Security Threats of Unmanned Aerial Vehicles

Ashok Vajravelu, N. Ashok Kumar, Swagata Sarkar, and Sheshang Degadwala

Abstract Civilian drones and military drones are the two primary classifications of unmanned aerial vehicles (UAVs), which are commonly known as drones. Drones are used for a wide range of tasks and are also referred to by their other name, unmanned aerial vehicles. The deployment of unmanned aerial vehicles for a broad range of tasks has shown phenomenal expansion over the course of the previous decade. Recently, a new generation of small unmanned aerial vehicles has been available for purchase, highlighting the growing danger that these devices present. This article discusses the potential threats to national security that unmanned aerial vehicles pose, including but not limited to the following: terrorist attacks; unauthorized surveillance and reconnaissance; smuggling; electronic eavesdropping; mid-air collisions; and electronic eavesdropping. It also analyzes the various forms of UAV incursions according to the objective for which they were carried out and the amount of expertise possessed by the operator. In the communication frameworks of the drones, several cryptographic approaches have been included. These techniques include key agreement, authentication, encryption and decryption, integrity, blockchain, and digital signatures. Civilian drones and military drones are the two types that may be differentiated based on the functions that they are designed to do.

Keywords Unmanned aerial vehicle · Security threats · Smart drones · Cybersecurity · Data privacy

A. Vajravelu
Department of Electronics, Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia

N. Ashok Kumar
Department of ECE, Mohan Babu University, Erstwhile of Sree Vidaynikethan Engineering College, Tirupati, Andhra Pradesh 517102, India

S. Sarkar (✉)
Artificial Intelligence and Data Science Department, Sri Sairam Engineering College, West Tambaram, Chennai, India
e-mail: swagata.b.sarkar@gmail.com

S. Degadwala
Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_5

1 Introduction

In this post-atomic age, the majority of applications for drone technology may be found in the military and other defensive settings. The use of drone technology in military settings is seeing tremendous expansion. These little gadgets are now hovering around 200 feet above the earth in the air. This height range varies from one gadget to the next as well as depending on the intended use. This range may be measured in feet, meters, or kilometers, depending on your preference. The amount of time that these intelligent gadgets can remain airborne varies, too, depending on the device [1, 2]. Table 1 contains a discussion of the differences in frequency as well as their attributes.

2 Security, Protection, and Secrecy Apprehendions of Drones

Drone technology provides a variety of advantages and benefits to humans. It is utilized in everyday operations, the military, and weather monitoring, among other things. Nevertheless, despite their benefits, there are a number of privacy and safety risks linked with them. Breach of privacy and security should be dealt with in the appropriate manner. When using drones for recording or picture capture, care must be taken to protect the privacy and confidentiality of the subjects being filmed or photographed [15]. There are a number of studies that have been conducted, all of which evaluate and talk about the risks that are linked with using drones for sanctuary and risk assessment. Message-passing networks must meet the requirements for confidentiality, dependability, obtainability, verification, and non-denial

Table 1 Variations in frequency and their characteristics

Parameters	2 GHz	5 GHz
Frequency band	Low speed	High speed
Cost	Cheap	Costly
Range	Extended range	Undersized range
Effect of noise	Noisy	Less noisy
interference	Prone to interference	Less prone to interference
Physical barriers	Overcome physical barriers	Unable to overcome physical barriers
Performances	Disturb Wi-Fi speed	Don't disturb Wi-Fi speed

of possessions. This is something that AAA's procedures and progressions can help with:

- Authorization can be obtained by granting access to the drone or UAV's control unit.
- Verification can be achieved through the use of multi-level authentication with a knowledge-specific key, identity verification, and biometric verification.

Drones provide a number of security risks, which may take the form of either physical or cyber assaults. It is mandatory to place restrictions on the usage of drones in public places and on private property. The inappropriate usage of drones is also becoming more common by the day. This use further complicates matters for the general populace and civilians. When flying their drones in restricted regions, owners of drones usually control them over Bluetooth or Wi-Fi channels. This might result in a loss of financial resources. Hacking Wi-Fi networks and Bluetooth signals may be accomplished with the use of drones. A compromise of this magnitude raises a great number of privacy and security concerns among individuals. The most significant dangers to drones are shown in Fig. 1, which may be seen below. There is also discussion of potential countermeasures to these dangers. The following is a rundown of some of the most pressing and impending security concerns.

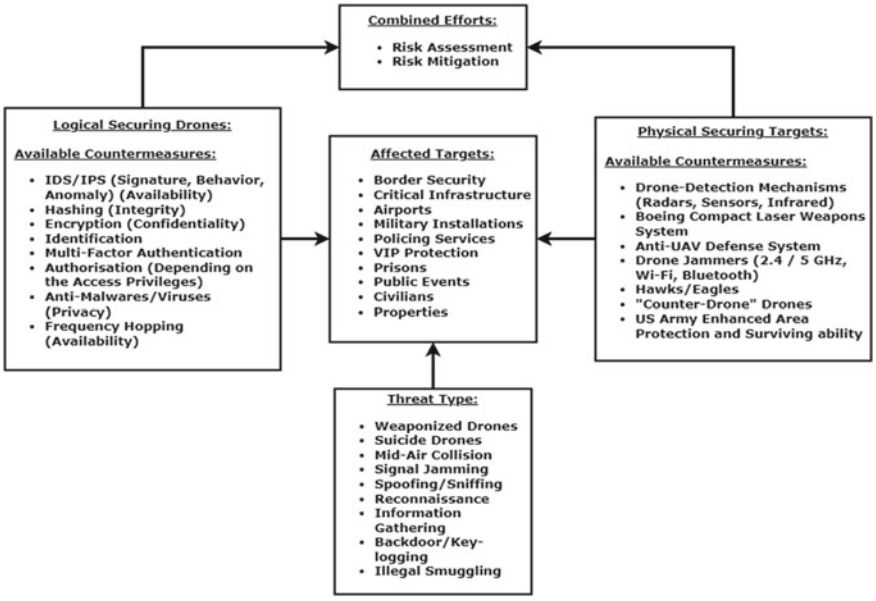

Fig. 1 Drone threats taxonomy

3 Existing Approaches for Drone Cyber-Security Methods

The following are the many sorts of major security approaches that are used to ensure drone cybersecurity. This categorization takes into account the goals and intentions of the attacker. In the following paragraphs, we will cover the various methods now in use to address drone safety concerns.

A. ***Drone Network Security***

When drones are in the air and communicating with a base station, there are several opportunities for security breaches. In order to find a solution to these kinds of issues, researchers came up with a system of intrusion detection that can identify illicit activity. The techniques of intrusion detection monitor network traffic in order to identify suspicious activity. There are many different ways for detecting intrusions, and these approaches are used to investigate abnormalities. These approaches include methodologies such as rule-based detection, signature-based detection, and anomaly-based detection.

B. ***Drone Information Safety***

The data sent by drones has to be converted into packets in order to prevent the communication network from being overloaded. This kind of packing makes it possible to communicate in a reasonably risk-free manner. Nevertheless, such packaging is responsible for a wide variety of issues. One research article delves into the topic of cipher security, which safeguards data from prying eyes.

C. ***Scientific Resolutions***

The drone industry makes use of scientific methods, one of which involves analyzing the traffic on a network through the application of forensic monitoring techniques. This monitoring enables the identification as well as the detection of illegal access and capture.

4 Security Threats to Drones

The size of the drone, the purpose it serves, and the controlling system all factor into the complexity of its security. Wi-Fi, namely the IEEE 802.11 communication protocol, is used in many instances to operate the drone. Wi-Fi networks, along with their respective ground stations, form the foundation for the majority of communication systems built inside drones. These networks are susceptible to having their security compromised. Due to the lack of adequate encryption on their circuits, professional drones run the risk of being stolen. The man-in-the-middle attack is the second method of network hijacking that has been identified by the research community. These assaults are only feasible up to a distance of two kilometers. The obstacle that has shown itself so far is that there is no encryption, which makes it possible for humans to take control of drones. The Internet of Drones is a relatively new development in the field of drone safety (IoD). The idea is widely used in both

the military and commercial sectors of drones. The Internet of Things has a broad variety of uses, including both civilian and military drones at the same time. The fundamental issue with drones is that they are designed without taking into account any kind of safety features. There were significant risks to users' personal information and privacy associated with the design of drone technology. The primary challenges confronting the field of Internet of Things (IoT) security have been identified as privacy leakage, data confidentiality, data protection, data flexibility, data accessibility, and data encryption and decryption procedures.

Researchers from a wide variety of fields have conducted a large number of studies over the last several years, during which time they have uncovered a wide variety of dangers to data privacy and data security. The discovered forms of cyberattacks may be broken down into four categories: compromised component attacks, jammers attacks, compromised protocol-based attacks, and jammers attacks. Table 2 provides an overview of the potential dangers that have been recognized as falling under each of these four categories of cyberattacks, as discovered by the literature research. As can be seen in Table 2, the bulk of the work that has been done on the cybersecurity and data privacy of industrial drones consists of little more than the identification of potential dangers. There is no known answer to the problems posed by these dangers. An attempt was made to encrypt data sent from a drone to a base station using a Key Encryption technique for secure packet delivery [18]. This was done in the hopes of preventing unauthorized access to the data. Over the last several years, the scientific community has been more interested in the use of miniature drones. These drones are extremely popular not only due to the fact that they have a shorter wingspan, but also due to the fact that they are lightweight. These tiny drones pose a danger not only to the safety and privacy of people but also to the security and privacy of governments. Other research, such as [16, 19–23], are also shedding light on the frequent problems and dangers associated with drone security.

Tian was able to ensure that the privacy of the drones Network by providing an efficient privacy-preserving authentication framework for edge-assisted internet of drones [24]. This framework was able to keep sensitive information private. In a similar manner, Hell described a drone system that might be used for the purpose of securing and monitoring a factory [25]. For reasons of safety, this system was able to keep an eye on a specific section of the plant where the action was taking place. Tosato presented a similar application in 2019, in which he offered an autonomous application of a swarm of drones for detecting industrial gas. The application was titled "Autonomous Application of a Swarm of Drones for Detecting Industrial Gas" [26]. This application was likewise comparable to the one shown by Tosato. These kinds of drones are becoming more popular in today's market for the purpose of monitoring and surveillance in an industrial area or an agricultural field for the purpose of risk management.

A. Gap Analysis of Drone Security Using Machine Learning

Learning on a machine may be split down into a few basic categories, including supervised learning, unsupervised learning, semisupervised learning, reinforcement learning, deep learning, and a few more. In the recent past, it was discovered that

Table 2 Threat to smart drones from typical cybersecurity and data privacy

	Common cybersecurity threats	Threats identified citations	Countermeasures citations
Protocol-based attacks	Security of communication link		
	Data confidentiality protection	[1]	
	Replay attack	[3, 4]	[5]
	Privacy leakage	[1, 6]	
	De-authentication attack	[7, 8],	
Sensors based attacked	GPS spoofing/jamming attack	[9–11]	[12, 13]
	Motion sensors spoofing	[14]	[15]
	UAV spoofing/jamming attack	[9]	
Compromised component	IoT security threats	[9], [S], [16]	
	Control/data interception	[9, 17]	
Jammers	Denial of service	[7–9]	
	Stop packet delivery	[18]	[18]

various attempts have been made to use machine learning solutions to handle cybersecurity attacks for mobile networks [27], wireless sensor networks [28], cloud computing [29], and Internet of Things (IoT) systems. This was discovered in the process of conducting a literature review. [27] Wireless sensor networks [28] Cloud computing [29] Internet of Things (IoT) systems [29–31], and other types of systems. Table 3 provides a summary of the different efforts made in the past to apply machine learning to the problem of ensuring the safety of various kinds of wireless networks. On the other hand, no evidence of any prior work has been uncovered that used machine learning-based cybersecurity solutions to address vulnerabilities posed by drones.

In addition, we recommend using a security solution that is based on machine learning in conjunction with Blockchain in order to improve the mechanisms that are used for authentication and access control in drone security. This can be accomplished by combining the two technologies. During the course of the in-depth survey of the literature that was carried out from 2010 to 2020 in the field of security, safety, and privacy concerns regarding drones and UAVs, more than thirty contributions were discovered in the form of research papers, the majority of which were published in journals issued by IEEE and ACM. The vast majority of these articles focus on the issues and problems that have arisen in the field of cybersecurity in recent years. These include GPS spoofing, IoT spoofing, drone hijacking, device interception, data privacy, and many other types of comparable cybersecurity concerns. However, the bulk of the published research only focuses on identifying the most significant dangers and problems to the safety of drones.

Table 3 Attacks and the security techniques

Sr. No.	Attacks	Security technique	Machine learning solution
1	Jamming	Secure offloading	Q-learning [27, 28] DQN [32]
2	Denial of service	Secure offloading	Neural Networks [29] Multivariate correlation analysis [33] Q-learning [34]
3	Malware	Access control	Q/Dyna-Q/PDS K-nearest neighbors Random Forest
4	Intrusion	Access control	Naive Bayes Support vector machine Neural network K-NN
5	Spoofing	Authentication	SVM DNN Dyna-Q Q-learning
6	Traffic blockage	Authentication	Q-learning

The vast majority of these studies do not provide any remedies or preventative steps to deal with the identified security risks. Only in [35] is the idea of utilizing blockchain for safe data transport using drones that are enabled with 5G and the internet of things. Nevertheless, a significant amount of human identification of threat types and levels is required by this system. A key-based authentication of devices that are not legitimate for the purpose of providing security is required for other initiatives as well, most notably in the field of Internet of Things-based drones. There is currently a significant research gap that needs to be filled in order to make drones secure and safe from major cybersecurity threats. Filling this gap is necessary in order to make drones usable for commercial and industrial reasons.

Drone/UAV security vulnerabilities and threats

There are many uses and applications for drones and unmanned aerial vehicles, and the list keeps growing as new technologies emerge. However, some of them have restricted operational resources, while others raise a variety of issues about safety, privacy, and security [3, 4]. It is recommended that licensing, regularization, and a variety of procedures (oversight) be implemented in order to place restrictions on the use of superfluous and/or nefarious UAV-based photography. Authorities in every region of the globe have to make it a top priority to enact laws and guidelines that regulate surveillance practices and procedures. The network coverage that is provided by a UAV cannot be compared to the network coverage that is provided by any Wireless Sensor Network (WSN) or Mobile Ad-hoc Network in terms of network security and risk assessment [5]. This is because of limitations on the available resources, since the UAV-based coverage is far larger and more extensive than that of WSN

and MANETs. The following recommendations pertaining to AAA (Authorization Authentication Accounting) may be useful for unmanned aerial vehicles:

- ***Authorization***: Providing the controller of the UAV with administrative privileges in order to prevent any hostile takeovers with administrative rights.
- ***Authentication***: In order to prevent unauthorized access and control, unmanned aerial vehicles require a stringent authentication method.
- ***Accounting***: In the event that a UAV or drone is used to engage in illegal activity, the owner can be identified and brought to justice. Due to the ease of access, mischievous or criminal entities are able to use drones and unmanned aerial vehicles to conduct illegal surveillance, launch cyberattacks, and initiate privacy threats against individuals and organizations. Drones and other unmanned aerial vehicles are having their myriad mechanical and operational capabilities abused in order to carry out malicious acts [10]. The efforts that are made to make unmanned aerial vehicles and drones more secure and rigid also make them more effective for engaging in malicious activities. These kinds of events make the growth of UAVs and drones a double-edged sword.

4.1 Security Concerns

UAVs are an excellent option for illegal activity since they can be transported easily, are inexpensive, are readily available, do not need much maintenance, and are easy to handle. UAVs are often used by criminals and terrorists to carry out damaging actions and acts of sabotage, for instance. UAVs are efficient carriers for potentially hazardous chemicals or explosive materials because of their ability to attach a diverse selection of payloads. Further contributing to their usefulness is the fact that they can access areas that are inaccessible to people. They are able to transport anything, either undetected or in a stealthy manner [11].

4.2 Safety Concerns

Concerns around drones and other unmanned aerial vehicles go beyond only safety. Any drone that is flying over people or property runs the risk of experiencing a malfunction and crashing. These types of collisions have the potential to cause damage to structures as well as personal injury to persons [12]. There have been reports of events of this kind from all across the globe. Unfortunately, accidents to humans caused by unmanned aerial vehicles and drones are rather prevalent. A passenger plane was damaged by an unmanned aerial vehicle in April

of 2016. (British AirwaysBA727). As a result of these incidents, the following recommendations about public safety might be made:

- ***Safety Feature***: Strong winds significantly increase the risk that an unmanned aerial vehicle or drone will be hacked or will become difficult to control. In these kinds of predicaments, there ought to be a choice between turning it off and regaining control of the situation.
- ***Weak Signal or jamming***: As part of a cyberattack, unmanned aerial vehicles and drones are more susceptible to being hacked and taken over when signal jamming is used.
- ***Design/Architecture safety***: The vast majority of the unmanned aerial vehicles and drones that are readily available to the general public are rotary-based kinds.

These drones have the capability of having extra safety measures. Although it is reasonable to assume that the addition of such safeguards would have an impact on the design and could cause performance issues, ensuring people's safety must come first. Regarding the precautionary precautions that should be taken with consumer drones and unmanned aerial vehicles, a standard has to be developed and implemented. These requirements should also contain elements that prevent accidents from occurring.

4.3 Privacy Concern

Privacy concerns have been brought to the forefront as a result of the ease with which unmanned aerial vehicles that are fitted with high-definition cameras and other electronic components can be acquired by anyone. Without the subjects' knowledge, it is simple to record or monitor someone while they are on their own private property. According to the Canadian Public Safety (CPS), unmanned aerial vehicles have given rise to a significant number of issues about safety, security, and privacy [13]. People have been subjected to extortion and other forms of illegal activity as a consequence of being photographed or recorded without their knowledge. In order to better govern how unmanned aerial vehicles are used, legal laws should be developed regulating the capturing of private photographs or recordings without the owner's agreement when utilizing UAVs, flying past premises, or hovering at window level.

Existing threats for drones/UAVs

Several unmanned aerial vehicles currently available on the market have significant design flaws because there is a lack of standardization. The absence of wireless security is one of the aspects of these problems that causes the most cause for concern.

Some researchers also carried out various forms of cyber-attacks on unmanned aerial vehicles in a simulated setting in order to test the impact and vulnerabilities [33]. Such experiments comprises of the following:

- ***DoS Attack***: Researchers controlled unmanned aerial vehicles via simultaneous requests. The excessive number of queries caused the response to become overloaded, which in turn caused the UAV system to fail.
- ***Buffer-Overflow***: After altering the packet request for controlling the drone or unmanned aerial vehicle, the researchers brought the system that was supposed to be in charge of operating the drone or UAV to a crashing halt.
- ***ARP Attack***: The researcher used the cache-poisoning strategy as part of the Address Resolution Protocol (ARP) assault, which ultimately led to the uncoupling of the UAV from its controller.

An assault on a UAV's operating system (OS) or micro-controller unit is another facet of a cyber-attack on a UAV. This facet is distinct from attacks on communication connections or on ground control, which are two other aspects of cyber-attacks on UAVs. The operating systems used for UAVs are often fairly similar to those used for smartphones. Because of this commonality, numerous assaults that are successful against smartphone operating systems might also be advantageous when applied to unmanned aerial vehicle systems. Because of advances in technology and UAVs, the number of potential attack vectors against UAVs is growing. In the modern day, the availability of various forms of attacks is almost limitless thanks to advances in technology. The assaults that have been successfully carried out for instructional objectives are shown in Fig. 2, which may be found in references [33, 34]. GPS spoofing is one of the most popular forms of cyberattack against unmanned aerial vehicles and drones, and it is one of the threats described in this section. Signal jamming, de-authentication, and zero-day attacks are the most typical kinds of GPS assaults. Jamming the signal may also be used.

5 Existing UAV/Drone Security Systems and Countermeasures

The first step in mitigating security risks posed by drones and other unmanned aerial vehicles is to categorize the different kinds of assaults, as well as their targets and their goals. The following table details some of the most prominent cyberattacks that have been carried out against unmanned aerial vehicles and drones. Additionally, the type of the assault as well as certain preventative measures against the attacks are highlighted in the table. The verification procedure of a UAV or drone is the focus of the vast majority of the attacks detailed in Table 6. This demonstrates the need of making improvements to the authentication process used for UAVs and drones (Tables 4 and 5).

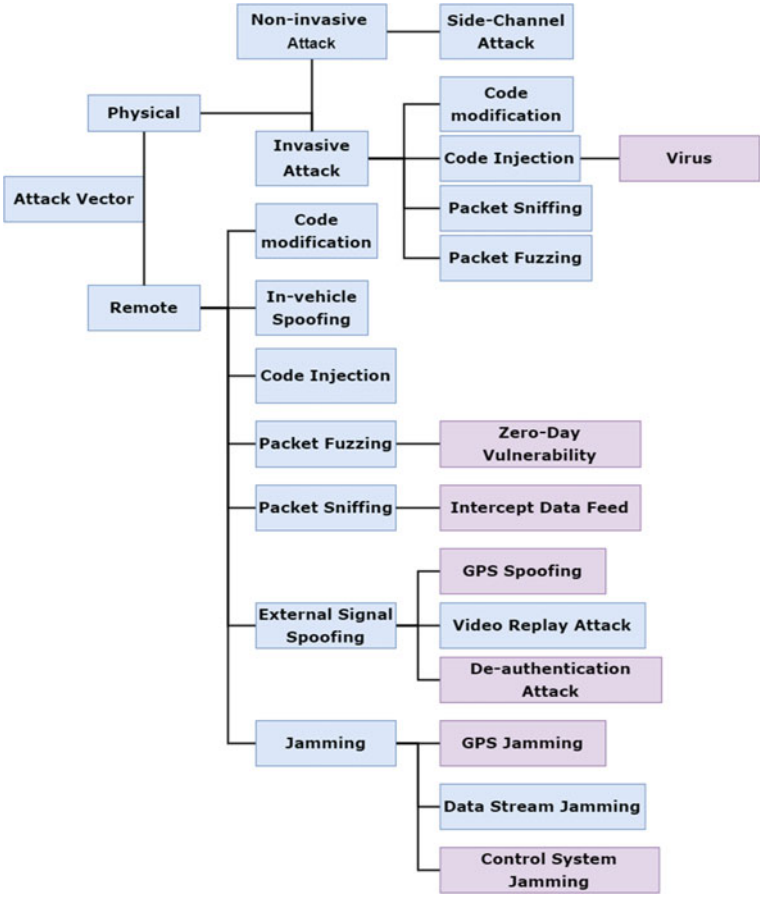

Fig. 2 Attack vector for drones/UAVs with known incidence or educational goal is shown in gray

5.1 Current Countermeasures

Wireless communication networks are beset by a slew of security weaknesses and threats. Recently, machine learning (ML)-based intrusion detection systems (IDS) have shown to be very successful against network threats. Several academics are focusing on resource management issues in machine learning-based intrusion detection systems. This is due to the fact that machine learning-based solutions need more resources than other kinds of solutions. Blockchain technology is also among the most effective methods for protecting the privacy and safety of unmanned aerial vehicles and drones [18].

Table 4 Logical counter measures for UAV/drone in an urban environment

Counter measure	Details
Wi-Fi jamming	Wi-Fi-based drone/UAV operates using a 2.4 GHz frequency. A conventional jammer can jam these frequencies within a limited range and can be used for privacy purposes
Wi-Fi air crack	Although it is an attacking method, it can be used to take control of any illegal or privacy-invading UAV/drone
Three-way handshake	Although it is also an attacking method, it can be used to deauthorize or even jam communication between the UAV/drone and the controller
DoS	Websploit Wi-Fi jammer can be an effective method to jam or de-authenticate UAV from its controller. However, to conduct DoS based attack, some knowledge about the communication channel is required
GPS spoofing	Encryption of civilian-based equipment is very costly and making it vulnerable to GPS spoofing attacks

Table 5 UAV/drone security limitations

Limitation	Details
Availability	UAV/drones are easily accessible for everyone to purchase. There is no owner registration or license registration for purchasing a UAV/drone
Design issue	Due to the absence of standardization, manufacturers are failing to comply with necessary requirements i.e., safe design, factory authentication, etc.
Policies	Standardization and policies are absent for UAV/drone operations and operators. In some countries, policies are defined for UAV/drones flying in proximity of sensitive areas. However, a general set of operating policies for a UAV/drone are still not available
Non-real-time countermeasures	Due to a lack of standardization for design and operational software, the current UAV/drones do not have real-time protection during flight. If a UAV/drone is compromised during flight it cannot be retained by the original owner
Limited testing	Due to limited testing, the available control and communication units are vulnerable to several types of attacks
Forensic limitations	In case of a harmful event, the limited availability of forensic tools and methods makes it difficult to identify the malicious operator of UAV/drones involved in the dangerous act
Unreliable security	Based on the hostile operational environment of UAV/drones, the default security measures are not suitable. Due to the harsh operating environment of UAV/drones, a robust security protocol is necessary. But due to design and resource limitations, improving security measures is very challenging
Authentication	Based on recent events as shown in Table 6, the currently employed authentication method for UAV/drone can easily be compromised. Except for the UAV/drones operated for defense purposes as they have trailered software to cope with the requirements
Limited frequency bands	The UAV/drones are being operated within a limited range of frequencies. Making them an easy target for jamming-based attacks

Table 6 Recommendations for improving UAV/drone security and privacy

Measure	Description
Licensing	Every UAV/drone should be registered and licensed. Such measures will make it easy for the authorities to identify the owner of any harmful drone/UAV
Flying permit	A flying permit similar to a driving license should be issued with a registered drone/UAV. Such regulation would limit. UAV/drone-based illegal or harmful activity
Education	The public should be educated on the harmful or illegal use of UAV/drones
Laws	Based on harmful and illegal events, laws should be introduced for the misuse of UAV/drones
Restricted zones	Areas that are classified or could pose a danger to drones/UAVs should be marked. Map-based public applications should also indicate areas that are no-fly zones for UAV/drones
Non-lethal measures	Non-lethal tools to counter drones/UAVs should be publically available. Such tools can play an important role in urban areas
Machine learning	Security tools such as ML-based IDS can vastly improve the security architecture of drones/UAVs
Multi-factor authentication	Rigid authentication methods can help in stopping several common security threats

5.1.1 Security for UAV/Drone Communication Networks

In the race to meet the most recent challenges in network security, ML-based intrusion detection systems have emerged as some of the most effective technologies. In most cases, IDS may be divided into the following three categories:

- ***Rule-Based***: The purpose of utilizing these kinds of IDS in the UAV domain is to identify false data-injection attacks, more specifically those that target signal strength between UAV and ground control.
- ***Signature-Based***: Signature-based intrusion detection systems (IDS) have also been used by some researchers on UAVs. The authors of the paper used a bio-inspired cyber-attack method that targets airborne networks in their research. Signature-based intrusion detection systems are just as ineffective against unknown and complex attacks as rule-based intrusion detection systems.
- ***Anomaly-Based***: In order to protect UAV networks from jamming assaults, these kinds of IDS are utilized. Jamming attacks include denial of service attacks, distributed denial of service attacks, triggering malfunctions, and attacks based on sensors. The high resource requirement is the only significant problem associated with anomaly-based ML IDS.

There has been an uptick in the amount of unmanned aerial vehicles and drones, which has resulted in an increase in the variety of potential solutions for the UNV communication network. In certain articles, the problems with the physical layer of the UAV communication network were discovered, and an iterative approach that

was based on optimizing techniques was suggested. This algorithm demonstrated an improved detection rate of assaults. In a similar vein, additional publications have investigated concerns with ADS-B, line of sight, air-to-ground, and eavesdropping wireless communications, as well as air-to-air wireless communications. Researchers have come up with a number of potential solutions, some of which include making use of modulation, dual antennas, game theory-based algorithms, or Q-learning-based techniques. Encryption, in addition to these ways, is another essential component for ensuring the safety of communication between UAVs. Researchers have been looking at other types of encryption that do not need a lot of resources. Since conventional encryption techniques don't take resources or latency into account, none of those things is considered to be a relevant consideration. Not only does encryption guarantee the safety of communications, but it's also a great tool for verifying the legitimacy of unmanned aerial vehicles and drones.

5.1.2 Data Security

Data that is collected by a UAV or drone is first aggregated onboard the UAV before being sent in any direction. The reduction of network traffic is significantly helped by this aggregation in a significant way. On the other hand, the act of aggregating data and encrypting it results in additional problems. The symmetric cipher is not safe enough to defend against advanced attack techniques, and the asymmetric cipher demands a significant amount of computational power as well as a significant amount of resources. The use of an asymmetric encryption necessitates an increase in the storage overhead. Because of these limitations, researchers are exploring towards strong encryption techniques that are also lightweight for the purpose of protecting UAV and drone data.

5.1.3 Forensic Approaches

The field of digital forensics has the potential to play a pivotal role in determining the various forms of assaults carried out by UAVs and devising effective defenses against them. A general framework for NF was proposed by the authors of article, which may be found here (Network Forensics). The framework performs an analysis on the data that is sent via firewalls or IDS in order to discover any anomalies. In order to accomplish its mission, the framework's primary focus is not only on locating the unusual occurrence but also on tracing the origin of the activity. In another research, the authors propose an NF framework that makes use of DIP (Digital Investigation Process) and a number of other digital investigation approaches organized hierarchically. The methodology described in this study utilizes a two-tiered structure. Assessment, countermeasures, data collecting and analysis, writing up an incident report, and finally, event closure make up the first layer of this process.

The second tier is an object-oriented sub-phase that may be found. In addition, a forensic investigation of a UAV or drone may be divided down into three primary

components. In a similar vein, a number of other researchers have suggested various approaches of using forensic methodologies to defend against sophisticated and complicated assaults. The reason why the forensic technique is being emphasized is because, as time passes, the nature of assaults and the goals they seek to achieve become more complicated and harder to determine. Both the culprit and the manner of assault may be determined with the assistance of forensic science. Once the sort of assault has been determined, the proper preventative measures may be put into place to forestall any such incidents.

6 Physical and Logical Attacks Countermeasures

According to the report, the number of incidents involving aircraft and drones increased from 6 to 93 between the years of 2014 and 2017. This highlights how vital it is for the authorities to address concerns over the privacy and safety of UAVs. Because of the rise in the number of cyberattacks on drones and other unmanned aerial vehicles, the government has to implement stringent laws and guidelines to reduce the impact of these worries. Because unmanned aerial vehicles are becoming more common among members of the general public, there is a heightened risk that they may become the target of unlawful activity. Physical and local countermeasures are the two categories into which civilian or domestic UAV defenses are separated.

Keeping in mind that the rational countermeasure for use against UAVs in urban areas does not include cutting-edge technology and is restricted in both its range and its functioning. The rational defenses against unmanned aerial vehicles (UAVs) and drones in an urban setting are outlined in Table 4.

6.1 Military and Government Counter-Measure Techniques

When it comes to countermeasures that are rooted on the military, the availability of resources is often not a concern. As was said previously, the employment of unmanned aerial vehicles and drones is not restricted to observation; rather, they may be used to conduct assaults or to designate sites for attacks, which makes them hazardous instruments on the battlefield. Figure 3 illustrates a few of the most common drone and unmanned aerial vehicle defenses. The armed forces of every nation on earth are very well prepared to counter threats posed by unmanned aerial vehicles and drones. Only a small portion of the information that is widely known and accessible to the public on anti-UAV and anti-drone weapon systems is included. Different strategies are used by government and military agencies in the process of drone detection. It is possible to identify them (UAVs or drones) by the use of audio, video, motion, thermal, radio, and RF-based detection technologies. All of these approaches come with their own set of benefits and drawbacks.

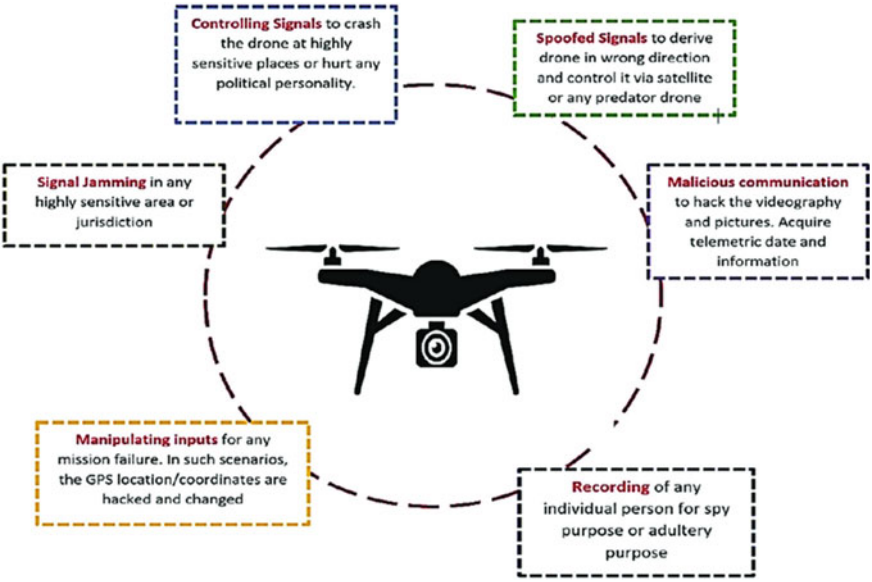

Fig. 3 Security and Privacy threats of UAVs

Security implementation limitations

There are still many obstacles to overcome in order to successfully adopt and put into practice stringent security procedures for UAVs and drones. Table 5 outlines some of the most important concerns about the limits of UAVs and drones in terms of security. Standardizing the design of UAVs and drones, as well as communication protocols and basic factory default security measures, is one way to address the majority of the aforementioned restrictions.

Recommendations and summary

Tables 5 and 6 provide many suggestions that might enhance the level of privacy and protection afforded by UAVs and drones. There are some broad suggestions included in Table 5 that might be of assistance in enhancing the privacy and safety of UAVs. While Table 6 provides an inventory of the most current blockchain-based technologies for protecting the privacy and safety of UAVs, In addition, in order to address concerns relating to safety and privacy, regulatory bodies and the industry as a whole need to work together to regularize and standardize unmanned aerial vehicles and drones. Blockchain technology has the potential to provide UAVs and drones security that is both highly effective and significantly improved. The need for more processing resources is the sole issue that has to be addressed when considering blockchain-based solutions. On the other hand, the improvement that blockchain brings in terms of security and privacy is more than sufficient. This is due to the fact that blockchain may be decentralized. The blockchain-based solution has the

potential to be a highly good choice for unmanned aerial vehicles that have been created with military and government applications in mind.

6.2 Criminal Attackers

These kinds of assaults may be either physical or intellectual in nature:

- **Physical Attacks**: The most significant risk is connected to the problem of private property monitoring, in which drones may easily be utilized to violate people's physical privacy. This is the most significant risk. The fact that drones are able to penetrate geoboundaries is a highly concerning problem. According to BBC News, people were able to smuggle narcotics, phones, and even blades inside high-security prisons while escaping ground monitoring. This was done in order to provide inmates with these items. This is often accomplished with the help of an octocopter that has the capacity to lift 20 pounds. Additionally, these kinds of assaults involve crashing drones into specific persons (accidentally or purposely) or crashing them into the properties of people, which may cause damages ranging from minor to severe. There is also a risk associated with the use of tiny quadcopters like the DJI Phantom 3, which has a range of 16,000 feet (480 m) and can fly at an altitude of 4000 feet (1220 m). This is a significant challenge, particularly with regards to accidents involving birds, which may result in significant difficulties for the engines of aircraft.
- **Logical Attacks**: Logical attacks include the use of a rogue Access Point (AP). Therefore, a potential attacker has the ability to get sensitive information, such as passwords and credit card data, from users. This also involves attaching a Raspberry Pi device to a drone and configuring it to intercept and take control of other nearby drones. This may be done in order to take over other people's drones. This transforms the malicious drone into a rogue access point (AP) for other drones and devices in the vicinity, and it is also capable of introducing malware into linked cellphones by intercepting and redirecting the data traffic of users, as well as via phishing (malicious links, fake advertisement, or false update). In point of fact, many other types of drone assaults, including as jamming and spoofing, were described and analyzed.

Finally, an adversary might target and exploit the sensor inputs of an unmanned aerial vehicle by manipulating the relevant settings in order to deceive the sensors.

6.3 Terrorist and Insurgent Attacks

Since these drones might be exploited by terrorists for nefarious objectives, the proliferation of drones has led to the emergence of major dangers and difficulties. When it comes to the use of drones, keeping them out of the wrong hands might

have devastating effects. In fact, drones are being used by insurgents and terrorists alike. ISIS has also issued an instructive graphic describing their assaults in February 2017, utilizing a pro-ISIS channel known as "Ninawa Province," to display the video obtained before to a terrorist strike. This comes against the background of its increased usage of attack drones in Iraq and Syria. The terrible impact that drones have on the morale of both military and civilian people have caused the whole globe to become very frightened about the significant safety and security dangers posed by drones. In most cases, the following goals are related with terrorists making use of drones:

- **Drone Footage Interception**: Interception efforts of video streams and footage by military drones and unmanned aerial vehicles (UAVs) were common and often effective. One illustration of this would be the incident in 1997 in which Israeli drone video was captured before any further encryption was applied. An further instance of this took place during the Iraqi conflict, when rebels were able to intercept US predator drones by using initially a program with a value of $26 and subsequently the SkyGrabber software respectively.
- **Airstrike Disruption**: ISIS operators would fly and target the airstrike calling team in Raqqa, tricking their opponents into thinking it was a friendly drone hovering overhead. This strategy was adopted by ISIS in order to disrupt airstrikes that were being carried out against them in Raqqa. First, ISIS operators would wait for their adversaries to fly a drone. These drones were equipped with explosives the size of 40-mm grenades and had the ability to strike their target with a high degree of precision.
- **Burning/Incendiary Kites**: In a nutshell, the operation of drones and other unmanned aerial vehicles may be used in a variety of settings. As was just discussed, the danger posed by drones and other unmanned aerial vehicles is extremely concerning and appears to be growing at an alarming rate, particularly as the year 2020 draws closer. This is due to the growing number of instances in which criminals and terrorists use drones and other UAVs to carry out harmful activities. According to the information presented in this section, drones have been used in a variety of fields not just for beneficial goals, but also for harmful ones.

7 Drones Security, Safety and Privacy Concerns

The usage of drones presented benefits on a wide variety of fronts, ranging from the commercial to the personal. However, there are a variety of security, safety, and privacy concerns associated with drone systems. The most senior level of government should address the concerns raised by the many security and privacy risks posed by drones. In addition, there should be a very tight method in place to prevent the capability of drones to capture photographs and record videos of people and properties without the legal consent of the owners of such individuals and things. Traditional wireless networks, such as Wireless Sensor Networks (WSNs) and Mobile Ad-hoc

Networks (MANETs), are not the same as a drone-assisted public safety network from the point of view of security and threat analysis. This may be explained by the fact that it requires less power and carries less information in comparison to a public safety network that is helped by drones. In addition, the coverage area of the drone is larger and more extensive than that of WSNs and MANETs. As a result, the issues posed by security are mostly associated with the restrictions placed on UAVs about their resources as well as their latency. In addition, it is of the utmost importance to make certain that the qualities of secrecy, integrity, availability, authentication, and non-repudiation are satisfied through communication channels. This is carried out in accordance with the methodology and rules established by the AAA:

- **Authorisation**: by bestowing privileges on the personnel operating the UAV.
- **Authentication**: by using something only you have access to as part of a multi-factor authentication system, something you have (your username), and something you are (your biometric information) are considered to be your possessions.
- **Auditing/Accounting**: by conducting searches for and maybe arresting lawful drone and UAV owners in the event that illegal or harmful activity occurs.

The use of drones by malevolent organizations to carry out physical and cyber-attacks is a danger to society because it violates the privacy of the society's citizens and threatens the safety of the general public. These assaults may be carried out using drones. In point of fact, several technological and operational qualities of drones are being abused and misused for the purpose of planning and carrying out future attacks. This involves carrying out crucial activities based on offensive reconnaissance as well as conducting surveillance with the intention of following certain persons and certain places, which creates difficulties with both safety and privacy. In the event that a drone has a malfunction and crashes into a neighboring home, park, parked vehicle, or humans, this presents another potential threat to public safety.

The outcome of this would be the destruction of property as well as the injury or death of people. The present security procedures do not provide protection for such connections since they are based on the assumption that no one could approach them at a distance that would allow them to be compromised or that would allow them to access internal networks through wireless signals. These assumptions lead to poor single factor authentication and the use of common passwords that can be readily cracked, particularly when there is no encrypted connection present. Additionally, these assumptions lead to the usage of usual passwords. Because of this, it is just as simple to steal information from a private building as it is from a public coffee shop.

An adversary would take use of such weaknesses in order to compromise security, safety, and/or privacy. The most significant concerns to the safety of drones are outlined in Fig. 4, along with the countermeasures that may be taken to counteract each one. Following that, we will provide a brief summary of the present and upcoming security problems.

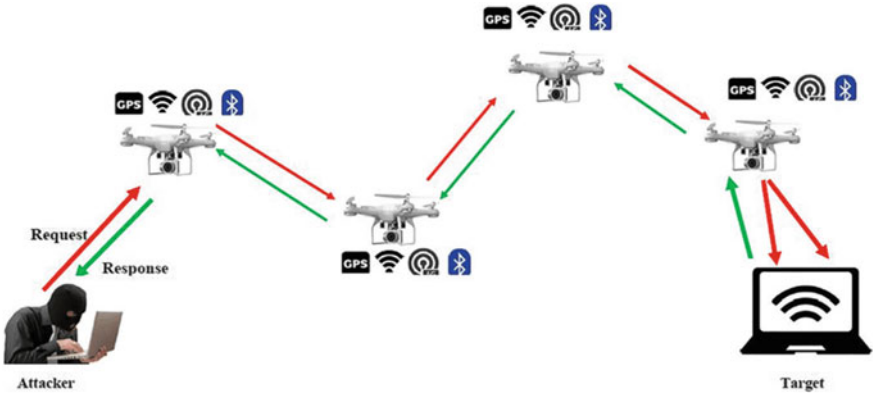

Fig. 4 Stepping stone attack using multiple UAVs

7.1 Security Concerns

The qualities of the drones, including their portability, affordability, and simplicity of operation and maintenance, make them an attractive option for criminals. Terrorists have also begun to focus more on the use of drones to carry out their attacks. This is mostly due to the fact that the nature of drones makes it less likely that they would be discovered. Drones may be armed and modified to deliver lethal poisons or bombs, and they can also be fitted with weapons to strike important infrastructure. In fact, this is already possible.

In addition, persons who are congregating in difficult-to-reach areas may be exposed to the detonation of explosives carried by drones. Because of this, it is much simpler for a terrorist to accomplish their goal, particularly considering the fact that drones combine the stealth of a suicide bomber with the range of an airplane. There is widespread fear among military experts about the possibility that drones may be employed for espionage against the United States. This is because ISIS is able to re-arm drones that are available for purchase in the commercial market and adapt them for use in combat operations over Iraq and Syria.

7.2 Safety Concerns

Both “safety” and “security” are not necessarily synonymous with one another. Outside of the realm of the military, civilian drones and unmanned aerial vehicles have the potential to malfunction and crash into a nearby house or a group of people in November of 2016, a youngster from Stourport-on-Severn, Worcester, United Kingdom, who was 18 months old at the time, had his eyeball slashed in two by the propeller of an uncontrollable drone. Before arriving at Heathrow Airport in April 2016, a passenger plane operated by British Airways and with the flight number

BA727 was struck by a drone. Nonetheless, there were no reports of casualties, and all 132 passengers and five members of the crew were unharmed. As a direct consequence of these occurrences, the following top issues about safety have been identified:

- **Signal Distortion-Jamming**: Because of this, a UAV is susceptible to being hacked, hijacked, and having its GPS or signal jammed as part of an act of cyberterrorism or cybercrime. This is primarily due to the fact that the UAV's command-and-control operation center is vulnerable to being exploited.
- **Lack of Governments Regulation and Awareness**: in particular with regard to the safety procedures and features that must be implemented to guarantee the safe incorporation of UAs into the national airspace domain.

7.3 Privacy Concerns

People's privacy is also at a high risk of being exposed by unwanted flying guests, which can record their movements and capture images of them. This is an indicator of how much our privacy is exposed to such a developing danger, and it should concern us. According to the Canadian Public Safety, unmanned aerial vehicle technology have produced a wide variety of concerns with regard to the gathering of photographs and videos. Blackmailing and other forms of fraud were related with this tactic, which consisted of threatening to reveal private photographs or films of the victim that were taken from above without their consent. The potential risks to one's privacy may, in general, be broken down into three distinct categories.

- **Physical Privacy**: entails flying unmanned aircraft systems (drones) over the property of another person or getting very close to their windows. As a result, the victims' right to personal freedom is put in jeopardy because their assailants have the ability to surreptitiously record videos and take pictures of themselves acting in potentially inappropriate ways.
- **Location Privacy**: is based on following and identifying individuals using a drone that is flying and buzzing over them without the persons being monitored being aware that they are being watched.
- **Behaviour Privacy**: is a situation in which the presence of a flying drone might influence how people behave and respond, particularly when they are aware that they are being watched. Because of this, not only would their freedom be restricted, but also their private would be violated and their privacy would be invaded. When it comes to the Internet of Things (IoT), particularly when it comes to drones and other unmanned aerial vehicles, security, safety, and privacy are essential needs that must be met. In this part, we will discuss the primary issues about privacy, safety, and security that may be imposed as a result of security breaches. These primary problems need to be addressed as soon as humanly feasible; if they aren't, the unlawful use of these substances will continue to steadily grow, which is particularly likely given the lack of stringent regulations, legal limits,

and consequences. Following this, we will discuss the primary security flaws and dangers that need to be taken into account in order to ensure that the safety of the drones is not jeopardized.

8 Drones Existing Threats and Vulnerabilities

The use of unmanned aerial vehicles and drones is increasingly seen as a significant risk to information security.

- **Prone to Spoofing**: The configuration and flight controllers of several types of unmanned aerial vehicles with many rotors were analyzed, and the results showed numerous flaws. Tests conducted shown that information may be readily obtained, manipulated, or injected by using GPS spoofing. These experiments revealed that this is possible. Because of this flaw in the data connection, hackers now have full control over the drone and may intercept and spoof transmissions.
- **Prone to Malware Infection**: Users are able to pilot drones using wireless remote controls such as mobile phones. This method, on the other hand, was proven to be vulnerable; it makes it possible for cybercriminals to generate a reverse-shell TCP payload, inject it into the memory of the drone, and use it to discreetly install malware on the computers that are responsible for operating the ground stations.
- **Prone to Data Interference and Interception**: telemetry feeds are utilized to monitor the vehicles and ease the sharing of information over open non-secure wireless communication, which leaves them subject to a variety of dangers. These include the stealing of data, the introduction of harmful material, and the modification of pre-determined flight trajectories.
- **Prone to Manipulation**: Due to the fact that drones follow pre-programmed and pre-defined flight paths, manipulation is possible, and this has the potential to have catastrophic repercussions.
- **Prone to Technical Issues**: A great number of drones have a variety of technical difficulties. This includes program issues such as a failed connection between a user's device and the drone, which might cause the drone to either crash or take off in the wrong direction. It is important to be aware that the batteries have a lower life lifetime in cold conditions, which results in a shorter flying duration as well as the possibility of malfunctioning.
- **Prone to Operational Issues**: The lack of flying abilities among drone owners is another big challenge, as is the variety of drones that are now in use. This has the potential to inflict significant damage and/or injuries to both workers and/or property. In point of fact, drones are delicately constructed, which means that even a little mishap might cause the drone to crash. If one of the rotaries fails to operate well or completely ceases operating, it might result in considerable turbulence, making it difficult to keep control of the drone. This would, in almost all circumstances, result in the drone plummeting to the ground. For instance, described an event in which an Israeli drone violated the airspace above Lebanon

and then crashed in the south of the country owing to a combination of technical and operational difficulties.

- **Prone To Natural Issues**: Due to the fact that they are so lightweight, drones are sometimes unable to endure the effects of wind. In addition, if the temperature is really high, the engine can overheat and stop working, causing the drone to crash. Additionally, the battery may burst into flames, resulting in significant property damage and even bodily danger. Drones do not come with any kind of protection against the rain, thus it is impossible for them to fly in it. This presents another problem for the industry. When drones fall into bodies of water like lakes, rivers, beaches, or even pools, they often cease functioning instantly. The reduced vision, which may drop from a few meters to less than a meter, can cause a breakdown in communications between the drone and the GPS, which in turn sends the drone outside of its control area until it crashes. Owners are recommended not to fly their drones during fog for this reason.

9 Drones Existing Cyber-Countermeasures

An attacker's primary reasons, aims, and goals may be used to categorize the primary countermeasures that can be implemented to secure drones from security threats. These countermeasures can be divided into the following groups. Following is a discussion on the many approaches that may be taken to ensure the safety of drones' networks, communications, and data.

9.1 Securing Drones/UAVs Networks

Drone networks are vulnerable to a number of attacks and problems related to security. Intrusion Detection Systems, often known as IDSes, have recently been implemented in order to identify harmful behaviors carried out by UAVs and drones as well as suspicious assaults that may be directed against them. In normal operation, an intrusion detection system (IDS) will monitor and analyze both incoming and outgoing network data in order to look for unusual behavior. Examining the data audits (trails) that were gathered at various points along the network is their plan for locating and determining the source of cyberattacks. In the following, we will discuss the many different IDS strategies that may be used to defend drone networks from unauthorized users.

- **Rule-Based Intrusion Detection** Strohmeier et al. devised a rule-based intrusion detection technique for the purpose of protecting the connection between an airplane and a ground station and published their findings. The purpose of this endeavor is to identify assaults of bogus data injection, particularly those

that target the signal strength. They demonstrated that it is possible to identify attackers within a minute and a half. The authors made use of a UAV-IDS that was based on behavior rules. The guidelines for appropriate behavior were developed on the basis of predetermined attack models, which included careless, random, and opportunistic assaults. This enabled for the reduction of detection mistakes, including the rates of false positives and false negatives, while maintaining a crucial balance between the UAVs' level of safety and their overall performance. Mitchell et al. proposed BRUIDS, an adaptive behavior-rule specification-based intrusion detection system, in the article. This system is able to identify hostile UAVs in airborne systems. The findings of the simulation demonstrated that BRUIDS is capable of achieving a greater detection rate in comparison to the multi-trust anomaly-based IDS strategy, all while maintaining a reduced percentage of false positives. Rule-based intrusion detection systems, on the other hand, have a problem managing its complexity, which need human interaction for rules setting. In addition, this kind of intrusion detection system (IDS) is unable to identify unknown threats.

- **Signature-Based Intrusion Detection** An ADS-B intrusion detection framework was described by Kacem et al. in their paper, which was built to protect an aircraft against cyberattacks that target ADS-B communications. A system like this one is constructed using signature detection methods, which include analyzing the GPS location of an aircraft. A bio-inspired detection technique was developed by Casals et al. and published for the purpose of detecting cyber-attacks that target aerial networks. However, in the same way that a rule-based IDS is unable to identify unknown assaults, a signature-based IDS is also unable to detect attacks that use dynamic signatures.
- **Anomaly-Based Detection** In the UAV industry, the primary function of an anomaly-based detection intrusion detection system (IDS) is to protect against jamming attempts. An anomaly-based learning system was proposed by Rani et al. in their paper to defend UAV nodes against DoS and DDoS assaults. This system prevents the motors of drones from operating at temperatures that are outside of their normal range. This method provides the possibility to avert motor failure by landing the drone in the event that it has overheated, although it does not completely prevent the problem. The results of the experiments show that it is possible to securely operate the drone by using the information provided by the sensors. A method was designed to defend against distributed denial of service attacks, and its performance was evaluated using real-time traffic. The findings demonstrated an accurate identification of many distinct kinds of anomalies. However, further testing is necessary before determining whether or not it is effective.

An Intrusion Detection and Response Framework (IDRF) was introduced by Sedjelmaci et al. with the purpose of protecting a UAV network from assaults on data integrity and network availability, as well as protecting a UAV-aided VANET from hostile threats. These kinds of attacks can be particularly damaging. This strategy works to identify malicious network abnormalities by operating at the level of the

UAV as well as the base station. Mitchell et al. developed a specification-based intrusion detection system (IDS) in their paper for the purpose of securing sensors and actuators that are integrated in a UAS. The IDS was tested on UAVs to study the impact that an attacker's behavior might have on the system in order to determine how successful their solution is. According to the findings, the approach makes an effective trade-off between a high detection probability and a high false positive rate in order to provide improved safety for applications that use UAS. In view of the fact that gateways for drone networks could be operating under certain restrictions (fog nodes), there is a need for a lightweight host-based anomaly detection approach that calls for just a minuscule amount of processing resources. Either a straightforward method of machine learning or a statistical strategy using the fewest available characteristics may be used to accomplish this goal. This structure should be built on top of a hybrid approach. A system like this one would rely on both machine learning and the expertise of human security professionals.

9.2 Securing Drones/UAV Communications

There has been a growth in the number of drone and unmanned aerial vehicle (UAV) film interceptions, which led to the presentation of several ways to secure UAV communication. The results of the simulation demonstrated a substantial increase in the level of discretion provided by UAV communication systems, which was one of the objectives of the project. The findings of the simulation indicated an increase in the secrecy rates of communications between ground stations and unmanned aerial vehicles (UAVs and G2Us). An iterative sub-optimal approach was proposed by the authors by utilizing the block coordinate descent method, the S-procedure, and the successive convex optimization method. The findings of the simulation demonstrated a discernible rise in their worst-case average secrecy rate.

The results of the simulation demonstrated a successful reduction in the UAV assault rate as well as an improvement in the system's capability for maintaining secret. Encryption of drone and unmanned aerial vehicle communications is an absolute need, and should be used in addition to modulation methods. Various cryptographic techniques, including the encryption and authentication of messages, were recently suggested in this context as potential solutions. In addition, this may be done in such a manner that the source authentication, together with the integrity and confidentiality of the data that is being transferred, is maintained. Elliptic Curve Cryptography, often known as ECC, digital signatures, hashing, and other cryptographic processes are all included into UAV applications under TPPA. The use of battery-powered devices across long distances necessitates the use of lightweight cryptographic methods and protocols in order to ensure the confidentiality of drone communications. Recent research provided novel cryptographic methods that only need one round of functions or a small number of iterations. In addition, authentication mechanisms that already exist to protect users' privacy may make use of these lightweight cryptographic algorithms with just a little amount of additional

latency. Additionally, the settings of the physical layer may be used for multi-factor authentication.

9.3 Securing Drones Data

It is necessary to combine all of the data that is obtained by drones in order to reduce the amount of traffic that is regularly delivered to the base station. Unfortunately, present HE solutions have problems with either their performance or their level of security. Both symmetric and asymmetric ciphers have security flaws, although symmetric ciphers are more susceptible to attacks that combine plaintext and ciphertext, while asymmetric ciphers have a higher computational and resource cost, in addition to the storage overhead that is associated with them.

9.4 Forensic Solutions

Within the realm of unmanned aerial vehicles and drones, digital forensics methods are seeing considerable use. Through the use of a chain-of-custody that is composed of six stages, the purpose of such a model is to pinpoint the origin of the assault. Another framework was described, and it promotes a complete multi-tier hierarchical digital investigation paradigm by using a Digital Investigation Process (DIP). The following are the two levels that make up this structure:

1. **First-Tier**: consists of three phases: the period of assessment and incident response, the phase of data collecting and analysis, and the phase of presenting results and closing the event.
2. **Second-Tier**: consists of a phase that is focused on objects. Bouafif et al. published the findings of their digital forensic investigation carried out on a Parrot AR drone 2.0 in the article. This may be accomplished by the examination of flight records, the recognition of artifacts, and the recording of digital information from the drones. Clark et al. introduced an open source forensics tool called DRone Open source Parser (DROP). This program parses proprietary data files taken from the DJI Phantom III's nonvolatile internal storage as well as text files found on the mobile device that is used to operate the drone. According to the findings, it is feasible to determine GPS positions, battery life, and total flying duration, in addition to having the capacity to connect a specific drone to the mobile device that controls it based on the serial number of the drone. Further investigation indicated that it is possible to retrieve data for forensic purposes by physically removing the Secure Digital (SD) card from the drone.

This framework was the product of an investigative procedure that was based on a physical crime scene. In addition, a procedure for conducting a forensic examination

of a UAV was described in. This procedure, which followed a step-by-step method based on three primary initial stages, was offered.

- **Preparation Phase**: This is done so that the chain of command may be identified after the UAV has fallen and been taken as the first piece of equipment to be confiscated. It makes it possible to conduct a traditional forensic investigation in order to identify any DNA or fingerprints that could be on the drone or UAV. Therefore, a conventional piece of evidence, such as witness statements, together with a digital piece of evidence might be integrated.
- **Examination Phase**: Identifying the data storage locations is just one step in the process. This necessitates the use of non-destructive extraction methods, utilizing either commercial or non-commercial forensic tools, in order to safeguard the original data. Alternatively, destructive extraction methods may be utilized.
- **Reporting and Analysis Phase**:

  It is based on an initial analysis of the extracted data. As a result, it is essential to have a solid understanding of how the recording function works in order to successfully intercept the data and convert it into a format that can be read by humans. In addition, a well-fitting forensic model that was given the name "waterfall model" was proposed as a reaction to the large disparities that existed between several commercial models.

  It has become necessary to build effective countermeasures in order to retrieve genuine evidence. It is important for these anti-anti-forensics solutions to be created in a manner that allows them to withstand anti-forensics approaches while still preserving the primary functionality of drone systems. This section provided an overview of the various security solutions that are currently available for safeguarding drone systems. These solutions included both cryptographic and non-cryptographic approaches. In essence, the goal of the cryptographic solutions is to secure the communication between the drones as well as the data that is conveyed, while the goal of the non-cryptographic solutions (IDS) is to identify and recover from any potential security threats. The following subsections detail the typical assaults carried out by UAVs, also known as unmanned aerial vehicles, on various healthcare equipment.

Deauthentication attack

One kind of distributed denial of service attack is known as a deauthentication assault. This assault may be carried out in any of two ways:

(1) **Against the authenticated Clients**: An assortment of deauthentication frames are sent to the clients by the attacker, with the request that they severe their connection to the access point (AP).
(2) **Against the AP**: The attacker starts the process of re-authenticating all of the connected clients by sending a series of deauthentication packets to the access point. Through the process of re-authentication, valid clients and AP engage in

this handshake with one another. This assault is initiated with the intention of disconnecting every single client that is currently connected [36].

Stepping stone attack

The stepping stone assault is a kind of attack in which numerous hosts, or unmanned aerial vehicles (UAVs) in this example, are used to launch an attack on the target. The stepping stone assault, which makes use of several UAVs, is seen in Fig. 4. The attacker sets up the UAV network such that all of the drones are linked to each other through a mobile hotspot.

Drone-in-the-middle (DitM) attack

The UAVor drone-in-the-middle (DitM) attack is used to take control of the communication path between two devices, then intercept and reroute all of the communications that are being sent and received. The DitM attack is depicted in Fig. 5, which can be found here. When it comes to BAN and IMD, the actual device itself serves as the target, and the data receiver of the device takes the place of the Wi-Fi router in this scenario.

Cloud assisted UAV attack

The majority of unmanned aerial vehicles (UAVs) on the market today are developed with advanced features such as internet of things, sensor cloud, and cloud. The attacker will utilize the UAVs that are equipped with cloud capabilities to remotely store the data that has been compromised. This will allow the attacker to retrieve the data at a time and place of his choice. In most cases, the data packets that are created by a wireless network are enormous, which necessitates the use of advanced processing in order to extract important information. UAVs that just have little storage space and a small amount of backup battery power are unable to complete these sophisticated

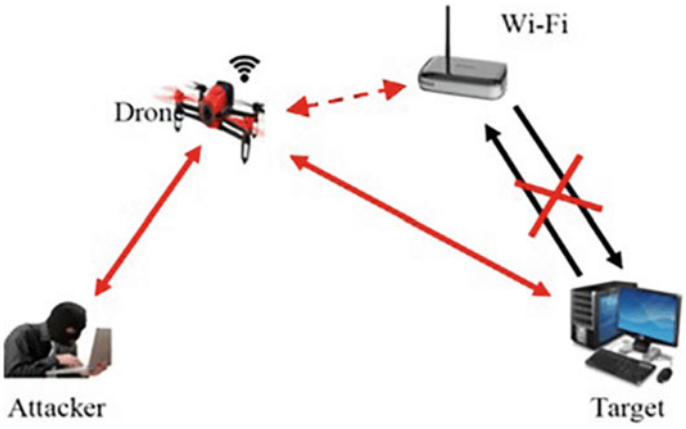

Fig. 5 UAV in the middle attack

calculations. UAVs that are helped by the cloud may be used so that data can be readily sent to the cloud with low drain on the battery. This helps reduce the load of storage while also extending the life of the battery (as shown in Fig. 3).

Evil twin attack

The evil twin assault, which is shown in Fig. 4, is similar to a DitM attack; however, rather than the UAV inserting itself in the midst of a data stream, the evil twin attack involves the UAV taking over as the receiver for the BAN or IMD. The assault that comes from the evil twin is carried out in two distinct stages. At first, the attacker will produce deauthentication probes with the intention of deauthenticating clients that are connected to a genuine access point. Next, the adversary will start a bogus access point, spoofing the MAC address, reallocating the channels used by the original AP, and broadcasting the SSID [36]. This will allow the adversary to assume the identity of the legitimate AP. Last but not least, the clients are compelled to go through another round of authentication with the UAV playing the role of the AP.

Wifiphishing

Wifiphishing is a form of masquerading attack that is carried out on a Wi-Fi network in order to steal sensitive information such as login passwords, information regarding medical accounts, and other similar data. There are two stages to the process of wifiphishing. The first phase of the attack is an evil twin attack, and the second phase involves a fake login page that is forcefully displayed on the client side. This page prompts the clients to enter the valid credentials in order to re-connect with the access point (AP). In a similar vein, the adversary can make use of any phishing pages in order to acquire vital information such as passwords for patient portals.

UAV cyber attack experiment

The HackerUAV that is seen in Fig. 5 is used to transport a Raspberry Pi3 that is powered by batteries. The Hacker unmanned aerial vehicle has an average flying duration of 35 min. A Wi-Fi hotspot may also be enabled by configuring and attaching an external Wi-Fi adapter to the Raspberry Pi3 module [3]. All of the traffic that is collected is kept not just on the local hard disk but also in Dropbox, which is a cloud storage service that is accessible online.

UAV cyber attack scenarios

Two separate tests are carried out as part of this study to illustrate the cyberattack capabilities of UAVs. The first reveals how to get into healthcare automation systems, while the second shows how to take over and manipulate BAN healthcare equipment.

The term “smart hospital automation” refers to an automated hospital control system that gives consumers the ability to operate a variety of hospital appliances by means of Wi-Fi sensor devices [5]. Applications such as this include the automated identification of patients and healthcare professionals, the monitoring of hospital resources using RFID technology, and the management of lighting, TVs, and other environmental systems like as HVAC [10]. If an attacker is able to get into any one of the gateway devices remotely at a wireless smart hospital, then it provides a

channel for the attacker to break into additional smart devices that are linked with the compromised gateway device. A denial of service assault is used as an example in this scenario to investigate how a UAV may hack into smart hospital Wi-Fi routers and other wireless systems. The unmanned aerial vehicles (UAVs) are built with the capability of disrupting the wireless signal that runs between the device controllers and the gateway device. After the signals are disrupted, the link between the UAVs and the hospital control system will be severed, and the UAVs will assume control of the whole hospital control system.

10 Conclusions

An age of autonomous aerial vehicles is about to begin as a direct result of the current trend and exponential rise in the usage of unmanned aerial vehicles and drones. The use of unmanned aerial vehicles and drones brings a number of benefits to both the military and the civilian sectors. Despite this, substantial issues over privacy and safety have arisen as a direct result of the widespread usage and accessibility of the internet. These gadgets have become particularly valuable instruments for deceitful actions as a result of their adaptability, cheap cost, simplicity of deployment, and mobility. These vehicles (UAV/drone) are still quite effective for carrying out damaging acts, despite the availability of various defenses against the malicious use of these vehicles. There are also extremely serious concerns about privacy when it comes to UAVs and drones. In today's technology era, protecting one's privacy is one of the most important concerns for both people and businesses.

Because they are autonomous, flexible, and easy to use, as well as having a low cost and energy consumption, drones and unmanned aerial vehicles have ushered in a new era of aviation that features autonomous aerial vehicles in both the civilian and military spheres. This has resulted in a multitude of benefits, including economic, commercial, and industrial, and it has led to a new era of aviation overall. However, the widespread usage of these technologies has resulted in a multitude of safety, security, and privacy concerns. These concerns have surfaced in the form of a variety of cyber assaults, threats, and problems, all of which are described in this article. This report included a complete analysis of these (security and privacy) issues, which included an outline of the reasons that are driving these concerns along with potential countermeasures. The study also included a variety of suggestions, one of which was the use of already available blockchain-based solutions. These technologies may offer increased data integrity, authenticity, and accessibility to unmanned aerial vehicles and drones. According to the findings of the UAV tests, there are four potential security risk mitigation strategies that should be used to protect medical BAN and IMD devices in addition to other Wi-Fi enabled equipment in hospitals from being compromised by an external agent. These four strategies for risk reduction are examples of the latter kind of security approach and entail the addition of additional security features to the device in question via the use of programming.

References

1. Bombe MK (2020) Unmanned aerial vehicle (UAV) market worth $21.8 billion by 2027- pre and post COVID-19 market analysis report by Meticulous Research. Retrieved from https://www.meticulousresearch.com/download-samplereport/cp_id=5086. Accessed on 18 Aug 2022
2. Kumar R, Kumar P, Tripathi R, Gupta GP, Gadekallu TR, Srivastava G (2021) SP2F: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. Comput Netw 187:107819
3. CyanogenMod (2017) CyanogenMod android operating system. Retrieved from https://github.com/CyanogenMod
4. Dinan S (2017) Mexican drug cartels using drones to smuggle heroin, meth, cocaine into U.S.—Washington Times. Retrieved from https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-usingdrones-to-smuggle-heroi/
5. DJI (2018) Phantom 3 Professional—specs, FAQ, tutorials, downloads and DJI GO—DJI. Retrieved from https://www.dji.com/phantom-3-pro/info#specs
6. Irizarry MJ, Gheisari B (2012) Walker, usability assessment of drone technology as safety inspection tools. Electron J Inf Technol Constr 17:194–212
7. Bowden M (2013) How the predator drone changed the character of war. Smithson Mag. Retrieved from https://www.smithsonianmag.com/history/how-the-predatordrone-changed-the-character-of-war-3794671/. Accessed on Nov 2022
8. O'Donnell S (2017) Consortiq. Retrieved from https://consortiq.com/short-history-unmanned-aerialvehicles-uavs/. Accessed on Nov 2022
9. Chen R, Yang B, Zhang W (2020) Distributed and collaborative localization for swarming UAVs. IEEE Internet Things J 8:5062–5074
10. Gartner (2018) Gartner says worldwide sales of smartphones recorded first ever decline during the fourth quarter of 2017. Retrieved from https://www.gartner.com/newsroom/id/3859963gnuplot.(2017).gnuplottool. Retrieved from http://www.gnuplot.info/download.html
11. Rambling D (2017) Islamic state now using off-the-shelf drones I. Defense content from Aviation Week. Retrieved from http://aviationweek.com/defense/islamicstate-s-new-weapon-choice-shelf-drones
12. Horsman G (2016) Unmanned aerial vehicles: a preliminary analysis of forensic challenges. Digit Invest 16:1–11. https://doi.org/10.1016/J.DIIN.2015.11.002
13. Jain U, Rogers M, Matson ET (2017) Drone forensic framework: sensor and data identification and verification. In: 2017 IEEE sensors applications symposium (SAS). IEEE, pp 1–6. https://doi.org/10.1109/SAS.2017.7894059
14. Karlsson K-J, Glisson WB (2014) Android anti-forensics: modifying CyanogenMod. In: 2014 47th Hawaii international conference on system sciences. IEEE, pp 4828–4837. https://doi.org/10.1109/HICSS.2014.593
15. Kernel (2009) Linux_2_6_32—Linux Kernel Newbies. Retrieved from https://kernelnewbies.org/Linux2_6_32
16. de Croon GCHE, Groen MA, De Wagter C, Remes B, Ruijsink R, van Oudheusden BW (2012) Design, aerodynamics and autonomy of the DelFly. Bioinspir Biomim 7:025003
17. Chan KW, Nirmal U, Cheaw WG (2018) Progress on drone technology and their applications: a comprehensive review. AIP Conf Proc 2030:020308
18. Berg TR (2020) Air Space Mag. Retrieved from https://www.airspacemag.com/daily-planet/first-map-compiledaerial-photographs-180973929/. Accessed on Nov 2022
19. Ali BS, Saji S, Su MT (2022) An assessment of frameworks for heterogeneous aircraft operations in low-altitude airspace. Int J Crit Infrastruct Prot 37:100528
20. Wright S (2019) Ethical and safety implications of the growing use of civilian drone. UK Parliament website (science and technology committee)
21. Coach U (2020) Master list of drone laws (organized by state and country). Retrieved from https://uavcoach.com/drone-laws/. Accesses on Nov 2022
22. Aljehani M, Inoue M, Watanbe A, Yokemura T, Ogyu F, Iida H (2020) UAV communication system integrated into network traversal with mobility. SN Appl Sci 2:2749

23. Cheaw BH, Ho HW, Abu Bakar E (2019) Wing design, fabrication, and analysis for an X-wing flapping-wing micro air vehicle. Drones 3:65
24. Teoh ZE, Fuller SB, Chirarattananon P, Prez-Arancibia NO, Greenberg JD, Wood RJ (2012) A hovering flapping-wing microrobot with altitude control and passive upright stability. In: Proceedings of the 2012 IEEE/RSJ international conference on intelligent robots and systems, Vilamoura-Algarve, Portugal, pp 3209–3216
25. Professionals, drones and remotely piloted aircraft (UAS/RPAS)-frequencies and radio licenses, Traficom (2021). Retrieved from https://www.traficom.fi/en/transport/aviation/drones-and-remotely-piloted-aircraft-uasrpasfrequenciesand-radio-licences. Accessed on Nov 2022
26. Carnahan C (2014) ISO/TC 20/SC 16 unmanned aircraft systems. Retrieved from https://www.iso.org/committee/5336224.html. Accessed on Nov 2022
27. Luo A (2016) Drones hijacking. Dejean. Maarse M, Sangers L, Ginkel JV, Pouw M (2016) Digital forensics on a DJI Phantom 2 Vision + UAV
28. Majendie A, Chia K (2018) The future of flying is all about drones—Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-02-08/in-the-global-game-of-hideand-seek-the-drones-are-winning
29. Parrot (2017) Quad copter AR drone 2.0 power edition I. Parrot Store Official. Retrieved from https://www.parrot.com/uk/drones/parrot-ardrone-20-power-edition#parrot-ardrone-20-power-edition-details
30. Hartmann KSC (2013) The vulnerability of UAVs to cyber, in cyber conflict (CyCon). In: Proceedings of the 2013 5th international conference, Tallinn, Estonia
31. Abdullah, Q.A. Introduction to the Unmanned Aircraft Systems. Available online: https://www.eeducation.psu.edu/geog892/node/643 (accessed on November2022).
32. Mikelionis L (2018) Drug cartels using drones to smuggle drugs at border. Fox News. Moskwa W (2016) World drone market seen nearing $127 billion in 2020. PwC Says—Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-05-09/world-drone-market-seennearing-127-billion-in-2020-pwc-says
33. Pleban J-S, Band R, Creutzburg R (2014) Hacking and securing the AR drone 2.0 quadcopter: investigations for improving the security of a toy
34. Creutzburg R, Akopian D (eds) International society for optics and photonics, vol. 9030, p 90300L. 10.1117 / 12.2044868
35. Pilot (2022) What's the difference between drones, UAV, and UAS? Definitions and terms. Pilot Institute. Retrieved from https://pilotinstitute.com/drones-vs-uav-vs-uas/. Accessed on Nov 2022
36. Carrier B (2002) Open source digital forensics tools: the legal argument