drones

MDPI

Review

Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats

Ghulam E. Mustafa Abro [1,2,3,4,*], Saiful Azrin B. M. Zulkifli [1,3], Rana Javed Masood [5], Vijanth Sagayan Asirvadam [3] and Anis Laouiti [2]

1 Center for Automotive Research and Electric Mobility (CAREM), Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak, Malaysia
2 Samovar, Telecom SudParis, CNRS, Institut Polytechnique de Paris, 9 Rue Charles Fourier, 91011 Paris, France
3 Electrical and Electronic Engineering Department, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak, Malaysia
4 Condition Monitoring Systems (CMS) Lab, NCRA, Mehran University of Engineering and Technology (MUET), Jamshoro 67480, Sindh, Pakistan
5 Electronic Engineering Department, Usman Institute of Technology (U.I.T.), Karachi 75300, Sindh, Pakistan
* Correspondence: ghulam_20000150@utp.edu.my or mustafa.abro@ieee.org

Abstract: It has been observed that unmanned aerial vehicles (UAVs), also known as drones, have been used in a very different way over time. The advancements in key UAV areas include detection (including radio frequency and radar), classification (including micro, mini, close range, short range, medium range, medium-range endurance, low-altitude deep penetration, low-altitude long endurance, and medium-altitude long endurance), tracking (including lateral tracking, vertical tracking, moving aerial pan with moving target, and moving aerial tilt with moving target), and so forth. Even with all of these improvements and advantages, security and privacy can still be ensured by researching a number of key aspects of an unmanned aerial vehicle, such as through the jamming of the control signals of a UAV and redirecting them for any high-assault activity. This review article will examine the privacy issues related to drone standards and regulations. The manuscript will also provide a comprehensive answer to these limitations. In addition to updated information on current legislation and the many classes that can be used to establish communication between a ground control room and an unmanned aerial vehicle, this article provides a basic overview of unmanned aerial vehicles. After reading this review, readers will understand the shortcomings, the most recent advancements, and the strategies for addressing security issues, assaults, and limitations. The open research areas described in this manuscript can be utilized to create novel methods for strengthening the security and privacy of an unmanned aerial vehicle.

Keywords: unmanned aerial vehicle; advancement; classification; tracking and communication threats

check for updates

Citation: Abro, G.E.M.; Zulkifli, S.A.B.M.; Masood, R.J.; Asirvadam, V.S.; Laouiti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones* **2022**, *6*, 284. https://doi.org/10.3390/drones6100284

Academic Editor: Diego González-Aguilera

Received: 22 August 2022
Accepted: 11 September 2022
Published: 1 October 2022

1. Introduction

Technology has advanced, and as a result, the world of today has seen a number of ground-breaking developments. These outcomes have been demonstrated to be more trustworthy, approachable, and economical in our everyday lives. In addition, people now engage with one another in novel ways in their social circles. Additionally, unmanned aerial vehicles (UAVs) are employed for both commercial and private purposes in addition to being heavily utilized in military contexts. The market potential for medium-sized drones has been estimated by the China Unmanned Aerial Vehicle Industry (CUAVI) to reach CNY 80 billion by 2025 [1], whereas the Federal Aviation Administration (FAA) concluded that there are currently 3 million drones flying in the US sky and that number will increase by four times by the end of 2022 [2]. Drone use is increasing because of its value in a variety of jobs, including through the live broadcasting of events, aerial video shoots, the mobility to move packages from one location to another, and simple navigation as shown in Figure 1. These drones are commonly employed for transportation purposes due to their cheap maintenance requirements, ability to take-off and land vertically, ability to hover, and high degree of mobility. These drones are frequently outfitted with computer vision and internet of things (IoT)-like features, particularly for the swarming of drones [3,4], and they have proven to be an effective choice for surveillance and rescue-related missions [5]. There are, however, a few important elements that are connected to UAV security worries. This collection contains the story of the Iranian military jamming an American drone's control signals [6]; nonetheless, it is still difficult to create a security control module for UAVs that is completely foolproof. Additionally, the first drones were unmanned balloons loaded with explosives that were used to assault Venice in Italy [7]. Later, in 1915, the British troops employed these unmanned balloons for photographic-based surveillance during the renowned Battle of Neuve Chapelle [8]. During this time, cameras were not as advanced; hence, this strategy was suggested to improve visibility [8]. In order to find various terrorists, several of them were also used during the Afghan War [9,10]. Prior to today, these drones were usually utilized for military operations, but they are now also chosen for the majority of domestic applications, to the point that Amazon began using drones to carry packages in 2014 [11]. They have also been utilized in fields including agriculture [1,2], for checking building sites [3], and to greatly assist law enforcement organizations with emergency rescue operations. The United States of America started making pilotless aircrafts that could maneuver for roughly a kilometer in the early 1910s. During World War II, the US started developing advanced UAV programs, such as the N2C-2 drone and the OQ-2 communications plane [9], but these endeavors were both expensive and unreliable. In the late 1980s, the US started developing sophisticated drones, and they already have some top-notch micro unmanned aerial vehicles. Drones are also being used in the media business for aerial photography and filmmaking. Drone use is expanding quickly, and at the same time, security and privacy issues have grown more complicated and serious.

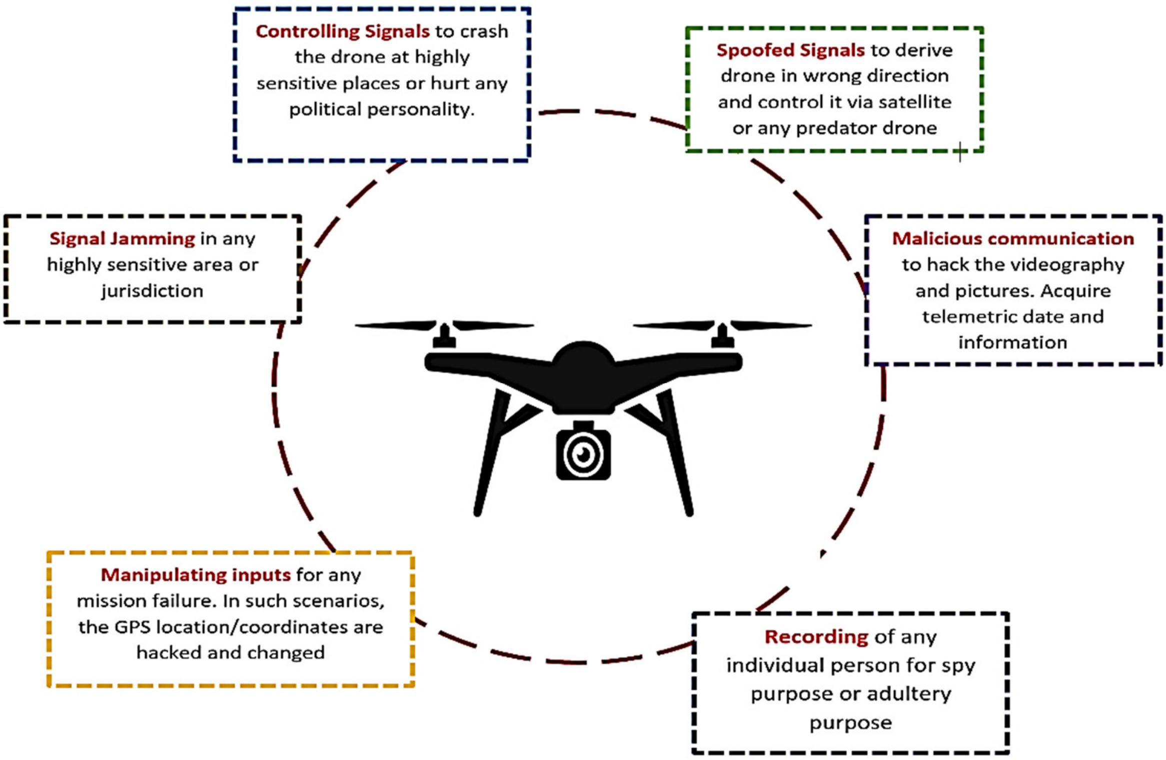

Figure 1. Security and privacy threats of UAVs.

The major goal of this review article is to give readers a comprehensive understanding of the new advancements that have led to the issues surrounding unmanned aerial vehicles (UAVs), including security threats, privacy concerns, and other limits that are important and cannot be disregarded. To give readers a thorough understanding of the subject, the manuscript has been organized into 10 sections. The major goal is to identify these issues and give all scholars access to a single resource that will allow them to fully understand the most recent trends and work to advance their field.

Section 2 contains the regulatory standards, whereas Section 3 describes the classification of various unmanned aerial vehicles (UAVs). Section 4 of the document discusses the structures and techniques of communication. In Section 5, it is specifically mentioned how and why drones are used. Section 6 covers the key security challenges and weaknesses, whereas Section 7 covers the present constraints. The most recent methods to address these restrictions are also discussed in Section 8, along with open research areas and recommendations in Section 9. The thorough conclusion to this work can be found last, but by no means least, in Section 10.

2. Study Related to Regulations

Many countries have been following the standard regulations to ensure the security and privacy implications of drones. Many of them have started to propose several step-by-step procedures to license their UAVs [12,13]. If these regulations are not followed, then unlicensed drones are taken under custody and proper legal action is taken against the pilot [12]. As per the media news broadcasted by the British Broadcasting Corporation (BBC), the CAA and FAA have declared some standard operating procedures (SOPs) to maneuver the UAVs at a low altitude [14], which are mentioned below:

- The users or operators of a registered UAV must carry the proof of license while operating the UAV.
- The maximum height at which the UAV can maneuver is 400 feet only.
- UAVs must be kept away from the airfields and, in case of necessity, one may acquire the written permission from relevant boards or authorities.
    - In the case of a UAV crash, legal action can be taken against any harmful actions or the damage that occurred from UAV failure.
    - UAVs with computer vision or camera surveillance are not allowed to maneuver within 50 m of people or any crowd.
    - UAVs will be summoned if they are not flown within the operator's line of sight.
    - UAVs will be summoned if they are flown at night without proper lighting.

The above standard rules and SOPs ensure the secure operation of drones.

It is also noted that with a dramatic rise in the drone industry, various countries have inducted their own rules as well [15]. Mainly, to operate a UAV, there are three fundamental components: the first is the ground control room (GCR); the second one is the communication method, for example, satellite, radio frequency, etc., as illustrated in Figure 2; and last, but certainly not the least, is the UAV itself. There are three different methods to communicate with a drone, i.e., satellite, radio signal, and internet, as shown in Figure 2 [15]. The essential license-exempted radio equipment, along with the frequencies, is mentioned in Table 1 [16].

The standard bandwidth through which a communication is established between a UAV and the ground control room (GCR) is mentioned in Table 1, whereas the other standards are still in progress for the safe operations of a UAV in any vicinity [17].

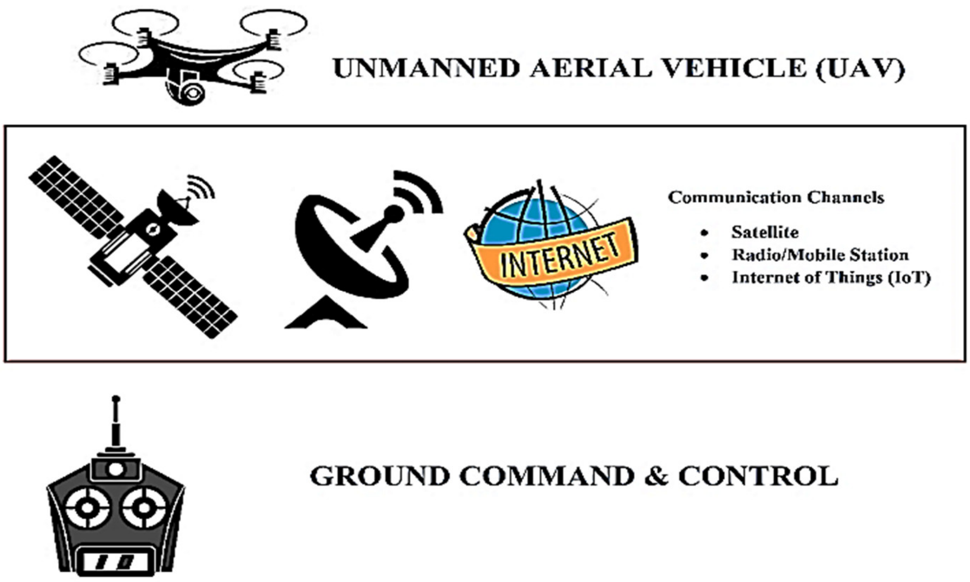

Figure 2. Communication channels mostly used to control UAVs.

Table 1. Frequencies through which GCR communicates with UAVs.

Sr. No.	Bandwidth	Description
1	2.4 KHz to 2483.500 MHz	The appropriate standard is EN 300 328, which is digital wideband data transmission equipment, and sometimes, the standard used is EN 300 440, which is general short-range devices. **Purpose:** Mostly used for short-range surveillance or short-range maneuvering missions.
2	5.47 KHz to 57250 MHz	Operational power is less or equal to 1 watt, whereas the power spectral density is less the 50mW/1 MHz frequency. The standard is EN 201 893, which is known as RLAN equipment. **Purpose:** Long stay in sky operations, used mainly for aerial photography.
3	5.725 KHz to 5875 MHz	Its operational power rating is less than 25 mW and standard is EN 300 440, which is general short-range devices. **Purpose:** Used for short-range surveillance with fast maneuvering and manipulating tasks.
4	5030 to 5091 MHz	This is the frequency used only for the International Telecommunication Union (ITU) and, therefore, cannot be used for communication with drones. **Purpose:** Used in such operations where data sharing is important with ground control room (GCR).

3. Classification of UAVs

One must understand the real sense of calling any drone a UAV. Not all drones can be classified as UAVs. A UAV can be controlled autonomously without a pilot and can be controlled remotely [17].

3.1. Classification of Drones

Drone is a very generic term and can refer to intelligent or autonomous vehicles such that there are unmanned aerial vehicles of different types. This can be hexarotors, quadrotors, multirotors or wing-based air vehicles. Mainly discussing the flying drones, they can be classified into three main categories as follows:

- Rotary-wing drones;
- Fixed-wing drones;
- Hybrid-wing drones;
- Flapping-wing drones.

The drones with a vertical take-off and landing (VTOL) feature and that can hover at a high rate are known as rotary-wing drones. The most common example is a quadrotor unmanned aerial vehicle that has four brushless DC motors. Drones with the capability to fly aggressively and glide even with heavy payloads are known as fixed-wing drones. They perform a horizontal take-off and landing (HTOL). Lastly, the drones that have both fixed and rotary wings are known as hybrid-wing drones. They are designed to have both features of rotary- and fixed-wing drones so that they can perform HTOL and VTOL along with high-rate hovering. Some of the robots are designed to exhibit the flying motion of a fly [18], and here they proposed a 5% more power-efficient wing by changing the wing stiffener pattern parametrically. An experimental aerodynamic analysis found that this could relate to increased wing stiffness, as well as indications of vortex generation during the flap cycle. The experiments reported an improved generated lift, allowing the DelFly to be outfitted with a yaw-rate gyro, pressure sensor, and microprocessor. These flapping-wings were later scaled to the micro level and are known as flapping-wing micro air vehicles (FWMAVs), due to inspiration taken from microscopic insects. These FWMAVs have the ability to perform activities in urban and interior environments. However, there are many hurdles for the successful flight of these vehicles that are replicating insect flight, including their design, manufacture, control, and propulsion [19,20].

3.2. Classification of UAVs Based on Ground Command and Control

It is already shown in Figure 2 that any UAV can be controlled remotely using a ground command and control mechanism, either by mobile phone, radio channel frequency, or the internet of things [21]. Therefore, these UAVs are classified based on their ability to fly over long distances without any intervention. These types are mentioned below as:

- Fully autonomous controlled UAVs: These are the UAVs that can perform different tasks without any intervention from human beings and are fully automated.
- Remotely operated UAVs: These UAVs are designed to execute the task as directed by a human being. Thus, they have a human as their main operator.
- Remotely pilot-controlled UAVs: Drones where all tasks and maneuvers are performed by the human-based remote control from the GCR.

The above-referred classification is summarized in Table 2 [22] along with the pros and cons of the UAVs.

Table 2. Classification of UAVs based on wing type and altitude.

Factors	Based on Wing Type			Based on Altitude	
	Fixed-Wing Type	**Rotary-Wing Type**	**Hybrid-Wing Type**	**Low Altitude Below 400 ft**	**High Altitude Above 400 ft**
Hovering	No	Yes	Yes	Yes	Yes
Small Size	No	Yes	Yes	Yes	No
Transport goods	Yes	Low weight	Yes	Yes	No
Battery time (in hour)	>1 h	1 h	>1 h	>1 h	>1 h
Maneuver speed	High Speed	Low speed	High speed	High Speed	High Speed
Flexible deployment of communication	No	No	No	Yes	No
Cost effective	Expensive	Cheap	Expensive	Cheap	Cheap
Endurance	High	Low	Medium	Low	High

In the above, the reader might be confused with the term of flexible deployment of communication. This states the proper coverage at which the drone can be controlled and stabilized for any sort of task. There are some research contributions that have classified the drones based on their altitude, as demonstrated in Figure 3 along with their examples [23,24].

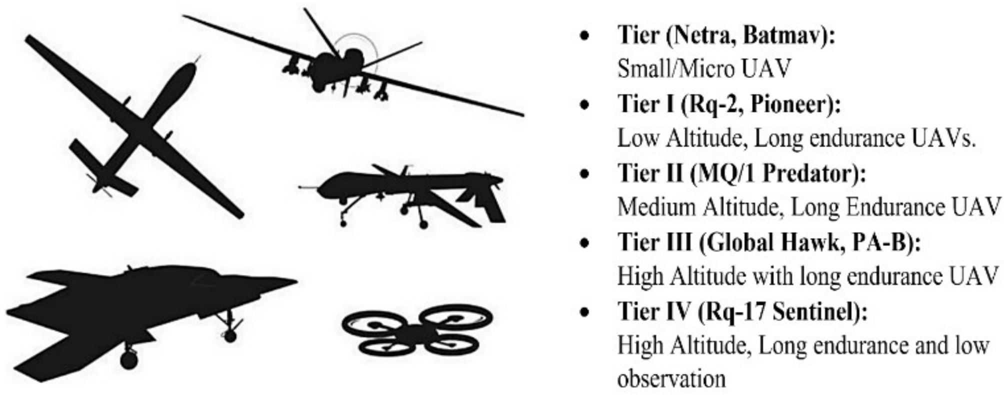

Figure 3. Classification of UAVs in terms of altitude.

4. Communication Methods and Architecture

Today, one may see the variety of several drones being opted for commercial and domestic use. This is because they are cost effective and are controlled remotely from anywhere. In military operations, mostly the micro or miniature-type UAVs are used, but there are some major limitations in terms of size and weight. In Figure 3, tier II and III UAVs have several requirements such as being able to deploy sensors, and having a global positioning system (GPS), communication module, and efficient batteries. This is illustrated further in Figure 4. Although there are huge advancements being noticed in the field of drones or unmanned aerial vehicles (UAVs), at the same time, there are some limitations associated with the software and hardware support.

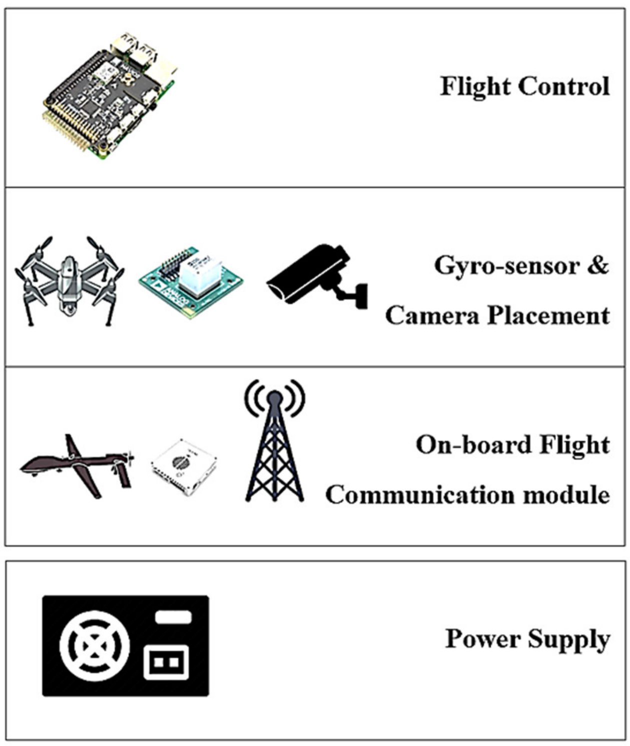

Figure 4. Components of an unmanned aerial vehicle.

The UAVs which are proposed for military operations have some advanced sensors which are not accessible to ordinary people. These sensors enable drones to carry additional payloads. After studying different UAVs, one may subdivide UAVs into their five major components as follows:

- Drone airframe;
- Onboard controller;
- Payload capability;
- Communication system;
- Efficient batteries.

Discussing the airframe of a UAV, one must consider aspects such as aerodynamics, a lightweight structure, and stability. These can be some of the constraints to designing the UAV airframe. Moreover, the onboard controller is the main thing that maneuvers the drone. Therefore, it must be equipped with all essential sensors such as the accelerometer, gyro sensor, pressure sensor, GPS, and camera. While designing the drone, one should consider the factor of payload variation. In this way, the drone may carry some nominal amount of weight from one place to another [25]. Another important component is the communication system where the drone requires some communication equipment such as a sitcom, modem, or radio channel-based equipment. This will ensure the communication and control between a UAV and the ground control room (GCR). Lastly, the UAV must have a reliable power source that can help it to fly for a specific time to fulfil the task. Mostly, lithium batteries are considered as the main power source for these UAVs [26].

Communication Methods

When one discusses the communication aspect of UAVs, one is directed toward several integral subcomponents such as the communication protocols, the network type, and the UAV model itself. This means that with the change of communication method, one may induct the number of components and this will change the architecture of the system [27]. Many researchers have suggested several topologies and designs. This has been illustrated in Figure 4 along with the altitude range. One may opt for a different communication module and protocol as per the mission and the nature of task type [28]. Moreover, with the advent of 5G networks, several constraints such as data rate, latency, and coverage have been resolved. This advancement in communication technology not only improved these areas, but also helps to improvise the positioning and control of drones in several critical rescue and surveillance missions; for that purpose, people have used advanced flight controls and multiple sensors as well, along with camera placement, controlled and communicated in different ways as per their altitude as shown in Figure 5. These technologies are summarized later in Table 3 [29].

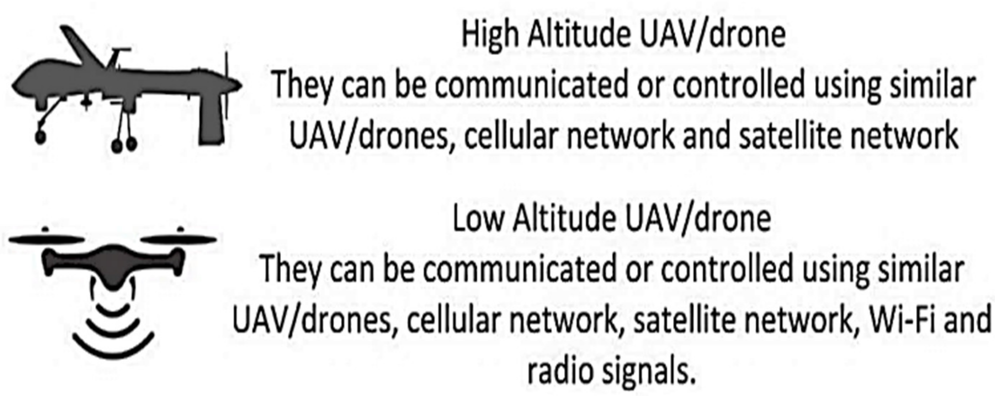

Figure 5. Communication methods for high- and low-altitude levels.

Table 3. Classification of UAVs based on communication channels.

Technique	Channel Width	Band	Bit Rate	Range	Latency	Mobility Support
Wi-Fi	20 MHz	2.4 GHz to 5.2 GHz	6–54 Mbps	100 m	10 ms	Low
GPS	2 MHz	1176 to 1576 MHz	50 bps	-	10 ms	Higher
UMTS	5 MHz	700 to 2600 MHz	2 Mbps	10 Km	20–70 ms	High
5G	2.16 GHz	57 to 64 GHz	Up to 4 Gbps	50 m	-	Ultra-High
LTE	20 MHz	700 to 2690 MHz	Up to 300 Mbps	30 Km	10 ms	Very High
LTE-A	Up to 100 MHz	450 MHz to 4.99 GHz	Up to 1 Gbps		-	Very High

Due to high security concerns, the modern UAVs are controlled using the line-of-sight method at a low altitude, whereas for high altitudes, researchers have given preference to GPS and the beyond-line-of-sight (BLoS) technique. Table 4 describes these techniques in brief [30].

Table 4. Communication based on satellite type.

Type of Communication	Elevation in Km	Number of Satellites	Satellite Life	Handoff Frequency	Doppler	Gateway Cost	Propagation Path Loss
Geostationary Earth orbit (GEO)	Up to 36,000	3, no polar coverage	15+	NA	Low	Very expensive	Highest
Medium Earth orbit (MEO)	5000–15,000	8–20 global	10–15	Low	Medium	Expensive	High
Low Earth orbit (LEO)	500–1500	40–800 global	3–7	High	High	Cheap	Least

Tables 3 and 4 are very important for the readers to understand the significance of the several channels based on different bandwidths and satellites, respectively. Discussing Table 3, it communicates the different wireless communication methods, but at the same time, it shares that the communication will have a latency rate as well. The table also shares the channel width, band interval, and most importantly, the mobility support for the readers to design their drones accordingly.

Discussing Table 4, it communicates the type of communication based on satellite type. This will help the reader to see the elevation in kilometers, number of satellites, satellite life, handoff frequency doppler gateway cost, and most importantly, propagation path loss of each satellite communication [31].

5. Utilization of UAVs in Different Domains

The potential of UAVs and drones has been proved already, and this domain covers every type of utilization from personal usage to military purpose, as illustrated in Figure 6.

These UAVs can be more efficient in performing several missions if they are equipped with a camera, smart sensors, and processors. With these essential components, one may see 100 plus applications of drones mentioned by several researchers, such as in [32].

Please note that Figure 6 shows the areas where UAVs are utilized mostly in general, whereas Figure 7 shows the benevolent usage where UAVs are commonly used. The term malevolent usage shows the areas and specific domains where people have witnessed an incremental increase in utilizing the drones over the last few decades. Factors such as diligence, cost, mobility in the areas where humans are unable to reach, payload options, and risk compel everyone to use drones/UAVs. Now, depending on the type of drone, they may be used in a better way. Commonly, it is seen that the design of drones is dependent on the type of mission they perform in the field [33]. Thus, categorizing them all with respect to their domains may lead to understanding their architecture in a better way. This has been illustrated in Figure 7, where every domain has its own privacy and security needs [33,34].

Figure 6. Utilization of drones in several domains.

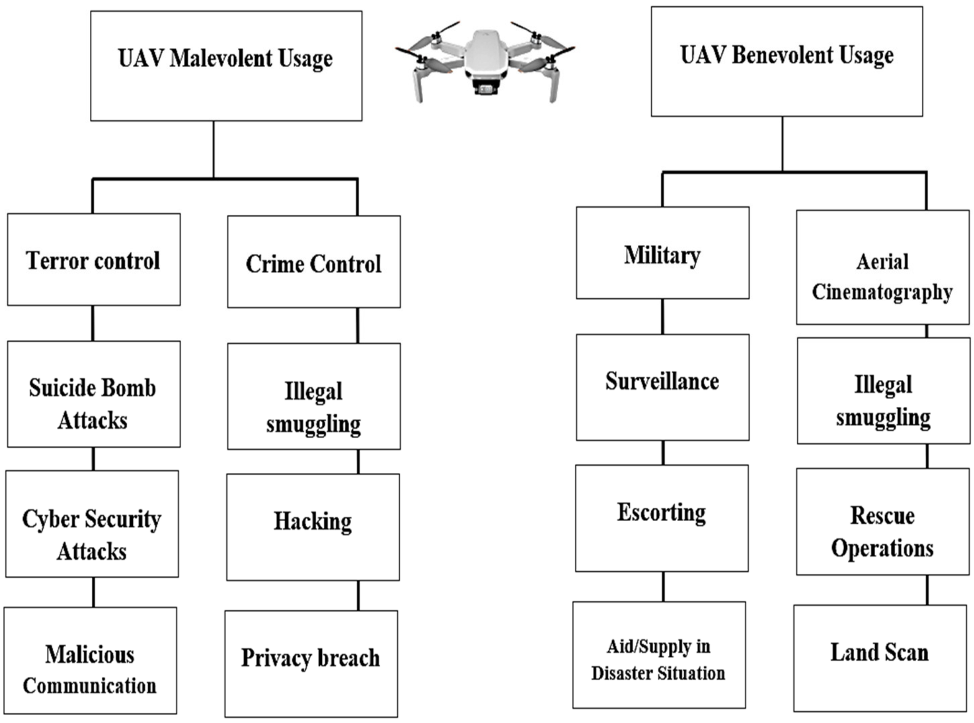

Figure 7. Malevolent and benevolent usages of a drone.

6. Security Threats Related to UAVs

UAVs offer several perks as the technology advances, but still, there are some constraints associated with privacy, security, and safety concerns [35,36]. Regularization and some important measures to license the utilization of drones is a very significant aspect. This limits unnecessary aerial photography. Most of the authorities in the world ensure this aspect and provide strict policies over uninformed aerial photography. If one discusses the network security point and the risk analysis, it is an admitted fact that the coverage is quite different as compared to any sort of wireless sensor network (WSN) or any mobile ad hoc networks (MANETs) [37]. The reason is because of the resource constraints, as UAV-related coverage is broader and wider than WSNs or MANETs.

The framework that sets the rules to operate drones in any vicinity is known as authentication, authorization, and accounting (AAA), which states several privileges to the controller of a drone to operate as per the mentioned administrative rights, whereas it also shares some of the rigid authentication procedures for drones to protect the control of a drone so that it may not be diverted to any other unknown entity. Moreover, in case of any uncertainty or illegal activity by drone, one may easily track down the operator. This is done to limit illegal surveillance, cyberattacks, and privacy threats. Thus, several mechatronic engineering solutions have been presented to overcome these malicious activities [38].

These drones are low cost and easily available in markets nowadays, and therefore, they are easy to use for any sort of criminal activity. Their ability to carry a wide range of external payloads make them more dangerous as it could lead to drones carrying any harmful chemical or explosive thing. Moreover, their ability to reach places where normal human beings cannot makes them more lethal because they can deliver anything without coming under anyone's notice [39]. It should be noted that security is not the only concern, but one may also see a safety concern if drones are flying over any populous place and, due to any number of faults, may crash, which can lead to several types of tragedies [40]. These sorts of incidents have been reported often. One of the examples is when a UAV faced a collision with British Airways BA727, which was a passenger aircraft in April 2016. After looking over these incidents and issues, one may ensure below the mentioned public safety measures:

- It is a high probability that a drone can be hacked or may deviate from its path due to heavy wind disturbance. Thus, there should be a reset option available which may turn the drone to a hovering condition only and help to gain the control back.
- There are certain areas where drones may face signal jammers and, later, can be controlled for a cyberattack. Thus, drones must have some sort of filter that may detect if there is any signal jammer nearby.

The third safety measure is related to its design, as most drones have open propellers as shown in Figure 8. In case of uncertainty, these propellers may go off and may harm anyone nearby; thus, the safety design as shown in Figure 9 is necessary to avoid any harm during a crash.

Figure 8. UAVs with open propellers.

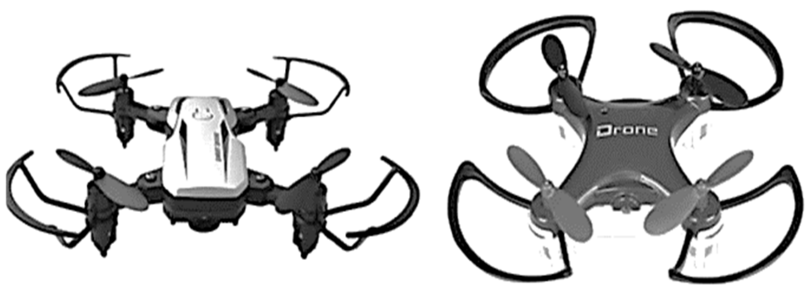

Figure 9. UAVs with closed and safety propellers.

Lastly, there are some serious privacy concerns as well. Since UAVs on the market can easily be procured with high-definition cameras, this may lead to the recording of any private property without permission. Due to this reason, Canadian Public Safety (CPS) stated that these UAVs are prohibited from flying over any property without mutually agreed permission [41].

7. Current Vulnerability Issues of UAVs

For these UAVs, unfortunately, there is neither a standardization of policies nor the availability of wireless security [42–44]. This leads to several threats, as highlighted in Table 5. There are researchers who have addressed different types of cyber-attacks associated with the several types of UAVs in a pre-controlled environment [45–50]. Such practical validations include the crashing of drones with many parallel requests and modifying the request packet known as the buffer-overflow attack, whereas some researchers went for the cache-poisoning approach that leads to the shutdown of communication between the drone and GCR. In all conditions, most attacks occur to target the operating system or, in other words, the microcontroller of the drone [51]. Since there are huge advancements in the technology, UAVs have a high probability of experiencing such attacks, as shown in Figure 9 [52–58]. From these attacks, the most common attack is GPS spoofing, such as signal jamming, de-authentication. and zero-day attacks.

Table 5. Summary of all current vulnerability issues in UAVs.

Vulnerability Type	Description
Malware issue	In various cases, it has been observed that these UAVs are generally connected and controlled via cell phone or any sort of remote control. These techniques are, thus far, not safe [43] and, therefore, the UAVs are easy to be hacked using a reverse-shell TCP payload that can be injected into UAV memory. Furthermore, this leads to installation of malware over UAVs automatically.
Spoofing	These are the issues related to the communication method, usually with serial port connections that are not encrypted properly [44]. Due to this spoofing issue, the information associated with GPS can be taken and altered.
Manipulation and other common concerns	The flying paths which UAVs must track are pre-programmed before; therefore, these paths can be altered [45], whereas the common issues are related to wind, overheating, or any predator bird harming the lightweight drone easily [46].
Physical design and control system constraints	There are various challenges with unmanned aerial vehicle control system design, such as the sluggish convergence rate, which prevents the drone from performing fast or aggressive maneuvers, and one may notice faults in the flight or divergence from the target trajectory [47,59,60]. This slow convergence rate and glitches are caused by the physical architecture of drones or the planned control system, which is primarily intended to stabilize the drone in uncertain conditions.
Sensorization issue	Since these UAVs depend on sensors, thus, it is also proved that the ultrasonic waves may attack the MEMS gyro sensors [47].
Wi-Fi constraints	Operating drones using a Wi-Fi facility may be risky. This is proved in [48] where the connection was disrupted with the help of software and changing the control of the UAV.
GPS issue	Automatic Dependent Surveillance–Broadcast depends on the GPS module, which is not encrypted sometimes and may lead to spoofing [49].
Firmware issue	The bugs available in the first prototype and first algorithm which come to the front after usage [50].
Sky Jack-based attacks	Sky Jack is one software used to conduct the attacks related to de-authentication of targets during control [51].
Controller issues	These issues are related to the operation control unit and may puzzle the controller by changing the live feed to some other video [52].

8. Current State-of-the-Art Solutions

The very first and significant thing to resolve the threats is to identify them first. Thus, Table 5 and Figure 10 classify these attacks. Moreover, there are several contributions which address these sorts of attacks along with the suitable measures [58]. In recent times, researchers have utilized machine learning approaches to demonstrate the intrusion detection system (IDS). Thus, machine learning (ML)-based IDS is one of the areas where researchers are still working to improve the results [59,60]. Blockchain is also among the most effective approaches for UAV/drone security and privacy [12]. This ML-based IDS technique is from the robust technique, and it is categorized into three kinds as mentioned below:

- Rule-based IDS;
- Signature-based IDS;
- Anomaly-based IDS.

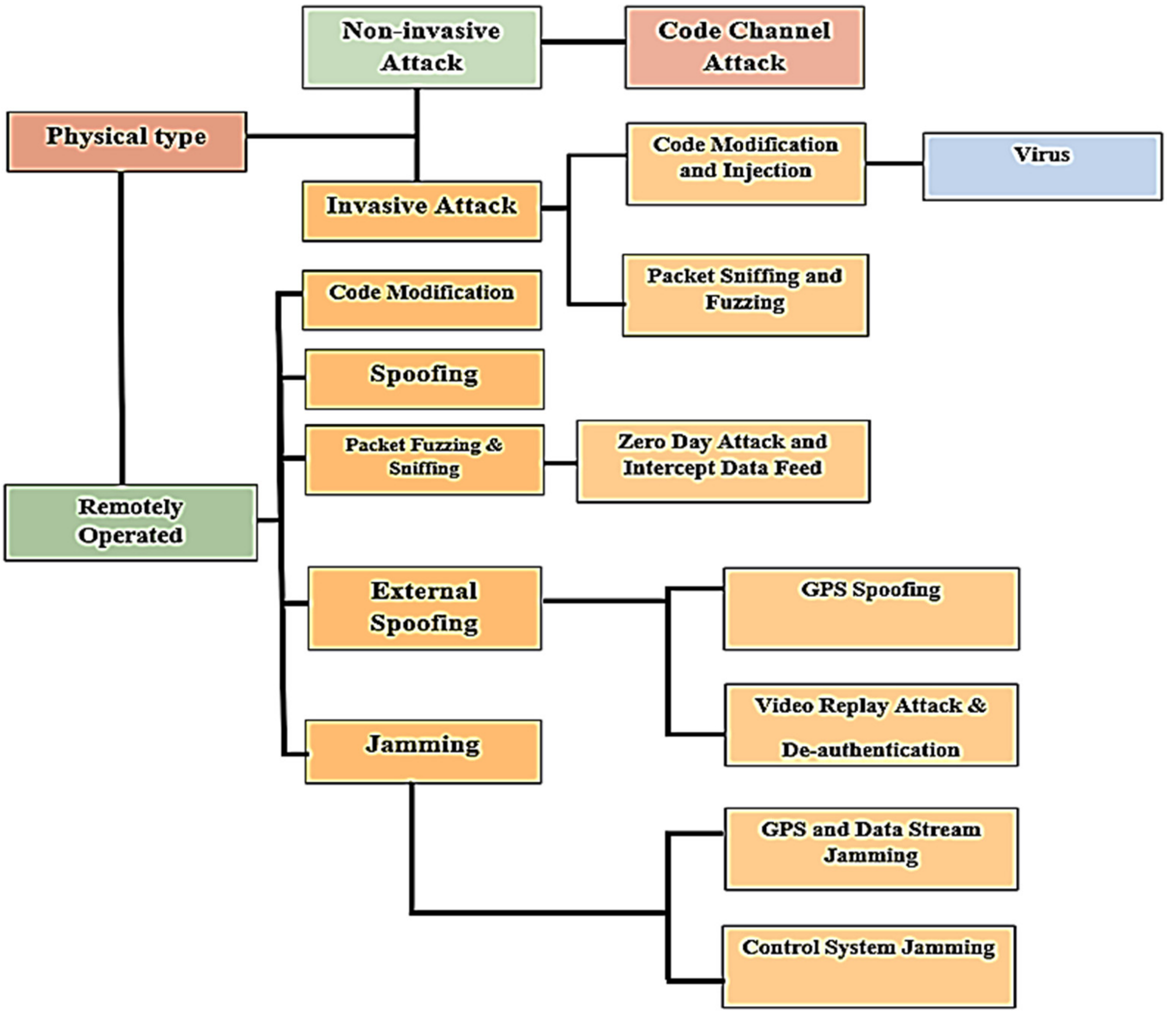

Figure 10. UAV attack vector with reported incidents.

Above are the major approaches for detecting threats that intrusion detection systems utilize to inform the operator in the ground control room (GCR). Rule-based threat detection is a new approach enabled by artificial intelligence (AI) [61]. In comparison to others, it is more reliant on technology and less on manual interaction. Signature-based detection works well for recognizing known threats. It uses a pre-programmed list of known threats and their indicators of compromise to operate (IOCs). An indicator of compromise (IOC) could be a distinctive behavior that typically precedes a malicious network attack, such as file hashes, malicious sites, known byte sequences, or even the content of email subject headings. A signature-based IDS examines network packets and compares them to a database of known IOCs or attack signatures to detect any suspicious behavior. Anomaly-based intrusion detection systems, on the other hand, can alert you to unusual behavior. An anomaly-based detection system uses machine learning to educate the detection system to recognize a normalized baseline rather than searching for known threats. All network activity is compared to the baseline, which represents how the system ordinarily performs. Rather than looking for known IOCs, anomaly-based IDS simply detects any unusual behavior to generate alarms.

To identify the false data injection attacks, one may use the rule-based approach. This is used to target the signal strength in between the UAV and ground control room (GCR) and can be useful for any sort of known attack, pattern, or technique only. Some research papers have proposed a signature-based IDS over drones [62] where they addressed bio-inspired cyberattacks associated with air-born networks. Last, but certainly not least, is the anomaly-based IDS scheme which is used against jamming attacks [62]. The only limitation of anomaly IDS is the huge resource requirement.

Similarly, there are some researchers who have suggested some algorithm schemes with forensic methods to address the advanced and complex attacks. They are complex and difficult to identify [63–69]. With the help of forensics, both perpetrator and method of attack can be identified. With the identification of the attack type, appropriate countermeasures can be implemented to avoid any future incident. As per the survey of [70], between 2014 and 2017 incidents among airplanes and drones amplified from 6 to 93, which makes it very important for the authorities to address security and privacy issues for UAVs. Due to an increase in cyberattacks on drones/UAVs, the government needs to introduce strict policies and standards to minimize these concerns. With the popularity of UAVs among the civilian population, attacks and the illegal use of UAVs will likely proliferate. Civilian or domestic UAV countermeasures are divided into physical and local countermeasures, which are already proposed but still can be improved.

There are several survey papers that address the latest integration of UAVs into cellular networks and discuss the inference issues [71], as well as those, like this paper, that address the significant concerns related to the standardization and regulation of drones and their privacy. In addition to this, the manuscript focuses on the issues related to addressing these limitations while communicating from the drone to the ground control room (GCR). Some of the researchers proposed survey papers also on the quantity and quality of service requirements and discussed network-relevant mission parameters [72], which is unlike this paper that discusses the safety, privacy, and adaptability features of drones.

9. Open Research Areas and Recommendations

After studying the previous sections, it is noted that there is still a need to improve some of the areas associated with unmanned aerial vehicles (UAVs). These areas are very significant and one may address these concerns to enhance the utilization of drones [73,74]. One of the important areas is path loss, where one needs to propose the channel model to hold on to the communication at higher carrier frequencies, and even in the presence of tall concrete buildings. This area is in regard to the latency in the communication, which should be less than 1 millisecond and remains as an area of concern [75,76].

In addition to these areas, one may work over the reliability aspect, where one may improve the drones with ultra-reliable communication so that even with the increase in UAVs in the sky, the communication can be performed easily. It is noted that these drones have not been operated in the sky for a long time, which is because of the battery life. Hence, battery optimization for drones is also one of the areas where researchers may engage themselves to increase the flight time.

Last, but certainly not least, is the amalgamation of artificial intelligence and computer vision algorithms in a drone to improve the mobility of the drone without any collision. This will protect the drone in terms of data logging and security [77–84]. This manuscript also suggests some of the recommendations that may improve the privacy and security aspects, such as the registration of drone licenses. This will ensure the authorities identify the specific drone that has created an inconvenience in the jurisdiction [85–91]. Moreover, there must be flying permits allotted after necessary training to limit the illegal utilization of drones in any activity.

Another recommendation is to educate the public about the legal and illegal usage of such autonomous unmanned aerial vehicles and the laws related to it so that if they witness anything around, they may easily report it. In any vicinity, there are some restricted zones; thus, the market drones must be operated based on a built-in map [92–95] as per the local regions. In this way, when any drone is forced to enter into any barred jurisdiction, it will automatically revert to the ground using the vertical take-off and landing (VTOL) mode. In terms of security tools, this paper proposes the machine learning-based IDS system [96–98] to improve the security infrastructure of UAVs, and lastly, there should be rigid multi-factor authentication methods that tackle the security threats easily.

There are several future recommendations to increase the standards for the security and privacy aspects of UAVs. These aspects are improved by proposing an approach which is based on a pairing certificate so that other strange entities may not easily connect or communicate with our UAV. Some of them are based on identification/authentication protocols [99–103]. To secure the drone more and make it less vulnerable, researchers have also used a symmetric searchable encryption method (SSE) [104] as well. Some researchers have proposed an internet of things (IoT) feature also for the same purpose [105–108]. In terms of identifying an unknown input observance, one may see an intelligent control algorithm that stabilizes the UAV in the presence of an unknown input [108–110] and devise it in trajectory and altitude levels to identify unknown system dynamics online by utilizing filtering manipulations that possess a concise structure, low calculation consumption, and asymptotic error convergence. In addition to this, the manuscript highlights the major domains and compares them with some of the latest review papers on UAVs for contrast. This is the significance of this article, which is seen in Table 6.

Table 6. Summary of all major domains along with reference list.

Area/Domain	[82]	[75,76]	[57]	[47]	[20,32]	[4]
Regulations and classification					•	
Communication methods				•	•	•
Applications	•	•		•		•
Security issues and solutions	•	•			•	
Physical and logical attacks					•	
Open research area				•	•	•
Recommendations			•	•	•	

One can observe from the above chart that the first column lists the issues that have already been covered in the paper, whereas the first row lists the number of review manuscripts that state or debate the same theme. After reading through Table 6, one can find this article to be more thorough in determining the future answer quickly and effectively. A black dot in the table above indicates the articles in which the topics were directly mentioned.

A statement in support of integrating UAVs with contemporary trends of communication and a control system is developed by evaluating various research contributions linked to UAVs and communication aspects to identify the limits [104,111]. To get over the limitations, more research is still needed to examine the subtopics below:

- There is a need to address the area of high-speed mobility, as there are huge chances to hack the communication links through the ground control room or with neighboring UAVs.

- In some of the integrated solutions, i.e., the space-air-ground network, one may see a frequent issue of synchronization, and thus, it is desirable to re-design some cooperation incentives for using cross-layered protocols with linked reliability. In this way, there will be less chances of any security attacks.
- One more aspect is to recommend a lightweight mechanism for UAVs to prevent attacks, such as eavesdropping, a man-in-the-middle attack [112,113], and so on. There are a number of artificial intelligence solutions which are recommended in [28] for addressing the security in cellular network-based controlled UAVs for delivering packages.
- Integrating UAVs with the IoT can result in endurance and reliability, but at the same time, it consumes the maximum battery capacity which is generally small; thus, this may lead UAVs toward possible collisions and can be a high-risk threat.
- Lastly, proposing a big data deep reinforcement learning approach to enable the dynamic arrangement of networking, caching, and computing resources for improving the performance of UAVs with secure operations in smart cities.

Thus, with all the above recommendations and in contrast to these topics, our manuscript provides a detailed direction for future work.

10. Conclusions

The use of UAVs has increased dramatically, ushering in an era of autonomous systems and vehicles. These drones are quite important because they have many benefits for both civil and military concerns. However, with this rise in usage, severe privacy and security concerns are also evident. The most frequent reason why these drones are chosen in any sneaky assault is because they are readily available and inexpensive to obtain.

There have been numerous scientific contributions that have already addressed the countermeasures to these worries; however, there are still some areas that have not been addressed and can, therefore, still be exploited for any negative purposes, such as privacy and security issues. In this current, technological age, these two challenges cannot be disregarded. As a result, this review paper offers a thorough examination of these two pressing issues by providing a quick summary of the causes of each worry, as well as potential solutions. The existing solutions and a number of recommendations are presented in this study, which claims that the UAV drones can be enhanced if proper data integration, authentication, and accessibility factors are treated seriously.

Author Contributions: Conceptualization, G.E.M.A., A.L., R.J.M., V.S.A. and S.A.B.M.Z.; methodology, A.L.; software, G.E.M.A. and A.L.; validation, V.S.A., R.J.M. and S.A.B.M.Z.; formal analysis, A.L.; investigation, V.S.A. and A.L.; resources, S.A.B.M.Z. and G.E.M.A.; data curation, S.A.B.M.Z., V.S.A. and A.L.; writing—original draft preparation, G.E.M.A.; writing—review and editing, G.E.M.A. and S.A.B.M.Z.; visualization, V.S.A. and S.A.B.M.Z.; supervision, A.L., S.A.B.M.Z., R.J.M. and V.S.A.; project administration, G.E.M.A.; funding acquisition, S.A.B.M.Z. and G.E.M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The article processing charges were financed by the Research Management Center, Universiti Teknologi PETRONAS, Malaysia, under the Research Fund, which was supported by Yayasan Universiti Teknologi Petronas (YUTP), award number 015LC0-316.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to express their gratitude to the Centre of Graduate Studies (CGS), Universiti Teknologi, PETRONAS, Malaysia, and the Erasmus+ Program for giving them the opportunity to study abroad as exchange students at Telecom SudParis, France and conduct this research using the cutting-edge resources of that country's university. Finally, I would like to express my gratitude to the Department of Electrical and Electronic Engineering for offering me a position to pursue PhD studies through YUTP Funding, grant number 015CL0-316.

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

References

1. Bombe, M.K. Unmanned Aerial Vehicle (UAV) Market Worth $21.8 billion by 2027- Pre and Post COVID-19 Market Analysis Report by Meticulous Research. 11 June 2020. Available online: https://www.meticulousresearch.com/download-sample-report/cp_id=5086 (accessed on 18 August 2022).
2. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Gadekallu, T.R.; Srivastava, G. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Comput. Networks* **2021**, *187*, 107819. [CrossRef]
3. Israr, A.; Abro, G.E.M.; Sadiq Ali Khan, M.; Farhan, M.; Zulkifli, B.M.; ul Azrin, S. Internet of things (IoT)-Enabled unmanned aerial vehicles for the inspection of construction sites: A vision and future directions. *Math. Problems Eng.* **2021**. [CrossRef]
4. Chen, R.; Yang, B.; Zhang, W. Distributed and Collaborative Localization for Swarming UAVs. *IEEE Internet Things J.* **2020**, *8*, 5062–5074. [CrossRef]
5. Hayat, S.; Yanmaz, E.; Muzaffar, R. Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2624–2661. [CrossRef]
6. Chan, K.W.; Nirmal, U.; Cheaw, W.G. Progress on drone technology and their applications: A comprehensive review. *AIP Conf. Proc.* **2018**, *2030*, 020308. [CrossRef]
7. Hartmann, K.S.C. The vulnerability of UAVs to cyber, in Cyber Conflict (CyCon). In Proceedings of the 2013 5th International Conference, Tallinn, Estonia, 4–7 June 2013.
8. Bowden, M. How the Predator Drone Changed the Character of War, Smithsonian Magazine. November 2013. Available online: https://www.smithsonianmag.com/history/how-the-predatordrone-changed-the-character-of-war-3794671/ (accessed on 18 August 2022).
9. Ekramul, D. First Successful Air-Raid in History. 22 August 2019. Available online: https://www.daily-bangladesh.com/english/First-successful-Air-raid-in-history/27424 (accessed on 18 August 2022).
10. O'Donnell, S. Consortiq. Available online: https://consortiq.com/short-history-unmanned-aerialvehicles-uavs/ (accessed on 18 August 2022).
11. Berg, T.R. Air Space Mag. 10 January 2020. Available online: https://www.airspacemag.com/daily-planet/first-map-compiled-aerial-photographs-180973929/ (accessed on 18 August 2022).
12. Abdullah, Q.A. Introduction to the Unmanned Aircraft Systems. Available online: https://www.eeducation.psu.edu/geog892/node/643 (accessed on 18 August 2022).
13. Miah, A. *Drones: The Brilliant, the Bad and the Beautiful*; Emerald Group Publishing: Bently, UK, 2020. [CrossRef]
14. Ali, B.S.; Saji, S.; Su, M.T. An assessment of frameworks for heterogeneous aircraft operations in low-altitude airspace. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100528. [CrossRef]
15. Wright, S. Ethical and safety implications of the growing use of civilian drone. UK Parliam. *Website Sci. Technol. Commit.* **2019**.
16. Coach, U. Master List of Drone Laws (Organized by State & Country). Available online: https://uavcoach.com/drone-laws/ (accessed on 18 August 2022).
17. Aljehani, M.; Inoue, M.; Watanbe, A.; Yokemura, T.; Ogyu, F.; Iida, H. UAV communication system integrated into network traversal with mobility. *SN Appl. Sci.* **2020**, *2*, 2749. [CrossRef]
18. de Croon, G.C.H.E.; Groen, M.A.; De Wagter, C.; Remes, B.; Ruijsink, R.; van Oudheusden, B.W. Design, aerodynamics and autonomy of the DelFly. *Bioinspir. Biomim.* **2012**, *7*, 025003. [CrossRef]
19. Cheaw, B.H.; Ho, H.W.; Abu Bakar, E. Wing Design, Fabrication, and Analysis for an X-Wing Flapping-Wing Micro Air Vehicle. *Drones* **2019**, *3*, 65. [CrossRef]
20. Teoh, Z.E.; Fuller, S.B.; Chirarattananon, P.; Prez-Arancibia, N.O.; Greenberg, J.D.; Wood, R.J. A hovering flapping-wing microrobot with altitude control and passive upright stability. In Proceedings of the 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, Vilamoura-Algarve, Portugal, 7–12 October 2012; pp. 3209–3216. [CrossRef]
21. Professionals, Drones and Remotely Piloted Aircraft (UAS/RPAS)-Frequencies and Radio Licenses, Traficom. 17 July 2021. Available online: https://www.traficom.fi/en/transport/aviation/drones-and-remotely-piloted-aircraft-uasrpasfrequencies-and-radio-licences (accessed on 18 August 2022).
22. Carnahan, ISO/TC 20/SC 16 Unmanned Aircraft Systems. 2014. Available online: https://www.iso.org/committee/5336224.html (accessed on 18 August 2022).
23. Irizarry, M.J.; Gheisari, B. Walker, Usability Assessment of Drone Technology as Safety Inspection Tools. *Electron. J. Inf. Technol. Constr.* **2012**, *17*, 194–212.
24. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.-H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tut.* **2019**, *21*, 2334–2360. [CrossRef]
25. Lowbridge, C. Are Drones Dangerous or Harmless Fun? *BBC News*. 5 October 2015. Available online: https://www.bbc.com/news/uk-england-34269585 (accessed on 18 August 2022).
26. Federal Aviation Authorities, Recreational Flyers & Modeler Community-Based Organizations. 18 February 2020. Available online: https://www.faa.gov/uas/recreational_fliers/ (accessed on 18 August 2022).
27. Pilot, What's the Difference Between Drones, UAV, and UAS? Definitions and Terms. Pilot Institute. 22 March 2020. Available online: https://pilotinstitute.com/drones-vs-uav-vs-uas/ (accessed on 18 August 2022).

28. 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. Tutorials* **2019**, *21*, 3417–3442. [CrossRef]
29. Nagpal, K. Unmanned Aerial Vehicles (UAV) Market, Q Tech Synergy. 24 December 2016. Available online: https://defproac.com/?p=2041 (accessed on 18 August 2022).
30. Pastor, E.; Lopez, J.; Royo, P. A Hardware/Software Architecture for UAV Payload and Mission Control. In Proceedings of the 2006 IEEE/AIAA 25TH Digital Avionics Systems Conference, Portland, OR, USA, 15–18 October 2006; pp. 1–8. [CrossRef]
31. VanZwol, J. Design Essentials: For UAVs and Drones, Batteries are Included, Machine Design. 4 April 2017. Available online: https://www.machinedesign.com/mechanical-motionsystems/article/21835356/design-essentials-for-uavs-and-drones-batteries-are-included (accessed on 18 August 2022).
32. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.; Jayakody, D.N.K.; Wang, H.-C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 102739. [CrossRef]
33. Ullah, H.; Nair, N.G.; Moore, A.; Nugent, C.; Muschamp, P.; Cuevas, M. 5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases. *IEEE Access* **2019**, *7*, 37251–37268. [CrossRef]
34. Luo, C.; Miao, W.; Ullah, H.; McClean, S.; Parr, G.; Min, G. Unmanned aerial vehicles for disaster management. In *Geological Disaster Monitoring Based on Sensor Networks*; Springer: Singapore, 2019; pp. 83–107.
35. Hosseini, N.; Jamal, H.; Haque, J.; Magesacher, T.; Matolak, D.W. UAV Command and Control, Navigation and Surveillance: A Review of Potential 5G and Satellite Systems. In Proceedings of the 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2019; pp. 1–10. [CrossRef]
36. IvyPanda, Unmanned Aerial Vehicles Essay. 13 January 2020. Available online: https://ivypanda.com/essays/unmanned-aerial-vehicles-essay/ (accessed on 20 December 2020).
37. Valavanis, K.P.; Vachtsevanos, G.J. UAV Applications: Introduction. In *Handbook of Unmanned Aerial Vehicles*; Springer: Dordrecht, The Netherlands, 2015; pp. 2639–2641. [CrossRef]
38. Shakhatreh, H.; Sawalmeh, A.H.; Al-Fuqaha, A.; Dou, Z.; Almaita, E.; Khalil, I.; Othman, N.S.; Khreishah, A.; Guizani, M. Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. *IEEE Access* **2019**, *7*, 48572–48634. [CrossRef]
39. Cook, K.L.B. The Silent Force Multiplier: The History and Role of UAVs in Warfare. In Proceedings of the 2007 IEEE Aerospace Conference, Big Sky, MT, USA, 3–10 March 2007; pp. 1–7. [CrossRef]
40. Siddiqi, M.A.; Khoso, A.M. Aziz, Analysis on Security Methods of Wireless Sensor Network (WSN). In Proceedings of the SJCMS 2018, Sukkur, Pakistan, 10 December 2018.
41. Cavoukian, A. *Privacy and Drones: Unmanned Aerial Vehicle*; Information and Privacy Commissioner: Toronto, ON, Canada, 2012.
42. Kafi, M.A.; Challal, Y.; Djenouri, D.; Doudou, M.; Bouabdallah, A.; Badache, N. A Study of Wireless Sensor Networks for Urban Traffic Monitoring: Applications and Architectures. *Procedia Comput. Sci.* **2013**, *19*, 617–626. [CrossRef]
43. Mansfield, K.; Eveleigh, T.; Holzer, T.H.; Sarkani, S. Unmanned aerial vehicle smart device ground control station cyber security threat model. In Proceedings of the 2013 IEEE International Conference Technology Homel Security (HST), Walthan, MA, USA, 12–14 November 2013; pp. 722–728. [CrossRef]
44. Smith, K.W. Drone Technology: Benefits, Risks, and Legal Considerations. *Seattle J. Environ. Law (SJEL)* **2015**, *5*, 291–302.
45. Eyerman, J.; Hinkle, K.; Letterman, C.; Schanzer, D.; Pitts, W.; Ladd, K. *Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns*; Institute of Homeland Security and Solutions: Washington, DC, USA, 2013.
46. Syed, N.; Berry, M. *Journo-Drones: A Flight over the Legal Landscape*; American Bar Association: Chicago, IL, USA, 2014.
47. Rahman, M.F.B.A. *Smart CCTVS for Secure Cities: Potentials and Challenges*; Rajaratnam School of International Studies (RSIS): Singapore, 2017.
48. Kim, A.; Wampler, B.; Goppert, J.; Hwang, I.; Aldridge, H. Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. *Aerospace Res. Cent.* **2012**, 2438. [CrossRef]
49. Zeng, Y.; Zhang, R.; Lim, T.J. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Commun. Mag.* **2016**, *54*, 36–42. [CrossRef]
50. Soria, P.R.; Bevec, R.; Arrue, B.C.; Ude, A.; Ollero, A. Extracting Objects for Aerial Manipulation on UAVs Using Low Cost Stereo Sensors. *Sensors* **2016**, *16*, 700. [CrossRef]
51. Erdelj, M.; Natalizio, E. Drones, Smartphones and Sensors to Face Natural Disasters. In Proceedings of the 4th ACM Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, Paris, France, 10–15 June 2018; pp. 75–86. [CrossRef]
52. Son, Y.; Shin, H.; Kim, D.; Park, Y.; Noh, J.; Choi, K. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In Proceedings of the 24th USENIX Security Symposium, Washington, DC, USA, 12–14 August 2015.
53. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and Privacy Issues of UAV: A Survey. *Mob. Netw. Appl.* **2019**, *25*, 95–101. [CrossRef]
54. Strohmeier, M.; Schafer, M.; Lenders, V.; Martinovic, I. Realities and challenges of nextgen air traffic management: The case of ADS-B. *IEEE Commun. Mag.* **2014**, *52*, 111–118. [CrossRef]
55. 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. [CrossRef]

56. Hartmann, K.; Giles, K. UAV exploitation: A new domain for cyber power. In Proceedings of the 2016 8th International Conference Cyber Conflict, Tallinn, Estonia, 31 May–3 June 2016; pp. 205–221. [CrossRef]
57. Rivera, E.; Baykov, R.; Gu, G. A Study on Unmanned Vehicles and Cyber Security. In Proceedings of the Rivera 2014 ASO, Austin, TX, USA, 2014.
58. Junejo, I.N.; Foroosh, H. GPS coordinates estimation and camera calibration from solar shadows. *Comput. Vis. Image Underst.* **2010**, *114*, 991–1003. [CrossRef]
59. Wang, W.; Huang, H.; Zhang, L.; Su, C. Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-to-Peer Netw. Appl.* **2020**, *14*, 2681–2693. [CrossRef]
60. Zhang, L.; Zhang, Z.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment. *IEEE Syst. J.* **2021**, *16*, 2822–2833. [CrossRef]
61. Currier, C.; Moltke, H. *Spies in the Sky*; The Intercept: New York, NY, USA, 2016.
62. Yağdereli, E.; Gemci, C.; Aktaş, A.Z. A study on cyber-security of autonomous and unmanned vehicles. *J. Déf. Model. Simulation: Appl. Methodol. Technol.* **2015**, *12*, 369–381. [CrossRef]
63. Lee, Y.S.; Dongseo University; Kang, Y.-J.; Lee, S.-G.; Lee, H.; Ryu, Y. An Overview of Unmanned Aerial Vehicle: Cyber Security Perspective. *IT Converg. Technol.* **2016**, *4*, 30. [CrossRef]
64. Wu, L.; Cao, X.; Foroosh, H. Camera calibration and geo-location estimation from two shadow trajectories. *Comput. Vis. Image Underst.* **2010**, *114*, 915–927. [CrossRef]
65. Krishna, C.G.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199. [CrossRef]
66. Siddiqi, M.A.; Pak, W. Optimizing Filter-Based Feature Selection Method Flow for Intrusion Detection System. *Electronics* **2020**, *9*, 2114. [CrossRef]
67. Strohmeier, M.; Lenders, V.; Martinovic, I. Intrusion Detection for Airborne Communication Using PHY-Layer Information. In *Proceedings of the International Conference Detection of Intrusions and Malware, and Vulnerability Assessment*; Springer: Cham, Switerland, 2015; pp. 67–77. [CrossRef]
68. Gil Casals, S.; Owezarski, P.; Descargues, G. Generic and autonomous system for airborne networks cyber-threat detection. In Proceedings of the 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC), IEEE, New York, NY, USA, 5–10 October 2013; pp. 4A4-1–4A4-14. [CrossRef]
69. Rani, C.; Modares, H.; Sriram, R.; Mikulski, D.; Lewis, F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. *J. Déf. Model. Simul. Appl. Methodol. Technol.* **2015**, *13*, 331–342. [CrossRef]
70. Zhang, G.; Wu, Q.; Cui, M.; Zhang, R. Securing UAV Communications via Joint Trajectory and Power Control. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1376–1389. [CrossRef]
71. Shao, X.; Wang, L.; Li, J.; Liu, J. High-order ESO based output feedback dynamic surface control for quadrotors under position constraints and uncertainties. *Aerosp. Sci. Technol.* **2019**, *89*, 288–298. [CrossRef]
72. Li, B.; Fei, Z.; Zhang, Y. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. *IEEE Internet Things J.* **2018**, *6*, 2241–2263. [CrossRef]
73. Lee, Y.-S.; Kim, E.; Kim, Y.-S.; Seol, D.-C. Effective Message Authentication Method for Performing a Swarm Flight of Drones. *Emergency* **2015**, *3*, 95–97. [CrossRef]
74. Pilli, E.S.; Joshi, R.; Niyogi, R. A Generic Framework for Network Forensics. *Int. J. Comput. Appl.* **2010**, *1*, 251–408. [CrossRef]
75. Beebe, N.L.; Clark, J.G. A hierarchical, objectives-based framework for the digital investigations process. *Digit. Investig.* **2005**, *2*, 147–167. [CrossRef]
76. Jain, U.; Rogers, M.; Matson, E.T. Drone forensic framework: Sensor and data identification and verification. In Proceedings of the 2017 IEEE Sensors Application Symposium (SAS), Glasgow, UK, 31 October 2017; pp. 1–6. [CrossRef]
77. Roder, K.; Choo, N.K.R.A. Le-Khac, Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone As A Case Study. *arXiv Prepr.* **2018**, arXiv:1804.08649.
78. Siddiqi, M.A.; Ghani, N. Critical Analysis on Advanced Persistent Threats. *Int. J. Comput. Appl.* **2016**, *141*, 46–50. [CrossRef]
79. Siddiqi, M.A.; Yu, H.; Joung, J. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices. *Electronics* **2019**, *8*, 981. [CrossRef]
80. Khan, N.A.; Jhanjhi, N.Z.; Brohi, S.N.; Almazroi, A.A.; Almazroi, A.A. A secure communication protocol for unmanned aerial vehicles. *CMC-COMPUTERS MATERIALS CONTINUA* **2022**, *70*, 601–618. [CrossRef]
81. Wild, G.; Murray, J.; Baxter, G. Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters. *Aerospace* **2016**, *3*, 22. [CrossRef]
82. Goodrich, M. Drone Catcher: "Robotic Falcon" can Capture, Retrieve Renegade Drones, Michigan Tech. 7 January 2016. Available online: https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html (accessed on 18 August 2022).
83. McNabb, M. Dedrone Acquires the Anti Drone Shoulder Rifle, Batelle's Drone Defender, Drone Life. 9 October 2019. Available online: https://dronelife.com/2019/10/09/dedrone-acquires-theanti-drone-shoulder-rifle-batelles-drone-defender/ (accessed on 18 August 2022).

84. Capello, E.; Dentis, M.; Mascarello, L.N.; Primatesta, S. Regulation analysis and new concept for a cloud-based UAV supervision system in urban environment. In Proceedings of the Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), IEEE, (2017), Carnfiled, UK, 25–27 November 2017; pp. 90–95. [CrossRef]
85. Joglekar, R. 4 Strategies for Stopping 'Rogue' Drones from Flying in Illegal Airspace. *ABC News*. 23 December 2018. Available online: https://abcnews.go.com/Technology/strategies-stoppingrogue-drones-flying-illegal-airspace/story?id=59973853 (accessed on 18 August 2022).
86. Friedberg, S. A Primer on Jamming, Spoofing, and Electronic Interruption of a Drone, Dedrone. 19 April 2018. Available online: https://blog.dedrone.com/en/primer-jamming-spoofing-andelectronic-interruption-of-a-drone (accessed on 18 August 2022).
87. Cyber, T.E.O. How To Crack WPA/WPA2 Wi-Fi Passwords Using Aircrack-ng, Medium. 5 November 2019. Available online: https://medium.com/@TheEyeOfCyberBuckeyeSecurity/howto-crack-wpa-wpa2-wi-fi-passwords-using-aircrack-ng-8cb7161abcf9 (accessed on 18 August 2022).
88. Yaacoub, J.-P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
89. 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.
90. Gaspar, J.; Ferreira, R.; Sebastião, P.; Souto, N. Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms. *Wirel. Pers. Commun.* **2020**, *115*, 2729–2754. [CrossRef]
91. Ezuma, M.; Erden, F.; Anjinappa, C.K.; Ozdemir, O.; Guvenc, I. Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques. In Proceedings of the 2019 IEEE Aerospace Conference; IEEE: Piscataway, NJ, USA, 2019; pp. 1–13. [CrossRef]
92. Digulescu, A.; Despina-Stoian, C.; Stănescu, D.; Popescu, F.; Enache, F.; Ioana, C.; Rădoi, E.; Rîncu, I.; Șerbănescu, A. New Approach of UAV Movement Detection and Characterization Using Advanced Signal Processing Methods Based on UWB Sensing. *Sensors* **2020**, *20*, 5904. [CrossRef]
93. 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]
94. Choudhary, G.; Sharma, V.; Gupta, T.; Kim, J.; You, U. Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives. In Proceedings of the MobiSec 2018: The 3rd International Symposium on Mobile Internet Security, Cebu, Philippines, 29 Auguest–1 September 2018.
95. Noura, H.N.; Salman, O.; Chehab, A.; Couturier, R. DistLog: A distributed logging scheme for IoT forensics. *Ad Hoc Networks* **2019**, *98*, 102061. [CrossRef]
96. Cohen, R.S. The Drone Zappers, Air Force Magazine. 22 March 2019. Available online: https://www.airforcemag.com/article/the-drone-zappers/ (accessed on 18 August 2022).
97. Mizokami. Air Force Downs Several Drones with New ATHENA Laser Weapon System, Popular Mechanics. 8 November 2019. Available online: https://www.popularmechanics.com/military/research/a29727696/athena-laser-weapon/ (accessed on 18 August 2022).
98. Federal Aviation Administration, Become a Drone Pilot, Become a Pilot. 19 May 2021. Available online: https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot/ (accessed on 18 August 2022).
99. Transport Canada, Where to Fly your Drone, Drone Safety. 19 February 2021. Available online: https://tc.canada.ca/en/aviation/drone-safety/where-fly-your-drone (accessed on 18 August 2022).
100. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
101. Sinha Satyajit, Securing IoT with Blockchain, Counterpoint. 11 May 2018. Available online: https://www.counterpointresearch.com/securing-iot-blockchain/ (accessed on 18 August 2022).
102. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2021**, *18*, 7059–7067. [CrossRef]
103. Zhang, L.; Zou, Y.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Resource allocation and trust computing for blockchain-enabled edge computing system. *Comput. Secur.* **2021**, *105*, 102249. [CrossRef]
104. Zhang, L.; Peng, M.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4315. [CrossRef]
105. Shao, X.; Yue, X.; Liu, J. Distributed adaptive formation control for underactuated quadrotors with guaranteed performances. *Nonlinear Dyn.* **2021**, *105*, 3167–3189. [CrossRef]
106. Li, M.; Guo, C.; Yu, H.; Yuan, Y. Event-triggered containment control of networked underactuated unmanned surface vehicles with finite-time convergence. *Ocean Eng.* **2022**, *246*, 110548. [CrossRef]
107. Rahman, Z.; Yi, X.; Khalil, I. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet Things J.* **2022**. [CrossRef]
108. Yu, S.; Das, A.K.; Park, Y.; Lorenz, P. SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments. *IEEE Trans. Veh. Technol.* **2022**. [CrossRef]
109. Gaurav, B.; Kumar, D.; Vidyarthi, D.P. BARA: A blockchain-aided auction-based resource allocation in edge computing enabled industrial internet of things. *Future Gener. Comput. Syst.* **2022**.

110. Yuan, L.; Zhang, Y.; Wang, J.; Xiang, W.; Xiao, S.; Chang, L.; Tang, W. Performance analysis for covert communications under faster-than-Nyquist signaling. *IEEE Commun. Lett.* **2022**.
111. Zhang, W.; Shao, X.; Zhang, W.; Qi, J.; Li, H. Unknown input observer-based appointed-time funnel control for quadrotors. *Aerosp. Sci. Technol.* **2022**, *126*, 107351. [CrossRef]
112. Challita, U.; Ferdowsi, A.; Chen, M.; Saad, W. Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs. *IEEE Wirel. Commun.* **2019**, *26*, 28–35. [CrossRef]
113. Sanjab, A.; Saad, W.; Basar, T. Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6. [CrossRef]