Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.029075

REVIEW

A Survey on Sensor- and Communication-Based Issues of Autonomous UAVs

Pavlo Mykytyn[1,2,*], Marcin Brzozowski[1], Zoya Dyka[1,2] and Peter Langendoerfer[1,2]

[1]IHP-Leibniz-Institut für Innovative Mikroelektronik, Wireless Systems, Frankfurt (Oder), 15236, Germany

[2]BTU Cottbus-Senftenberg, Faculty 1: MINT, Cottbus, 03046, Germany

*Corresponding Author: Pavlo Mykytyn. Email: mykytyn@ihp-microelectronics.com

Received: 01 February 2023 Accepted: 20 June 2023 Published: 17 November 2023

ABSTRACT

The application field for Unmanned Aerial Vehicle (UAV) technology and its adoption rate have been increasing steadily in the past years. Decreasing cost of commercial drones has enabled their use at a scale broader than ever before. However, increasing the complexity of UAVs and decreasing the cost, both contribute to a lack of implemented security measures and raise new security and safety concerns. For instance, the issue of implausible or tampered UAV sensor measurements is barely addressed in the current research literature and thus, requires more attention from the research community. The goal of this survey is to extensively review state-of-the-art literature regarding common sensor- and communication-based vulnerabilities, existing threats, and active or passive cyber-attacks against UAVs, as well as shed light on the research gaps in the literature. In this work, we describe the Unmanned Aerial System (UAS) architecture to point out the origination sources for security and safety issues. We evaluate the coverage and completeness of each related research work in a comprehensive comparison table as well as classify the threats, vulnerabilities and cyber-attacks into sensor-based and communication-based categories. Additionally, for each individual cyber-attack, we describe existing countermeasures or detection mechanisms and provide a list of requirements to ensure UAV's security and safety. We also address the problem of implausible sensor measurements and introduce the idea of a plausibility check for sensor data. By doing so, we discover additional measures to improve security and safety and report on a research niche that is not well represented in the current research literature.

KEYWORDS

Unmanned aerial vehicle; unmanned aerial system; cyber security and privacy; drone swarm; security vulnerabilities; cyber-threats; cyber-attacks; plausibility check

Nomenclature

UAV	Unmanned aerial vehicle
UAS	Unmanned aerial system
GCS	Ground control station
IMU	Inertial measurement unit
FDI	Fault detection and isolation
FTC	Fault tolerant control

VLOS	Visual line of sight
BVLOS	Beyond visual line of sight
DoS	Denial of service
UWB	Ultra-wideband

1 Introduction

The advancement in UAV technology over the past few years has enabled new practical applications for UAVs, such as the delivery of goods [1–5], surveillance and mapping of large areas [6–10], search and rescue missions [11–16], disaster response [17–22], smart farming [23–26], precision agriculture [27–31], wildlife and marine monitoring [32–37] and more. A market study in 2021 has shown that in Germany alone, there are over 430,000 UAVs in use, 90% of which are used privately and 10% commercially [38]. A recent report also shows that the commercial drone market revenue was at $69 billion in 2017 and is projected to grow by more than 11% and surpass $141 billion by 2023 [39]. UAVs will represent an essential part of our technological society as their popularity and number are steadily increasing. The factors that drive the expansion and adoption of UAVs worldwide are platform flexibility, low maintenance, quick deployment, autonomous navigation, multi-node and swarm capabilities, large area coverage, and progressive data collection techniques. UAVs rely heavily on wireless communication and sensor data for their operation. They also have limited computational and energy resources, making them vulnerable to a variety of cyber-attacks. It is important to mention that the increase in drone use and emerging of new application fields will pose new security, safety, and privacy challenges [40]. Taking into account legal requirements for size and weight [41] as well as limited computational and energy resources [42], UAVs are often disadvantaged in terms of security and safety. Typical UAV architecture designs are reliant on human supervision and do not take into account cyber-security threats, thus exposing UAVs to a variety of cyber-attacks [43]. Cyber-attacks against UAVs are feasible due to the lack of integration of appropriate security measures by the manufacturers in favor of higher performance, smaller latency, and longer battery life [44]. We classify cyber threats to UAVs into three types, namely: Sensor-based, Communication-based, and the Implausibility of the sensor measurements. Sensor-based threats include fault injection and Spoofing or Jamming of the sensors readings. Communication-based threats include Jamming, Eavesdropping, Man-in-the-Middle, and Replay attacks on the wireless communication link. The implausibility of sensor measurements implies that the sensor measurements might be faulty, spoofed, or incorrect due to internal or external uncertainties, especially if not verified through redundancy check or fault detection and isolation mechanisms. Internal uncertainties include issues related to sensor's hardware or software components, such as manufacturing flaws, software bugs, or communication failures. External uncertainties include issues related to the operational environment, such as weather conditions, electromagnetic interference, or operation of other aircraft in the vicinity. Additionally, sensors are prone to parametric and non-parametric uncertainties like calibration issues, control gains, or sensor noise. Sensor faults might lead to course deviation or serious system malfunction that could result in lost control, collision, or crash. Sensor measurements can also be interrupted, delayed, or lost during transmission, which significantly impacts the flight control and navigation system and compromises mission success. There are a few strategies present in the literature to tackle those issues. Redundancy check mechanisms are a good option to verify the plausibility of the sensor measurements; however, it is not always feasible to install redundant hardware on the drone platform due to the size, price, or other aspects. Moreover, if all of the sensors are spoofed, the measurements will be identical, which renders this approach ineffective for that particular scenario. Fault Detection and Isolation (FDI) mechanisms are a reasonable option [45], however, they perform a substantial

analysis of the measurement data through a model-based comparison or Machine Learning (ML) algorithm [43], which in turn requires significant spare computational power and increases delays [46,47]. Similarly, recursive analytics-based multi-sensor data fusion methods such as the variation of Kalman filters estimate the optimal system state based on the observational analytics of the current system state compared to the previous system state [48]. In learning-based multi-sensor data fusion methods such techniques as supervised, unsupervised, reinforced, and deep learning help to evaluate the quality of sensor data [49], predict the future values of sensor measurements [50], and in the case of a sensor outage, keep the system operational. However, a downside of the ML and Artificial Neural Networks (ANN) based methods is that they demand a substantial amount of quality training data, which could be challenging to obtain [51] and thus, limits their real-world application.

In this work, we aim to provide a comprehensive overview of the existing state-of-the-art literature concerning UAV safety and security categorized into sensor-based and communication-based cyber-threats and cyber-attacks, as well as focus specifically on the issue of implausible sensor measurements in UAVs, which we found to be largely unaddressed in the existing literature. Despite the abundance of literature and popularity of this research topic, we discovered that except for the methods mentioned above, other simple yet effective solutions to confirm the plausibility of sensor measurements are practically non-existent. The few solutions described above that do exist in the literature require hardware redundancy, substantial data analysis, or an extensive amount of quality training data and are computationally intensive, limiting their practical use in real-world scenarios. Our article highlights this limitation and presents alternative ideas and solutions to address the issue of implausible sensor measurements. We argue that these alternative approaches offer a more practical and effective means of ensuring UAV security and safety and emphasize the need for further research in this area. We also present available countermeasures and solutions to mitigate security threats and detect or prevent cyber-attacks. The main contributions of this work are:

- Denomination of security and safety requirements for the Unmanned Aerial Systems (UAS) operation.
- A comprehensive overview of the available state-of-the-art literature and categorization of the threats, attacks, and vulnerabilities into the sensor-based and communication-based categories.
- Overview of the mechanisms to check the plausibility of sensor measurements.
- Finally, we emphasize on the security aspects that require more attention during the design of an autonomous UAV system.

The rest of this paper is structured in the following way. Firstly, in Section 2, we provide an overview of the related work regarding UAV security and safety. In Section 3, we describe the general UAS architecture, common UAV types based on their design, UAV swarm communication architecture, and the overall security requirements. Section 4 provides a detailed description of the sensor-based and communication-based security vulnerabilities, threats, attacks, and existing countermeasures. Section 5 presents an overview of the plausibility check mechanisms for sensor measurements. Finally, Section 6 concludes this work.

2 Related Work

In this section, we provide an overview of the research literature regarding security vulnerabilities, threats, attacks, and countermeasures as well as existing approaches to the sensor and actuator fault diagnosis, and plausibility check of sensor data. We highlight the major challenges for each category and examine the state of the art while also providing an overview of the authors' classification. We

decided to evaluate the related work based on the coverage of the security vulnerabilities, threats, cyber-attacks, and countermeasures by the authors. Additionally, we considered the categorization of the security issues provided by the authors and the completeness of each of the categories mentioned above. Lastly, due to the importance of correct and plausible sensor measurements and their significant impact on the UAV's safety, we decided to include the plausibility check of sensor measurements as an additional factor. Table 1 represents an overview of the coverage of security issues in the existing surveys and related literature.

Allouch et al. [52] briefly discussed the security threats to UAVs from the communication protocol's perspective. They suggested the integration of an encryption algorithm into the MAVlink protocol to counter Man-in-the-Middle and Eavesdropping attacks. They also categorized the threats into three categories, namely Confidentiality, Integrity, and Availability. However, they do not provide an overview of other cyber-attacks or plausibility checks for sensor measurements. Vattapparamban et al. [53] discussed cybersecurity from the perspective of smart cities. They go into detail about describing Wi-Fi de-authentication and GPS Spoofing attacks. However, their overview only discusses those two cyber-attacks and provides limited insight. Cyber-attack classification and categorization as well as mitigation techniques and countermeasures are not provided in their work. In [54], the authors surveyed the security, privacy, and safety aspects of civilian drones. They divided cyber-physical attacks into two categories according to the affected components, namely Flight controller attacks and Data link attacks. However, their work is limited in terms of sensor attacks and mitigation techniques. Davidson et al. [55] concentrated on the optical flow sensor Spoofing attack and provided insight into the category of sensor Spoofing attacks. However, they did not cover communication-based cyber-attacks. Instead, they explored the mitigation techniques and suggested an algorithm to exclude malicious input from the sensor measurements. In [43], the authors focused on the Inertial Measurement Unit (IMU) sensor fault data injection attacks and their detection. They simulated two different fault data injection attacks on the IMU sensor and proposed a neural network-based detection algorithm. However, no categorization, classification, or mitigation techniques against the attacks were discussed. In [56], the authors surveyed UAV Networks for civil applications from the communication standpoint. They provided details about the UAS components and their individual issues as well as briefly addressed the security, safety, and privacy issues of UAVs. However, no categorization or countermeasures were given. In [57], the authors explored the attacks on an unencrypted communication channel between a UAV and a Ground Control Station (GCS) by performing a Man-in-the-Middle attack. Their work, however, only describes one specific type of a communication-based cyber-attack and possible countermeasures against it, but does not categorize, classify, or mention other cyber-attacks. The authors in [58] mentioned recent real-world and simulated cyber-attacks on small and large UAVs that were documented in the literature. They provided a taxonomy of vulnerabilities by attack vector and by target, without a detailed description of each of the vulnerabilities. Their overview lacks clarity in the classification of cyber-attacks, as well as a description of threats and countermeasures against them. In [59], the authors provided an overview of GPS Spoofing/Jamming and Wi-Fi de-authentication attacks. Their work, however, does not mention any other cyber-attacks, or classify the presented ones. Authors in [60] and [47] solely focused on the detection and isolation of the UAV's sensor and actuator faults. In [60], they applied a Fault Tolerant Control (FTC) scheme to detect sensor and actuator faults, whereas in [47], they employ the FDI approach by using the extended proportional and multiple integral filters. Both of their simulations have shown good results. However, in terms of coverage, neither of them mentions any other cyber-attacks. In [61], the authors categorized the cyber-attacks by reviewing the security issues of two commercially available drones, namely DJI Phantom 4 and Parrot Bebop 2. Their overview, however, only covers a few cyber-attacks specific to those commercially available

drones and is limited to them. In [62], the authors classified cyber-attacks on UAVs into the Privacy, Integrity, Confidentiality, Availability, and Trust categories. They described the attacks in each category but did not provide countermeasures or mitigation techniques against them. Authors in [63] and [64] surveyed quadrotors on a few different topics, among them sensor fault diagnosis and tolerant control. They differentiate between IMU, accelerometer, and magnetometer sensor faults and discuss the countermeasures and detection mechanisms present in the literature. However, their overview does not provide any categorization, or description of the security threats and attacks. In [65], the authors categorized attacks on drones into physical, protocol-based, and sensor attacks. Their work mentions both, sensor and communication-based attacks as well as countermeasures against them. However, their work lacks a description of vulnerabilities and threats. In [66], the authors surveyed UAVs on cellular communication and describe the main cyber-attacks on the communication link. However, they do not categorize the attacks or discuss the countermeasures against them. Zhi et al. [67] analyzed the security threats on sensors and overviewed some of the communication link vulnerabilities. The discussion of the communication vulnerabilities, however, was limited. Their work did not mention countermeasures or mitigation techniques against any of the attacks. The authors in [68] provided a brief overview of the UAV communication architecture and discussed the topic of software-defined networking (SDN) and its features. They concentrated on cyber-attacks targeting communication and analyzed SDN-based countermeasures against them. However, they did not discuss any sensor-related vulnerabilities or cyber threats. In [69], the authors classified the attacks into three categories, Physical layer, Communication layer, and Application layer attacks. They also differentiated between unmanned aerial, ground, space, and sea vehicles. Their work lacks a detailed description of the individual threats and attacks, as well as a vulnerability overview. Yaacoub et al. [40] presented a good overview of drone vulnerabilities, countermeasures, and security requirements. Their overview of cyber-attacks, however, did not include any classification or categorization. The authors in [70] categorized cyber-attacks into Sensor attacks, Control Unit attacks, and Communication Unit attacks. They provided a good overview of the attacks in each category but did not discuss the countermeasures against them. In [71], the authors concentrated on the communication-based vulnerabilities, threats, and attacks for different categories of drones such as rescue, agricultural, military, and delivery. However, their work does not categorize or classify the attacks. Shafique et al. [72] provided a comprehensive overview of the communication-based as well as some sensor-based vulnerabilities and countermeasures against them. Their overview, however, lacks sensor-based vulnerabilities and attacks. In [73], the authors categorized cyber-security threats into four categories: protocol, sensor, compromised component, and jammers. Their work, however, does not describe individual attacks and countermeasures against them. In [74], the authors surveyed the security and privacy issues of UAVs from the Internet of Drones perspective. They classified cyber-attacks on UAVs into navigational signals, data injection, malware installation, message alteration, position alteration, and algorithm-based attacks. They also classified mitigation techniques against those attacks into Integrity, Availability, Confidentiality, and Privacy. However, their security threat classification lacks a description of vulnerabilities. In [75], the authors divided the security and privacy issues of UAVs into 4 categories: hardware, sensor, software, and communication issues. They discussed threats and attacks in each category separately, providing a good overall overview and coverage of each category. However, they did not discuss sensor measurements' plausibility check or credibility. In [76] and [77], the authors provided a taxonomy of security threats based on a threat vector. In [76], they concentrated on the communication attacks, whereas in [77], they covered communication and sensor attacks but do not provide a classification. Both authors discussed countermeasures to the mentioned threats and attacks. In [78–81], the authors addressed another key issue of detecting and responding to partial or full actuator failures, which is vital for a reliable and robust operation. In [78]

and [80], the authors both presented similar approaches. In [78], the authors developed a third-order Thau observer able to reveal the rotational state estimation fault in the presence of quadrotor faults. The developed observer is able to recognize up to two faulty actuators instantly by using the estimated rotational state error. They assessed the performance and accuracy of the observer in a simulation and confirmed smaller estimation errors when compared to Kalman filter-based mechanisms. In [80], the authors used a nonlinear Thau observer on a Hexacopter to generate residuals, detect failures, and isolate them. Their method can detect and isolate up to two actuator failures. The authors in [79] proposed a fault detection and diagnosis method based on the extended Kalman filter (EKF) and multiple-model adaptive estimation (MMAE). They used EKF to estimate actuator deflections, assign a conditional probability to each faulty actuator and diagnose the faults using the MMAE algorithm. They verified their method using simulation and confirmed that it can accurately diagnose actuator faults. In [81], the authors presented an actuator FDI method based on an ANN that was trained using the data from four separate accelerometers. They then implemented their method on a microcontroller and tested its efficiency and processing time. The tests showed a detection rate of 98.08% and real-time processing capabilities.

Table 1: Comparison of the related work on sensor-based and communication-based security threats and plausibility check of sensor measurements

Year	Citation	Sensor-based			Communication-based			Plausibility check
		T/V	A	C	T/V	A	C	
2016	[53]	–	✓	–	–	✓	–	–
2016	[54]	✓	–	–	✓	✓	✓	–
2016	[55]	–	✓	✓	–	–	–	–
2016	[43]	–	✓	✓	–	–	–	–
2016	[56]	–	–	–	✓	–	–	–
2016	[57]	–	–	–	–	✓	✓	–
2017	[58]	–	✓	–	–	✓	–	–
2017	[59]	–	✓	✓	–	✓	✓	–
2017	[60]	–	–	✓	–	–	–	✓
2018	[61]	–	✓	✓	✓	–	–	–
2018	[62]	–	✓	–	–	✓	–	–
2018	[63]	✓	–	–	–	–	–	✓
2018	[47]	–	–	✓	–	–	–	✓
2019	[65]	–	✓	✓	–	✓	✓	–
2019	[52]	–	–	–	–	✓	✓	–
2019	[66]	–	✓	✓	–	✓	✓	–
2019	[67]	✓	✓	–	–	✓	–	–
2019	[68]	–	✓	✓	–	✓	✓	–
2020	[69]	–	✓	✓	–	✓	✓	–
2020	[40]	–	–	–	✓	✓	✓	–
2020	[70]	–	✓	–	–	✓	–	–
2021	[72]	✓	–	✓	✓	–	✓	–
2021	[71]	–	✓	–	✓	✓	✓	–
2021	[64]	✓	–	–	–	–	–	✓

(Continued)

Table 1 (continued)

Year	Citation	Sensor-based			Communication-based			Plausibility check
		T/V	A	C	T/V	A	C	
2021	[73]	✓	✓	–	–	✓	–	–
2021	[75]	✓	✓	✓	✓	✓	✓	–
2021	[74]	–	✓	✓	–	✓	✓	–
2022	[76]	✓	–	–	–	✓	✓	–
2022	[77]	✓	–	–	–	✓	✓	–
2023	This work	✓	✓	✓	✓	✓	✓	✓

Fig. 1 below represents the literature chart by the year of publication. From the chart, we can clearly see that the number of relevant publications about UAV's security issues started steadily increasing from 2016 on, and with the new application areas for UAVs this field of research will only become more relevant in the future.

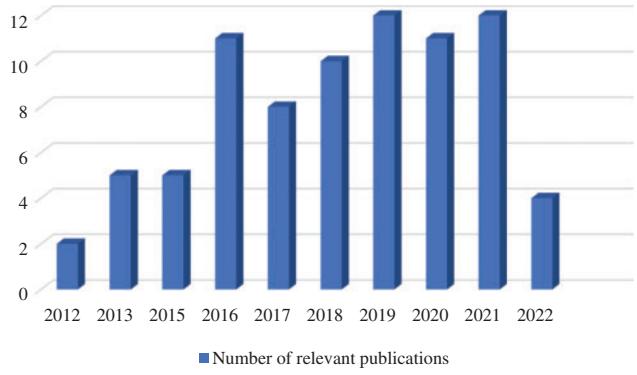

Figure 1: Publications on UAV's security issues year-wise

Fig. 2 represents the number of mentionings of each cyber-attack in the reviewed literature. GPS Spoofing/Jamming category includes both GPS Spoofing and GPS Jamming attacks on the GPS receiver. Our literature overview confirms that both attacks were the most commonly mentioned in the literature, present in 28% of all of the overviewed literature. The sensor attacks category includes all types of sensor channel attacks and fault injection attacks on UAVs.

3 Unmanned Aerial System Architecture

A general UAS architecture consists of a UAV, GCS, and a wireless communication link between them [82]. UAV is the central component in the UAS architecture. It is controlled remotely either by sending steering commands through the GCS's software or by employing a remote pilot to operate the aircraft via the remote controller. Knowing the UAS architecture components and understanding the information flow and interaction mechanisms between them is crucially important to identify its limitations and vulnerabilities correctly. Fig. 3 represents the general architecture of an autonomous UAS, including the UAV on the left side, GCS on the right side, and the communication link between them in the middle.

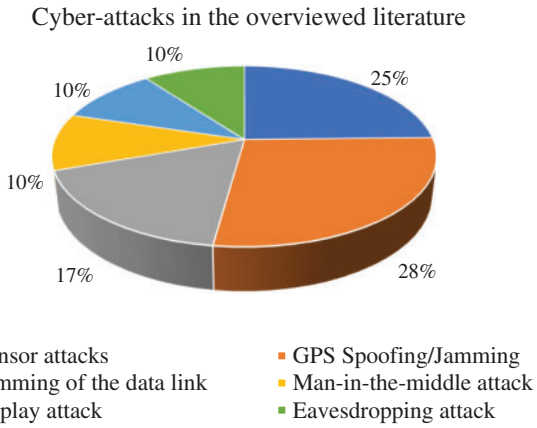

Figure 2: Percentage of the prevalence of the sensor-based and communication-based cyber-attacks in the overviewed literature

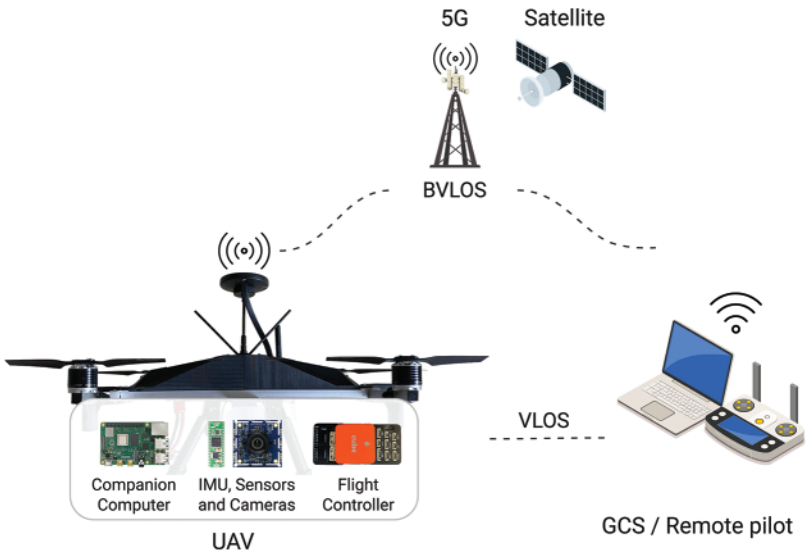

Figure 3: The architecture of an autonomous UAS

3.1 UAS Components

The left side of Fig. 3 represents a UAV with its main hardware components required for the operation. To enable an autonomous flight such hardware components as flight controller, IMU, electronic speed controller, magnetometer, gyroscope, infrared, ultrasonic or ultra-wideband (UWB) distance measuring sensors, GPS receiver, and companion computer are needed [83]. The flight controller is responsible for the stabilization and control during flight, processing of the acquired sensor data, converting them into meaningful steering commands, and transmitting them to directly control the motors and actuators. IMU sensors and cameras are responsible for gathering real-time measurements in the surrounding environment such as distances to other UAVs and obstacles, altitude, speed, tilt, yaw, acceleration, drone's current location, and deviation from the defined course. The companion computer in turns serves as a central computing unit to enable real-time processing of the sensor data, autonomous navigation, and collision avoidance algorithm execution.

The absence of a pilot onboard the UAV makes monitoring of the environment highly dependent on the set of onboard sensors. Relying on the sensors for operation makes UAVs vulnerable to sensor attacks. These include physical interference with the sensors [55] as well as sensor spoofing, Jamming, or fault injection. For example, GPS receivers and IMUs typically work in unison for navigation and accurate position estimation. However, because civil GPS signals are unencrypted and unauthenticated, an adversary can spoof [84] or jam [85] the GPS signal and thus cause a course deviation, collision, or even a crash of the UAV.

The right side of Fig. 3 depicts a GCS that is usually represented by a laptop, phone, or tablet running corresponding software and connected to a UAV over a wireless communication link [86,87]. GCS enables remote control, mission planning, and monitoring of the UAV's critical data in real-time by sending commands over the wireless communication link using telemetry radios. Some of the most popular open-source GCS software applications are "Mission Planner" and "QGroundControl". The number and presence of GCS operators/remote pilots might differ depending on the UAV's size, type, and mission category. Due to the fact that GCS is usually represented by a laptop, phone, or tablet, it is vulnerable to malicious software injection. Additionally, open-source GCS software applications are susceptible to bugs and malfunctions.

3.2 UAV Types

Autonomous UAVs can be classified into four main types based on their body design, flying style, and specific tasks they need to fulfill. Fig. 4 represents four main UAV types and their subtypes, namely fixed-wing, rotary-wing, flapping-wing, and aerostats [88]. Fixed-wing UAVs have an airplane-like design. They are intended to be flown over large distances and are able to stay airborne for extended periods of time, making them suitable for surveying, mapping, intelligence gathering, and reconnaissance missions [89,90]. Rotary-wing UAVs, on the other hand, are equipped with rotors, which allow them to take off and land vertically or hover in place, making them ideal for close-up inspections and maneuver-intensive applications. They are often used for aerial photography, search and rescue operations, and inspection of critical infrastructure [91,92]. A hybrid of both fixed-wing and rotary-wing UAVs is the so-called vertical take-off and landing (VTOL) UAV that has a body of a fixed-wing aircraft with additional rotors for vertical take-off and landing [93]. These UAVs do not require a launch pad or a runway to take off. If needed, they can hover in one place and are also suitable for long-distance flights. Flapping-wing UAVs mimic the flapping motion of birds or insects and are able to operate in gusty environments at low speeds without generating extensive amounts of noise [94]. They are mainly used for research and development purposes, as their complex design makes them expensive to produce and challenging to operate [95]. Aerostats include unmanned balloons and blimps that can be anchored to the ground or flown freely in the air. They can stay airborne for weeks or months at a time and are designed to be floating sensor platforms, making them ideal for scientific research operations, weather monitoring, or reconnaissance [96].

Fig. 5 illustrates some of the subtypes of the UAV types presented in Fig. 4. Fig. 5a shows a Single rotor UAV with one main rotor to generate lift and a tail rotor for control. Figs. 5e and 5i represent a Quadcopter with four rotors arranged in a square configuration and a Hexacopter with six rotors arranged in a hexagonal configuration, respectively. Fig. 5b demonstrates a V-tail UAV with an inverted V-shaped tail, Fig. 5f displays a Delta-wing UAV with a triangular body-wing, and lastly, Fig. 5j demonstrates a VTOL UAV that can take off and land vertically like a quadrotor but has a fixed-wing body. Figs. 5c and 5g depict an Ornithopter UAV that mimics a bird's flight and a flying insect UAV that mimics an insect's flight, respectively. Figs. 5d and 5h depict a Blimp UAV and Balloon UAV filled with lighter-than-air gases that provide them with lift.

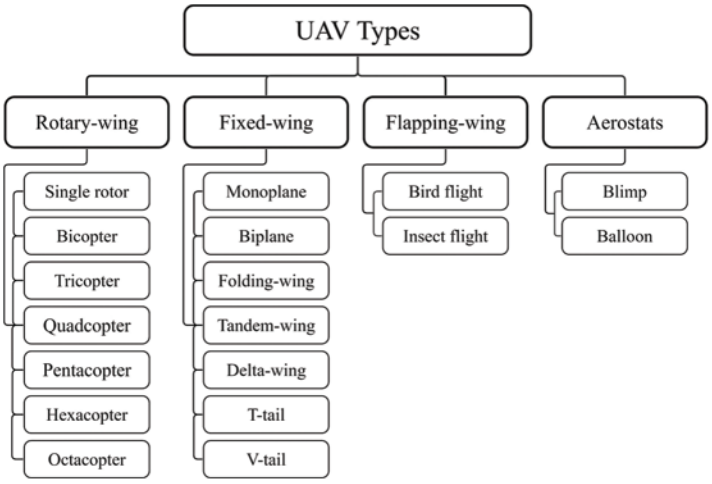

Figure 4: Classification of UAVs by their design type

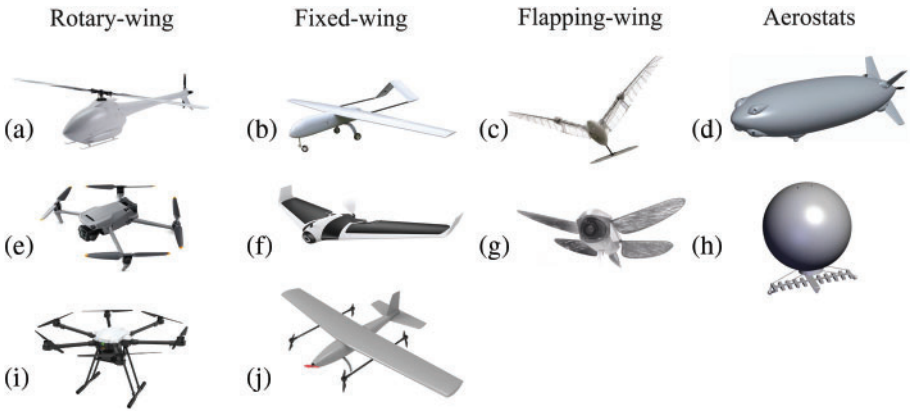

Figure 5: Rotary-wing, fixed-wing, flapping-wing, and aerostat subtypes: (a) Single rotor; (b) V-tail; (c) Ornithopter; (d) Blimp; (e) Quadcopter; (f) Delta-wing; (g) Flying insect prototype; (h) Balloon; (i) Hexacopter; (j) VTOL

3.3 Wireless Communication Link

The wireless communication link is arguably one of the most important parts of an autonomous UAV operation. When talking about the wireless communication link between a drone and a GCS, it can be split into two categories, namely: Visual Line of Sight (VLOS) and Beyond Visual Line of Sight (BVLOS) [75]. BVLOS communication can be realized using cellular or satellite area coverage. The wireless communication link enables data and command exchange between a UAV and a GCS. Command exchange from a GCS to a UAV includes particular steering commands, target location points, flight path, and mission commands and is referred to as uplink. Data exchange from a UAV to a GCS includes live telemetry feed as well as drone status updates and location info. It is referred to as a downlink. To enable the command exchange between a UAV and a GCS, a widely popular lightweight publish-subscribe and point-to-point messaging protocol called MAVlink [97] is often used. On the hardware side, open-source short-range 433/900 MHz telemetry radios are a popular option [98]. However, in most cases, the capacity of these radios is only sufficient for point-to-point and

low throughput communication, e.g., if other communication technologies are unavailable. The VLOS communication between a UAV and a GCS can be established using other wireless communication technologies such as Sub-GHz, LoRa Wi-Fi, or 5G/LTE. Additionally, when flying in a swarm, UAVs can communicate with one another by relying on the UWB modules, as well as all of the above-mentioned communication technologies. Each of these technologies has its own advantages and disadvantages. Some of the advantages of the Sub-GHz technology are low power consumption, long transmission range, multi-point and mesh communication support, and resistance to interference. On the other hand, the throughput and data transmission rates are quite low. LoRa Wi-Fi modules have a higher power consumption, smaller transmission range, and are more susceptible to interference and cyber-attacks. However, they offer significantly more throughput and higher data rates for shorter transmission distances. 5G/LTE cellular modules have similar power consumption as well as data throughput rates. However, data transmission rates and operational range depend heavily on cellular coverage, which is also its main disadvantage.

Due to the limitations in computational and energy resources, UAVs are disadvantaged in terms of data transmission privacy, security, and authenticity. They rely on lightweight communication protocols designed to be used without encryption or authentication, therefore making them vulnerable to such cyber-threats as Eavesdropping, Man-in-the-Middle, Jamming, and Replay attacks. Fig. 6 represents information, telemetry, and command exchange flow between a UAV, GCS, and the environment.

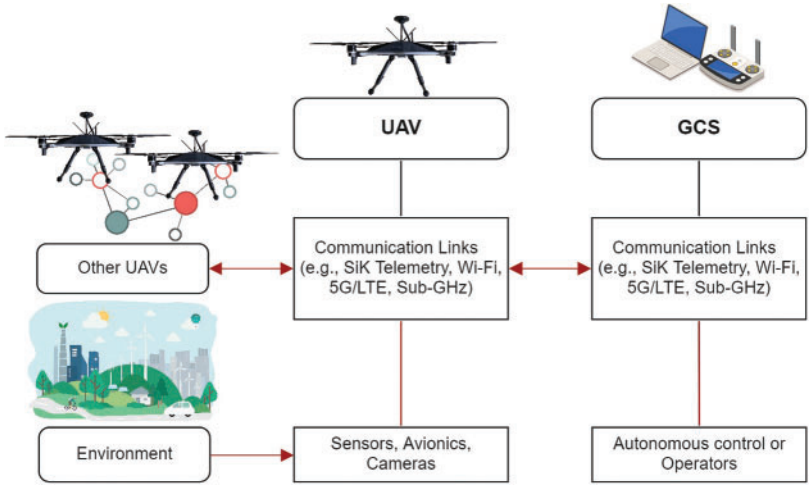

Figure 6: Information flow between UAVs, GCS, and the environment

3.3.1 UAV Swarm Communication Architecture

UAV swarms can be operated using a centralized or distributed communication architecture. Fig. 7 represents the division and subtypes of both communication architectures. In a centralized communication architecture, each swarm member is directly connected to the GCS in a centralized communication architecture. However, in this case, peer-to-peer communication between the UAVs is usually unavailable. The connection can be established using short-range telemetry radios, Sub-GHz radios, LoRa Wi-Fi, 5G/LTE, or a Satellite. Fig. 8 below represents centralized communication architectures. Fig. 8a depicts short-range VLOS communication, whereas Figs. 8b and 8c illustrate mid-range and long-range BVLOS communication.

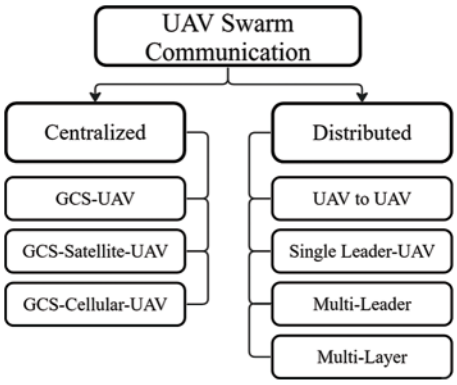

Figure 7: Classification of the UAV swarm communications

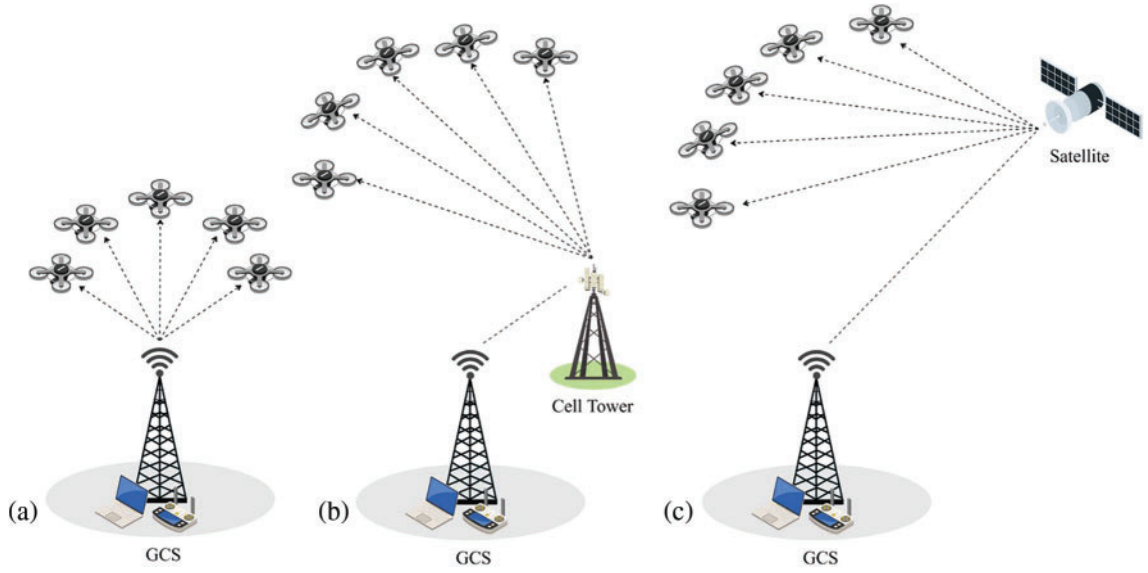

Figure 8: Centralized UAV swarm communication architecture: (a) short-range VLOS communication; (b) mid-range BVLOS communication; (c) long-range BVLOS communication

In a distributed communication architecture, a swarm of UAVs communicates in a peer-to-peer fashion without requiring a central authority such as GCS [99]. Distributed communication architecture can provide flexibility and robustness but may also require more sophisticated communication algorithms and protocols to be efficient [100]. Fig. 9 represents distributed UAV swarm communication architectures. In Fig. 9a, a single leader UAV acts as a mediator between the GCS and the other UAVs that form an ad-hoc network. The communication within the formed ad-hoc network could be performed using UWB radios or any other above-mentioned short-range communication technologies. The communication between the leader UAV and the GCS can take place using the same short-range or other mid-, and long-range communication technologies. However, in this architecture design, the single point of failure is the leader UAV. Fig. 9b depicts the architecture where multiple leader UAVs coordinate separate smaller subgroups of UAVs. The leader UAVs are connected to the GCS in a centralized manner, but the subgroup communication is conducted internally without the GCS. Fig. 9c illustrates a multi-layer architecture where the upper layer ad-hoc network consists

of the leader UAVs and the lower layer ad-hoc networks consists of the subordinate UAVs. The upper-layer UAVs can communicate with the subordinate lower-layer ad-hoc networks as well as with the GCS, thus eliminating the single point of failure vulnerability.

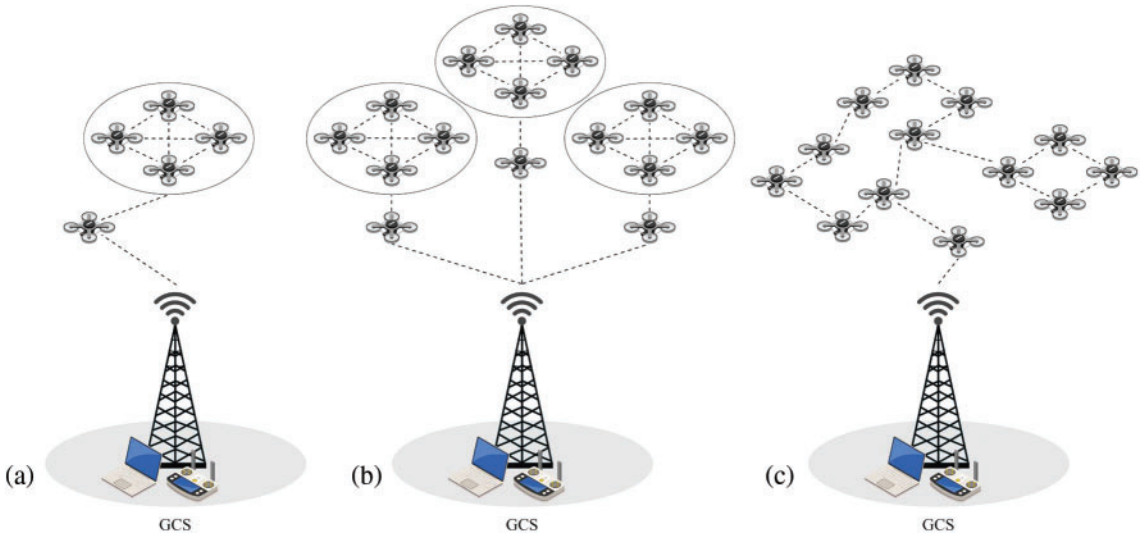

Figure 9: Distributed UAV swarm communication architecture: (a) Single-leader; (b) multi-leader; (c) multi-layer

3.4 Security and Safety Requirements

The availability of the UAV is essential for mission execution and operation. UAVs have to stay accessible to authorized users like a remote pilot or GCS and vice versa at all times for communication, mission adjustments, and updates. Any unintentional communication interruptions or intentional attacks targeting the availability of a UAV have to be detected and mitigated as soon as possible to ensure UAV's safety. Attacks that disrupt availability can be carried out by interfering with the link that is used to communicate the information between a UAV and a GCS. To disrupt the communication, an attacker often either occupies the communication channel or floods it with a significant volume of random traffic. This renders the communication resources between the UAV and GCS inaccessible. Availability attacks can be further subdivided into Communication or GPS Jamming [101] and Network flooding or Denial of Service (DoS) [71] attacks. During the availability attack, the adversary can prevent or delay important real-time monitoring from reaching the ground station, thus putting UAV's safety at risk. Availability attacks can be conducted without substantial expertise or information about the target, thus rendering their execution relatively probable.

The integrity of the transmitted data is a crucial security and safety requirement of the UAV operation. The most common attacks targeting data integrity are Man-in-the-Middle attack [102], Replay attack [103], GPS and other Sensor Spoofing [104], and Hijacking attack [105]. Integrity attacks are carried out by either altering the transmitted data or inserting malicious data to overwrite the genuine data. Compromising data integrity could lead to malicious control of the UAV by an adversary resulting in mission failure, drone theft, or a crash. To prevent that from happening, wireless communication has to be secured through authentication mechanisms such as message signing and incorporation of a timestamp to render these attacks ineffective.

Confidentiality of the transmitted data is another critical part of UAS's security. Without data confidentiality, sensitive information such as control commands from the GCS and UAV's location coordinates can be easily intercepted by an attacker. By intercepting the communication data, an attacker gains unauthorized access to confidential information. Most confidentiality attacks are passive, where the adversary gains access to the communication between the UAV and the GCS without interfering in order to stay undetected. Confidentiality attacks can be further specified into eavesdropping attacks, identity Spoofing attacks [55], unauthorized access attacks, and traffic analysis attacks [106]. To mitigate all of the above-mentioned attacks, a cryptographic solution such as an encryption algorithm, has to be implemented into the wireless communication channel between the UAV and GCS. Fig. 10 depicts the cyber-attacks targeting UAV's availability, integrity, and confidentiality.

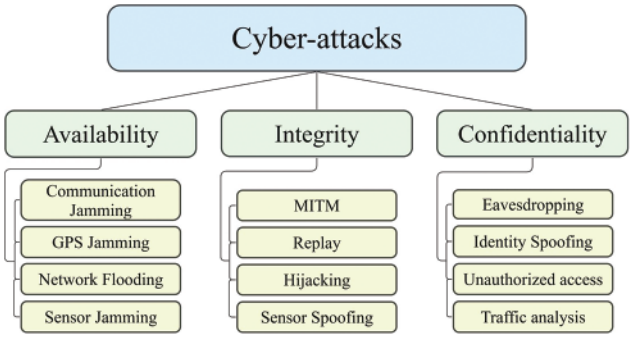

Figure 10: Cyber-attacks on UAV's availability, integrity, and confidentiality

Safety of the UAV operation, flight, and mission execution involve human safety, the safety of any property that may be present in the environment, and the safety of the UAV itself. To ensure the safety of all of the above-mentioned elements, a few important requirements have to be implemented into the UAV's design as well as hardware and software architecture. The first important requirement is to offer redundancy in the system's hardware architecture for the most critical subsystems to provide a fallback option in the event of a malfunction or cyber-attack. The second important requirement is to use isolated power domains for optional hardware components that can be powered on and off by request to compensate for sudden voltage collapse and isolate faulty hardware without affecting the entire system. The third important requirement is to ensure that the hardware components, such as companion computers, have the computational throughput to guarantee a safe system operation. It is critical for UAV safety to use fail-safe mechanisms for collision prevention and handling of other emergencies, such as communication link or GPS signal loss, detection of a Jamming or other cyber-attack, sensor failures, and sensor measurements implausibility. An essential safety requirement is the integration of a collision avoidance algorithm to avoid collisions with other UAVs as well as other stationary objects like buildings or trees to ensure a successful mission execution.

4 Sensor- and Communication-Based Vulnerabilities, Threats, Attacks and Countermeasures

This section describes the taxonomy of communication-based and sensor-based vulnerabilities, threats, attacks, and available countermeasures. It is worth pointing out the main differences between a vulnerability and a threat to give a bit more insight. A vulnerability is a weakness or a flaw in the hardware, software, system design, or architecture which an adversary could exploit to achieve their malicious goal. In other words, attackers can find their way into the system. Vulnerabilities expose

the system to threats and attacks, therefore increasing their probability. A threat is an incident during which the vulnerability could be exploited to achieve a malicious objective, such as theft, illegally acquiring data, damaging or destroying the UAV and objects around it, etc. A threat significantly impacts the system's security, whereas vulnerability might exist without causing any harm until exploited. We decided to categorize the security vulnerabilities, threats, and attacks according to the affected system components into sensor-based and communication-based categories. Fig. 11 visualizes the transition from a security or safety vulnerability to a cyber-attack.

Figure 11: Transition vector of the security and safety issues

4.1 Sensors-Based Vulnerabilities, Threats, and Attacks

Table 2 below presents an overview of the literature's sensor-based vulnerabilities, threats, attacks, and countermeasures. Accurate analysis of the vulnerabilities, threats, and attacks allows for an improved system design and efficient integration of countermeasures into the system architecture. One of the main difficulties when conducting such analysis is the lack of unified design and standardization in the UAV's system architecture due to the broad range of its applications. Nevertheless, as mentioned above, such cyber-physical systems as UAVs constantly interact with the environment and rely heavily on sensor measurements for operation and navigation, making them vulnerable to sudden changes in weather conditions and cyber-physical sensor attacks. In hostile environments, compromised sensor readings might cause the system to fail and crash. Intentional electromagnetic interference, for instance, could interfere with critical system components like gyroscopes and accelerometers and significantly degrade the quality of the measurements vital for drone stabilization and flight control [107]. To operate efficiently, UAVs use optical flow and LiDAR sensors for obstacle detection and localization. These sensors are especially crucial for autonomous navigation and collision avoidance algorithms [108]. However, in practice, experiments in [55] and [109] have shown that these sensors are vulnerable to laser attacks. Most civilian UAVs also use unencrypted and unauthenticated GPS signals for navigation, which makes them vulnerable to GPS Spoofing and Jamming attacks [84,85]. GPS Spoofing and Jamming attacks can also take place simultaneously. For example, an attacker can start a GPS Jamming attack to disconnect the UAV from an authentic GPS satellite, followed by an immediate execution of a GPS Spoofing attack. During the GPS Spoofing attack, an adversary takes advantage of the low signal power of civil GPS signal and overpowers it with a fake GPS signal coming from a transmitter nearby, resulting in an incorrect estimate of the UAV's current location. If the attack mentioned above is successful, an adversary can navigate the UAV to a desired location or even force it to land by transmitting the no-fly zone coordinates.

4.1.1 Countermeasures

To mitigate the effects of intentional electromagnetic interference on MEMS gyroscopes, in [110], the authors suggested shielding the gyroscope from acoustic resonance attacks and improving the sensor's structural characteristics to render these attacks ineffective. To cope with the acoustic attacks on the accelerometer, in [111], the authors suggested a redesign of the internal components to handle acoustic interference, and developed software defense mechanisms for the sensors already deployed in the field. To defend optical flow sensors from laser attacks, in [55], the authors suggested replacing the standard averaging flow algorithm with the random sample consensus (RANSAC) algorithm. The effects of a laser attack on the optical flow sensor were reduced significantly with the use of a suggested RANSAC algorithm.

Table 2: Sensor-based vulnerabilities, threats, attacks, and countermeasures

Vulnerability	Cyber—physical threat/attack	Countermeasures
Vulnerability of MEMS sensors to acoustic attacks	Intentional electromagnetic and acoustic interference on MEMS gyroscope and accelerometer [107,111]	Sensors shielding and isolation [110]; improving the hardware design [111]
Optical flow sensor vulnerability to laser attacks	Laser attack on the optical flow sensor [55]	Modification of the operation algorithm [55]
Vulnerability of LiDAR sensors to optical signal attacks	Optical signal attacks on LiDAR [109]	Attack identification and mitigation mechanism [109]
Unencrypted and unauthenticated GPS signals	GPS spoofing attack [84,112]	Using authenticated and encrypted GPS signals; spoofing attack detection mechanisms [112,113]
Dependency on the GPS signals for autonomous navigation	GPS Jamming attack [85]	Return-to-home in GPS—denied environment [114]; mitigation of the GPS Jamming effect [115]

To protect the LiDAR modules against optical signal attacks, the authors in [109] suggested a framework consisting of attack detection and mitigation. The detection method is based on using the data from three sensors (two cameras and one LiDAR) to obtain two versions of disparity maps and then detect an attack by analyzing the distribution of disparity errors. Thus, the affected LiDAR sensors are detected and their measurements are temporarily substituted by the available cameras. To detect a GPS Spoofing attack, the authors in [112] differentiated between processing the received GPS signal properties and using additional sensors to aid the detection process. They mention a GPS Spoofing detection method based on the Received Signal Strength Indicator (RSSI) of the received GPS signal. In [113], the authors proposed a vision-based GPS Spoofing detection mechanism based on using visual odometry. This method compares the relative sub-trajectory of a UAV from real-time visual odometry with its simulated replica from GPS within a moving window along the flight path and thus, if the deviation is present, the attack is declared detected. In [114], the authors proposed a mechanism to safely execute the return-to-home maneuver during a GPS Jamming attack based on repurposing the received telemetry radio signal's angle of arrival to mitigate the effects of GPS

Jamming attacks. By analyzing the received signal's angle of arrival, UAV is navigated back to the base station, where it could land safely by the GSC operator. In [115], the authors proposed a low-cost anti-Jamming system based on using cascaded adaptive notch filter modules. These modules are composed of second-order infinite-impulse response filters with a lattice structure and are able to mitigate one continuous wave of interference each, thus mitigating the effects of a Jamming attack.

In [116], the authors claimed that GPS Spoofing and Jamming attacks are the most common types of cyber-attacks on UAVs registered so far, with 53% of all of the cyber-attacks present in their literature, respectively. Table 3 represents an overview of sensor-based threats, attacks, and countermeasures divided into two categories, namely sensor channel attacks with fault injection and GPS Spoofing and Jamming attacks.

Table 3: Sensor-based security threats, attacks, and countermeasures present in the reviewed literature

Type of cybersecurity threat/attack	Name of the cyber physical threat/attack	Provided an overview	Proposed countermeasures
Sensor-based	Sensor channel attacks and fault injection	[43,47,54,55,60,63–65,67,69,70,72–75,107,109,111]	[43,47,55,60,65,69,74,75,109–111]
	Spoofing/Jamming of the GPS signal	[53,58,59,61,62,64–68,70–77,84,85,117]	[59,61,65,66,68,69,72,74,75,113–115]

4.2 Communication-Based Vulnerabilities, Threats, and Attacks

To execute autonomous missions, UAVs have to maintain a stable connection with the GCS for flight control and data exchange at all times. Wireless communication among the UAVs in a swarm is also crucial for avoiding collisions and enabling data exchange within a swarm. The wireless communication link between a UAV and a GCS is often the weakest part of the UAS architecture due to its mostly unencrypted and unauthenticated nature [118]. One of the easiest and most common ways for attackers to disrupt the communication between a UAV and a GCS is to jam the wireless data exchange [119]. On a physical layer, the easiest way to disrupt communication is to execute a Jamming attack by overpowering the authentic radio signal with a stronger interfering signal of the same frequency, thus overriding the authentic signal and blocking the receiver from acquiring the intended data. If a Jamming attack is effective, UAV loses connection with GCS and goes into fail-safe mode, often returning back to the launch position [103]. Jammers can be proactive or reactive. Reactive Jammers scan the environment for the presence of wireless communication. If the communication is detected, only then the Jamming attack is initiated. On the other hand, Proactive Jammersonstantly emit interfering signals regardless of whether the communication occurs [120]. A Jamming attack on a network layer is sometimes referred to as a DoS attack and is executed by flooding the network with a large number of artificial requests, thus restricting legitimate users from using the network [121]. A DoS attack could be launched in three different ways: buffer overflow, flooding of the network, and Spoofing of the transmission packets. Because the communication channel between a UAV and GCS is often public, unencrypted, and unauthenticated, the risk and possibility of a Man-in-the-Middle attack rise significantly. During the Man-in-the-Middle attack, the attacker eavesdrops on the communication and acts as a mediator between the UAV and the GCS. The adversary intercepts outgoing packets from the sender, modifies them, and forwards them to the recipient, making it look

like they came from a trusted source [71]. By executing the Man-in-the-Middle attack, an attacker can prematurely end the mission or even take full control of the UAV by modifying the steering commands.

The use of an unsecured communication channel poses a risk of another cyber-attack, namely a message Replay attack. During the Replay attack, the adversary eavesdrops on the communication link and records a sequence of legitimate commands sent between a UAV and a GCS. The recorded commands are then played back at a different point in time to achieve a malicious goal. This attack is countered by ensuring the integrity of the exchanged data and embedding a timestamp with each sent message. However, only including the timestamp alone without ensuring data integrity is not sufficient to mitigate the effects of a Replay attack because the attacker can falsify the timestamp to appear up to date and thus, still achieve their malicious objective.

Unsecured communication channels are also vulnerable to another type of passive cyber-attack called Eavesdropping which violates the confidentiality of the transmitted data. Eavesdropping could be applied to both uplink and downlink communication. Eavesdropping on the uplink is done mainly to gather reconnaissance on the mission plans and GPS location coordinates of the UAV or GCS. Eavesdropping on the downlink could reveal a live video feed, confidential photos, and sensor readings [75].

Table 4 below presents an overview of the communication-based vulnerabilities, threats, attacks, and countermeasures available in the literature.

4.2.1 Countermeasures

To counter the effects of a Jamming attack on the physical level of the communication link, a Jamming detection mechanism based on the signal properties such as RSSI, Packet Delivery Ratio (PDR), and ML techniques was proposed in [122]. In [123], the authors proposed a spectrogram-tailored ML method able to detect four types of Jamming attacks, namely barrage, protocol-aware, single-tone, and successive-pulse. To mitigate the effects of a Jamming attack on a network level of the communication link, also referred to as a DoS attack, authors in [124] developed an Intrusion Detection System operated by a deep machine learning algorithm based on previously experienced DoS attacks. To tackle Man-in-the-Middle attacks, the authors in [125] proposed a lightweight digital signature protocol solution to authenticate the communication and, thus, validate each received command by comparing the signatures. To detect Replay attacks, in [126], the authors suggested an approach based on training a ML algorithm on the pilot's behavior to recognize malicious control commands distinct from the regular pilot's flying manner. Their approach is based on the assumption that every UAV operator has a distinct flying pattern when it comes to controlling a UAV using RC's levers or joysticks. The operator's behavior is defined by the sequence of flight commands sent to the drone using a standard radio control transmitter.

Physical Layer Security

The physical layer is the lowest layer of the communication protocol stack. It deals with the transmission and reception of the physical signals using the responsible hardware over the communication channel. Physical Layer Security (PLS) refers to the utilization of techniques and measures to protect the wireless communication link between the UAV and the GCS from interference, interception, and unauthorized access. Some of the most common PLS techniques are hardware accelerated encryption, spread spectrum techniques such as Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS), transmitted signal power control, and the use of directional antennas. However, recently, a few novel techniques have been proposed to enhance PLS for UAVs. The authors

proposed UAV-enabled mobile relayingn [127]. To improve the security of wireless communication link, the authors implemented a buffer-aided mobile relay. This allowed data to reach the intended receiver more quickly and independently, which is crucial for real-time applications. The authors employed Reconfigurable Intelligent Surfaces (RIS)n [128] to assist the wireless transmission from the UAV to the GCS in the presence of an eavesdropper. RIS are planar structures composed of several simple passive components, such as antenna arrays or metamaterials. Metamaterials consist of tiny repetitive structures containing meta-atoms arranged in a certain pattern to produce the necessary electromagnetic characteristics. RIS can be electronically controlled to reflect, transmit, or absorb electromagnetic waves, allowing for wireless communication and sensing systems to adapt to changing environmental conditions. The authors aimed at maximizing security by jointly optimizing the phase shifts of RIS as well as the transmit beamforming vector and location of the UAV. In [129], the authors suggested using physical layer network features to generate a high rate of artificial noise to secure the data transmission between two UAVs in the presence of a passive eavesdropper. Artificial noise technology refers to the deliberate addition of noise to a communication channel to enhance its security and confidentiality. This technique is used in wireless communication systems to prevent eavesdropping and interference by creating random interference signals that are superimposed on the transmitted signal. By doing so, it becomes more difficult for unauthorized users to decode the signal, as they would also have to filter out the random noise. The authors employed auto-encoder/decoder convolutional neural networks trained by deep learning algorithms to compress and un-compress images. By introducing artificial noise to the transmission channel, the authors reduced the channel capacity available for unauthorized users and thus prevented eavesdroppers from detecting data transmission.

In summary, physical layer security in UAVs involves employing a combination of different techniques to protect the wireless communication link from unauthorized access, interference, and interception and allows to ensure reliable and secure wireless communication between the UAVs and the GCS.

Table 4: Communication-based vulnerabilities, threats, attacks, and countermeasures

Vulnerability	Cyber—physical threat/attack	Countermeasures
Dependability of autonomous operation on communication with GCS	Jamming attack [101]	Jamming detection and mitigation mechanisms [120,122,123,130]
Unauthenticated radio communication	Man-in-the-Middle attack [71]	Authentication mechanisms [125]
Unauthenticated radio communication and lack of a timestamp	Replay attack [103]	Detection mechanisms and introduction of a timestamp [126,131,132]
Unencrypted radio communication	Eavesdropping attack [133]	Encrypted and authenticated communication [52],

In [131], the authors simulated a frequency based Replay attack detection mechanism by comparing the energy of a sine wave with a time-varying frequency introduced into the closed-loop system. They checked if the time profile of the frequency components in the output signal is compatible with the authentication signal. To mitigate the effect of a Replay attack, in [132], the authors introduced

a timestamp for each message and suggested a mechanism to estimate the time needed for receiving and validating the message and compare it with the actual time it takes to receive and validate the message by the receiver. If the difference between the estimated and actual time is larger than the threshold, a Replay attack is then declared detected. In [52], the authors integrated a few different encryption algorithms into the MAVlink communication protocol on a network level to provide exchanged data confidentiality. The simulation showed that Eavesdropping attacks on the encrypted MAVlink communication can be countered. In [116], the authors concluded that a Jamming attack on the communication link is the second, after GPS Jamming attack, a most common type of cyber-attack on UAVs registered so far, representing 32% of all of the cyber-attacks in their reviewed literature, respectively.

Table 5 below represents a literature overview of the communication-based threats, attacks, and countermeasures divided into five sub-categories according to each cyber-physical threat/attack. These include Jamming of the communication link, Man-in-the-Middle attack, Replay attack, and Eavesdropping on the communication link.

Table 5: Communication-based security threats, attacks, and countermeasures present in the reviewed literature

Type of cybersecurity threat/attack	Cyber physical threat/attack	References providing an overview	References providing countermeasures
Communication — based	Jamming attack on the communication link	[40,54,62,65,66,68,70,72–77,134]	[40,54,68,72–77]
	Man-in-the-Middle attack	[40,57,62,74–77]	[40,52,57,74–77]
	Replay attack	[58,62,73–77]	[74–77]
	Eavesdropping on the communication link	[40,66,69,74–77]	[40,52,74–77]

5 Plausibility Check of Sensor Measurements

As already stated, UAVs rely heavily on sensor measurements to fly, navigate and avoid environmental obstacles. Therefore, it is important to ensure the sensors' measurements are authentic and not erroneous, modified, or spoofed through sensor-based attacks. Accelerometer, gyroscope, magnetometer, barometer, GPS receiver, ultrasonic proximity, laser proximity, UWB, and LiDAR sensors are just a few of the variety of possible sensors carried onboard a UAV. Additionally, drones can serve as active sensor platforms to gather various sensor measurements and accomplish mission tasks. UAV sensors are regularly subjected to unforeseen changes in flying conditions. Combined with the volatile flying environment, the risk of a sensor failure inevitably increases. For instance, incorrect distance measurements to objects or other UAVs can result in a collision that otherwise could be avoided if the sensor measurement were verified for plausibility. To ensure the UAV's safety, stable and consistent operation, and fulfillment of the mission's objective, a time-sensitive plausibility check of sensor measurements must occur.

Plausibility check of sensor measurements is a method for determining if the data obtained by the sensor is plausible, i.e., acceptable and reasonable. It involves comparing sensor readings to a set of predicted or probable values to determine if they fall within an acceptable range. One way of

confirming or denying the plausibility of sensor measurements is to examine and compare the data from different sensors that, in theory, should be identical and assert its plausibility or implausibility based on the comparison. It is not always feasible to check the accuracy of sensor measurements, but any apparent faults, failures, malfunctions, errors, or deviations should be detected using the plausibility check. A plausibility check has the benefit of not being as computationally intensive as ML or AI algorithms because it does not require a substantial analysis of the measured data, unlike ML or AI algorithms. That could be an advantage due to the limitations and constraints in terms of computational resources and latency requirements, as well as a disadvantage due to the inability to detect sophisticated deviation patterns simultaneously. Realization of the plausibility check requires multiple sources of the measured data for comparison. Hardware redundancy is one of the most common plausibility checks in hardware. Having multiple sensors taking measurements simultaneously and then comparing them to enable error or malfunction detection allows for ensuring a plausible result. Fig. 12 depicts an integration example of a plausibility check into the UAV's sensor data processing pipeline. Raw sensor data that might contain influence from electromagnetic noise, sensor faults, or cyber-attacks is checked for plausibility and only then utilized further for navigation, stabilization, and flight control or collision avoidance purposes.

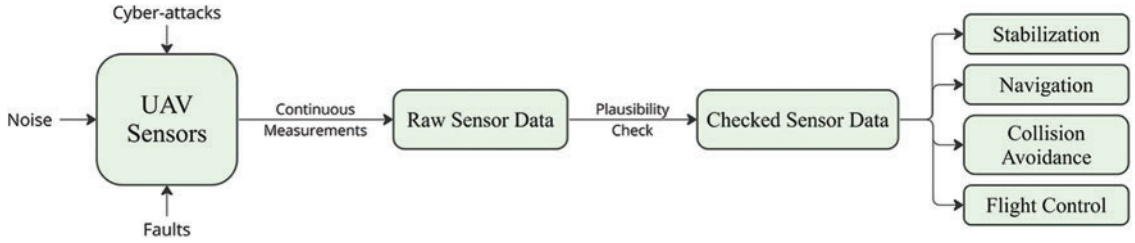

Figure 12: Plausibility check integration example into the sensor data processing pipeline

In real-time applications, there are several limitations that a plausibility check of sensor measurements might face. Time constraint is one of them. Plausibility checks must be conducted quickly enough to ensure that sensor data is processed in real-time and no delays or additional overhead is introduced. Otherwise, it might bring more harm than benefit. Computational resources constraint is another one. To confirm or deny the plausibility of sensor data, a set of necessary computational operations has to be performed. Therefore, ensuring that the plausibility check can be performed without undermining other subsystems' performance is important. Physical constraints of the sensors, such as range, resolution, or sensitivity, can impact the quality, accuracy, and reliability of a plausibility check. Sensor drift, noise, and bad weather conditions might also contribute to measurement inaccuracies. This must be taken into account when designing the plausibility check mechanism. It is crucial to consider these limitations while developing a plausibility check for real-time applications. The plausibility check mechanism and other error correction techniques and signal processing algorithms can ensure accurate and reliable sensor measurements.

An example of the plausibility check implemented in software could be a verification algorithm for the distance measurement between UAVs through the difference in their GPS coordinates and through the UWB ranging taken between them, as illustrated in Fig. 13. By comparing both distances, we can confirm or deny their plausibility. A plausibility check can also serve as an additional indicator for sensor attack detection. Table 6 below presents some examples of the plausibility check in UAVs.

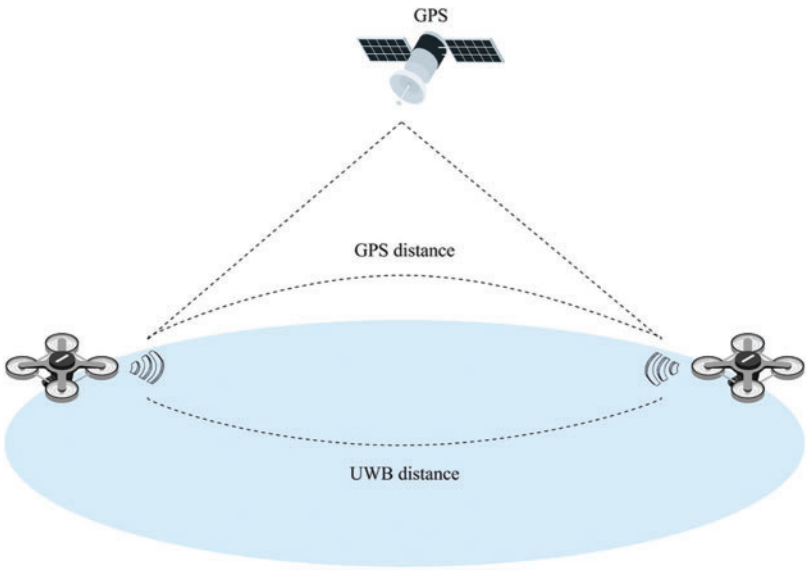

Figure 13: Plausibility check of the measured distance between two UAVs

Fig. 14 represents possible standalone techniques that can be combined or used independently to implement the plausibility check and ensure a stable and robust UAV operation. Hardware and software redundancy are among the most common techniques to ensure the plausibility of measured data. However, as already stated above, installing redundant hardware is not always feasible due to numerous limitations. ML and ANN techniques have opened a novel approach to anomaly detection [135]. They overcome the drawbacks of rule-based and signature-based techniques by effectively detecting unforeseen threats [136]. However, they are not optimal for computationally constrained and power-limited applications.

Table 6: Examples of sensor measurement plausibility confirmation

Name of a vulnerability	Type of a threat	Type of a sensor	Plausibility check
Implausible sensor measurements	GPS Spoofing attack	GPS receiver	GPS *vs*. UWB distance comparison [137]
Implausible sensor measurements	Sensor error	Altitude sensor	Providing redundant hardware components

FDI methods can be divided into Model-based, Knowledge-based, Analytical redundancy, and Signal processing [138]. A Model-based approach is built on a mathematical model, whereas the Knowledge-based approach is not dependent on a model but is rather constructed around the knowledge of the past system's performance. Analytical redundancy employs analytical relationships explaining the dynamical interconnection between system components, whereas Signal processing utilizes signal measurements instead of a system model, extracts signal characteristics and diagnoses faults with appropriate signal analysis and prior knowledge of the correct system state [139]. FTC can be passive, active, or hybrid. Passive FTC is designed for specific hardware faults, relying on a predefined description of a fault, and cannot dynamically adjust to the new types of faults. Active FTC, conversely, does not rely on specific fault descriptions but rather on FDI to detect faults and can

readjust the system parameters for optimal performance [140]. Hybrid FTC combines both techniques. Mutual verification combines and compares sensor measurements obtained from principally different types of sensors, measuring identical values. Thus, if the comparison demonstrates inconsistencies, it is the first sign of implausibility. Depending on the UAV system characteristics and requirements, the techniques described above can be combined or used separately to conduct the plausibility check of sensor data and ensure a safe and secure UAV operation.

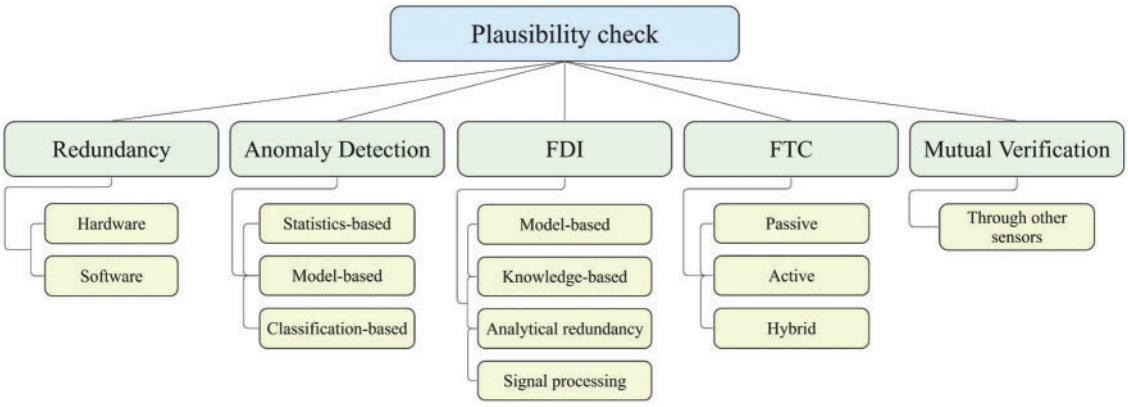

Figure 14: Techniques that can be used to implement the plausibility check

6 Conclusion

With the current pace of advancements in UAS technology, it is becoming clear that the number of UAVs autonomously and semi-autonomously roaming the sky to fulfill their missions will substantially increase in the next years. Taking that into account, it is important to ensure that they do so safely without endangering the people and environment around them. In this paper, we described the common UAS architecture to examine and pinpoint the sources of security and safety issues of a common UAS platform right at the beginning of its architectural design. We illustrated the key components of a common UAS architecture and different UAV design types and provided a list of security and safety requirements they have to meet in order to reduce or even fully eliminate the risk of being affected by a cyber-attack. We surveyed state-of-the-art literature to identify the most common cyber-attacks on UAVs and reflected them in a diagram. The surveyed literature was also evaluated for completeness and coverage of the vulnerabilities, threats, cyber-attacks, and countermeasures presented in the form of a comprehensible table. Additionally, we provided a clear definition between the security vulnerabilities, threats, and attacks and grouped them into sensor-based and communication-based categories, followed by an explanation of their reasoning. Furthermore, we discussed possible solutions in the literature to mitigate and eliminate the security and safety concerns mentioned above. Next, we introduced the idea of a plausibility check for sensor measurements, its benefits, and possible ways of its implementation. Finally, by discussing the plausibility check of sensor data, we have established the research area in terms of security and safety that is not well represented in the literature and, thus, requires additional attention.

Acknowledgement: The authors would like to acknowledge that this work would not have been possible without the support of the Brandenburg University of Technology Cottbus-Senftenberg and Leibniz Institute for High Performance Microelectronics (IHP).

Funding Statement: This research has been partially funded by the Federal Ministry of Education and Research of Germany under Grant Numbers 16ES1131 and 16ES1128K.

Author Contributions: The authors of this paper have contributed equally to the research and writing of this manuscript. The authors have collaborated closely throughout the entire research process, engaging in discussions and sharing ideas to foster a comprehensive review of Sensor-based and Communication-based issues of autonomous UAV swarms. All of the authors approved the final submitted version of this manuscript.

Availability of Data and Materials: All the reviewed research literature and used data in this research paper consists of publicly available scholarly articles, conference proceedings, books, and reports. The references and citations are contained in the reference list of this manuscript and can be accessed through online databases, academic libraries, or by contacting the respective publishers.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Amazon Staff (2022). Amazon prime air prepares for drone deliveries. https://www.aboutamazon.com/news/transportation/amazon-prime-air-prepares-for-drone-deliveries
2. Heutger, M., Kückelhaus, M. (2014). Unmanned aerial vehicles in logistics: A DHL perspective on implications and use cases for the logistics industry. DHL Customer Solutions & Innovation.
3. Zipline Instant Delivery & Logistics (2023). Technology. https://www.flyzipline.com/technology
4. Wingcopter Solutions (2023). https://wingcopter.com/solutions
5. SkyDrop Delivery Drone (2023). https://getskydrop.com/
6. Alvear, O., Zema, N. R., Natalizio, E., Calafate, C. T., Yu, G. (2017). Using UAV-based systems to monitor air pollution in areas with poor accessibility. *Journal of Advanced Transportation, 2017,* 8204353. https://doi.org/10.1155/2017/8204353
7. Yao, H., Qin, R., Chen, X. (2019). Unmanned aerial vehicle for remote sensing applications—A review. *Remote Sensing, 11(12),* 1443. https://doi.org/10.3390/rs11121443
8. Trotta, A., di Felice, M., Montori, F., Chowdhury, K. R., Bononi, L. (2018). Joint coverage, connectivity, and charging strategies for distributed UAV networks. *IEEE Transactions on Robotics, 34(4),* 883–900. https://doi.org/10.1109/TRO.2018.2839087
9. Schofield, G., Katselidis, K. A., Lilley, M. K. S., Reina, R. D., Hays, G. C. (2017). Detecting elusive aspects of wildlife ecology using drones: New insights on the mating dynamics and operational sex ratios of sea turtles. *Functional Ecology, 31(12),* 2310–2319. https://doi.org/10.1111/1365-2435.12930
10. Huang, H., Savkin, A. V., Li, X. (2020). Reactive autonomous navigation of UAVs for dynamic sensing coverage of mobile ground targets. *Sensors, 20(13),* 3720. https://doi.org/10.3390/s20133720
11. Abdelkader, M., Fiaz, U. A., Toumi, N., Mabrok, M., Shamma, J. (2021). RISCuer: A reliable multi-UAV search and rescue testbed. arXiv:2006.06966.
12. Stuchlík, R., Stachoň, Z., Láska, K., Kubicek, P. (2015). Unmanned aerial vehicle—Efficient mapping tool available for recent research in polar regions. *Czech Polar Reports, 5(2),* 210–221. https://doi.org/10.5817/CPR2015-2-18
13. Silvagni, M., Tonoli, A., Zenerino, E., Chiaberge, M. (2017). Multipurpose UAV for search and rescue operations in mountain avalanche events. *Geomatics, Natural Hazards and Risk, 8(1),* 18–33. https://doi.org/10.1080/19475705.2016.1238852

14. Surmann, H., Worst, R., Buschmann, T., Leinweber, A., Schmitz, A. et al. (2019). Integration of UAVs in urban search and rescue missions. *2019 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, pp. 203–209. Würzburg, Germany, 9/2/2019–9/4/2019. https://doi.org/10.1109/SSRR.2019.8848940
15. Lygouras, E., Santavas, N., Taitzoglou, A., Tarchanidis, K., Mitropoulos, A. et al. (2019). Unsupervised human detection with an embedded vision system on a fully autonomous UAV for search and rescue operations. *Sensors, 19(16),* 3542. https://doi.org/10.3390/s19163542
16. Kulkarni, S., Chaphekar, V., Uddin Chowdhury, M. M., Erden, F., Guvenc, I. (2020). UAV aided search and rescue operation using reinforcement learning. *SoutheastCon 2020*, Raleigh, NC, USA, 3/28/2020–3/29/2020, pp. 1–8. IEEE. https://doi.org/10.1109/SoutheastCon44009.2020.9368285
17. Hock, P., Wakiyama, K., Oshima, C., Nakayama, K. (2019). Drone monitoring system for disaster areas. 1686–1690. https://doi.org/10.1145/3319619.3326885
18. Erdelj, M., Król, M., Natalizio, E. (2017). Wireless sensor networks and multi-UAV systems for natural disaster management. *Computer Networks, 124,* 72–86.
19. Restas, A. (2015). Drone applications for supporting disaster management. *World Journal of Engineering and Technology, 3(3),* 316–321. https://doi.org/10.4236/wjet.2015.33C047
20. Estrada, M. A. R., Ndoma, A. (2019). The uses of unmanned aerial vehicles –UAV's-(or drones) in social logistic: Natural disasters response and humanitarian relief aid. *Procedia Computer Science, 149,* 375–383. https://doi.org/10.1016/j.procs.2019.01.151
21. Munawar, H. S., Ullah, F., Qayyum, S., Khan, S. I., Mojtahedi, M. (2021). UAVs in disaster management: Application of integrated aerial imagery and convolutional neural network for flood detection. *Sustainability, 13(14),* 7547. https://doi.org/10.3390/su13147547
22. Hildmann, H., Kovacs, E. (2019). Review: Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety. *Drones, 3(3),* 59. https://doi.org/10.3390/drones3030059
23. Reddy Maddikunta, P. K., Hakak, S., Alazab, M., Bhattacharya, S., Gadekallu, T. R. et al. (2021). Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE Sensors Journal, 21(16),* 17608–17619. https://doi.org/10.1109/JSEN.2021.3049471
24. Almalki, F. A., Soufiene, B. O., Alsamhi, S. H., Sakli, H. (2021). A low-cost platform for environmental smart farming monitoring system based on IoT and UAVs. *Sustainability, 13(11),* 5908. https://doi.org/10.3390/su13115908
25. Bacco, M., Berton, A., Ferro, E., Gennaro, C., Gotta, A. et al. (2018). Smart farming: Opportunities, challenges and technology enablers. *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, pp. 1–8. Tuscany, Piscataway, NJ, IEEE. https://doi.org/10.1109/IOT-TUSCANY.2018.8373043
26. Croptracker (2023). Drone technology in agriculture. https://www.croptracker.com/blog/drone-technology-in-agriculture.html
27. Rydberg, A., Söderström, M., Hagner, O., Börjesson, T. (2007). Field specific overview of crops using UAV (Unmanned Aerial Vehicle). In: *Precision agriculture '07*, pp. 357–364. https://doi.org/10.3920/978-90-8686-603-8
28. Delavarpour, N., Koparan, C., Nowatzki, J., Bajwa, S., Sun, X. (2021). A technical study on UAV characteristics for precision agriculture applications and associated practical challenges. *Remote Sensing, 13(6),* 1204. https://doi.org/10.3390/rs13061204
29. Islam, N., Rashid, M. M., Wibowo, S., Wasimi, S., Morshed, A. et al. (2021). Machine learning based approach for weed detection in chilli field using RGB images. *The International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery*, pp. 1097–1105. Cham: Springer. https://doi.org/10.1007/978-3-030-70665-4_119

30. Chebrolu, N., Labe, T., Stachniss, C. (2018). Robust long-term registration of UAV images of crop fields for precision agriculture. *IEEE Robotics and Automation Letters, 3(4),* 3097–3104. https://doi.org/10.1109/LRA.2018.2849603
31. DJI Enterprise (2023). Precision agriculture with drone technology. https://enterprise-insights.dji.com/blog/precision-agriculture-drones
32. Kabir, R. H., Lee, K. (2021). Wildlife monitoring using a multi-UAV system with optimal transport theory. *Applied Sciences, 11(9),* 4070. https://doi.org/10.3390/app11094070
33. Mangewa, L. J., Ndakidemi, P. A., Munishi, L. K. (2019). Integrating UAV technology in an ecological monitoring system for community wildlife management areas in Tanzania. *Sustainability, 11(21),* 6116. https://doi.org/10.3390/su11216116
34. Ventura, D., Bonifazi, A., Gravina, M. F., Belluscio, A., Ardizzone, G. (2018). Mapping and classification of ecologically sensitive marine habitats using unmanned aerial vehicle (UAV) imagery and object-based image analysis (OBIA). *Remote Sensing, 10(9),* 1331. https://doi.org/10.3390/rs10091331
35. Adams, K., Broad, A., Ruiz-García, D., Davis, A. R. (2020). Continuous wildlife monitoring using blimps as an aerial platform: A case study observing marine megafauna. *Australian Zoologist, 40(3),* 407–415. https://doi.org/10.7882/AZ.2020.004
36. Lopez-Tello, C., Muthukumar, V. (2018). Classifying acoustic signals for wildlife monitoring and poacher detection on UAVs. *2018 21st Euromicro Conference on Digital System Design (DSD)*, pp. 685–690. Prague, Piscataway, NJ, IEEE. https://doi.org/10.1109/DSD.2018.00006
37. Lee, S., Song, Y., Kil, S. H. (2021). Feasibility analyses of real-time detection of wildlife using UAV-derived thermal and RGB images. *Remote Sensing, 13(11),* 2169. https://doi.org/10.3390/rs13112169
38. Verband Unbemannte Luftfahrt. Analysis of the German drone market. https://www.verband-unbemannte-luftfahrt.de/en/analysis-of-the-german-drone-market
39. TechSci Research (2018). Global Drones Market Size, Share Growth, Trend and Forecast 202. https://www.techsciresearch.com/report/global-drones-market/1345.html
40. Yaacoub, J. P., Noura, H., Salman, O., Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things, 11,* 100218. https://doi.org/10.1016/j.iot.2020.100218
41. Lee, D., Hess, D. J., Heldeweg, M. A. (2022). Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis. *Technology in Society, 71,* 102079. https://doi.org/10.1016/j.techsoc.2022.102079
42. Abdilla, A., Richards, A., Burrow, S. (2015). Power and endurance modelling of battery-powered rotorcraft. *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 675–680. Hamburg, Germany, IEEE. https://doi.org/10.1109/IROS.2015.7353445
43. Abbaspour, A., Yen, K. K., Noei, S., Sargolzaei, A. (2016). Detection of fault data injection attack on UAV using adaptive neural network. *Procedia Computer Science, 95(4),* 193–200. https://doi.org/10.1016/j.procs.2016.09.312
44. Wang, W. (2016). You can hijack nearly any drone mid-flight using this tiny gadget. https://thehackernews.com/2016/10/how-to-hack-drone.html
45. D'Amato, E., Mattei, M., Notaro, I., Scordamaglia, V. (2018). UAV sensor FDI in duplex attitude estimation architectures using a set-based approach. *IEEE Transactions on Instrumentation and Measurement, 67(10),* 2465–2475. https://doi.org/10.1109/TIM.2018.2838718
46. Tu, Z., Fei, F., Eagon, M., Zhang, X., Xu, D. et al. (2018). Redundancy-free UAV sensor fault isolation and recovery. arXiv:1812.00063v1.
47. Guo, D., Wang, Y., Zhong, M., Zhao, Y. (2018). Fault detection and isolation for unmanned aerial vehicle sensors by using extended PMI filter. *IFAC-PapersOnLine, 51(24),* 818–823. https://doi.org/10.1016/j.ifacol.2018.09.669

48. Zhuang, Y., Sun, X., Li, Y., Huai, J., Hua, L. et al. (2023). Multi-sensor integrated navigation/positioning systems using data fusion: From analytics-based to learning-based approaches. *Information Fusion, 95(3),* 62–90. https://doi.org/10.1016/j.inffus.2023.01.025
49. Huang, X., Deng, H., Zhang, W., Song, R., Li, Y. (2021). Towards multi-modal perception-based navigation: A deep reinforcement learning method. *IEEE Robotics and Automation Letters, 6(3),* 4986–4993. https://doi.org/10.1109/LRA.2021.3064461
50. Li, D., Jia, X., Zhao, J. (2020). A novel hybrid fusion algorithm for low-cost GPS/INS integrated navigation system during GPS outages. *IEEE Access, 8,* 53984–53996. https://doi.org/10.1109/ACCESS.2020.2981015
51. Yang, T., Lu, Y., Deng, H., Chen, J., Tang, X. (2023). Acquisition and processing of UAV fault data based on time line modeling method. *Applied Sciences, 13(7),* 4301. https://doi.org/10.3390/app13074301
52. Allouch, A., Cheikhrouhou, O., Koubaa, A., Khalgui, M., Abbes, T. (2019). MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems. arXiv:1905.00265.
53. Vattapparamban, E., Guvenc, I., Yurekli, A. I., Akkaya, K., Uluagac, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. *2016 International Wireless Communications*, pp. 216–221. IEEE.
54. Altawy, R., Youssef, A. M. (2017). Security, privacy, and safety aspects of civilian drones. *ACM Transactions on Cyber-Physical Systems, 1(2),* 1–25. https://doi.org/10.1145/3001836
55. Davidson, D., Wu, H., Jellinek, R., Ristenpart, T., Singh, V. (2016). *Controlling UAVs with sensor input spoofing attacks*.
56. Hayat, S., Yanmaz, E., Muzaffar, R. (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Communications Surveys & Tutorials, 18(4),* 2624–2661. https://doi.org/10.1109/COMST.2016.2560343
57. Rodday, N. M., Schmidt, R. D. O., Pras, A. (2016). Exploring security vulnerabilities of unmanned aerial vehicles. *NOMS 2016–2016 IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey. https://doi.org/10.1109/NOMS.2016.7502939
58. Krishna, C. L., Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194–199. IEEE.
59. He, D., Chan, S., Guizani, M. (2017). Communication security of unmanned aerial vehicles. *IEEE Wireless Communications, 24(4),* 134–139. https://doi.org/10.1109/MWC.2016.1600073WC
60. Boche, A., Farges, J. L., de Plinval, H. (2017). Reconfiguration control method for multiple actuator faults on UAV. *IFAC-PapersOnLine, 50(1),* 12691–12697. https://doi.org/10.1016/j.ifacol.2017.08.2257
61. Dey, V., Pudi, V., Chattopadhyay, A., Elovici, Y. (2018). Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. *International Conference on Vlsi Design & International Conference on Embedded Systems*, pp. 398–403. IEEE Computer Society.
62. Choudhary, G., Sharma, V., Gupta, T., Kim, J., You, I. (2018). Internet of drones (IoD): Threats, vulnerability, and security perspectives. arXiv:1808.00203.
63. Shraim, H., Awada, A., Youness, R. (2018). A survey on quadrotors: Configurations, modeling and identification, control, collision avoidance, fault diagnosis and tolerant control. *IEEE Aerospace and Electronic Systems Magazine, 33(7),* 14–33. https://doi.org/10.1109/MAES.2018.160246
64. Fourlas, G. K., Karras, G. C. (2021). A survey on fault diagnosis and fault-tolerant control methods for unmanned aerial vehicles. *Machines, 9(9),* 197. https://doi.org/10.3390/machines9090197
65. Nassi, B., Shabtai, A., Masuoka, R., Elovici, Y. (2019). SoK—Security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps. arXiv:1903.05155.
66. Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L. G. et al. (2018). Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials,* 3417–3442.

67. Zhi, Y., Fu, Z., Sun, X., Yu, J. (2020). Security and privacy issues of UAV: A survey. *Mobile Networks and Applications, 25(1),* 95–101. https://doi.org/10.1007/s11036-018-1193-x
68. McCoy, J., Rawat, D. B. (2019). Software-defined networking for unmanned aerial vehicular networking and security: A survey. *Electronics, 8(12),* 1468. https://doi.org/10.3390/electronics8121468
69. Tan, Y., Wang, J., Liu, J., Zhang, Y. (2020). Unmanned systems security: Models, challenges, and future directions. *IEEE Network, 34(4),* 291–297. https://doi.org/10.1109/MNET.001.1900546
70. Guo, R. X., Tian, J. W., Wang, B. H., Shang, F. T. (2020). Cyber-physical attack threats analysis for UAVs from CPS perspective. *2020 International Conference on Computer Engineering and Application*, pp. 259–263.
71. Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C. et al. (2021). Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 23(4),* 2802–2832. https://doi.org/10.1109/COMST.2021.3097916
72. 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
73. Majeed, R., Abdullah, N. A., Mushtaq, M. F., Kazmi, R. (2021). Drone security: Issues and challenges. *International Journal of Advanced Computer Science and Applications, 12(5)*. https://doi.org/10.14569/IJACSA.2021.0120584
74. Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T. et al. (2021). Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access, 9,* 57243–57270. https://doi.org/10.1109/ACCESS.2021.3072030
75. Mekdad, Y., Aris, A., Babun, L., Fergougui, A. E. L., Conti, M. et al. (2021). A survey on security and privacy issues of UAVs. arXiv:2109.14442.
76. Tsao, K. Y., Girdler, T., Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks, 133,* 102894. https://doi.org/10.1016/j.adhoc.2022.102894
77. Siddiqi, M. A., Iwendi, C., Jaroslava, K., Anumbe, N. (2022). Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering, 19(3),* 2641–2670. https://doi.org/10.3934/mbe.2022121
78. Tutsoy, O., Asadi, D., Ahmadi, K., Nabavi-Chasmi, S. Y. (2023). Robust reduced order thau observer with the adaptive fault estimator for the unmanned air vehicles. *IEEE Transactions on Vehicular Technology, 72(2),* 1601–1610. https://doi.org/10.1109/TVT.2022.3214479
79. Gao, J., Zhang, Q., Chen, J. (2020). EKF-based actuator fault detection and diagnosis method for tilt-rotor unmanned aerial vehicles. *Mathematical Problems in Engineering, 2020,* 1–12. https://doi.org/10.1155/2020/8019017
80. Nguyen, N. P., Mung, N. X., Hong, S. K. (2019). Actuator fault detection and fault-tolerant control for hexacopter. *Sensors, 19(21),* 4721. https://doi.org/10.3390/s19214721
81. Puchalski, R., Bondyra, A., Giernacki, W., Zhang, Y. (2022). Actuator fault detection and isolation system for multirotor unmanned aerial vehicles. *2022 26th International Conference on Methods and Models in Automation and Robotics (MMAR)*, pp. 364–369. https://doi.org/10.1109/MMAR55195.2022.9874283
82. Zolich, A., Johansen, T. A., Cisek, K., Klausen, K. (2015). Unmanned aerial system architecture for maritime missions. Design & hardware description. *2015 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, pp. 342–350. https://doi.org/10.1109/RED-UAS.2015.7441026
83. Boubeta-Puig, J., Moguel, E., Sánchez-Figueroa, F., Hernández, J., Carlos Preciado, J. (2018). An autonomous UAV architecture for remote sensing and intelligent decision-making. *IEEE Internet Computing, 22(3),* 6–15. https://doi.org/10.1109/MIC.2018.032501511

84. Su, J., He, J. P., Cheng, P., Chen, J. M. (2016). A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. *IFAC-PapersOnLine, 49(22),* 291–296. https://doi.org/10.1016/j.ifacol.2016.10.412
85. Ferreira, R., Gaspar, J., Sebastião, P., Souto, N. (2020). Effective GPS jamming techniques for UAVs using low-cost SDR platforms. *Wireless Personal Communications, 115,* 2705–2727. https://doi.org/10.1007/s11277-020-07212-6
86. Arnold, K. P. (2016). The UAV ground control station types, components, safety, redundancy, and future applications. *International Journal of Unmanned Systems Engineering, 4(1),* 37–50.
87. Mohammad, H. S. (2020). *Design of unmanned aerial systems*. https://www.wiley.com/en-us/Design+of+Unmanned+Aerial+Systems-p-9781119508625
88. Alghamdi, Y., Munir, A., La, H. M. (2021). Architecture, classification, and applications of contemporary unmanned aerial vehicles. *IEEE Consumer Electronics Magazine, 10(6),* 9–20. https://doi.org/10.1109/MCE.2021.3063945
89. Noor, N. M., Harun, N., Abdullah, A. (2020). The fixed wing UAV usage on land use mapping for gazetted royal land in Malaysia. *IOP Conference Series: Earth and Environmental Science, 540(1),* 12006. https://doi.org/10.1088/1755-1315/540/1/012006
90. Gómez-Gutiérrez, Á., Gonçalves, G. R. (2020). Surveying coastal cliffs using two UAV platforms (multirotor and fixed-wing) and three different approaches for the estimation of volumetric changes. *International Journal of Remote Sensing, 41(21),* 8143–8175. https://doi.org/10.1080/01431161.2020.1752950
91. Jacobsen, R. H., Matlekovic, L., Shi, L., Malle, N., Ayoub, N. et al. (2023). Design of an autonomous cooperative drone swarm for inspections of safety critical infrastructure. *Applied Sciences, 13(3),* 1256. https://doi.org/10.3390/app13031256
92. National Drones (2020). How drone inspections are changing infrastructure management. National Drones. https://nationaldrones.com.au/how-drone-inspections-are-changing-infrastructure-management/
93. Sonkar, S., Kumar, P., Philip, D., Ghosh, A. (2020). Low-cost smart surveillance and reconnaissance using VTOL fixed wing UAV. *2020 IEEE Aerospace Conference*, pp. 1–7. Big Sky, MT, USA, IEEE. https://doi.org/10.1109/AERO47225.2020.9172554
94. Abbasi, S. H., Mahmood, A., Khaliq, A. (2021). Bioinspired feathered flapping wing UAV design for operation in gusty environment. *Journal of Robotics, 2021,* 1–14. https://doi.org/10.1155/2021/8923599
95. Lane, P., Throneberry, G., Fernandez, I., Hassanalian, M., Vasconcellos, R. et al. (2020). Towards bio-inspiration, development, and manufacturing of a flapping-wing micro air vehicle. *Drones, 4(3),* 39. https://doi.org/10.3390/drones4030039
96. Miller, J. M., Decrossas, E. (2018). Using small unmanned aerial systems and helium aerostats for far-field radiation pattern measurements of high-frequency antennas. *2018 IEEE Conference on Antenna Measurements & Applications (CAMA)*, pp. 1–4. Vasteras, IEEE. https://doi.org/10.1109/CAMA.2018.8530671
97. Micro Air Vehicle Communication Protocol (2009). MAVLink Developer Guide. https://mavlink.io/en/
98. ArduPilot Dev Team. SiK Telemetry Radio—Copter Documentation. https://ardupilot.org/copter/docs/common-sik-telemetry-radio.html
99. Khan, M., Qureshi, I., Khanzada, F. (2019). A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET). *Drones, 3(1),* 16. https://doi.org/10.3390/drones3010016
100. Hanna, S. S. N. (2021). *UAV swarm enabled communications: System design for spectrum and energy efficiency with security considerations*. University of California, USA: Los Angeles ProQuest Dissertations Publishing.

101. Brito, A., Sebastião, P., Souto, N. (2019). Jamming for unauthorized UAV operations-communications link. *2019 International Young Engineers Forum (YEF-ECE)*, Costa da Caparica, Portugal. https://doi.org/10.1109/YEF-ECE.2019.8740828
102. Rani, C., Modares, H., Sriram, R., Mikulski, D., Lewis, F. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 13(3),* 331–342. https://doi.org/10.1177/1548512915617252
103. Benkraouda, H., Barka, E., Shuaib, K. (2018). Cyber-attacks on the data communication of drones monitoring critical infrastructure. *Computer Science & Information Technology (CS & IT),* 83–93. https://doi.org/10.5121/csit.2018.81708
104. Ceccato, M., Formaggio, F., Tomasin, S. (2020). Spatial GNSS spoofing against drone swarms with multiple antennas and wiener filter. *IEEE Transactions on Signal Processing, 68,* 5782–5794. https://doi.org/10.1109/TSP.2020.3028752
105. Hartmann, K., Giles, K. (2016). UAV exploitation: A new domain for cyber power. *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia.
106. Navid, A. K., Sarfraz, N. B., Jhanjhi, N. Z. (2020). UAV's applications, architecture, security issues and attack scenarios: A survey. In: *Intelligent computing and innovation on data science*, pp. 753–760. https://doi.org/10.1007/978-981-15-3284-9_81
107. Kim, S. G., Lee, E., Hong, I. P., Yook, J. G. (2022). Review of intentional electromagnetic interference on UAV sensor modules and experimental study. *Sensors, 22(6),* 2384.
108. Braga, J. R. G., Velho, H. F. D. C., Shiguemori, E. H. Estimation of UAV position using LiDAR images for autonomous navigation over the ocean. *2015 9th International Conference on Sensing Technology (ICST)*, pp. 811–816. Auckland, IEEE. https://doi.org/10.1109/ICSensT.2015.7438508
109. Zhang, J., Zhang, Y., Lu, K., Wang, J., Wu, K. et al. (2021). Detecting and identifying optical signal attacks on autonomous driving systems. *IEEE Internet of Things Journal, 8(2),* 1140–1153. https://doi.org/10.1109/JIOT.2020.3011690
110. Khazaaleh, S., Korres, G., Eid, M., Rasras, M., Daqaq, M. F. (2019). Vulnerability of MEMS gyroscopes to targeted acoustic attacks. *IEEE Access, 7,* 89534–89543. https://doi.org/10.1109/ACCESS.2019.2927084
111. Trippel, T., Weisse, O., Xu, W., Honeyman, P., Fu, K. (2017). WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Paris, France. https://doi.org/10.1109/EuroSP.2017.42
112. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation, 2012,* 127072. https://doi.org/10.1155/2012/127072
113. Varshosaz, M., Afary, A., Mojaradi, B., Saadatseresht, M., Ghanbari Parmehr, E. (2020). Spoofing detection of civilian UAVs using visual odometry. *ISPRS International Journal of Geo-Information, 9(1),* 6. https://doi.org/10.3390/ijgi9010006
114. van den Bergh, B., Pollin, S. (2019). Keeping UAVs under control during GPS jamming. *IEEE Systems Journal, 13(2),* 2010–2021. https://doi.org/10.1109/JSYST.2018.2882769
115. Chien, Y. R. (2015). Design of GPS anti-jamming systems using adaptive notch filters. *IEEE Systems Journal, 9(2),* 451–460. https://doi.org/10.1109/JSYST.2013.2283753
116. Dahlman, E., Lagrelius, K. (2019). *A game of drones: Cyber security in UAVs (Bachelor Thesis)*. KTH Royal Institute of Technology, Sweden.
117. Hartmann, K., Steup, C. (2013). The vulnerability of UAVs to cyber attacks—An approach to the risk assessment. *5th International Conference on Cyber Conflict*, IEEE. https://doi.org/10.1109/WCNCW.2013.6533331
118. Nawaz, H., Ali, H. M., Laghari, A. A. (2021). UAV communication networks issues: A review. *Archives of Computational Methods in Engineering, 28(3),* 1349–1369. https://doi.org/10.1007/s11831-020-09418-0

119. Almasoud, A. (2023). Jamming-aware optimization for UAV trajectory design and internet of things devices clustering. *Complex & Intelligent Systems, 9,* 4571–4590. https://doi.org/10.1007/s40747-023-00970-3
120. Mykytyn, P., Brzozowski, M., Dyka, Z., Langendoerfer, P. (2021). Jamming detection for IR-UWB ranging technology in autonomous UAV swarms. *2021 10th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro. https://doi.org/10.1109/MECO52532.2021.9460250
121. Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., Guizilini, V. (2016). The impact of DoS attacks on the AR.Drone 2.0. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)*, Recife, Brazil.
122. Greco, C., Pace, P., Basagni, S., Fortino, G. (2021). Jamming detection at the edge of drone networks using multi-layer perceptrons and decision trees. *Applied Soft Computing, 111,* 107806. https://doi.org/10.1016/j.asoc.2021.107806
123. Li, Y., Pawlak, J., Price, Al Shamaileh, K., Niyaz, Q. et al. (2022). Jamming detection and classification in OFDM-based UAVs via feature- and spectrogram-tailored machine learning. *IEEE Access, 10,* 16859–16870. https://doi.org/10.1109/ACCESS.2022.3150020
124. Khan, I., Abdollahi, A., Khan, M., Uddin, I., Ullah, I. (2021). Securing against DoS/DDoS attacks in Internet of flying things using experience-based deep learning algorithm. https://doi.org/10.21203/rs.3.rs-271920/v1
125. Li, Y., Pu, C. (2020). Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack. *2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE)*, pp. 92–97. Guangzhou, China. https://doi.org/10.1109/CSE50738.2020.00020
126. Shoufan, A. (2017). Continuous authentication of UAV flight command data using behaviometrics. *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, Abu Dhabi, United Arab Emirates. https://doi.org/10.1109/VLSI-SoC.2017.8203494
127. Wang, Q., Chen, Z., Mei, W., Fang, J. (2017). Improving physical layer security using UAV-enabled mobile relaying. *IEEE Wireless Communications Letters, 6(3),* 310–313. https://doi.org/10.1109/LWC.2017.2680449
128. Wang, W., Tian, H., Ni, W., Hua, M. (2021). Reconfigurable intelligent surface aided secure UAV communications. *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 818–823, Helsinki, Finland. https://doi.org/10.1109/PIMRC50174.2021.9569667
129. Khadem, B., Mohebalizadeh, S. (2020). Efficient UAV physical layer security based on deep learning and artificial noise. arXiv:2004.01343.
130. Pärlin, K., Riihonen, T., Turunen, M. (2019). Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems. *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, Budva, Montenegro. https://doi.org/10.1109/ICMCIS.2019.8842761
131. Sánchez, H. S., Rotondo, D., Vidal, M. L., Quevedo, J. (2019). Frequency-based detection of replay attacks: Application to a quadrotor UAV. *2019 8th International Conference on Systems and Control (ICSC)*, pp. 289–294. Marrakesh, Morocco. https://doi.org/10.1109/ICSC47195.2019.8950619
132. Baayer, A., Enneya, N., Koutbi, M. (2012). Enhanced timestamp discrepancy to limit impact of replay attacks in MANETs. *Journal of Information Security, 3(3),* 224–230. https://doi.org/10.4236/jis.2012.33028
133. Kong, P. Y. (2021). A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access, 9,* 148244–148263. https://doi.org/10.1109/ACCESS.2021.3124996
134. Javaid, A. Y., Sun, W., Devabhaktuni, V. K., Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. *2012 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, IEEE. https://doi.org/10.1109/THS.2012.6459914
135. Park, K. H., Park, E., Kim, H. K. (2021). Unsupervised fault detection on unmanned aerial vehicles: Encoding and thresholding approach. *Sensors, 21(6),* 2208. https://doi.org/10.3390/s21062208

136. Ciaburro, G., Iannace, G. (2020). Improving smart cities safety using sound events detection based on deep neural network algorithms. *Informatics, 7(3),* 23. https://doi.org/10.3390/informatics7030023

137. Mykytyn, P., Brzozowski, M., Dyka, Z., Langendoerfer, P. (2023). GPS-spoofing attack detection mechanism for UAV swarms. *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–8. Budva, Montenegro, IEEE. https://doi.org/10.1109/MECO58584.2023.10154998

138. Gao, Y. H., Zhao, D., Li, Y. B. (2012). UAV sensor fault diagnosis technology: A survey. *Applied Mechanics and Materials, 220–223,* 1833–1837. https://doi.org/10.4028/www.scientific.net/AMM.220-223.1833

139. Pouliezos, A. D., Stavrakakis, G. S. (1994). Analytical redundancy methods. In: *Real time fault monitoring of industrial processes*, pp. 93–187. Dordrecht: Springer.

140. Zhang, S., Li, Y., Liu, S., Shi, X., Chai, H. et al. (2020). A review on fault-tolerant control for robots. *2020 35th Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, pp. 423–427. Zhanjiang, China. https://doi.org/10.1109/YAC51587.2020.9337672