future internet

MDPI

Review

Watch the Skies: A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges

Amr Adel [1,2,*] and Tony Jan [1]

[1] Centre for Artificial Intelligence Research and Optimization (AIRO), Torrens University Australia, Ultimo, NSW 2007, Australia; tony.jan@torrens.edu.au

[2] School of Computing, Eastern Institute of Technology, Auckland 1010, New Zealand

[*] Correspondence: amr.adel@torrens.edu.au or avandenadel@eit.ac.nz

Abstract: In the rapidly evolving landscape of drone technology, securing unmanned aerial vehicles (UAVs) presents critical challenges and demands unique solutions. This paper offers a thorough examination of the security requirements, threat models, and solutions pertinent to UAVs, emphasizing the importance of cybersecurity and drone forensics. This research addresses the unique requirements of UAV security, outlines various threat models, and explores diverse solutions to ensure data integrity. Drone forensics, a field dedicated to the investigation of security incidents involving UAVs, has been extensively examined and demonstrates its relevance in identifying attack origins or establishing accident causes. This paper further surveys artifacts, tools, and benchmark datasets that are critical in the domain of drone forensics, providing a comprehensive view of current capabilities. Acknowledging the ongoing challenges in UAV security, particularly given the pace of technological advancement and complex operational environments, this study underscores the need for increased collaboration, updated security protocols, and comprehensive regulatory frameworks. Ultimately, this research contributes to a deeper understanding of UAV cybersecurity and aids in fostering future research into the secure and reliable operation of drones.

Keywords: unmanned aerial vehicles (UAVs); drone cybersecurity; threat models; drone forensics; security challenges; forensic methodologies

check for updates

Citation: Adel, A.; Jan, T. Watch the Skies: A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges. *Future Internet* **2024**, *16*, 250. https://doi.org/10.3390/fi16070250

Academic Editor: Francesco Buccafurri

Received: 28 May 2024
Revised: 10 July 2024
Accepted: 10 July 2024
Published: 13 July 2024

1. Introduction

Unmanned aerial vehicles (UAVs), more commonly known as drones, have seen exponential growth in their applications over the past decade. Once exclusively associated with military and defense operations, drones now permeate a plethora of sectors ranging from agriculture and surveillance to package delivery and environmental monitoring. According to the Federal Aviation Administration (FAA), the number of commercial drones in the United States is expected to have tripled by 2023, reaching an estimate of over 835,000 [1]. Similarly, the Consumer Technology Association predicts that global sales of drones will be approximately 20 million by 2034. This escalating ubiquity underscores the importance of understanding and addressing the cybersecurity and forensic aspects related to UAVs.

Drone forensics, a niche yet rapidly developing field within digital forensics, involves the process of uncovering, analyzing, and interpreting digital data from a drone system for investigative purposes. Whether it is to probe a security incident, identify an attacker, or determine the cause of an accident, drone forensics provide valuable insights into the events surrounding the UAV. This field has become more critical as drones are equipped with high-capacity storage, advanced sensors, and complex communication systems, which often hold sensitive data and are susceptible to various cybersecurity threats.

A crucial component in the UAV architecture, the ground control system (GCS), serves as the hub for human–drone interaction. It is the control station from which operators direct the flight of a drone and manage its functionalities. While the GCS provides a means to leverage the versatility of drones, it also exposes a vulnerable attack surface for cybercriminals. The vulnerabilities of the GCS and their implications for drone operation and security form an essential aspect of UAV security and forensics.

The significance of drone forensics and security cannot be overstated in today's increasingly drone-dependent world. As drones continue to find applications in security-sensitive sectors, such as military surveillance, law enforcement, and delivery of goods, any security lapses could result in dire consequences, including threats to national security, invasion of personal privacy, and loss of valuable assets. This underscores the urgent need for robust cybersecurity measures and effective forensic methodologies that can secure UAVs against potential attacks and aid in the investigation post any security incidents.

This paper used a systematic literature review to understand the field comprehensively. We searched Scopus and IEEE Xplore with keywords: "Unmanned Aerial Vehicles (UAVs)", "Drone Cybersecurity", "Drone Cybersecurity Threat Models", "Drone Forensics", "Security", and "Drone Forensic Methodologies" for articles published since 2018. By aggregating and analyzing scholarly articles, industry reports, case studies, and government publications, this paper presents a holistic view of current drone threat models, forensic approaches, and security challenges.

1.1. Research Methodology and Selection Criteria

The research methodology of this review includes a systematic analysis of the existing literature, case studies, and empirical data on drone security, forensic approaches, and persistent security challenges. This approach aims to provide a comprehensive understanding of UAV security and forensics, highlighting key components, challenges, and potential solutions. The research methodology and source selection criteria are outlined below:

A thorough search of scholarly databases, online repositories, and professional journals was conducted to find relevant articles, books, reports, and conference proceedings on drone security, forensics, and industry applications. A systematic search query using relevant keywords and phrases related to UAV security, forensics, and industry applications was designed. Data were gathered from various platforms, including Google Scholar, ACM Digital Library, ScienceDirect, IEEE Xplore, Scopus, and Springer using the following search queries:

1. Query A: (("drone security" OR "UAV security" OR "unmanned aerial vehicle security") AND ("forensics" OR "cybersecurity" OR "digital forensics") AND ("smart cities" OR "urban management"));
2. Query B: (("drone forensics" OR "UAV forensics") AND ("data integrity" OR "digital evidence" OR "incident response") AND ("cyber attacks" OR "security threats"));
3. Query C: (("unmanned aerial vehicle" OR "drone technology") AND ("threat models" OR "attack vectors" OR "security vulnerabilities") AND ("data protection" OR "encryption" OR "secure communication"));
4. Query D: (("drone operation" OR "UAV deployment") AND ("security protocols" OR "forensic methodologies") AND ("case studies" OR "real-world applications"));
5. Query E: (("drone forensic analysis" OR "UAV forensic techniques") AND ("machine learning" OR "artificial intelligence" OR "predictive analytics") AND ("emerging trends" OR "future research" OR "innovation")).

The research selection process, detailed in Appendix A, began with 2154 records identified through database searches. After removing 1608 duplicates and ineligible records, 546 remained for screening. Of these, 383 were excluded based on relevance and quality. Out of 163 papers sought, 47 were not retrievable, leaving 116 for eligibility assessment. Exclusions included 40 non-peer-reviewed, 25 irrelevant, 10 lacking empirical support, 17 older publications, and 11 non-English papers, totaling 103 exclusions. Ultimately, 13 studies were included in the review, with 113 studies considered for final analysis.

The review followed strict inclusion and exclusion criteria to ensure study relevance and quality, as detailed in Appendix B. The inclusion criteria were: peer-reviewed status, relevance to UAV security and forensics, empirical evidence, publication within the last 10 years, and availability in English. Each study was verified for these criteria. Exclusions were non-peer-reviewed, irrelevant, lacking empirical support, older than 10 years, or not in English. This systematic approach ensured the review included only high-quality, relevant, and recent studies, enhancing the robustness and reliability of the findings.

1.2. Comparison to Other Survey Papers and Contributions

Several surveys have explored the landscape of UAV security and forensics, each focusing on different subtopics. In 2023, Sighag et al. [2] presented a Cyber4Drone survey paper that provided a systematic review of cybersecurity and forensic challenges for unmanned aerial vehicles (UAVs), including an analysis of threat models, security and privacy issues, and a taxonomy of drone forensic techniques and tools. In the same year, Ceviz et al. [3] published a survey paper focusing on security issues, threats, and solutions for unmanned aerial vehicles (UAVs) and flying ad hoc networks (FANETs), including an analysis of the attack surface, potential threats, prevention and detection countermeasures, and simulations of four routing attacks on FANETs. Shafik et al. [4] provided an overview of the cybersecurity threats and challenges faced by unmanned aerial vehicles (UAVs), explored various cybersecurity strategies and techniques to protect UAVs, and identified future research directions to mitigate cybersecurity risks in UAVs. In 2022, Pandey et al. [5] conducted a comprehensive survey on security threats and mitigation techniques in UAV communications. Siddiqi et al. [6] presented an analysis of the security- and privacy-related concerns of UAVs, offering countermeasures and recommendations. Wang et al. [7] provided a comprehensive survey of the current achievements in physical layer security (PLS) for UAV communications.

Despite these valuable contributions, several gaps remain in the existing literature. Many surveys have focused on specific aspects of UAV security or forensics and often lack a comprehensive analysis. Our study aims to provide a holistic overview encompassing security requirements, threat models, and forensic approaches. The rapid evolution of UAV technology has introduced new security challenges that necessitate ongoing research. Existing surveys often lack a forward-looking perspective to address emerging threats. Thus, there is a critical need for a unified framework that integrates cybersecurity practices with forensic methodologies to enhance both preventive and investigative capabilities.

Our survey significantly advanced the field of UAV security and forensics by providing an integrated analysis that bridges cybersecurity measures with forensic methodologies. This comprehensive approach covers security requirements, threat models, attack vectors, forensic methodologies, and mitigation techniques. It identifies emerging challenges due to the rapid evolution of UAV technology, proposes future research directions, and emphasizes the need for continuous innovation. The survey advocates for a unified framework to enhance both preventive and investigative capabilities and supports standardized protocols and best practices. By synthesizing previous research, it highlights key contributions and gaps and offers practical recommendations for improved UAV security and forensics. Serving as a crucial resource, it supports ongoing research, industry applications, and policy development across interdisciplinary fields, ensuring that the findings are broadly relevant and impactful.

The contribution of this paper lies in its exhaustive review of drone threat models, exploration of forensic approaches used for investigating drone-related incidents, and analysis of persistent security challenges. In addition, it delivers a systematic taxonomy of drone forensics, detailing key artifacts, relevant tools, and benchmark datasets. This survey will serve as a significant resource for researchers, practitioners, and policymakers aiming to bolster the security and integrity of UAV operation.

The remainder of this paper is organized as follows: Section 2 provides an overview of drone technologies. Section 3 addresses drone security vulnerabilities and evolving attack vectors. Section 4 focuses on a detailed review of drone security solutions. Section 5 presents intriguing future research opportunities, and Section 6 concludes the paper.

2. Overview of Drone Technologies

2.1. Drone Anatomy

The anatomy of a drone is a sophisticated integration of various technological components that enables it to perform a wide range of functions, from simple recreational flying to complex commercial tasks [8].

Figure 1 illustrates the essential components and functionalities of drones, including the flight controller, propellers, brushless motors, and gimbal systems, and their roles in operation. Each part is vital for the drone's flight, navigation, and tasks like video recording or streaming [9].

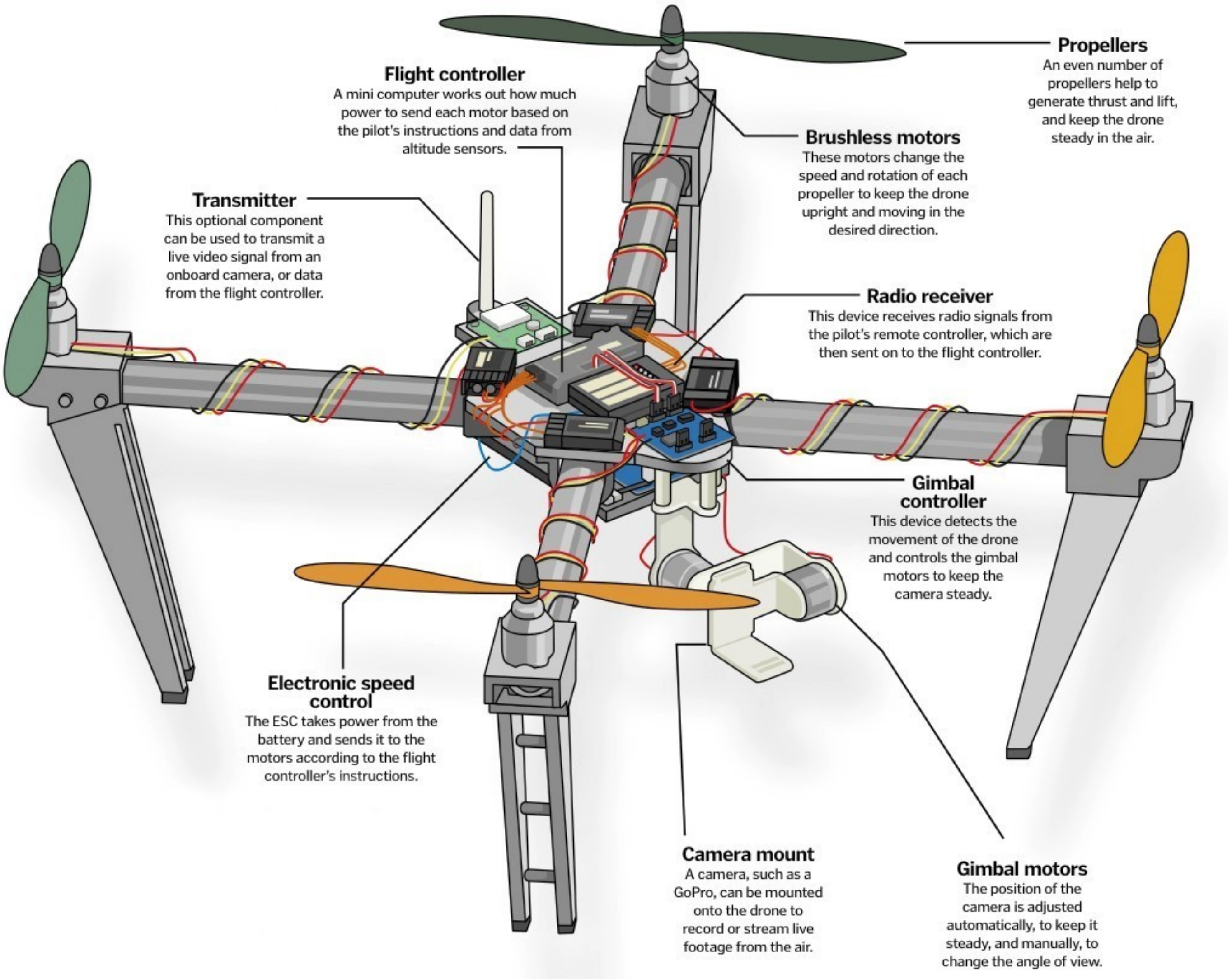
Propellers
An even number of propellers help to generate thrust and lift, and keep the drone steady in the air.
Flight controller
A mini computer works out how much power to send each motor based on the pilot's instructions and data from altitude sensors.
Brushless motors
These motors change the speed and rotation of each propeller to keep the drone upright and moving in the desired direction.
Transmitter
This optional component can be used to transmit a live video signal from an onboard camera, or data from the flight controller.
Radio receiver
This device receives radio signals from the pilot's remote controller, which are then sent on to the flight controller.
Gimbal controller
This device detects the movement of the drone and controls the gimbal motors to keep the camera steady.
Electronic speed control
The ESC takes power from the battery and sends it to the motors according to the flight controller's instructions.
Camera mount
A camera, such as a GoPro, can be mounted onto the drone to record or stream live footage from the air.
Gimbal motors
The position of the camera is adjusted automatically, to keep it steady, and manually, to change the angle of view.

Figure 1. Anatomy of drones.

The flight controller, a minicomputer, processes sensor inputs and pilot commands to maintain stable flight, enabling both basic maneuvers and advanced navigation. Brushless motors, chosen for efficiency and reliability, adjust propeller speed and rotation to create lift and thrust, which are crucial for speed and stability [10]. Propellers are aerodynamically designed to optimize performance.

Communication with the operator is managed through a radio receiver and transmitter, which handle commands and data such as live video feeds or telemetry [11]. The gimbal controller and motors stabilize mounted devices like cameras, ensuring steady footage. Electronic speed controllers (ESCs) regulate motor power from the battery to adjust propeller speed for smooth flight dynamics [12].

Each drone component enhances its flight capabilities and broadens its applications, making drones versatile tools for civilian and commercial use for usages such as aerial photography or complex surveillance [13].

Drone operations involve multiple layers to ensure optimal performance across tasks, with usages ranging from aerial photography to complex data collection and analysis [14–17]. The architecture of a drone system is divided into specific functional layers:

- **Planning layer**: Defines missions or services and develops executable plans; this is essential for disaster management.
- **Flight management layer**: Executes the planned route, managing dynamic flight, obstacle avoidance, and real-time path modifications to ensure secure mission completion.
- **Control layer**: Interfaces directly with drone hardware, sending commands to sensors and actuators and handling real-time adjustments to maintain the stability and trajectory.

The drone's hardware includes the frame, motors, propellers, and electronic speed controllers (ESCs) and enables physical operation. Sophisticated equipment like GPS and antenna systems ensure communication with ground control and navigational accuracy via GPS and RTK networks. In scenarios with multiple drones, robust data link systems facilitate drone-to-drone communication for coordinated task execution [18,19]. Figure 2 illustrates the multi-layered approach to drone operations and highlights key components and communication frameworks that enable autonomous and coordinated functions.

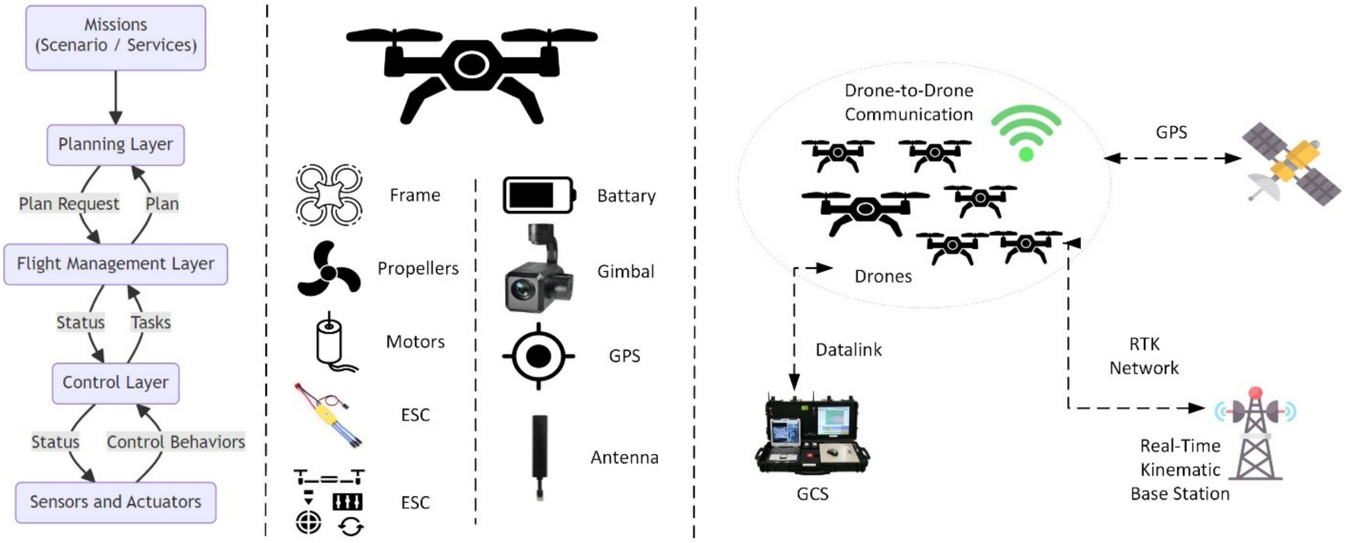

Figure 2. Drone operations and system architecture.

2.2. Drone Forensics Artifacts

The meticulous examination and analysis of various artifacts are paramount to understanding the operations and interactions of these aerial devices within their operational environments. These artifacts, which range from flight logs to system firmware, provide a rich tapestry of data critical for forensic investigators [20–24]. Each artifact holds specific insights into the drone's performance, activities, and any anomalies, which may indicate misuse or malfunctions.

Table 1 categorizes key drone forensic artifacts and details their primary sources and descriptions.

Table 1. Drone forensic artifacts: E is for Exif data, F is for system files, G is for ground controller, L is for logs, M is for memory card, and O is for observation.

Artifact Name	Source	Description
Flight Logs	L	Records of flight data including times, altitudes, and GPS coordinates.
System Firmware	F	The embedded software that controls drone operations.
GPS Data	E, L	Data capturing the drone's geographical position during flights.
Controller Inputs	G	Records of commands input by the operator during flight.
Video Files	M	Recorded footage from drone flights stored on memory cards.
Photo Files	M, E	Images captured during flight, often containing Exif metadata such as timestamps and camera settings.
Battery Information	L	Data regarding battery status and history during flights.
Communication Logs	L, G	Logs detailing the communication between the drone and its ground controller.
Error Reports	F, L	System-generated reports detailing malfunctions or errors during operation.
Maintenance Records	F, L	Logs related to drone servicing, updates, and repairs.
Wi-Fi Data	L	Information about Wi-Fi networks used for control and data transmission.
Serial Number	F	Unique identifier of the drone, often embedded in system files or visible on the drone body.
Telemetry Data	L	Real-time data on various flight parameters such as speed, altitude, and orientation.
Crash Reports	L	Detailed reports generated when a drone experiences a crash or significant malfunction.
Configuration Files	F	Files that determine the settings and options of the drone's operating system.
Propeller Data	O	Observations and data regarding the condition and performance of the drone's propellers.
Firmware Update Logs	F	Logs documenting the history and details of firmware updates applied to the drone.
Environmental Data	L	Data collected during flight related to environmental conditions such as temperature and wind speed.
Security Protocols	F	Information regarding the encryption and security measures used to protect drone communications and data storage.

3. Drone Vulnerabilities and Attack Vectors

The emerging risks associated with drone technology pose significant threats to data security, infrastructure integrity, and public safety [25]. Attackers may exploit zero-day vulnerabilities and security loopholes to infiltrate drone communication networks [26,27]. Drone forensics has emerged as a critical field that aims to determine attackers' motives through meticulous investigations [28]. This systematic process involves the collection, preservation, and analysis of digital, software, and hardware evidence from drones [29]. Furthermore, drone forensics can guide the development of new technologies or policies that mitigate the effects of similar future attacks and enhance overall security levels [30].

This section explores various drone security attacks to provide structured guidance for the forensic investigation of drones. Vulnerabilities in communication media and frequency-based weaknesses compound these risks. Even advanced drones that are equipped with cameras and GPS capabilities are not immune to such threats. A taxonomic classification of drone attacks detailing their impacts, execution tools, and mechanisms is presented in Table 2.

Table 2. Categorization of drone attack methods for target zones (Z). Z1: UAVs, Z2: communication systems, Z3: control hubs, Z4: command centers, and Z5: Regulatory Bodies, Production Facilities, and Associated Equipment.

Drone Attacks	Tools/ Mechanisms	Impact	Security Requirements	Attack Surfaces	Key Papers
GPS Spoofing	GPS signal simulators	Misdirection, route deviation	Enhanced route security	Z1: UAVs	[31–34]
Signal Jamming	Radio frequency jammers	Loss of control, crashing	Robust signal integrity	Z1: UAVs, Z2: Communication Systems	[35–39]
Unauthorized Access	Hacking tools	Data theft, control takeover	Access control improvements	Z3: control hubs, Z4: command centers	[40–45]
Physical Attack	High-energy lasers	Damage, destruction	Structural integrity checks	Z1: UAVs	[46–50]
Network Intrusion	Malware, spyware	Data breach, system compromise	Enhanced cybersecurity measures	Z2: Communication Systems, Z4: command centers	[51–54]
Battery Tampering	Physical interference	Power loss, mid-air failure	Reliable power supply systems	Z1: UAVs	[55,56]
Firmware Hacking	Custom firmware	Altered behavior, backdoors	Secure firmware protocols	Z1: UAVs, Z3: Control Hubs	[57–63]
Sensor Blinding	Directed bright lights	Impaired vision, collision	Improved sensor protection	Z1: UAVs	[64–68]
Denial of Service	Flooding networks	Disrupted operations	Network resilience	Z2: Communication Systems, Z3: Control Hubs	[69–74]
Data Interception	Sniffing tools	Espionage, data leakage	Data encryption standards	Z2: Communication Systems	[75–79]
Protocol Exploitation	Exploitation kits	Command hijacking	Secure communication protocols	Z3: Control Hubs	[80–86]
Malicious Code Injection	Trojans, viruses	Malfunctions, unsafe operations	Malware detection systems	Z1: UAVs, Z4: command centers	[87,88]
Ransomware Attack	Ransomware	Locked systems, ransom demand	Anti-ransomware strategies	Z4: command centers	[4,89–91]
Eavesdropping	Audio–visual surveillance	Privacy invasion	Privacy safeguards	Z2: Communication Systems, Z4: command centers	[92–95]
Supply Chain Attack	Compromised components	Integrated vulnerabilities	Supply chain security	Z5: regulatory bodies, production facilities, and associated equipment	[96–98]
Insider Threat	Sabotage by insiders	System sabotage, data theft	Internal security measures	Z3: Control Hubs, Z4: command centers	[99–102]
Regulatory Non-compliance	Bypassing controls	Legal penalties, shutdown	Compliance management	Z5: regulatory bodies, production facilities, and associated equipment	[103–105]

3.1. GPS Spoofing

GPS spoofing transmits false GPS signals to manipulate a drone's navigation to redirect it from its intended path. This can lead to theft, operational interference, or unauthorized payload delivery and poses serious risks in security-sensitive environments. Defenses include advanced cryptographic techniques, multi-sensor fusion, and anomaly detection systems to identify and mitigate deviations [106,107].

3.2. Signal Jamming

Signal jamming disrupts drone communication by flooding frequencies with high-intensity signals, severing the link between the drone and its operator. This can cause loss of control, autonomous landing, or system failure, causing risk to critical applications like law enforcement or emergency response. Countermeasures involve frequency-hopping and spread-spectrum technologies and robust fail-safe mechanisms to guide drones to safety during communication loss [108].

3.3. Network Intrusion

Network intrusion involves hacking drone control channels to intercept data or insert malicious commands, leading to data theft, surveillance, payload hijacking, or weaponization. This threat is heightened with IoT-connected drones. Protection requires secure communication protocols, regular software updates, and comprehensive network monitoring to detect and respond to unauthorized access [109].

3.4. Malicious Code Injection

Malicious code injection targets drone software through compromised firmware updates or security vulnerabilities. This can manipulate drone behavior, disable safety features, or extract confidential data, making drones unreliable or dangerous. Prevention includes strict code integrity checks, secure update mechanisms, and regular security audits [110].

3.5. Physical Tampering

Physical tampering involves altering drone hardware components like microSD cards, sensors, or communication modules, potentially enabling espionage or sabotage. Defending against this requires tamper-detection systems and strict physical security protocols, such as utilizing physical unclonable functions (PUFs) [111].

3.6. Eavesdropping

Drones equipped with surveillance tools can eavesdrop, gathering sensitive information undetected. This poses privacy risks and potential corporate espionage threats. Countermeasures include no-fly zones, anti-drone technologies, and strict regulatory measures to prevent unauthorized drone flights over private property [112].

3.7. Supply Chain Interference

Supply chain interference involves inserting vulnerabilities during drone manufacturing, which would affect entire fleets if the compromised components are widespread. Mitigation requires stringent security protocols, vetting suppliers, and thorough security audits and tests on components before integration [113].

4. Drone Forensics and Security Solutions—Review

In the realm of drone cybersecurity and forensics, a number of studies have delved into identifying threat models, evaluating security measures, and developing forensic methodologies.

In 2017, Renduchintala et al. [114] made substantial strides in the realm of drone forensics by proposing a comprehensive framework for the examination of digital flight logs from micro-drones. The authors recognized the security concerns arising from the increased public use of unmanned aerial vehicles (UAVs), or drones. Given the drones' ability to access potential targets closely, the authors were motivated to develop a forensic framework capable of thoroughly inspecting the drone's activities post-flight. Specifically, their paper scrutinized the crucial log parameters of an autonomous drone and proposed an in-depth software architecture related to drone forensics. Preliminary results indicated the potential of their under-development software, which boasted a user-friendly graphical user interface (GUI) that allowed users to extract and examine onboard flight information. Their work is significant because it aims to equip the forensic science community with a practical tool to investigate drone-related crime cases more effectively.

In 2018, Azhar et al. [115] tackled the growing need for effective forensic analysis of drones, particularly those involved in unlawful activities. They recognized the substantial rise in drone-related offenses due to their easy accessibility and robust carrying capacities. To address this, the authors focused on extracting and identifying significant artifacts from recorded flight data and associated mobile devices. They employed a range of open-source tools, which were complemented by basic scripts they developed to facilitate the analysis. Their research specifically examined two popular drone systems: the DJI Phantom 3 Professional and the Parrot AR Drone 2.0. The authors stressed the importance of adhering to forensically sound methods as per the guidelines of the Association of Chief Police Officers (ACPO). Their findings emphasized that, while drone operations vary, generic methods can be effectively applied for the extraction and analysis of data from drones and associated devices, thereby significantly contributing to advancements in the drone forensics field.

In the same year, Bouafif et al. [116] addressed the field of drone forensics and the associated challenges. They emphasized the growing popularity of unmanned aerial vehicles (UAVs), or drones, which possess powerful information acquisition and processing capabilities along with intelligent surveillance and reconnaissance features. However, the misuse of drones for illegal and potentially criminal activities poses significant threats to individuals, organizations, public safety, and national security. Despite the increasing importance of drone forensics, it remains a relatively underexplored research topic. The authors presented important results from a forensic investigation analysis conducted on the Parrot AR Drone 2.0 and offered new insights into the field.

In 2019, Iqbal et al. [117] explored drone forensics, focusing on identifying and analyzing drone vulnerabilities. They highlighted the susceptibility of drones to various types of attacks, such as GPS spoofing and de-authentication, which pose challenges to forensic investigations and could potentially lead to criminal activities. The authors advocated standardized drone forensics to enhance security, identify vulnerabilities, and resolve drone-related crimes. Their research included a case study of potential attacks on the Parrot Bebop 2 drone and the process of evidence collection. They also proposed a framework for small-scale drone forensics and drone ontology for context data modeling. Their work provided significant insights into drone vulnerabilities and the importance of forensic science in managing drone-related crimes.

In the same year, Kao et al. [118] focused on drone forensic investigation, with the DJI Spark drone serving as a case study. The authors highlighted the rise in drone crimes due to the carrying capabilities and widespread availability of drones. They emphasized the importance of drone forensic analysis in addressing these crimes. The paper detailed the process of collecting, examining, correcting, and analyzing crucial artifacts extracted from the recorded flight data. It also presented crime reconstruction techniques for temporal analysis and explored the associations between drones, mobile phones, and SD cards. By exploring and evaluating these relational artifacts, the authors aimed to uncover valuable insights into the relationships among the different components involved in drone-related crimes. This work contributes to the field of drone forensics by providing a systematic approach for artifact analysis and crime reconstruction, focusing on the DJI Spark drone.

In 2019, Mantas et al. [119] addressed the field of drone forensics, with a specific focus on forensics related to flight data logs. They recognized the decreasing cost of unmanned aerial vehicles (UAVs) and drones, which has led to their widespread adoption in various civilian and business applications. However, the features offered by drones have also been maliciously exploited, thereby increasing the need for drone forensics. This work aims to fill a gap in the literature by investigating forensics on flight data logs, specifically focusing on the widely used Ardupilot platform and its dataflash and telemetry logs. The authors discussed a methodology for collecting the necessary information, analyzing it, and constructing a timeline of events. They also developed an open-source tool that facilitates this process and tested it using data provided by VTO Labs. This study contributes to the field of drone forensics by providing insights into the analysis of flight data logs and offering a practical tool for forensic investigations in this domain.

In 2020, Yousef et al. [120] delved into drone forensics by performing a meticulous analysis of the emerging DJI models. They acknowledged the challenges posed by rapidly evolving drone technology, particularly due to drones' escalating use in digital crimes. The authors emphasized the need for forensic examiners to be well-versed in drone technology, forensic methods, and the capabilities of existing tools to effectively extract crucial information for forensic investigations. Their study analyzed the data extracted from four popular hobbyist drone models (DJI Mavic 2 Pro, DJI Mavic Air, DJI Spark, and DJI Phantom 4) and compared the applicability and capability of several commercial and open-source forensic tools. Their findings highlighted the difficulties in analyzing newer drone models due to enhanced security measures. Therefore, they stressed the need for novel forensic processes and specialized tools to enhance drone forensic analysis.

In 2021, Al et al. [121] conducted a case study to explore drone forensics and digital forensic investigations for common drone models. The authors highlighted the growing prevalence of drones, which have become a societal norm in our daily lives. They emphasized the privacy challenges posed by drones, as they can capture high-quality aerial photos, store and transmit data, and potentially invade privacy or expose sensitive information if misused or intercepted by hackers. Recognizing the increasing misuse of drones in criminal activities, the authors stressed the need for a novel methodological approach to conduct digital forensic analyses on seized drones. This study investigated six popular drone brands that are commonly associated with criminal activities and extracted forensically relevant data such as location information, captured images and videos, flight paths, and ownership details of confiscated drones. The experimental results demonstrated the potential of drone forensics in aiding law enforcement agencies by providing valuable information that is crucial for criminal investigations.

In the same year in 2021, Al et. al., [122] addressed the opportunities in drone forensic models. They acknowledged the significant impact of unmanned aerial vehicles (UAVs) or drones on surveillance and supply chain logistics by enabling access to previously inaccessible areas. However, the increased adoption of drones has also led to an upsurge in drone-related criminal activities, raising concerns related to security and forensics. To gain a deeper understanding of the current state of research and potential mitigation approaches, the authors conducted a detailed review of existing digital forensic models using a Design Science Research method. This study provides valuable insights into research challenges and opportunities in investigating drone-related incidents. The authors propose a potential generic investigation model and emphasize the relevance of these findings for forensic researchers and practitioners for developing a guided methodology for drone-related event investigation. Additionally, they highlighted the importance of this study as a foundation for the development of international standardization for drone forensics.

In their seminal work in 2022, Alotaibi et. al. [123] proposed a novel framework aimed at improving the readiness of forensic investigations in the drone field. Recognizing the unique complexities and challenges associated with drone forensics, the authors proposed a comprehensive model that emphasized preparedness to efficiently collect, analyze, and preserve the data involved in drone-related incidents. Their framework offers a structured approach to digital evidence handling, which is key to successful forensic investigations. Importantly, it is designed to be applicable in diverse scenarios, regardless of the specificities of the drone system or nature of the incident. This contribution is significant because it enhances the capabilities of forensic teams for dealing with drone-related security breaches, thereby improving the overall security landscape of the rapidly evolving UAV sector.

In 2022, Lan et al. [124] focused on drone forensics: specifically, by conducting a case study of the DJI Mavic Air 2 drone. They acknowledged the increasing prevalence of cost-effective and high-performance unmanned aerial vehicles (UAVs) in the consumer market, which leads to an increase in their leisure and business applications. Consequently, there has been growing demand for digital forensic examinations of these devices. The authors explored and discussed the forensic examination process specifically for DJI drones, which are popular in Singapore. They presented their findings by examining the exposed File Transfer Protocol (FTP) channel and extracting the data-at-rest from the drone's memory chip. The extraction was carried out using the chip-off and chip-on techniques, and the authors demonstrated their methodology for retrieving data from the drone. This research contributes to the field of drone forensics by providing insights into the forensic examination process for DJI drones, thus contributing to our understanding of the digital forensics of UAVs.

In 2022, Da Silva et al. [125] developed an efficient platform using the MQTT protocol for UAV control and DoS attack detection and demonstrated its robustness through tests on latency and network and memory consumption with a high true positive rate for DoS detection using advanced machine learning techniques. In 2023, Buccafurri et al. [126] addressed the need for communication anonymity within MQTT for IoT networks by proposing MQTT-anonymous (MQTT-A), which ensured the anonymity of publishers and subscribers through P2P collaboration among intermediate bridge brokers by using standard MQTT primitives and without requiring changes to existing infrastructure. This protocol was validated through global experimental tests and showed reasonable latency tradeoffs and minimal impact on network performance. In 2019, Xiong et al. [127] introduced a hybrid SDN and MQTT communication system for battlefield UAV swarms that was designed to be flexible, adaptable, and intelligent in order to support dynamic swarm formations, flexible data transmission, and enhanced security with a QoS-based multi-path routing framework. Case studies validated its practical effectiveness, although a more detailed discussion of the challenges and limitations would strengthen these studies. Collectively, these papers make significant contributions to secure, efficient, and anonymous communication systems for UAVs.

In 2022, Baig et al. [128] focused on drone forensics and machine learning with the aim of sustaining the investigation process. They recognized the increasing adoption of drones to address various challenges and provide support and convenience in areas such as medical supply delivery, surveillance, weather data collection, and home delivery services. However, the authors also acknowledge that drones have been misused for criminal activities. Their research entails a survey of artificial intelligence techniques in the literature that are relevant for processing drone data and uncovering criminal activity. Additionally, they proposed a novel model that leveraged machine learning to classify drone data as part of a digital forensic investigation. The authors concluded that properly trained machine learning models hold promise for accurately assessing drone data obtained from crime scenes. Their work paves the way for academia and industry practitioners to adopt machine learning techniques for the effective use of drone data in forensic investigations, contributing to the advancement of drone forensics.

In more recent years, the following key technologies have emerged in drone security:

Drone security module: The work of Schiller [129] in 2023 and the earlier work of Kim et al. [130] considered a drone security module that can encrypt control signals and telemetry data between the UAV and the ground control station (GCS). These encryption mechanisms employed advanced cryptographic algorithms to secure data in transit, protecting against eavesdropping and unauthorized access. Their modules ensured the confidentiality (C) and integrity (I) of the communications, targeting UAVs (Z1), communication systems (Z2), and control hubs (Z3). However, their modules did not specifically address the availability (A) of the system, leaving it susceptible to denial-of-service (DoS) attacks. A further review of drone security modules was discussed by Samantha et al. [131].

Blockchain for secure data storage: The work of Cheema et al. [132], Bera et al. [133], Singh et al. [134], and Gupta et al. [135] considered blockchain technology to secure data transmitted to and from drones. By creating an immutable ledger of all interactions, the blockchain ensured that data integrity was maintained, preventing tampering or unauthorized modifications. These solutions targeted all security zones, including UAVs (Z1), communication systems (Z2), control hubs (Z3), command centers (Z4), and regulatory bodies (Z5). It provided comprehensive security coverage across confidentiality (C), integrity (I), and availability (A), although the potential for signal hijacking remained a concern.

Drone-assisted public safety networks: The work of Minhas et al. [136] and He et al. [137] proposed that UAVs augment public safety networks by being deployed to strategic positions. Their approaches utilized real-time data transmission and processing to enhance situational awareness and response times. The primary security targets were UAVs (Z1), communication systems (Z2), control hubs (Z3), and command centers (Z4). Their solutions enhanced integrity (I) and availability (A) by ensuring reliable data transmission and operational continuity in public safety operations. A further review of drone-assisted public safety networks is shared by Ali et al. [138].

Machine learning for threat detection: Studiawan et al. [139] in 2023, Abu et al. [140], and Guerber et al. [141], alongside many scholars, studied various machine learning algorithms, such as the random forest classifier, to be implemented to detect network attacks, including DoS, port scanning, and brute force attempts. This predictive analytics approach analyzed network traffic patterns to identify anomalies indicative of security breaches. It targeted UAVs (Z1), communication systems (Z2), control hubs (Z3), command centers (Z4), and regulatory bodies (Z5). The solution enhanced confidentiality (C), integrity (I), and availability (A) by providing the early detection and mitigation of threats. A comprehensive review was provided by Heidari et al. [142] in 2023.

Blockchain for UAV signal security: The work of Haefeez et al. [143] in 2023, Kumar et al. [144], Ch et al. [145], and Rana et al. [146] applied blockchain technology to secure the signal transmission between controllers and UAVs. Their methods secured the communication protocol, ensuring that signals were authentic and had not been tampered with. The primary targets were UAVs (Z1), communication systems (Z2), control hubs (Z3), and command centers (Z4). While enhancing confidentiality (C) and integrity (I), the approach required robust mechanisms to ensure signal availability (A).

Software-defined networks (SDNs) for drone swarms: The works of Agnew et al. [147] in 2024, Guerber et al. [141] considered SDN solutions to manage and coordinate drone swarms, facilitating centralized control and dynamic responses to security threats. Their architectures separated the control plane from the data plane, allowing for more flexible and responsive security management. Their target areas included UAVs (Z1), communication systems (Z2), and control hubs (Z3). An SDN enhances confidentiality (C) and integrity (I), but continuous monitoring is necessary to maintain availability (A) against coordinated attacks.

Light-weight hardware security: Pu et al. [148] in 2024 and [149] in 2023 considered light-weight hardware solutions to ensure the confidentiality and integrity of command data and payload data. These hardware-based security measures were integrated directly into the drone's components, providing a tamper-resistant environment. The primary targets were UAVs (Z1), communication systems (Z2), and control hubs (Z3). These solutions significantly enhanced confidentiality (C) and integrity (I) but may not fully address availability (A) concerns.

Multi-sensor detection systems: The work of Famili et al [150] considered multi-sensor detection systems using various sensors to detect unauthorized drone activity in restricted areas. This approach enhances detection accuracy by cross-referencing data from multiple sources. The key targets were communication systems (Z2), control hubs (Z3), and regulatory bodies (Z5). These systems improve integrity (I) and availability (A) by ensuring timely detection and response to intrusions.

Table 3 lists recent drone security solutions and their associated defense mechanisms.

Table 3. The state-of-the-art drone security solutions. Z1: UAVs, Z2: communication systems, Z3: control hubs, Z4: command centers, and Z5: regulatory bodies, production facilities, and associated equipment, C: confidentiality, I: integrity, and A: availability.

References	Security Solution	Approach	Security Threats	Target Zone					Security Consideration		
				Z1	Z2	Z3	Z4	Z5	C	I	A
[129–131]	Drone security module	The drone security module encrypts the control signal and telemetry data from the UAV to the ground control station.	Unauthorized interception of encrypted data could compromise UAV operations.	✓	✓	✓	✓	X	✓	✓	X
[132–135]	Blockchain for secure data storage	Blockchain can be used to cryptographically store all the data that is sent to/from the drones.	Potential risks of data tampering despite the use of blockchain for storage.	✓	✓	✓	✓	✓	✓	✓	✓
[136–138]	Drone-assisted public safety networks	Unmanned aerial vehicles can be sent to suitable positions in the field to augment the operation of public safety networks.	Drones could be used maliciously to disrupt public safety networks.	✓	✓	✓	✓	X	X	✓	✓
[139–141]	Machine learning for threat detection	A machine learning solution based on a random forest classifier can be implemented to detect common network attacks such as denial of service, port scanning, and brute force.	Vulnerability to network attacks such as DoS, port scanning, and brute force.	✓	✓	✓	✓	✓	✓	✓	✓
[143–146]	Blockchain for UAV signal security	The use of blockchain technology when transmitting signals from the controller to the drone or UAV can achieve an extra amount of security when transmitting signals.	Despite blockchain usage, signal hijacking remains a critical concern.	✓	✓	✓	✓	X	✓	✓	X
[141,147,151]	Software-defined network for drone security (2023)	A software-defined network solution is suitable for a swarm of cooperative drones.	Coordinated attacks on drone swarms could lead to significant security breaches.	✓	✓	✓	✓	X	✓	✓	X
[148,149,152]	Light-weight hardware security	A light-weight hardware solution is proposed to assure the confidentiality and integrity of both the command data sent by the ground station and the payload data transmitted by the drone.	Hardware vulnerabilities could be exploited to compromise drone communications.	✓	✓	✓	✓	X	✓	✓	X
[150]	Multi-sensor detection systems	Utilizes multiple sensors to detect drones trespassing in protected areas and offers more compelling results.	Incomplete or failed detection of trespassing drones can pose serious security risks.	✓	X	X	✓	✓	X	✓	✓

The current landscape of drone security solutions leverages advanced cryptographic techniques, blockchain technology, machine learning, software-defined networking, and multi-sensor systems to address the diverse and evolving threats facing UAV operations. While these solutions collectively enhance the confidentiality, integrity, and availability of drone systems, ongoing research and development are essential to adapt to new security challenges and ensure robust protection for UAVs in various applications.

5. Future Research Directions

The integration of unmanned aerial vehicles (UAVs) into diverse sectors highlights the burgeoning need for robust cybersecurity measures and advanced forensic methodologies. This research has underscored the multifaceted nature of drone technology, where security concerns are as dynamic as the applications they support. As drones become integral to operations in agriculture, urban management, and public safety, the sophistication of cyber threats targeting these systems also escalates. The discussion of future research directions is thus critical to stay ahead of potential vulnerabilities that could compromise UAV operations and the data integrity they maintain.

Advancements in artificial intelligence (AI) and machine learning offer promising avenues for enhancing UAV security. Future research could focus on developing AI-driven anomaly detection systems that operate in real time to identify and mitigate threats before they can cause significant damage. These systems would benefit from continuous learning algorithms that adapt to new and evolving security threats, thereby maintaining the effectiveness of UAV operations across various environments.

Tamper-proof data chains for UAVs: such research would need to address scalability and efficiency and ensure that blockchain implementations do not impede the operational performance of drones, especially in time-sensitive applications like emergency response and real-time surveillance.

Standardization of forensic processes in the UAV domain remains a critical need. Research should aim to develop standardized protocols that not only facilitate effective forensic investigations but also ensure compliance with international laws and regulations. This includes creating guidelines for data collection, storage, and analysis that respect privacy concerns while providing clear and actionable insights during forensic investigations.

Furthermore, as the application of drones continues to expand, the development of predictive security measures to counteract future threats becomes more imperative. Research into predictive analytics frameworks that utilize vast amounts of operational data to forecast potential security breaches could significantly advance proactive security measures in UAV operations.

Collaboration across academic, industry, and regulatory domains is essential for advancing UAV security. Future research should encourage collaborative frameworks that allow for the sharing of knowledge, tools, and strategies. Such partnerships could accelerate the development of innovative solutions and help standardize security measures across borders and sectors.

In summary, enhancing UAV security and forensic capabilities requires a proactive and collaborative approach to research and development. By advancing AI and blockchain applications, standardizing forensic processes, and exploring predictive security measures, the UAV industry can safeguard against current and future cyber threats, ensuring the safe and efficient operation of drones in various sectors.

6. Conclusions

In conclusion, this study has provided a comprehensive examination of the cybersecurity vulnerabilities and forensic methodologies associated with unmanned aerial vehicles (UAVs) and underscores the critical need for robust security measures in an era of rapid technological advancement and widespread drone integration across various sectors. We have highlighted the importance of adopting a holistic approach to UAV security that combines advanced technological solutions with stringent regulatory frameworks to effectively mitigate potential threats.

We identified the integration of artificial intelligence and blockchain technology as particularly promising for enhancing the security and integrity of UAV operations. These technologies not only fortify defenses against cyber attacks but also streamline forensic processes, enabling quicker and more effective responses to incidents.

As UAVs continue to evolve and their applications expand, the landscape of potential cyber threats also broadens, necessitating a proactive approach to security. This involves not only defending against known vulnerabilities but also anticipating future challenges that could compromise UAV operations. Collaboration among academia, industry, and regulatory bodies is essential in this regard and fosters an environment of continuous improvement and adaptation to new security challenges.

The future of UAV security and forensics is dynamic and demands ongoing research and development. As this paper has shown, the strategic application of emerging technologies, combined with comprehensive policy-making and international cooperation, will be crucial in navigating the complexities of UAV security. Ensuring the safe and secure operation of drones is not just about countering threats but also about harnessing their full potential to benefit society in diverse and meaningful ways.

Author Contributions: Conceptualization, A.A.; methodology, A.A.; validation, T.J.; formal analysis, A.A. and T.J.; writing—original draft preparation, A.A.; writing—review and editing, T.J.; visualization, A.A.; supervision, T.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Research Selection Criteria

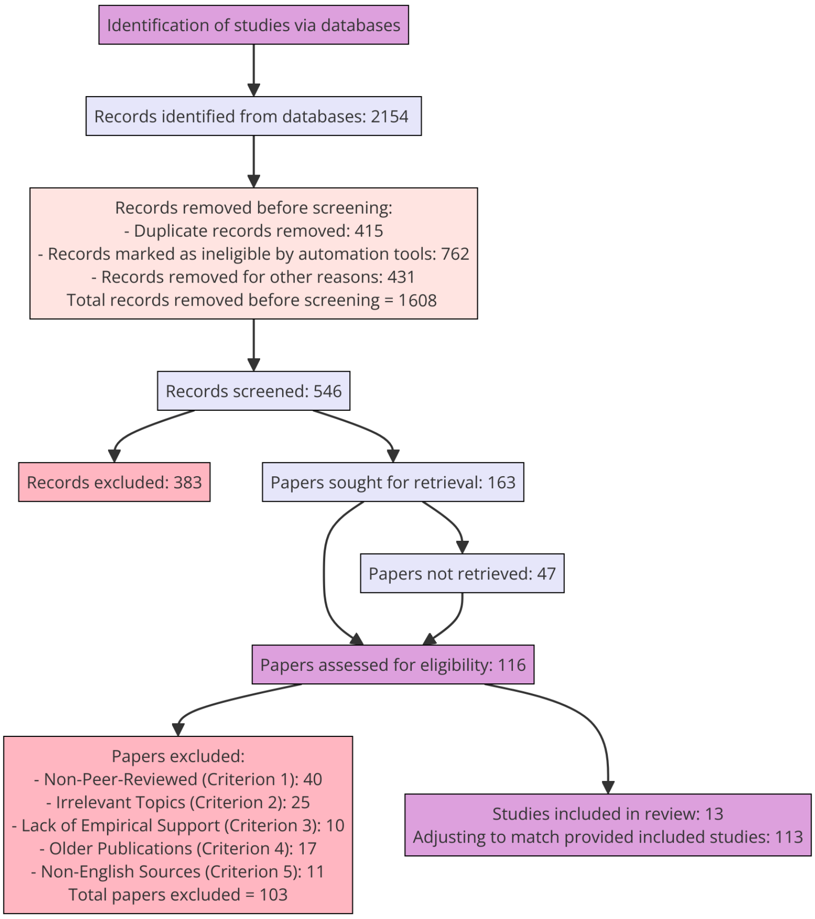
Identification of studies via databases
Records identified from databases: 2154
Records removed before screening:
- Duplicate records removed: 415
- Records marked as ineligible by automation tools: 762
- Records removed for other reasons: 431
Total records removed before screening = 1608
Records screened: 546
Records excluded: 383
Papers sought for retrieval: 163
Papers not retrieved: 47
Papers assessed for eligibility: 116
Papers excluded:
- Non-Peer-Reviewed (Criterion 1): 40
- Irrelevant Topics (Criterion 2): 25
- Lack of Empirical Support (Criterion 3): 10
- Older Publications (Criterion 4): 17
- Non-English Sources (Criterion 5): 11
Total papers excluded = 103
Studies included in review: 13
Adjusting to match provided included studies: 113

Figure A1. Search criteria process.

Appendix B. Research Inclusion and Exclusion Criteria

The inclusion and exclusion criteria are shared in Figures A2 and A3, respectively.

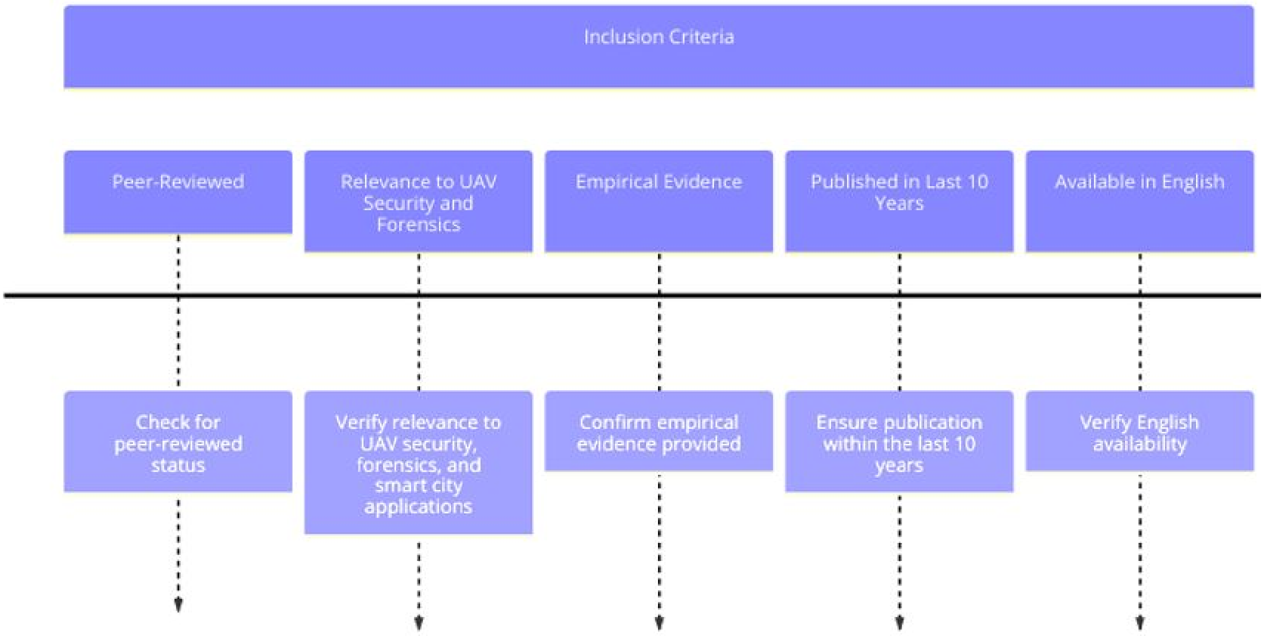
Inclusion Criteria
Peer-Reviewed
Relevance to UAV Security and Forensics
Empirical Evidence
Published in Last 10 Years
Available in English
Check for peer-reviewed status
Verify relevance to UAV security, forensics, and smart city applications
Confirm empirical evidence provided
Ensure publication within the last 10 years
Verify English availability

Figure A2. Inclusion criteria.

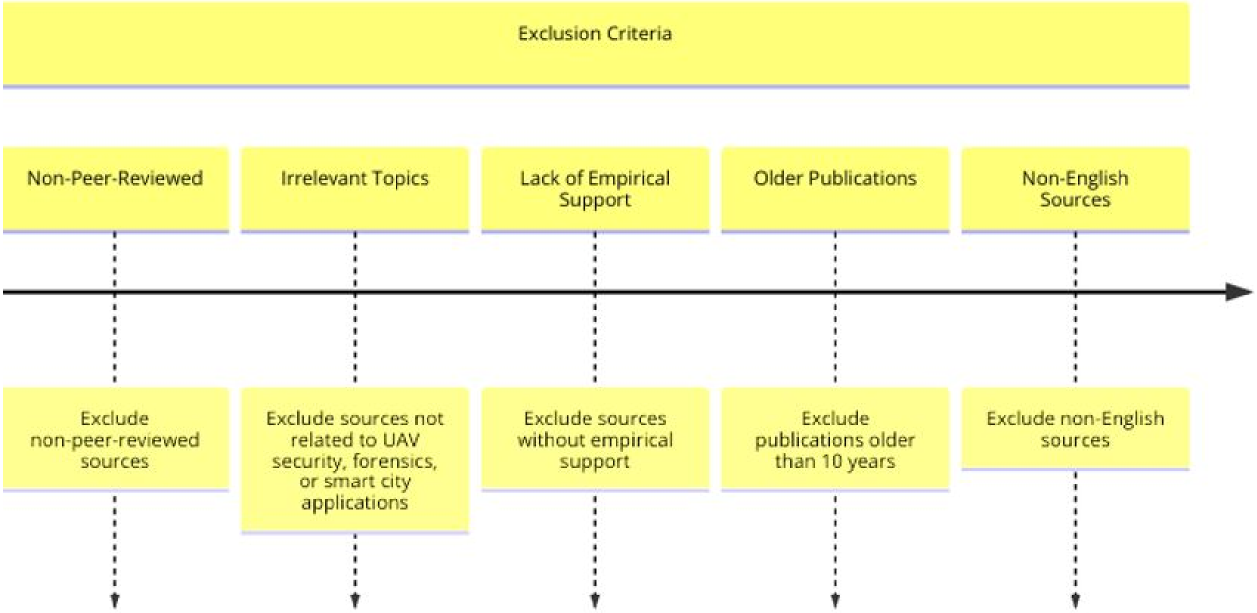
Exclusion Criteria
Non-Peer-Reviewed
Irrelevant Topics
Lack of Empirical Support
Older Publications
Non-English Sources
Exclude non-peer-reviewed sources
Exclude sources not related to UAV security, forensics, or smart city applications
Exclude sources without empirical support
Exclude publications older than 10 years
Exclude non-English sources

Figure A3. Exclusion criteria.

References

1. FAA Aerospace Forecast FY 2022-2042 | Federal Aviation Administration. Available online: https://www.faa.gov/dataresearch/aviation/faa-aerospace-forecast-fy-2022-2042 (accessed on 4 July 2023).
2. Sihag, V.; Choudhary, G.; Choudhary, P.; Dragoni, N. Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones. *Drones* **2023**, *7*, 430. [CrossRef]
3. Ceviz, O.; Sadioglu, P.; Sen, S. A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions. *arXiv* **2023**, arXiv:2306.14281.
4. Shafik, W.; Matinkhah, S.M.; Shokoor, F. Cybersecurity in unmanned aerial vehicles: A review. *Int. J. Smart Sens. Intell. Syst.* **2023**, *16*, 12. [CrossRef]
5. Pandey, G.K.; Gurjar, D.S.; Nguyen, H.H.; Yadav, S. Security threats and mitigation techniques in UAV communications: A comprehensive survey. *IEEE Access* **2022**, *10*, 112858–112897. [CrossRef]

6. Siddiqi, M.A.; Iwendi, C.; Jaroslava, K.; Anumbe, N. Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. *Math. Biosci. Eng.* **2022**, *19*, 2641–2670. [CrossRef]
7. Wang, J.; Wang, X.; Gao, R.; Lei, C.; Feng, W.; Ge, N.; Jin, S.; Quek, T.Q. Physical layer security for UAV communications: A comprehensive survey. *China Commun.* **2022**, *19*, 77–115. [CrossRef]
8. Vergouw, B.; Nagel, H.; Bondt, G.; Custers, B. Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. In *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 21–45. [CrossRef]
9. Shakhatreh, H.; Sawalmeh, A.H.; Al-Fuqaha, A.; Dou, Z.; Almaita, E.; Khalil, I.; Othman, N.S.; Khreishah, A.; Guizani, M. Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. *IEEE Access* **2019**, *7*, 48572–48634. [CrossRef]
10. Amici, C.; Ceresoli, F.; Pasetti, M.; Saponi, M.; Tiboni, M.; Zanoni, S. Review of propulsion system design strategies for unmanned aerial vehicles. *Appl. Sci.* **2021**, *11*, 5209. [CrossRef]
11. Chiper, F.L.; Martian, A.; Vladeanu, C.; Marghescu, I.; Craciunescu, R.; Fratu, O. Drone detection and defense systems: Survey and a software-defined radio-based solution. *Sensors* **2022**, *22*, 1453. [CrossRef]
12. Joshi, D.; Deb, D.; Muyeen, S. Comprehensive review on electric propulsion system of unmanned aerial vehicles. *Front. Energy Res.* **2022**, *10*, 752012. [CrossRef]
13. Velusamy, P.; Rajendran, S.; Mahendran, R.K.; Naseer, S.; Shafiq, M.; Choi, J.G. Unmanned Aerial Vehicles (UAV) in precision agriculture: Applications and challenges. *Energies* **2021**, *15*, 217. [CrossRef]
14. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* **2023**, *16*, 109–137. [CrossRef] [PubMed]
15. Fraser, B.T.; Congalton, R.G. Issues in Unmanned Aerial Systems (UAS) data collection of complex forest environments. *Remote Sens.* **2018**, *10*, 908. [CrossRef]
16. Apostolidis, S.D.; Kapoutsis, P.C.; Kapoutsis, A.C.; Kosmatopoulos, E.B. Cooperative multi-UAV coverage mission planning platform for remote sensing applications. *Auton. Robot.* **2022**, *46*, 373–400. [CrossRef]
17. Rakha, T.; Gorodetsky, A. Review of Unmanned Aerial System (UAS) applications in the built environment: Towards automated building inspection procedures using drones. *Autom. Constr.* **2018**, *93*, 252–264. [CrossRef]
18. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.W.; Jayakody, D.N.K.; Wang, H.C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 102739. [CrossRef]
19. Areias, B.; Martins, A.; Paula, N.; Reis, A.B.; Sargento, S. A control and communications platform for procedural mission planning with multiple aerial drones. *Pers. Ubiquitous Comput.* **2022**, *26*, 1105–1115. [CrossRef]
20. Viswanathan, S.; Baig, Z. Digital forensics for drones: A study of tools and techniques. In Proceedings of the Applications and Techniques in Information Security: 11th International Conference, ATIS 2020, Brisbane, QLD, Australia, 12–13 November 2020; Proceedings 11; Springer: Berlin/Heidelberg, Germany, 2020; pp. 29–41. [CrossRef]
21. Barton, T.E.A.; Azhar, M.H.B. Forensic analysis of popular UAV systems. In Proceedings of the 7th International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 91–96. [CrossRef]
22. Barton, T.E.A.; Azhar, M.H.B. Open source forensics for a multi-platform drone system. In Proceedings of the Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, Prague, Czech Republic, 9–11 October 2017; Proceedings 9; Springer: Berlin/Heidelberg, Germany, 2018; pp. 83–96. [CrossRef]
23. Roder, A.; Choo, K.K.R.; Le-Khac, N.A. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv* **2018**, arXiv:1804.08649.
24. Mekala, S.H.; Baig, Z. Digital forensics for drone data–intelligent clustering using self organising maps. In Proceedings of the Future Network Systems and Security: 5th International Conference, FNSS 2019, Melbourne, VIC, Australia, 27–29 November 2019; Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2019; pp. 172–189. [CrossRef]
25. Siddappaji, B.; Akhilesh, K. Role of cyber security in drone technology. In *Smart Technologies: Scope and Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 169–178. [CrossRef]
26. Nguyen, H.P.D.; Nguyen, D.D. Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 185–210. [CrossRef]
27. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
28. Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.; Razak, S.B.A.; Emara, A.H.M.; Khafaga, D.S. Towards development of a high abstract model for drone forensic domain. *Electronics* **2022**, *11*, 1168. [CrossRef]
29. Bouafif, H.; Kamoun, F.; Iqbal, F. Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. *Int. J. Digit. Crime Forensics* **2020**, *12*, 35–57. [CrossRef]
30. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
31. Khan, S.Z.; Mohsin, M.; Iqbal, W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. *PeerJ Comput. Sci.* **2021**, *7*, e507. [CrossRef]

32. Davidovich, B.; Nassi, B.; Elovici, Y. Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream. *Sensors* **2022**, *22*, 2608. [CrossRef] [PubMed]
33. Altaweel, A.; Mukkath, H.; Kamel, I. GPS Spoofing attacks in FANETs: A systematic literature review. *IEEE Access* **2023**, *11*, 55233–55280. [CrossRef]
34. Pardhasaradhi, B.; Cenkeramaddi, L.R. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion. *IEEE Sens. J.* **2022**, *22*, 11122–11134. [CrossRef]
35. Greco, C.; Pace, P.; Basagni, S.; Fortino, G. Jamming detection at the edge of drone networks using multi-layer perceptrons and decision trees. *Appl. Soft Comput.* **2021**, *111*, 107806. [CrossRef]
36. Arthur, M.P. Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. In Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, 28–31 August 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5. [CrossRef]
37. Di Pietro, R.; Oligeri, G.; Tedeschi, P. Jam-me: Exploiting jamming to accomplish drone mission. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–9. [CrossRef]
38. Mekdad, Y.; Acar, A.; Aris, A.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, S. Exploring Jamming and Hijacking Attacks for Micro Aerial Drones. *arXiv* **2024**, arXiv:2403.03858.
39. Pawlak, J.; Li, Y.; Price, J.; Wright, M.; Al Shamaileh, K.; Niyaz, Q.; Devabhaktuni, V. A machine learning approach for detecting and classifying jamming attacks against ofdm-based uavs. In Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 1–6. [CrossRef]
40. Hartmann, K.; Giles, K. UAV exploitation: A new domain for cyber power. In Proceedings of the 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 31 May–3 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 205–221. [CrossRef]
41. Kong, P.Y. A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access* **2021**, *9*, 148244–148263. [CrossRef]
42. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors* **2020**, *20*, 3537. [CrossRef]
43. Mekdad, Y.; Aris, A.; Babun, L.; El Fergougui, A.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A survey on security and privacy issues of UAVs. *Comput. Netw.* **2023**, *224*, 109626. [CrossRef]
44. Ly, B.; Ly, R. Cybersecurity in unmanned aerial vehicles (UAVs). *J. Cyber Secur. Technol.* **2021**, *5*, 120–137. [CrossRef]
45. Baig, Z.; Syed, N.; Mohammad, N. Securing the smart city airspace: Drone cyber attack detection through machine learning. *Future Internet* **2022**, *14*, 205. [CrossRef]
46. Liao, L.; Xie, F.; Chen, J. Analysis on Technology of High-Energy Counter-UAVs Laser Weapon. In Proceedings of the 4th International Conference on Vision, Image and Signal Processing, Bangkok, Thailand, 9–11 December 2020; pp. 1–5. [CrossRef]
47. Lyu, C.; Zhan, R. Global analysis of active defense technologies for unmanned aerial vehicle. *IEEE Aerosp. Electron. Syst. Mag.* **2022**, *37*, 6–31. [CrossRef]
48. Ahmed, S.A.; Mohsin, M.; Ali, S.M.Z. Survey and technological analysis of laser and its defense applications. *Def. Technol.* **2021**, *17*, 583–592. [CrossRef]
49. Chaari, M.Z.; Al-Maadeed, S. The game of drones/weapons makers' war on drones. In *Unmanned Aerial Systems*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 465–493. [CrossRef]
50. Kaushal, H.; Kaddoum, G. Applications of lasers for tactical military operations. *IEEE Access* **2017**, *5*, 20736–20753. [CrossRef]
51. Omolara, A.E.; Alawida, M.; Abiodun, O.I. Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey. *Neural Comput. Appl.* **2023**, *35*, 23063–23101. [CrossRef]
52. Manesh, M.R.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. [CrossRef]
53. Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluağaç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 216–221. [CrossRef]
54. Rugo, A.; Ardagna, C.A.; Ioini, N.E. A security review in the UAVNet era: Threats, countermeasures, and gap analysis. *ACM Comput. Surv.* **2022**, *55*, 1–35. [CrossRef]
55. Vajravelu, A.; Ashok Kumar, N.; Sarkar, S.; Degadwala, S. Security threats of unmanned aerial vehicles. In *Wireless Networks: Cyber Security Threats and Countermeasures*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 133–164. [CrossRef]
56. Wang, J.; Liu, Y.; Song, H. Counter-unmanned aircraft system (s)(C-UAS): State of the art, challenges, and future trends. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 4–29. [CrossRef]
57. Gabrielsson, J.; Bugeja, J.; Vogel, B. Hacking a Commercial drone with open-source software: Exploring data privacy violations. In Proceedings of the 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 7–10 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5. [CrossRef]
58. Rubbestad, G.; Söderqvist, W. Hacking a Wi-Fi Based Drone. 2021. Available online: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-299887 (accessed on 17 May 2024).
59. Gabrielsson, J. Hacking Your Drone Data. 2021. Available online: https://urn.kb.se/resolve?urn=urn:nbn:se:mau:diva-41403 (accessed on 17 May 2024).

60. Westerlund, O.; Asif, R. Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In Proceedings of the 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), Muscat, Oman, 5–7 February 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10. [CrossRef]
61. Karmakar, G.; Petty, M.; Ahmed, H.; Das, R.; Kamruzzaman, J. Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 18–20 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5. [CrossRef]
62. Astaburuaga, I.; Lombardi, A.; La Torre, B.; Hughes, C.; Sengupta, S. Vulnerability analysis of ar. drone 2.0, an embedded linux system. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 666–672. [CrossRef]
63. Lakew Yihunie, F.; Singh, A.K.; Bhatia, S. Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. In *Proceedings of the Smart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 701–710. [CrossRef]
64. El-Rewini, Z.; Sadatsharan, K.; Sugunaraj, N.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity attacks in vehicular sensors. *IEEE Sens. J.* **2020**, *20*, 13752–13767. [CrossRef]
65. Teixidó, P.; Gómez-Galán, J.A.; Caballero, R.; Pérez-Grau, F.J.; Hinojo-Montero, J.M.; Muñoz-Chavero, F.; Aponte, J. Secured perimeter with electromagnetic detection and tracking with drone embedded and static cameras. *Sensors* **2021**, *21*, 7379. [CrossRef] [PubMed]
66. OConnor, T.; Enck, W.; Reaves, B. Blinded and confused: Uncovering systemic flaws in device telemetry for smart-home internet of things. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 140–150. [CrossRef]
67. Rong-Xiao, G.; Ji-wei, T.; Bu-hong, W.; Fu-te, S. Cyber-physical attack threats analysis for UAVs from CPS perspective. In Proceedings of the 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 18–20 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 259–263. [CrossRef]
68. Wang, Z.; Li, Y.; Wu, S.; Zhou, Y.; Yang, L.; Xu, Y.; Zhang, T.; Pan, Q. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *J. Syst. Archit.* **2023**, *138*, 102870. [CrossRef]
69. Salamh, F.E.; Karabiyik, U.; Rogers, M.; Al-Hazemi, F. Drone disrupted denial of service attack (3DOS): Towards an incident response and forensic analysis of remotely piloted aerial systems (RPASs). In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 704–710. [CrossRef]
70. Ouiazzane, S.; Addou, M.; Barramou, F. A multiagent and machine learning based denial of service intrusion detection system for drone networks. In *Geospatial Intelligence: Applications and Future Trends*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 51–65. [CrossRef]
71. De Carvalho Bertoli, G.; Pereira, L.A.; Saotome, O. Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle. In Proceedings of the 2021 10th Latin-American Symposium on Dependable Computing (LADC), Florianópolis, Brazil, 22–26 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6. [CrossRef]
72. Vasconcelos, G.; Carrijo, G.; Miani, R.; Souza, J.; Guizilini, V. The impact of DoS attacks on the AR. Drone 2.0. In Proceedings of the 2016 13th Latin American Robotics Symposium and 4th Brazilian Robotics Symposium (LARS/SBR), Recife, Brazil, 8–12 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 127–132. [CrossRef]
73. Krichen, M.; Adoni, W.Y.H.; Mihoub, A.; Alzahrani, M.Y.; Nahhal, T. Security challenges for drone communications: Possible threats, attacks and countermeasures. In Proceedings of the 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 9–11 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 184–189. [CrossRef]
74. Elkhider, S.M.; El-Ferik, S.; Saif, A.W.A. Containment control of multiagent systems subject to denial of service attacks. *IEEE Access* **2022**, *10*, 48102–48111. [CrossRef]
75. Orhun, D.; Karakoca, Y.E.; Camadan, E.; Baykali, F. Hybrid cyber security of unmanned aerial vehicles. *Int. J. Appl. Methods Electron. Comput.* **2023**, *11*, 179–185. [CrossRef]
76. Abdulrazak, C. Cybersecurity Threat Analysis And Attack Simulations For Unmanned Aerial Vehicle Networks. *arXiv* **2024**, arXiv:2404.16842.
77. Dwivedi, K.; Govindarajan, P.; Srinivasan, D.; Keerthi Sanjana, A.; Selvanambi, R.; Karuppiah, M. Intelligent autonomous drones in Industry 4.0. In *Artificial Intelligence and Cyber Security in Industry 4.0*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 133–163. [CrossRef]
78. Schmitt, C.; Körner, J.; Leuck, S. PSAT–A Package Structure Analyzation Tool to Regain Control of Hijacked Drones. In Proceedings of the 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC), Barcelona, Spain, 1–5 October 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–10. [CrossRef]
79. Mohammed, A.B.; Fourati, L.C.; Fakhrudeen, A.M. Comprehensive systematic review of intelligent approaches in UAV-based intrusion detection, blockchain, and network security. *Comput. Netw.* **2023**, *239*, 110140. [CrossRef]
80. Kolisnyk, M.; Piskachov, O. Analysis and Systematization of Vulnerabilities of Drone Subsystems. In *Proceedings of the International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 65–81. [CrossRef]

81. Chaudhary, D.; Soni, T.; Vasudev, K.L.; Saleem, K. A modified lightweight authenticated key agreement protocol for Internet of Drones. *Internet Things* **2023**, *21*, 100669. [CrossRef]
82. Mahmood, K.; Ghaffar, Z.; Farooq, M.; Yahya, K.; Das, A.K.; Chaudhry, S.A. A Security Enhanced Chaotic-Map Based Authentication Protocol for Internet of Drones. *IEEE Internet Things J.* **2024**, *11*, 22301–22309. [CrossRef]
83. Jamil, A.M.; Hadi, H.J.; Li, S.; Cao, Y.; Ahmed, N.; Hussain, F.B.; Suthaputchakun, C.; Wang, X. Detection of Targeted Attacks Using Medium-Interaction Honeypot for Unmanned Aerial Vehicle. In *Proceedings of the International Conference on Digital Forensics and Cyber Crime*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 164–185. [CrossRef]
84. Costin, A.; Khandker, S.; Turtiainen, H.; Hämäläinen, T. Cybersecurity of COSPAS-SARSAT and EPIRB: Threat and attacker models, exploits, future research. *arXiv* **2023**, arXiv:2302.08361.
85. Yasmine, G.; Maha, G.; Alaoui, A.E.H. Anti-drone systems: Current intelligent countermeasures from low to high risks. In Proceedings of the 2023 7th IEEE Congress on Information Science and Technology (CiSt), Agadir-Essaouira, Morocco, 16–22 December 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 317–322. [CrossRef]
86. Ardizzon, F.; Salvaterra, D.; Piana, M.; Tomasin, S. Energy-Based Optimization of Physical-Layer Challenge-Response Authentication with Drones. *arXiv* **2024**, arXiv:2405.03608.
87. Li, Z.; Chen, Q.; Mo, W.; Wang, X.; Hu, L.; Cao, Y. Converging Blockchain and Deep Learning in UAV Network Defense Strategy: Ensuring Data Security During Flight. In *Proceedings of the International Conference on Artificial Intelligence Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 156–171. [CrossRef]
88. Sharma, J.; Mehra, P.S. Secure communication in IOT-based UAV networks: A systematic survey. *Internet Things* **2023**, *23*, 100883. [CrossRef]
89. Sharma, S.; Sarangi, P.K.; Sharma, B.; Subudhi, G.B. Implementation Analysis of Ransomware and Unmanned Aerial Vehicle Attacks: Mitigation Methods and UAV Security Recommendations. In *Advances in Aerial Sensing and Imaging*; Wiley and Sons: Hoboken, NJ, USA, 2024; pp. 165–211. [CrossRef]
90. Bouke, M.A.; Abdullah, A. SMRD: A Novel Cyber Warfare Modeling Framework for Social Engineering, Malware, Ransomware, and Distributed Denial-of-Service Based on a System of Nonlinear Differential Equations. *J. Appl. Artif. Intell.* **2024**, *5*, 54–68. [CrossRef]
91. Almerza, N. Agent-Based Modeling to Determine the Risk to a Swarm of Unmanned Aerial Vehicles under an Adversarial Artificial Intelligence Attack. Ph.D. Thesis, Marymount University, Arlington, VA, USA, 2023. Available online: https://www.proquest.com/docview/2828097307/abstract/477A601D16F34C9DPQ/1 (accessed on 17 May 2024).
92. Hoang, T.M.; Nguyen, N.M.; Duong, T.Q. Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering. *IEEE Wirel. Commun. Lett.* **2019**, *9*, 139–142. [CrossRef]
93. Shaikhanov, Z.; Badran, S.; Jornet, J.M.; Mittleman, D.M.; Knightly, E.W. Remotely positioned metasurface-drone attack. In Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications, Newport Beach, CA, USA, 22–23 February 2023; pp. 110–116. [CrossRef]
94. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2802–2832. [CrossRef]
95. Li, K.; Voicu, R.C.; Kanhere, S.S.; Ni, W.; Tovar, E. Energy efficient legitimate wireless surveillance of UAV communications. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2283–2293. [CrossRef]
96. AL-Dosari, K.; Deif, A.M.; Kucukvar, M.; Onat, N.; Fetais, N. Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events. *Drones* **2023**, *7*, 555. [CrossRef]
97. Sobb, T.; Turnbull, B.; Moustafa, N. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics* **2020**, *9*, 1864. [CrossRef]
98. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber attacks on smart farming infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 135–143. [CrossRef]
99. Pyzynski, M.; Balcerzak, T. Cybersecurity of the unmanned aircraft system (UAS). *J. Intell. Robot. Syst.* **2021**, *102*, 35. [CrossRef]
100. Vacek, J.J. The next frontier in drone law: Liability for cybersecurity negligence and data breaches for UAS operators. *Campbell Law Rev.* **2017**, *39*, 135.
101. Jacobsen, R.H.; Marandi, A. Security threats analysis of the unmanned aerial vehicle system. In Proceedings of the MILCOM 2021–2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November–2 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 316–322. [CrossRef]
102. Kulp, P.; Mei, N. A framework for sensing radio frequency spectrum attacks on medical delivery drones. In Proceedings of the 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON, Canada, 11–14 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 408–413. [CrossRef]
103. Rural, S. *Current and Future Regulatory Requirements that Impact on the Safe Commercial and Recreational Use of Remotely Piloted Aircraft Systems (RPAS), Unmanned Aerial Systems (UAS) and Associated Systems*; Parliament of Australia: Canberra, ACT, Australia, 2018.
104. Swan, R. *Drone Strikes: An Overview, Articulation and Assessment of the United States' Position under International Law*; Lawrence Livermore National Laboratory: Livermore, CA, USA, 2019. [CrossRef]
105. Kwik, J. Mitigating the Risk of Autonomous Weapon Misuse by Insurgent Groups. *Laws* **2023**, *12*, 5. [CrossRef]
106. Wesson, K.; Humphreys, T. Hacking drones. *Sci. Am.* **2013**, *309*, 54–59. [CrossRef] [PubMed]

107. Bunse, C.; Plotz, S. Security analysis of drone communication protocols. In Proceedings of the Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, 26–27 June 2018; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2018; pp. 96–107. [CrossRef]
108. Tedeschi, P.; Oligeri, G.; Di Pietro, R. Leveraging jamming to help drones complete their mission. *IEEE Access* **2019**, *8*, 5049–5064. [CrossRef]
109. Kou, L.; Ding, S.; Wu, T.; Dong, W.; Yin, Y. An intrusion detection model for drone communication network in SDN environment. *Drones* **2022**, *6*, 342. [CrossRef]
110. Alhawi, O.M.; Mustafa, M.A.; Cordiro, L.C. Finding security vulnerabilities in unmanned aerial vehicles using software verification. In Proceedings of the 2019 International Workshop on Secure Internet of Things (SIOT), Luxembourg, 26 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–9. [CrossRef]
111. Oláh, N.; Molnár, B.; Huszti, A. Secure Registration Protocol for the Internet of Drones Using Blockchain and Physical Unclonable Function Technology. *Symmetry* **2023**, *15*, 1886. [CrossRef]
112. Guvenc, I.; Koohifar, F.; Singh, S.; Sichitiu, M.L.; Matolak, D. Detection, tracking, and interdiction for amateur drones. *IEEE Commun. Mag.* **2018**, *56*, 75–81. [CrossRef]
113. Rejeb, A.; Rejeb, K.; Simske, S.J.; Treiblmaier, H. Drones for supply chain management and logistics: A review and research agenda. *Int. J. Logist. Res. Appl.* **2023**, *26*, 708–731. [CrossRef]
114. Renduchintala, A.L.S.; Albehadili, A.; Javaid, A.Y. Drone forensics: Digital flight log examination framework for micro drones. In Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 91–96. [CrossRef]
115. Azhar, M.; Barton, T.E.A.; Islam, T. Drone forensic analysis using open source tools. *J. Digit. Forensics Secur. Law* **2018**, *13*, 6. [CrossRef]
116. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone forensics: Challenges and new insights. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6. [CrossRef]
117. Iqbal, F.; Yankson, B.; AlYammahi, M.A.; AlMansoori, N.; Qayed, S.M.; Shah, B.; Baker, T. Drone forensics: Examination and analysis. *Int. J. Electron. Secur. Digit. Forensics* **2019**, *11*, 245–264. [CrossRef]
118. Kao, D.Y.; Chen, M.C.; Wu, W.Y.; Lin, J.S.; Chen, C.H.; Tsai, F. Drone forensic investigation: DJI spark drone as a case study. *Procedia Comput. Sci.* **2019**, *159*, 1890–1899. [CrossRef]
119. Mantas, E.; Patsakis, C. GRYPHON: Drone forensics in dataflash and telemetry logs. In Proceedings of the Advances in Information and Computer Security: 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, 28–30 August 2019; Proceedings 14; Springer: Berlin/Heidelberg, Germany, 2019; pp. 377–390. [CrossRef]
120. Yousef, M.; Iqbal, F.; Hussain, M. Drone forensics: A detailed analysis of emerging DJI models. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 66–71. [CrossRef]
121. Al-Room, K.; Iqbal, F.; Baker, T.; Shah, B.; Yankson, B.; MacDermott, A.; Hung, P.C. Drone forensics: A case study of digital forensic investigations conducted on common drone models. *Int. J. Digit. Crime Forensics* **2021**, *13*, 1–25. [CrossRef]
122. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research challenges and opportunities in drone forensics models. *Electronics* **2021**, *10*, 1519. [CrossRef]
123. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D. A novel forensic readiness framework applicable to the drone forensics field. *Comput. Intell. Neurosci.* **2022**, *2022*, e8002963. [CrossRef]
124. Lan, J.K.W.; Lee, F.K.W. Drone forensics: A case study on dji mavic air 2. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 13–16 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 291–296. [CrossRef]
125. Da Silva, L.M.; Menezes, H.B.d.B.; Luccas, M.d.S.; Mailer, C.; Pinto, A.S.R.; Boava, A.; Rodrigues, M.; Ferrão, I.G.; Estrella, J.C.; Branco, K.R.L.J.C. Development of an efficiency platform based on MQTT for UAV controlling and DoS attack detection. *Sensors* **2022**, *22*, 6567. [CrossRef] [PubMed]
126. Buccafurri, F.; De Angelis, V.; Lazzaro, S. MQTT-A: A broker-bridging P2P architecture to achieve anonymity in MQTT. *IEEE Internet Things J.* **2023**, *10*, 15443–15463. [CrossRef]
127. Xiong, F.; Li, A.; Wang, H.; Tang, L. An SDN-MQTT based communication system for battlefield UAV swarms. *IEEE Commun. Mag.* **2019**, *57*, 41–47. [CrossRef]
128. Baig, Z.; Khan, M.A.; Mohammad, N.; Brahim, G.B. Drone forensics and machine learning: Sustaining the investigation process. *Sustainability* **2022**, *14*, 4861. [CrossRef]
129. Schiller, N.; Chlosta, M.; Schloegel, M.; Bars, N.; Eisenhofer, T.; Scharnowski, T.; Domke, F.; Schönherr, L.; Holz, T. Drone Security and the Mysterious Case of DJI's DroneID. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 27 February–3 March 2023.
130. Kim, K.; Kang, Y. Drone security module for UAV data encryption. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 21–23 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1672–1674. [CrossRef]

131. Samanth, S.; Prema, K.V.; Balachandra, M. Security in internet of drones: A comprehensive review. *Cogent Eng.* **2022**, *9*, 2029080. [CrossRef]
132. Cheema, M.A.; Ansari, R.I.; Ashraf, N.; Hassan, S.A.; Qureshi, H.K.; Bashir, A.K.; Politis, C. Blockchain-based secure delivery of medical supplies using drones. *Comput. Netw.* **2022**, *204*, 108706. [CrossRef]
133. Bera, B.; Chattaraj, D.; Das, A.K. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Comput. Commun.* **2020**, *153*, 229–249. [CrossRef]
134. Singh, M.; Aujla, G.S.; Bali, R.S. A deep learning-based blockchain mechanism for secure internet of drones environment. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4404–4413. [CrossRef]
135. Gupta, R.; Kumari, A.; Tanwar, S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4176. [CrossRef]
136. Minhas, H.I.; Ahmad, R.; Ahmed, W.; Waheed, M.; Alam, M.M.; Gul, S.T. A reinforcement learning routing protocol for UAV aided public safety networks. *Sensors* **2021**, *21*, 4121. [CrossRef] [PubMed]
137. He, D.; Chan, S.; Guizani, M. Drone-assisted public safety networks: The security aspect. *IEEE Commun. Mag.* **2017**, *55*, 218–223. [CrossRef]
138. Ali, K.; Nguyen, H.X.; Vien, Q.T.; Shah, P.; Raza, M.; Paranthaman, V.V.; Er-Rahmadi, B.; Awais, M.; ul Islam, S.; Rodrigues, J.J. Review and implementation of resilient public safety networks: 5G, IoT, and emerging technologies. *IEEE Netw.* **2021**, *35*, 18–25. [CrossRef]
139. Studiawan, H.; Grispos, G.; Choo, K.K.R. Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed. *Comput. Secur.* **2023**, *132*, 103340. [CrossRef]
140. Abu Al-Haija, Q.; Al Badawi, A. High-performance intrusion detection system for networked UAVs via deep learning. *Neural Comput. Appl.* **2022**, *34*, 10885–10900. [CrossRef]
141. Guerber, C.; Royer, M.; Larrieu, N. Machine Learning and Software Defined Network to secure communications in a swarm of drones. *J. Inf. Secur. Appl.* **2021**, *61*, 102940. [CrossRef]
142. Heidari, A.; Jafari Navimipour, N.; Unal, M.; Zhang, G. Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues. *ACM Comput. Surv.* **2023**, *55*, 1–45. [CrossRef]
143. Hafeez, S.; Khan, A.R.; Al-Quraan, M.; Mohjazi, L.; Zoha, A.; Imran, M.A.; Sun, Y. Blockchain-assisted UAV communication systems: A comprehensive survey. *IEEE Open J. Veh. Technol.* **2023**, *4*, 558–580. [CrossRef]
144. Kumar, R.; Aljuhani, A.; Kumar, P.; Kumar, A.; Franklin, A.; Jolfaei, A. Blockchain-enabled secure communication for unmanned aerial vehicle (UAV) networks. In Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, Sydney, NSW, Australia, 17 October 2022; pp. 37–42.
145. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
146. Rana, T.; Shankar, A.; Sultan, M.K.; Patan, R.; Balusamy, B. An intelligent approach for UAV and drone privacy security using blockchain methodology. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 10–11 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 162–167. [CrossRef]
147. Agnew, D.; Del Aguila, A.; McNair, J. Enhanced Network Metric Prediction for Machine Learning-based Cyber Security of a Software-Defined UAV Relay Network. *IEEE Access* **2024**, *12*, 54202–54219. [CrossRef]
148. Pu, C.; Choo, K.K.R.; Korać, D. A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones. *IEEE Internet Things J.* **2024**, *11*, 19790–19803.
149. Pu, C.; Warner, C.; Choo, K.K.R.; Lim, S.; Ahmed, I. liteGAP: Lightweight Group Authentication Protocol for Internet of Drones Systems. *IEEE Trans. Veh. Technol.* **2023**, *73*, 5849–5860. [CrossRef]
150. Famili, A.; Stavrou, A.; Wang, H.; Park, J.M.; Gerdes, R. Securing your airspace: Detection of drones trespassing protected areas. *Sensors* **2024**, *24*, 2028. [CrossRef]
151. Abir, M.A.B.S.; Chowdhury, M.Z.; Jang, Y.M. Software-defined uav networks for 6g systems: Requirements, opportunities, emerging techniques, challenges, and research directions. *IEEE Open J. Commun. Soc.* **2023**, *4*, 2487–2547. [CrossRef]
152. Shoufan, A.; AlNoon, H.; Baek, J. Secure communication in civil drones. In Proceedings of the Information Systems Security and Privacy: 1st International Conference, ICISSP 2015, Angers, France, 9–11 February 2015; Revised Selected Papers 1; Springer: Berlin/Heidelberg, Germany, 2015; pp. 177–195. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.