2019). Therefore, this study began by capturing GMM and K-Means clustering outputs to demonstrate variations in key indicators such as flight path and pitch and roll indicators. Subsequently, various machine learning algorithms were used to assess the relative consistency and accuracy of each approach to data processing and anomaly detection. Intending to identify a lightweight procedure for in-flight drone fingerprinting and anomaly detection, this procedure was designed to either include or exclude those techniques that would offer the highest level of analytical consistency.

A unique challenge in drone anomaly detection stems from the hardware constraints and network bandwidth limits that affect onboard security and threat monitoring. This study proposes a two-tier anomaly detection framework starting with a pre-screening step that flags anomalies or attacks using a lightweight model, followed by a fine-grained detection step to confirm an anomaly and further distinguish it using a heavyweight model. In real-world applications, ML models for the pre-screening step can be deployed on drones, while models used for the detection step can be deployed on a centralized server. It is important to note that a DoS attack, even for legacy systems, is hard to distinguish from flash crowds comprising legitimate network traffic, though their impact on the victim device (in this case, drones) is the same (Adi et al, 2016). As such, it was necessary to consider the specific machine learning methods used. Of these, the random forest classifiers represent a form of ensemble-based classifiers, used for effective and robust image classification.
of the data captured by a drone. In contrast, SVMs represent supervised machine learning algorithms which are part of the linear classifier family. They both operate by constructing an N-dimension hyperplane which maximizes the margin between two identified classes of data. Finally, a Naïve Bayes classifier represents a simple probabilistic technique applying the Bayes theorem to assign a posterior probability that a given data sample belongs to a given class, based on the pre-training of the classification algorithm. Each of these machine learning methods were weighed and considered for inclusion in the machine learning model developed over the course of this study. The procedure for applying various machine learning algorithms to the normalized and pre-processed datasets is outlined as follows:

- Download and installl Python Release 3.11
- Deploy the Scikit-learn libraries
- Conduct K-Means and GMM tests to establish baseline measure for comparison and visualize in-cluster aberrations relative to drone flight patterns.
- Adopt various algorithmic solutions (Random Forest, Naïve Bayes, Linear Regression, SVM) to data analysis.
- Increase the number of estimators to weigh consistency and/or accuracy of output.
- Calculate optimal curvature of the algorithmic differentiation capability.
• Present quantitative comparisons of key indicators for ML effectiveness (e.g. accuracy, precision, recall, training time)

• Identify the best fit solution and make recommendations.

After presenting the evidence related to machine learning outputs, the concept of drone fingerprinting that has been previously analyzed by Clark et al. (2017), Li et al. (2017), and Medaiyese et al. (2021) was considered. Specifically, operators must not only be able to monitor the operational status of all drones in a given swarm, but they must be able to rapidly identify the fault profile of potentially infected or disrupted drones following an attack. This means that whilst datasets might demonstrate variations in pitch, roll, altitude, etc. due to flocking behavior, machine learning systems must be able to parse aberrations to determine which criteria predict a malicious attack and not normative behavior. By applying several techniques developed in prior studies to the VTO Labs dataset interpretation in whole (e.g., a combined swarm rather than individual drone activities), the antecedents to a reliable and predictable drone fingerprinting and compromise identification model have been developed and presented. The end result is a theoretical model that can be adopted to future experiments in order to utilize integrated signal data to improve the reliability of drone flocking through in-swarm security data.
3.5. Limitations and Challenges

Though the datasets in this research were anonymized, there were potential ethical concerns considered when selecting and structuring the data for this investigation. For example, while this research provides drone operators with improved security protocol and attack-based analytical capabilities, it may inadvertently affect authorities’ ability to control and capture rogue drones, such as those that affected London’s Gatwick Airport in 2018 (O’Malley, 2019). Further, there is a form of security reciprocity; models predicting security threats create heightened security profiles and improved automated attack detection capabilities that are beneficial for drone operators across commercial, military, and civilian populations, but they may also inform perpetrators’ countermeasure design and enhance their innovation and accuracy. Whilst these security techniques can be used to mitigate future threats, drone owners and operators must continue advancing their own technological capabilities and security protocols.

The computational set influence key measures captured within this study such as classification, thereby predicting cost profiles according to scalability and technological demands (e.g., number of drones). This study has undertaken efforts to maintain a lightweight and relatively simple solution that could be transferred to any formation of drones (individual or swarm) so that operators can increase their security standards and flight reliability. Despite such efforts, the results may not necessarily be cost effective in future applications where multiple or large-scale swarm datasets
make processing and analysis more complex. Although DJI and the Phantom Drone are widely recognized in the industry as high-functioning quadcopters, there is an array of drone manufacturers whose precision and communication standards could skew the accuracy of this evidence when considered for other models or systems. Therefore, the reliability and application of this data is limited to the target case, but this study’s methods and approach could be transferred to other applications in the future and maximize their security monitoring capabilities. This consideration for the transformative and practical applications of this study to future scaling cases is discussed throughout the subsequent chapters.

3.6. Summary

This chapter provided an in-depth view of the methods adopted in this study and highlighted the importance of data processing and analysis in framing the practical and accurate assessment of anomalous events in drone flight management. The procedure selected for this study is designed to systematically distill the range of algorithmic and analytical tools into best-fit solutions for future applications. Therefore, the results presented in the following chapter draw upon replicable techniques that can be integrated and applied to an array of future data analysis and security management problems. Ultimately, these stages extend prior research in this field by demonstrating the effectiveness of specific classifiers and prescribing a lightweight, onboard supplement for real-time security monitoring and threat assessment.
4.1. Introduction

The lack of onboard data encryption and end-to-end network security has resulted in various exploitable security vulnerabilities that threaten drone operations. For drone manufacturers and flight operators, the relationship between control and performance is viewed as direct or linear. However, with exploits and security threats becoming more complex and diverse, the scope of risks to drone operations is a circular, oftentimes, fragmented proposition. To analyze this phenomenon, a dedicated series of real-time data from public repositories has been downloaded and processed, thereby applying machine learning techniques to the design and implementation of a reliable, lightweight security monitoring solution. The following sections progress through the stages of this analysis, demonstrating the variations in drone operations, the consequences of data and signal aberrations, and the proposed machine learning solution to this complex problem.
4.2. Dataset

Several sources of evidence considered for this study, including field research and recorded data. Despite the advantages of performing field-based research, it restricted the likelihood of achieving consistent and comparable outcomes, and therefore, recorded data became the core target for the data collection procedure. A standardized dataset was downloaded from a public server at VTO Labs (2022) to maximize the reliability and comparability of the data analysis. These DAT files included 40 distinct flight logs captured from flights undertaken by a specific DJI model, the Phantom 4 drone. Once downloaded, the DAT files were converted to CSV files that could be viewed and visualized using dedicated software. This study used the DatCon to perform the conversion, whilst the CSVView software was used for the viewer and visualization model of the output dataset. Although the specific database may have contained a significant number of DAT files, pre-processing and factor validation exercises revealed that only 20 datasets were valid. The following section provides a brief overview of each software suite employed and their role in normalizing and focusing the underlying datasets.

4.2.1 Time Series and State Signal

The Version 4, 2020 iteration of DatCon was designed to convert a DAT log file for various drone models (e.g., Phantom 3, 4, Mavic Pro) into a CSV file. These files are generated by the Go and Fly apps provided by the drone manufacturer and can
be processed and converted regardless of platform. Figure 8 depicts the user interface and highlights several essential input elements, including the time axis specifications, the output file specifications, the input file specifications, and the Menu Bar to fine-tune the process. Within the Menu Bar there are several preferences. One specific preference that must be selected to improve the relative accuracy of the data outputs is the ‘Validate Coords’ checkbox, which directs the software to remove incorrect (intuitive, localized) GPS coordinates from the map display.

![DatCon User Interface](source: DatCon, 2020)

The Time Axis Panel allows the researcher to select Smart Time Axis process-
ing to engage automatic time settings in the axis panel, or to specify explicit time intervals in order to reduce the relative output size of the CSV. Further, interval selection can target specific time series or may exclude an aberrational event such as weather events or electromagnetic interference. The Time Axis Shift checkboxes on the panel shift time to start at either Flight Start, Motor Start, or Recording Start, allowing the researcher to control where 0.0 is set for the recorded dataset. In this instance, the default options were used, focusing on the flight start indicator so that the entirety of the flight route could be analyzed.

The CSV panel allows the researcher to specify the size of the CSV file by specifying an explicit sampling rate which ranges from 1Hz to more than 214 million Hz. Whilst lower sample rates produce a smaller subset, they are considerably less precise. The software is set to default to 30Hz; however, this is designed for single flight or single unit data analysis. By applying a consistent 10 Hz sampling rate to the DatCon procedure in the current study, the CSV files attained a sufficient degree of fidelity, but could be managed and analyzed using a moderate and non-excessive level of computing power and visualization. Other options such as the output file specifications were ignored, leaving the default settings active to ensure post-output comparability.

The output of the DatCon CSV is organized into signal groups that subdivide signals into their corresponding columns in the CSV. For example, signal groups such as Longitude, Altitude, and MagYaw are used to display GPS coordinates and the
associated rotation of the craft relative to the static points in space. As field names are proprietary and defined by the onboard software used by the UAV, selective and targeted definition of output signals may be required depending upon the length and accuracy of the field designation. For this study, the following core field codes were used to specify and normalize the analytical output of the CSV data:

- **Time Series Signals:**
  
  Air Speed
  
  Attitude Mode
  
  Battery Status
  
  Battery Info
  
  Compass Filter
  
  Clock
  
  Controller
  
  GPS
  
  Inertial Measurement Unit
  
  Motor and Motor Control
  
  On Screen Display Data
  
  Radio Controller Information
• State Signals: Unique signatures and/or radio frequency fingerprints that represent:

  Transient state of the RF signal during power on/off
  
  Steady state of the RF signal during flight
  
  Signal to Noise Ratio

Despite the importance of state signals in detecting intrusions and analyzing RF interference (Medaiyese et al., 2021), they were considered to exceed the scope of the current exploratory analysis. Therefore, only time series signals were selected for this study. Figure 9 provides a brief representation of some of the 288 features included in the flight log output. Within each of these field groupings, many different modifiers were identified, with variations specific to the drone traits and/or flight variables recorded during each of the associated events. From the perspective of flight diagnosis, comparison of prior studies in this field helped determine (e.g., Bronz et al., 2020; Medaiyese et al., 2021; Baig et al., 2022; Syed et al., 2022) that the osd_data:navHealth category was associated with GPS signal and RC signal strength dimensions that could be linked to DoS attacks and/or signal interference. Other factors such as variations in IMU_ATTI(0):Latitude and IMU_ATTI(0):Longitude during the flight path could be linked to aberrant changes in flight behavior, thereby representing a malicious hijacking attack. Figure 9 presents some of these fields and their associated description related to drone flight operations and navigation or signal health.
4.3. Drone Flight Logs Analysis

Developed as a technological solution to the complexity of DatCon outputs, CSVView (2022) supports drone flight log visualization and a variety of output file types including TXT and DAT. The simplified SigPlayer is used to display flight variables across the X-Y axis and provides status information that is subdivided into either State or Time Series datasets. For each of the 20 DAT files, a CSV visualization was created, resulting in overlaid dimensions that could be independently compared and, through charting visual anomalies, analyzed across the time series datasets. For example, Figure 9 provides a normalized representation of the navigational health reported for Flight 05, a path which includes a buildup of speed, continuous operational flight, and then a decline in speed prior to landing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMU ATTI(0): Latitude</td>
<td>Drone’s geographic north-south location relative to Earth’s surface</td>
</tr>
<tr>
<td>IMU ATTI(0): Longitude</td>
<td>Drone’s geographic east-west location relative to Earth’s surface</td>
</tr>
<tr>
<td>IMU ATTI(0):distanceTravelled</td>
<td>Distance traveled by the drone from the start point</td>
</tr>
<tr>
<td>osd data:navthealth</td>
<td>Navigation health of the drone relative to the number of GPS satellites that it is connected to where 0=unreliable and 5=excellent signal reception</td>
</tr>
</tbody>
</table>

Figure 9: Fields Included in Drone Flight Log Output
By selecting specific indicators such as the relative height of the drone, the navigational health of the GPS signal, and the controller pitch, Figure 10 depicts a phase-based relationship between input factors and drone performance during the representative flight. The model highlights a relatively consistent relationship across these various criteria, with several exceptions during drone phase changes (e.g., take-off, landing, elevation change).
In contrast to the relatively constant flight health reported during Flight 05, Figure 11 demonstrates the anomalous representation of intra-flight disruptions at two key points during Flight 028 that indicate deficiencies in flight health function. Appendix A provides a data-based representation of those key indicators that highlight variations during the Flight 028 path including distinct changes in height, signal strength, and GPS strength that could signal anomalous effects and malicious actors.
Combining the same indicators from the normative flight path in the previous model, Figure 12 provides a visualization of an aberrational flight path that includes significant disruption of navigational health at two key points, a progressively increasing, but inconsistent flight height, and a variable pitch effect that resulted in several severe, unpredictable outcomes. Although this behavior could be attributed to pilot errors or programmed rise/fall activities, the significant drop in navigational health at key points during the flight path suggests interference or a ground-based event.
Figure 13: Multivariate Representation of Aberrant Patterns in Flight 28

When overlayed in Figure 13, the implications of flight disruption on flight nav health are identifiable by distinctive changes in motor performance at the same points in which flight health was negatively impacted. Specifically, at the first anomalous point, there was a significant decline in the motor speed of the Left Front motor. At the second anomalous point, there was a significant decline in the motor speed of the Right Back motor. Each of these outputs could potentially lead to an in-flight catastrophe, route change, or high-risk behavior. In a swarm environment, the consequences for multiple drones encountering aberrations during planned flight patterns could severely undermine the performance of the exercise or mission.
A similar correlation between the flight navigation health and the anomalous decline in motor speed can be seen in Flight 013, wherein a single point of critical failure almost resulted in immediate cessation of drone operations. Figure 14 overlays four different motor speeds with the navigation health during the flight period. Importantly, following the loss of motor function, subsequent motor performance was found to operate at a much higher speed than previously recorded during the drone flight path, signaling a distinct and measurable change in behavior. This form of post-interference compensatory behavior could lead to higher battery drain, lower range, and unreliable flight planning in the event of targeted disruptions.
Within the normalized flight data there are paired indicators of consistency, where correlation between flight speed, motor speed consistency, navigational health, and other time series indicators like relative height and UAV pitch can be used to systematically model expected behavior. Alternatively, disruptive or anomalous events, such as GPS attacks, utilize jamming, hijacking, and interference to contravene flight health, as demonstrated by the preceding two examples. Reliability, as framed by the regular, consistent signal health is moderated by variations in the onboard signal received by the drones in this analysis. Figure 15 provides a multi-dimensional representation of the consequences of anomalous events during drone flights, as highlighted at the early stage of the flight path for Flight 035. Specifically, this model demonstrates a loss of GPS signal fidelity, a significant decline in navigational health, and a subsequent loss of latitudinal and longitudinal coordinate awareness prior to
recovery and signal normalization.

Figure 16: Nav Health, Height, Lat, Long, and GPS Disruption Flight 35

A comparative review of flights across all 20 of these sub samples has revealed that where most drones encountered some form of interference or disruption, it is direct signal interference that most significantly affected drone reliability and flight path continuity. In fact, where some drone navigational health readings were highly consistent, variations in GPS readings such as the loss of longitude or latitude could be compensated during the flight and path recovery was attainable. However, when disruptions were more significant, as in Flight 035, the effects over the long-term flight performance were significant. Such impacts are shown in Figure 16, where early-phase disruptions led to an inconsistent flight path, whilst mid-term in-flight patterns demonstrate a significant increase in elevation and very localized lat/long coordinates.
Figure 17: Geolocation Route for Drone Flight 35

Although difficult to diagnose post hoc, DoS attacks on drone operations result in a severe loss of navigational health, interference with the drone power supply, and/or a sudden decline in drone motor speed. Figure 17 depicts a significant motor speed disruption for Flight 036 that occurred despite receiving consistent GPS signal during the flight period (light blue line). Due to the loss of motor continuity, the relative flight height of the drone declined significantly, resulting in a crash or near-
crash effect. In this instance, a hijack attack may have been used to access the drone ground controller or to take remote control over the drone via intermediary communication or onboard signal exploits.

Figure 18: Flight Disruption Model Flight 36

Returning to the anomalous signal patterns and navigational health observed in Flight 035, Figure 18 demonstrates the effects of a DoS attack on the RC controller frame loss and the relative signal strength. As these flights were recorded in non-urban areas with low levels of environmental signal interference, barring other onboard deficiencies such as controller signal losses or distance effects, the frame loss and signal strengths effects should have remained constant during the flight. However, the data suggests that interference, potentially from a DoS attack or other signal-jamming or dilution effect (e.g., other drones on same channel nearby) resulted in anomalies during the flight path.
In developing the training model for this study, anomaly data was critical to providing the machine learning system with sufficient criteria for an accurate probabilistic representation of external (versus internal or onboard) interference. Events during which communication between the control unit and the drone was lost were selected for representations of DoS attacks in the training set.

Returning to the aberrational flight path observed for Flight 028, it is possible to clearly identify the impact of a DoS or other related interference-based event at a key point during the flight path. Despite thousands of lines of data, the drone recorded during this period, inference was observed at key variations in the RC signal strength reporting, as shown in the fifth column of this chart. The resulting impact involved a shift in the OSD_Data RC connection from “Connected” status to “DisConnected.” The consequences of this event were significant, as demonstrated in the fourth column or RC_Info:failSafe when the drone shifted from “Hover” to “Landing” status. This was an unplanned, failure-based system response that could have caused serious loss...
of equipment or other negative impact. Whilst the model in this figure provides only the initiating lines of code related to the change in direction of travel, it is clear that following the response, the drone transitioned from a rising effect to a landing effect. Later recovery of the RC signal reversed this trend from landing to hovering and the drone again rose to its predefined flight height. The gaps in Figure 19 are data-dependent and suggest that there was a significant change in the flight pattern of Flight 028 as further reinforced in the complete data in Appendix A.

<table>
<thead>
<tr>
<th>Key Variation Report Data from Flight 028</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMU_ATT[0].direction OffTrav[Mag].C</td>
</tr>
<tr>
<td>IMU_ATT[0].direction OffTrav[Ir].C</td>
</tr>
<tr>
<td>GPS: velD</td>
</tr>
<tr>
<td>RC_Info: allSafe</td>
</tr>
<tr>
<td>RC_Info: sigS: strength: C</td>
</tr>
<tr>
<td>OSD_data: connectedToRC</td>
</tr>
<tr>
<td>80.22126883</td>
</tr>
<tr>
<td>80.22126883</td>
</tr>
<tr>
<td>-0.06 Hover</td>
</tr>
<tr>
<td>66.666667 Connected</td>
</tr>
<tr>
<td>-0.06 Hover</td>
</tr>
<tr>
<td>66.666667 Connected</td>
</tr>
<tr>
<td>-0.04 Hover</td>
</tr>
<tr>
<td>66.666667 Connected</td>
</tr>
<tr>
<td>-0.04 Hover</td>
</tr>
<tr>
<td>66.666667 Connected</td>
</tr>
<tr>
<td>-0.03 Hover</td>
</tr>
<tr>
<td>9.523809 Connected</td>
</tr>
<tr>
<td>-0.03 Hover</td>
</tr>
<tr>
<td>9.523809 Connected</td>
</tr>
<tr>
<td>-0.02 Hover</td>
</tr>
<tr>
<td>9.523809 Connected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
<tr>
<td>-0.01 Landing</td>
</tr>
<tr>
<td>0 DisConnected</td>
</tr>
</tbody>
</table>

Figure 20: Key Variation Report Data from Flight 28

4.4. Model Design Stages and Classifier Selection

This study was split into two stages, including procedural imperatives related to the management and converting the data into comparable outputs that could be
adapted to machine learning initiatives. As presented in Figure 20 this procedure involved pursuing two outputs, namely the K-Means cluster analysis and the GMM machine learning output that could be compared for accuracy and consistency following the execution of these procedures. To train the dataset for the machine learning exercise, the flight logs were converted to DAT and then to CSV. Narrowing the sample dataset through pre-processing was imperative to reduce the range of overlapping and unnecessary measurement criteria, thereby restricting the data to a series of comparable classification dimensions.
Figure 21: Procedural Design of GMM and Machine Learning Analysis
The K-Means cluster was the first data processing performed, with several key indicators modeled to show the integral consistency of the dataset. For example, Figure 21 demonstrates the flight path cluster measured by distance traveled across all flight domains, with latitude clustering providing the central modifier. Within this model, it is evident that the longest flights were flown along the 40.2 latitude, whilst shorter flights were flown below 39.6 latitude.

![Figure 22: K-Means Flight Path Clustering by Distance Traveled](image)

The second dimension demonstrated in Figure 23 was the pitch vs controller throttle which included a positive and negative domain for increasing and decreasing throttle response. Whilst the majority of flights fell within the mid-band pitch data,
the model highlights outliers that can be used to identify possible in-flight aberrations.

Figure 23: K-Means Pitch vs Controller Throttle Analysis

Where the K-Means output groups the flight records into three individual banded color groups based upon Euclidean distances from the center of the clusters, Figure 23 presents the GMM output, markedly different. Specifically, the granularity of the GMM clustering effect demonstrates a smaller pitch range, banding a larger number of throttle-based actions across two longitudinal pitch bands that are able to better highlight aberrational events where pitch moved beyond the normal mediative banding.
The K-Means trajectory cluster shown in Figure 24 creates some confusion due to the banding effects across the three shaded areas, with high-pitch, high-roll events linked together with other, normative data outputs.
In contrast, the GMM output in Figure 25 highlights the same pitch vs roll dataset but reduces the visual noise by clustering outlying datasets into a single banded dark color. Mid-range and central grouping plots fall within the mediative zero for pitch and roll, but variations beyond the 100 (pitch) and 20 (roll) degree zones provide indications of possible aberrational behavior (e.g., Dos, hijack attempts, loss of RC signal).
The pre-processing initiative identified a series of 12 flight path classifiers that could be extrapolated from the extensive series of 283 indicators. For most flights, the onboard data reports determined the integrity and completeness of the data provided. In some cases, due to data recording malfunction or flight failure, reports were incomplete or blank. This is why only 20 complete reports comprising all 12 of the flight path classifiers in Figure 26 were included out of the total 38. These classifiers were selected because of their direct relationship to UAV flight operations (e.g., motor speed, RC signal) and the relative accuracy of such flight operations (e.g., GPS, distance, pitch). As demonstrated in the preceding CSV visualizations, the correla-
tion between RC signal and UAV motor speed is significant, as are the associated flight behaviors. Key indicators such as NavHealth are correlated with GPS indicators such as height, latitude, and longitude and represent the core vulnerabilities associated with DoS and hijack-based attacks.

<table>
<thead>
<tr>
<th>Motor Speed</th>
<th>GPS Indicator</th>
<th>RC Indicator</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFront</td>
<td>IMU_ATT(0):relativeHeight</td>
<td>RC_Info:frame_lost:0</td>
<td>distanceTravelled</td>
</tr>
<tr>
<td>LFront</td>
<td>IMU_ATT(0):Latitude</td>
<td>Osd_data:navHealth</td>
<td>IMU_ATT(0):roll:C</td>
</tr>
<tr>
<td>RBack</td>
<td>IMU_ATT(0):Longitude</td>
<td></td>
<td>IMU_ATT(0):pitch:C</td>
</tr>
<tr>
<td>LBack</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 27: Core Flight Path Classifiers

4.5. Machine Learning Analysis

The machine learning analysis was administered using a local machine configured with an Intel Core i9-13900 2.0GHz processor, 16 GB of RAM, and a dedicated Python installation with the Scikit-learn library installed. Four clustering algorithms including Random Forest, Naïve Bayes, Linear Regression, and Support Vector Machines (SVM) were adapted for this study. By splitting the datasets into two samples, a training set comprising 80 percent of the available data from the 20 flights was initially segmented, whilst a 20 percent reserve dataset for validation and model analysis was subdivided. Central indicators of model performance such as accuracy, precision, and recall were established in relation to the accuracy of the algorithmic solutions.
Whilst output accuracy for three of the four algorithmic classifiers (Linear Regression, Naïve Bayes, and SVM) were assessed via standardized outputs, the random forest solution allows for model parameterization through the Max-depth function. Recognized as the relative depth of the tree function within the random forest, the complexity of the output is controlled by the Max-depth established for the algorithm. As a potentially influential selection decision, the impacts of such complexity on flight anomaly analysis could have negative implications on UAV securitization. Therefore, modulating the max-depth to establish an optimized, fit-based solution was an important stage of his procedure. The Max-depth range extends from 2 to 6, whilst the value for the number of trees in the random forest was between 5 and 15.

The training and analysis outputs were recorded according to their relative accuracy, the precision of the anomaly detection capabilities, the data recall, and the training time for each of the four algorithmic classifiers. The initial 80 percent subset of data was classified using a supervised machine learning procedure to ensure that accuracy and cross-comparability of the training outputs would be similar across the four modalities. With RF variations and GPS disruption serving as the primary predictors of anomalous flight paths and potentially malicious attacks, it became possible to modulate the relationship between normal and abnormal flight data. Once the training sets had been applied to each of the algorithmic functions, a supervised machine learning exercise involving classifier labeling was performed for the remaining 20 percent and a comparative performance output of the four algorithms was recorded.
Figure 27 depicts this comparative accuracy, precision, recall, and training time. This first model refers to the detection rates exhibited within the central training set. The Random Forest classifier was the most accurate while the SVM classifier was the least accurate. Importantly, the Random Forest approach was also the most precise by a significant margin. Whilst other classifiers reported higher recall times, this outcome was likely due to the tuning and complexity of the Random Forest depth and estimation outputs. Finally, Naïve Bayes had the lowest training time and SVM had the highest, while both Random Forest and Linear Regression maintained a relatively consistent, mid-range time.

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>Training Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Forest</td>
<td>0.9787</td>
<td>0.9832</td>
<td>0.845</td>
<td>0.3589</td>
</tr>
<tr>
<td>Naïve Bayes</td>
<td>0.8798</td>
<td>0.5645</td>
<td>0.984</td>
<td>0.0452</td>
</tr>
<tr>
<td>Linear Regression</td>
<td>0.8544</td>
<td>0.5453</td>
<td>0.991</td>
<td>0.4324</td>
</tr>
<tr>
<td>SVM</td>
<td>0.8434</td>
<td>0.4987</td>
<td>0.983</td>
<td>142.543</td>
</tr>
</tbody>
</table>

Figure 28: Comparison of Machine Learning Classifiers (Detection)

When combined with the remaining 20 percent of the dataset, the accuracy of the classifiers decreased in relation to the Random Forest, but increased across the other three algorithms, likely due to the extended models being assessed. The precision declined for the Random Forest, but also declined across all three other
classifiers, leading to performance degradation that could result in higher false positive readings. The recall performance was lower for all four classifiers, whilst the training time increased.

The performance in recall consistency is important when weighing the accuracy of multi-drone swarm anomaly analyzes. Training time is also an important consideration when weighing the overall efficiency of the assessment period, particularly during mission critical drone flights. These findings presented in Figure 28, suggest that despite lower recall performance, the Random Forest classifier demonstrates higher, more reliable performance overall. The Naïve Bayes classifier might demonstrate higher training time performance and recall outcomes, however the lack of precision constrains replication and future anomaly mapping.

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>Training Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Forest</td>
<td>0.9545</td>
<td>0.8935</td>
<td>0.7924</td>
<td>1.4563</td>
</tr>
<tr>
<td>Naïve Bayes</td>
<td>0.8839</td>
<td>0.4575</td>
<td>0.9689</td>
<td>0.0533</td>
</tr>
<tr>
<td>Linear Regression</td>
<td>0.8755</td>
<td>0.4535</td>
<td>0.9645</td>
<td>1.0543</td>
</tr>
<tr>
<td>SVM</td>
<td>0.8773</td>
<td>0.4254</td>
<td>0.9753</td>
<td>156.583</td>
</tr>
</tbody>
</table>

Figure 29: Comparison of Machine Learning Classifiers (Combined Execution)

To demonstrate the modulation of the Random Forest classifier, several different max-depth levels (2-6) and a broad range of estimators (5-7) were tested to
modulate the overall performance outcome. Figures 28 and 29 present the effects of these changes. The evidence demonstrates that accuracy, precision, and recall increased significantly with higher levels of depth; however, training time was also increased. As more estimators were added, accuracy levels and recall performance increased; however, precision decreased beyond 9 estimators, presenting an optimal state for model structuring. To summarize, the optimal solution to achieve the highest level of accuracy, precision, and recall with the lowest training time included a max depth of 6 and an estimator of 9.

<table>
<thead>
<tr>
<th>max_depth</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>Training Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.9438</td>
<td>0.8687</td>
<td>0.7402</td>
<td>0.2374</td>
</tr>
<tr>
<td>3</td>
<td>0.9515</td>
<td>0.9787</td>
<td>0.8445</td>
<td>0.2566</td>
</tr>
<tr>
<td>4</td>
<td>0.9787</td>
<td>0.9832</td>
<td>0.8454</td>
<td>0.3589</td>
</tr>
<tr>
<td>5</td>
<td>0.9895</td>
<td>0.9925</td>
<td>0.9386</td>
<td>0.3945</td>
</tr>
<tr>
<td>6</td>
<td>0.9938</td>
<td>0.9947</td>
<td>0.9545</td>
<td>0.4578</td>
</tr>
</tbody>
</table>

Figure 30: Max Depth Effects in RF Classifier
4.6. Swarm Modeling and Drone Fingerprinting

For both commercial and military operations, drone swarm modeling requires a classification system capable of predicting behavior on the basis of probabilistic constructs (e.g., path predictions, flight height, GPS location, and intra-swarm proximity. The preceding research demonstrates how algorithmic clustering models can be used to predict anomalous behavior in individual drones. However, the problem grows increasingly complex when differentiating between individual drones within a singular swarm. Characterized as particle swarm optimization pathfinding (PSOP), the algorithmic method of autonomous navigation for drones across dynamic environments requires considering several geo-spatial relationships including swarm positioning (e.g., flocking), obstacle avoidance (e.g., buildings, birds), and start-stop objectives (e.g., explicit or dependent) (Pyke and Stark, 2021). Introduced by Pyke and Stark (2021) as the ‘drone flock control’ (DFC) model, incorporating each of

<table>
<thead>
<tr>
<th>n_estimators</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>Training Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.9458</td>
<td>0.9785</td>
<td>0.7387</td>
<td>0.1354</td>
</tr>
<tr>
<td>7</td>
<td>0.9543</td>
<td>0.9734</td>
<td>0.7488</td>
<td>0.1825</td>
</tr>
<tr>
<td>9</td>
<td>0.9654</td>
<td>0.9645</td>
<td>0.7587</td>
<td>0.2852</td>
</tr>
<tr>
<td>11</td>
<td>0.9645</td>
<td>0.8954</td>
<td>0.8248</td>
<td>0.3545</td>
</tr>
<tr>
<td>13</td>
<td>0.9769</td>
<td>0.9854</td>
<td>0.8312</td>
<td>0.3785</td>
</tr>
<tr>
<td>15</td>
<td>0.9798</td>
<td>0.9868</td>
<td>0.8414</td>
<td>0.4032</td>
</tr>
</tbody>
</table>

Figure 31: Estimator Effects in RF Classifier
these elements into a singular, probabilistic output provides navigation assistance for drones operating within dynamic, often unpredictable environments.

As an individual unit within the drone swarm, each device retains its own hard coded serial numbers and information datasets. For example, Figure 31 provides a visual representation of the forensic drone teardown performed by Watson (2022) at VTO labs. Each drone can be physically identified through various p indicators such as the serial number, the QR code for the SD card reader, and other dedicated numerical indicators. However, the fingerprinting problem requires virtually monitoring drone flight behavior and not only detecting threats to such behavioral outcomes, but triggering swarm responses that are consistent, cohesive, and flock-based (e.g., bank left, pitch right, rise to 57m, return home).
In swarm operations, the Reynolds flocking rule-set establishes the parameters to prevent in-air collisions from swarm-based UAVs (Watson et al., 2003; Hauert et al., 2011); however, it lacks the ability to execute pathfinding or obstacle avoidance. The PSOP algorithm developed by Pyke and Stark (2021) is expressed as follows and proposes a viable solution for swarm dynamics according to inter-route pathfinding, distance optimization, and swarm navigation:

\[ v(t) = wv(t - 1) + c_1 r_1(p_{est} - p) + c_2 r_2(g_{est} - p) \]
The equation includes key variables such as velocity \( v(t) \), constants \( c \) relative to the particle swarm algorithm, and the current position \( (p_{\text{best}}, g_{\text{best}}) \). Although the general operations of such particle-based swarm dynamics exceeds the scope of the current study, the procedural analytics proposed by Pyke and Stark (2021) offer an identity-based fingerprinting solution that can be used in the current security problem to establish swarm-based flocking determination relative to the pathfinding expectation (e.g., point A-point B in relative telemetry to Drones 1-8). Where current positions \( (p_{\text{best}}, g_{\text{best}}) \) can be continuously evaluated to determine which drones have been established in which quadrants or long-lat positions, during the pathfinding exercise, Pyke and Stark (2021) determined that the quality of the positions decays, resulting in a precedence towards traversed paths. Within the flocking module, the scriptable object maintains the dataset for the target route including the associated obstacles, the target coordinates, and the navigational requirements. All drones simultaneously can access this centralized data, ascribing location data and absolute telemetry to each individual drone according to their flocking state (e.g., static or moving).

The resulting variables can be used to establish the fingerprinting domain according to key indicators such as signal strength, absolute location, and telemetry. In optimizing their drone flocking model, Jia et al. (2019) identified four primary constraint dimensions including flight characteristics (attitude angle, velocity, speed), inter-agent distance, forward motion, and adjustment time. Whilst the Reynolds
flocking theorem remains the guiding principle for flight path navigation and flock cohesion, to establish the parameters for in-flock security and anomaly detection, the degrees of freedom afforded to individual drones relative to this central murmuration must be considered. By establishing intra-swarm RF signal strength monitoring and time intervals, two interrelated models of drone fingerprints can be compared against packetized profiles that include expected identifiers including MAC address, transmission frequency, service-set identifier (SSID) patterns, and acknowledgement size (Li et al., 2017). This model, therefore, makes several underlying assumptions that predict the ability to model and interpret drone identity patterns and network relationships:

- Assumption 1: UAVs utilize a standardized hardware and software profile that will allow for similar, normative intra-network communication patterns.

- Assumption 2: Individual drones can be uniquely identified by their MAC address, establishing a verifiable, known fingerprint for starting operations.

- Assumption 3: Drone swarms are characterized by explicit rules and/or behaviors that predict flight patterns including altitude, direction, separation, cohesion, and alignment.

- Assumption 4: UAVs outside of flight tolerances default to recovery measures including landing and return to home.

Based upon the intrusion detection models presented in the preceding sections,
a security profile of each drone can be determined alongside clear, probabilistic indicators of network intrusion and/or flight disruption. The model extrapolated from this profiling relies upon two primary dimensions: the normative swarm center (e.g., the geolocated center of the flocking behavior) and the fingerprint criteria (proximity RF, MAC ID, operational tolerances). This distinction between expectation and real-time outcomes reinforces the previously developed machine learning solution by allowing system-based tolerances to be defined and instruments to be trained prior to launch. The expectation validated by two previous empirical models (Jia et al., 2019; Pyke and Stark, 2021) is that multi-dimensional drone fingerprinting will redefine the nature of security profiling, linking the archetypes for normative behavior to both individual and in-swarm flocking maneuvers.

Based upon the evidence presented in the preceding machine learning exercise, Figure 33 summarizes the design of a swarm-based drone signaling and fingerprinting security protocol. Cloud-based machine learning analysis is conducted separately from the swarm operations, thereby reducing the onboard demand for computing power and battery consumption. Both home and end waypoints are independent GPS coordinates that are transmitted from the control module through the swarm data exchange module and accepted on the basis of authorized communication. This swarm data exchange is an in-network, onboard software suite that is proposed to form the basic onboard Random Forest processing of several basic criteria including Motor Speed (within or outside tolerances), RF signal (in-swarm and control
module), GPS stability, and relative location (e.g., height, lat, long) to the swarm. As designed, the model presented in Figure 33 includes two interconnected machine learning modules including the higher-powered, higher computing cloud-based solution which will monitor swarm activity for security threats and deviations from the prescribed route. Additionally, the onboard criteria-based processing solution will only be responsible for comparative benchmarking of drone behavior in which state values include ‘normative,’ ‘deviant_within_tolerances,’ ‘deviant_outside_tolerances,’ and ‘aberrant.’ Based upon the Reynolds flocking theorem these specifications will be trained within the system according to their degrees of freedom from the collective mean, thereby imposing three conditions upon the optimal swarm state including separation, alignment, and cohesion.

Figure 33: Swarm Flocking Optimisation Model with Machine Learning Integration
4.7. Summary

This chapter has presented a multi-dimensional analysis of drone flight patterns, network security, and threat detection capabilities. Whereas the monitoring data for single drone and swarm flights varies, the same underlying predictors of signal anomalies and behavioral inconsistencies are monitorable and therefore, defensible. Field-based criteria integrated into the machine learning testing set can expand the detection algorithm to include swarm-based parameters (e.g., separation, cohesion, alignment) in the assessment of both individual and swarm-based normalization. Both autonomous and operator interventions can be initiated to maximize the likelihood of drone recovery when behavior variations are detected (e.g., route departure, motor speed, GPS signal strength, swarm fidelity). Such security monitoring and interventions are critical for modern flight environments where signal interruptions and malicious attacks continue to threaten the continuity of swarm operations. The following chapter will discuss these findings and propose a fingerprinting solution that incorporates the probabilistic monitoring of machine learning solutions into a risk-averse flight solution that can improve swarm continuity and recovery.
Chapter V.

Discussion and Analysis

5.1. Introduction

The experimental methods developed for this study combine an array of theoretical propositions including machine learning, swarm dynamics, and particle theory into a composite framework for mitigating diverse security threats to drone technology. Due to the overlap between known and expected dimensions, it is possible to train an AI system to monitor drone flight regularity and identify incidences of aberration that can be linked to serious security threats. For both commercial and military operators, therefore, networked solutions for both individual and swarm-based drone fingerprinting are essential antecedents to device continuity and recovery. The following sections discuss these findings, drawing upon the theoretical and conceptual underpinnings of core research in this field to outline a practical model for detecting security compromises in various drone operations scenarios.
5.2. Findings and Practical Implications

Research Objective 1 This study was undertaken to evaluate a significant problem for drone operations: the vulnerability of in-flight systems to hacking and signal disruption. Whilst these problems are widely acknowledged throughout literature and experimental research, the persistent evolution of malicious actor capabilities makes standardization of security protocols a challenging prospect. Accordingly, the first objective of this research was to critically evaluate the available methods and techniques for identifying compromised drone data from within a wider set of healthy data. The procedures for such data-driven experimentation were researched, with consideration given to a variety of techniques that ranged from onboard sensors to data mining and machine learning capabilities. Ultimately, this study develops a solution that combines the best-fit techniques of multiple researchers into a single, streamlined model capable of demonstrating the current and future proposition of data sensing and drone performance analysis via onboard, lightweight probabilistic solutions.

Specifically, the performance data modeling approach developed for this study expanded on preceding techniques employed by Li et al. (2017), Jia et al. (2019), Medaiyese et al. (2021), and Baig et al. (2022). The scope of research spans several critical challenges in drone operations including flight path detection, security monitoring, swarm particle theory, and drone fingerprinting. By extrapolating publicly accessible data from the VTO Labs database, the results of this study are both...
replicable and extendable, allowing future datasets to integrate into more complex or comparative studies. Given the range of data each drone captured (e.g., 288 features), the stages of this data analysis were designed to selectively process those indicators with the most direct linkage to the primary concern of this study: the threat to drone security by malicious attacks. Therefore, by targeting those performative behaviors, the evidence analyzed during this procedure was assessed according to its possible applications to real-world hacking and disruption events.

Figures 34 and 35 demonstrate two different, but interrelated threats to drone operational continuity. The DoS attack, a phenomenon thoroughly analyzed in prior research by Vasconcelos et al. (2016), Chibli et al. (2021), and Feng and Tornert (2021), utilizes force flows of data to overwhelm key onboard resources for drones including the GPS signal and/or the RF signal. If the operator cannot communicate effectively with the drone, then aberrant behaviors, including sudden decrease in motor speed, directional changes, landing, or fall, are likely. Whilst the hijack attack researched by Feng et al. (2020), Yaacoub et al. (2020), and Doyle et al. (2021) involves a direct takeover of drone control or drone operations by outside actors, the end result of this interference is similar to that of the DoS. This observed consistency in threat profiling is important when weighing the security risks and vulnerabilities to drones, particularly when analyzing this phenomenon from a probabilistic perspective, as was applied to the previous machine learning exercises.
Research Objective 2 The second research objective in this study was to develop and deploy a machine learning model to scan for and detect normative and aberrant drone operations and hijacking.
rational flight behavior across drone swarms on a large scale. This research objective was accomplished in the preceding chapter by applying visualization technologies to the clustering and interpretation of drone flight logs that were downloaded from VTO Labs. The analytical model involved a series of four machine learning exercises that targeted the relationships between normalized datasets and possible anomalies that were identified via the K-Means and GMM clustering analysis. The Naïve Bayes, Random Forest, Linear Regression, and SVM models were trained and tested according to a significant scale of data spanning 12 criteria in four performance-critical categories. The outputs of this model were then weighed against the practical applications for more complex, swarm-based systems to propose a model capable of fingerprinting individual drones, modeling drone flight behavior, and identifying possible risk factors and abnormalities.

Research Objective 3 Once the machine learning model had been developed, the third research objective was to evaluate the optimal size of the drone dataset required to ensure that most indicators of compromise can be robustly and consistently identified. The current dataset included a total of 20 instances that provided complete data relative to the same 12 criteria. Incomplete flights or flights with significant faults or failures were excluded so the training exercise could be completed consistently and reliably. The output of the multi-test Random Forest classifier included an optimized max depth of 6 trees and a mid-range level of 9 estimators to maximize data accuracy, precision, recall, and training time. These findings suggest that a large training
set of between 20 and 60 flights could be used to train on anomalies and establish the baseline dataset for normalized data comparisons. Supervised training sessions such as those Feng et al. (2020) and Baig et al. (2020) employed have shown the positive relationship between machine learning accuracy and data-based indicators of reliability and consistency in identifying abnormal behaviors. Thus, for initial training, supervised training can be employed in the future, whilst real-time operations can rely upon AI-supported expectancy-based model comparisons and probabilistic reasoning.

Research Objective 4 The final research objective for this study was to recommend the ideal form of machine learning to optimize the detection of compromised signatures, based upon both real time and post-flight data analysis. Given these findings, it was evident that the Random Forest solution provided the greatest degree of accuracy and consistency in predicting both normal and abnormal datasets. As this instrument used multiple testing sweeps to maximize the depth and probabilistic accuracy of the analysis, this algorithmic solution is the best-fit model for future machine learning training. These findings confirm the evidence presented by Aldaej et al. (2022) and Baig et al. (2022) regarding the efficacy and analytical value of the Random Forest classifier, particularly when benchmarked against other variations such as the Naïve Bayes and SVM. In framing the type of analytical protocol and the underlying criteria that are best represented by this machine learning approach, however, it is important to consider variations in the recorded datasets and these
machines’ ability to analyze the effects of flight path variations and changing signal status on drone performance and/or swarm consistency.

Researchers such as Guerber et al. (2021) have cautioned that although Random Forest classifiers offer precise interpretations of data-based anomalies, the binary nature of the classification scheme (e.g., anomalous or normal) can lead to artificial or inconsistent observations. Future applications of this machine learning solution will need to consider the multivariate combination of multiple modeling solutions, and potentially incorporate additional analytical layers using Linear Regression (LR) or SVM or another appropriate machine learning model to validate assumed or observed attack vectors. In fact, Aldaej et al. (2022) subdivide the machine learning classifiers into specific solutions according to the various attack indicators and security approaches as demonstrated in Figure36. Although these proposed solutions are based upon field-based comparisons using singular or specific attack vectors, this study selected the Random Forest solution because of its broad, multivariate application to an array of onboard signaling criteria. For example, if GPS signals are low and drone height levels are responding uncharacteristically (e.g., bobbing up and down, rising in height, landing immediately), then signal jamming and or spoofing can be modeled using the Random Forest solution.
5.3. Risk Assessment and Drone Security

One of the core challenges in identifying the nature of risks associated with UAV flights is that technological tactics are increasingly varied, ranging from direct (e.g., hacking) to indirect (e.g. signal jamming) attacks. Yaacoub et al. (2020) suggest that the reliability of drone-based communications is based upon three primary domains including authorization (who is controlling the UAV), authentication (how is such control awarded), and auditing (how are security threats being monitored and managed). In developing security countermeasures, Singh and Verma (2017) proposed threat-based models which weigh the relative likelihood of an attack against the possible consequences or impacts of such an attack to predict the overall severity of the event. Importantly, such modeling allows drone operators to weigh countermeasures according to their breach difficulty levels, whereby high difficulty/high impact attacks such as node compromises or communication interference require different countermeasures than low difficulty/low impact attacks such as insider or signal jamming.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Security Technique</th>
<th>Machine Learning Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamming</td>
<td>Secure Offloading</td>
<td>Q-Learning, DQN</td>
</tr>
<tr>
<td>DoS</td>
<td>Secure Offloading</td>
<td>Neural Network, Multivariate</td>
</tr>
<tr>
<td>Intrusion</td>
<td>Access Control</td>
<td>Correlation Analysis</td>
</tr>
<tr>
<td>Malware</td>
<td>Access Control</td>
<td>Naive Bayes</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
<td>Random Forest</td>
</tr>
<tr>
<td>Traffic Blockage</td>
<td>Authentication</td>
<td>SVM</td>
</tr>
</tbody>
</table>

Figure 36: Data Security for Intelligent Drones (Source: Aldaej et al., 2022, p.5)
threats (Singh and Verma, 2017).

The analysis of the datasets in the current study revealed that severe flight disruption was directly linked to one of two causes: the loss of a steady GPS signal which triggered a RTH event, and the loss of a control-based RC signal which triggered abnormal motor activities and ultimately, a forced landing protocol until communications were recovered. For operators engaging in in-flight behavior, these findings suggest that it is more likely they will be unable to defectively diagnose the cause of abnormal activities without some degree of deeper investigation and data analysis. Whilst the current study and prior research by Baig et al. (2022) have demonstrated the viability of real-time signal monitoring, the onboard technologies to achieve such outcomes are likely to exist outside of the software structure and file system installed on these drones by the manufacturer. Although the question remains unanswered as to why companies like DJI are not more security-oriented, the practical challenges associated with upscaling and improving onboard data monitoring may ultimately explain the tradeoff costs that have often been made. For example, the negative impact of onboard signal monitoring on flight time and battery life could be so significant that both operators and manufacturers may be averse to including such rigorous security protocols and software suites for drone operations.

Beyond this burden of data management and resource optimization, how and why data from drone activities is being recorded and analyzed must also be considered. Due to the operational risks associated with drone control, Vacca et al. (2017) argue
that emergent data protection and privacy rights guidelines are redefining the scope of security administration and responsibility for drone operators across the public sector. However, as reported by Kumar and Agrawal (2021), drones are also being used for criminal activities as individuals exploit the remote and relatively cost-effective functionality of these technological innovations as drone visualization and sensing capabilities continue to improve. Therefore, digital forensics is an important discipline for both the drone operators (e.g., recognizing security risks) and for law enforcement agencies or invested parties who require forensic capabilities to diagnose and analyze drone behavior and datasets. The value of the VTO Labs (2022) solution for the current study was reflected by the accessibility of data and the download and capture capabilities by such a useful tool as DatCon. As these files are simply bytes of data stored in various, accessible file trees, it becomes possible to convert behavioral evidence (both positive and negative) into mappable and charitable outputs through CSVViewer or other software suites. Essentially, this means that both criminals and legitimate operators now possess the resources to diagnose and interpret flight data abnormalities via public, open-source software solutions.

Recognizing data mining and intervention opportunities for malicious actors, hardening and securing existing UAVs becomes an imperative for at-risk and stability-critical facilities. For government agencies or military organizations, the need to protect critical facilities against unauthorized observation or surveillance has resulted in an emergent study of signal monitoring and probabilistic decomposition.
For example, Medaiyese et al. (2021) provided a drone detection model based upon the reductive machine learning analysis of RF signals within a dedicated zone. Even without specific UAV control signals provided, the model successfully parsed through the RF noise to identify signal patterns that fell along varying frequencies (e.g., Bluetooth, WiFi, RF). The subdivision of these various signals into their signal strength and range enabled analysts to determine and fingerprint the specific drone signal identifiers without access to onboard datasets (Medaiyese et al., 2021). This observation is critical because it demonstrates the possibility for outside agents to reverse engineer signal data to not only hijack drone RF signals, but to strategically interfere with other on-channel broadcast data such as GPS coordinates and operational specifications (e.g., motor speed, telemetry).

The paper has demonstrated that the likelihood of malicious or exploitative attacks can be predicted and monitored by identifying variations in drone data patterns, specifically those that lie outside of the operational norm. Whereas prior research by Baig et al. (2022) and Syed et al. (2022) has demonstrated the value and practical viability of drone data analysis for security threat identification in post hoc cases, there is an immediate need for real-time data management and risk analysis during drone flights to prevent loss, crash, or civilian impact. The model proposed in this study draws upon novel fingerprinting techniques by Clark et al. (2017) and Li et al. (2017) to not only selectively classify drone data according to flight normalization, but to fingerprint and classify in-flight
behavior according to swarm-based traits and cluster tolerances such as in-network signal strength, RF stability, and UAV identifiers. From this perspective of selective UAV identification, multiple criteria can be adopted for modeling the unique signatures of individual drones or the collective signatures of drone swarms. In the future, operators will need to select which variables are most reliable (e.g. MAC id) and which performance factors (e.g. GPS signal strength) are most directly linked to flight path anomalies. Despite the operational advantages of drones in military theater, the relative threat to civilian life and property is significant, particularly with risks of hijacking or signal interference. Johnson (2020) describes the role of suicide drones in targeting enemy strongholds and sensor arrays as military systems deploy AI-supported decision-making to reduce the fallibility of human interference. The problem with this approach is that it shifts awareness protocols into machine learning specifications, requiring systems to make life/death decisions on the basis of rules that may or may not conform to the evolving standard of engagement (Johnson, 2020). Drone swarm operational efficiency, for example, can be threatened by interference from malicious actors with behavioral disruption (e.g., GPS spoofing) used to redirect targets and GPS navigation towards undesirable locations. Where such tactical threats were once considered science fiction, AI – with machine learning and onboard drone decision-making – is redefining the nature of warfare according to sensors and systems tolerances.
5.4. DoS and UAV Hijacking

Given the abnormalities observed in the CSViewer datasets and the outlying indicators recorded in both the K-Means and GMM clustering exercises, DoS activities are likely the most common drone hacking and disruption initiatives. Specifically, the DoS threat is one of secondary consideration, whereby normative operational specifications that are based upon dedicated communications between controller and UAV must constantly compensate for signal interference and various dilutive forces such as environmental or structural influences (Feng and Tornert, 2021). In a recent study, Chibi et al. (2021), determined that by leveraging drone swarm communications, the RSSI data and in-air triangulation of swarm communications could be used to mitigate such flood-based interruptions. Given the evidence observed in these current datasets, it is likely that DoS attacks will target specific RF channels, overwhelming system tolerances with false signals and network demands. Active signal switching capabilities, variations between 2.4 GhZ and 5 GhZ, and various sending channels can be used to randomize the communications channels utilized by the drone swarm. Coordination between onboard triggering mechanisms and control modules or intra-swarm randomization would provide the necessary switching standard to effectively dispel the most targeted DoS attacks.

Early exploitation research conducted by Vasconcelos et al. (2016) revealed that due to the lack of network security and the relatively simplistic procedure for information access and interception using standard network management resources
such as Hping3 and a LOIC attack, drones could not only be manipulated, but could be completely shut down and crashed via remote connections. Researchers like Feng et al. (2020) have adopted machine learning models, such as SVM, to demonstrate how model training can be used to identify hijack efforts and model the effects of the hijacking attempt on drone flight path performance during maneuvers. However, with more than 18.8 seconds of delay, such approaches were vulnerable to overfitting and inconsistent detection effects, requiring an algorithmic solution that could be lightweight, precise, but time sensitive. For the current study, the Random Forest model offered a training time of just 1/3rd of a second, with potential real-time processing parameters contingent upon the scale and complexity of the dataset. In fact, these findings suggest that similar to the reduced criteria developed by Feng et al. (2020), the most effective threat detection solutions are those that utilize limited criteria to model specific attack vectors (e.g., DoS, Hijack, interference).

As the range of drone operations continues to adapt to a growing number of interference forces, environmental disruptions, and anomalous events, the need for high probability, high accuracy models to analyze potentially severe threats such as signal jamming or DoS is becoming a central priority in both academic research and fieldwork (Pardhassaradhi and Cenkeramaddi, 2022). For example, the RSSI-based algorithm proposed by Chibi et al. (2021) represents a sensor-based, practical solution for DoS attack sensing and threat mitigation through ground station-based interference monitoring when operating drones in the field. Although dependent
upon the accuracy of the signal tracking and locational measurements, the triangulation of data points through swarm-based coordination is capable of increasing the system fidelity and improving measurement reliability. Similarly, the ground-based radar support solution proposed by Pardhasaradhi and Cenkermaddi (2022) provides a centralized, control support solution for monitoring variations in atmospheric and signal events near drone swarms, allowing for detection of spoofing attacks or signal interference. Such technologies leverage onboard data tracking via the IMU modules on the swarm drones to capture real time datasets, whilst providing ground support through high-power, advanced radar analytics that can determine whether a threat is real or fabricated (Pardhasaradhi and Cenkermaddi, 2022). Combined attacks on drone operators have the potential to severely disrupt or redirect drone flight paths, thereby resulting in unauthorized or inconsistent maneuvers. Evidence presented by Zheng and Sun (2020) regarding GPS spoofing offers a compelling representation of the technologically uncomplicated resources needed to misdirect drone location data or manipulate onboard location sensors towards an alternative pathway. In considering these three attacks, it is possible to diagnose data from within the proposed data analysis procedure introduced in the current study:

- Forced Landing: GPS spoofer will signal that drone is in a restricted airspace and forcibly trigger landing protocol.

  Observation: Data highlighted several abnormal drone flight paths during which immediate declines in height were reported alongside changes in drone
motor speed across all four rotors.

- Criteria: Drone Motor Speed, Relative Height, GPS Signal Strength

- False Direction Guiding: GPS spoofer will target drone during hover activities, reporting false coordinates and then guiding drone recovery activities towards alternative location.

  Observation: Data demonstrated unplanned variations in Long Lat data that would result in drone location shifting (even if minimal) beyond the normative bounds of the flightpath.

- Criteria: Long, Lat, GPS Signal Strength, RC Signal Strength.

- Landing in False Area: GPS spoofer will perform DoS or signal jamming attack to trigger drone Return to Home function. Drone will be redirected to hacker-defined GPS coordinates for landing.

  Observation: Data indicated sudden R2H function followed by flight recovery, potentially signaling path departure. No false landings reported, but long-term signal interference could lead to change in location.

- Criteria: GPS Signal Strength, RC Signal Strength, Long Lat, Height.

5.5. Swarm and Flocking Flight Fingerprinting

The Reynolds flocking theorem proposes that flight inter-dynamics amongst bodies in flight are based upon three primary variables: separation, alignment, and
cohesion (Pyke and Stark, 2021). Extended into the context of autonomous UAV flight operations, Jia et al. (2019) formally defined separation as a representation of the minimum interagent distance required for both normative (path-dependent) and compensatory (interference or object-influenced) flight operations. For in-air operations to succeed, this core concept of separation is translated into a 3-dimensional vector and includes multiple agent indicators such as altitude, attitude, longitude, and latitude in a model that is dependent upon the scale of the UAV swarm. Therefore, as predicted by Jia et al. (2019), it is possible to establish predefined system tolerances to preserve swarm continuity even if flight is affected by unforeseen variables or interference as long as such tolerances are maintained (e.g., minimum distance between drones). Although similar to separation, alignment in the Reynolds flocking theorem is also a 3-dimensional vector that predicts the relationship between drones relative to the center of the in-flight path. In this way, the point of rotation for all drones outside of the central drone becomes relative to this center, reducing the number of GPS calculations and sensing vectors needed to maintain continuous flight operations (Pyke and Stark, 2021). When integrated with AI-based capabilities, the flocking behavior of drones can be optimized in microsecond decision-making, thereby eliminating the need for external operators, and centralizing the flight path and obstacle avoidance capabilities according to the intrinsic structure of the swarm itself (Johnson, 2020).

Finally, there is a concept of swarm cohesion that has both spatial (e.g., distance between drone bodies) and technological conditions (e.g., signal strength). Ra-
dio wave coupling in the model proposed by Jia et al. (2019) involves establishing time parameters for signal exchange, whereby variations in distance either increases or decreases flight path cohesion. Although spatial coupling is based upon the physical relationship between drones, technological coupling can be monitored in accordance with radio wave frequency strength and the change in both intra-drone (e.g., between 2 or more drones) and intra-swarm (e.g., the link between central drone and each outlying drone). The current study focused on a single drone with a single channel radio communication to a central controller. However, by normalizing channel switching behavior according to some form of encrypted or predefined pattern (e.g., Morse code) it is possible to validate network connections under similar principles to high security technologies such as RFID chips and IoT devices (Karimibuki et al., 2019).

Although commercial applications of drone swarms in light shows or property mapping have demonstrated small-scale operations of large drone masses, the mobilization of such swarms in more complex environments requires a more dynamic approach that is based upon the critical condition of network cohesion. In military applications, Hambling (2021) reports that governments are aggressively pursuing drone swarm technology for both passive (e.g., reconnaissance, search, terrain analysis) and active (e.g., missile defense, attacking, signal jamming) field interventions. Whereas commercial drone swarms maintain a relatively small degrees of freedom standard for intra-drone signal connections, in military applications, the scope of these drone flocks can be extended significantly, allowing greater distances at greater speeds to
be covered by smaller flocks with higher degrees of collective coordination (Hambling, 2021). Whereas coordinate-based drone operations require explicit coordinates and GPS monitoring relative to a specific target, more complex swarm-based operations consider the dynamic relationship between the flight environment (e.g., buildings, terrain, threats) and the murmuration of the swarm.

The complexity of signal and telemetry fingerprinting within the swarm increases by acknowledging drone swarms’ autonomous flight navigation capabilities. Based upon the quantitative techniques and algorithmic solutions presented in the preceding chapter, there are several governing relationships that can be used to model the probability of normative or aberrational behaviors in swarm activities.

- Separation: The relationship between drones relative to the swarm center can be modeled in relation to environmental influencers (e.g. buildings, trees, wires, other drones) to determine an optimal state that is measured over flight time.
  
  Indicators: Difference of Lat/Long, Alt/Att

- Alignment: The coordinated structure of the flight path relative to predefined 3-dimensional guidelines (e.g. line, square, ball, helix).
  
  Indicators: RF Signal Strength (between drones)

- Cohesion: The nature of intra-swarm cohesion relative to all outlying points and the center of the swarm.
  
  Indicators: Difference of expected vs realized swarm footprint, difference
The complexity of machine learning and analysis in drone swarms is recognized in this field of research as a challenge that must be overcome through model optimization and best-fit solutions. The current study has demonstrated the practical applications of high reliability and accuracy models like Random Forest to individual drone data analysis; however, within broader swarm networks, other variables such as drone swarm flight trajectory, drone cluster algorithm, drone swarm error correction methodologies must be considered. Ahn et al. (2019) revealed that swarm noise relative to a variety of overlapping signals and flight indicators need to be eliminated through data processing procedures that require more complex solutions such as deep neural networks. By weighting behavioral normality according to probabilistic indicators as presented in Appendix B, such modeling draws distinctions between drone performance factors, demonstrating clearly identifiable normal and abnormal behavior. In this way, through a general fingerprinting of all drone signatures within a given swarm and continuous tracking of explicit abnormalities and variations over time, anomalous behavior can be linked back to various security threats or disruptive signaling influences, thereby allowing operators to respond more effectively.

5.6. Security Protocol, Monitoring, and Drone Fingerprinting

The flight spoofing approach demonstrated by Zheng and Sun (2020) utilized the control message spectrum to analyze the transmission standard to the drone in
flight. The evidence revealed that by relying upon a spectrum banded communication protocol, the drone was naturally resistant to interference, noise, and jamming without some form of high bandwidth, highly invasive tool that might overwhelm this communication (Zheng and Sun, 2020). However, as evidenced in this study’s dataset, when criteria such as RF Signal Strength decline, drone flight performance also declines, leading to at-risk vulnerabilities. In swarm protocol, however, signal variations can be mitigated by extending the relationship between the control signal and the drone flight path to include proximity signals from other drones in formation. Intra-swarm fingerprinting authenticates the drone’s identity, and coordinated, cross-swarm transmission signals can be used to reduce the likelihood that signal DoS or interference will affect in-flight behavior of the swarm.

Regardless of attack vectors or post hoc digital forensics, what drone operators require in today’s advanced technological market is real-time data collection and AI-supported analytics. Lu et al.’s (2017) research was close to proposing a real-time solution that involved designing and installing an onboard sensor to the bottom of a DJI drone. The problem with this approach was that it was hardware- and software-specific and, therefore, could not be used naturally to capture and diagnose evidence that was interwoven into other drone operations systems and data files. The current study has proposed a lightweight solution that could be installed within the root code of the drone software, thereby allowing a cloud-based remote connection to process the larger datasets, whilst onboard sensors could monitor performance according to
explicit specifications and performance requirements. Abnormal operations, however, is a variable, a condition that is not defined consistently across operational specifications. For example, Lu et al. (2017) demonstrated how drone motor temperature increased according to the types of flying maneuvers that were being conducted, suggesting that optimality and normality are conditional to the drone type and the operator input.

Although the data collected for this study confirms that the Random Forest machine learning algorithm is the most precise and accurate representation of normal and anomalous data from drone flight records, these findings do suggest that other, isolative approaches such as SVM or KNN might offer an improved fingerprinting solution in future data analysis. Karimibiuki et al. (2019) recognized that in autonomous drone swarms independently controlled by autonomous IoT modules, both SVM and KNN algorithms are effective at isolating identifying datasets and highlighting specific indicators that represent the underlying drone fingerprint. Such findings could offer a very simple binary solution to autonomous drone networks where fingerprinting based on factor-defined authentication could be used to apply a pass-fail standard to drone integration in mobile swarms. When a drone is hijacked, Karimibiuki et al. (2019) report that variations in flight paths or flight behavior can be quickly detected within the system and an autonomous device like an IoT sensor module could quickly take the affected drone offline. These applications are valuable to the commercial sector as they would authenticate, fingerprint, and allow into service drones that are in
factory settings or warehouses (Tubis et al., 2021). Similarly, in military swarm activities, when drone spoofing is used to create artificial drone signatures, automated AI decision-making systems can utilize single-stream data points (e.g. telemetry, GPS, RF) to quickly and efficiently eliminate those agents from the operational network (Hambling, 2021). Additional testing will be needed to determine whether particular algorithms like Random Forest or SVM are more effective for specific risk profiles and threat vectors, providing a more comprehensive representation of threat mitigation based upon changing situational conditions.

5.7. Scenario Modeling and Security Management

The practical use case for drone risk analysis is broad and encompasses the range of usage conditions and real-world applications that might threaten the continuity and reliability of drone function and operational achievements. By constructing a scenario to model the potential applications of the proposed machine learning solution based upon the insights and focus of prior researchers, the value of this novel procedure for future applications can be demonstrated:

Exterior Flight, Swarm Activity, Hard Target (Surveillance and Defense Hardened), Military Scenario: Military operators have reliable intelligence that a known terrorist is locked inside a four-walled compound in a remote city. They plan to breach the walls using direct, physical force but must use surveillance to attain some degree of certainty before entry. A three-drone swarm is deployed from more than 15km
away and flown at high altitude until they reach the compound’s coordinates. The swarm descends and captures live video and still images of the compound defenses and weaponry.

Risk Profile: Due to the target’s reputation, the compound surveillance is likely to include active video feeds and some degree of radar or proximity-based analysis. The drone swarm will likely be able to reach the compound coordinates undetected at sufficient altitude but will be at risk upon descending to lower levels. The signal jamming and hijacking risks are significant due to local radio broadcasting capabilities. A DoS attack could cause drones to fail and fall from the sky or initiate RTH functions without capturing needed intelligence.

Mitigation Strategy: Real-time monitoring of signal threats, application of Random Forest machine learning classifier to analyze expected versus realized drone behavior both within and outside of swarm. Active visual monitoring of video feed for actor threats with live weaponry. Central control-based recovery protocol initiated in the event of a threat.

Key Indicators: GPS signal strength, RC signal strength (control), RC signal strength (proximal), motor speed, Lat, Long, video stream stability.

Intervention and Response: Detection may be inevitable; therefore, data monitoring and reporting is the priority. Visual intelligence takes precedence over drone survival; and therefore, active signal switching and channel adjustments are needed to ensure that operators retain control over the swarm as long as possible.
Interior Flight, Swarm Activity, Soft Target, Commercial Scenario: Company A has hired an outside drone operator to perform overnight logistics monitoring in a large-scale warehouse. Swarm operations are expected to cover the full scope of warehouse operations in a continuous circular rotation pattern to identify the flow and continuity of the floor-based team operations.

Risk Profile: On-site access will be restricted to authenticated operational personnel and staff members with proper identification. Exterior access to parking lot and warehouse grounds is restricted by privacy fences and guardhouses. Internal threats from employees or authorized visitors could lead to signal disruption or micro-scale GPS spoofing. External threats would require some degree of line of sight or insider awareness to directly affect drone movement through hijacking and DoS. Environmental interference and/or frequency jamming could lead to system collapse and drone failure.

Mitigation Strategy: Onboard Random Forest machine learning capabilities provide real time flight path analysis and swarm flocking comparisons to identify aberrations and inconsistencies. Operator alerts are automated and based upon micro-specifications associated with very low flight behavior tolerances (within 80

Indicators: RC proximity strength (to swarm), RC strength (to controller), motor speed, relative height, GPS signal strength, pitch, roll Intervention and Response: Aberrations in single drone behavior require RTH or immediate landing to prevent crash. Aberrations in swarm behavior require immediate land or return to
Exterior Flight, Single Drone, Random Flight Path, Civilian Scenario: Real estate developer utilizes single quadcopter drone to survey and visually map all four property corners of 1.8 acre rural land. Operator is located at the entry to the property and operates a handheld RC controller with video feed. Flight path is semi-automated with directional controls pre-defined, but video surveying is operator controlled.

Risk Profile: Due to the remote profile of the surveillance site, the overall risk profile of the flight is minimal. The likelihood of a localized actor interfering with drone operations is very low as detection risks would be high. Long-range signal jamming and/or DoS or hijacking attacks could be possible but would require strong signal and equipment. Direct threats to property or human casualties are negligible due to undeveloped status of land.

Mitigation Strategy: Operator monitored flight path using key indicators to ensure consistency and operational stability. Post-flight data analysis to be conducted to identify any possible threats and any variations in flight stability. GPS route consistency threshold established at 80Key Indicators: GPS signal, RC signal, Motor Speed, Relative Height Intervention and Response: In the event of aberrational drone behavior, user intervention performed to trigger return to home response. If drone movement continues, then land on demand response is triggered. Any incongruous behavior or out-of-range activities should be evaluated for associated threats to inform future vigilance.
Although these scenarios are hypothetical, they demonstrate the cross-event applicability of the proposed machine learning model. Drone sensor data remains constant across flight paths regardless of mission-specific objectives. There is an expectation that motor speeds, altitude, and signal strength will remain constant along a normative arc that can be recovered in the event of an anomaly. Evidence presented by Sindhwani et al. (2021), who purposefully disabled critical components on a self-flying delivery drone, revealed that state recovery was a function of recognition, compensation, and route amendments. In this way, researchers who are able to trigger anomalous events and utilize machine learning responses can test the resiliency and continuity of drone flight capabilities and improve flight recovery outcomes. Such approaches are similar to modern avionics and AI-supported aircraft flight systems which are capable of countering interference or human error by revising tolerances and adapting aircraft performance to protect against catastrophe or failure. The evidence collected for this study confirms that insights and analytics are valuable representations of anomalous events, but to realize specific, in-scenario responses, future research will need to test against the resiliency of the flight system as a whole.

5.8. Summary

This chapter discussed the findings from the data analysis and machine learning procedures tested during this exploratory study. By drawing upon the insights and evidence from prior researchers and combining these findings with the broader
compendium of knowledge, theories, and empirical findings, the results of this study were extended to several practical applications. Firstly, this chapter has demonstrated a strong, productive relationship between data analysis techniques and drone threat detection capabilities, both in post hoc and real-time cases. Secondly, the multi-dimensional insights captured in relation to drone security vulnerabilities have highlighted several severe limitations in relation to hijacking, GPS spoofing, and signal interference. Finally, this chapter has presented a model of data-oriented analytics that can be applied to future drone monitoring exercises to assess the at-risk vulnerability of individual and swarm drones during operation. The following chapter will conclude these findings, focusing on the primary contribution of this research to this field, and recommend additional tests and analyses that could be used in the future to assess the evolution of drone security measures.
Chapter VI.

Conclusions

6.1. Conclusions

The ubiquity of drones in both civil and military aviation is reshaping the risks associated with flight operations and reliability. As malicious actors target drones using innovative and advanced radio frequency technologies, the need for operators to recognize drone compromise and implement recovery initiatives is imperative. Accordingly, the primary aim of this investigation was to determine an efficient machine learning algorithm to quickly, autonomously, and consistently identify drones within a swarm that have been compromised and help operators implement immediate recovery steps to maintain operational continuity. Through a comprehensive review of the core theories and concepts related to drone security and data analysis, this paper developed a structural solution for capturing and analyzing onboard data reports. Subsequent experimentation with this dataset involved a multi-solution machine learning experiment that ultimately revealed a highly productive solution for future security threat monitoring and analysis. The end result of this study proposes a security management model that can be deployed across both individual and swarm
drone operations to realize a more productive, real-time solution to drone security management.

Central to the navigation of UAVs is an expectation that radio frequency signals will remain consistent throughout the flight plan, directing the drone through a central control module to perform tasks according to locational, telemetry, and inertial variations. However, prior evidence in this field has confirmed that such signals are not only exploitable, but can be hijacked and translated into redirection effects that decrease the reliability of a drone during flight and may lead to severe or catastrophic failure. From spoofing to DoS attacks to drone hijacking, the opportunity to target, exploit, and append drone operations remains a significant threat to a variety of civil and military operations. Moreover, as hackers recognize the exploitability of these UAVs, they are developing subversive tactics to force behaviors that could potentially lead to property or individual damages if operators are not immediately and consistently aware of the attack. Therefore, preliminary analysis of the literature in this field confirmed that drones are exploitable, vulnerable, and often unreliable resources that require a more productive and dynamic security protocol to achieve heightened reliability and operational continuity.

The data being recorded during drone flights is significant as it provides operators and digital forensic investigators with resources that can be used to diagnose events leading to a fall or misdirection. From motor speed to RC signal strength to GPS guidance, several studies have demonstrated that the key to diagnosing drone
attacks is linked to real-time, in-flight data collection. One of the problems with drone data monitoring, however, is that due to battery and computing constraints, these aircrafts are restricted in their ability to record, analyze, and report variations in behavior. Instead, operators are tasked with observing such misdirection or changes during flight (which is difficult at long distances) or must accept post hoc data analysis via more comprehensive computing systems. This study recognized this challenge, and therefore, targeted the best fit solution for achieving drone performance analysis during real time conditions, analyzing evidence and data specifically related to such models to determine the best fit techniques for reliable analytical solutions.

By systematically analyzing VTO Labs’ data from a post hoc drone report model, it was possible to design and implement a structured, semi-supervised machine learning solution to increase the predictability and reliability of security monitoring standards. This study utilized a pre-processing cluster model and K-Means and GMM to identify outlying drone patterns that were representative of possible interference or malicious attacks. It then identified key criteria related to drone flight performance (e.g., motor speed, GPS signal strength) to model variations in drone behavior across repeatable tests. Using Python and the Scikit library, four machine learning models were trained and tested for accuracy, precision, recall, and training time. The results could then be compared as a best-fit model of machine learning behavioral analysis.

Although several studies have applied similar techniques in research, they have only considered post hoc analysis of such data indicators. However, for drones in a
swarm, Reynolds flocking theorem proposes that there is an expectation of separation, alignment, and cohesion that can trace consistent or aberrant drone behavior throughout the flight path. By establishing drone fingerprinting signals that are based upon quantitative indicators such as MAC data or signal strength (relative to the center of the swarm), it becomes possible to apply an on-board, in-network, lightweight solution to drone security and reliability analysis.

The contribution of this study to the broader field of research includes a practical representation of this model and its underlying criteria, a recommendation of a best fit machine learning solution (RF), and a designed model that can be used to integrate this approach into real time security monitoring. Whereas the ability of machine learning algorithms to identify security threats in highly complex systems was not in question, the accuracy and consistency of such systems was of critical concern during the course of this study. The findings revealed that there are trade-off when selecting particular machine learning solutions, particularly when real-time monitoring and data analysis needs to be sufficiently reliable to direct activities towards more productive interventions. Ultimately, the variables collected for this study represented core criteria that could be linked to variations in flight operations. By modeling security threats, weighing the type of risks posed to drone flight activities, and then identifying criteria for classifying and identifying such threats, a rolling or adapting risk register can be applied to future system optimization and drone data analysis. These findings offer further confirmation of the clear value of an adaptive
system, particularly one with the computing power of algorithmic models to weigh disruptive events against normative, optimized flight behavior.

This study answered four primary research questions through layers of research and analysis. The summary of these findings outline the importance of this research to drone security management innovation and development. The first question asked how a researcher could best analyze compromised drones and uninfected drone datasets to develop a collection of indicators of compromise (IOCs) so as to create robust signatures of infection. The approach adopted for this study of DAT-CVS-ML Analysis is currently accepted as the best-fit solution, affording in-depth, multivariate analysis of drone flight logs via a variety of charting, statistical, and interpretive techniques. Importantly, the procedure for this study was extended to include the relationship between swarm technologies and drone proximity data, highlighting a model that can be developed into a deeper, real-time approach to data analysis in the future.

The second core research question asked how a machine learning model could be deployed in a real-life environment to scan for and detect drones that are compromised on a large scale. This study has proven that data-based pre-processing and model analysis can be used to systematically compare flight-based variables related to various security threats and onboard drone vulnerabilities. From fingerprinting through specific proximity signals to GPS strength monitoring to motor speed analysis, the opportunity to scan across multiple drones in real-time is emerging as a
resultof an AI-supported, machine learning discipline that can apply Random Forest techniques to the detection of abnormal behavioral patterns. Ultimately, the evidence collected and tested revealed that drone signature data can be used to establish a networked identity that extends throughout an operating swarm or series of interconnected UAVs. Similar to signal spoofing and interference, such digital fingerprints or signatures must be monitored during the flight lifecycle to ensure that drones are not being replaced or spoofed within a given swarm.

The third question was more difficult to answer as this research explored the optimal size of the drone dataset needed to be sure that most indicators of compromise (IOCs) will be covered. The challenge with this question is that it presupposes that IOCs will be normalized or predictable. As evidenced from the datasets analyzed, drone records are often varied and in many cases, reflect the continuity of the onboard recording modules and packetization. This also means that determining threats or drone compromise in relation to external attacks requires the ability to distinguish between aberrational flight patterns due to control or drone causes and aberrational flight patterns due to malicious attacks. Continuity modeling and multiple supervised training sessions with a high-powered machine learning solution like Random Forest was found to be extremely accurate with a max depth of 6 and 9 estimators when applied to a sample set of 20 drone data records. This guideline can be applied to future testing, but researchers should remain cautious when estimating causal or interference effects without sufficient supporting data.
The final research question asked what the most unobtrusive way would be to deploy infected drone detection algorithms, and which form of machine learning will support the optimal detection of signatures in the fastest most efficient manner. The findings confirm that the Random Forest approach was the most effective, yielding the highest performing, highest reliability results. Despite the lower performance in recall time, it is hypothesized that due to the number of branches and complexity of the forest tree structure, recall became diluted with greater accuracy and reliability. Whereas other approaches such as Naïve Bayes may offer a faster solution, the relative accuracy of the Random Forest solution is superior and should be considered the default standard for future testing. Regarding any possible intrusion effects on such detection algorithms, these techniques could be allied via real time, low-energy modeling systems where pre-trained solutions are embedded in onboard drone programming, whilst full-spectrum, higher computing capabilities remain linked to the central control module. This approach would also work for drone swarm applications, as various computational responsibilities could be adopted by individual drones, with monitoring specifications calibrated according to their position in the underlying cluster.

Based upon these findings, this paper concludes that machine learning data analysis provides a viable, lightweight, real-time option for increasing UAV security resiliency. From drone identification and signal fingerprinting to operational monitoring and continuity interventions, the advantages of this probabilistic analytical
approach are significant and compelling. The methods described in this study confirm earlier research in this field and validate the procedural advantages of Random Forest classification and data analysis in identifying aberrations with consistency. Ultimately, the model developed for this study can be used to test other UAV datasets to confirm the validity of the proposed model and to develop low-power, lightweight real-time data analysis capabilities for in-flight security monitoring and management. Through advanced signal analysis, a swarm-based proposal is also introduced that can be applied to upscaled drone configurations, thereby extending the applications of this research beyond the scope of single drone management. This research therefore concludes that to improve the reliability and continuity of future drone operations, a machine learning solution that can provide operator information related to key criteria integrated into a standardized training set and algorithm supported analytical model is needed.

6.2. Limitations

Priori research in this field emphasizes that security threats are abnormal, and therefore, are viewed as an unlikely, but potentially severe phenomenon that must be avoided wherever possible. For critical sectors such as military applications, security threats become more likely, magnifying the consequences of exploitation and hijacking, and threatening the broader welfare of individuals or property if such threats are not addressed. The techniques developed for this study drew upon data from a
single, commercial grade drone that was published by VTO Labs in 2018. Although valuable from a comparative perspective, the forensic analysis of this drone data did not reveal or highlight any specific security threat that occurred during the various flights. Further, the observed nature of the variations in the dataset were based upon assumed interruptions despite the possibility that other factors (e.g., environmental, user error) resulted in a loss of signal between the control unit and the UAV. Therefore, this study confronts a critical limitation in terms of the overall reliability of the interpretations made regarding this specific drone data and the possibility of malicious actions against the device or operator. Despite this limitation, the machine learning training that was conducted and the specific criteria identified for modeling variations in drone flight performance were representative of the same types of behavior that would likely occur during a security incident. Therefore, whilst future research should consider capturing real-time data from monitored hijacking attempts, DoS attacks, and signal interference tactics, the representative value of the findings in this study are based upon their practical applications to the design and implementation of machine learning solutions in the future. The following section offers several recommendations for additional studies that could reduce these limitations and their potential impact on the reliability of these findings and the proposed security threat monitoring model.
6.3. Research Contribution

The precedent established by prior research on drone security risks has increased the industry’s overt willingness to recognize that existing security standards are simply inadequate. For drones equipped with encryption technologies, onboard data remains protected; however, operational threats are manifest as malicious actors exploit the remote nature of these UAVs to their advantage. The range of available hijacking, DoS, spoofing, and signal interference tactics is broadening, and for motivated individuals or groups, the ubiquity of drones in both civil and military applications presents many opportunities for exploitation. On the research and operational side of the drone equation, this study has confirmed that there is a need for security protocol and software support that will not only identify possible risks, but will utilize real-time data tracking to identify when such risks are affecting drone performance. Whereas drones are vulnerable to technological exploits, the synthesis of prior research captured during this study confirms that operators and control systems are equally as vulnerable. Therefore, by developing a machine learning solution able to monitor network security and drone performance and identify in real-time the moment when a malicious actor attempts to gain control over the flight profile, the evidence presented herein suggests that risk mitigation and avoidance becomes possible. In addition to this observation, the techniques employed have confirmed several prior studies and the approaches adopted for structuring data pre-processing, machine training, dataset analysis, and output presentation. Further, an extension of
swarm concepts and flocking theory has been presented to demonstrate the potential viability of a cohesive and centralized means by which dedicated swarm communications can be used to prevent outside attacks or interference. Ultimately, this study contributes several new models for evaluating existing onboard security standards and software capabilities and proposes a multistage training system that can utilize a highly effective machine learning algorithm like Random Forest to increase the security of UAV flight operations.

6.4. Recommendations

The scope of research in this field has expanded, particularly in the past three years with visionary researchers like Zheng and Sun (2020), Baig et al. (2022) and Syed et al. (2022) recognizing the need for deeper, AI-supported solutions for drone security. Onboard, lightweight security systems may have been introduced to some models in the form of data encryption; however, the vulnerability of these RF systems to hijacking, DoS, and interference is persistent. Whilst the current study has focused on intrusion detection from a post hoc perspective, the transparency of this evidence confirms that real-time applications are needed to address future vulnerabilities. Therefore, by drawing upon the proposed novel model outlined in this research and applying the Random Forest, pre-trained classifier to an unsupervised monitoring solution, there are a variety of additional studies that will need to be conducted to test such onboard functionality. We have the following recommendations inline with
our original research objectives:

Recommendation (i). Real-time data analysis should be integrated into the flight monitoring profile, and several data processing stages should be tested, including data conversion (DAT to CSV), Python analysis, and transmission/reporting. One of the untested conditions that is discussed throughout this study but has yet to be viably implemented in practice is real time security monitoring. By establishing a normalized threat profile for both individual and swarm UAVs, it is possible to pre-classify security threats according to their deviation from this baseline standard. By starting with automated drone flight pathways, operators can transfer flight control responsibilities to software systems and instead focus on monitoring systems for various security threats. This means that two primary displays are needed including flight tracking (normal, deviant, aberrant) and risk profile (low, medium, high).

Recommendation (ii). An alternative study should be developed to focus on drone hardening, drawing upon the current findings to inject fingerprinting data into the control system responsible for flight management and route wayfinding. Based upon the Reynolds flocking theorem discussed herein (Separation, Alignment, Cohesion), a dedicated fingerprint profile can be designed to isolate drone movements within a specific swarm. By adding the security profiling developed in this study to that swarm data management, risk factors can be weighed for both rising and falling risk profiles as the swarm navigates a dedicated route.

Recommendation (iii). Future researchers should explore the relationship be-
tween the techniques outlined in this study and the capabilities of innovative hackers to propose a white hat hacking solution. This exploit-based study would increase knowledge regarding security threats and would highlight potential system vulnerabilities for future reconciliation. Whilst security preparedness may form the basis for threat mitigation, it also results in the increased exposure of systems to attacks by innovative hackers leveraging known exploits to take advantage of a given drone or swarm. However, the findings introduced in this study create normative standards of data management that might become obsolete once malicious actors recognize their vulnerabilities.

6.5. Summary

The long-term proposition of security administration is based upon the willingness of the industry to adopt new standards of practice, creating solutions that will address both in-flight and post hoc monitoring needs. These findings confirm that the proposed machine learning solution is both viable and precise for tracking disruptive threats to drone operations including DoS, hijacking, and signal interference. Further insights regarding drone fingerprinting and intra-swarm RC data monitoring have highlighted the importance of proximity vectors in framing a form of mesh security network around the UAV flight perimeter. By adapting the novel solution proposed herein to future design of security platforms, it is predicted that threat mitigation will become a function of system hardening, thereby aligning AI-supported threat mon-
itoring systems with structurally protected flight management protocol. Ultimately, this investigation adds another layer to an increasingly complex field of research that seeks to transform UAV security management into a probabilistic discipline. These procedures create a foundation upon which more innovative and dynamic procedures can be layered over time to systematically reduce the security vulnerabilities, focusing on the primary contribution of this research to this field, and recommend additional tests and analyses that could be used in the future to assess the evolution of drone security vulnerabilities affecting UAV flight security.

detection and monitoring for swarm drone flights. *Applied Sciences*, 9, 1-17.

Aldaej, A., Ahanger, T.A., Atiquzzaman, M., Ullah, I., and Yousufudin, M.
(2022). Smart cybersecurity framework for IoT-empowered drones; Machine learning

Arora, A., Shoeibi, N., Sati, V., Gonzalez-Briones, A., Chamoso, P., and Cor-

Arthur, M. (2019). Detecting signal spoofing and jamming attacks in UAV
networks using a lightweight IDS. *2019 International Conference on Computer, In-
formation and Telecommunication Systems (CITS)*.

and machine learning: Sustaining the investigation process. *Sustainability*. 14, 4861,
1-15.

airspace: Drone cyber attack detection through machine learning. *Future Internet*,
14(205), 1-19.


ISO. (2018) ISO 31000. ISO.


Pardhasaradhi, B. and Cenkeramaddi, L.R. (2022). GPS spoofing detection


UN. (1944). Convention on international civil aviation. UN, 7 December.

or mapping tools for environmental monitoring? The need for legal framework is required. *Transportation Research Procedia*, 25, 51-62.


VTO Labs (2022) *Drone Forensics*.


Zibaei, E. Banescu, S. and Pretschner, A. (2018). Diagnosis of safety in-
### Figure 37: Real Dataset from Drone Flight 28

<table>
<thead>
<tr>
<th>a</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
<th>IMU A (°/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>154</td>
<td>09:58:07</td>
<td>09:58:16</td>
<td>09:58:26</td>
<td>09:58:36</td>
<td>09:58:46</td>
<td>09:58:56</td>
<td>10:00:06</td>
<td>10:00:16</td>
<td>10:00:26</td>
<td>10:00:36</td>
<td>10:00:46</td>
<td>10:00:56</td>
<td>10:01:06</td>
</tr>
<tr>
<td>155</td>
<td>09:59:07</td>
<td>09:59:16</td>
<td>09:59:26</td>
<td>09:59:36</td>
<td>09:59:46</td>
<td>09:59:56</td>
<td>10:00:06</td>
<td>10:00:16</td>
<td>10:00:26</td>
<td>10:00:36</td>
<td>10:00:46</td>
<td>10:00:56</td>
<td>10:01:06</td>
</tr>
<tr>
<td>156</td>
<td>10:00:07</td>
<td>10:00:16</td>
<td>10:00:26</td>
<td>10:00:36</td>
<td>10:00:46</td>
<td>10:00:56</td>
<td>10:01:06</td>
<td>10:01:16</td>
<td>10:01:26</td>
<td>10:01:36</td>
<td>10:01:46</td>
<td>10:01:56</td>
<td>10:02:06</td>
</tr>
</tbody>
</table>

---
Figure 9. Anomaly classification result: (a) normal probability of x70, (b) average probability of vehicles.

Figure 38: Time History of Kinematic Variables
Figure 39: Moving Average