OPEN ACCESS

Manuscript ID:
ASH-2023-11026650

Volume: 11

Issue: 2

Month: October

Year: 2023

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 06.07.2023

Accepted: 25.08.2023

Published: 01.10.2023

Citation:
Alotaibi, Ahad, et al. "Ubiquitous Unmanned Aerial Vehicles (UAVs): A Comprehensive Review." *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. 2, 2023, pp. 62–90.

DOI:
https://doi.org/10.34293/sijash.v11i2.6650

Ubiquitous Unmanned Aerial Vehicles (UAVs): A Comprehensive Review

Ahad Alotaibi
Department of Engineering and Design
School of Engineering and Informatics
University of Sussex, United Kingdom
https://orcid.org/0009-0008-0410-2705

Chris Chatwin
Department of Engineering and Design
School of Engineering and Informatics
University of Sussex, United Kingdom

Phil Birch
Department of Engineering and Design
School of Engineering and Informatics
University of Sussex, United Kingdom

Abstract
Unmanned aerial vehicles (UAVs) or drones have found applications in various fields including military operations, construction, parcel delivery, mapping, medical, search and rescue missions, exploration of hidden areas, monitoring power lines and oil rigs, precision farming, aerial surveillance, and wireless communication. Due to their modular flexibility and programmability, drone technologies have become a strategic industrial/commercial sector that has gained significant attention as it redefines and combines different emerging domains, such as: service and delivery convergence, lean manufacturing, environmental monitoring and security. The use of swarms of interconnected UAV systems has gained popularity in providing innovative approaches to tasks requiring wide-area multiple collaborative sensors. However, despite advances in maneuverability, user interface, and cost-effectiveness, drones still face limitations in flight autonomy due to restricted flight time for continuous missions. Battery endurance, drone weight, and payload are critical development vectors. This review highlights the importance of drones, their future development priorities and functionality. Specifically, it focuses on UAV classification, swarms, and charging. Moreover, it explores UAV applications, challenges, and security issues based on recent research and development. Additionally, the study delves into anti-drone technology that can assist countries in controlling and ensuring the safe utilization of drones.

Keywords: Unmanned Aerial Vehicle (UAV), Swarm of Drones, Satellite, Challenges, Security, Applications.

Introduction

The use of unmanned aerial vehicles (UAVs), also known as drones, has seen a tremendous increase in recent years across various sectors. From military and surveillance to agriculture and package delivery; drones are being used to accomplish tasks that would have been impossible or difficult by conventional means. UAV technology has evolved to the extent that highly flexible drones are now available in a diverse range of types, sizes, and capabilities.

According to a report by the Federal Aviation Administration (FAA), the number of drones in the US reached 7 million by 2020, which represents an exponential growth from the 42,000 drones in 2016 (Federal Aviation Administration, United States). This significant increase in drone usage highlights their importance in various fields, including search and rescue, infrastructure inspection, and environmental monitoring.

However, drones still face challenges that limit their widespread usage, such as their limited flight time, battery endurance, and weight. One solution to these challenges is using systems of multiple UAVs. Using a swarm of drones can provide various advantages, such as greater flexibility, faster completion of tasks, redundancy, and better coverage. A swarm of drones is a group of autonomous unmanned aerial vehicles (UAVs) that operate cooperatively to perform a common task or achieve a specific goal. The drones in a swarm communicate with each other and coordinate their actions using wireless communication protocols and advanced algorithms.

Swarm technology is inspired by the collective behaviour of social animals, such as ants, bees, and birds, and is based on the principle of distributed intelligence. Each drone in the swarm is designed to perform a specific task and is equipped with sensors, cameras, and other types of data-gathering equipment that allow it to gather information about its surroundings and communicate with other drones in the swarm.

The use of a swarm of drones offers many advantages over a single drone, including increased reliability, flexibility, and efficiency. Swarms can adapt to changing environments and tasks, and can continue to operate even if some drones in the swarm fail or are damaged.

Swarm technology has many potential applications in a variety of fields, including military, surveillance, agriculture, search and rescue, and disaster response. However, the development of swarm technology also raises concerns about privacy, security, and the potential for drones to be used for malicious purposes.

Recent research has shown that using drone swarms can provide benefits across many sectors. In agriculture, for instance, drones can be used to perform crop monitoring and spraying with enhanced precision and efficiency (Ghazali et al.). In the construction industry, drones can be used to inspect buildings and bridges and monitor the progress of construction sites (Onososen et al.). In addition to these sectors, drones are also being used in emergency response, such as search and rescue, to provide real-time situational awareness (Sanz-Martos et al.).

This review aims to provide a comprehensive study of multiple UAVs, classification, swarms and charging. The primary focus of the paper is to explore the potential of swarm technology, its applications, and the challenges associated with its implementation. Furthermore, this paper will discuss the current research studies and development in the field of drone swarms, along with anti-drone techniques, which help countries to control and maintain the safe use of drones.

Overall, this review paper aims to provide a clear understanding of the potential of drones, as well as the challenges and limitations that come with their usage. By analyzing current research and development, the paper aims to identify areas where further research and innovation can contribute to the growth and advancement of this technology. The remainder of this paper is organized as follows: Section II provides an overview of the work contributed to the swarm of drones. Section III discusses the concept of swarm technology, characteristics, classifications, standardizations and charging in addition to communication. Section IV highlights the potential security challenges and solutions, while Section V explores anti-drone techniques. Section VI discusses the future challenges, followed by the conclusion in Section VII.

Related Work

Drones, also known as unmanned aerial vehicles (UAVs), have been in existence for over a century, with their use dating back to World War I when both the British and the Germans used them for surveillance purposes (Newcome). However, it was not until the 1960s that the first modern UAV was developed, the "Queen Bee" drone, which was used by the British military for target practice. This "Queen Bee" drone evolved from an earlier UAV that was used in the 1900's (Dalamagkidis et al.).

Since then, drones have been used for various purposes, including military operations, scientific research, and civilian applications. In the 1990s, drones were extensively used for military operations, particularly during the Gulf War, where they played a critical role in reconnaissance, surveillance, and target acquisition (Cook).

In recent years, there has been a significant increase in the use of drones for civilian purposes, including search and rescue, disaster relief, aerial photography, surveying, and delivery services (Qu et al.). For instance, Amazon has been developing drone delivery services, where packages can be delivered to customers within 30 minutes of their order being placed (Singireddy and Daim).

Furthermore, drones have been used for scientific research purposes, particularly in studying environmental changes and for conservation efforts. In 2021, a study published in the European Journal of wildlife research reported on the effectiveness of automatic aerial wildlife species identification from drone footage (Petso et al.).

In recent years, there has also been significant research focused on improving the performance and capabilities of drones, particularly with regards to autonomy and the development of swarms of drones. For instance, a study published in the journal IEEE Access in 2022 proposed a new optimized framework for managing swarm behavior in drones, demonstrating the potential for swarm intelligence in enhancing the performance and efficiency of drone-based systems (Qamar et al.).

Another recent development in drone technology is the use of artificial intelligence (AI) and machine learning (ML) algorithms, which have enabled drones to perform more complex tasks autonomously, such as object recognition and avoidance. In 2020, a study published in Mathematical Problems in Engineering journal reported on the use of a deep neural network for object detection in drone-based systems, demonstrating the potential of AI in enhancing the performance and capabilities of drones (Sun et al.). As drones continue to evolve, it is expected that their use will continue to expand, particularly with the development of new technologies such as AI and swarm intelligence.

The design of drones has evolved significantly over the past century, from the early rudimentary models to the sophisticated unmanned aerial vehicles (UAVs) we have today. Early drones were simple, remote-controlled aircraft that were primarily used for reconnaissance & surveillance purposes. One of the earliest models was developed by the British in 1917, called the "Aerial Target" or "Queen Bee," which was used for target practice (Atkins). These early drones were powered by gasoline engines and had limited range and endurance.

During World War II, drones were used for more complex operations, including as target drones for anti-aircraft gunnery practice and as guided bombs. The first jet-powered drone, the Kettering Bug, was developed by the United States in 1944 and was used as an unmanned flying bomb (Zaloga).

In the post-war era, the development of remote-controlled drones continued, with the United States leading the way. The 1960s saw the development of drones for surveillance and reconnaissance purposes, including the Lightning Bug and the Aquila drones (DeVore). These drones were typically launched from aircraft and had limited range and endurance.

The 1980s and 1990s saw significant advancements in drone technology, particularly in the areas of autonomy and payload capacity. The United States began to develop drones for use in military operations, including the Predator and Global Hawk (Cook). These drones were designed for long-range reconnaissance and surveillance missions and were equipped with advanced imaging and communication systems.

In recent years, there has been a significant increase in the use of drones for civilian purposes, including search and rescue, disaster relief, and aerial photography. The design of these drones has focused on making them more compact, lightweight, and efficient, with longer flight times and higher payload capacity.

One of the latest trends in drone design is the use of biomimicry, where drones are designed to mimic the flight patterns and behaviors of birds and insects. For example, researchers at Harvard University have developed a drone called the Robobee, which is modeled after the behavior of bees (Wood). This drone is equipped with a high-speed camera and sensors that allow it to fly and navigate autonomously.

Another trend in drone design is the use of hybrid power systems, which combine electric motors with combustion engines. These systems provide greater endurance and range than traditional electric or gasoline-powered drones (Yang). In addition, new materials and manufacturing techniques are being developed that allow for the creation of lighter, more durable drones. Advances in technology and materials have led to the development of sophisticated, autonomous drones that are used for a wide range of applications. The latest trends in drone design focuses on making drones more efficient, compact, and biomimetic, with longer flight times and higher payload capacity.

The architecture of a drone encompasses the various components and subsystems that enable it to operate, including the airframe, propulsion system, control system, and communication system. Over the years, there have been significant advancements in drone architecture, with researchers exploring new designs and technologies to enhance the performance, capabilities, and safety of drones.

One of the key areas of research in drone architecture is the development of new airframe designs. In recent years, there has been a trend towards smaller and more lightweight designs, which enable drones to be more agile and manoeuvrable. For instance, the use of carbon fiber and other lightweight materials has enabled the creation of drones that are both robust and lightweight (Kornbluh et al.). In addition, researchers have explored the use of unconventional airframe designs, such as quadrotors, which have become increasingly popular due to their ability to perform complex manoeuvres (Baballe et al.).

Another important component of drone architecture is the propulsion system, which provides the necessary thrust to lift the drone off the ground and control its movement. In recent years, there has been significant research focused on developing new propulsion systems that are more efficient and reliable. For instance, the use of electric motors has become increasingly popular, due to their low weight and high efficiency (Gutfleisch et al.). In addition, researchers have explored the use of hybrid propulsion systems, which combine electric motors with internal combustion engines (Sliwinski et al.).

The control system is another critical component of drone architecture, as it enables the pilot or autonomous system to control the movement and operation of the drone. In recent years, there has been significant research focused on developing new control systems that are more reliable and responsive. For instance, the use of fly-by-wire systems, which use computer-controlled electronic systems to control the drone's movement, has become increasingly popular (Yağdereli et al.). In addition, researchers have explored the use of autonomous control systems, which enable drones to operate independently without human intervention (Venugopal).

The communication system is also an important component of drone architecture, as it enables the drone to transmit and receive data and commands. In recent years, there has been significant research focused on developing new communication systems that are more reliable and secure. For instance, the use of satellite communication systems has become increasingly popular, due to their ability to provide reliable communication over long distances (Kuzlu et al.). In addition, researchers have explored the use of mesh network communication systems, which enable drones to communicate with each other and share information (Sharma et al.).

The control of drones is a crucial aspect of their operation, as it directly affects their stability, manoeuvr ability, and overall performance. Over the years, researchers have developed numerous control methods and algorithms to improve the control of drones.

One common approach is to use PID (Proportional-Integral-Derivative) controllers, which are widely used in industrial automation systems. PID controllers rely on feedback from sensors to adjust the drone's motor speeds and ensure it maintains its desired position and altitude (Merheb et al.). However, PID controllers are not always effective in dealing with nonlinearities and uncertainties, which can affect the drone's stability and control accuracy.

To overcome this limitation, researchers have developed more advanced control methods such as Model Predictive Control (MPC) and Nonlinear Model Predictive Control (NMPC) (Kouzoupis et al.). These methods use a mathematical model of the drone's dynamics and combine it with predictions of its future behaviour to generate control inputs that optimize for a given performance objective.

Another approach is to use artificial intelligence (AI) techniques such as deep reinforcement learning to train the drone's control system (Çetin et al.).

Reinforcement learning involves training the drone to make decisions based on rewards and penalties received during its operation. This approach has been shown to be effective in improving the drone's control performance in dynamic environments with changing conditions.

Moreover, swarm intelligence has been applied to control groups of drones to achieve collaborative tasks such as formation flight and cooperative surveillance (Alsamhi et al.). In swarm intelligence, the drones communicate and coordinate their actions based on local interactions, leading to emergent behaviours at the group level.

The choice of control method depends on the specific application and the complexity of the drone's dynamics. Furthermore, the development of new control methods and algorithms is an active area of research, with the aim of improving the performance and autonomy of drones.

The communication between drones, and between drones and their operators, is crucial for the safe and efficient operation of drone systems. Over the years, various communication technologies have been developed and utilized for drone communication, including Wi-Fi, cellular networks, satellite communication, and dedicated communication protocols.

One of the main challenges in drone communication is ensuring reliable and secure communication in environments with high interference and limited bandwidth. To address this challenge, researchers have proposed various solutions such as cognitive radio-based communication, multi-hop communication, and dynamic channel allocation. In a study published in the journal IEEE Communications Magazine in 2019, researchers proposed a cognitive radio-based communication system for drone networks. The proposed system utilized spectrum sensing and dynamic spectrum access techniques to efficiently utilize the available frequency bands, resulting in improved communication performance (Chriki et al.).

Another approach to addressing the communication challenges in drone networks is multi-hop communication, where messages are transmitted through a series of intermediate nodes to reach their destination. In a study published in the journal IEEE Transactions on Wireless Communications in 2019, researchers proposed a multi-hop communication protocol for drone networks, which utilized a hybrid communication scheme that combined both direct and relayed communication to achieve reliable and efficient communication in a range of scenarios (Wang et al.).

Additionally, researchers have explored the use of dedicated communication protocols for drone communication, such as the Dronecode protocol and the MAVLink protocol. These protocols are specifically designed for drone communication and enable efficient communication between drones and their operators.

In a study published in the journal Drones in 2020, researchers investigated the use of the MAVLink protocol for swarm communication in drone networks. The study demonstrated the potential of the protocol in enabling reliable and efficient communication in swarm-based drone systems (Sharma).

Finally, the use of satellite communication has also been explored for drone communication, particularly for long-distance and beyond-line-of-sight operations. In a study published in the journal IEEE Communications Magazine in 2020, researchers proposed a satellite-based communication system for drone networks, which utilized a low-Earth-orbit satellite constellation to provide reliable and efficient communication over long distances (Yang).

Overall, the communication of drones is a critical area of research that plays a crucial role in ensuring the safe and efficient operation of drone systems. The development of new communication technologies and protocols will continue to be a focus of research as drone systems continue to evolve and become increasingly integrated into a range of applications.

Unmanned aerial vehicles (UAVs), or drones, have become increasingly popular, and as their utilization expands, so do the security concerns associated with them. Drones are vulnerable to various types of cyber-attacks, and the consequences of such attacks can be severe, ranging from loss of control over the drone to theft of sensitive data.

One of the primary security challenges associated with drones is the need to protect them against unauthorized access or takeover. This can be accomplished through a variety of means, including encryption, authentication, and intrusion detection systems. Several approaches to enhance the security of drone communication have been suggested by researchers. These include utilizing secure communication protocols like Transport Layer Security (TLS) and incorporating access control mechanisms to ensure that only authorized individuals are able to access the drone's control systems (Usman et al.).

Another area of concern is the physical security of drones. Drones can be stolen or physically attacked, which can compromise their functionality or lead to the theft of sensitive data stored on board. To address this issue, researchers have developed anti-theft mechanisms, such as geofencing and automatic return-to-home protocols, which help to prevent unauthorized access and theft (Maluleke).

A significant security threat associated with drones is their potential use as weapons, either by terrorists or other malicious actors. To mitigate this threat, researchers have proposed several solutions, including developing counter-drone systems that can detect and neutralize hostile drones. These systems typically rely on a combination of sensors and jamming technology to disrupt the communication between the drone and its operator (Hartmann and Steup). Finally, researchers have also explored the use of machine learning algorithms to enhance the security of drones. For instance, researchers have proposed the use of anomaly detection algorithms to detect unusual behaviour in the drone's control systems, which can indicate a cyber-attack (Fahim and Sillitti).

As the use of drones has become increasingly popular, so has the need to protect against them. Anti-drone technology refers to the various methods used to detect, track, and counter rogue drones that may pose a threat to safety, privacy, or security. Below are some of the latest developments in anti-drone technology:

Radio Frequency (RF) Jamming: RF jamming is one of the most common and effective methods of disabling drones. This technique involves the use of a jamming device that sends out a powerful radio signal to disrupt the drone's control link and GPS signals, causing it to lose connection and fall out of the sky. However, this technique can also disrupt legitimate communication systems and is illegal in many countries without the appropriate authorization (Ezuma et al.).

Drone Detection Systems: Drone detection systems use various technologies such as post-radar, acoustics, and optical sensors to detect and track drones. These systems can help identify the location and trajectory of the drone, allowing authorities to take appropriate measures to intercept it. For instance, one such system is Drone Shield, which uses acoustic sensors and pattern recognition algorithms to detect and identify drones up to 750m away (Barchyn et al.).

Drone Capture Nets: Drone capture nets are physical barriers designed to catch and disable drones mid-flight. These nets can be deployed from the ground or from another drone and use a combination of advanced sensors and algorithms to ensure accurate targeting of the drone. For instance, one such system is Skywall 100, which uses a compressed air launcher to deploy a net over the target drone and bring it to the ground safely (Tupitsyn).

Laser Systems: Laser systems are another effective anti-drone technology that uses high-powered lasers to disable the drone's motors and other critical components. This technique is often used in military applications and can be highly effective in neutralizing hostile drones. For instance, one such system is the Silent Hunter laser weapon system, which uses a 30kW laser to disable drones up to 7km away (Tupitsyn).

Radio Frequency Identification (RFID) Tags: RFID tags are small electronic devices that can be attached to drones to help track and identify them. These tags can be used to enforce no-fly zones and prevent unauthorized drone flights in sensitive areas. For instance, one such system is the AeroScope system, which uses RFID tags to identify and track drones in real-time (Dudczyk et al.).

Anti-drone technology is rapidly evolving, and new techniques are constantly being developed to detect and neutralize rogue drones. As drone use continues to grow, the need for effective anti-drone technology will become increasingly critical in ensuring safety, privacy, and security.

Swarm of drones has become a popular research topic due to its potential applications in various fields. One application of swarm of drones is in agriculture, where they can be used for precision farming, crop monitoring, and pest control (Raj et al.). In construction, swarms of drones can be used for surveying and mapping large construction sites, as well as for monitoring progress and detecting safety hazards (Tkáč and Mésároš). Swarms of drones can also be used in search and rescue operations, where they can cover a larger area and search for missing persons more efficiently than a single drone (Mayer et al.). Another application is in the entertainment industry, where swarms of drones can be used for light shows and aerial displays (Ahn et al.). There are also potential applications in the military, where swarms of drones can be used for surveillance, reconnaissance, and target acquisition (Elmeseiry et al.). As the technology for swarm of drones continues to improve, their applications will likely expand into new fields and industries.

Characteristics of Drones

Unmanned aerial vehicles (UAVs) possess distinct characteristics enabling them to perform a wide range of tasks. They are equipped with aerodynamic designs and flight control systems, allowing for stable flight and maneuverability. Figure (1) below shows an overview of unmanned aerial vehicles. Characteristics of UAV's are listed below:

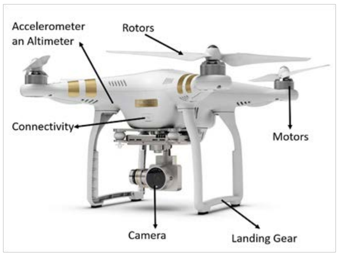


Figure 1 UAV Overview

Aerodynamics

UAVs are designed with aerodynamic principles in mind to achieve stable flight. Aerodynamics is the study of how air interacts with solid objects, such as an aircraft or a drone. This interaction creates forces that influence the motion of the object, allowing it to maintain stability and control during flight. In this section, detailed explanation of aerodynamics of the quad copters drones is introduced to illustrate how UAV's fly. There are four primary forces at play in UAV flight: lift, weight, thrust, and drag as shown in figure (2) below:

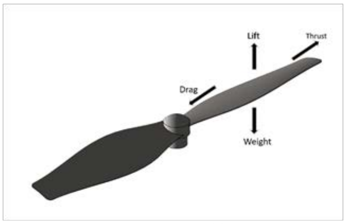


Figure 2 Forces that Affect UAV Flight

The lift force pulls the wing up and the weight force counteracts this downwards. Furthermore, the thrust force is necessary in order to generate an airflow and drag opposes the forward movement. In a steady and straight flight, all forces acting on the wing are in equilibrium, so that no resulting force remains. No resulting force means that the aircraft or rotor blade does not become faster or slower, nor does it climb or descend. If this balance is intentionally or unintentionally disturbed, the UAV climbs or descends, becomes faster or slower.

The aim of the typical wing shape is to maintain an optimal balance between lift and drag and to enable lift even at different speeds. This can be achieved by "tilting" a surface slightly towards the airflow, which creates a pressure difference between the top and bottom of the aerofoil. This angle between the wing chord and the airflow direction is called the angle of attack. By increasing the angle of attack of a wing, the air above the wing is accelerated, causing the pressure to drop. Below the wing, the air presses a little against the surface, which creates a higher-pressure underneath. The result is a force on the wing, which pulls it upwards – this is lift.

In addition to the angle of attack, the speed of the airflow plays a role in the strength of the lift: the faster the wing moves through the air, the higher the lift. In the case of a UAV with propellers, the lift increases accordingly with a higher rotation speed of propellers.

The Unmanned Aerial Vehicle or, UAV can move around three orthogonal axes in all three spatial directions: The longitudinal axis goes length ways through the aircraft; movements around the longitudinal axis are called "roll" and the type of control is called lateral control. The lateral axis runs transversely to the direction of flight: with a surface UAV it can be thought of running through the wings; movements around the lateral axis are called pitch and the type of control is called longitudinal control. The normal axis runs vertically from top to bottom through the UAV; movements around the vertical axis are called yaw and the type of control is called directional control as shown figure (3a) below:

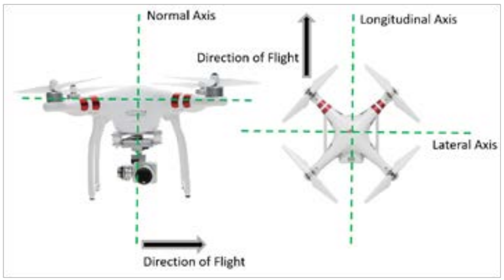


Figure 3a UAV Movements Overview

All axes are perpendicular to each other. In the case of multi-rotor UAV, which usually have a symmetrical structure, the front direction is often marked so that the directions of movement can be clearly identified. The movements of multi-rotor UAV are implemented by varying the propeller speed. Elevator, rudder and ailerons are used by UAV with wings. A multi-rotor UAV or multi-copter has three directions of movement shown in figure (3b):

- Up and down
- Rotating around its own axis
- Sideways, forward and backward.

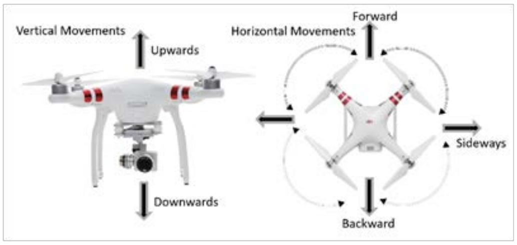


Figure 3b UAV Movements Overview

The propellers of the UAVs do not all rotate in the same direction. As a rule, the opposite propellers turn in the same direction, the directly neighboring propellers in the opposite direction. This prevents unwanted rotation around the UAV's own axis. To take-off with a UAV, the total upward force generated by all propellers must be stronger than the gravitational force. This is achieved by rotating the propellers faster. Once the desired flight altitude has been reached, the speed of the propellers is reduced until there is a balance between lift and weight.

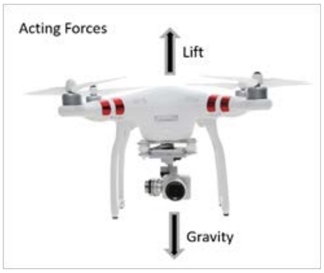


Figure 3c UAV Movements Overview

In order to descend with the UAV, the lift generated by the propellers must be slightly less than the gravitational pull. To turn around its axis, the total force of one pair of opposing propellers must be greater than that of the other pair. An example: if, propellers 1 and 4 turn faster than 2 and 3, the UAV turns clockwise around its own axis. This can be achieved by increasing the force on propellers 1 and 4 or reducing it to propellers 2 and 3.However, if only the force on propellers 1 and 4 is increased, the UAV would climb due to the increased lift. To prevent this, the speed of propellers 2 and 3 must be reduced at the same time as shown in figure (3d).

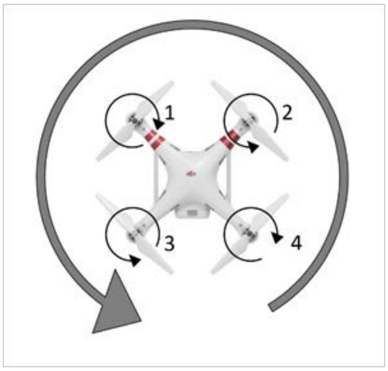


Figure 3d UAV Movements Overview

Flight Control System

The flight controller, acting as the central processing unit of a drone, functions as its intelligence hub. It consists of a compact enclosure housing intelligent electronics and software that oversee and manage all aspects of the drone's operations. Similar to the varying size and complexity of brains in different organisms, flight controllers also exhibit diversity in terms of their dimensions and intricacy. Drones use sophisticated flight control systems to maintain stability and control during flight. These systems include gyroscopes, accelerometers, and magnetometers to measure orientation, altitude, and speed. They also incorporate control algorithms to adjust the drone's motors or rotors for stability and maneuvering. Figure (4) below shows an example of flight controller.

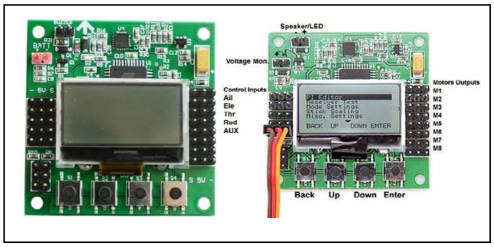


Figure 4 Drone Flight Controller

Propulsion

Based on their wing-type, UAVs can be classified into six groups, as depicted in Figure (5): fixed-wing UAVs, multi-rotary wing UAVs, unmanned helicopters, blimps, parachute-wing UAVs, and flapping-wing UAVs. Presently, fixed-wing and multi-rotary wing UAVs are the primary choice for both military and civilian applications (Boon et al.). Examples of fixed-wing UAVs include the U.S. Air Force's Global Hawk UAVs and China's Cai-Hong and Wing Loong series UAVs, which exhibit exceptional performance and are capable of adapting to the complex conditions of the battlefield (Brown et al.). On the other hand, multi-rotary wing UAVs are renowned for their cost-effectiveness, user-friendly operation, lightweight construction, portability, and stable flight performance, making them widely utilized in civilian applications (Azeta et al.). For instance, Chinese company Da Jiang Innovations has introduced the "Yu" Mavic series and "Xiao" Spark series of UAVs, specifically designed to meet the demands of aerial photography in everyday life. Additionally, UAVs can be categorized into mini, micro, and nano scales based on their size, as well as classified into different types, including low-speed, subsonic, transonic, supersonic, and hypersonic, based on their flight speeds. Figure (5) shows different types of drones.

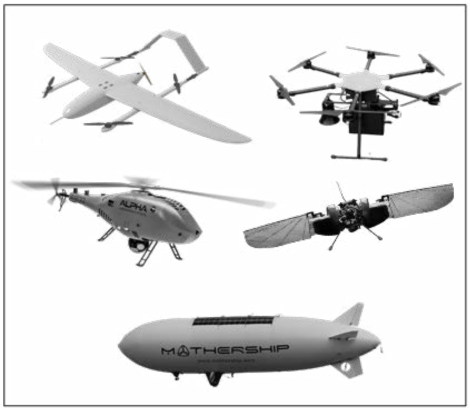


Figure 5 Different types of drones

Navigation and Positioning

Navigation and positioning in drones are critical for their precise control and accurate flight. Drones rely on a combination of sensors, systems, and algorithms to determine their position and navigate in their environment.

The Global Navigation Satellite System (GNSS) comprises a cluster of strategically positioned satellites that play a crucial role in generating and transmitting positioning, timing, and navigation data from space to sensors on Earth. These sensors, commonly referred to as receivers, utilize this data to determine precise locations. Satellite networks serve as a supplementary solution to existing infrastructure, extending global connectivity in situations where terrestrial networks are inaccessible or impractical.

However, satellite networks vary in their capabilities. Service providers offer different solutions based on the orbits they have access to. Therefore, comprehending the impact of Earth's distance on performance is essential when making decisions about choosing a satellite service. There are three main orbit classes: GEOSTATIONARY EARTH ORBIT (GEO), MEDIUM EARTH ORBIT (MEO), and LOW EARTH ORBIT (LEO) as shown in figure (6) below:

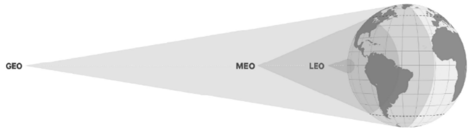


Figure 6 Different Orbital Altitudes and Coverage Areas

There are many studies and articles that focus on the comparison of each type of orbits. It is commonly known that for navigation and positioning purposes the medium earth orbit or MEO is the best option to use. MEO benefits are: low latency, long life time, and a small size of network making it easy to maintain. Examples of MEO's GNSS include:

- USA's NAVSTAR Global Positioning System (GPS).
- Europe's Galileo.
- IRNSS Satellite by India.
- Russia's Global'naya Navigatsion naya Sputnikovaya Sistema (GLONASS).
- China's BeiDou Navigation Satellite System.

  The United States Government (USG) owns and the United States Space Force (USSF) operates the Navstar Global Positioning System, also known as GPS. Since 1993, GPS has been consistently offering positioning, navigation, and timing services to both military and civilian users across the globe (Department of Defense United States). The system enables an infinite number of users, equipped with either a civil or military GPS receiver, to determine precise time and location anywhere in the world, regardless of weather conditions or the time of day. The United States Space Force (USSF) is in charge of the system's design, development, procurement, operation, maintenance, and enhancement. At the core of this system is a network of approximately 32 satellites orbiting the Earth, although this number may slightly change due to the retirement or replacement of older satellites. The GPS system is comprised of three segments: space, control, and user, which are detailed below:
- The Space Segment comprises a minimum of 24 functioning satellites that are positioned in six circular orbits, approximately 20,200 km (10,900 NM) above the Earth. These orbits have an inclination angle of 55 degrees and a period of 11 hours and 58 minutes. While not an explicit mandate, the satellites are usually distributed across primary orbital slots to ensure that at any given time, users worldwide will have an uninterrupted view of at least six satellites.
- The Control Segment is comprised of a main control station situated in Colorado Springs, along with five monitoring stations and three ground antennas distributed worldwide. The monitoring stations are responsible for tracking all GPS satellites within their field of view and gathering ranging data from their broadcasts. This collected information is conveyed back to the master control station, where highly accurate satellite orbits are computed. Subsequently, the information is formatted into updated navigation messages for each satellite. The ground antennas play a dual role by transmitting and receiving signals for satellite control and monitoring, as well as transmitting the updated information to each satellite.
- The User Segment encompasses the elements essential for land, sea, or airborne operators to receive GPS satellite broadcasts and accurately calculate their precise position, velocity, and time. This segment comprises receivers, processors, and antennas that facilitate these operations.

GPS receivers are integrated into various devices, such as phones, cars, fitness wearables, and drones, allowing users to connect to the GPS network. The method used to accurately determine the location of a GPS receiver is known as triangulation. Within the network, each satellite emits signals that are time stamped and intercepted by GPS receivers on the ground. These signals travel as radio waves at the speed of light. By measuring the duration it takes for the signals to reach the receiver from multiple satellites, the distance between the receiver and each satellite can be calculated. Analyzing data from several satellites allows for the efficient and precise determination of any GPS receiver's location on Earth. (Integrity And Continuity Analysis From GPS Name).

GLONASS, another Global Navigation Satellite System, was initially developed by the Soviet Union as an experimental military communication system in the 1970s. However, with the end of the Cold War, the Soviet Union recognized the commercial potential of GLONASS due to its capabilities for transmitting weather broadcasts, communications, navigation, and reconnaissance data. The first GLONASS satellite was launched in 1982, and by 1993, the system was declared fully operational. Despite facing a period of decreased performance, Russia committed to improving GLONASS and ensuring a minimum of 18 active satellites. Presently, GLONASS boasts a complete constellation with 24 satellites. Over time, there have been advancements in GLONASS satellites, with the latest generation known as the GLONASS-M, as depicted in Figure (7).

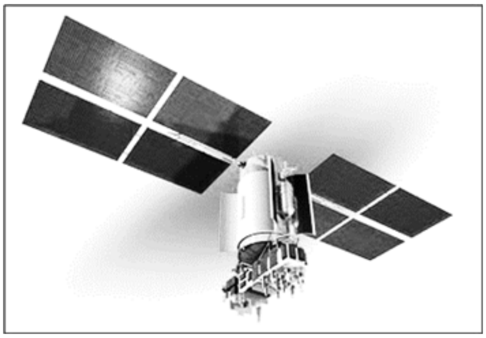


Figure 7 GLONASS Satellite

Glonass Consists of the Following Segments

The Space Segment of GLONASS comprises a constellation of 24 satellites divided into three orbital planes, each containing eight satellites. The arrangement of the GLONASS constellation repeats approximately every eight days. To ensure synchronization, each satellite completes precisely 17 orbital revolutions over an orbital period of around 8/17 of a sidereal day. In each orbital plane, the satellites are evenly distributed, and a specific satellite consistently occupies the same position in the sky at the same sidereal time each day. These satellites are positioned in nearly circular orbits with an inclination of 64.8 degrees and an orbital radius of 19,140 kilometers (11,893 miles), which is approximately 1,060 kilometers (659 miles) closer to Earth compared to GPS satellites (Matosevic et al.).

The Control Segment of GLONASS consists of the system control center and a network of command tracking stations situated across Russia. Comparable to the GPS control segment, the GLONASS control segment carries out multiple tasks. It continuously monitors the health of the satellites, computes ephemeris corrections, and establishes the satellite clock deviations in relation to GLONASS time and UTC. Twice a day, the control segment uploads essential corrections to the satellites to guarantee precise positioning and timing information.

Galileo, the Global Navigation Satellite System of Europe, offers a precise and reliable global positioning service that is under civilian control. To ensure compatibility and interoperability between GPS and Galileo for users, the United States and the European Union have been collaborating since 2004. Galileo provides a reliable and uninterrupted service even under extreme circumstances, except for the most severe situations. It quickly notifies users of any satellite failures, ensuring their awareness within seconds. This makes Galileo well-suited for safety-critical applications, such as air and ground transportation. The initial deployment of Galileo involved launching experimental satellites, including the first one in December 2005 and the second in April 2008. These satellites were part of the Galileo System Test Bed (GSTB) and aimed to assess crucial Galileo technologies that were already in development under contracts with the European Space Agency (ESA). Following this, four in-orbit validation satellites were launched between 2011 and 2012 to verify the functionality of the fundamental Galileo space and ground segment (Yayla et al.).

The Galileo navigation system ensures coverage at all latitudes through a network of satellites. The constellation is well-optimized and includes spare satellites to prevent any noticeable impact in case of satellite loss. Two Galileo Control Centers in Europe oversee the operation of the satellites. Data from thirty Galileo Sensor Stations is transmitted to the control centers through a redundant communication network. The sensor stations' data helps compute integrity information and synchronize satellite time with ground station clocks. Uplink stations around the world facilitate communication between the control centers and the satellites. Galileo also incorporates a global Search and Rescue (SAR) function, utilizing the Cospas-Sarsat3 system. Each Galileo satellite is equipped with a transponder that transfers distress signals to the Rescue Coordination Centre, enabling timely rescue operations. Additionally, the system provides feedback to users, informing them that their distress signals have been detected and help is on the way. This feature is considered a significant improvement compared to existing systems, which lack user feedback.

MEO orbits are characterized by altitudes ranging from 2,000 kilometers to approximately 36,000 kilometers. On the other hand, LEO satellites operate at altitudes below 2,000 kilometers. GPS satellites complete two orbits around the Earth per day, while LEO constellations have a significantly shorter orbital period of less than 128 minutes, resulting in at least 11.25 orbits per day. This discrepancy in orbital periods also means that GPS satellites remain visible for extended periods, whereas LEO satellites can only be seen for less than 15 minutes at a time. Apart from altitude, there are other distinctions between the GPS constellation and LEO constellations. Due to their significantly closer proximity to Earth, LEO satellites benefit from stronger signal strength compared to GPS. Signals received from LEO satellites on Earth's surface can be up to 1,000 times (30 decibels (dB)) stronger than GPS signals. This enhanced signal strength offers advantages such as better penetration through obstructions, reduced multipath effects, and improved resistance to interference. LEO signals theoretically have the potential to reach areas inaccessible to traditional GPS, including indoor environments. Some well-known LEO satellites include Starlink and OneWeb.

Starlink is a satellite constellation system designed to provide worldwide internet coverage, particularly in rural and remote areas with limited or no internet access. Spearheaded by SpaceX, a private aerospace company founded by Elon Musk in 2002, Starlink aims to establish a global broadband network using a constellation of low Earth orbit (LEO) satellites to offer high-speed internet services. This technology builds upon existing satellite internet systems that have been in use for decades. Instead of relying on cable-based technologies like fiber optics, Starlink utilizes radio signals transmitted through space to deliver internet data. Ground stations on Earth send signals to satellites in orbit, which then transmit the data to Starlink users on the ground. Each satellite in the Starlink constellation weighs 573 pounds and has a flat design. A single SpaceX Falcon 9 rocket can transport up to 60 satellites. The ultimate objective of Starlink is to create a low-latency network in space that enables edge computing on Earth. Constructing a global satellite network is a significant challenge, but it is particularly valuable due to the requirement for low latency. To meet this demand, SpaceX has proposed launching approximately 42,000 satellite units, approximately the size of tablets, into low orbit across the globe.

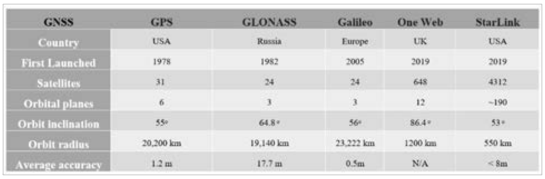
Nevertheless, Starlink faces competition in the space race from OneWeb, HughesNet, Viasat, and Amazon. HughesNet has been offering signal coverage from a distance of 22,000 miles above Earth since 1996. However, Starlink takes a slightly different approach and introduces the following enhancements (Gahír and Novák):

- Rather than utilizing a small number of large satellites, Starlink opts for a vast network of thousands of small satellites. SpaceX has ambitious plans to deploy up to 42,000 satellites, aiming to provide comprehensive satellite coverage globally, even in remote areas, while minimizing service interruptions.
- Starlink employs Low Earth Orbit (LEO) satellites that orbit the Earth at a mere 300 miles above its surface. This closer proximity than the geostationary orbit enables faster internet speeds and lower latency compared to traditional satellite systems.
- The latest Starlink satellites are equipped with laser communication components, enabling direct signal transmission between satellites. This technology reduces the reliance on numerous ground stations for communication purposes.

An alternative option that has been proposed is to utilize the Starlink system for satellite navigation purposes, similar to how GPS is used. While the primary objective of Starlink is to offer global internet connectivity, there are engineers who believe it can be modified to serve as a satellite navigation system as well. Non-SpaceX researchers have explored this possibility and successfully triangulated signals from six Starlink satellites to pinpoint a specific location on Earth. They were able to achieve an impressive level of accuracy, with measurements showing an error margin of less than 8 meters (Hartnett).

By referring to the table (1) presented below, one can compare the accuracy of different navigation systems and determine which system has deficiencies and in which specific area. In terms of accuracy, GPS and Galileo stand out as clear frontrunners, with average deviations of 1.2 and 0.5 meters respectively. On the other hand, the GLONASS systems demonstrate marginally poorer performance with deviation values of 17.7 meters (Kassas et al.).

Table 1 LEO vs MEO Comparison



GNSS	GPS	GLONASS	Galileo	One Web	StarLink
Country	USA	Russia	Europe	UK	USA
First Launched	1978	1982	2005	2019	2019
Satellites	31	24	24	648	4312
Orbital planes	6	3	3	12	~190
Orbit inclination	55°	64.8°	56°	86.4°	53°
Orbit radius	20,200 km	19,140 km	23,222 km	1200 km	550 km
Average accuracy	1.2 m	17.7 m	0.5m	N/A	< 8m

The advancement in miniaturization technology has enabled satellite receivers to be integrated into drones, including lightweight and highly portable models. This integration of satellite communications has positively impacted drone flights in terms of safety and autonomous capabilities. Safety has always been a major concern in drone development, and satellites have emerged as a crucial component for various safety features. These features range from beginner-friendly flight modes to more advanced tracking and geo-fencing systems, making drones more easily accessible and ensuring drone pilots are accountable for maintaining airspace safety.

The integration of satellite technology is essential for enabling automated flight, which is considered one of the most advanced capabilities of modern drones. Not only is it fascinating to observe a drone effortlessly navigate with minimal human control, but the utilization of satellites greatly enhances the accuracy and consistency of drone flight. This advancement has unlocked numerous commercially valuable opportunities for drones, ranging from agricultural management to search and rescue missions. The integration of GPS technology with drones has been a groundbreaking development that has significantly facilitated the broader acceptance and utilization of drones across various industries. Satellites have made possible a wide array of features that enhance the performance and functionality of drones:

Satellite Stabilization

The application of a swarm of drones can significantly enhance and maintain drone/satellite stabilization. Effective communication between the drones ensures synchronization and enables stable control of the drones. This innovative approach offers several advantages, such as improved stability and accuracy, swift response to disturbances, redundancy in the event of drone failure..

Return to Home

In instances where a drone loses connection with its remote controller or experiences low battery power, it typically initiates a function known as “return to home” (RTH) (Goudarzi and Richards). This function guarantees that the drone will automatically navigate back to either its initial take-off point or the present location of the remote control. By using RTH, drone pilots have been saved from the frustration of losing their drones or experiencing crashes due to depleted batteries. Satellites play a vital role in facilitating the safe and effective return of a swarm of drones to their home base. Through global communication coverage and navigation capabilities, satellites enable the drones to establish communication and receive instructions from ground control systems. Leveraging satellite-based GPS technology, the drones can precisely determine their current position and calculate the optimal route back to their designated home coordinates. Satellite communication protocols ensure real-time coordination between the drones and ground control, allowing for adjustments to flight parameters and progress monitoring. Additionally, satellites contribute to safety by providing updates on weather conditions and potential obstacles, enabling drones to avoid hazards during their return journey. The redundancy provided by multiple satellites ensures uninterrupted communication and continuous monitoring of the drones’ progress, enabling immediate response to any deviations from the intended return path. Overall, satellites play a crucial role in enabling the successful implementation of the return-to-home functionality for a swarm of drones.

Object Tracking

The utilization of satellites greatly enhances the tracking capabilities of a swarm of drones.

Satellites play a crucial role in enabling efficient communication, navigation, and positioning, ensuring effective tracking of the drones. Satellite communication acts as a reliable and global channel for the swarm, maintaining constant connectivity and facilitating real-time updates on the drones' location, status, and movements. This continuous communication ensures seamless tracking and provides the ground control system with accurate and up-to-date information about the swarm's whereabouts. Furthermore, satellite-based navigation systems, such as GPS, play a vital role in accurately tracking the drones. Drones equipped with GPS receivers can precisely determine their location and transmit this data to the ground station via satellite communication, enabling real-time monitoring and ensuring the drones stay on the intended trajectory. Satellites also offer precise timing information, promoting synchronization among the drones in the swarm and facilitating coordinated formations and movements, enhancing the effectiveness of tracking the entire swarm as a unified entity. Additionally, satellite positioning enables geo-location capabilities, particularly valuable when tracking the swarm in remote or inaccessible areas. It provides accurate drone position determination, even in challenging or unfamiliar environments, allowing for easier tracking over vast geographic regions. Satellites also contribute to the reliability and resilience of the tracking feature, as they operate from high altitudes, offering a broader line-of-sight and reducing the likelihood of signal obstructions or interference compared to ground-based communication systems. This ensures consistent tracking of the swarm, even in areas with limited terrestrial infrastructure or rough terrains. Overall, the integration of satellite technology enhances the tracking capabilities of a drone swarm, providing a reliable communication channel, accurate navigation and positioning systems, synchronization support, and resilient tracking capabilities. The use of advanced camera drones has also introduced new opportunities in cinematography, allowing for automatic subject identification and tracking. Optical recognition is commonly employed in drones with these features, but some also offer GPS-aided tracking. This feature utilizes a hand held beacon held by the subject, enabling the drone to follow their GPS position. Although hand held beacons are not widely available, they prove to be extremely valuable, particularly for drone pilots who prefer to avoid bulky remote controllers (Jacobsson et al.).

GPS Waypoints

By utilizing GPS waypoints, a drone operator can easily set predetermined flight paths for the drone to autonomously navigate. The drone will move from one waypoint to another, pausing only when directed by the operator, when battery levels are critical, or when the designated route has been completed. This particular capability has revolutionized drones, making them valuable tools for extensive surveillance and remote sensing studies. Automated drone flight plays a crucial role in various applications including drone-based mapping, precision agriculture, thermal mapping, and other endeavors that involve gathering data utilizing drones' unique perspectives. During the surveying process, the drone operator simply establishes the survey parameters or outlines a specific flight path for the drone to follow. Subsequently, the drone will traverse this path, collecting the necessary data (Kangunde et al.). In addition to minimizing pilot involvement, the advantage of this feature lies in the ability to save and replicate flight paths as necessary, accommodating multiple drones if needed.

Geo Fencing

GeoFencing is a relatively recent innovation within the drone industry that enables drones to detect their presence in controlled or restricted airspace, thus preventing unauthorized flights. However, this feature has generated mixed reactions, with certain drone pilots expressing frustration regarding its limitations, while drone manufacturers argue for its value in enhancing safety. In essence, geofencing functions by cross-referencing a drone's GPS coordinates with a database of restricted or controlled airspace zones. If the drone is located within these designated no-fly areas, it must undergo an unlocking process before a new flight can occur. The exact procedure for unlocking a drone depends on the severity of flight restrictions in the specific no-fly zone (Tony et al.). Currently, it remains uncertain whether geofencing will become a standard feature in future drones. While ensuring the safety of national airspace is of utmost importance, it is also necessary to consider the freedom of drone pilots to operate without unnecessary obstacles.

Future work and experiments will focus more on new LEO technology and how to integrate with the drone elements. In 2023, Ohio State University conducted research revealing that an innovative algorithm could achieve an unparalleled level of accuracy in pinpointing the location of a stationary receiver on the ground. By analysing signals from eight LEO satellites for approximately 10 minutes, the algorithm successfully converged on the receiver with an impressive error margin of merely 5.8 meters (Kozhaya et al.).

Remote Control and Telemetry

Remote control and telemetry systems are integral components of drone operations, enabling communication between the operator and the unmanned aerial vehicle (UAV). Remote control systems consist of a controller held by the operator and a receiver installed on the drone. They employ wireless communication protocols using radio frequencies or Wi-Fi to establish a link. The operator uses the controller's joysticks, buttons, or switches to send commands to the drone, specifying desired flight manoeuvres or actions. These commands are transmitted wirelessly to the drone's receiver, which interprets them and adjusts the drone's flight controls accordingly. Telemetry systems, on the other hand, provide real-time data feedback from the drone to the operator. This data includes crucial information such as altitude, speed, battery voltage, GPS coordinates, sensor readings, and other flight parameters (Rodrigues et al.). Telemetry systems use similar wireless communication methods as the remote control systems to transmit data from the drone to the operator's ground station. The operator can monitor this telemetry data on a display or interface, allowing them to assess the drone's status, make informed decisions, and maintain situational awareness during flight. Remote control and telemetry systems play a vital role in ensuring safe and efficient drone operations by facilitating real-time control and monitoring capabilities for both manual and autonomous flights.

Onboard Sensors and Cameras

On-board sensors and cameras are essential components of drones, enabling them to collect data and gather valuable information about their surroundings. Drones can be equipped with a wide range of sensors and cameras depending on their intended applications. Optical sensors, such as high-resolution cameras, allow drones to capture images and videos from aerial perspectives. These cameras can be equipped with various lenses and filters to capture specific details or wavelengths of light, including visible light, infrared, or multispectral data (Morales et al.). Thermal imaging cameras, another common sensor, detect heat signatures and enable drones to conduct thermal inspections, search and rescue operations, or detect anomalies. LiDAR sensors utilize laser pulses to measure distances and generate 3D point clouds of the environment, enabling drones to perform accurate mapping, terrain modelling, or obstacle avoidance. Additionally, drones can be equipped with sensors like accelerometers, gyroscopes, magnetometers,and GPS receivers for precise positioning, orientation, and navigation. These sensors contribute to the overall stability, control, and autonomous capabilities of the drone. Onboard sensors and cameras play a crucial role in various fields, including aerial photography, surveillance, environmental monitoring, precision agriculture, infrastructure inspection, and scientific research, providing valuable data and insights from a bird's eye view.

Power Source

The power source is a critical component of drones, providing the necessary energy for propulsion, control systems, sensors, and onboard electronics. Drones typically rely on rechargeable batteries, with lithium-polymer (Li-Po) and lithium-ion (Li-ion) batteries being the most common types used (Townsend et al.). These batteries offer a high energy density, lightweight design, and relatively long discharge times, making them suitable for drone applications. The capacity of the battery directly impacts the flight time of the drone. Larger capacity batteries can provide extended flight durations, while smaller capacity batteries are used in compact drones. The voltage of the battery must also match the requirements of the drone's electronic systems and motors. To ensure safe and efficient operation, drones often employ battery management systems (BMS) that monitor the battery's state of charge, voltage levels, and temperature. This helps prevent overcharging, undercharging, and thermal runaway, enhancing the overall safety and longevity of the batteries. Advances in battery technology continue to drive improvements in drone flight endurance and performance, with ongoing research focused on developing lighter, more efficient, and higher-capacity power sources for drones. High payload drones use IC engines or gas turbines with fixed wings, as with Global Hawk. Hybrid systems use batteries combined with heat engines. However, for the mass market there is continuous research and innovation in battery technology, which is the dominant source of power for commercial drones.

Payload Capacity

Payload capacity is a crucial consideration in the design and operation of drones, referring to the maximum weight a drone can carry in addition to its own weight. The payload capacity of a drone is determined by various factors, including its size, structural strength, power source, and aerodynamic capabilities. The payload capacity directly influences the types of tasks and applications a drone can perform. For example, drones used in aerial photography or cinematography may need to carry high-resolution cameras and stabilizing equipment, while drones employed in delivery services may need to transport packages or medical supplies. The payload capacity also affects the flight performance of the drone, including its endurance, manoeuvrability, and stability. Exceeding the payload capacity can strain the motors, decrease flight times, and compromise the safety and control of the drone. Drone manufacturers provide specifications on the maximum payload capacity, and it is crucial for operators to carefully consider and adhere to these limits to ensure safe and efficient operations. Advancements in drone technology continue to push the boundaries of payload capacity, allowing for the transportation of heavier payloads and expanding the range of applications in fields such as aerial surveying, agriculture, disaster response, and more (Greenwood et al.).

Software And Control Algorithms

Software and control algorithms are integral components of drones, enabling precise control, autonomous flight, and intelligent functionality. Drones rely on software systems to interpret commands from the operator or autonomously navigate their environment. Flight control software processes inputs from various sensors, such as accelerometers, gyroscopes, and GPS, to stabilize the drone, maintain its desired attitude, and execute flight maneuvers. These control algorithms incorporate principles of feedback control, adjusting motor speeds or control surfaces to counteract disturbances and maintain stability. Additionally, autonomous drones employ sophisticated algorithms for tasks like way point navigation, obstacle detection and avoidance, and path planning (Lin and Peng). These algorithms analyze sensor data, map the environment, and make decisions based on predefined objectives or dynamically changing conditions. Machine learning and artificial intelligence techniques are also utilized to enhance the capabilities of drones, enabling tasks such as object recognition, tracking, and intelligent behavior. Software updates and firmware upgrades are regularly released to improve drone performance, add new features, and address security vulnerabilities. Software and control algorithms play a crucial role in optimizing the flight performance, safety, and intelligence of drones, enabling them to perform complex tasks in a variety of applications, including aerial mapping, surveillance, inspection, and scientific research.

Battery Charging

Battery charging is a critical aspect of drone operation, as it directly impacts flight time, performance, and overall reliability. Drones typically use rechargeable batteries, such as lithium-polymer (Li-Po) or lithium-ion (Li-ion); lithium-polymer (Li-Po) batteries provide a high energy density and lightweight design. Proper charging procedures are essential to ensure optimal battery performance and longevity. Charging protocols for drone batteries often involve balancing multiple cells within the battery pack to ensure uniform charging and prevent cell voltage imbalances. Dedicated battery chargers are used, equipped with safety features and charging algorithms that monitor and control the charging process. Charging rates must be within the recommended limits specified by the battery manufacturer to prevent overheating and potential damage. Fast-charging technologies have emerged, allowing for quicker recharge times, but caution must be exercised to avoid compromising battery lifespan. It is important to adhere to manufacturer guidelines, including using approved chargers and avoiding overcharging or discharging batteries excessively. Proper storage and handling of batteries are also crucial to prevent degradation and maintain their performance. Advances in battery technology and charging systems continue to improve charging efficiency and safety, enabling longer flight times and enhancing the overall reliability and usability of drone systems.

Regulatory Compliance

Regulatory compliance is a critical aspect of operating drones, as it ensures the safe and responsible use of unmanned aerial vehicles (UAVs) in accordance with legal and regulatory frameworks. Governments and aviation authorities around the world have established regulations to govern the operation of drones to address concerns regarding safety, privacy, and airspace management. These regulations typically cover aspects such as drone registration, pilot certification, flight restrictions, operational limitations, and privacy protection. Regulatory compliance requires drone operators to understand and adhere to these rules, which can vary from country to country. Compliance may involve obtaining permits or licenses, following specific flight procedures, maintaining a certain distance from people, buildings, and sensitive areas, and respecting the privacy of individuals. Additionally, compliance often entails adhering to airspace regulations, such as avoiding controlled airspace, airports, or other restricted areas. Drone operators are responsible for staying up-to-date with the latest regulations, as they are subject to change or may require updates as technology evolves. Compliance with regulations not only ensures safety and mitigates risks but also promotes responsible and ethical drone operations. It is essential for drone operators to be aware of and comply with the regulatory requirements applicable to their specific geographical location or the areas in which they intend to operate (Hodgson and Sella-Villa).

Security Challenges and Solutions

The emergence of swarm technology in the field of unmanned aerial vehicles (UAVs) has introduced a multitude of possibilities, but it has also brought about a range of security challenges. This section explores the various security challenges associated with swarm of drones and presents potential solutions to address these concerns. The use of drones in various applications, including surveillance, package delivery, and aerial photography, has raised concerns regarding security challenges. Some key security challenges associated with drones are as follows:

Unauthorized Access: Unauthorized access in a swarm of drones poses a significant security challenge. Swarms of drones are often used for collective tasks like surveillance, search and rescue operations, or distributed sensing. In such scenarios, it is crucial to ensure that only authorized individuals or systems have control over the entire swarm. However, unauthorized access can occur when malicious actors gain control over one or more drones within the swarm. This can be achieved by exploiting vulnerabilities in communication protocols, drone control systems, or even utilizing sophisticated techniques like drone-deception attacks. Once unauthorized access is established, attackers can manipulate the drone’s movements, alter its mission objectives, or even inject malicious payloads into the swarm. This can lead to serious consequences such as compromised data integrity, disruption of swarm behavior, or the use of the drones for malicious activities. To mitigate this risk, robust authentication and encryption mechanisms are essential. Implementing secure communication protocols, including cryptographic techniques, can help ensure that only authorized entities can control the swarm (Khan et al.). Additionally, continuous monitoring and anomaly detection algorithms can aid in detecting and responding to unauthorized access attempts in real-time. Adequate training and awareness programs should also be implemented to educate drone operators about the risks associated with unauthorized access and best practices for maintaining secure control over the swarm.

Data Breaches: Data breaches in a swarm of drones can have severe implications for privacy and security. Drones are equipped with various sensors and cameras that collect a vast amount of data during their operations. This data might include images, videos, location information, or even sensitive information if drones are used for surveillance or data-intensive tasks (Albalawi and Song). If proper security measures are not in place, these data sets can become vulnerable to breaches by malicious actors. Breaching the data in a swarm of drones can expose sensitive information, compromise individuals' privacy, or reveal sensitive locations and activities. The consequences of such breaches can range from identity theft, blackmail, or unauthorized surveillance to more significant issues like leaking classified information or critical infrastructure vulnerabilities. To mitigate data breach risks in a swarm of drones, encryption techniques should be applied to secure the storage and transmission of collected data. Implementing access controls and user authentication mechanisms can help prevent unauthorized access to stored data. Regular security audits, vulnerability assessments, and updates of the drone systems' software and firmware are also vital to ensure that any potential vulnerabilities are promptly identified and addressed. Moreover, data minimization practices should be followed, where only necessary data is collected and retained, reducing the potential impact of breaches. Additionally, educating drone operators about best practices for data protection and privacy can help raise awareness and ensure responsible data handling within swarms of drones.

Communication Interference: Drones within a swarm rely on wireless communication to exchange information, synchronize movements, and coordinate their collective tasks. However, this communication link is susceptible to various forms of interference. Malicious actors can exploit vulnerabilities in the communication protocols or deploy jamming devices to disrupt the signals between drones, leading to communication failures and loss of control. Communication interference can also result in drones receiving incorrect or manipulated instructions, causing them to deviate from their intended paths or disrupt the overall swarm behavior (Uddin et al.). Such interference can have severe consequences, including collisions between drones, failed mission objectives, or the compromise of data integrity. To mitigate communication interference risks, several countermeasures can be implemented. Encryption techniques should be employed to secure the communication channels, ensuring that transmitted data remains confidential and protected from unauthorized manipulation. Additionally, adopting frequency-hopping or spread-spectrum techniques can make it more challenging for attackers to disrupt or jam the communication signals. Monitoring for signal disruptions, employing signal strength analysis, and implementing resilient communication protocols can aid in detecting and mitigating interference attempts. Furthermore, establishing protocols for authentication and verification of commands exchanged between drones within the swarm can help detect and mitigate attempted communication interference by unauthorized entities. Regular testing, maintenance, and updates of the communication systems are essential to ensure their reliability and resilience against potential interference.

Malware and Cyber-attacks: The threat of malware and cyber-attacks in a swarm of drones presents a significant security challenge. Malicious actors can exploit vulnerabilities in the software and systems of drones to gain unauthorized access or inject malicious code, resulting in compromised operations and potential misuse of the swarm. Malware specifically designed for drones can hijack control, manipulate sensor data, or disrupt communication channels, leading to loss of control, compromised data integrity, and even physical damage. A successful cyber-attack on a swarm of drones could allow attackers to take over the entire swarm, potentially using it for malicious purposes or revealing sensitive information collected by the drones (Lykou et al.). To mitigate this risk, several security measures should be implemented. First, regular software updates and patches must be applied to drones to address any identified vulnerabilities. Implementing secure coding practices and adhering to cybersecurity best practices during the development of drone software can help prevent the introduction of vulnerabilities. Additionally, incorporating robust authentication and access control measures ensures that only authorized entities can interact with the swarm's systems. Monitoring systems for unusual behavior, network traffic analysis, and intrusion detection systems can aid in detecting and thwarting malware and cyber-attacks. Educating drone operators and users about potential threats and implementing training programs to raise awareness about cybersecurity practices are also crucial. Collaborative efforts among drone manufacturers, cybersecurity experts, and regulatory bodies are necessary to establish industry-wide standards for securing drones from malware and cyber-attacks.

Physical Threats: Drones operating within a swarm can be physically targeted or used as a delivery mechanism for harmful payloads. These threats can range from intentional attacks aimed at disabling or damaging the drones to using the swarm as a means to transport explosives, chemical agents, or other malicious payloads. Successful physical attacks on a swarm can result in the destruction of drones, disruption of swarm behavior, or the release of hazardous materials. Such threats present risks to infrastructure, public safety, and national security. Mitigating physical threats requires a multi-faceted approach. Implementing physical safeguards for drones, such as tamper-evident mechanisms, secure storage, or anti-tampering technologies, can help protect against unauthorized access or tampering. Regulatory measures and guidelines should be established to enforce responsible drone usage and deter malicious activities (Yahuza et al.). Employing geo-fencing and airspace management systems can prevent drones from flying in unauthorized areas or sensitive locations. Implementing countermeasures like anti-drone systems, such as frequency jammers or drone-capturing technologies, may be necessary to safeguard against external physical threats. Vigilance and training of drone operators, maintenance personnel, and security personnel play a crucial role in identifying and responding to potential physical threats. Collaboration among law enforcement agencies, security experts, and relevant stakeholders is vital to develop comprehensive strategies for mitigating physical threats in a swarm of drones and ensuring the safe and secure operation of this technology.

Airspace Intrusion: Airspace intrusion by a swarm of drones poses a significant security concern. With the increasing popularity and accessibility of drones, the risk of unauthorized drones entering restricted airspace and interfering with manned aircraft has grown. Intruding a swarm of drones into restricted zones or controlled airspace can disrupt flights, jeopardize aviation safety, and potentially lead to accidents or collisions. The consequences of such intrusions include grounding flights, delaying operations, and even the potential for catastrophic incidents. To mitigate airspace intrusion risks, several measures can be taken. Implementing geofencing and geo-location technologies can help prevent drones from entering restricted areas or sensitive locations. Authorities can enforce regulations and create no-fly zones that are communicated and enforced through geofencing technology. Drone identification systems using transponders or unique identification codes can aid in distinguishing authorized drones from intruders. Collaboration between drone manufacturers and relevant aviation authorities is crucial to ensure compliance with airspace regulations (Baig et al.). The development and implementation of integrated airspace management systems can provide real-time information about drone traffic and enable effective monitoring and response to potential intrusions. Additionally, countermeasures such as detection systems, pulse radar systems, and anti-drone technology can help identify and track unauthorized drones, allowing authorities to take swift action. Public education and awareness campaigns can also play a role in promoting responsible drone usage and safe airspace practices. Overall, a combination of regulatory frameworks, technological solutions, and public cooperation is necessary to prevent airspace intrusions by swarms of drones and maintain aviation safety.

Addressing these security challenges requires implementing robust security measures, including encryption of data transmission, authentication protocols, secure software and firmware, measures to detect and prevent physical tampering, and regulations defining safe and responsible drone usage. Regular security assessments and updates are also crucial in mitigating these challenges.

Anti-Drones

As the prevalence of swarm drones increases, so does the need for effective anti-drone techniques to mitigate potential security risks and ensure public safety. There are several advanced anti-drone techniques that can be employed to counter swarm attacks and mitigate potential security risks. These techniques involve various methods that focus on disrupting communication signals, disabling or destroying the drones in mid-air, physically capturing them, or detecting and tracking them.

Jamming Technology: Jamming technology is a widely employed technique used to counter swarm drones by disrupting their communication signals and rendering them ineffective. The effectiveness of this technique lies in the ability to disrupt the control link between the drone and its operator, essentially jamming the radio frequencies used for communication. Jamming devices emit high-power radio frequency signals on the same frequency bands used by the drones, creating interference that disrupts the signals between the drone and its operator. These devices can be fixed or mobile, allowing for flexibility in deployment. There are different types of jamming devices for countering drones. Frequency jamming devices emit signals across a wide range of frequencies that are commonly used for drone control, such as 2.4 GHz and 5.8 GHz (Šimon et al.). By saturating the entire frequency spectrum, these jammers effectively neutralize the control link, preventing the drone from receiving commands or transmitting data. Another type of jamming device is the protocol-specific jammer. These devices target specific communication protocols used by drones, allowing for more precise and efficient jamming. By identifying and jamming the specific protocol used by the drone, these devices can disrupt the communication while minimizing interference in the surrounding frequencies. Furthermore, jamming technology can be categorized as reactive or proactive. Reactive jammers detect the presence of a drone by analysing its radio frequency emissions and then initiate jamming. Proactive jammers continuously emit jamming signals, regardless of the presence of a drone, to maintain a constant safeguard against potential threats. Proactive jammers provide continuous protection but may encounter legal restrictions in certain jurisdictions.

It's important to note that the effectiveness of jamming technology can be influenced by various factors. These factors include the distance between the jamming device and the drone, the power output of the jammer, the frequency range it covers, and the resilience of the drone's communication system. Some advanced drones employ frequency-hopping or encryption techniques to mitigate the effects of jamming. It's worth mentioning that while jamming technology can be an effective countermeasure, it may also interfere with legitimate radio communications within the operating range of the jammer. Therefore, proper assessment, planning, and coordination with relevant authorities are essential to ensure that the jamming activities do not disrupt critical communication systems or violate legal regulations. Overall, jamming technology is an important anti-drone technique due to its ability to disrupt drone communication and control links. Deploying jamming devices can effectively neutralize the threat posed by swarm drones and ensure the safety and security of the surrounding area. However, careful consideration of legal and operational aspects is crucial for responsible and effective implementation.

High-powered Lasers: High-powered lasers have emerged as a powerful anti-drone technique to counter swarm attacks, enabling the disablement or destruction of drones in mid-air. These lasers work by targeting critical components of the drones, such as cameras, propellers, or on-board electronics, to disrupt their function. The use of high-powered lasers offers several advantages as an anti-drone technique. Firstly, lasers can be precise and accurate, allowing operators to focus the beam on specific areas of the drone. This precision allows for targeted disablement, minimizing collateral damage to the surrounding environment (Park et al.). Secondly, lasers provide a fast response time, enabling operators to quickly neutralize drones within seconds or even fractions of a second. This rapid response is crucial when dealing with swarm attacks that involve multiple drones operating in close proximity. Lastly, the scalability of laser systems makes them suitable for countering both small and large drone targets. To counter drones, high-powered laser systems emit intense beams of laser light at the drones' critical components. For instance, the laser can be directed at the drone's cameras to blind them, rendering the drone incapable of capturing clear images or video. Focusing the beam on the drone's propellers can cause them to melt or break, rendering the drone unable to maintain stable flight. By targeting the on-board electronics, lasers can disrupt or destroy crucial systems, effectively neutralizing the drone. The power output of the laser determines its effectiveness against drones. Higher-power lasers tend to be more effective in disabling or destroying drones. However, it's important to note that the use of high-powered lasers for anti-drone purposes may be subject to various legal and safety regulations. Operators must adhere to these regulations to ensure safe usage and prevent unintended negative consequences. Additionally, operators need to consider the range and beam divergence of the lasers. Range determines the maximum distance at which the laser can effectively disable or destroy a drone, while beam divergence affects the width and spread of the laser beam. Efficient anti-drone laser systems utilize beam directors, mirrors, or adaptive optics to focus and stabilize the laser beam, maintaining high accuracy and reducing the impact of atmospheric disturbances. While high-powered lasers offer an effective countermeasure against drones, there are factors to consider. A reliable power supply is essential; hence, they are excellent for defending ships. The weather conditions, including fog, rain, or dust, can affect the laser's performance and effectiveness. Additionally, the range and angle of attack can influence the success of laser-based anti-drone engagements. Given these considerations, high-powered lasers present a viable anti-drone technique for countering swarm attacks. With their precision, speed, and scalability, lasers offer a fast and accurate means of disabling or destroying drones, enhancing the security and safety of the surrounding area. However, adherence to legal regulations and responsible usage is imperative to avoid any unwanted repercussions.

Interceptor Drones: Interceptor drones have emerged as an effective anti-drone technique for countering swarm attacks. These specialized drones are designed to capture or neutralize rogue drones by physically intercepting them in mid-air. Interceptor drones are equipped with various mechanisms or tools to capture or disable the target drone. One common method involves using nets or physical barriers to entangle or immobilize the rogue drone. The interceptor drone deploys a net that is designed to envelop and ensnare the target, rendering it incapable of continuing its flight or mission (Yang and Quan). This approach is particularly useful when dealing with smaller drones that can be captured safely without causing damage or risk to the surrounding environment. Another method employed by interceptor drones is the use of physical barriers to collide with the rogue drone and force it to land or crash. These barriers can take the form of lightweight but sturdy structures that are deployed from the interceptor drone. By colliding with the rogue drone, the interceptor drone disrupts its flight path or disables its propulsion system, effectively neutralizing the threat. The interceptor drones are equipped with advanced sensors, cameras, and imaging systems to detect and track the target drones. These sensors enable the interceptor drone to accurately identify the target's position, speed, and trajectory. The information gathered is used to plan and execute intercept manoeuvres effectively. Intercepting swarm drones presents unique challenges compared to dealing with individual drones. Interceptor drones need to be agile, quick, and capable of operating in complex and dynamic environments with multiple targets. They must also have efficient communication systems to coordinate with other interceptor drones or ground-based control stations, ensuring synchronized actions to counter the swarm.

Additionally, the autonomy of interceptor drones is critical. These drones should possess advanced artificial intelligence algorithms to make decisions on interception strategies in real-time. This autonomy enables the interceptor drones to adapt to changing situations and successfully engage multiple targets within the swarm. Intercepting drones also requires proper training and skilled operators. Human supervision and intervention may be necessary in certain scenarios to ensure the safety of the operation and prevent unintended consequences.

Intercepting drones with other drones offers a mobile and flexible approach, allowing the interception to take place at various altitudes and locations. Interceptor drones can be deployed from ground stations, aircraft carriers, or even launched mid-flight from larger aircraft. The development of interceptor drones as an anti-drone technique introduces an additional layer of defence against swarm attacks. By physically capturing or neutralizing rogue drones, interceptor drones provide a means to safely remove threats from the airspace without relying solely on electronic or jamming methods. When combined with other anti-drone technologies and systems, interceptor drones enhance the overall effectiveness and resilience of anti-drone defences.

Radar, Sensor Systems & EM: Radar systems utilize electromagnetic waves, such as radio waves or microwaves, to detect and track objects in the airspace. They work by emitting a signal and then analysing the reflected signal when it bounces back off the object. In the context of anti-drone techniques, -radar systems play a crucial role in detecting and tracking unmanned aerial vehicles (UAVs), or drones, that may pose a security threat.

There are several types of radar systems used for anti-drone purposes:

Surveillance Radar

Surveillance radars have a wide-angle coverage and are capable of detecting drones at long distances. They continuously scan the airspace, creating a comprehensive situational awareness of the drone activities in the monitored area (Yun et al.). Surveillance radars can distinguish between drones and other flying objects like birds or airplanes, reducing the chances of false alarms.

Tracking Radar

Once a drone is detected by a surveillance radar, the tracking radar takes over to precisely track and monitor the drone's position, speed, altitude, and direction of travel (Guvenc et al.). Tracking radars employ advanced algorithms and signal processing techniques to effectively follow the drone's movement, even in challenging environments with dense foliage or urban clutter.

Ground-Based Radar Systems

Ground-based radar systems are stationary installations that are commonly deployed around critical infrastructure, airports, or other sensitive areas to provide continuous coverage against unauthorized drone intrusions (Casagli et al.). These systems often work in concert, enabling multiple radar installations to merge the detected drone tracks and provide a more accurate representation of the threat scenario.

In addition to radar systems, sensor technologies also play a crucial role in anti-drone techniques. Here are some sensor systems commonly used:

Acoustic Sensors

Acoustic sensors detect drones by listening for the unique sound signatures generated by their propellers or engines (Miller et al.). By analyzing the frequency and intensity of the sounds, sophisticated algorithms can differentiate between different drone models and even classify the drone's flight intentions.

Electro-Optical (EO) Sensors

EO sensors use cameras and infrared technology to provide visual detection and tracking of drones. These sensors can identify and track drones based on their heat signatures and help operators visually recognize and classify the threat from a safe distance (Elsayed et al.). EO sensors can be used during both day and night, making them effective for 24/7 surveillance.

Radio Frequency (RF) Sensors

RF sensors monitor the electromagnetic spectrum to detect and identify the radio signals emitted by drones and their remote controllers. These sensors can help determine the presence of unauthorized drone activity even before the drone physically enters the protected area (Al-Emadi and Al-Senaid). RF sensors are especially useful in countering autonomous and swarm drone attacks, where the drones communicate with each other to coordinate their actions.

By integrating radar and sensor systems into a comprehensive anti-drone defence strategy, organizations can enhance their capabilities to detect, track, classify, and mitigate potential drone threats. These technologies provide early warning, situational awareness, and actionable intelligence for timely responses and effective countermeasures.

Pulsed Electro-magnetic (EM) radiation can also be used to damage and disrupt the operation of drones. Pulsed radar systems, magnetrons and gyrotrons can be used to induce excessive currents in integrated circuit electronic systems built into the drone hardware, this will cause the drone to fail.

Drone-Defeat Systems: Drone-defeat systems are designed to actively counter and neutralize rogue or unauthorized UAVs (Unmanned Aerial Vehicles) that pose a threat. These systems employ various technologies to disable, disrupt, or take control of the unauthorized drone, ensuring the protection of critical infrastructure, public safety, and sensitive areas (Conley). Here are some key techniques used in drone-defeat systems:

GPS Spoofing: Many UAVs rely on GPS (Global Positioning System) for precise navigation and positioning. Drone-defeat systems can employ GPS spoofing to deceive the drone's onboard GPS receiver by providing false positioning information. By manipulating the GPS signals, the system can misdirect the drone, making it lose its way or causing it to land or return to its point of origin.

Kinetic Systems: For scenarios that require more immediate and direct action, kinetic systems utilize physical force to physically disable or destroy the drone. These systems can include anti-drone projectiles, net-based solutions, or even trained birds of prey that are trained to intercept and capture the drone safely (Castrillo et al.). Kinetic systems are often used in high-security areas where the risk of drone threats is significant.

Directed Energy Weapons: Directed energy weapons, such as gyrotrons or radio frequency-based systems, are advanced technologies used to disrupt drones. These systems use intense beams of energy to disable the drone by overheating or damaging its components, like the batteries or micro-electronic systems. Directed energy weapons provide a precise, non-lethal alternative to neutralize drones, allowing for immediate disruption without causing collateral damage.

Drone Capture Systems: Another approach is to physically capture the hostile drone using specially designed devices like nets or drones equipped with nets. When a threat is detected, these systems launch a net towards the drone to entangle it and subsequently bring it down safely. Once captured, the drone can be analyzed or disposed of appropriately.

It is important to note that the use of drone-defeat systems should comply with local regulations and legal frameworks. The priority is to protect against potential threats while ensuring the safety of the surrounding environment and minimizing the impact on innocent by standers. Overall, drone-defeat systems provide active countermeasures against unauthorized drone activity, mitigating potential risks and protecting critical assets. These technologically advanced systems work in tandem with detection systems and radar/sensor systems to create a comprehensive anti-drone defence strategy.

Legislation and Regulations: Legislation and regulations play a crucial role in implementing effective anti-drone techniques and ensuring the safe and responsible use of unmanned aerial vehicles (UAVs). Government bodies across the world have recognized the need for rules and regulations to mitigate potential risks associated with drone operations (Tsiamis et al.). Here are some key aspects related to legislation and regulations for anti-drone techniques:

Registration and Licensing: Many countries require drone operators to register their drones with the appropriate regulatory authorities. This process helps establish accountability and enables authorities to identify the owner or operator in case of any violations or incidents. Additionally, some jurisdictions may require operators to obtain licenses or permits to operate drones in certain locations or under specific circumstances, such as commercial use or beyond visual line of sight operations.

Operational Restrictions: Governments enforce operational restrictions to prevent misuse and enhance safety. These can include limitations on flight altitude, distance from airports/helipads, proximity to sensitive areas (such as prisons, government buildings, or critical infrastructure), and flight over crowds or populated areas. Regulations may also define "no-fly zones" where drone operations are entirely prohibited or require specific authorization for flights in designated airspace.

Remote Identification: Remote identification regulations aim to ensure that drones can be identified by law enforcement and aviation authorities while in flight. This can help deter malicious or unauthorized activities and enable authorities to track and take appropriate action against non-compliant operations. Remote identification may involve visible markings, unique identification codes, or broadcasting information such as the operator's contact details or flight information.

Anti-Drone Systems: Legislation may define the permitted use of anti-drone systems and technologies by authorized entities, such as law enforcement or critical infrastructure operators. This includes rules regarding jamming, GPS disruption, directed energy weapons, and other counter-drone technologies to prevent their misuse or interference with legitimate drone operations. Governments often regulate the use of anti-drone systems to ensure the safety of airspace and protect privacy rights.

Privacy and Data Protection: As drones can capture and transmit images or collect personal data, privacy regulations are essential. Governments impose restrictions on the use of drones for surveillance purposes and require operators to comply with data protection laws. These regulations typically govern the collection, storage, and sharing of data obtained during drone operations, ensuring that privacy rights are respected.

Enforcement and Penalties: Legislation establishes penalties and enforcement mechanisms to deter non-compliance with drone regulations. This may include fines, suspension or revocation of licenses, and in severe cases, criminal charges. The presence of suitable enforcement mechanisms encourages compliance and helps mitigate potential risks associated with irresponsible drone use.

Legislation and regulations are continuously evolving to keep pace with the rapid advancements in drone technology. Governments collaborate with industry stakeholders, aviation authorities, and privacy advocates to strike a balance between promoting innovation and ensuring safety. By having comprehensive, well-enforced regulations, authorities can effectively mitigate risks associated with drones and maintain the safe integration of drones into the airspace ecosystem.

To effectively counter swarm drone attacks, a combination of these techniques can be implemented in an integrated defense system. This multi-layered approach ensures a higher probability of success in neutralizing the threats posed by swarm drones while maintaining the safety and security of the surrounding environment.

Future Challenges and Technology

The future of drone technology encompasses a myriad of challenges that will shape our world in unforeseen ways, low-cost drones have become a disruptive technology that is reshaping the balance of military power. One of the foremost challenges lies in effectively coordinating and managing swarms of drones. As the number of drones in our skies increases, ensuring their safe and coordinated operation becomes paramount. Additionally, technological advancements are necessary to improve their battery life, range, and payload capacity, allowing them to carry out more complex and longer missions. The development of robust communication networks and advanced artificial intelligence algorithms will be vital in enabling drones to autonomously navigate in complex environments, avoid collisions, and adapt to unforeseen situations. Furthermore, ensuring the security and privacy of individuals and organizations becomes increasingly crucial in a world filled with an extensive deployment of drones. Overcoming these challenges will not only redefine the ways in which drones operate, but also open up endless possibilities for their applications in industries like logistics, surveillance, emergency response, and even urban air transportation. With continued research and innovation, the future of swarm drones holds great promise, transforming our world in unprecedented ways.

Conclusion

In conclusion, the use of unmanned aerial vehicles (UAVs) or drones has experienced significant growth in recent years across various sectors. The availability of highly flexible drones in different types, sizes, and capabilities has revolutionized industries such as military, surveillance, agriculture, and package delivery. The exponential increase in the number of drones highlights their importance and potential impact on search and rescue, infrastructure inspection, and environmental monitoring. Despite their advantages, drones still face certain limitations, such as limited flight time, battery endurance, and weight. To address these challenges, the concept of using swarm technology, inspired by collective animal behavior, has emerged. Swarm technology allows for the coordination and communication of multiple autonomous UAVs to perform tasks cooperatively. This approach offers advantages such as increased reliability, flexibility, and efficiency, even in the face of failures or damage to individual drones. The potential applications of drone swarms span various industries, including military, surveillance, agriculture, search and rescue, and disaster response. Research has shown that swarm technology can improve precision and efficiency in areas such as crop monitoring, construction site inspection, and emergency response. However, the development of swarm technology also raises concerns about privacy, security, and the potential for misuse.

This review paper has explored the potential of swarm technology, its applications, and the challenges associated with its implementation. It has discussed the current research studies and developments in the field of drone swarms, as well as anti-drone techniques to ensure their safe use. The analysis of current research and development has identified areas where further innovation and research can contribute to the growth and advancement of this technology. In conclusion, the use of drone swarms holds great promise for addressing the limitations of individual drones and achieving more efficient and robust operations. However, it is essential to address concerns related to privacy, security, and potential misuse. Further research and innovation in swarm technology, along with the development of effective anti-drone techniques, will play a crucial role in realizing the full potential of drones and ensuring their safe and responsible utilization in various sectors.

References

Ahn, Hyohoon, et al. “Real-Time Drone Formation Control for Group Display.” *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication,* 2019, pp. 778-85.

Al-Emadi, Sara, and Felwa Al-Senaid. “Drone Detection Approach Based on Radio-Frequency using Convolutional Neural Network.” *IEEE International Conference on Informatics, IoT, and Enabling Technologies*, 2020, pp. 29-34.

Albalawi, Maisa, and Houbing Song. “Data Security and Privacy Issues in Swarms of Drones.” *Integrated Communications, Navigation and Surveillance Conference,* 2019.

Alsamhi, S. H., et al. “Survey on Artificial Intelligence based Techniques for Emerging Robotic Communication.” *Telecommunication Systems*, vol. 72, no. 3, 2019, pp. 483-503.

Atkins, Ella, et al. *Unmanned Aircraft Systems*. John Wiley, 2017.

Azeta, J., et al. “An Experimental Evaluation of LTA on the Performance of a Drone.” *Procedia Manufacturing*, vol. 35, 2019.

Baballe, Muhammad Abubakar, et al. “The Unmanned Aerial Vehicle (UAV): Its Impact and Challenges.” *Global Journal of Research in Engineering & Computer Sciences*, vol. 2, no. 3, 2022, pp. 35-39.

Baig, Zubair, et al. “Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning.” *Future Internet*, vol. 14, no. 7, 2022.

Barchyn, Thomas E., et al. “Plume Detection Modeling of a Drone-Based Natural Gas Leak Detection System.” *Elementa: Science of the Anthropocene*, vol. 7, 2019.

Boon, Marinus, et al. “Comparison of a Fixed-Wing and Multi-Rotor UAV for Environmental Mapping Applications: A Case Study.” *International Conference on Unmanned Aerial Vehicles in Geomatics*, 2017, pp. 47-54.

Brown, Shannon T., et al. “The High-Altitude MMIC Sounding Radiometer for the Global Hawk Unmanned Aerial Vehicle: Instrument Description and Performance.” *IEEE Transactions on Geoscience and Remote Sensing*, vol. 49, no. 9, 2011.

Casagli, Nicola, et al. “Spaceborne, UAV and Ground-Based Remote Sensing Techniques for Landslide Mapping, Monitoring and Early Warning.” *Geoenvironmental Disasters*, vol. 4, no. 1, 2017.

Castrillo, Vittorio Ugo, et al. “A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones.” *Drones*, vol. 6, no. 3, 2022.

Çetin, Ender, et al. "Counter a Drone in a Complex Neighborhood Area by Deep Reinforcement Learning." *Sensors*, vol. 20, no. 8, 2020.

Chriki, Amira, et al. "Centralized Cognitive Radio Based Frequency Allocation for UAVs Communication." *International Wireless Communications & Mobile Computing Conference*, 2019.

Conley, Keith. *Involuntary Signal-Based Grounding of Civilian Unmanned Aerial Systems (UAS) in Civilian Airspace.* The University of Southern Mississippi, 2019.

Cook, Kendra L. B. "The Silent Force Multiplier: The History and Role of UAVs in Warfare." *IEEE Aerospace Conference*, 2007.

Dalamagkidis, Konstantinos, et al. *On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations*. Springer, 2012.

Department of Defense, United States. *Global Positioning System Standard Positioning Service Performance Standard*. 2008.

DeVore, Marc R. "Reluctant Innovators? Inter-Organizational Conflict and the U.S.A.'s Route to Becoming a Drone Power." *Small Wars & Insurgencies*, vol. 31, no. 4, 2020, pp. 701-29.

Dudczyk, Janusz, et al. "Multi-Sensory Data Fusion in Terms of UAV Detection in 3D Space." *Sensors*, vol. 22, no. 12, 2022.

Elmeseiry, Nourhan, et al. "A Detailed Survey and Future Directions of Unmanned Aerial Vehicles (UAVs) with Potential Applications." *Aerospace*, vol. 8, no. 12, 2021.

Elsayed, Mohammed, et al. "Review on Real-Time Drone Detection based on Visual Band Electro-Optical (EO) Sensor." *International Conference on Intelligent Computing and Information Systems*, 2021, pp. 57-65.

Ezuma, Martins, et al. "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference." *IEEE Open Journal of the Communications Society*, 2020, pp. 60-76.

Fahim, Muhammad, and Alberto Sillitti. "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review." *IEEE Access*, vol. 7, 2019.

Federal Aviation Administration, United States. *FAA Aerospace Forecast: Fiscal Years 2018-2038*. 2018.

Gahír, Jakub, and Andrej Novák. *Analysis of Satellite Navigation Systems Usable in General Aviation*. 2022.

Ghazali, Mohamad H. M., et al. "Drone Implementation in Precision Agriculture - A Survey." *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 4, 2022, pp. 67-77.

Goudarzi, Hirad, and Arthur Richards. "Semi-Autonomous Drone Control with Safety Analysis." *Drone Systems and Applications*, vol. 11, 2023.

Greenwood, William W., et al. "Applications of UAVs in Civil Infrastructure." *Journal of Infrastructure Systems*, vol. 25, no. 2, 2019.

Gutfleisch, Oliver, et al. "Magnetic Materials and Devices for the 21st Century: Stronger, Lighter, and More Energy Efficient." *Advanced Materials*, vol. 23, no. 7, 2011, pp. 821-42.

Guvenc, Ismail, et al. "Detection, Tracking, and Interdiction for Amateur Drones." *IEEE Communications Magazine*, vol. 56, no. 4, 2018, pp. 75-81.

Hartmann, Kim, and Christoph Steup. "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment." *International Conference on Cyber Conflict*, 2013.

Hartnett, Michael. *Performance Assessment of Navigation Using Carrier Doppler Measurements from Multiple LEO Constellations*. Air University, 2022.

Hodgson, Michael E., and David Sella-Villa. "State-Level Statutes Governing Unmanned Aerial Vehicle Use in Academic Research in the United States." *International Journal of Remote Sensing*, vol. 42, no. 14, 2021.

Integrity and Continuity Analysis from GPS Name. Nottingham Scientific Limited, https://www.caa.co.uk/Documents/Download/1851/bbb482d8-8881-4889-9d31-b445ae6f6016/34

Jacobsson, Martin, et al. "A Drone-mounted Depth Camera-based Motion Capture System for Sports Performance Analysis." *International Conference on Human-Computer Interaction*, 2023, pp. 489-503.

Kangunde, Vemema. "A Review on Drones Controlled in Real-Time." *International Journal of Dynamics and Control*, 2021.

Kassas, Zahar M., et al. "Navigation with Multi-Constellation LEO Satellite Signals of Opportunity: Starlink, OneWeb, Orbcomm, and Iridium." *IEEE/ION Position, Location and Navigation Symposium,* 2023, pp. 338-343.

Khan, Muhammad Asif, et al. "On the Detection of Unauthorized Drones-Techniques and Future Perspectives: A Review." *IEEE Sensors Journal*, vol. 22, no. 12, 2022.

Kornbluh, Roy, et al. "Application of Electrolaminates for the Development of Biomimetic Morphing Unmanned Aerial Vehicles." *Journal of Composite Materials*, vol. 57, no. 4, 2023, pp. 759-69.

Kouzoupis, Dimitris, et al. "Recent Advances in Quadratic Programming Algorithms for Nonlinear Model Predictive Control." *Vietnam Journal of Mathematics*, vol. 46, no. 4, 2018, pp. 863-82.

Kozhaya, Sharbel. "Multi-Constellation Blind Beacon Estimation, Doppler Tracking, and Opportunistic Positioning with OneWeb, Starlink, Iridium NEXT, and Orbcomm LEO Satellites." *IEEE/ION Position, Location and Navigation Symposium,* 2023.

Kuzlu, Murat, et al. "Communication Network Requirements for Major Smart Grid Applications in HAN, NAN and WAN." *Computer Networks*, vol. 67, 2014, pp. 74-88.

Lin, Huei-Yung, and Xing-Zhong Peng. "Autonomous Quadrotor Navigation with Vision Based Obstacle Avoidance and Path Planning." *IEEE Access*, vol. 9, 2021.

Lykou, Georgia, et al. "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies." *Sensors*, vol. 20, no. 12, 2020.

Maluleke, Witness. "The Use of Drones in Policing Stock Theft by the Selected Rural South African Livestock Farmers Introduction and Problem Formulation." *Journal of the Social Sciences*, vol. 48, no. 4, 2020, pp. 634-52.

Matosevic, M., et al. "A Comparison of Accuracy Using a GPS and a Low-Cost DGPS." *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 5, 2006.

Mayer, Sven, et al. "Drones for Search and Rescue." 1st International Workshop on Human-Drone Interaction, 2019.

Merheb, Abdel-Razzak, et al. "Emergency Control of AR Drone Quadrotor UAV Suffering a Total Loss of One Rotor." *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 2, 2017, pp. 961-71.

Miller, Alexander, et al. "Navigation of Underwater Drones and Integration of Acoustic Sensing with Onboard Inertial Navigation System." *Drones*, vol. 5, no. 3, 2021.

Morales, Alejandro, et al. "A Multispectral Camera Development: From the Prototype Assembly until its Use in a UAV System." *Sensors*, vol. 20, no. 21, 2020.

Naethe, Paul, et al. "Calibration and Validation from Ground to Airborne and Satellite Level: Joint Application of Time-Synchronous Field Spectroscopy, Drone, Aircraft and Sentinel-2 Imaging." *Journal of Photogrammetry, Remote Sensing and Geoinformation Science,* vol. 91, 2023, pp. 43-58.

Newcome, Laurence R. *Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles*. American Institute of Aeronautics and Astronautics, 2004.

Onososen, A. O., et al. "Impediments to Construction Site Digitalisation Using Unmanned Aerial Vehicles (UAVs)." *Drones*, vol. 7, no. 1, 2023.

Park, Seongjoon, et al. "Survey on Anti-Drone Systems: Components, Designs, and Challenges." *IEEE Access*, vol. 9, 2021.

Petso, Tinao, et al. "Review on Methods used for Wildlife Species and Individual Identification." *European Journal of Wildlife Research*, vol. 68, no. 1, 2021.

Qamar, Suleman, et al. “Autonomous Drone Swarm Navigation and Multitarget Tracking with Island Policy-Based Optimization Framework.” *IEEE Access*, vol. 10, 2022.

Qu, Wenqiu, et al. “Preliminary Concept of Urban Air Mobility Traffic Rules.” *Drones*, vol. 7, no. 1, 2023.

Raj, E. Fantin Irudaya, et al. “Precision Farming in Modern Agriculture.” *Smart Agriculture Automation using Advanced Technologies*, 2021, pp. 61-87.

Rodrigues, Thiago A., et al. “In-Flight Positional and Energy Use Data Set of a DJI Matrice 100 Quadcopter for Small Package Delivery.” *Science Data*, vol. 8, no. 1, 2021.

Sanz-Martos, Sebastian, et al. “Drone Applications for Emergency and Urgent Care: A Systematic Review.” *Prehospital and Disaster Medicine*, vol. 37, no. 4, 2022, pp. 502-08.

Sharma, Abhishek, et al. “Communication and Networking Technologies for UAVs: A Survey.” *TechRxiv*, 2020.

Simon, O., et al. “Commercial UAV Jamming Possibilities.” *International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2022.

Singireddy, Shiva Ram Reddy and Tugurl U. Daim. “Technology Roadmap: Drone Delivery – Amazon Prime Air.” *Innovation, Technology, and Knowledge Management*, 2018.

Sliwinski, Jacob, et al. “Hybrid-Electric Propulsion Integration in Unmanned Aircraft.” *Energy*, vol. 140, 2017.

Sun, Chenfan, et al. “Object Detection from the Video Taken by Drone via Convolutional Neural Networks.” *Mathematical Problems in Engineering*, 2020.

Tkáč, Matus, and Peter Mésároš. “Utilizing Drone Technology in the Civil Engineering.” *Journal of Civil Engineering*, vol. 14, no. 1, 2019, pp. 27-37.

Tony, Lima Agnel, et al. “Lane Geometry, Compliance Levels, and Adaptive Geo-fencing in CORRIDRONE Architecture for Urban Mobility.” *International Conference on Unmanned Aircraft Systems*, 2021.

Townsend, Ashleigh, et al. “A Comprehensive Review of Energy Sources for Unmanned Aerial Vehicles, their Shortfalls and Opportunities for Improvements.” *Heliyon*, vol. 6, no. 11, 2020.

Tsiamis, Nikolaso, et al. “A Comparative Analysis of the Legislation Evolution for Drone Use in OECD Countries.” *Drones*, vol. 3, no. 4, 2019.

Tupitsyn, Nikolay. “Estimation of the Required Dimension of Net to Capture Drone.” *Electronics and Control Systems*, vol. 1, 2021, pp. 94-99.

Uddin, Zahoor, et al. “Amateur Drones Detection: A Machine Learning Approach Utilizing the Acoustic Signals in the Presence of Strong Interference.” *Computer Communications*, vol. 154, 2020, pp. 236-45.

Usman, Muhammad, et al. “Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography.” *Electronics*, vol. 11, no. 7, 2022.

Venugopal, Hridya. “Development of Control Systems that Operate Independently without Human Intervention.” *i-manager’s Journal on Instrumentation & Control Engineering*, vol. 10, no. 2, 2022, pp. 25-35.

Wang, Hui-Ming, et al. “Secrecy and Covert Communications against UAV Surveillance via Multi-Hop Networks.” vol. 68, no. 1, 2020, pp. 389-401.

Wood, Robert, et al. “Flight of the Robobees.” *Scientific American*, 2013, pp. 61-65.

Yahuza, Muktar, et al. “Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges.” *IEEE Access*, vol. 9, 2021.

Yang, Kun, and Quan. “An Autonomous Intercept Drone with Image-based Visual Servo.” *IEEE International Conference on Robotics and Automation*, 2020.

Yang, Xin. *Low Earth Orbit (LEO) Mega Constellations - Satellite and Terrestrial Integrated Communication Networks*. University of Surrey, 2018.

Yang, Xingbang, and Xuan Pei. “Hybrid System for Powering Unmanned Aerial Vehicles: Demonstration and Study Cases.” *Hybrid*

Technologies for Power Generation, 2022, pp. 439-73.

Yang, YunaXi, et al. "Preliminary Assessment of the Navigation and Positioning Performance of BeiDou Regional Navigation Satellite System." *Science China Earth Sciences*, vol. 57, 2013, pp. 144-52.

Yayla, Gokay, et al. "Accuracy Benchmark of Galileo and EGNOS for Inland Waterways." *International Ship Control Systems Symposium*, 2020.

Yağdereli, Eray, et al. "A Study on Cyber-Security of Autonomous and Unmanned Vehicles." *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 12, no. 4, 2015.

Yun, Joongsup, et al. "Parametric Investigation on Simulated Staring FMCW Radar for Anti-Drone Swarms." *IEEE Radar Conference*, 2020.

Zaloga, Steven J. *Unmanned Aerial Vehicles: Robotic Air Warfare 1917–2007*. Bloomsbury Publishing, 2011.

Author Details

Ahad Alotaibi, *Department of Engineering and Design, School of Engineering and Informatics, University of Sussex, United Kingdom,* ***Email ID****: aa2758@sussex.ac.uk*

Chris Chatwin, *Department of Engineering and Design, School of Engineering and Informatics, University of Sussex, United Kingdom*

Phil Birch, *Department of Engineering and Design, School of Engineering and Informatics, University of Sussex, United Kingdom*