Safety and Security Issues in Employing Drones

Durga Prasad Srirangam, K. Hemalatha, Ashok Vajravelu, and N. Ashok Kumar

Abstract The use of drones has been steadily growing over the past few years, not only in a variety of businesses and governmental organizations but also among private individuals. This is due to the rapid deployment of drones for a variety of applications, which can be accomplished by merely attaching the application-specific devices to drones, which are typically controlled by a remote or a smartphone. However, the breakthroughs that have been made in the use of drones have also opened up security challenges. In many applications, the orders that are sent to the drones and the data that is transmitted from the drones are not encrypted. As a result of the fact that drones are also used for illegal and criminal activities by bad actors, it is necessary to add technology for attack detection, protection, and preventive countermeasures in drones, in addition to regulation on the usage of drones through law enforcement by the government agencies. In this chapter, we will analyze the exploiting of drone vulnerabilities such as GPS spoofing, Downlink intercept, and Data exploitation. Additionally, we will examine how to neutralize threats and countermeasures that should be addressed for the safety of the drones.

D. P. Srirangam
Department of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India
e-mail: prof.srirangam@gmail.com

K. Hemalatha
Department of Electronics and Communication Engineering, Kongu Engineering College, Erode, India
e-mail: khemalatha.ece@kongu.edu

A. Vajravelu (✉)
Department of Electronics, Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
e-mail: ashok@uthm.edu.my

N. Ashok Kumar
Department of ECE, Mohan Babu University (Erstwhile of Sree Vidaynikethan Engineering College), Tirupati, Andra Pradesh 517102, India
e-mail: ashoknoc@gmail.com

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_4

Keywords Drones · Security · Unmanned aerial vehicle (UAV) · Jamming attack · Spoofing attack · Data interception attack · KeyLogging attack · MSG injection attack · Eavesdropping attack

1 Introduction

UAVs Security Issues

As a result of recent improvements in technology, unmanned aerial vehicles (UAVs) are now capable of carrying out critical, difficult, and intricate missions. Because of this, they have a lot of security problems, which leaves them vulnerable to attacks that might be quite damaging. Additional attacks are carried out in an effort to gain control of the UAV or to destroy it. The severity of the repercussions is proportional to the nature of the attack. There are not many tools that might be used as hacking tools [1]. As an element of the Internet of Things ecosystem, researchers began beefing up the security of unmanned aerial vehicles (UAVs). In general, it necessitates the efficient construction of a variety of approaches connected to the many IoT deployment and connection regions. In this part, we focus on security and privacy concerns associated with UAVs, as well as attacks carried out by UAVs. This section discusses the use of unmanned aerial vehicles (UAVs) to launch system attacks as well as UAVs charging system attacks. In this section, we also explain the reasons that led to our work on battery depletion attacks against UAVs. The research findings that were discussed before, which will be used in the next subsections, indicate a variety of worries and problems with UAVs. These study studies evaluated a variety of distinct forms of attacks, in addition to several outcomes.

UAVs Security Concerns

When dealing with any form of digital technology, the most important thing you can focus on is keeping yourself safe. To ensure the safety of the UAV system, it is essential to perform the necessary preventative measures. UAV systems are vulnerable to cyberattacks and the deterioration of their functions, both of which have a direct impact on the key contributor. Therefore, attacks on the system or failures in the system lead to significant problems. Park et al. [2] discusses a variety of security concerns in further detail. In these kinds of situations, the attacker causes disruption to the availability, integrity, and confidentiality of the drone. Due to the fact that private information has been revealed, it is now quite easy for a competitor to establish the sensitive information that pertains to the UAV. In addition, the authors in [3] demonstrated that UAV networks are vulnerable to attacks and sensor flaws, proving that UAV networks are sensitive. It is possible for the adversaries to gain access to the communication lines of the UAV, which would then enable them to connect and take control of the UAV. Canis [4] highlighted a variety of different kinds of attacks and categorized them into two broad sectors based on the components of UAVs that were targeted and the attack route. Canis [4] also highlighted a number of different kinds of attacks. There are two types of vector attacks: those that are carried out physically and those that are carried out remotely. A swarm of unmanned aerial vehicles (UAVs) was disrupted during strikes staged at Russia's Hmeimim airfield in 2019. This is only one example of the myriad effects that might result from security flaws. 13 hostile fixed-wing unmanned aerial vehicles (UAVs) were sent to attack the airbase itself. It has expanded throughout a broad variety of areas in Syria, including the Latakia Governorate, the town of Hmeimim, which is located close to Latakia, and a range of 250 km. Despite this, the vulnerabilities that are already there allow attackers the opportunity to become more skilled and proactive in their activities.

1.1 Attacks on UAVs-Based Systems

The systems that are used by UAVs are comparable to those that are used by other IoT systems that are currently in use. They must utilize a centralized server in order to store data and connect to a network in order to carry out wireless communication. In the event that the system is attacked, the mission of the UAV will be terminated, which is a vulnerability in the security. The primary purpose of attacks against systems based on UAVs is to either crash the system or modify the data that is stored on the system. There are a variety of cyberattacks that may target systems based on UAVs, including the following:

Jamming attack: GPS Jamming, Control Stream Jamming, and Data Stream Jamming are the three forms of jamming that are associated to this attack, which comes in at number two on the list of most prevalent attacks [1, 4–8]. The opponents look for Radio Frequency (RF) signals broadcasting in the same frequency range as the drone that is being attacked, and then transmit transmissions that are incompatible with those signals. The attack is organized utilizing nodes that are based on a wireless channel concept in order to accomplish range-based localization. The antenna on the jammer may receive signals coming from any direction. This antenna will transmit radio frequency signals in a manner that is uniformly radiated in all azimuthal directions. An research that was reported in shows that it is not always safe to utilize specific transmitters in order to intercept remote control signals. This is the case even if the jammer is located far closer to the UAV than the operator who is in charge of commanding it using the remote controller. An anonymous individual performed a GPS Jamming attack on May 10, 2012, in South Korea, while testing [4]. This attack was reported to have taken place. During the attack, a rotor based on an Austrian unmanned aerial vehicle known as the Schiebel Camcopter S-100 collided with the ground control station, causing two remote pilots to sustain injuries.

Spoofing attack: The [9] attack is comparable to the jamming attack; however, it has a greater degree of intricacy. Instead of seeking to disrupt existing signals, the adversary will generate false signals in a random but controlled fashion. These signals will then counterfeit and fake the GPS position. As a result, the drone's behavior will be altered as a result of these phony signals, and it will be guided to a destination that is distinct from the primary course that was planned. It culminates in the victim being bound with bogus data for their latitude and longitude. The process is carried out invisibly, without causing any disruption to the normal functioning of the GPS.

Data Interception attack: The [10] Intercept Data attacks constitute a breach of confidentiality and may have far-reaching repercussions for the drone in question. The exploit gives unauthorized attackers the ability to access data via an unauthorized file reader when the system is in contact, while it is in flight, or while it is at rest. A video containing the stolen information was found by the American military defense in Iraq on the laptop of an activist who had been taken into custody. This led to the identification of a data interception attack in [4]. According to this information, the footage was obtained by utilizing SkyGrabber to intercept the unencrypted communication lines that existed between the several flying UAVs. Consequently, data interception attempts will be carried out whenever a non-secure and easily accessible wireless transmission is used. It is difficult to spot an attack of this kind.

KeyLogging attack: A form of monitoring software is designed to record keystrokes and steal data from a computer. Malicious software that logs keystrokes has emerged on the scene as a form of tracking spyware that collaborates with legitimate software to share resources. Creech Air Force Base in Nevada was the location where [11] discovered a keylogging attack that was carried out against US Predator. It was launched once a connection had been made between the Predator and Reaper ground control stations and a removable hard drive. This will result in the capture and transmission of sensitive information.

MSG Injection attack: This type of attack is known as an integrity attack, and it can be carried out through remote access if the targets are [5, 10]. The process of immunizing genuine faux communications with malicious payloads is known as injecting a malicious payload. The messages are backed by a structure that is an exact replica of the structure of the authentic message. They use a second phony UAV to divert the attention of the GS system as well as the UAV. According to this, the process of deleting messages and the process of modifying messages both use the same injection technique. Injecting malicious software, such as viruses, worms, or Trojan horses, will therefore result in the modification of sensitive data. Specific system technologies, such as StackGuard and StackOFFence, are used to protect unmanned aerial vehicles (UAVs). The first instrument is an automatic adaptive detection and prevention technique, while the second instrument is an attack mitigation mechanism. Both instruments work together to protect against attacks.

Eavesdropping attack: A stealthy and unobtrusive attack on the secrecy of the UAV is represented by the coordinates [5, 7, 12, 90]. It is being construed as an illegal real-time eavesdropping of the communication channels being conducted by the party. Without disrupting the transmission of the network, a hostile vehicle eavesdrops on the conversations taking place between the UAV entities. During this attack, sensitive data is gathered without compromising the quality of the signal received by a genuine receiver. Therefore, listening in on a private network is a breach of privacy. Eavesdropping is referred to as a sort of man-in-the-middle attack. On the other hand, the attacker creates a second network that is associated with the victim and sends messages as if they are chatting with a legitimate person. This makes it seem as if the victim is communicating with a third party.

Distributed denial of service (DDoS) attack: Sending an excessive number of requests during the mission [5, 13] is a popular kind of direct attack that might hinder the availability of the UAV. Through the use of data connections, the adversary might provide erroneous data in the form of continuous requests. As a consequence of this, the ever-increasing volume of network traffic will result in the communication channel becoming overloaded, which will prevent the connection from being established.

Sybil attack: The condition arises when an adversary builds several nodes in the network that are distinct from one another using either stolen or manufactured identities. This action will increase the likelihood that a hostile entity will be able to intercept a routing message and manage the Peer to Peer (P2P) overlay network. Through the use of threats, the adversary may achieve an excessive amount of authority and exert control over the system's performance in all aspects.

Blackhole attack: The sort of attack that [14] falls under is referred to as a denial of service attack, and it is classified as a form of lethal attack. In order to get a route that will continue to flow to the target node, a malicious node will pull all data packets by offering incorrect information in order to gain the route. The information packets are sent to the black hole by the source node, rather than being sent to the node that is designated as the destination. If the nodes are given inaccurate information on the routing data, the protocol for determining routes will be significantly disrupted. As a consequence of this, the adversary will access these packets while the data is being sent via the black hole. The attacker will advertise a large number of false paths in the hope of attracting data traffic. During this specific attack, a directed pull attack will be initiated, and all routing data will undergo a full transformation.

Grey hole attack: The [15] may change their mindset from one of authenticity to one of a sinkhole. A similar idea has been proposed for the grey hole, in which malevolent nodes block the transit of data across the network by broadcasting incorrect routing information. Because of this, it is an expansion of the attack on the black hole. The node might function in either a harmful or a regular state depending on how it was configured.

Fake information dissemination (FID) attack: This event [5] takes place anytime the intruder sends out a bogus GPS signal in order to change the course of the UAV and get data via impersonating. An attacker may carry out a FID attack on a network by creating forged authentication messages by making use of legitimate routing packets that have been obtained from malicious devices. The malicious node's fake injection will result in the destruction of the routing table used by the other nodes. As a direct result of this, the nodes will suffer a loss of packets due to an error in the routing. In addition to that, the pace at which packets are sent will slow down.

Replay attack: A [10, 13] attack is a kind of cyber warfare that is analogous to a denial of service attack and involves either eavesdropping on legitimate data transmissions or slowing them down in order to retransmit altered data in lieu of an intercepted message without first decrypting it. Eavesdropping, keylogging, and notably Sybil attacks are examples of the kind of cyberattacks that have the potential to completely ruin the availability of data throughout the whole system.

Attacks on the UAVs-Charging Systems

A comparable embedded power mechanism is the UAVs charging system [16]. The charging mechanism of the UAV is susceptible to attacks, which might result in the destruction of the whole UAV. These kinds of problems have the potential to halt the functioning of the UAV. Recently, experts have been working toward the goal of improving the safety of the UAV charging system. The author of the work cited in [17] constructed a model that includes an analysis of energy requirements. The algorithm will make an accurate projection of the demands that will be made on the drone based on the amount of energy that will be required to complete the permitted mission. A direct result of this is that this model will be aware of attacks, which will have the effect of lessening the vulnerability of the charging system. Temperature and actual discharge rate are only two of the many factors that have a substantial influence on the operation of the charging system. Because of this, the resistance of the battery as well as the power supply will be altered. In addition, this typical system is vulnerable to a variety of attack patterns, which presents a danger. In addition, defects in voltage control [18] may generate a wide variety of problems for the charging systems of UAVs. Because of this vulnerability, customers might be overcharged or undercharged.

Additionally, it shortens the lifespan of the battery and causes harm to the contributing unit. The unmanned aerial vehicle (UAV) was the victim of an attack in [8], during which the attacker created bogus requests that caused damage to the charging system. It led to a problem with an excessive amount of energy as well as an excessive decrease in voltage. The charger control unit could need to be tampered with, or the data sources might need to be manipulated, in order to achieve this goal. For instance, [8] uncovered a variety of charging system potential concerns, including as the WPT's ineffective functioning. In addition, the authors investigate the attacks that are designed to control the charging process in [19]. The malicious software takes over and changes the software that is utilized by the rapid-charging station when an unmanned aerial vehicle (UAV) is linked to the station. The attack will transform the unmanned aerial vehicles into high-speed chargers and will cause damage to the charging infrastructure. This malicious power strike is sneaky and swift, with little warning or opportunity for resistance. It has the potential to alter the configuration and add more work up to the point where it causes harm to the whole system. As a result, any unmanned aerial vehicle (UAV) that is attached to or linked to the charging station will constitute a threat.

Attacks that Result in UAV Battery Depletion

Depletion of Battery (DoB) [20] is a particular kind of attack that might be used to target UAVs and induce increased power consumption on a variety of different levels. Because of this, failure is difficult to anticipate, and when it does happen, the damage may not be able to be repaired due to the complexity of the situation. According to the first notification, rapid battery depletion may be identified if it was found that there was an unanticipated drop in the amount of remaining battery capacity that was observed between follow-up visits. As a consequence of this, these types of attacks are the most typical reasons for the failure of a mission, and they have the ability to cause a loss of connection as well as a crash. During the course of the attack, many sensors will fail, and several functionality will become less effective until they are completely disabled. The DoB has a much increased risk of an electrical component failing, which will result in a rapid discharge of the battery. UAVs are particularly susceptible to DoB attacks due to the fact that these attacks may take advantage of the UAV's autonomy, its physical motions in the surroundings, its wired and wireless communication channels, or all of these things concurrently. DoB allows the attacker to reveal the software and hardware computing units, as well as the data and physical architecture of the target unmanned aerial vehicle (UAV). Attacks that deprive the target of energy are similar to those that disrupt service (DoS) [21]. Attacks that use denial of service may hasten the discharge of a battery by up to 18.5% [21]. In addition, there is an attack known as Denial of Sleep (DoS) [13] that seeks to accomplish the same thing. It is predicated on limiting the amount of time the UAV spends in sleep mode in order to increase the amount of power consumption until the battery is completely depleted. In addition, the adversary modifies the charge parameter in order to carry out cross-layer attacks [13] in order to drain the UAV battery in an indirect manner. However, there are two different kinds of attacks that drain the battery:

Attacks without physical contact: This first kind encompasses attacks that do not need to have any kind of direct physical contact with the device. These are examples of attacks against wireless channels. Recent attacks are made up of two-channel kinds of energy crisis control systems each. They are known as the control data transmission channel and the GPS data transfer channel respectively. The transmission of GPS data is used in order to ascertain the geographical position of the UAV. As a result, the GPS channel is the focus of the attacker, who uses an Omni antenna to cause interference. The purpose of the attack is to either prevent the signals from reaching the receiving side entirely or to send them with incorrect locations. Additionally, when the UAV gets many commands, it may travel in a haphazard manner, which causes additional drain on the battery. The second channel is used to synchronize instructions with the UAV. These instructions may concern GPS data, network settings, or the overall state of the UAV.

Attacks with physical contact: This kind is discharged when the unmanned aerial vehicle (UAV) is in the standby state. The attack begins from several different entries based on this information, including the physical component, the USB interface, and the microcircuit. Additionally, the invader will compel the main rotors of the UAV to operate at full power and use more charge if they attach a physically enormous weight to the UAV in order to create an imbalance. Finn et al. [22] conducted an experimental investigation to investigate the effect that weight has on the amount of electricity used by UAVs. The first of two unmanned aerial vehicles (UAVs) utilized in the experimental setup had a total weight of 30 kg and 8 motors; the second UAV had extra payloads that brought the total weight up to 35 kg while maintaining the same number of motors. For each test, notes were taken on the movement sets of lifting, hovering, and landing that required the most power. The amount of electricity used is calculated depending on the rotational speed (RPM). According to the findings of this research, the values improved across the board in the subsequent test.

According to [23], there are two different methods that a UAV may be used to launch a denial of service attack:

- The attacker is continually sending requests by providing bogus communication packets in order to fool the target. As a consequence of this, the unmanned aerial vehicle (UAV) will need a percentage of additional energy for the authentication process in order to analyze each request, which will cause the battery to run down.
- By producing electromagnetic (EM) noise with the intention of causing a high mistake rate at the UAV. Because of this, there will be a rise in the total amount of retransmissions, which will result in an increase in energy usage. Because of the increasing noise, the UAV could be compelled to boost its transmission power, which would shorten the battery's lifespan.

There are many different things that may go wrong with a UAV's battery, including overcharging, which can cause the battery to boil, draining, leaking, improper setup, and using up all of the available energy. In addition, there are other contributors to the depletion of energy. For example, the research presented in [17, 24] analyzes the impact that elements such as payload, movement, hovering, communication, and speed have on the amount of energy that is expended. Last but not least, unless the battery of the vehicle is totally drained during the trip, there is a possibility that it will not have enough time to return to the base and efficiently perform its mission. As a result, the logistical operations of the infrastructure can experience a large amount of disruption.

Attacks Assessments of UAVs-Based Systems

A classification system for attacks using UAV-based systems is going to be presented in this part. These attacks are organized into four distinct groups, which are as follows:

1. Attacks directed against the fundamental software
2. Attacks on the monitoring systems
3. Attacks on the various avenues of communication
4. Incursions against the GPS channel.

Proposed taxonomy: The majority of UAV attack types may be categorized according to the kind of attacker, the offenses committed, and the aims of the attack. The modeled chain is an illustration of the series of attacks that are based on UAVs.

The actual act of attacking may be broken down into four distinct steps. An adversary equipped with a relative goal, attack vector, and the ability to define the attack entry. After then, it reaches an attack depth that was previously determined. Last but not least is the attack's effect, often known as the damage it does. This sequence lends credence to the taxonomy that was suggested. The taxonomy provides an overview of all the different types of attacks that may be mounted against the UAV-based system. Every strike is equipped with a unique set of behavior characteristics that are realized to target one or more layers. In particular, the attacker may take advantage of one or more vectors in order to carry out further attacks. These attacks have been categorized according to the preceding chain in order to provide answers to the following questions about their purposes:

- Attacker: Who exactly is the one doing the attacking?
- Attack Vector: What causes it to be activated? Which layer has it established a presence on? What really is the danger? Is it a direct attack, or is it being carried out by a distant auxiliary? Who or what exactly are the targets of the UAV's attacks?
- Attack Type: Describe the characteristics of the attack being made. Are there some attacks that are more specialized than others?
- Attack Offenses: Identifying Vulnerabilities That Were Targeted What were the weaknesses that were exploited? What kind of fallout will there be from the attack? In a manner that is more formal, each dimension of the taxonomy is defined as follows:

Attacker: Attacks may be carried out by a variety of persons or organizations, including terrorists, spies, thieves, and hacktivists, with the intention of achieving a variety of other objectives in a variety of attack locations and positions. Researchers looked at a variety of potential attacker situations for unmanned aerial vehicles (UAVs), including terrorist airstrikes, hijacking, and surveillance. Their findings may be found in [10]. In addition, the report disclosed that UAV thieves were responsible for a recent incident in which Iranian troops stole a US RQ-170 Sentinel. Hacking into unmanned aerial vehicles (UAVs) was done with the use of a software system called SkyGrabber [9]. There are several different UAVs hijacking software programs, such as SkyJack, which were designed to hack and operate the UAV wirelessly by using an autonomous middleware. In addition, the word "Terror by Joystick" that was thrown into the flight path of the airplane sheds light on the nefarious acts that terrorists have carried out using UAVs. As a result, criminals pose a risk that justifies the employment of UAVs to wreak havoc on society.

Attack Vector: Attacks may be conducted using a variety of vectors, such as a direct attack or a distant attack via medium entries. Attacks from a distance intercept data using an auxiliary tool, allowing them to be compromised by questionable internal processes. The control software, the sensors, the communication channels, and the GPS channel are the auxiliary that are being referred to here. These four are the primary targets that attackers aim at most of the time. The entities that are being attacked are the surface, also known as the element that is being targeted by an attack. This component is part of the basic system that the physical vehicle utilizes. Unmanned Aerial Vehicles (UAVs) have a dialogue with the world around them. As a consequence of this, it could take the form of an intrinsic component, a virtual or physical environment, or both.

Attack Depth: The severity of these dangers is determined by their characteristics, which place them into one of four distinct categories of attacks. The opponent intends to get intelligence by infecting the UAV with malware, exploiting it for the aim of acquiring information or anything familiar, intercepting its transmissions in order to break them, and authenticating itself. Threats to computer network security may use data in clandestine ways to accomplish their objectives without the awareness of system operators. The nature of the exploitation, such as injection or modification, may be used to categorize the different types of attacks [11]. In addition, fabrication is included as one of the typical specified methods of attacking authentication [10]. The most recent attack is a bait for the unmanned aerial vehicle (UAV) authenticity, which enables the attacker to get privileged access to the components in order to fabricate bogus information and deliver it to them. There are several various forms of attacks that may modify the content of the UAV or alter its decision-making in the event of specialized attacks.

Attack Offences: As a direct consequence of this, their data will be pilfered, altered, and corrupted. Other crimes can be committed as a result of these attacks, such as data theft, an authentication crime that involves cracking and stealing, and fuzzing, which is when criminals try to find zero-day exploits by using a technique called fuzzing. Because of this, they have the potential to cause fuzzing in the system by interfering with the process, the communication, and the functionalities. As a result, attacks based on UAVs are able to sneak up on targets through a variety of channels by utilizing a planned entry and fixed damage for exit.

Software-based attacks: The processing of data for a decision-making system is the responsibility of software based on UAVs [11]. It is in charge of regulating the sensors, as well as the protocols for navigation and communication, as well as connecting the various components. To a large extent, the base program is the one that is in charge of establishing the flight parameters. Attacks may easily be launched against these components. As a consequence of this, the software that runs the drone base does not have any stringent security features that prevent hostile applications from changing the data. There are many different kinds of software that may be used in attacks, such as the buffer overflow. It is software designed to target the operating systems of UAVs. The attacker searches for memory blocks and then populates those blocks with unnecessary data in order to squander the space that has been allotted for data. Because of this, the system will be forced to execute random codes, which will make it possible to manage and monitor these systems. In addition, other sophisticated attacks on the core program might potentially get critical data. For example, a Structured Query Language Injection, sometimes known as a SQL injection attack, is used against data-driven applications. In addition, some malicious actors choose to begin their attack on the embedded Software Defined Radio (SDR) boards because of the ease with which they may get access to these boards and the lack of protection they provide. In the end, foundation Software security flaws are continuously maintained owing to faults in the microcontroller system, with suitable authentication and permission assessment.

Attacks on the Sensors

The drone is equipped with a variety of sensors that are capable of carrying data and providing readings. Because of this, attackers see sensors as a potential target for their activities. They are using them as the attack surface in order to intercept from them. The data that is being delivered to these sensors is being corrupted as a result of these attacks. "Sensor input spoofing attack" was the name given by the intruders to the attack that they developed in and carried out using sensors. This exemplified the efficacy of attacks mounted against UAVs using the sensors. Additionally, Nichols et al. suggested a method through which the adversary sends bogus data to the drone by means of an onboard sensor in order to throw it off. In addition, in [13], the adversary interferes physically with the UAV sensors in order to disrupt their availability, and then they conduct a DDOS attack. Against the other hand, there have been no recorded attacks on sensors in the form of connected cameras to UAV [4]. However, research such as [11] has shown that the sensor may be protected to protect the data transfer inside the network.

Attacks the communication protocols: In most cases, ground control stations and unmanned aerial vehicles use distinct communication protocols. Micro Air Vehicle Link (MAVLink) protocol, UranusLink, and UAVCAN are the most important communication protocols. The following is a list of the vulnerabilities and failures that are associated with these protocols:

MAVLink: A library for marshalling data that was developed with the intention of establishing a lightweight message serialization mechanism. It has the highest level of support among its contemporaries. In addition to the fundamental ideas, this protocol suffers from a striking deficiency in the presence of structured references. In spite of the fact that certain dangers are there, there is no safeguard in place to ensure that the communications that are sent are accurate. In addition, the security surrounding the transmission of the communications is subpar. Because of this, it is necessary to strengthen the security of the end-to-end connection between the GCS and the UAVs.

UranusLink: Is a protocol that handles data in packets and can produce both unreliable and reliable services. This protocol is very different from the other protocols already in use for interacting with UAVs. It includes the checksum that can be used to verify that the original message was transmitted successfully and that it was received. However, it was unable to check whether the message had been altered in any way. As a consequence of this, a straightforward checksum does not guarantee the secrecy or integrity of the data. On the other hand, there is a lack of sufficient experimental evidence to support the UranusLink hypothesis.

UAVCAN: Is a protocol for controller area network that is based on the CAN bus and is available as open source. Its purpose is to provide private communication while using reliable car networks. Due to the lack of shielding that the protocol offers, it is not advised for use in sensitive missions or on the system. 6.5. Attacks made against the GPS channels are used to carry out attacks on wireless networks, including GPS Jamming and GPS Spoofing. Emulators of computers were used in each of these most recent attacks. There is a variety of jammers available. First, there is the basic constant jammer, which sends out a signal of continual interference using the default amount of power. Additionally, a straightforward regular jammer that has a high-power transmission that is distributed in packets. The continual transmission may provide the impression of a higher capacity than it really has. The random jammer only makes sporadic transmissions, which brings us to our second point. Both high power and moderate power appraisals are problematic in their own ways. In addition, the complex jammer may be used to describe a reactive jammer. In this particular type of jammer, the signal won't be transmitted until the transmission target has first been established and then identified. In addition, the intelligent jammer is one that possesses prior knowledge of the leverage protocols and modulation that are currently being used. In conclusion, ensuring the safety of the GPS channels is very necessary for the UAVs to successfully complete the task.

GPS-Spoofing Attack Detection Technology

For Guidance, Navigation, and Control, Unmanned Aerial Vehicles (UAVs) of today mainly depend on the Global Navigation Satellite System (GNSS) (GNC). When it comes to the GNSS choices that are now accessible, the Global Positioning System (GPS) is the satellite navigation system that is most extensively adopted and used. Autonomous unmanned aerial vehicles (UAVs) are even more reliant on flying aids such as autopilots, navigational systems, and dynamic positioning systems than traditional UAVs. In addition to its well-known precise location function, the Global Positioning System (GPS) also provides time synchronization to an accuracy of around 10 billionths of a second by making use of the atomic clocks that are carried by the satellites themselves (Wei and Sikdar 2019). Time-sensitive systems, like synchrophasors found in power grid systems, use GPS time in order to conduct offline engineering assessments and synchronous state estimations [25]. All of these technologies have been developed with the presumption that the GPS services may be trusted (Bhatti and Humphreys 2017).

In order for unmanned aerial vehicles (UAVs) that rely on GPS to operate safely, the location information they receive must be precise, reliable, and continuous. However, a number of studies have demonstrated that it is possible to fake or disrupt GPS signals due to the inherent flaws and weaknesses that are present in the system. It is simple to interfere with GPS services by transmitting high-power jamming signals in the direction of the victim platform due to the low signal strength, which is approximately − 130 dBm. Because the civil GPS services do not have encryption or authentication mechanisms, it is simple to replicate or fabricate the satellite signals, which can then be used for the launch of sophisticated GPS spoofing attacks. This is because the signals can be easily replicated. In addition to this, the civil GPS services do not have any authentication mechanisms.

GPS spoofing is the process of recreating or falsifying the creation of the GPS signals in order to trick a particular GPS device or receiver by altering its Position, Velocity, and Timing (PVT) characteristics. This is done in order to mislead the device or receiver. This is done with the intention of tricking the GPS device or receiver that is in issue (Psiaki and Humphreys 2016). As a result of the spread of low-cost, user-tunable Software Defined Radios (SDRs) and online open source projects and tutorials for hobbyists and newcomers, it is now possible to launch GPS spoofing attacks against UAVs. This begs for more robust spoof-resilient safeguards to be included in from the beginning, especially for the sake of the safety of mission-critical aerial applications (Huang and Yang 2015).

If an attempt to spoof a drone's GPS coordinates is successful, the attack could result in the drone crashing or the flight path being altered, both of which are potentially disastrous outcomes. According to the findings of a number of studies, an adversary can force a GPS-guided drone to deviate from its course or even hijack it if the adversary is aware of the drone's current position and intended travel path (Noh et al. 2019). These findings were reached by Seo et al. and Noh et al., respectively. By using spoofing, it is possible to circumvent the safety feature known as "Geofencing," and as a result, the targeted drone may be coerced into flying in restricted airspace (Schmidt 2015). This weakness may be used by drug smugglers and others in order to violate regulated boundaries between prisons for the purpose of selling drugs and conducting unlawful surveillance (US National PNT Advisory Board 2018). If a military-grade unmanned aerial vehicle (UAV) that is armed is somehow stolen and then utilized by a terrorist group, the resulting devastation might be catastrophic (Fig. 1).

The Department of Homeland Security (DHS) carried out an unclassified test exercise on June 19, 2012 at White Sands Missile Range (WSMR) under the codename "GYPSY". This was the first time that it was proven that civil GPS systems are susceptible to spoofing attacks, and it was the first time that this vulnerability was demonstrated [25]. During that particular exercise, a GPS spoofing attack was carried out at a height of forty feet against the mini-drone known as "Hornet," which resulted in the manipulation of "Hornet's" perceived position and time. This attack was carried out at a height of forty feet. When an American RQ-170 Sentinel drone was successfully seized by the Iranian Army (Hartmann and Steup 2013), another significant GPS spoofing allegation was made against a military-grade UAV by the Iranian Army. On the other hand, the veracity of the allegation as well as the specifics of how the UAV was taken are not confirmed and are a source of controversy. In 2016, it was claimed that Mexican drug dealers and traffickers had deceived an unmanned aerial vehicle (UAV) belonging to the United States Customs and Border Protection agency via a spoofing attack on its GPS signal (Khan 2020). Additionally, comparable GPS-based spoofing attacks have also been proven in a number of other publications (Zheng and Sun 2020) against Hornet Mini, DJI's Matrice 100.

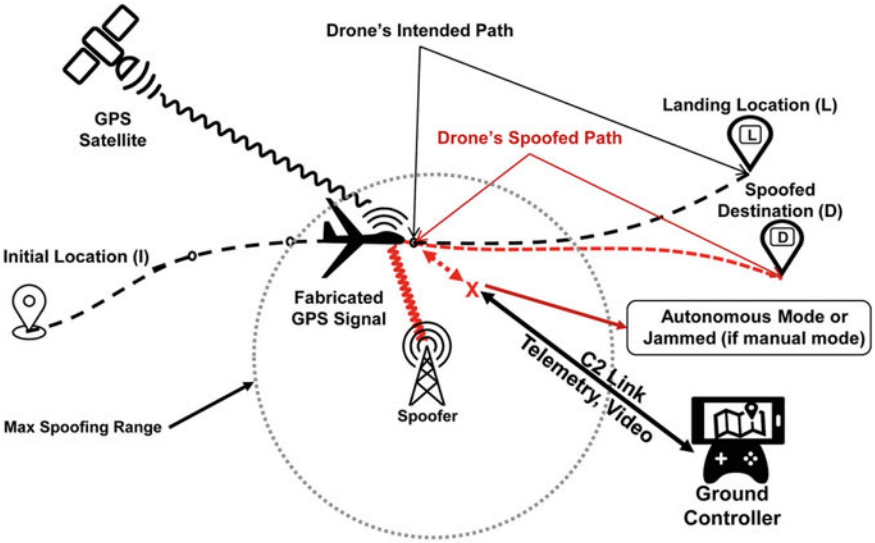

Fig. 1 GPS spoofing

1.2 Development of GPS Anti-Spoofing Technology Components for UAVs

In this section, we will talk about the internal architecture of a software package that is able to put our GPS anti-spoofing solution into action. This software package is capable of preventing spoofing by using our approach. The internal architecture is comprised on two primary parts, both of which were discussed before. They are a piece of software that can simulate attacks and another piece of software that can detect attacks (analyzer).

To begin, let's have a look at the overarching structure of the software application, which can be shown in Fig. 2.

The attack simulation software module on the left provides, as can be seen from the picture, the entire capability that enables an interchange of data with other modules. This is made possible by the module's provision of the leftmost slot. A database is also used to store the information that was obtained from the navigation system. The provision of extra redundancy requires that this step be taken. The data are not lost in the event that there are issues with communication between the attack simulation software module and the attack detection module (analyzer). The green square represents the interface that allows data to be transmitted from the module that analyzes attacks to the module that simulates attacks. The module for updating publications, which can be identified by the presence of a gray rectangle, is designed to transmit information on the attack to the control system. The updated subscriber (shown by a rectangle in orange), which is responsible for receiving data from the field controller, then sends that data to the raw data processing module (indicated

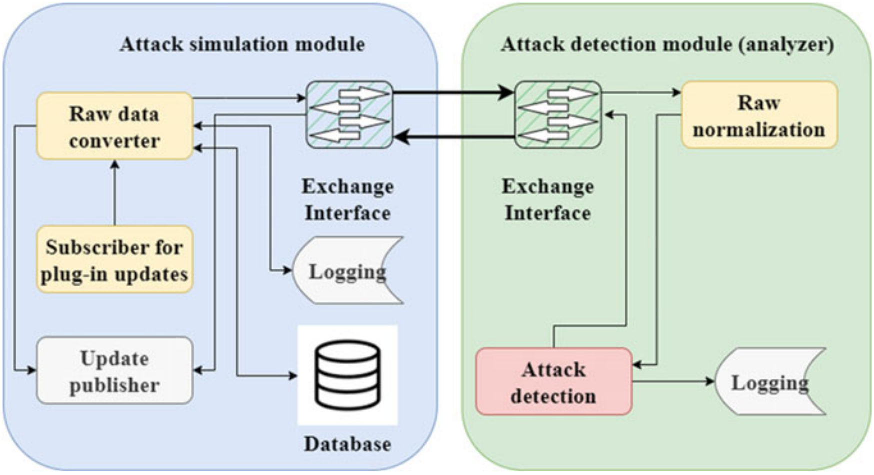

Fig. 2 Software application of attack simulation module

by a rectangle in yellow), which is responsible for normalizing the data. After the raw data have been translated, they are then transferred to the analyzer module via the interface (which is represented by a green square). At this point, the data are either normalized or communicated to the attack detection module, depending on which module is highlighted with a yellow rectangle (pink rectangle). A logging log is maintained by the attack detection module, which is required for the debugging process. The data are sent over the interface to the publishing module in order to alert the control system about the present status of the unmanned aerial vehicle (UAV), which occurs either when an attack is detected or when the behavior is normal.

Because the attack detection module is independent from the attack simulation software module, and because there is a client/server connection between the two, it is essential to anticipate any dangers that may be caused by this link. Even if the interaction is programmed at the software level, every external contact between modules carries with it the risk of a connection failure, delays, data loss, blockage of communication, or a break in the channel. This is true even if the interaction is implemented at the software level. For the purpose of gathering data and issuing control directives, ROS2 was selected to serve as an interlayer between the flight controller and the control board. The flight controller is responsible for providing the GPS spoofing attack simulation software module with any new information. The attack simulation module is a subscriber to the control module and receives instructions for establishing or altering parameters from it. These commands come from the control module. Tabular representation of the parameters received from other systems for use in analysis may be found in Table 1. As soon as it has an update, the attack simulation module immediately begins sending data to the analyzer in a sequential fashion. In this scenario, the attack simulation module will continually keep waiting for the analyzer to provide a response to the data that it has received.

Table 1 The set of parameters for analysis

Number	Description	Range of values
1	The speed after GPS satellite positioning	(0; 40), 0.1 m/s
2	GPS track angle	(−180, 180), degrees
3	GPS satellite number	(0; 34)
4	GPS altitude	(0;1000), unit 0.1 m
5	Integrated navigation latitude	(−90;90), 0.0000001 degree
6	Integrated navigation longitude	(−180;180), 0.0000001 degree

As a result, the attack simulation module not only manipulates the data, but it also functions as a layer between ROS2, external UAV modules, and the attack analyzer. This technique lessens the strain placed on the attack analyzer while simultaneously boosting the processing speed necessary to identify an attack.

As a result, the primary information that is received from the flight controller will be moved to its own subject that is specifically designed for subscribers, and information on the pace of the flight will also form its own topic. Both of these subjects are followed by the software component that simulates an attack using GPS spoofing.

The module of the attack simulation program allows for the generation of datasets based on various factors. At the same time, the module may switch between three distinct modes of operation, each of which is determined by the level of strength of the attack. The state of having no enemy attacking you is referred to as the initial mode. In this setting, no data will be created at all. The attack simulation may be canceled out completely by activating this option. The second mode is one that does significant damage. This mode represents a circumstance in which the values of every parameter, with a few notable exceptions, are liable to change. A mild attack constitutes the third mode. This mode is equivalent to a scenario in which data for just the most fundamental characteristics, such as the GPS noise level, the number of GPS satellites, and the GPS flight altitude, are fabricated (Fig. 3).

1.3 Experimental Research Methodology

The following are some of the most important and desirable qualities that should be present in a system that can defend against GPS spoofing attacks by simulating their impact on an unmanned aerial vehicle (UAV):

- Timely notification of the beginning of an attack;
- Accuracy of attack detection;

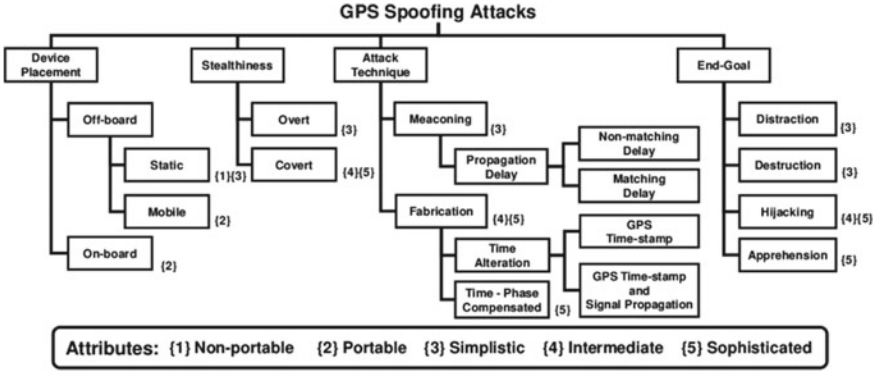

Fig. 3 Taxonomy of GPS spoofing attacks

- The plausibility of the forged attack data;
- The amount of time spent simulating the data.

The time relative to the beginning of the attack and the time the notice was sent to the operator are taken into consideration to decide whether or not the notification was delivered in a timely manner. In addition, there shouldn't be any dire effects for the unmanned aerial vehicle (UAV) itself for a certain amount of time. Using mistakes of the first and second type, estimations of the confidence interval, and testing hypotheses against confidence intervals, the accuracy of attack detection may be evaluated and improved.

The likelihood of making a type I mistake refers to the wrong rejection of the null hypothesis, sometimes known as a "false alarm". Type I errors occur when researchers incorrectly reject the null hypothesis. In this particular scenario, we are discussing the process of notifying an attack while simultaneously seeing no changes related with the attack itself. The possibility of staying within the bounds of the null hypothesis even when it is demonstrably false is an example of type II mistake (also known as "missing a goal"). In the context of this discussion, we are referring to a scenario in which an attack is carried out, but the system views the condition as being entirely normal.

The following accomplishments were made toward the goal of tackling the challenge of building a GPS spoofing detection mechanism for unmanned aerial vehicles (UAVs):

- An initial investigation was carried out, which paved the way for the development of a mathematical framework for the purpose of resolving the issue.
- A set of cyber-physical parameters that may be used to identify an attack was established as a consequence of conducting an analysis of parameters and techniques of data normalization. This set of parameters can be used to determine whether or not an attack has occurred.

- An investigation of the Kullback–Leibler divergence measure, which was used in the search for anomalies, was carried out. As a result, the quality of anomaly identification has been made much better.
- A novel technique for detecting attacks based on the characteristics of the sensor system of an unmanned vehicle has been presented. This technique enables the UAV to identify an attack in real time and independently without the requirement for previous information about the reference change of sensor values. The value of entropy, which may be thought of as the difference in the probability distributions of cyber-physical characteristics, is what serves as the foundation for this approach to problem solving.

As a part of the process of finding a solution to the problem of developing the architecture of anti-spoofing technology, the architecture of anti-spoofing technology for OS ROS2 was developed and described. It was constructed as a result of the publisher-subscriber concept, and it can be distinguished by the following characteristics:

- The use of this technology should allow for the detection of an attack, as well as the notification of the operator and any essential subsystems of the UAV about the fact that an attack has occurred. After receiving word of an attack, UAV control systems have the responsibility of ensuring that countermeasures are put into effect.
- It is not necessary to establish and record changes in indicators during normal operation in order to detect an attack using this technology. Instead, the system must ensure the recording of anomalies in real time by analyzing the degree of change in indicators obtained over the course of the previous period of time and for the period of time that is currently being measured. This is one of the features of this technology.
- The following activities need to be completed before the technology may be implemented: an interface has been developed for the purpose of collecting data on the state of the navigation system, which is required to detect a change in its state, from the flight controller or any other subsystem that can provide the required data set, the format and types of values transmitted parameters, the possibility of implementing a GPS spoofing attack on the simulation model is provided, and its effective parameters are determined; the possibility of transmitting a signal about the fact that the navigation system has been compromised; and the possibility of transmitting a signal about When compared to other methods, our approach provides a better level of accuracy in the detection of attacks. In addition to this, it is simpler to put into action, and one does not need a significant quantity of data in order to construct a decision-making system or train a neural network. Support Vector Machines, for instance, provide detection accuracy of up to 80%. A detection accuracy of up to 90% may be achieved using the deep learning approach in conjunction with the support vector machine [8]. The accuracy of our attack detection approach for a fleet of UAVs may reach as high as 96%, but at the same time, it has a false positive rate of 3.5%. Additionally, in our plan, unmanned aerial vehicles (UAVs) do not function independently, and the

system operates at the level of both UAVs and base stations to identify potentially dangerous deviations.

1.4 Secure Communication in UAVs

There is no need for extra assistance from the network infrastructure to use UAVs for the purpose of conducting surveillance over a vast region. Communication between the UAVs and the GCS allows for the continuous transmission of vital information while the UAVs are in flight. The dynamic topology brings forth additional difficulties as a result of the information that is being exchanged. The transfer of data from one node to the GCS is often handled by unmanned aerial vehicles (UAVs). The data that is being transferred is susceptible to several types of attacks. The majority of sensitive information in military applications is sent between two authorized users through wireless communication channels. This occurs in the majority of military applications. Due to the fact that the wireless channel is an unsecured medium, it is quite feasible to access the information by means of launching cyberattacks such as those targeting the integrity, availability, and confidentiality of the data. Multiple kinds of security protocols are used to encrypt the data transfer and verify the identities of the users in order to shield it from the prying eyes of potential adversaries. For instance, symmetric and asymmetric security protocols are used in order to ensure the confidentiality of the communication that takes place between the UAV and the GCS.

The encryption and decryption processes can only be carried out successfully with the usage of a single private shared key when using symmetric security protocols. While utilizing asymmetric security protocols, two distinct keys, one of which is kept secret and the other of which is kept public, are used. When anything is encrypted, a public key is used, whereas a private key is necessary for decoding. In sections II-A1 and II-A2, respectively, more coverage is given to these two distinct categories of security procedures. The authentication methods that are used to verify the identity of the transmitter are also discussed in Section IIA2 of the document. This is done to assure that the message that was received is genuine and was not delivered by an adversary. Lightweight authentication procedures are discussed in Section II-A3, which is intended for usage in situations that demand less memory and a lower level of computational complexity.

1. **Cryptographic Symmetric Security Protocols**

   Cryptographic methods are used often these days because of their capacity to guarantee availability, integrity, and secrecy. In particular, symmetric protocols are used in order to secure the protection of sensitive data, which may include text, photos, audio, or video. In symmetric security protocols, the information is encrypted using the same key that is used to decode it; this means that both the sender and the recipient of the information need to have the same key in order to access the original data. The employment of symmetric security protocols, such as the one time pad (OTP), is common practice when it comes to ensuring the safety of data transmissions. OTP mandates that the key size correspond exactly to the size of the data that has to be protected. In the context of pictures, for instance, if an image has M rows and N columns of pixels, the length of the key has to be equal to the length of the original image, which may be expressed as M times N. The OTP encryption is used to further bolster the safety of the wireless communication MAV connection described in reference [26].

A function that encrypts and decrypts the data is used in order to ensure the data's safety during transmission. The unmanned aerial vehicles (UAVs) may be controlled via a variety of instructions, such as "start UAV," "takeoff command," and "autopilot enable." These directives are all in the form of bits, which may be either 0 or 1, depending on how they are represented. When all of the bits are put together, a lengthy text is produced, which may then be encrypted using a specific method for more protection. OTP-based encryption systems each have their own set of advantages and disadvantages. For example, the size of the key has to be exactly the same as the length of the data. It is necessary for us to provide the key to the recipient if we are going to deliver data of a significant amount. As a result, the distribution of keys becomes problematic since it uses up a lot of bandwidth. In addition, the key may only be used once, which implies that for every safe transfer, a new key is required [26]. This necessitates the creation of new keys.

Applying several resilient transformation methods like discrete wavelet and discrete cosine transforms, for example, may make the system that is described in [26] more secure. These techniques can be used to enhance the scheme. Initially, the original message is changed into new frequency coefficients, which are entirely distinct from the original message. In addition, transformation carried out via the use of frequency coefficients is much quicker than transformation carried out directly on the original message [27, 28]. In the paper [10], a chaotic Lorenz system is utilized to encrypt and decode the original communications, as well as the messages that have been altered. Unpredictability over the long run is a feature of chaotic Lorenze systems, which also have the capacity to produce additional randomness by even minute adjustments to the seed values. The unmanned aerial vehicle (UAV) is responsible for gathering the data from the sensors and camera, after which it transmits the information to the Lorenz chaotic based encoder. It does not encrypt the raw message in an immediate manner. The information is first reduced to a form that can be understood in bits, and then it is encrypted. Up to the very end of the original data, the bits are constantly encrypted. Following the completion of the encrypting procedure, the UAV then delivers the information that has been encrypted to the receiver. The receiver then decrypts the information by following the opposite procedure of the chaotic Lorenze system. The suggested encryption method has a symmetrical structure, which means that the key that was used to encrypt the data in its original form by the sender is also used by the receiver to decrypt the data. Having said that, the procedure that was suggested [10] also has a few flaws. For instance, the suggested method does not include any kind of procedure for scrambling the data. In point of fact, the safety of any encryption method is contingent not only on the level of confusion (scrambling), but also on the level of diffusion [20].

2. **Cryptographic Asymmetric Security Protocols**

   When it comes to security, asymmetric protocols make use of two distinct keys. The first is known as the public key, while the second is known as the private key. The information is encrypted with the public key and decrypted using the user's private key. This process is performed by the user at both the transmitter and receiver ends. It is not required to keep the public key a secret due to the fact that once the information is encrypted using the public key, it cannot be decoded with the same public key that was used to encrypt it. Instead of the public key, retrieving the information requires the use of a secret key, also known as a private key. The authors of [1] propose a data authentication protocol that makes use of an asymmetric key algorithm technique in order to check whether the data received by the UAV was sent from the authentic ground station or the eavesdropper. This allows the authors to check whether the data was sent from the authentic ground station or the eavesdropper.

   For the purpose of ensuring that communications sent between the UAV and the GCS are not intercepted, asymmetric security protocols are used. On the other hand, symmetric key exchanges between the UAV and the GCS almost always make use of asymmetric protocols. This is because symmetric key exchanges involve a lot of extra transmission. Additionally, asymmetric security methods are used in order to guarantee the data integrity during transmission from one set of sensors or devices to another.

3. **Lightweight Authentication Protocols for UAV**

   Using encryption and authentication mechanisms that aren't too taxing on the system is another method for keeping sensitive information hidden from potential attackers. If these lightweight techniques are used, it's possible that the information may be encoded in a shorter amount of time. Additionally, it does not make extensive use of the program memory, which enables the UAV to carry out activities more quickly. In the paper [18], the authors provide a lightweight encryption protocol that is capable of functioning suitably despite the presence of frequent context switching in an environment that is substantially multi-tasked. The authors of article [13] present a lightweight blockchain-based stable routing algorithm for the networking of swarm unarmed aerial systems. This method is intended to prevent collisions among the systems (UAS). Wang et al. have employed a lightweight blockchain as a bargaining chip in order to improve the routing of swarm UAS networking that utilizes 5G cellular network technology. This was done in order to improve the routing of unmanned aerial system (UAS) swarms. The lightweight blockchain algorithm is distinct from traditional routing algorithms in that it is able to easily avoid the vindictive connections from the attackers, identify malicious UASs, and reduce the intensity of attacks from spiteful UASs. These are all things that traditional routing algorithms are unable to do. Additionally, the lightweight blockchain algorithm can identify malicious UASs.

The proposed algorithms for swarm UAVs are ones that aim to broaden the networking capabilities of deployment for swarm UAVs over a broad range. Through the use of the Internet of Things, low-cost devices may be integrated into UAVs in order to protect data from being stolen by intruders (IoT). Encrypting the data using session keys that are already known to the exact nodes that are going to be participating is a good way to lessen the damage that may be done by cyberattacks. On the other hand, due to performance limits, it is very difficult for low-cost IoT installations to embody the essential capabilities for both generations of secure session keys and encoding/decoding of the secret information. This is because it is very difficult for low-cost IoT installations to meet these requirements simultaneously. This is due to the nature of the constraints that have been placed. In their research, Demeri and colleagues made use of a low-cost aerial platform that included a number of cryptographic accelerators. This allowed them to implement a secure and public key data transmission system at the same time [21]. This may be found in their publication. An approach to design that combines software and hardware has led to the creation of drones that are free of charge thanks to the incorporation of the components via the use of application programming interference (API) that is moldable and expandable. UAVs are providing a significant amount of relief to the general population as a result of recent developments in wireless communication technology and the shrinking of all electronic gadgets. In addition, cybersecurity for unmanned aerial vehicles, also known as UAVs, is receiving an increasing amount of attention as a consequence of potential risks to national security, significant strategic and financial information, and the expanding significance of aerial applications. A lightweight authentication protocol was suggested in [29] to offer secure communication between UAVs and ground stations in order to provide security and authentication to the communication parties in addition to ensuring the privacy of the data. This was done in order to offer secure communication between UAVs and ground stations. This was done in order to ensure that the data is kept private.

A packet capture, also known as PCAP, was specified in the suggested plan in order to guarantee the confidentiality of the communications that took place between the two parties. The PCAP is based on the idea that both the UAV and the ground station use the seed values of the chaotic maps. These seed values then cause the chaotic maps to randomly shuffle the original message in accordance with the sequence that is produced by the chaotic maps [29]. UAVs are no longer considered reliable for device seizing and dabble attacks due to recent developments in remote areas and the easy availability of minimal resources. This is because of the developments. Because of this, there is a greater possibility that hostile actors would steal the data held in UAVs. Haque et al., in their paper [22], are solely concerned with the safe transmission of data that unmanned aerial vehicles (UAVs) provide to the base station. Data security and lightweightness were both topics of discussion, and a new framework was proposed as a solution to meet the necessary requirements. Specific encryption is carried out so that the system may remain as lightweight as possible. In addition to the use of cryptography, the suggested method also makes use of watermarking as a means of improving both the data's integrity and its level of secrecy. The stability between the UAVs in an environment with limited resources is something that may be achieved via the use of selective encryption. The use of selective encryption may also have some advantages, especially in real-time applications where it is required to undertake speedy processing. This is because selective encryption may reduce the amount of data that has to be processed.

4. **Physical Layer Security in UAVs**

The so-called secrecy rate [30] is a widely used performance parameter in the physical layer security architecture. This refers to the maximum speed at which sensitive information may be sent without being compromised. Traditional encryption systems have flaws in the way key distribution is handled and require a significant amount of processing time. It is possible for secure transmission to be supported by an investigation of the physical features of cellular channels. Physical layer security, often known as PLS, is a technique that is routinely used to provide the highest possible level of confidentiality for data that is being transported from one node to another. In point of fact, it is obligatory for any and all security controls as well as communication devices that are installed on the UAV. PLS takes use of the properties of cellular channels such as fading, interference, and noise in order to improve the signal reception at the authorized receiver while simultaneously lowering the quality of the signal that is received by the eavesdropper [23, 31]. This is in contrast to the traditional cryptographic security approaches, which rely on mathematical algorithms to decipher messages. Incorporating cryptographic protocols is one way to do PLS. There are various cryptographic security protocols that have been presented in the literature that provide a significant degree of security; nevertheless, there is no framework that offers a level of security that is ideal. As a result, PLS is receiving a growing amount of serious attention. Several works on PLS have been offered in order to improve and make the most of the level of secrecy that may be achieved via wireless communication in UAVs [13, 32, 33]. A number of decades ago, in order to enhance the performance of the preexisting PLS schemes, static relay-based communication systems were put into operation. UAV-enabled mobile relaying is a relatively new sort of reliance technique that has formed as a result of the remarkable advancements that have been achieved in self-driving vehicles such as UAVs. This method has developed into an essential piece of technology as a direct result of these advancements. In the paper [12], the authors suggest an enhanced version of a PLS system that makes use of mobile reliance that is provided by UAVs. To make the communication system more secure, a buffer-aided mobile relay has been implemented. This makes it possible for data to arrive independently and more rapidly, which is beneficial for applications that need real-time processing.

5. Learning-Based Intrusion Detection

The user may direct a digital machine to carry out a variety of activities, and the machine will respond accordingly. Machine learning (ML), deep learning, and neural networks are often utilized methods that are frequently employed in order to perform the automation of the operations. Training and testing are the two stages that machine learning algorithms go through. During the training phase, the model takes what it has learned from the data and uses it to make predictions about what will happen in the future. During the testing phase, the accuracy of the training model is assessed, and it is possible to enhance it by using a variety of different tactics. Pattern recognition may be used for intrusion detection in UAVs using learning-based approaches, which can be applied in such systems. After receiving training, the UAV will be able to detect the pattern of the incursion after it has occurred. Deep reinforcement learning and a weighted least squares method are used by the authors of paper [34] to estimate the strength of the jamming signal. This is done with the assistance of a convolution neural network (CNN) [35]. The suggested method begins with the initial step of selecting a relay power factor by taking into account the bit error rate (BER) as well as the channel gain. A convolutional neural network is used in the process of initializing the weights, which will ultimately be equivalent to the anti-jamming relays. These weights are kept up to date with the use of a method called stochastic gradient descent [64]. The BER value is then sent to the UAV from the base station after this step. In the event that the learning parameter is higher than the power factor associated with the relay power, the apparatus will choose a relay power at random. If it goes over zero, the unmanned aerial vehicle will use a technique called reinforcement learning to transmit a message along with a value for the power that was chosen at random. Take into consideration that the randomly selected relay power may contribute to a higher mistake rate. The algorithm may be able to avoid jamming of the UAVs and communications to some degree in the event that there is a large mistake rate; however, this may come at a very high cost (Fig. 4).

6. Rules-Based Intrusion Detection

It is necessary to provide a piece of hardware with certain instructions in order to endow it with intelligent behavior. When doing rule-based activities, it is necessary for the user to establish certain rules. The choice is made by the device based on those guidelines, and it then communicates its verdict to the base station. In the case of UAVs, various sets of rules are loaded onto the chip of the UAV for each individual job, and threshold values for the acceptance of each rule are calibrated. For instance, if the threshold is set at 80%, this indicates that the particular function will only be carried out by the UAV if it determines that the real state of the rules is either equal to or more than 80%, and vice versa. A novel intrusion detection system based on the particular behavior criteria was presented in reference to [66], with the goal of minimizing the number of false negative predictions. Within the framework of the suggested detection approach, seven distinct attacks,

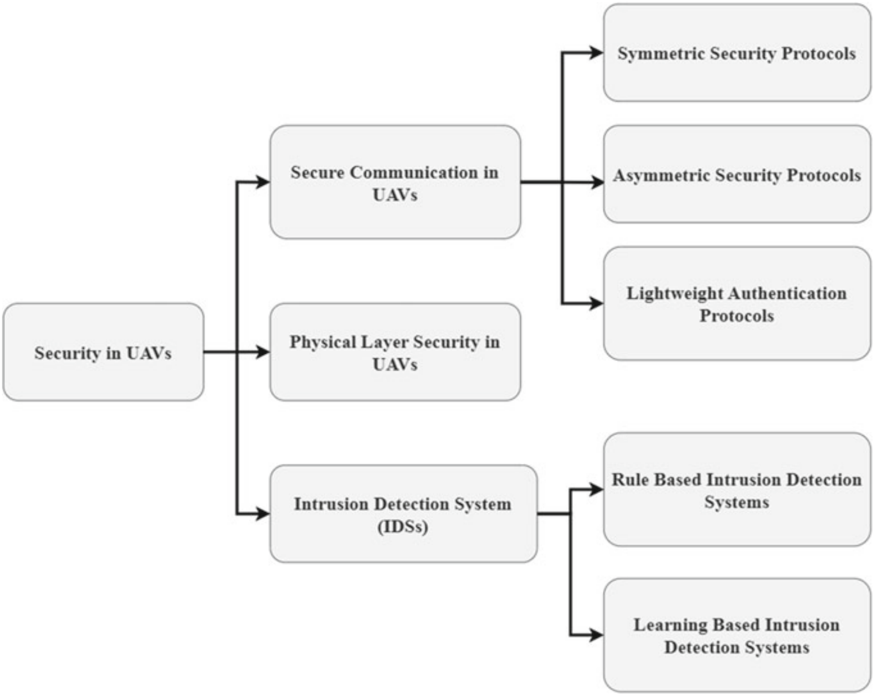
Security in UAVs
Secure Communication in UAVs
Physical Layer Security in UAVs
Intrusion Detection System (IDSs)
Symmetric Security Protocols
Asymmetric Security Protocols
Lightweight Authentication Protocols
Rule Based Intrusion Detection Systems
Learning Based Intrusion Detection Systems

Fig. 4 Security categories in UAVs

all of which are connected to availability, confidentiality, and integrity threats, were examined. The unmanned aerial vehicle (UAV) will initiate self-defense procedures if it is subjected to any of these seven types of attacks. When the unmanned aerial vehicle (UAV) first exits the secure zone, it immediately begins arming its weapons in preparation for an impending attack. Second, actions are carried out whenever the readings from the sensors do not match those from the trusted node. Third, the proper steps are conducted if negative suggestions are received about the trusted node and positive recommendations are made regarding the UAV that is acting inappropriately. The fourth indication is responsible for handling the circumstance in which the UAV deploys its landing gear in a location that is not acceptable. These four attacks are examples of attacks against the system's integrity. When the UAV begins providing data to individuals or organizations that are not authorized to receive it, the fifth indication becomes active. This exploit mirrors the secrecy attack that was described before. The seventh and final attack indication happens when the unmanned aerial vehicle (UAV) utilizes additional thrust to cross the limitation altitude that has been established by the authorized person. The sixth attack indicator takes place when the UAV deploys its countermeasures without first studying any attacks. The availability

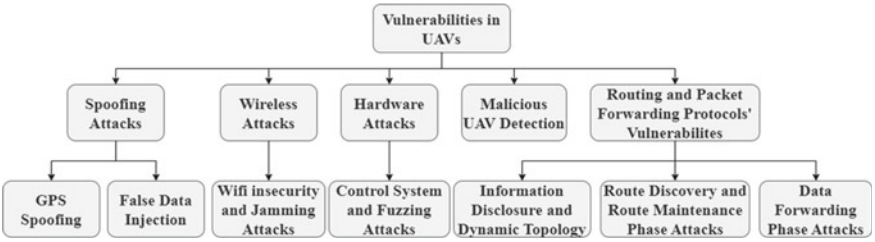
Vulnerabilities in UAVs
Spoofing Attacks
Wireless Attacks
Hardware Attacks
Malicious UAV Detection
Routing and Packet Forwarding Protocols' Vulnerabilites
GPS Spoofing
False Data Injection
Wifi insecurity and Jamming Attacks
Control System and Fuzzing Attacks
Information Disclosure and Dynamic Topology
Route Discovery and Route Maintenance Phase Attacks
Data Forwarding Phase Attacks

Fig. 5 Vulnerabilities in UAVs

attack is represented by the sixth and seventh attacks respectively. The aforementioned seven attacks are taken into consideration, and once an attack has been detected, the unmanned aerial vehicle (UAV) immediately begins a defensive phase to protect itself against the attacks described above. Additionally, intrusion detection systems, often known as IDS, are used in order to identify any abnormalities that may have occurred inside the network. In order to protect the systems from any dangers, the IDSs will now eliminate the negative effects of the attack. An intrusion detection system (IDS) is a crucial component of a network of unmanned aerial vehicles (UAVs) that helps identify potentially harmful nodes and defends genuine UAVs from attack (Fig. 5).

2 Conclusion

In this study, we offered a detailed overview and in-depth analysis of current attempts towards GPS spoofing. Specifically, we focused on how these efforts may be improved. Particularly, location spoofing of unmanned aerial vehicles (UAVs) was discussed in great depth. This was accomplished by associating GPS reliance with the operating modes of UAVs and assessing attack variants for static, limpet, and mobile (follower) spoofers. With the use of well created faked GPS signals, an adversary might misdirect, put in danger, destroy, or even hijack a spoofed unmanned aerial vehicle (UAV). We also offered a unique taxonomy to identify attack capabilities, location, stealthiness, and aims of multifarious spoofing strategies, while also categorizing and discussing the existing literature according to the definitions of our taxonomy. This was done when spoofing techniques are used. In addition to this, the report discussed some of the unresolved issues that might stimulate additional research in certain fields. In light of the many GPS spoofing attacks that have been carried out against aerial platforms, surface vehicles, and other statics services, it is imperative that security-aware and spoof-resistant GPS services be designed. On the other side, GPS spoofing has also showed promising possibilities for parametric defense to disable hostile drones. This is because of its ability to fool GPS receivers.

References

1. Yaacoub JPA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2019) Securing internet of medical things systems: limitations, issues and recommendations. Fut Gener Comput Syst 105:581–606
2. Park J, Kim S, Suh K (2018) A comparative analysis of the environmental benefits of drone-based delivery services in urban and rural areas. Sustainability 10(3):888
3. Humphreys T (2012) Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. University Texas Austin, Austin
4. Canis B (2015) Unmanned aircraft systems (UAS): commercial outlook for a new industry
5. Stocker C, Bennett R, Nex F, Gerke M, Zevenbergen J (2017) Review of the current state of UAV regulations. Remote Sens 9(5):459
6. Barfield F (2002) Autonomous collision avoidance: the technical requirements. In: Proceedings of the IEEE national aerospace and electronics conference, pp 808–813
7. Sharma R, Ghose D (2009) Collision avoidance between UAV clusters using swarm intelligence techniques. Int J Syst Sci 40(5):521–538
8. Johnson LK, Dorn AW, Webb S, Kreps S, Krieger W, Schwarz E, Shpiro S, Walsh PF, Wirtz JJ (2017) An INS special forum: intelligence and drones/eyes in the sky for peacekeeping: the emergence of UAVs in UN operations/the democratic deficit on drones/the German approach to drone warfare/pursuing peace: the strategic limits of drone warfare/seeing but unseen: intelligence drones in Israel/drone paramilitary operations against suspected global terrorists: us and Australian perspectives/the ‘terminator conundrum’ and the future of drone warfare. Int Natl Sec 32(4):411–440
9. Thiels CA, Aho JM, Zietlow SP, Jenkins DH (2015) Use of unmanned aerial vehicles for medical product transport. Air Med J 34(2):104–108
10. Rango A, Laliberte A, Steele C, Herrick JE, Bestelmeyer B, Schmugge T, Roanhorse A, Jenkins V (2006) Using unmanned aerial vehicles for rangelands: current applications and future potentials. Environ Pract 8(3):159–168
11. Sedjelmaci H, Senouci SM (2018) Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution. J Supercomput 57:1–17
12. Mushtaq MF, Jamel S, Mohamad KM, Khalid SKA, Deris MM (2017) Key generation technique based on triangular coordinate extraction for hybrid cubes. J Telecommun Electron Comput Eng 9(3–4):195–200
13. Du H, Heldeweg MA (2017) Responsible design of drones and drone services: legal perspective synthetic report
14. Ueno S, Higuchi T (2011) Collision avoidance law using information amount. In: Numerical analysis-theory and application. InTech, Allithurai
15. Hamza A, Akram U, Samad A, Khosa SN, Fatima R, Mushtaq MF (2020) Unmaned aerial vehicles threats and defence solutions. In: IEEE 23rd international multi-topic conference (INMIC)
16. Israelsen J, Beall M, Bareiss D, Stuart D, Keeney E, Berg J (2014) Automatic collision avoidance for manually tele-operated unmanned aerial vehicles. In: IEEE international conference on robotics and automation (ICRA), pp 6638–6643
17. Boulos MNK, Geraghty EM (2020) Geographical tracking and mapping of coronavirus disease covid-19/severe acute respiratory syndrome coronavirus 2 (sars-cov-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics. Int J Health Geogr 19:1–12
18. Finn RL, Wright D (2012) Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput Law Sec 28(2):184–194
19. Cavoukian A (2012) Privacy and drones: unmanned aerial vehicles. Information and Privacy Commissioner of Ontario, Ontario
20. Jumaat N, Ahmad B, Dutsenwai HS (2018) Land cover change mapping using high resolution satellites and unmanned aerial vehicle. In: IOP conference series: earth and environmental science

21. Wackwitz K, Boedecker H (2015) Safety risk assessment for UAV operation. In: Drone industry insights, safe airspace integration project, part one, Hamburg
22. Finn RL, Wright D, Friedewald M (2013) Seven types of privacy. In: European data protection: coming of age. Springer, New York
23. Ramon Soria P, Bevec R, Arrue B, Ude A, Ollero A (2016) Extracting objects for aerial manipulation on UAVs using low cost stereo sensors. Sensors 16(5):700
24. Clarke R (2014) The regulation of civilian drones' impacts on behavioural privacy. Comput Law Sec Rev 30(3):286–305
25. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA (2012) Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. Proc ION GNSS Meet 3:3591–3605
26. Yanmaz E, Kuschnig R, Quaritsch M, Bettstetter C, Rinner B (2011) On path planning strategies for networked unmanned aerial vehicles. In: IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp 212–216
27. Hernandez LH, Tsourdos A, Shin HS, Waldock A (2014) Multi-objective UAV routing. In: IEEE international conference on unmanned aircraft systems (ICUAS), pp 534–542
28. Vattapparamban E, Guvenc I, Yurekli AI, Akkaya K, Uluagac S (2016) Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: IEEE international wireless communications and mobile computing conference (IWCMC), pp 216–221
29. Carr EB (2014) Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace. Natl Centre Policy Anal 23:2014
30. Lin X, Wiren R, Euler S, Sadam A, Maattanen HL, Muruganathan SD, Gao S, Wang YPE, Kauppi J, Zou Z (2018) Mobile networks connected drones: field trials, simulations, and design insights. arXiv Preprint arXiv:1801.10508
31. Abdallah A, Ali MZ, Misic J, Misi VB (2019) Efficient security scheme for disaster surveillance UAV communication networks. Information 10(2):43
32. Kim SJ, Lim GJ, Cho J (2018) Drone flight scheduling under uncertainty on battery duration and air temperature. Comput Ind Eng 117:291–302
33. Tseng CM, Chau CK, Elbassioni K, Khonji M (2017) Autonomous recharging and flight mission planning for battery-operated autonomous drones. arXiv preprint arXiv:1703.10049
34. Basan E, Basan A, Nekrasov A, Fidge C, Sushkin N, Peskova O (2022) GPS-spoofing attack detection technology for UAVs based on Kullback-Leibler divergence. Drones 6:8. https://doi.org/10.3390/drones6010008
35. Khan SZ, Mohsin M, Iqbal W (2021) On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJComput Sci 7:e507. https://doi.org/10.7717/peerj-cs.507
36. Chan K, Nirmal U, Cheaw W (2018) Progress on drone technology and their applications: a comprehensive review. In: AIP conference proceedings, 2030. AIP Publishing, College Park, p 020308
37. Liu Z, Li Z, Liu B, Fu X, Raptis I, Ren K (2015) Rise of mini-drones: applications and issues. In: Proceedings of the 2015 workshop on privacy-aware mobile computing. ACM, New York, pp 7–12
38. Altawy R, Youssef AM (2017) Security, privacy, and safety aspects of civilian drones: a survey. ACM Trans Cyber Phys Syst 1(2):7
39. He D, Chan S, Guizani M (2017) Drone-assisted public safety networks: the security aspect. IEEE Commun Mag 55(8):218–223
40. Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM international conference on high confidence networked systems. ACM, New York, pp 135–142
41. Guvenc I, Ozdemir O, Yapici Y, Mehrpouyan H, Matolak D (2017) Detection, localization, and tracking of unauthorized UAS and jammers. In: Proceedings of the 2017 IEEE/AIAA 36th digital avionics systems conference (DASC), IEEE, pp 1–10
42. Sturdivant RL, Chong EK (2017) Systems engineering baseline concept of a multispectral drone detection solution for airports. IEEE Access 5:7123–7138

43. Shi X, Yang C, Xie W, Liang C, Shi Z, Chen J (2018) Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. IEEE Commun Mag 56(4):68–74
44. Nassi B, Shabtai A, Masuoka R, Elovici T (2019) Sok-security and privacy in the age of drones: threats, challenges, solution mechanisms, and scientific gaps. arXiv Preprint arXiv:1903.05155
45. Atherton KD (2016) The FAA says there will be 7 million drones flying over America by 2020. Popular Sci
46. Vattapparamban E, Guvenc I, Yurekli AI, Akkaya K, Uluagac S (2016) Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: Wireless communications and mobile computing conference (IWCMC), 2016 international, IEEE, pp 216–221
47. Dalamagkidis K, Valavanis KP, Piegl LA (2012) Aviation history and unmanned flight. on integrating unmanned aircraft systems into the national airspace system. Springer, New York, pp 11–42
48. Juul M (2015) Civil drones in the European Union, Eur. Parliament. Res. Serv. (ed.). Eur. Union
49. Stopforth R (2017) Drone licenses-necessities and requirements. II. Ponte 73(1):149–156
50. Campos VS (2018) European union policies and civil drones. Ethics and civil drones. Springer, Cham, pp 35–41
51. Miah A (2020) Regulating drones. In: Drones: the brilliant, the bad and the beautiful. Emerald Publishing Limited, Bingley
52. Wright S (2020) Ethical and safety implications of the growing use of civilian drone. UK Parliament Website (Sci. Technol. Committee)
53. Lowbridge C (2015) Are drones dangerous or harmless fun? BBC News, London. https://www.bbc.com/news/uk-england-34269585. Accessed 07 Sept 2018
54. Cress JJ, Sloan JL, Hutt ME (2011) Implementation of unmanned aircraft systems by the US geological survey. Geocarto Int 26(2):133–140
55. Lipsitch M, Swerdlow DL, Finelli L (2020) Defining the epidemiology of covid-19—studies needed. N Engl J Med 382(13):1194–1196
56. Jiang F, Deng L, Zhang L, Cai Y, Cheung CW, Xia Z (2020) Review of the clinical characteristics of coronavirus disease 2019 (covid-19). J Gen Intern Med 35:1–5
57. Majeed R, Abdullah NA, Ashraf I, Zikria YB, Mushtaq MF, Umer M (2020) An intelligent, secure, and smart home automation system. Sci Program 57:1–14
58. Zeng Y, Zhang R, Lim TJ (2016) Wireless communications with unmanned aerial vehicles: opportunities and challenges. arXiv preprintarXiv:1602.03602
59. Rudinskas D, Goraj Z, Stankunas J (2009) Security analysis of UAV radio communication system. Aviation 13(4):116–121
60. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE (2014) Unmanned aircraft capture and control via GPS spoofing. J Field Rob 31(4):617–636
61. Seo SH, Lee BH, Im SH, Jee GI (2015) Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. J Posit Navig Timing 4(2):57–65
62. Shafique A, Mehmood A, Elhadef M (2021) Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access 9:46927–46948. https://doi.org/10.1109/ACCESS.2021.3066778