drones

MDPI

*Review*

# Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones

**Vikas Sihag [1], Gaurav Choudhary [2,*], Pankaj Choudhary [1] and Nicola Dragoni [2]**

[1] Department of Cyber Security, Sardar Patel University of Police, Security and Criminal Justice, Jodhpur 342037, India; vikas.sihag@policeuniversity.ac.in (V.S.); mtcs20pc@policeuniversity.ac.in (P.C.)
[2] DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark, DK-2800 Kongens Lyngby, Denmark; ndra@dtu.dk
* Correspondence: gauch@dtu.dk

**Abstract:** Cyber Security and forensics for Unmanned Aerial Vehicles (UAVs) pose unique requirements, solutions, and challenges. As UAVs become increasingly prevalent for legitimate and illegal use, ensuring their security and data integrity is important. Solutions have been developed to tackle these security requirements. Drone forensics enables the investigation of security incidents involving UAVs, aiding in identifying attackers or determining the cause of accidents. However, challenges persist in the domain of UAV security and forensics. This paper surveys drone threat models, security, and privacy aspects. In particular, we present the taxonomy of drone forensics for investigating drone systems and talk about relevant artifacts, tools, and benchmark datasets. While solutions exist, challenges such as evolving technology and complex operational environments must be addressed through collaboration, updated protocols, and regulatory frameworks to ensure drones' secure and reliable operation. Furthermore, we also point out the field's difficulties and potential future directions.

**Keywords:** drone forensics; unmanned aerial vehicles; digital investigation; drone security



**Citation:** 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. https://doi.org/10.3390/drones7070430

Academic Editors: Emmanouel T. Michailidis, Demosthenes Vouyioukas and Petros Bithas

Received: 22 May 2023
Revised: 20 June 2023
Accepted: 25 June 2023
Published: 28 June 2023



## 1. Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are controlled and piloted remotely and are employed for defense and rescue missions. Drones were primarily used for defense purposes (for example, they are highly utilized in the Ukraine–Russia war), but in recent years, their use for civilian purposes has grown significantly. Drones are being used for tasks such as patrolling and policing, search and rescue, agrotech and videography, and preventing and identifying poachers due to the domination of the digital lifestyle. Additionally, drones have been found in unintended violations of no-fly zones, raising the possibility that terrorists could use them to cause terror and possibly other harm [1]. By 2025, the worldwide drone industry is anticipated to reach $42.8 billion, growing 13.8% annually [2].

Cyber forensics is the domain of forensic science that deals with gathering evidence from digital devices and analyzing events. Drone forensics deals with the forensic analysis of drones for investigation purposes. The popularity and affordability of drones have also increased their use in illegal activities. Investigations depend heavily on the drone taken from the crime scene and the gadgets it was attached to. Evidence can be gleaned from a drone and its ground controller, including the drone's identification number, prior flight locations, camera images, logs, and software used. Drone forensics are difficult because they rely on volatile memory and dynamic data that might be lost when the battery is discharged [3,4]. When criminals utilize technology to hide their tracks, law enforcement officers are left to try and retrieve evidence from their computers, phones, or storage drives for investigations. Authorities need a dependable way to extract data from these seized drones so that the evidence is stored and acceptable in court.

Currently, recreational drone usage dominates the landscape, with enthusiasts being the primary users. However, major companies such as Amazon, Google, and Meta have ambitious plans to incorporate drones into their operations for delivering goods and services. As the number of operational drones continues to rise, it is expected that an increase in security, privacy, and safety concerns will follow. Drones can be controlled remotely or autonomously through onboard computers [5]. Drones rely on a network of sensors and actuators that establish communication with the Ground Control System (GCS) via wireless links. Consequently, drones become vulnerable to potential attacks targeting their cyber and/or physical components, the interface between them, the wireless link, or even a combination of multiple components. In a popular example of drone takeover, an American drone that purportedly breached Iranian airspace was successfully landed by an Iranian cyber warfare team [6]. A possible sequence of events reveals that a combination of cyber attacks was deployed, wherein all contacts with the drone were initially cut off by jamming both the satellite and ground control signals. Further, a GPS spoofing attack was initiated to deceive the drone into believing it was landing in its home base by feeding it with manipulated GPS data to make it land in Iran.

Due to the significance of drone security, this paper analyzes recent drone system assaults in this article. This work also focuses on protocols, related threats, targeted security features, and solutions proposed in the literature. It examines the related security and privacy challenges of drones. It also presents a comprehensive drone forensics methodology for the analysis of drone systems and talks about relevant artifacts, tools, and benchmark datasets. The findings of this study will help academics and developers better understand the state of drone forensics and security today.

*Methodology:* The research methodology selected for this paper amounts to a systematic literature review, in which a rigid framework for searching the literature is used to answer precise research questions. This is to ensure accurate and impartial data search and retrieval. For the review of the literature, we used the snowballing approach. A preliminary collection of papers was identified via a database search utilizing relevant keywords and filters. The search engines used were DTU Findit, Google Scholar, Semantic Scholar, and Scopus. Following the selection of the beginning set, a number of iterations of snowballing were conducted, using the reference lists of the papers that had previously been included to find new ones to add (backward snowballing). Additionally, we took into account publications that mentioned previously processed ones (forward snowballing). Finally, all publications that were recognized moved on to the data extraction stage, which was carried out in line with the research study. In our review, we used keywords such as drone, UAV, security, and forensics and their synonyms and keyword combinations for searching. Figure 1 provides a glimpse of the publishing pattern over the last decade.

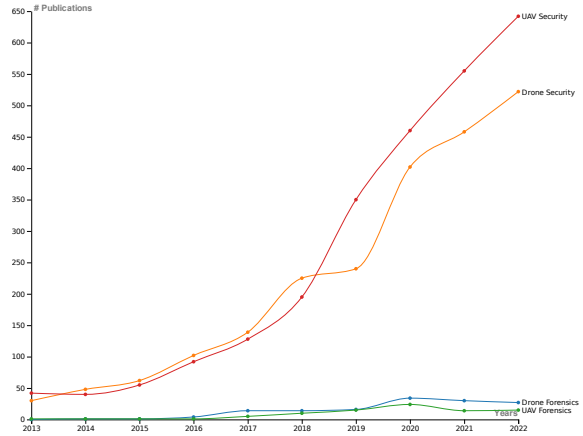


**Figure 1.** Number of publications over the last decade related to keywords: *Drone, UAV, Security* and *Forensics*. Note that the graph only accounts for publications having the desired keyword(s) in their title or abstract and belonging to the related field of research.

*Contributions of the paper:* This systematic survey aims to review and classify the existing drone forensic techniques. A taxonomy is designed based on forensic artifacts, their type, generation method, and location. In particular, we describe the process of conducting a UAV forensic investigation, together with drone artifacts, forensic analysis tools, and benchmark datasets. Furthermore, this review presents drone architecture, threat models, and attack scenarios. This survey would help in understanding the current state of the drone ecosystem.

*Structure of the paper:* In Section 3, we present an overview of the drone and its architecture. Section 4 defines the identified threats and attack models. Security and privacy issues of drone systems are detailed in Section 5. Section 6 discusses the proposed drone forensics framework, forensic artifacts, related tools, and benchmark datasets. Furthermore, we discuss and present future challenges in Section 7. Finally, we conclude this work in Section 8.

## 2. Related Works

Numerous review studies have covered the privacy and security concerns with drones. These earlier survey investigations have contributed to building a strong grasp of the problems. Table 1 compares our proposed work with a brief summary of the existing survey research on drone security problems and forensics. To the best of our knowledge, the level of security concerns and forensics related to the various categories of drones is lacking from the reviews that have already been published. Additionally, most papers offer scant details on the problems or conducted research before the drone paradigm existed. We identified related reviews/surveys in drone forensics during our keyword searches. Gulatacs et al. [7] introduced a comprehensive seven-phase framework for UAV digital forensics investigation. Their study focused on the Phantom III model and involved a meticulous examination of three distinct types of forensic evidence. Among the artifacts analyzed, the EXIF header of photographs taken by the UAV's onboard camera played a crucial role. Additionally, two log files stored as binary files were scrutinized, along with the EXIF headers of the captured images, which enabled the reconstruction of the UAV's flight path.

Salamh et al. [8] discussed discovering personally identifiable information, testing, and evaluating currently available forensic software tools. Furthermore, the researchers examined data storage mechanisms and evidence organization within two DJI UAV models, namely the Phantom 4 and Matrice 210. Their study also involved investigating the retrieval of flight trajectories from UAVs through the utilization of 3D visualization software. Yahuza et al. [9] examines recent trends in Internet of Drones (IoD) network security and privacy challenges and the extent of security and privacy vulnerabilities posed by various drone categories. It also discusses the necessity for a secure IoD architecture and recommends one. A detailed taxonomy of assaults on the IoD network is also presented.

Salamh et al. [10] present a ten-phase technical forensic process for studying forensic evidence from Remotely Piloted Aerial Systems (RPAS), which can help simplify drone identification and investigation. They analyzed drone photos from the Computer Forensics Reference Datasets (CFReDS) for drone identification. Clark et al. [11] discussed the primary account for specific file structures stored by the studied drone and the primary detailed forensic investigation of the DJI Phantom III drone. The research includes preliminary findings on TXT files, proprietary, encrypted, and encoded files on the drone's mobile device. These files contained a wealth of information, including GPS coordinates, battery life, and flight time. The widely acceptable open-access tool Drone Open Source Parser (DROP), which parses copyrighted DAT files taken from the drone's nonvolatile internal storage, is also presented.

Yaacoub et al. [12] examined the new hazards posed by drones in cyber attacks and methods to counter these attacks. Furthermore, they provided a comprehensive overview of the use of drones in various domains. A practical attack scenario is demonstrated against

a specific drone model. It enables them to adopt and develop new tactics and technologies for improved UAV attack detection and defense.

Al-Room et al. [13] looked into six different drone brands widely utilized in illegal activities and collected forensically relevant data such as GPS location, photographs and videos, flight paths of the drones, and information on the drone's ownership. The experiment showed that drone forensics might help law enforcement agencies acquire essential information for criminal investigations.

Security and privacy in the age of commercial drones are investigated by Nassi et al. [14]. It provides a framework for analyzing attack and prevention strategies, conducting a thorough evaluation, and identifying scientific flaws. It also includes a list of societal targets, profiles of attackers, an examination of threats, a technique for analyzing preventative measures, and a full review. They have also provided a method for evaluating countermeasures, comprehensive examination, and identification of scientific gaps.

The forensic investigation study thoroughly examines a Parrot AR drone 2.0 [15] to enhance our understanding of drone forensics, encompassing various challenges, forensic investigation procedures, and experimental discoveries. The authors provide novel perspectives on drone forensics by exploring forensic methodologies, obtaining access to the drone's digital storage, and retrieving significant data. These valuable insights aid digital forensic investigators in determining ownership, recovering flight data, and accessing media assets.

**Table 1.** Other related surveys and review articles on Drone Forensics (**A**: Attacks, **V**: Vulnerabilities, **T**: Threats, **C**: Countermeasures, ★: Forensic Investigation, ✓: Partial discussion, ✓☆: Full discussion).

| Year | Paper | Network Forensics | Security Aspects | | | | | | | | | | Privacy Aspects | | Models |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Communication | | | | Software | | | | | | | | |
| | | | A | V | T | C | A | V | T | C | A | C | | | |
| 2016 | [16] | ✓ | ✓☆ | | ✓☆ | ✓☆ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| 2017 | [11] | | ✓ | | | | | | | | | | | | ✓ |
| 2018 | [7] ★ | ✓ | ✓ | ✓ | | ✓ | | | | | | | | | ✓ |
| 2018 | [17] | ✓ | ✓ | | ✓☆ | | ✓ | | | | ✓ | | | | |
| 2019 | [10] ★ | ✓ | ✓ | | ✓ | | ✓ | | | | ✓ | | | | ✓ |
| 2019 | [18] ★ | | | | | | ✓ | | ✓ | | ✓ | ✓ | | | ✓ |
| 2019 | [19] | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | |
| 2019 | [20] | | | | | | ✓ | | | | ✓ | ✓ | | | |
| 2020 | [15] ★ | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | | | |
| 2020 | [12] | ✓ | ✓☆ | ✓ | | ✓☆ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| 2020 | [21] | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | | | |
| 2021 | [9] | | ✓ | | ✓☆ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | | |
| 2021 | [22] | | ✓ | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | | | |
| 2021 | [23] | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | ✓ | ✓ | | | |
| 2022 | [4] | | | | | | | | | | | | | | ✓ |
| 2022 | [24] | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | | | | | |
| 2023 | Proposed ★ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | ✓☆ | | | ✓☆ |

## 3. Overview of Drones

The primary components of a drone system include a Ground Station Controller, physical sensors, actuators, a Power Management System (PMS), a Flight Control Board (FCB), a rotor system, an Electronic Speed Controller (ESC), and a Transceiver Control Unit (TCU). These crucial elements, such as ESC, FCB, TCU, and PMS, can serve as potential sources for drone forensics procedures. They store vital data related to flight control, flight records, internal monitoring, and information from transceivers and sensors mounted on the drone. It is important to note that the specific components may vary depending on

the drone's purpose or usage. Additionally, inertial sensors are responsible for altering control surfaces and thrust, while navigation components, such as GPS, Compass, Galileo, GLONASS, or other inertial sensors, aid in drone navigation by adjusting thrust and control surfaces.

### *3.1. Drone Architecture*

The three primary components of a drone system are the drone, the Ground Control System (GCS), and the data communication link. An aircraft, a power source, a flight controller, a precise navigation system, and a sensor system are primary components of a drone. An architecture of a drone system and its primary components are shown in Figure 2.

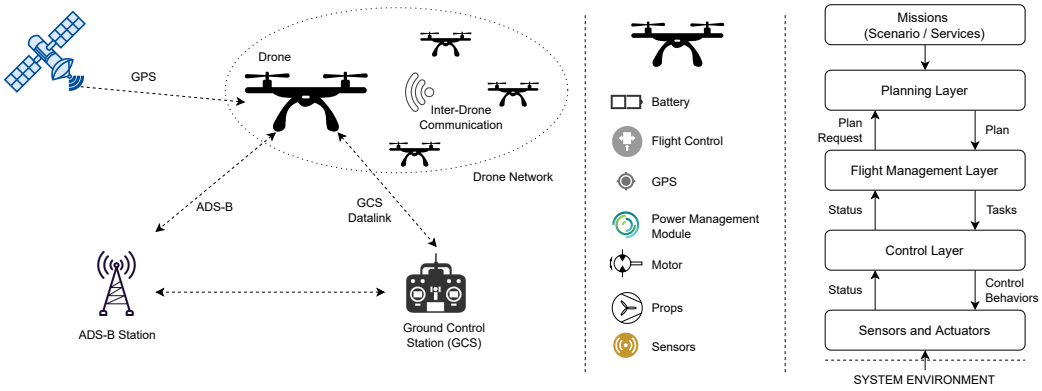


**Figure 2.** Drone system, components of drone and its architecture.

#### 3.1.1. Drone Craft

The drone system's central mobile component is the drone craft, which resembles a flying robot that can be operated remotely or fly autonomously using software-controlled flight plans integrated into the system. There are four main types of drones: Multi-Rotor Drones, Fixed-Wing Drones, Single-Rotor Drones, and Fixed-Wing Hybrid VTOL (Vertical Take-Off and Landing) drones. Multi-rotor aircraft equipped with multiple motors come in various configurations, such as tricopters (3 rotors), quadcopters (4 rotors), hexacopters (6 rotors), or octocopters (8 rotors). In contrast, fixed-wing drones are designed to function as airplanes with a single rigid wing, eliminating the need to maintain a constant airborne position and making them energy-efficient. Aside from the rotors, the flight controller is another crucial component of a drone craft. It collects sensor data, processes it into meaningful information, and depending on the control mode, either transmits the data to the Ground Control System (GCS) or directly updates the state of the actuator control units. The flight controller provides the GCS communication interface as depicted in Figure 2.

#### 3.1.2. Datalink

The datalink is the wireless connection between UAV and GCS that carries control and data signals. The UAV's operating range determines the communication link chosen. UAV operations are divided into Line-Of-Sight (LOS) missions, in which control signals are sent and received via direct radio waves, and Beyond Line-Of-Sight (BLOS) missions, in which the drone is controlled via satellite systems or a relaying aircraft, which could be a drone itself, based on their distance from the GCS.

#### 3.1.3. Ground Control Station

GCS is the base structure that allows human operators to manage and monitor drones throughout their missions. A GCS provides a wireless link to connect with the drone, allowing it to send commands and collect real-time data. GCSs vary in size depending on the drone's type and mission. It can be a self-contained facility with several workstations for tactical and strategic applications.

### 3.2. Drone Communications

Unmanned aerial systems are used for various defense and civilian purposes, including pollutant research, glaciology studies, wildfire management, disaster management, hurricane tracking, flood impact investigations, and illegal narcotic identification. A drone system or UAS must be able to communicate with other entities in its network. WiFi is a common mode of communication between UAVs and base stations. WiFi has a relatively low transmission range, often a few hundred meters. The range of radio communication is thousands of meters. As shown in Figure 2, a general drone network is made up of drones, ground control stations (GCS), navigation satellite systems, and air traffic control systems such as Automated Dependent Surveillance-Broadcast (ADS-B) systems. The following communication links are used to communicate between network entities:

- *GCS communication:* This datalink supports UAS and ground control station communications, and the GCS uses wireless signals to communicate with UAVs, allowing it to monitor network traffic and direct flight operations. These communications are based on short-range wireless technologies, making them prone to different attacks [25].
- *ADS-B communication:* Automatic Dependent Surveillance-Broadcast (ADS-B) has been adopted for aircraft Air Traffic Control (ATC) systems. Anonymous ground users and other aircraft can use ADS-B to periodically broadcast general navigation information through long-range RF signals. It operates on 1090 MHz and is a digital protocol. Standard identification and navigational data for the aircraft, such as altitude, GPS, and the aircraft's identification number, are included in ADS-B signals. Drones have lately started using ADS-B [26]. For smaller drones, conventional ADS-B systems are too large; hence, smaller ADS-B modules are required [27]. This enables DAA (detect and avoid) capabilities, enhancing safety for airspace users and providing easier drone identification and tracking.
- *GPS communication:* The controller must identify the drone's path for collision avoidance in Beyond Line-of-Sight (BLOS) operations. A drone connects with GPS satellites to transmit and receive data and information. As a result, UAVs can develop satellite network connectivity to collect their real-time GPS coordinates. Additionally, satellite communications are beneficial across large distances even without developed infrastructure and enable stable communication with higher data frequency.
- *Video transmission:* 1.3 GHz, 2.4 GHz, and 5.8 GHz are common RF data links for video transmission. (i) 1.3 GHz—This system can have a range of more than 40 miles and better penetration abilities, depending on the amount of power employed. Because of its low data rates, it provides poor video quality. (ii) The range of a 2.4 GHz system can be up to 15 miles. As 2.4 GHz is also utilized for control, using it for video will cause interference. (iii) The most widely used frequency for video transmission is 5.8 GHz because of its short wavelength and high data rate transfer capacity. Compared to the other options, it produces a clear video. However, it can only penetrate a restricted distance of 5 miles due to its small wavelength.

## 4. Threat Models and Attack Scenarios

The attacks on emerging drone technology bring risks to the safety and security of data, infrastructure, and the public. The attacker can exploit the zero-day vulnerabilities and security gaps to enter drone communication networks [28,29]. Drone forensics can play a significant role in identifying the attacker's objective. Drone forensics is a systematic investigation procedure that collects, preserves, and analyzes the drone's digital, software, and hardware-related evidence. Drone forensics can help to build a new technology/policy to reduce the impact of similar attacks in the future and help to increase the security level. This section discusses various drone security attacks to give systematic paths for the drone investigation process. Unreliable communication mediums and frequency-based vulnerabilities increase the attack risks [30]. The latest technology drones, which have their camera, and GPS signal associated with it, are also vulnerable to attacks. The taxonomy classification of Drone attacks with impacts and their execution tools and the mechanism is shown in Table 2.

**Table 2.** Taxonomy classification of Drone attacks with impacts and their execution tools and mechanism. Z1: Drones, Z2: Communication Networks, Z3: Base Stations, Z4: Ground Control Stations, Z5: Certification Authorities, Production and Manufacturing Units, and other involved devices.

| Drone Attacks | Tools/Mechanisms | Impact | Security Requirements | Attack Surfaces | Key Papers |
|---|---|---|---|---|---|
| Traffic Analysis and Network Stalking | SNMP, Packet sniffer, NetFlow | Privacy | Anti-spyware and packet filters | Z2 | [12,31–36] |
| Interception | Drone Monitoring Equipment, Acoustic Sensors | Privacy | Encryption technique | Z1,Z2,Z3,Z4 | [37,38] |
| Data Capturing and Forensics | Using serial connection, ExtractDJI, Datcon, Prodiscover Basic | Privacy | Encryption technique | Z1,Z2,Z5 | [15,39–43] |
| Location Tracing | Drone Monitoring Equipment, Acoustic Sensors, Radar | Privacy | Utilize counter-drone techniques | Z1,Z2 | [44–46] |
| Data/Information Leakage | Substitution and alteration, Modification, Duplication | Integrity | Use Secure channel switching and Encrypted data | Z1,Z2,Z3,Z4,Z5 | [47–50] |
| ACL Modifications | DroneSploit, hacking Tools | Integrity | Validate user-controllable input | Z1,Z2,Z3,Z5 | [51–53] |
| Man-In-Middle Attacks | Wifi attack, Remote-AT-Commands, WiFi Pineapple Nano, Raspberry Pi 3, Maldrone, SkyJack: | Integrity | a Public Key signed by a trusted Certificate Authority, encrypting the communication link, ensuring robust mutual authentication at both ends of the communication channel, and securely exchanging public keys | Z2,Z3 | [54–57] |
| Message Forgery | DroneSploit, Remote-AT-Commands | Integrity | Use Secure channel switching and Encrypted data | Z2,Z1,Z5 | [58–60] |
| Identity Spoofing and Key exploitations | Side-Channel Attacks, Weak Configuration, Vulnerability Exploitations | Confidentiality | Use secure and robust protocols with strong authentication | Z1,Z2,Z3,Z4,Z5 | [61–63] |
| Unauthorized Access and Controls | Drone Monitoring Equipment, DroneSploit, hacking Tools, Wifi attack, | Confidentiality | Utilize strong passwords | Z1,Z2,Z3,Z4,Z5 | [17,61,64,65] |
| Replay Attacks | Protocol Manipulation | Confidentiality | Use secure and robust protocols with strong authentication, and the authentication mechanism should include fresh message requests securely before data exchange or communication | Z2 | [66–71] |

**Table 2.** *Cont.*

| Drone Attacks | Tools/Mechanisms | Impact | Security Requirements | Attack Surfaces | Key Papers |
|---|---|---|---|---|---|
| Eavesdropping | Sniffing tools, Password Cracking, Scrambling/Distortion | Confidentiality | Use encryption technique | Z2 | [12,23,58,72–74] |
| Physical Attacks | Drone Countermeasures Equipment, High Power Microwave (HPM) Devices, Nets & Net Guns, High-Energy Lasers | Availability | Use physical security techniques and Trusted Secure platforms | Z1,Z3,Z4 | [9,12,16,75,76] |
| DoS Attacks/DDoS Attacks | Use logic attacks and resource attacks, Ping of Death, SYN Flood, SYN Flood, x | Availability | Use freshness and Countermeasure scheme against the resource exhaustion. | Z2 | [12,77–80] |
| GPS Spoofing | Mock GPS with Joystick. Mock Locations, Fake GPS ByteRev, Fake GPS Go Location Spoofer. | Availability | Use anti-spoofing techniques | Z2,Z3 | [62,81–85] |
| Channel Jamming | HPM Devices, RF Jammers, Radio Frequency (RF) Analyzers, HackRF and BladeR | Availability | Beamforming and dynamic relaying, Multipoint transmission | Z1,Z2,Z3,Z4 | [46,86–91] |
| Routing Attacks | Waypoint alterations, black or grey hole attacks | Availability | Secure Routing, Self- adaptability Mechanism | Z1,Z2,Z3 | [17,37,92–94] |
| Use of Fake Drones | Key loggers, Third-party Violations, Firmware replacement attacks | Trust | Trust verification, Encryption and sensor firmware robustness, timely Update firmware | Z5 | [95–98] |

### *4.1. RF Jamming*

RF connects a drone to the ground transmitter or remote control. Radio frequencies in ranges lie between 2.4 GHz to 5.8 GHz, and 2.4 GHz and 5.8 GHz are the most common frequency used to control a drone remotely. The attacker tries to identify the operating channel frequency and tune it to that frequency. On the same frequency as the target device, RF jammers broadcast strong signals compared to the target device's signals. The combination of broadcasted signals overwhelms the receiver, preventing it from decoding any target signals. Figure 3 shows a generalized RF jamming attack scenario. These attacks violate drone availability. The usage of frequency hopping and multiple narrow bandwidth signals with short bursts of transmission make jamming difficult.

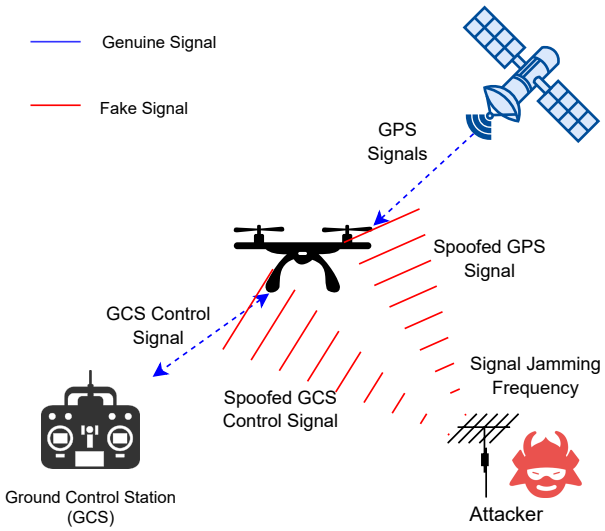


**Figure 3.** Jamming and spoofing attacks.

### *4.2. Cloning*

In a hostile physical environment, exposure to drones allows an adversary to capture, clone, or temper with these devices. An Iranian popular drone manufacturer's recent advanced long-range drones are accused of being designed by reverse engineering from a US drone captured in 2011 [99]. In a cloning attack, the attacker physically captures and possibly reprograms a drone and creates clone(s) by copying the captured one. The cloned drone can then be used to mount further attacks. The genuine user thinks he has all the authority over the drone, but in reality, he flies the clone of the drone, and the attacker drives the original drone. The attack can use identifiers, secret keys, hardwired keys, and stored data of cloned drones to eavesdrop on existing communication. Tamper-resistant hardware and drone behavioral monitoring can be used to counter such attacks. Remote attestation can be significant in detecting the trustworthiness of deployed drones.

### *4.3. GPS Spoofing*

Civil GPS is an extensively used protocol. GPS is used to find the location of the drone or UAV. GPS is a broadcast system only, and it tracks the drone with the help of satellites and measures the time of flights of the data signals. GPS works on the trilateration principle, in which the drone receives the signal from satellites in the form of place and time (sent and receive). In a GPS spoofing attack, the GPS receiver is made to believe that the drone is located differently than its actual physical location. Recent drones have inbuilt GPS sensors for location guidance and tracking for various missions with other features such as location hold, altitude hold, return to home function, etc. The GPS being unencrypted makes drones prone to a GPS spoofing attack. The adversary sends false or modified GPS signals to the drone. A commonly employed method known as a replay attack involves capturing and replaying the signal received from a satellite, introducing an additional delay. This technique needs real-time visibility of the satellites and a transmitter with sufficient power to overpower the direct signals received from the satellite. By manipulating the observed time-of-flight of the signal, a receiver can be deceived into believing it is located at a greater distance from the satellite than it is. Table 3 illustrates GPS frequency bands and their usage in different fields [25].

Another GPS-based attack is GPS jamming. Disconnecting the receiver from the authentic satellite can be an easy way. However, under the Wireless Telegraphy Act, it is an offense to "knowingly use" such a device to block GPS signals. Recently, a GPS jamming attack caused 46 drones to plummet during a display over Victoria Harbour [100]. These attacks can be detected by verifying the claimed position of satellites with various techniques, such as remote attestation and periodic or random location checking.

**Table 3.** Frequencies used by GPS channels in UAVs [25].

| Band | Frequency | Usage |
|---|---|---|
| L1 | 1575.42 MHz | L1 Civilian (L1C) |
| L2 | 1227.60 MHz | L2 Civilian (L2C) |
| L3 | 1381.05 MHz | Nuclear/Research |
| L4 | 1379.913 MHz | Research |
| L5 | 1176.45 MHz | Safety-of-life(SOL) Data |

### *4.4. Software Based Attack*

Attackers have demonstrated the use of software to hack the video feeds of Predator (and likely Reaper) drones. Software such as SkyGrabber Version 3.2 is popular for offline satellite internet downloads. It intercepts satellite data, including movies, music, pictures, etc., that are downloaded by other users and saves information on the hard disk. It exploits the unencrypted and unauthenticated communication link used for data feeds sent to the ground station using communication satellites. In this attack, the adversary needs to customize the satellite dish for selecting a satellite provider and start grabbing the data packets. The SkyGrabber intercepts data, assorts them into files, and saves the files locally. It is a downloadable computer program that has been used to capture drone images and video recordings. SkyGrabber software can take satellite internet data and assemble it in files such as .avi, .mp3, .mp4, etc., and save this file on hard disk [101]. Attackers use this software, and if the connection between the drone and ground station is unencrypted, they use it to access their videos and other files that are shared between the drone and ground station and can also be used to monitor.

Figure 4 illustrates image and video capture by sky grabber software in the BLOS scenario. These attacks violate drone confidentiality and integrity because the sky grabber software attack breaks the secretiveness and violates the access information. These attacks have some prevention techniques; Firstly, using a suitable cryptographic approach. The message sent between the drone and remote control is encrypted and not easily broken by the attacker. Another possible method is to have authentication to allow only authorized access to broadcasted information [101].

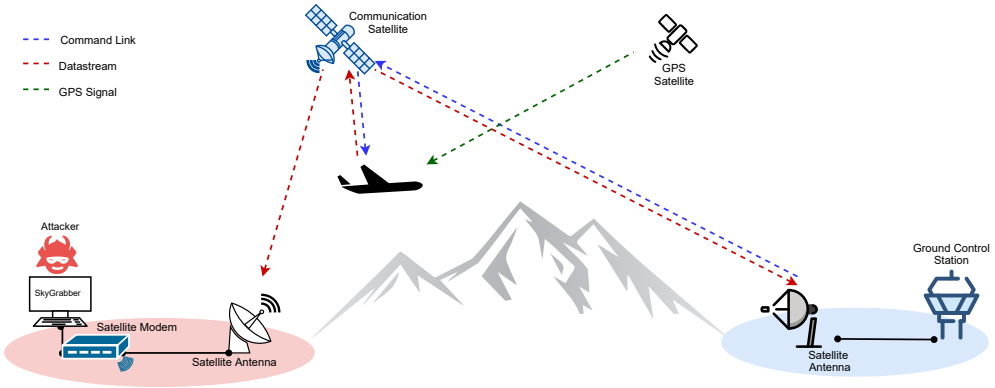


**Figure 4.** SkyGrabber software attack in Beyond Line Of Sight (BLOS) scenario.

### *4.5. RTL-SDR Attack*

Aviation sectors such as UAVs are vulnerable to SDR Attacks. The newest threat to aviation, RTL-SDR software, is installed on a system, and it has hardware used to connect to the tuned frequency and can listen to message exchanges between the devices. The common RTL-SDR frequency is 25 mhz–1750 mhz. It is used to receive and decode radio signals cheaply using a personal computer device. RTL-SDR explores the vulnerability of aviation. By the RTL-SDR, we can easily listen to all the information shared between the ground station (monitor or remote) and UAVs [102]. RTL-SDR is a software-hardware device installed in pc, and hardware is connected to a pc via USB or cable. The attacker tunes the frequency at which the drone flies

with the help of RTL-SDR. As tuning is comparatively easy in RTL-SDR because it knows the range of frequency the drone and other aviation devices are working. After tuning, the attacker eavesdrops on the information shared between the drone and GCS [103]. Hack-RF is a similar device used to work with radio frequency. The basic hack-RF 1 has a receiver and transmitter. The attacker can tune to an RF frequency by using it and can even transmit messages [104]. A hack-RF device can receive and transmit between 1 Hz and 6 GHz, which is better in terms of range than RTL-SDR.

As the connection shown in Figure 5, the pc, RTL-SDR dongle, and antenna are the leading equipment used in the link. Firstly the RTL-SDR dongle is connected to the pc; the SDR antenna is further connected to the SDR dongle. The SDR sharp software running on the system is simulated with the SDR dongle. These attacks violate the drone's confidentiality and integrity. When the communication between the drone and drone device control is encrypted, the attack is not easy to execute. A possible method to restrict this attack is to employ frequency hopping, employ message confidentiality, and user authentication.

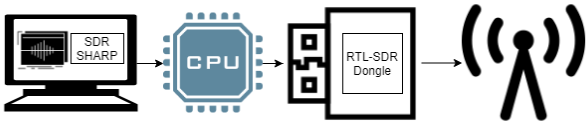


**Figure 5.** A basic RTL-SDR Configuration.

### *4.6. Deauth Attack*

Rather than disrupting a system by decrypting and intercepting network traffic, a Denial-of-Service (DoS) attack occurs when an attacker intentionally floods a system with excessive messages. The prevalence of DoS attacks can be attributed to their accessibility, as they do not require an in-depth understanding of network security or cryptography. A DoS attack can be executed without cracking passwords or gaining access to the targeted system. In the case of a Deauth attack, which is a type of DoS attack, a WLAN user becomes the target. The attacker sends deauthentication packets to a wireless access point (AP) with the intention of deceiving the AP into believing that the packets originated from a legitimate client or vice versa. Drone manufacturers develop mobile applications to control and configure drones, with these applications utilizing WiFi signals for drone operation. In a Deauth attack on a drone, WiFi is exploited to disconnect the drone, enabling further attacks in a chain. Tools such as the Aircrack-ng suite, ESP8266 Deauther software, and WiFi jammer hardware can be employed for such attacks. However, the effectiveness of this attack is limited when the packet transmission power is low or the access point lacks a public deauthentication code. Implementing WiFi encryption and following best password practices are significant preventive measures against such attacks.

### *4.7. ESC-PWM Signal Attack*

A drone's flight controller (FC) is comprised of sensors and an embedded processor. It is connected to the power distribution board, the radio unit, the Electronic Speed Controller (ESC), and the radio receiver. Each ESC unit is linked to an electric motor. Pulse Width Modulation (PWM) is employed to control the ESC units, which in turn control the electric motor that propels the drone. Many ESCs include built-in overheating and under-voltage protections that turn them off during extreme conditions. ESC behavior must be reliable under all circumstances. Few drones have firmware that is stored in volatile memory and requires uploading every time they are powered on. The performance of the flight controller can be impacted by changing this firmware. Once the firmware is uploaded, it is difficult to identify such changes [96]. As ESC firmware can be upgraded over a PWM servo cable, modifying the firmware to alter the functionality of the ESC once it receives a predefined PWM control signal could have disastrous consequences.

### 4.8. Sensor-Based Attack

UAVs are equipped with sensors for various applications to monitor specific tasks or functions in the air. In sensor-based attacks, the attacker manipulates or exploits the sensor data inputs and manages to manipulate or change such parameters to misguide the sensors; the most common example is inaccurate GPS data from sensors. Drones should use secure communication between the sensors and a proper authentication mechanism that can prevent access to any information from sensors. The misbehavior detection and intrusion detection mechanism can help to identify malicious data reading or compromised sensors [105]. Radar, infrared, and electro-optical sensors, among others, are all susceptible to manipulation. In electronic warfare, directed energy is employed to manipulate signals within the electromagnetic spectrum. This manipulation extends beyond radio and radar frequencies to encompass signals within the infrared, visible, and ultraviolet ranges [106].

### 4.9. Denial of Service Attack

Small drones are susceptible to denial-of-service attacks because the attacker can access the flight controller's settings and allow them to interfere with the UAV system. This means that someone with such access can modify flight control commands, including the shutdown command, which could be mistakenly triggered while the drone is in operation. Moreover, certain drones in this category have limited computational capabilities due to their small size. Consequently, bombarding these drones with random commands via the data link can result in unexpected behavior and potentially cause the drone to halt unexpectedly [16].

### 4.10. Man in the Middle (MITM) Attack

Using Man in the Middle attacks, adversaries with access to privileged networks may try to change network traffic in real time. This kind of attack enables the attacker to snoop on network traffic going to and/or coming from a specific device. The adversary has the ability to block, log, change, or inject traffic into the communication stream if a MITM attack is established. MITM attacks can be performed on a few drones (for example, XBee). Researchers have demonstrated how internal parameters (such as destination high and destination low) of the XBee chips can be remotely changed by the attacker. An attacker can eavesdrop on packets, block the operator, or even reroute packets.

## 5. Security and Privacy of UAVs

In this section, we go through the safety, security, and privacy concerns related to the use of drones. We specifically look at these systems' weaknesses to potential attacks that could lead to a malicious attack or drone crash, and we assess the security needs of such systems. The following specific privacy and security conditions must be satisfied for a secure safe flight operation:

- *Authorization*: Only authorized operators should be given access to the UAV system's resources, including the ground control station and the aircraft. During communication, an ongoing authentication process between the operator and the UAV is necessary.
- *Availability*: All components of the UAS should be assured to fulfill their respective activities under defined geographical and temporal conditions, ensuring that the system's availability is maintained throughout the operational period. It is also critical to manage the repair and update activities in a way that does not compromise the UAV system's availability when it is in use.
- *Integrity*: The UAS should be designed to verify that the telemetric data, GPS, and serial communications are authentic and have not been tampered with intentionally or inadvertently.

Table 4 presents state-of-the-art general drone security solutions and mechanisms used available in the literature. Furthermore, it analyzes security threats, targeted zones (Drones, Communication Networks, Base Stations, Ground Control Stations and Certification Authority), security considerations, parameters used, and open issues.

**Table 4.** The state-of-the-art general drone security solutions. Z1: Drones, Z2: Communication Networks, Z3: Base Stations, Z4: Ground Control Stations, Z5: Certification Authorities, Production and Manufacturing Units, and other involved devices, C- Confidentiality, I- integrity, A- Availability, T- Trust, NR- Non-Repudiation, BF: Brute Force, DA: DE-authentication Attacks, DL- Data Loss, DM- Data Modifications, WA: Waypoint Alterations, MIM- Man in Middle Attacks, WiA: WiFi attacks, PA: Physical attacks, SA: Spoofing Attacks, DoS: Denial of Services, JA: Jamming Attacks, RE: Resource Exhaustion, EA: Eavesdropping Attacks, RA: Replay Attacks, UA: Unauthorized Access, HA: Hardware-based Attacks, IA: Interception Attacks, BA: Behavioral Attacks.

| Authors | Security Solution | Used Mechanism | Security Threats | Targeted Zones | | | | | Security Considerations | | | | | Considered Parameters | Open Issues |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Z1 | Z2 | Z3 | Z4 | Z5 | C | I | A | NR | T | | |
| [107] | Drone privacy security | blockchain methodology | DL, DM, MIM | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ | Encryption, Time Stamp, Digital signature | Lack of Practical Adaptability and Not discussion respective factors |
| [108] | Random No. generator for cryptographic operations on the drone | Using sensor characteristics | WA, PS, SA, DM, DL | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | Dividing, shuffling, mixing and swap, power consumption, | Random number generation and cryptographic operation on a single will cause overhead, therefore the lightweight protocols are required. |
| [109] | Proposed countermeasure against the drone vulnerabilities | Validations, SDK authentication, and Encryptions | SA, DA, WiA, DoS | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | GPS Subframe Data, WPA security, MAC-Filtering and Hidden SSID | similar architecture and communication protocols need more security ad-ones |
| [110] | Drone embedded system security | SysML-Sec Methodology | MIM, PA, UA, DA | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Attack graphs, formal verification | The security requirements need verification and validations before secure design. |
| [111] | Countermeasures and Policies against drone attacks * | Vulnerabilities identifications | DoS, MIM, DA, JA, SA | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Multi-connection Prevention, telnet and FTP password, MAC Filtering | The adoption of multiple policies over a single framework are challenging. |
| [112] | Data Communication Security | Encryption of communication data and stored data | DL, DM, MIM | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Drone Security Modules | Drone security module is not suitable for encrypting large-scale streaming |

**Table 4.** *Cont.*

| Authors | Security Solution | Used Mechanism | Security Threats | Targeted Zones | | | | | Security Considerations | | | | | Considered Parameters | Open Issues |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Z1 | Z2 | Z3 | Z4 | Z5 | C | I | A | NR | T | | |
| [113] | Conceptual process model for Secure drone manufacturing processes | Dynamic security dedicated approach | HA, PA, GA, JA | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Vulnerability Analysis, Threat vector mapping | Drone specific manufacturing regulations needs more security policies to reduce the risk of threats. |
| [114] | Secure Authentication | ECC algorithm | DM, DL, MIM, RA, IA | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | Identity Authentication, Key consistency check | Limited power and computational capacity is an open challenge to adopt such authentication mechanisms. |
| [115] | Triaging Autonomous Drone Faults | AI-based assurance | DA, PA, SA, JA, WiA, BA | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | Assuring Autonomy, Inspection Autonomous Drones | Embedded System Anomalies, Sensor Anomalies, GPS, and Network anomalies are still open for considerations. |
| [116] | Authentication Security | Zero-Knowledge Authentication algorithm | BF, IA | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | Secret Key Generation | High distance between drone causes more authentication time than the usual. |
| [117] | Security Framework * | CPS threats | DA, DoS, BA, SA, WiA | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Traffic analysis | Each attack affects the traffic landscape in its way and creates unique patterns of behavior change, and it is not easy to monitor such patterns at run time. |
| [118] | Secure localization | Hierarchical aspect-oriented Petri nets | WA, DA, SA, JA | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | Context-aware security | Run-Time Petri net-based formulations required context and secure routings. There are certain open challenges with the run-time coordination with context. |

### *5.1. Network Security*

Multiple drones or swarm drones are used to complete the mission by creating a network and communicating with one another in terms of improving efficiency and productivity. However, there are various security vulnerabilities for both networking and control centers. Table 5 lays out the different attacks and security issues with respect to UAV networks. The challenge of multi-UAV communication requires the installation of a communication infrastructure. The table presents a comparative analysis of eavesdropping, DoS attack, forgery, replay, MITM, and protocol-based attacks. It includes solutions and limitations to network attacks.

**Table 5.** UAV Network Security issues and proposed solutions.

| Layer | Reference | Attacks/Threats | Proposed Solutions | Limitations |
|---|---|---|---|---|
| Network | | Eavesdropping | - datasets for predictive model training using K-means [119]<br>- framework for generating training data from wireless signals and creating features of testing data from wireless connections [119]<br>- Anti-Eavesdropping power control algorithm [120] | - Cryptography-based techniques require more processing and may result in high power usage. |
| Network | [121,122] | DoS Attacks | - Intrusion Detection System [123] | - GCS datalink affected<br>- False +ves and -ves with respect to anatomy-based IDS |
| Network | [37] | Forgery Attacks | - Creating a security architecture with multiple layers [25] | - In multi-UAVs, the network is more complex. |
| Network | [37] | Replay Attacks | - Implementing secure communication [124]<br>- Using authentication frameworks [22,121] | - DoS attack is triggred with multiple requests |
| Network | [125] | Man-in-the-Middle (MITM) Attack | - Using fingerprinting techniques for verifying the authenticity of UAVs [126]<br>- Encryption of control data for communication [127] | - Time-critical UAV systems face bandwidth limitations. |
| Transport | [128,129] | Protocol-based Attacks | - Using blockchain technique [130]<br>- Using IDS techniques for security<br>- framework for durability and trustworthiness that will enable the flight operation to be repaired even after attacks [131] | - The introduction of trade-offs between performance and security. |

### *5.2. Communication Security*

ADS-B Security

There are two forms of ADS-B: ADS-B in and out. Planes and helicopters are equipped with both types; however, limited UAVs are only equipped with ADS-B. The data transmitted by ADS-B is not secured because it broadcasts information to all adjacent planes. As a result, anyone can listen to the broadcast and even broadcast the data using low-cost technology [132]. Whenever one or more UAVs inside a region receive this broadcast, the initial flight will be disrupted, similar to GPS spoofing. As a result, there's a chance of a crash. Encryption and user identification have been offered as solutions to implement ADS-B security [133–135].

### *5.3. Privacy Issues of UAVs*

This segment covers unauthorized user parties receiving sensitive data monitored by UAVs, such as surveillance videos, pictures, and data collected. Additional types of sensitive information related to operating UAVs, including real-time GPS coordinates, speed, altitude, and battery status, should be treated as confidential and accessible solely to the operator. Ensuring the data privacy of flying UAVs is imperative for safeguarding the security of flight operations [136]. Insecure communications can be vulnerable to traffic analysis attacks, where adversaries can eavesdrop on the communication traffic to obtain sensitive details regarding the UAV's flight operations. The UAV's secrecy and privacy are affected by this form of passive attack. This segment covers unauthorized user parties receiving sensitive data monitored by UAVs, such as surveillance videos, pictures,

and data collected. Additional types of sensitive information related to operating UAVs, including real-time GPS coordinates, speed, altitude, and battery status, should be treated as confidential and accessible solely to the operator. Ensuring the data privacy of flying UAVs is imperative for safeguarding the security of flight operations []. Insecure communications can be vulnerable to traffic analysis attacks, where adversaries can eavesdrop on the communication traffic to obtain sensitive details regarding the UAV's flight operations. The UAV's secrecy and privacy are affected by this form of passive attack. This segment covers unauthorized user parties receiving sensitive data monitored by UAVs, such as surveillance videos, pictures, and data collected. Additional types of sensitive information related to operating UAVs, including real-time GPS coordinates, speed, altitude, and battery status, should be treated as confidential and accessible solely to the operator. Ensuring the data privacy of flying UAVs is imperative for safeguarding the security of flight operations []. Insecure communications can be vulnerable to traffic analysis attacks, where adversaries can eavesdrop on the communication traffic to obtain sensitive details regarding the UAV's flight operations. The UAV's secrecy and privacy are affected by this form of passive attack.

The attacker can launch a traffic monitoring attack on insecure connections by listening to the traffic and obtaining crucial flying operation details. The UAV's secrecy and privacy are affected by this form of passive attack. Digital data can be recovered using forensics techniques for data collection and analysis, even in protected conversations. Another sort of privacy attack that targets UAVs happens whenever an attacker gains unauthorized access to the UAS's vital components, such as sensors and storage (e.g., hijacking). The opponent in this scenario leaks flight data to the public, compromising flight operations.

## 6. Drone Forensics

The advancement of drone technology has expanded possibilities. Drones utilized for surveillance or payload delivery utilize a range of sensors and communication mechanisms to receive instructions from ground stations. The operational framework of a drone relies on an integrated system known as the Unmanned Aerial System (UAS), which encompasses various components such as computers, mobile devices, directional antennas, and towers, among others [4,137]. As a result, conducting a comprehensive investigation of the entire UAS is an integral part of drone digital forensics.

### *6.1. Drone Forensic Framework*

Digital forensics plays a crucial role in the successful prosecution of cybercriminals, encompassing a wide range of digital devices such as computer systems, network devices, mobile devices, and storage devices. To ensure an effective forensic investigation, there are several critical actions that must be followed. Therefore, it is essential to consider a number of important steps in order to perform a digital forensic investigation successfully. In this section, we propose a drone forensic framework, which outlines a step-by-step process for collecting evidence by an investigator.

Figure 6 illustrates the proposed framework for drone forensics. As shown in the figure, the framework consists of broadly four phases: collection, examination, analysis, and reporting. The framework is designed taking into consideration existing works in literature.

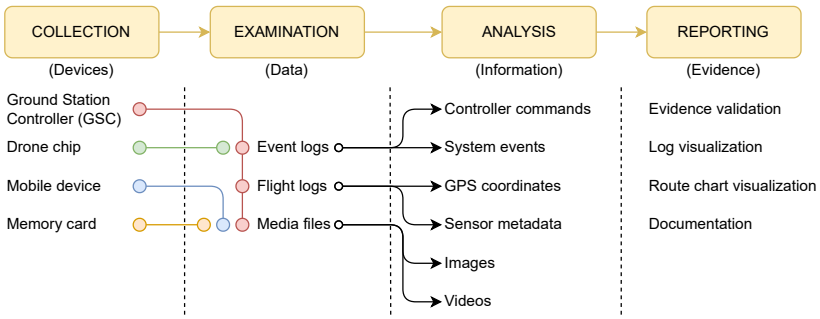


**Figure 6.** Forensic investigation framework for drones.

#### 6.1.1. Collection

In the forensic procedure, it is the initial stage. The devices or components that operate in the subsequent steps are identified and marked. Both pictures and notes of the scene are recorded. What device (or evidence) is present, where it is situated, how it is kept (in which format), and finally, safely isolating them are the primary determinants of the collection phase. Preventing tampering with digital evidence also involves prohibiting access to the collected devices. Seized devices such as memory cards and hard drives are isolated and forensically imaged to preserve and prevent data alteration of original media.

In terms of drone forensics, the relevant devices are the linked mobile device, memory card, drone chip, and Ground Station Controller (GSC). The accessible gadgets found and confiscated at the crime scene are identified and collected. Data stored in the device of interest is collected using different extraction methods. To be used for subsequent analysis, the data must be collected without affecting or affecting the source. A poor approach may make the evidence in court inadmissible. Thus, techniques for gathering evidence from a device should be reliable and forensically sound. The acquisition can be physical or logical. First, the logical extraction is performed by connecting the device to a forensic operating system. This provides quick access to the accessible data on the device's file system. Write blocks are employed wherever possible to maintain evidence integrity. After logical extraction, physical extraction is performed if required by employing JTAG, ISP, and Chip Off extractions.

Joint Test Action Group (JTAG), a manufacturing industry standard for testing printed circuit boards (PCBs), was created to test PCBs that had just come off an assembly line. Connecting the Test Access Ports (TAPs) on a PCB is a step in the procedure known as JTAG Forensics. The technique known as "chip-off forensics" entails removing a memory chip from a device and preparing it so that a chip reader may gather the raw data to produce a physical data dump. When used in forensics, In-System Programming (ISP) is the procedure of connecting to a flash memory chip with the goal of obtaining a device's complete memory contents. Before performing a chip-off, examiners first use a non-destructive technology such as JTAG or ISP.

#### 6.1.2. Examination

Once the devices have been identified and raw data extracted from them during the collection phase, the subsequent step is the examination phase. In this phase, the primary objective is to identify and extract data from the imaged devices. The raw data imaged or collected in the previous phase is forensically examined to identify logical files and logs. In terms of drone forensics, relevant logs and files are extracted from drones, mobile devices, GSC, and memory cards. Three major categories of data looked for during the examination phase are event logs, flight logs, and media files.

An event log is a chronologically ordered list of recorded events. Event logs are also a core component of OS. The recorded event in "Event Logs" originated from OS, network, hardware, or database query and is any significant action recognized by the OS. A general event log contains crucial information such as the date and time of the occurrence, the action of the event, severity, the process involved, and other relevant information such as hardware or logical addresses. They can be located in collected drone chips and the Ground Station Controller (GSC). Entries in event logs are generally due to warnings and errors by the camera, radio, battery, GCS failsafe, GPS, ADSB failsafe, and sensors [138].

During drone investigations, flight logs play a vital role as they contain extensive data in various formats. These logs primarily encompass crucial information such as the drone's location, speed, flight duration, gimbal angle, and camera shooting timing. Flight logs are typically found in the Ground Station Controller (GSC). Additionally, the examination of recorded media, such as photos and videos stored on the drone's memory card, holds significant importance in the investigative process. Popular drones store media-related files (.JPG, .MP4, and .DNG) in DCIM or MISC directory. Different media files can be located in GSC, drone chips, mobile devices, and memory cards.

For all relevant data items, the examiner needs to answer: What data were created?; How was the data created?; Who created the data?; Who edited the data?; and When was the data created?

#### 6.1.3. Analysis

The analysis phase involves correlating the examined data to extract information. Logs are analyzed to identify important events and metadata information. Event logs are useful in extracting controller commands and system events. They help in identifying the commands which were issued by the user during the flight to GSC. Flight logs are useful in extracting GPS coordinates and sensor metadata. Any hardware failures during flight can also be detected using them. Media files examined during the previous phase contain recorded videos and images. During the investigation, it is important to analyze the recorded media, such as photos and videos, stored on the drone's memory card. These media files contain valuable Exchangeable Image Format (EXIF) metadata, which includes GPS readings. To extract this EXIF data from the media files, Exiftool can be utilized as a reliable tool [139]. This becomes particularly useful when flight logs are unavailable, such as when the images were transferred to a separate storage device or if the drone suffered damage. Furthermore, in addition to providing the aforementioned information, examiners also assess how the obtained data is relevant to the case at hand. If required, the examiner reconstructs fragments of data and draws conclusions based on the evidence found. However, it might take numerous iterations of examination and correlation with other information.

#### 6.1.4. Reporting

During the reporting phase, the information gathered is consolidated and transformed into evidence, which is then presented in the form of a report. These reports play a crucial role in effectively communicating the information to all relevant parties. The report encompasses comprehensive details regarding the analyzed evidence, interpretation, and attribution. It includes a comprehensive account of the investigative processes employed, such as evidence collection methods, imaging procedures, the devices involved, the operating system, and the software utilized. It also involves the process of summarization and explanation of conclusions. These issues have critical importance for the report to be prepared. There are two important issues to consider while preparing the report: i. evidence validation, i.e., to demonstrate that evidence integrity is maintained during the investigation process; ii. the second one is to show that operations conducted are clear, transparent, and repeatable, putting aside exceptional situations.

With reference to drone forensics, the documentation must include log visualization and route chart visualization. Route charts are a visualization of GPS and flight data annotated on 3D or 2D maps. Tools such as "GeoPlayer", "GPS Visualizer", and "WebFlightPath" are tools helpful in generating route charts [140]. Table 6 presents a list of analyses of existing drone forensic tools, which can come in handy to the investigator. Event and flight logs often contain sensor and hardware information such as flight time, barometric altitude, and battery voltage. Log visualization tools are used to visualize them against flight duration.

### *6.2. Drone Forensics Artifacts*

Digital artifacts are digital entities with forensic value. The investigator, while performing drone forensics, collects data, information, or evidence of something that has occurred, such as logs, metadata, route chart, and many more. These artifacts help the investigator create a timeline of events and executions on a drone by a user.

The Ground Station Controller, Flight Control Board, and TCU (Transceiver Control Unit) constitute a potentially trustworthy form of evidence in terms of possible digital forensic artifacts. The ground station controlling unit can also be used to extract log and memory information. Data saved inside the memory, contents of various log files,

and electromagnetic wave data are all examples of digital forensic artifacts from drone equipment. Memory artifacts could come from the FCB. These elements include data from the aircraft's internal monitoring unit, flight record information, flight control information, and data from installed transmitters and sensors. Digital artifacts via respective transceivers and installed sensors, on the other hand, would provide additional verifiable data for the investigation [11,13,141].

**Table 6.** List of drone artifacts (E: Exif data; F: System files; G: Ground controller; L: Logs; M: Memory card; O: Observation).

| | Artifacts | Source | Description |
|---|---|---|---|
| **Files** | Images | M | Images captured |
| | Videos | M | Videos captured |
| | Text files | M | Config and log information |
| | DAT files | M | Encrypted logs |
| | Cache files | M | Temporary info of recent flight |
| | Config files | M | Drone configuration |
| | Binary files | M | Executables and system files |
| **Exif Data** | Timestamp | EL | Flight time info |
| | GPS data | EL | Geo location info |
| | Altitude | L | Drone height during flight |
| | Altitude reference | L | Altitude of home location |
| | Latitude Longitude | L | Geo location data |
| | Thumbnails | M | Media file info |
| **Log data** | Username | FM | user info |
| | Email address | M | username |
| | Drone serial number | OM | Unique id of drone |
| | Country code | F | Location info |
| | Aircraft model | FO | Maker info |
| | Manufacturer | OF | Developer info |
| | Firmware version | F | Firmware info |
| | Controller ID | OFM | GCS unique id |
| **PII** | Flight log data | L | Flight info |
| | Black box files | FM | Drone logs and damage status |
| | Flight air time | L | Duration of flight |
| | Sensor data | LFM | Different sensor logs |
| | Battery status | L | Battery consumption status |
| | Home location | GL | Initial flight location |
| | GPS Tracks | EL | Flight path identifiers |
| | Controller commands | GF | Commands sent during flight |
| | System events | FL | User events on drone |
| | Last connected time | FL | Recent user activity |
| **Sensor Logs** | GPS | LG | Location info |
| | Magnetometer | FL | Guides drone for magnetic field |
| | Accelerometer | L | Acceleration info |
| | Barometer | L | Atmospheric pressure info |
| | Altimeter | L | Altitude info |
| | Gyroscope | L | Drone stability |
| | Speedometer | L | Speed info |
| | Tilt sensors | L | Measure axis tilt |
| | Camera sensors | LM | For image capture |

In this section, we present a comprehensive analysis of forensic artifacts that an investigator looks for while performing drone forensics. The artifacts retrieved during

drone forensics are primarily categorized into EXIF data, files, log data, personal identifiable information, and sensor data. Few artifacts can be in multiple categories, and in some cases, an artifact can lead to generating other ones (e.g., media files store timestamps and geo-location information). Table 6 provides a list of drone artifacts and their classification. The source of the artifact can be EXIF data, system files, ground controller, memory card, or physical observation [8,43].

### *6.3. Drone Forensics Tools*

Tools are an important factor while performing digital investigation on the device and artifacts on the scene. Investigators are required to adhere to procedures for forensics and artifact retrieval. For example, locating Personal Identifiable Information (PII), recovering media files, analyzing GPS information, and visualizing drone route charts. As mentioned previously, forensic tools are a must in forensic examiners' toolkits. They required different stages of forensic investigation for drone chip-off extraction, mobile device forensics, memory card imaging, metadata extraction, logs, and flight data visualization.

In this section, we have performed a comprehensive analysis of tools popularly used during the forensic investigation of drones. They are classified based on their usage into categories: decoding, network, imaging, visualization, and miscellaneous purposes. Table 7 illustrates the compiled list. Decoding tools include the ones used to parse coded formats such as .csv, .dat, and log files. Network tools include the ones used for network traffic scanning, capture, and analysis. Imaging and analysis tools include the ones used for logical imaging, searching, acquiring, data viewing, analysis, and extraction. Visualization tools include the ones used for visualizing the analyzed data, such as flight path and telemetry data.

**Table 7.** Analysis of existing drone forensic tools (OS: Operating System, A: Android, L: Linux, M: MacOS, W: MS Windows, O: Online, Os: Open Source, Pr: Proprietary, Fw: Freeware).

| | Tools | Description | OS | Os | Pr | Fw | Papers |
|---|---|---|---|---|---|---|---|
| **Decoding** | DCode | Timestamps decoder | W | | | ✓ | [8] |
| | DatCon | Log Decoder for .dat files | MW | ✓ | | | [8,40,142–144] |
| | Phantomhelp | Convert .dat and .txt to CSV | O | | | ✓ | [40] |
| | CsvView | CSV file viewer | MW | ✓ | | | [40,141,144–146] |
| | DROP | DAT file parser | LW | ✓ | | | [11] |
| **Network** | Nmap | Port scanning tool | LMW | ✓ | | | [15,141,147] |
| | Aircrack-ng | Wi-Fi Network security tool. | LMW | ✓ | | | [147] |
| | Wireshark | Deep packets analyzer | LMW | ✓ | | | [144] |
| | Xplico | Network forensic analysis tool | L | ✓ | | | [144] |
| | Network Miner | Network sniffer and capturing tool | LMW | ✓ | | | [144] |
| **Imaging and Analysis** | dcfldd | dd + metadata to check integrity | L | | | ✓ | [144] |
| | Bitwalk | search binary files | L | ✓ | | | [8,142] |
| | UEFD 4PC | Mobile forensics framework | W | | ✓ | | [8,142] |
| | Exiftool (GUI) | Checks the exif data of files | LMWO | | | ✓ | [8,10,15,141,142,144–146] |
| | Autopsy | GUI version of Sleuth Kit | LMW | ✓ | | | [8,40,142,144] |
| | FTK Imager | Imaging tool and data viewer | LMW | ✓ | | | [146] |
| | Encase | Imaging and analysis tool | W | | ✓ | | [143] |
| | Magnet AXIOM | Acquire and analyze evidence | W | | ✓ | | [8,142] |
| | fsstat | Filesystem analysis | L | ✓ | | | [141,148] |
| | fsck.f2fs | Checks and correct f2fs FS | L | ✓ | | | [141] |
| | f2fs-tools | SSD and SD card analysis | L | ✓ | | | [141] |
| | XRY | Analyze and recover information | W | | ✓ | | [147] |
| | ExtractDJI | Extract and decompress .dat | MW | ✓ | | | [40] |
| | Oxygen Forensics | Information extraction | W | | ✓ | | [147] |
| **Miscellaneous** | Litchi | Log data conversion | A | ✓ | | | [145] |
| | HxD | Hexa decimal editor | W | | | ✓ | [8] |
| | 010 editor | File content analysis | LMW | | ✓ | | [10] |
| | DJI fly | Access to SkyPixel media | A | | | ✓ | [142] |
| | Open WRT | Embedded devices traffic analysis | L | ✓ | | | [142] |
| | Parben's E3 Universal | Data processing and analysis | MW | | ✓ | | [40] |
| | Kingo Rootkit | Android rooting | A | | | ✓ | [141,148] |
| | BlueStacks | Android emulator | WM | | | ✓ | [146] |
| | Winhex | Hex editor | W | | | ✓ | [10] |
| | MediaInfo | Media file analysis | LMWO | ✓ | | | [10] |
| | CyanogenMod OS | Custom rooted Android OS | A | ✓ | | | [141,148] |

**Table 7.** *Cont.*

| | Tools | Description | OS | Os | Pr | Fw | Papers |
|---|---|---|---|---|---|---|---|
| **Visualization** | Google Maps | Flight path with timestamp | ALMWO | | | ✓ | [145] |
| | Google Earth | Flight path with timestamp | ALMWO | | | ✓ | [8,10,15,144,145] |
| | GPS Visualizer | Geo data visualization | O | | | ✓ | [10] |
| | Dashware | Telementry data representation | W | | | ✓ | [144] |
| | ArcGIS PRO | 3D visualization | LMW | ✓ | | | [8] |
| | WebFlightPath | Flight log parser | LMW | | | ✓ | [10] |

### *6.4. Drone Forensic Datasets*

The information age has been ushered in by modern technology, which has made it simpler to create and store enormous data. Data generated and stored by a drone is vital during forensics. A dataset refers to a group of interconnected and distinct elements that possess varying interpretations depending on the situation, and it is employed for conducting experiments or analyses. The purpose of datasets is to assess or examine a particular process, such as evaluating a practitioner's performance in a training setting, assessing the capabilities of a tool or technique, or testing a hypothesis related to the functionality of the software or an application. A dataset may be used to analyze the situation and, more crucially, to aid in decision-making. A forensic dataset assists in the development and testing of forensic tools as well as investigator training prior to working on real-life scenarios. As a result, datasets and the applications that may be made with them are significant. In this section, we enlist various drone forensic datasets containing drone images acquired in different scenarios. The contents of these dataset ranges from logical, physical, and chip-off images. Moreover, some focus on RF signals acquired from different drone flights. Table 8 gives a comprehensive list of drone datasets available in the literature.

**Table 8.** Drone datasets available in the literature.

| Dataset | Remarks |
|---|---|
| CFReDS Drone Dataset [149] | Includes 82 drone images from 30 drone models. Forensic images of data storage areas, controller, connected mobile device, and computer. |
| Drone Detect [150] | Radio frequency dataset of DJI Mavic 2 Air S, DJI Mavic Pro, DJI Mavic Pro 2, DJI Inspire 2, DJI Mavic Mini, DJI Phantom 4, and the Parrot Disco. |
| SARD [151] | Search and Rescue Image dataset was created with the goal of identifying casualties and people in search and recovery operations in UAV photos and videos. Contains 1981 hand-tagged images retrieved from video frames in the collection. |
| Drone RF Signal [152] | Includes RF signals from several UAV remote controllers. There are 17 UAV radio controllers of eight multiple brands, each with 1000 RF signals lasting 0.25 milliseconds. |
| UAVs for payload delivery [153] | Dataset of payload delivery in a smart UAV delivery system. |
| Multi-Sensor Drone Detection [154] | UAVs included: a tiny version (Hubsan H107D+), a moderate drone (DJI Flame Wheel in quadcopter format), and a performance-grade model (DJI Flame Wheel in quadcopter configuration) (DJI Phantom 4 Pro). Includes 650 visible and infrared clips of UAVs, birds, aircraft, and choppers (365 IR and 285 visible). |
| UAV attack dataset [155] | The collection includes recordings from a normal flight and one in which the UAV is subjected to GPS spoofing and jamming. |
| DroneFace [156] | Face pictures acquired from a variety of angles and altitudes in an unrestricted atmosphere can be useful for future research into incorporating face detection and recognition methods into UAVs. |

**Table 8.** *Cont.*

| Dataset | Remarks |
| --- | --- |
| Drone Tracking [157] | Clips of a flying UAV being recorded using many commercial cameras and highly precise 3D UAV trajectory classification algorithm recorded by Fixposition's exact real-time RTK system. Ground truth time synchronization and ground truth camera positions are also included in several clips. |
| Amateur UAV Detection [158] | Non-drone, UAV-like "negative" entities are included in the dataset. Yolov2-tiny and Yolov3-voc versions were utilized with this dataset. Working with Yolo design and the darknet platform is usually recommended. |
| Phantom III drone imagery [159] | The imagery in this collection was captured using a Phantom III drone. A DJI FC300S visible light camera as well as a Senterra 1.2MP GS-0002 6.05 mm near-infrared camera placed on the UAV produced two sets of images. It gives you an image log with the GPS location of the collection points. |

## 7. Discussion and Directions for Future Works

Digital forensic professionals face challenges when conducting forensic investigations on Unmanned Aerial Vehicles (UAVs) due to the diverse range of digital components present in a typical UAV. This makes it challenging for forensic investigators to concentrate on a specific forensic tool that can retrieve all the necessary data for the investigation process.

In certain instances, acquiring an image file of the data from a UAV's airborne camera without compromising its integrity is difficult. In terms of forensic photography, numerous UAVs feature USB connectors that do not facilitate direct access to the internal disk.

Accessing flight data via onboard flight microcontrollers frequently demands special user authorization through the wireless controller, which is unlikely to be available to security agencies and forensic investigators. In addition, most flight data retrieved from the flight microcontroller is encrypted. As a result, the lack of a microcontroller complicates the forensic investigation process.

Software, hardware, and firmware for onboard UAVs have not yet been standardized, and they differ from one manufacturer to the other. There are currently no standard protocols for flight controllers; thus, there is no common format for flight data. Users can also boost the efficiency of a UAV by adding extra elements or changing it with Software Developer Kits given by many UAV manufacturers.

Accessibility to flight data via the internal flight controller chip frequently necessitates specific owner authorization via the wireless controller, which is unlikely to be available to law enforcement agencies and forensic experts. In addition, most flight data retrieved from the flight microchip is encrypted. As a result, the lack of a remote controller complicates forensic analysis.

UAVs rely significantly on a volatile memory, which means that the flight data recorded there would be lost if the battery is dead. Additionally, some sensor information can be designed to be transferred to a secure server inside a cloud infrastructure or to be shared on file-sharing or social websites.

It must be emphasized that although offering a way to do forensics, the majority of drone forensics research focuses on commercial drones that use proprietary software. As a result, their methodologies, or at least part of them, are difficult to standardize [160]. Due to developments in drone manufacturing, forensic frameworks and methods require regular updating. For reference, Table 9 lists acronyms used in the paper.

**Table 9.** Summary of drone-related notations.

| Notations | Full Name |
| --- | --- |
| ADS-B | Automatic Dependent Surveillance-Broadcast |
| BLOS | Beyond Line-Of-Sight |

**Table 9.** *Cont.*

| Notations | Full Name |
|---|---|
| EXIF | Exchangeable Image Format |
| FCB | Flight Control Board |
| GCS | Ground Control System |
| GSC | Ground Station Controller |
| GPS | Global Positioning System |
| JTAG | Joint Test Action Group |
| LOS | Line-Of-Sight |
| MITM | Man in the Middle |
| PII | Personal Identifiable Information |
| PMS | Power Management System |
| UAV | Unmanned Aerial Vehicle |

## 8. Conclusions

The skies are becoming crowded with flying objects as a result of the continued acceptance of UAVs in a variety of fields, from agriculture to shipping and from monitoring to rescue operations. UAVs' ability to provide unique services while saving time and money suggests that this trend will persist. Additionally, we have already seen their nefarious use in a number of physical and digital acts. Based on the aforementioned, it is evident that digital forensics investigations on drones will soon become the standard as a result of the proliferation of drones and the enemies' use of them. To conduct an investigation, insurance companies, law enforcement, security organizations, and private citizens will need to gather evidence from a drone. However, as already mentioned in this study, a drone differs significantly from conventional computer equipment. In actuality, a very complicated environment is created by its physical characteristics, mobility, and dual nature with regard to control.

We covered a thorough analysis of drone systems, subsystems, and networks, focusing on the threats they face and the consequences a cyber attack might have on their operations. A thorough categorization of known drone threats discovered by business and academia are also given. We further addressed security and privacy concerns and gave an overview of the attack surfaces and limitations of the domains. We provide the drone forensic framework's taxonomy and a thorough investigation. We have discussed the forensic approach to carry out the investigation process for drones and the framework for the same. In addition, the process of conducting a UAV forensic investigation is described, together with drone artifacts, forensic analysis tools, and benchmark datasets. The case studies are not included in the literature. Finally, we discussed the work that has been proposed in each area and indicated potential study directions.

**Author Contributions:** Conceptualization, V.S., G.C. and P.C.; methodology, V.S., G.C. and N.D.; validation, V.S., G.C. and N.D.; investigation, V.S., G.C. and N.D.; resources, G.C. and N.D.; Data curation, V.S., G.C. and P.C.; writing—original draft preparation, V.S., G.C., N.D. and P.C.; writing—review and editing, V.S., G.C. and N.D.; visualization, V.S., G.C. and P.C.; supervision, G.C., N.D. and V.S.; project administration, G.C. and N.D.; funding acquisition, G.C. and N.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work has been supported by project TRANSACT funded under H2020-EU.2.1.1.—INDUSTRIAL LEADERSHIP—Leadership in enabling and industrial technologies—Information and Communication Technologies (grant agreement ID: 101007260).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References


1. Elands, P.; de Kraker, J.; Laarakkers, J.; Olk, J.; Schonagen, J. *Technical Aspects Concerning the Safe and Secure Use of Drones*; TNO: Den Haag, The Netherlands, 2016.
2. Fu, C.H.; Tsao, M.W.; Chi, L.P.; Zhuang, Z.Y. On the dominant factors of civilian-use drones: A thorough study and analysis of cross-group opinions using a triple helix model (THM) with the analytic hierarchy process (AHP). *Drones* **2021**, *5*, 46. [CrossRef]
3. 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; pp. 1–6.
4. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D.; Alsewari, A.A. A comprehensive collection and analysis model for the drone forensics field. *Sensors* **2022**, *22*, 6486. [CrossRef]
5. Citroni, R.; Di Paolo, F.; Livreri, P. A novel energy harvester for powering small UAVs: Performance analysis, model validation and flight results. *Sensors* **2019**, *19*, 1771. [CrossRef]
6. Hartmann, K.; Steup, C. The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 4–7 June 2013; pp. 1–23.
7. GÜLATAŞ, İ.; BAKTIR, S. Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng.* **2018**, *14*, 32–53.
8. Salamh, F.E.; Mirza, M.M.; Karabiyik, U. UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics* **2021**, *10*, 733. [CrossRef]
9. 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]
10. Salamh, F.E.; Karabiyik, U.; Rogers, M.K. RPAS forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon H. *Sensors* **2019**, *19*, 3246. [CrossRef]
11. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digit. Investig.* **2017**, *22*, S3–S14. [CrossRef]
12. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
13. 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]
14. Nassi, B.; Bitton, R.; Masuoka, R.; Shabtai, A.; Elovici, Y. SoK: Security and privacy in the age of commercial drones. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 73–90.
15. 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]
16. Altawy, R.; Youssef, A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys. Syst.* **2016**, *1*, 1–25. [CrossRef]
17. Choudhary, G.; Sharma, V.; Gupta, T.; Kim, J.; You, I. Internet of Drones (IoD): Threats, vulnerability, and security perspectives. *arXiv* **2018**, arXiv:1808.00203.
18. Mei, N. An Approach to Unmanned Aircraft Systems Forensics Framework. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, 2019.
19. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
20. Nassi, B.; Shabtai, A.; Masuoka, R.; Elovici, Y. SoK-security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps. *arXiv* **2019**, arXiv:1903.05155.
21. Ghosh, T.; Rasheed, I.; Toorchi, N.; Hu, F. UAV Security Threats, Requirements and Solutions. In *UAV Swarm Networks*; CRC Press: Boca Raton, FL, USA, 2020; pp. 193–206.
22. Shafique, A.; Mehmood, A.; Elhadef, M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 46927–46948. [CrossRef]
23. 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. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
24. 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]
25. Hooper, M.; Tian, Y.; Zhou, R.; Cao, B.; Lauf, A.P.; Watkins, L.; Robinson, W.H.; Alexis, W. Securing commercial wifi-based uavs from common security attacks. In Proceedings of the MILCOM 2016-2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 1213–1218.
26. Strohmeier, M.; Lenders, V.; Martinovic, I. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 1066–1087. [CrossRef]
27. Park, S.; Kim, H.T.; Lee, S.; Joo, H.; Kim, H. Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access* **2021**, *9*, 42635–42659. [CrossRef]
28. Hosseinzadeh, M.; Sinopoli, B. Active attack detection and control in constrained cyber-physical systems under prevented actuation attack. In Proceedings of the 2021 American Control Conference (ACC), New Orleans, LA, USA, 25–28 May 2021; pp. 3242–3247.

29. Vedula, V.; Lama, P.; Boppana, R.V.; Trejo, L.A. On the detection of low-rate denial of service attacks at transport and application layers. *Electronics* **2021**, *10*, 2105. [CrossRef]
30. Chandramohan, D.; Vengattaraman, T.; Dhavachelvan, P. A secure data privacy preservation for on-demand cloud service. *J. King Saud Univ.-Eng. Sci.* **2017**, *29*, 144–150. [CrossRef]
31. Samland, F.; Fruth, J.; Hildebrandt, M.; Hoppe, T.; Dittmann, J.A.R. Drone: Security threat analysis and exemplary attack to track persons. *Intell. Robot. Comput. Vis. XXIX Algorithms Tech.* **2012**, *8301*, 158–172.
32. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. Detecting drones status via encrypted traffic analysis. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15–17 May 2019; pp. 67–72.
33. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. Picking a needle in a Haystack: Detecting drones via network traffic analysis. *arXiv* **2019**, arXiv:1901.03535.
34. Bisio, I.; Garibotto, C.; Lavagetto, F.; Sciarrone, A.; Zappatore, S. Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis. *IEEE Commun. Mag.* **2018**, *56*, 106–111. [CrossRef]
35. Munari, S.; Palazzi, C.E.; Quadrio, G.; Ronzani, D. Network traffic analysis of a small quadcopter. In Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, Niagara Falls, NY, USA, 23 June 2017; pp. 31–36.
36. Vanitha, N.; Ganapathi, P. Traffic analysis of UAV networks using enhanced deep feed forward neural networks (EDFFNN). In *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*; IGI Global: Hershey, PA, USA, 2020; pp. 219–244.
37. He, D.; Chan, S.; Guizani, M. Drone-assisted public safety networks: The security aspect. *IEEE Commun. Mag.* **2017**, *55*, 218–223. [CrossRef]
38. Čisar, P.; Pinter, R.; Čisar, S.M.; Gligorijević, M. Principles of Anti-Drone Defense. In Proceedings of the 2020 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Mariehamn, Finland, 23–25 September 2020; pp. 000019–000026.
39. 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]
40. 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; pp. 066–071.
41. Lan, J.K.W.; Lee, F.K.W. Drone Forensics: A Case Study on DJI Mavic Air 2. In Proceedings of the 2021 23rd International Conference on Advanced Communication Technology (ICACT), Pyeongchang-gun, Republic of Korea, 13–16 February 2022; pp. 291–296.
42. Atkinson, S.; Carr, G.; Shaw, C.; Zargari, S. Drone Forensics: The Impact and Challenges. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 65–124.
43. Viswanathan, S.; Baig, Z. Digital Forensics for Drones: A Study of Tools and Techniques. In *Applications and Techniques in Information Security, Proceedings of the 11th International Conference, ATIS 2020, Brisbane, QLD, Australia, 12–13 November 2020*; Springer: Singapore, 2020; pp. 29–41.
44. Barker, N.V. Development of a Drone-Mounted Wireless Attack Platform. Theses and Dissertations. 3224. 2020. Available online: https://scholar.afit.edu/etd/3224 (accessed on 10 June 2023).
45. Shin, J.M.; Kim, Y.S.; Ban, T.W.; Choi, S.; Kang, K.M.; Ryu, J.Y. Position tracking techniques using multiple receivers for anti-drone systems. *Sensors* **2021**, *21*, 35. [CrossRef]
46. Siddappaji, B.; Akhilesh, K. Role of cyber security in drone technology. In *Smart Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 169–178.
47. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Kim, D.I. Securing Data Sharing from the Sky: Integrating Blockchains into Drones in 5G and Beyond. *IEEE Netw.* **2021**, *35*, 78–85. [CrossRef]
48. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D. Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach. *IEEE Netw.* **2021**, *35*, 130–137. [CrossRef]
49. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A new secure data dissemination model in internet of drones. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
50. Kim, S.K.; Jang, E.T.; Lim, S.H.; Park, K.W. Reduction of Data Leakage Using Software Streaming. In *International Symposium on Mobile Internet Security*; Springer: Singapore, 2019; pp. 99–111.
51. Choudhary, G.; Sharma, V.; You, I. Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol. *Comput. Electr. Eng.* **2019**, *74*, 59–73. [CrossRef]
52. Sharma, V.; Choudhary, G.; Ko, Y.; You, I. Behavior and vulnerability assessment of drones-enabled industrial internet of things (iiot). *IEEE Access* **2018**, *6*, 43368–43383. [CrossRef]
53. Wazid, M.; Bera, B.; Das, A.K.; Garg, S.; Niyato, D.; Hossain, M.S. Secure Communication Framework for Blockchain-Based Internet of Drones-Enabled Aerial Computing Deployment. *IEEE Internet Things Mag.* **2021**, *4*, 120–126. [CrossRef]
54. Hamza, A.; Akram, U.; Samad, A.; Khosa, S.N.; Fatima, R.; Mushtaq, M.F. Unmaned Aerial Vehicles Threats and Defence Solutions. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6.
55. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F.; Kazmi, R. Drone Security: Issues and Challenges. *(IJACSA) Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 720–729. [CrossRef]

56. Jan, S.U.; Qayum, F.; Khan, H.U. Design and Analysis of Lightweight Authentication Protocol for Securing IoD. *IEEE Access* **2021**, *9*, 69287–69306. [CrossRef]
57. Nayyar, A.; Nguyen, B.L.; Nguyen, N.G. The internet of drone things (IoDT): Future envision of smart drones. In *First International Conference on Sustainable Technologies for Computational Intelligence, Proceedings of ICTSCI 2019*; Springer: Singapore, 2020; pp. 563–580.
58. Gope, P.; Sikdar, B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
59. Cheon, J.H.; Han, K.; Hong, S.M.; Kim, H.J.; Kim, J.; Kim, S.; Seo, H.; Shim, H.; Song, Y. Toward a secure drone system: Flying with real-time homomorphic authenticated encryption. *IEEE Access* **2018**, *6*, 24325–24339. [CrossRef]
60. Tanveer, M.; Zahid, A.H.; Ahmad, M.; Baz, A.; Alhakami, H. LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of drone environment. *IEEE Access* **2020**, *8*, 155645–155659. [CrossRef]
61. Khan, N.A.; Brohi, S.N.; Jhanjhi, N. UAV's applications, architecture, security issues and attack scenarios: A survey. In *Intelligent Computing and Innovation on Data Science*; Springer: Singapore, 2020; pp. 753–760.
62. Renyu, Z.; Kiat, S.C.; Kai, W.; Heng, Z. Spoofing attack of drone. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1239–1246.
63. Dahlman, E.; Lagrelius, K. A Game of Drones: Cyber Security in UAVs. 2019. Available online: http://www.diva-portal.org/smash/get/diva2:1350857/FULLTEXT01.pdf (accessed on 2 June 2023).
64. Kharchenko, V.; Torianyk, V. Cybersecurity of the internet of drones: Vulnerabilities analysis and imeca based assessment. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 24–27 May 2018; pp. 364–369.
65. Cho, G.; Cho, J.; Hyun, S.; Kim, H. SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles. *Appl. Sci.* **2020**, *10*, 3149. [CrossRef]
66. bin Mohammad Fadilah, M.S.; Balachandran, V.; Loh, P.; Chua, M. DRAT: A Drone Attack Tool for Vulnerability Assessment. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 16–18 March 2020; pp. 153–155.
67. Lenhart, M.; Spanghero, M.; Papadimitratos, P. Relay/replay attacks on GNSS signals. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 380–382.
68. Khan, A. Hacking the Drones. In *Open Web Application Security Project [Electronic Resource]* ; OWASP: Bel Air, MD, USA, 2016.
69. Restituyo, R.; Hayajneh, T. Vulnerabilities and attacks analysis for military and commercial iot drones. In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 8–10 November 2018; pp. 26–32.
70. Reed, T.; Geis, J.; Dietrich, S. *SkyNET: A 3G-Enabled Mobile Attack Drone and Stealth Botmaster*; WOOT: Carrollton, TX, USA, 2011; pp. 28–36.
71. Bunse, C.; Plotz, S. Security analysis of drone communication protocols. In *Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, 26–27 June 2018*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 96–107.
72. Hamamreh, J.M. Physical Layer Security Against Eavesdropping in the Internet of Drones (IoD) Based Communication Systems. Available online: http://acikerisim.antalya.edu.tr/handle/20.500.12566/894 (accessed on 10 June 2023).
73. Li, K.; Lu, N.; Zheng, J.; Zhang, P.; Ni, W.; Tovar, E. BloothAir: A Secure Aerial Relay System Using Bluetooth Connected Autonomous Drones. *ACM Trans. Cyber-Phys. Syst.* **2021**, *5*, 1–22. [CrossRef]
74. Dovgal, V.A.; Dovgal, D.V. Security Analysis of a Swarm of Drones Resisting Attacks by Intruders. Distance educational technologies. In Proceedings of the 5th International Scientific and Practical Conference, Yalta, Crimea, 22–25 September 2020; pp. 372–377.
75. Rani, C.; Modares, H.; Sriram, R.; Mikulski, D.; Lewis, F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. *J. Def. Model. Simul.* **2016**, *13*, 331–342. [CrossRef]
76. Fei, F.; Tu, Z.; Yu, R.; Kim, T.; Zhang, X.; Xu, D.; Deng, X. Cross-layer retrofitting of UAVs against cyber-physical attacks. In Proceedings of the 2018 IEEE International Conference on Robotics and Automation (ICRA), Brisbane, QLD, Australia, 21–25 May 2018; pp. 550–557.
77. Vasconcelos, G.; Miani, R.S.; Guizilini, V.C.; Souza, J.R. Evaluation of dos attacks on commercial wi-fi-based uavs. *Int. J. Commun. Netw. Inf. Secur.* **2019**, *11*, 212–223. [CrossRef]
78. Bonilla, C.A.T.; Parra, O.J.S.; Forero, J.H.D. Common security attacks on drones. *Int. J. Appl. Eng. Res.* **2018**, *13*, 4982–4988.
79. Lin, C.; He, D.; Kumar, N.; Choo, K.K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
80. Desnitsky, V.; Rudavin, N.; Kotenko, I. Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis management systems. In *International Symposium on Intelligent and Distributed Computing*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 323–332.
81. Eldosouky, A.; Ferdowsi, A.; Saad, W. Drones in distress: A game-theoretic countermeasure for protecting uavs against gps spoofing. *IEEE Internet Things J.* **2019**, *7*, 2840–2854. [CrossRef]

82. Arteaga, S.P.; Hernández, L.A.M.; Pérez, G.S.; Orozco, A.L.S.; Villalba, L.J.G. Analysis of the GPS spoofing vulnerability in the drone 3DR solo. *IEEE Access* **2019**, *7*, 51782–51789. [CrossRef]
83. 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]
84. 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; pp. 1–5.
85. Chapman, A. GPS Spoofing. *ECE Senior Capstone Project*. 2017 . Available online: https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/Red_Chapman.pdf (accessed on 1 June 2023).
86. Mead, J.; Bobda, C.; Whitaker, T.J. Defeating drone jamming with hardware sandboxing. In Proceedings of the 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, Taiwan, 19–20 December 2016; pp. 1–6.
87. Pirayesh, H.; Zeng, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *arXiv* **2021**, arXiv:2101.00292.
88. Li, Z.; Lu, Y.; Shi, Y.; Wang, Z.; Qiao, W.; Liu, Y. A dyna-q-based solution for uav networks against smart jamming attacks. *Symmetry* **2019**, *11*, 617. [CrossRef]
89. Leonardi, M.; Strohmeier, M.; Lenders, V. On Jamming Attacks in Crowdsourced Air Traffic Surveillance. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 44–54. [CrossRef]
90. Mead, J. *Prevention of Drone Jamming Using Hardware Sandboxing*; University of Arkansas: Fayetteville, AR, USA, 2016.
91. Wu, Q.; Mei, W.; Zhang, R. Safeguarding wireless network with UAVs: A physical layer security perspective. *IEEE Wirel. Commun.* **2019**, *26*, 12–18. [CrossRef]
92. Rojas Viloria, D.; Solano-Charris, E.L.; Muñoz-Villamizar, A.; Montoya-Torres, J.R. Unmanned aerial vehicles/drones in vehicle routing problems: A literature review. *Int. Trans. Oper. Res.* **2021**, *28*, 1626–1657. [CrossRef]
93. Dhein, G.; Zanetti, M.S.; de Araújo, O.C.B.; Cardoso, G., Jr. Minimizing dispersion in multiple drone routing. *Comput. Oper. Res.* **2019**, *109*, 28–42. [CrossRef]
94. Pu, C. Jamming-resilient multipath routing protocol for flying ad hoc networks. *IEEE Access* **2018**, *6*, 68472–68486. [CrossRef]
95. Salamh, F.E.; Karabiyik, U.; Rogers, M. A Constructive DIREST Security Threat Modeling for Drone as a Service. *J. Digit. Forensics Secur. Law* **2021**, *16*, 2. [CrossRef]
96. Petrovsky, O.; Prague, V. Attack on the drones. In Proceedings of the Virus Bulletin Conference, Prague, Czech Republic, 30 September–2 October 2015 ; p. 16.
97. Gregory, T.S.; Tse, Z.T.H.; Lewis, D. Drones: Balancing risk and potential. *Science* **2015**, *347*, 1323. [CrossRef]
98. Salamh, F.E.; Karabiyik, U.; Rogers, M.K.; Matson, E.T. Unmanned Aerial Vehicle Kill Chain: Purple Teaming Tactics. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 1081–1087.
99. Dangwal, A. 1st Evidence Of Russia-Operated Iranian Suicide Drone Emerges In Ukraine; Kiev Claims Downing Shahed-136 UAV, 2022. Available online: https://eurasiantimes.com/1st-evidence-of-russia-operated-iranian-drones-emerges-in-ukraine/ (accessed on 5 June 2023).
100. Wilson, R.L. Ethical issues with use of drone aircraft. In Proceedings of the IEEE 2014 International Symposium on Ethics in Engineering, Science, and Technology, Chicago, IL, USA, 23–24 May 2014; p. 56.
101. Vattapparamban, E.; Güvenç, İ.; Yurekli, A.İ.; 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; pp. 216–221.
102. Motlagh, N.H.; Taleb, T.; Arouk, O. Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE Internet Things J.* **2016**, *3*, 899–922. [CrossRef]
103. Goddemeier, N.; Daniel, K.; Wietfeld, C. Role-based connectivity management with realistic air-to-ground channels for cooperative UAVs. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 951–963. [CrossRef]
104. Bohagen, F.; Orten, P.; Oien, G.E. Design of optimal high-rank line-of-sight MIMO channels. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 1420–1425. [CrossRef]
105. Mitchell, R.; Chen, R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Trans. Syst. Man Cybern. Syst.* **2013**, *44*, 593–604. [CrossRef]
106. Son, Y.; Shin, H.; Kim, D.; Park, Y.; Noh, J.; Choi, K.; Choi, J.; Kim, Y. Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; pp. 881–896.
107. 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; pp. 162–167.
108. Cho, S.M.; Hong, E.; Seo, S.H. Random number generator using sensors for drone. *IEEE Access* **2020**, *8*, 30343–30354. [CrossRef]
109. Dey, V.; Pudi, V.; Chattopadhyay, A.; Elovici, Y. Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In Proceedings of the 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, India, 6–10 January 2018; pp. 398–403.

110. Li, L.W.; Lugou, F.; Apvrille, L. Security modeling for embedded system design. In *Graphical Models for Security, Proceedings of the 4th International Workshop, GraMSec 2017, Santa Barbara, CA, USA, 21 August 2017*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 99–106.
111. Pojsomphong, N.; Visoottiviseth, V.; Sawangphol, W.; Khurat, A.; Kashihara, S.; Fall, D. Investigation of Drone Vulnerability and its Countermeasure. In Proceedings of the 2020 IEEE 10th Symposium on Computer Applications Industrial Electronics (ISCAIE), Penang, Malaysia, 18–19 April 2020; pp. 251–255.
112. 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; pp. 1672–1674.
113. Thangavelu, S.; Janczewski, L.; Peko, G.; Sundaram, D. A Dynamic Security-dedicated Approach to Commercial Drone Vulnerabilities, Threat Vectors and Their Mitigation. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1054–1059.
114. Teng, L.; Jianfeng, M.; Pengbin, F.; Yue, M.; Xindi, M.; Jiawei, Z.; Gao, C.; Di, L. Lightweight security authentication mechanism towards uav networks. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA), Daegu, Republic of Korea, 10–13 October 2019; pp. 379–384.
115. Watkins, L.; Hamilton, D.; Kornegay, K.; Rubin, A. Triaging Autonomous Drone Faults By Simultaneously Assuring Autonomy and Security. In Proceedings of the 2021 55th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 24–26 March 2021; pp. 1–6.
116. Nisa, C.; Sudarsono, A.; Yuliana, M. Zero Knowledge Authentication Modification for Drone and Server Communication Security. *J. Mantik* **2021**, *5*, 1019–1029.
117. Mikhailova, V.D.; Shulika, M.G.; Basan, E.S.; Peskova, O.Y. Security architecture for UAV. In Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 13–14 May 2021; pp. 0431–0434.
118. Sharma, V.; Jayakody, D.K.; You, I.; Kumar, R.; Li, J. Secure and efficient context-aware localization of drones in urban scenarios. *IEEE Commun. Mag.* **2018**, *56*, 120–128. [CrossRef]
119. 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]
120. Zhang, G.; Wu, Q.; Cui, M.; Zhang, R. Securing UAV communications via trajectory optimization. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
121. 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 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), Recife, Brazil, 8–12 October 2016; pp. 127–132.
122. Muzzi, F.A.G.; de Mello Cardoso, P.R.; Pigatto, D.F.; Branco, K.R.L.J.C. Using Botnets to provide security for safety critical embedded systems-a case study focused on UAVs. *J. Phys. Conf. Ser.* **2015**, *633*, 012053. [CrossRef]
123. Choudhary, G.; Sharma, V.; You, I.; Yim, K.; Chen, R.; Cho, J.H. Intrusion detection systems for networked unmanned aerial vehicles: A survey. In Proceedings of the 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 560–565.
124. He, S.; Wu, Q.; Liu, J.; Hu, W.; Qin, B.; Li, Y.N. Secure communications in unmanned aerial vehicle network. In *Information Security Practice and Experience, Proceedings of the 13th International Conference, ISPEC 2017, Melbourne, VIC, Australia, 13–15 December 2017*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 601–620.
125. Rodday, N.M.; Schmidt, R.d.O.; Pras, A. Exploring security vulnerabilities of unmanned aerial vehicles. In Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016; pp. 993–994.
126. Alladi, T.; Bansal, G.; Chamola, V.; Guizani, M. SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15068–15077. [CrossRef]
127. Shoufan, A.; AlNoon, H.; Baek, J. Secure communication in civil drones. In *Information Systems Security and Privacy, Proceedings of the First International Conference, ICISSP 2015, Angers, France, 9–11 February 2015*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 177–195.
128. Koubâa, A.; Allouch, A.; Alajlan, M.; Javed, Y.; Belghith, A.; Khalgui, M. Micro air vehicle link (mavlink) in a nutshell: A survey. *IEEE Access* **2019**, *7*, 87658–87680. [CrossRef]
129. Khan, N.A.; Jhanjhi, N.Z.; Brohi, S.N.; Nayyar, A. Emerging use of UAV's: Secure communication protocol issues and challenges. In *Drones in Smart-Cities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 37–55.
130. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad. Hoc. Netw.* **2019**, *86*, 72–82. [CrossRef]
131. Highnam, K.; Angstadt, K.; Leach, K.; Weimer, W.; Paulos, A.; Hurley, P. An uncrewed aerial vehicle attack scenario and trustworthy repair architecture. In Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), Toulouse, France, 28 June–1 July 2016; pp. 222–225.
132. Choudhary, G.; Sihag, V.; Gupta, S.; Shandilya, S.K. Aviation attacks based on ILS and VOR vulnerabilities. *J. Surveill. Secur. Saf.* **2022**, *3*, 27–40. [CrossRef]
133. Yang, H.; Yao, M.; Xu, Z.; Liu, B. LHCSAS: A lightweight and highly-compatible solution for ADS-B security. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7.

134. Yang, H.; Zhou, Q.; Yao, M.; Lu, R.; Li, H.; Zhang, X. A practical and compatible cryptographic solution to ADS-B security. *IEEE Internet Things J.* **2018**, *6*, 3322–3334. [CrossRef]
135. Dave, G.; Choudhary, G.; Sihag, V.; You, I.; Choo, K.K.R. Cyber security challenges in aviation communication, navigation, and surveillance. *Comput. Secur.* **2022**, *112*, 102516. [CrossRef]
136. You, I.S.; Sharma, V.; Choudhary, G.; KO, Y.H. Method for Verifying Drone Included in Industrial Internet of Things System, by Using Petri-Net Modeling. U.S. Patent App. 17/255,497, 9 September 2021.
137. Baig, Z.; Khan, M.A.; Mohammad, N.; Brahim, G.B. Drone forensics and machine learning: Sustaining the investigation process. *Sustainability* **2022**, *14*, 4861. [CrossRef]
138. Diagnosing Problems Using Logs—Copter Documentation. Available online: https://ardupilot.org/copter/docs/common-diagnosing-problems-using-logs.html (accessed on 8 June 2023).
139. ExifTool by Phil Harvey. Available online: https://exiftool.org/ (accessed on 22 June 2023).
140. GeoPlayer. Available online: https://www.mathworks.com/help/driving/ref/geoplayer.html (accessed on 4 June 2023).
141. Azhar, M.; Barton, T.E.A.; Islam, T. Drone forensic analysis using open source tools. *J. Digit. Forensics Secur. Law* **2018**, *13*, 6. [CrossRef]
142. Stanković, M.; Mirza, M.M.; Karabiyik, U. UAV Forensics: DJI Mini 2 Case Study. *Drones* **2021**, *5*, 49. [CrossRef]
143. 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.
144. Llewellyn, M. *Dji Phantom 3-Drone Forensic Data Exploration*; Edith Cowan University: Perth, Australia, 2017.
145. Renduchintala, A.; Jahan, F.; Khanna, R.; Javaid, A.Y. A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Investig.* **2019**, *30*, 52–72. [CrossRef]
146. 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]
147. 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]
148. Barton, T.E.A.; Azhar, M. Open source forensics for a multi-platform drone system. In *Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, Prague, Czech Republic, 9–11 October 2017*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 83–96.
149. The CFReDS Project | Drone Data Set. Available online: https://cfreds-archive.nist.gov/ (accessed on 12 June 2023).
150. Swinney, C.J.; Woods, J.C. DroneDetect Dataset: A Radio Frequency dataset of Unmanned Aerial System (UAS) Signals for Machine Learning Detection & Classification. *IEEE Dataport* **2021**. [CrossRef]
151. Sambolek, S.; Ivasic-Kos, M. Search and Rescue Image Dataset for Person Detection—SARD. *IEEE Dataport* **2021**. [CrossRef]
152. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Drone Remote Controller RF Signal Dataset. *IEEE Dataport* **2020**. [CrossRef]
153. Vera-Amaro, R.; Burke, M.; Saad, W. Coordinated UAVs for payload delivery. *IEEE Dataport* **2021**. [CrossRef]
154. Svanström, F.; Alonso-Fernandez, F.; Englund, C. A dataset for multi-sensor drone detection. *Data Brief* **2021**, *39*, 107521. [CrossRef]
155. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. UAV Attack Dataset. *IEEE Dataport* **2020**. [CrossRef]
156. Hsu, H.J.; Chen, K.T. DroneFace: An open dataset for drone research. In Proceedings of the 8th ACM on Multimedia Systems Conference, Taipei, Taiwan, 20–23 June 2017; pp. 187–192.
157. Li, J.; Murray, J.; Ismaili, D.; Schindler, K.; Albl, C. Reconstruction of 3D ight trajectories from ad-hoc camera networks. In Proceedings of the 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Las Vegas, NV, USA, 24 October–24 January 2020; pp. 1621–1628.
158. Aksoy, M.; Orak, A.S.; Özkan, H.M.; Selimoğlu, B. Drone dataset: Amateur unmanned air vehicle detection. *Mendeley Data* **2019**, *4* . [CrossRef]
159. Jones, S.; DeClerck, F.; Fremier, A.; Ouedraogo, I. Phantom III drone imagery. *Harv. Dataverse* **2018**. [CrossRef]
160. Mantas, E.; Patsakis, C. Who watches the new watchmen? The challenges for drone digital forensics investigations. *Array* **2022**, *14*, 100135. [CrossRef]