Mathematical Biosciences and Engineering

MBE, 19(3): 2641–2670.
DOI: 10.3934/mbe.2022121
Received: 09 July 2021
Revised: 06 September 2021
Accepted: 24 November 2021
Published: 10 January 2022

http://www.aimspress.com/journal/MBE

Survey

Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations

Murtaza Ahmed Siddiqi[1], Celestine Iwendi[2,*], Kniezova Jaroslava[3] and Noble Anumbe[4]

[1] Computer Science Department, Sukkur IBA-University, Sindh, Pakistan
[2] School of Creative Technologies, University of Bolton, United Kingdom
[3] Information Systems Department, Faculty of Management, Comenius University in Bratislava, Slovakia
[4] Mechanical Engineering Department, University of South Carolina, Columbia, SC, USA

* **Correspondence:** Email: celestine.iwendi@ieee.org.

Abstract: Over time, the use of UAVs (unmanned aerial vehicles)/drones has increased across several civil and military application domains. Such domains include real-time monitoring, remote sensing, wireless coverage in disaster areas, search and rescue, product delivery, surveillance, security, agriculture, civil infrastructure inspection, and the like. This rapid growth is opening doors to numerous opportunities and conveniences in everyday life. On the other hand, security and privacy concerns for unmanned aerial vehicles/drones are progressively increasing. With limited standardization and regulation of unmanned aerial vehicles/drones, security and privacy concerns are growing. This paper presents a brief analysis of unmanned aerial vehicle's/drones security and privacy-related concerns. The paper also presents countermeasures and recommendations to address such concerns. While laying out a brief survey of unmanned aerial vehicles/drones, the paper also provides readers with up-to-date information on existing regulations, classification, architecture, and communication methods. It also discusses application areas, vulnerabilities, existing countermeasures against different attacks, and related limitations. In the end, the paper concludes with a discussion on open research areas and recommendations on how the security and privacy of unmanned aerial vehicles can be improved.

Keywords: UAV; Drone; UAV security; UAV privacy; UAV applications; UAV countermeasures; UAV threats; UAV architecture; blockchain

1. Introduction

For ages, the advancement of technology is one of the most promising and fruitful evolution. Bundled with uncertainty, technical advancements are successfully providing reliable, affordable, and user-friendly solutions to the problems we face in everyday life. Although the future is unknown, digital innovation continues to shape the future-encouraging people to adopt new hobbies and ways of interacting with everyday work and people. In recent times, UAV (Unmanned Aerial Vehicles)/drones are among the most prominent and rapidly increasing areas of interest for industrial, military, and personal applications. Research conducted by CUAVI (China Unmanned Aerial Vehicle Industry) predicted that the market scope of small domestic UAVs would be approximately 75 billion Yuan in China by 2025 [1]. The FAA (Federal Aviation Administration) highlighted that almost 2.5 million drones are presently flying in the US that is likely to reach almost 7 million drones by 2020 [2]. This rise in UAV/drone usage is due to several factors, i.e., growing demand for live streaming, real-time video shooting, image capture capabilities, mobility, ease of usage, etc. The UAV/drones have also been used for small goods transportation and last-mile delivery as they are easy to deploy, require low maintenance, have unique hovering ability, and have high mobility. The UAV/drones are also proving to be very effective in the domain of security, surveillance, and rescue operations [3,4]. On the other hand, the security concerns of UAVs are quite concerning to the stakeholders. In one incident, the Iranian military was able to take down a U.S. Lockheed Martin RQ-170 Sentinel drone by jamming the UAV's control signals [5]. Due to the design limitations and hostile operational domain, developing a full-proof security module for UAV/drones is a challenge for security experts. In terms of UAV/drone history, the earliest record of a UAV/drone dates back to the 18th century [6]. Apparently, in 1849 the Australians used unmanned balloons filled with explosives to attack Venice in Italian [7]. In 1915, the British military used unmanned balloons for photographic-based surveillance in the Battle of Neuve Chapelle [8]. During the early 19th century, cameras were not very advanced and different methods were used to enhance the visibility of the photograph taken by a camera attached to these floating objects [8].

The United States commenced UAV development during the First World War. In 1916, the US developed the first pilotless aircraft that could fly a steered distance of 1000 yards. Later in World War II, the US developed further advanced UAVs including the Curtiss N2C-2 drone and the Radio plane OQ-2 [9]. Despite a long history of military-based applications, UAVs were considered unreliable and expensive. However, in the 1980s this aspect began to change with the US leading the way to develop economical UAVs. In the 1990s and 2000, miniature and micro UAVs were introduced. During the 2000 afghan war, it was a Predator drone that located Osama bin Label in Afghanistan [10]. Although, UAV's were originally developed for military purposes. However, studies showed that it has a high potential in numerous domestic applications. In 2014, Amazon initially suggested using UAVs for delivery purposes [6]. Later UAVs/drone's potential was explored by several domestic domains i.e., agriculture [1,2], construction, law enforcement, search and rescue, photography for real state, cinematography, etc. With this exponential growth of the application domain, UAV/drone's security and privacy concerns became more severe. The core idea of this paper is to give readers an in-depth view of the rising security-related concerns of UAV/drones. To give a clear idea of these security and privacy concerns The rest of the paper is organized as follows. Section 2 covers the existing regulation for UAVs. In section 3 covers the classification of both drones and UAVs. Drone architecture and communication methods are discussed in section 4. Detailed discussion on the applications of

drone/UAVs is discussed in section 5. Drone/UAV security vulnerabilities and threats are covered in section 6. Section 7 covers the existing threats for drones/UAVs. Existing solutions and countermeasures for UAV/drone security are discussed in section 8. The physical and logical attack countermeasures are discussed in section 9. The limitations of existing security measures are discussed in section 10. Section 11 covers a brief overview of drone/UAV open research areas. Recommendations for improving security and privacy-related concerns for drones/UAVs with a summary of the paper are presented in section 12. Section 12 also presents a comparison between this paper and recent survey papers. Section 13 concludes the article.

2. Regulations

The licensing of UAV/drone is of paramount importance due to the associated privacy and security implications of their use. Governments all over the world are taking steps to licence these devices [11,12]. The danger unlicensed UAV/Drones over private property and sensitive military jurisdictionas and installations is grave. In some countries like Lebanon, unlicensed or illegal drones are often taken down and legal action is pursued against owners due to the grave security risks to government institutes and public safety [11]. According to BBC News (British Broadcasting Corporation) [13], the CAA (Civil Aviation Authority) and FAA [14] announced some basic drone operation codes for the owners to follow, some of these include:

- A requirement for users/operators to register their UAVs/drones and always carry the prof of registration when operating.
- A restriction not to exceed a flight height of 400 feet.
- A restriction from flying near airfields. If there is a need to operate a UAV/drone near an airfield, permission must be acquired in advance from the relevant authorities.
- Due to public safety concerns, UAV/drones must be operated carefully or legal action can be taken against the harmful actions of a UAV/drone operator
- UAV/drones with cameras are not allowed to fly within 50m of people, animals, structures, or vehicles.
- UAVs/drones must be flown within the operator's line of sight.
- UAVs/drones must not be flown at night without proper lighting.

The mentioned rules present a very general outline of UAV/drone operation. With the dramatic increase in the drone market in recent times, many countries and states have defined their own rules and regulations for the ownership and operation of UAVs/Drones [15].

A typical drone/UAV system has three main components. The first is the ground control station or ground command and control. Second is the communication link, which could be through satellite, telecommunication infrastructure, or even through another drone. The third component is the drone/UAV itself. Detailed discussion about the architecture of drones/UAVs will be covered in a later section. Three default methods for drone/UAV communication include Satellite, Radio Signal, and the Internet. As shown in Figure 1 [16] a drones/UAVs can be controlled or communicated through satellite, telecom infrastructure, and internet (i.e., IoTs, drones, UAV, etc.).

The most common frequencies for controlling UAV/drones from the ground are frequencies for license-exempt radio equipment. Table 1 highlight the most common frequencies for command and control link [17].

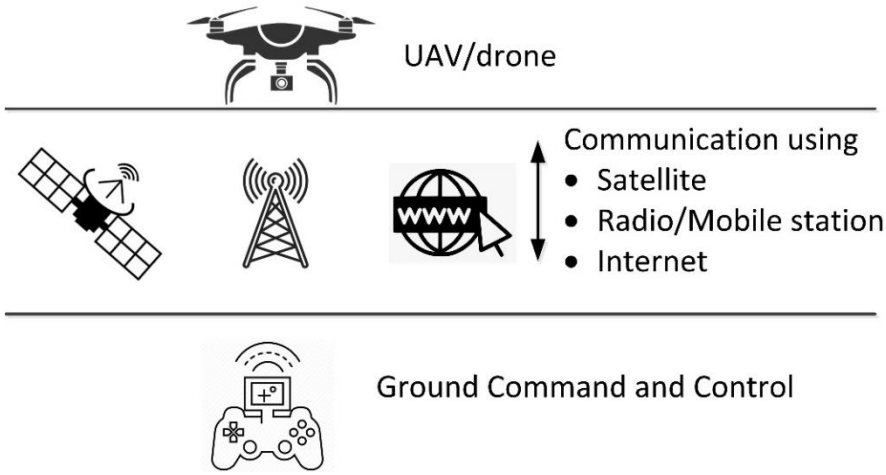

Figure 1. Default ways of drone/UAV communication through the ground command and control station.

Table 1. Common Frequencies for ground-based command and control for Drone/UAV.

Frequency	Details about ground control and control equipment
2400.000–2483.500 MHz	≤ 100mW, if the associated standard is EN 300 328 (Digital wideband data transmission equipment) ≤ 10mW, if the appropriate standard is EN 300 440 (General short-range devices).
5470.000–5725.000 MHz	The transmitter's operational power is ≤ 1W and the power spectral density of transmission is ≤ 50mW/1 MHz. The appropriate standard is EN 301 893 (RLAN equipment). The use of the mentioned frequency may change as it is under discussion within international cooperation and awaits a final decision.
5725.000–5875.000 MHz	The transmitter's operative power is ≤ 25mW and the appropriate standard is EN 300 440 (General short-range devices)
5030–5091 MHz	As per the International Telecommunication Union ITU, the frequency is assigned to the command and control of UAV or drones in cargo and passenger traffic and so it cannot be used for ground-based UAVs or drones.

Further standardization by ISO (International Organization for Standardization) committee ISO/TC 20/SC 16 [18] is still working to finalize standards for operating UAV/drones.

3. Classification

A drone can be defined as an unmanned aircraft that is controlled remotely or autonomously. A UAV flies without a pilot on board [19]. Every UAV is a drone; however, not all drones can be classified as UAVs.

3.1. Drones classification

The term drone is typically referred to as remotely (autonomously) controlled aircraft. This definition could include both submarines and land-based autonomous vehicles. Based on their flying mechanics, flying drones can generally be classified into three main types [20].

- *Multi-Rotor Drones or Rotary-wing drones*: Their main feature is the Vertical Take-off and Landing (VTOL) ability. Additionally, their ability to hover and high maneuverability play an important role in different applications.
- *Fixed-Wing Drones:* These types of drones are energy efficient compared to rotary-based drones. This is due to their capability to fly at high speed and glide. These drones can carry heavy payloads. The only concern for these types of drones is the runway, as they are Horizontal Take-Off and Landing (HTOL) drones.
- *Hybrid-Wing Drones:* As the name suggest, these type of drones have both fixed and rotary wings. These drones use gliding ability to travel fast, while rotary to perform hovering-based tasks.

3.2. UAVs classification

A UAV can fly remotely (autonomously) based on a ground command and control mechanism using a controller, mobile phone, or computer [21]. UAV's can be classified by their ability to fly autonomously over long distances. UAV control can be classified into three main types.

- *Full autonomous control*: Fully automated to perform different tasks.
- *Remote supervised control*: Based on tasks, the UAV can be automated and also operated by a human.
- *Remote pilot control*: Human-based remote command and control.

The referenced classifications have their own merits and demerits. Brief information regarding these drones/UAVs classifications can be seen in Table 2 [22].

Table 2. Drone/UAV basic classification.

Based on wing type			Based on altitude	
Rotary-wing	Fixed-wing	Hybrid	Low altitude platform	High altitude platform
• Can hover • Less battery life then fixed-wing • Low speed • Typical battery time 1-hour flight	• Similar to small aircraft • Cannot hover • Can transport high payloads • High speed • Battery life several hours	• Have both fixed and rotary wings • Can glide over the air and hover using rotary	• Quick and flexible deployment • Quick mobility • Usually flies up to several hours • Cost-effective	• High endurance (days or months) • Wide area coverage • Quasi-stationary Altitude above 17km

Some recent research work prefer to classify drones/UAVs based on their altitude. Figure 2 shows drone/UAV classification based on their altitude with some common examples [23].

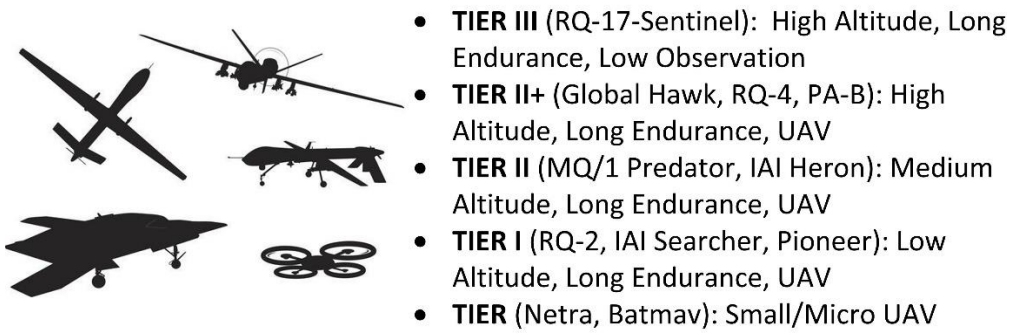

Figure 2. Drone/UAV classification based on altitude.

4. Drone/UAV architecture and communication methods

A large variety of commercial and military UAVs/drones exist today. Most commercial UAVs/drones are low-cost and remotely controlled. Mini and micro UAVs are gaining popularity for both commercial military applications. However, there are limitations in their application due to size and weight considerations. Tier II & III UAVs/drones, have high resource requirements (refer to Figure 2). Almost every UAV/drone is equipped with a combination of sensors, GPS, CPU, communication module, and batteries as shown in Figure 3. Due to advancements in technology, many UAVs/drones are approaching a point where they are finding commercial and military applications. It is believed that the lack of software and hardware support are the two main issues affecting the realization of their full potential [24].

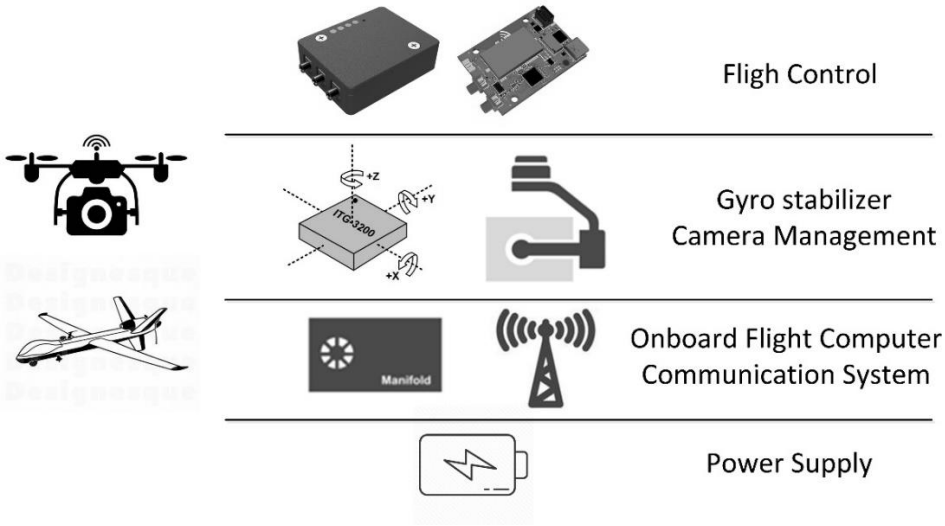

Figure 3. Main components of a Drone/UAV system.

Even though dependable autonomous UAVs exist, the main objective is to achieve the mission with additional payloads (i.e., sensors, camera, etc.). UAVs for defense or military applications are tailored for specific objectives and those equipment are not openly available for commercial UAVs application. As shown in Figure 3, a typical UAV can be broken down into five components.

- *Drone/UAV airframe:* The airframe of a drone/UAV must be very simple, aerodynamic, lightweight, and a stable. Size and weight are a constraint for any UAV, so efficient use of space is critical.
- *Onboard computer:* Onboard CPU is the heart of a drone/UAV. The onboard computer serves as the collector, collaborator, and controller for flight, onboard equipment, and sensors (i.e., GPS, camera, accelerometer, gyros, magnetometer, pressure, etc.)
- *Payload:* Drones/UAVs are utilized for several different purposes. Drones/UAVs designed for public and commercial use have different payload attachments compared to those developed for military applications. Examples of payloads include sensors, high definition cameras, infrared sensors, heat sensors, radiation sensors, or any military mission-based equipment, etc.
- *Communication system:* Every drone/UAV requires a set of communication systems. Either remotely controlled or automated. Communication equipment (i.e., radio, modem, sitcom, etc.) guarantees uninterrupted communication between UAV and its ground base station.
- *Battery:* Different UAVs have different requirements for the power source. Power sources are based on their size, objective, and range. Most Mini and Micro UAVs use Lithium power batteries [25].

4.1. Communication methods

Communication plays an integral part of both fully automated or remotely controlled UAVs. To engineer a suitable suite for UAVs, the communication protocols, communication network, and communication model play an integral part [26]. Several researchers have proposed different network architectures, antenna designs, and communication methods. As shown in Figure 4 there are three basic methods for UAV communication at different altitudes [27].

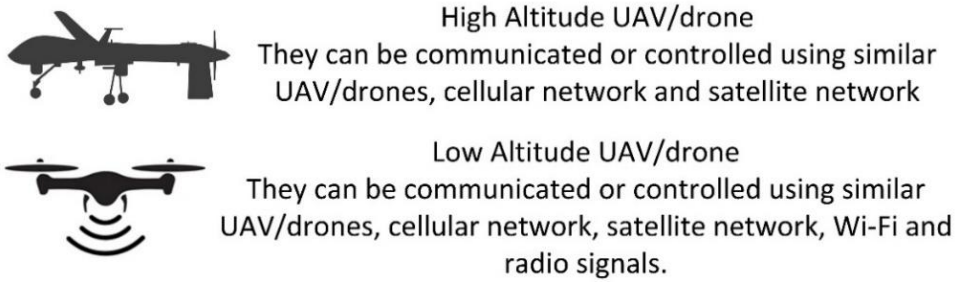

Figure 4. UAV/drone communication methods for different altitudes.

With the introduction of highly capable 5G networks, some issues like data rate, coverage, and latency can be addressed. The advancement in communication technology can play a significant role in positioning UAVs for critical missions. Some of the key parameters of the different communication technologies (including Wi-Fi and cellular communication) can be seen in Table 3 [28].

Most of the UAVs communicate based on LOS (Line of sight), but when it comes to high altitude UAV/drones, LOS-based communication (as in Table 3) is not suitable other than GPS. For BLOS (Beyond line of sight), Table 4 gives a brief overview of LEO (Low Earth Orbit), MEO (Medium Earth Orbit), and GEO (Geostationary Earth Orbit) satellites [29].

Table 3. Communication technologies summary for UAVs/Drones.

Technology	Frequency Band	Channel Width	Range	Bit Rate	Latency	Coverage	Mobility Support	UAV Support
Wi-Fi	2.4 GHz, 5.2 GHz	20 MHz	100 m	6-54 Mbps	10 ms	Intermittent	Low	Yes
GPS (Satellite)	1176–1576 MHz	2 MHz	-	50 bps	10 ms	Global	Quite High	Yes
UMTS	700–2600 MHz	5 MHz	10 Km	2 Mbps	20-80 ms	Global	High	Likely
LTE	700–2690 MHz	1, 4, 3, 5, 10, 15, 20 MHz	30 Km	Up to 300Mbps	10 ms	Global	Very High (350 km/h)	Likely
LTE-A	450 MHz – 4.99 GHz	Up to 100 MHz	30 Km	Up to 1 Gbps	-	Global	Very High (350 km/h)	Likely
5G	57.05–64 GHz	2.16 GHz	50 m	Up to 4 Gbps	-	Global	Ultra-High	Likely

Table 4. Details of satellite-based communication for drone/UAV.

Satellite Type	Satellite Elevation (km)	Orbital Period	Number of satellites	Satellite Life (years)	Handoff frequency	Gateway Cost	Doppler	Propagation path loss
LEO	500–1500	95–115 min	40–800 global	3–7	High	Very Expensive	High	Least
MEO	5000–12000	3–7 hours	8–20 global	10–15	Low	Expensive	Medium	High
GEO	35800	24 hours	3 no polar coverage	15+	None	Cheap	Low	Highest

Communication plays a vital role in the UAV/drone role and its architecture. Based on the mission and architecture of the UAV/drone, different communication modules are installed. Several UAVs/drones can carry a wide variety of payloads or attached modules based on the operational requirements [26].

5. Drone/UAV application areas

In the new scientific developments arena, UAVs/drone's potentials are on the higher side. The applications of UAVs cover a huge domain ranging from personal use to military applications as shown in Figure 5 [30]. Drones and UAVs can be equipped with several different sensors, cameras, and other payloads to perform many different tasks. UAVs/drones have over two hundred applications based on how they are used and what payloads they carry [31]. Due to rapid deployment, diligence, ability to reach areas where humans can't reach, risk, cost, mobility, and payload options, drone/UAV applications are always increasing and improving.

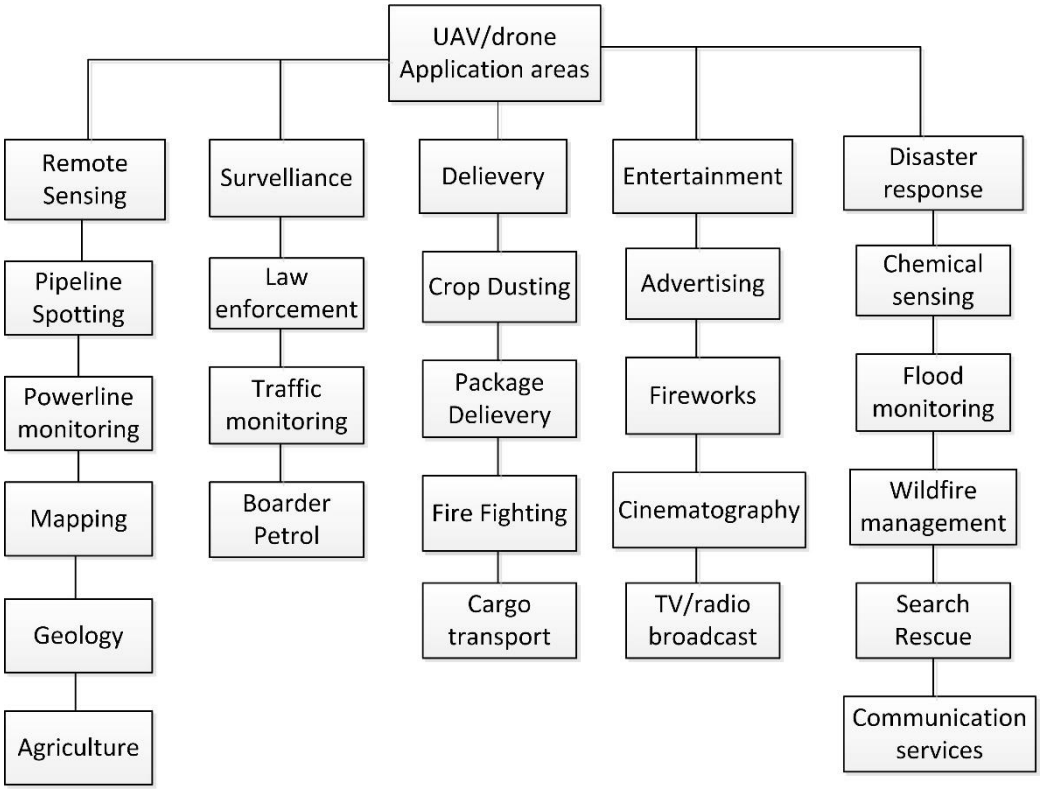

Figure 5. Drone/UAV applications.

5.1. Application domain

Drones/UAVs will play a key role in the coming future. As shown in Figure 5, the application areas for UAVs/drones are on the increase. Based on types and applications, they can be classified into diverse usage domains. Generally, drones/UAVs follow an architecture based on their application. Dividing them by domains can therefore be a very effective way of better understanding their architecture and peculiarities. Figure 6 gives a brief overview of their classification by domain [32,33].

From Figure 6, it is clear that each domain has its own security and privacy needs.

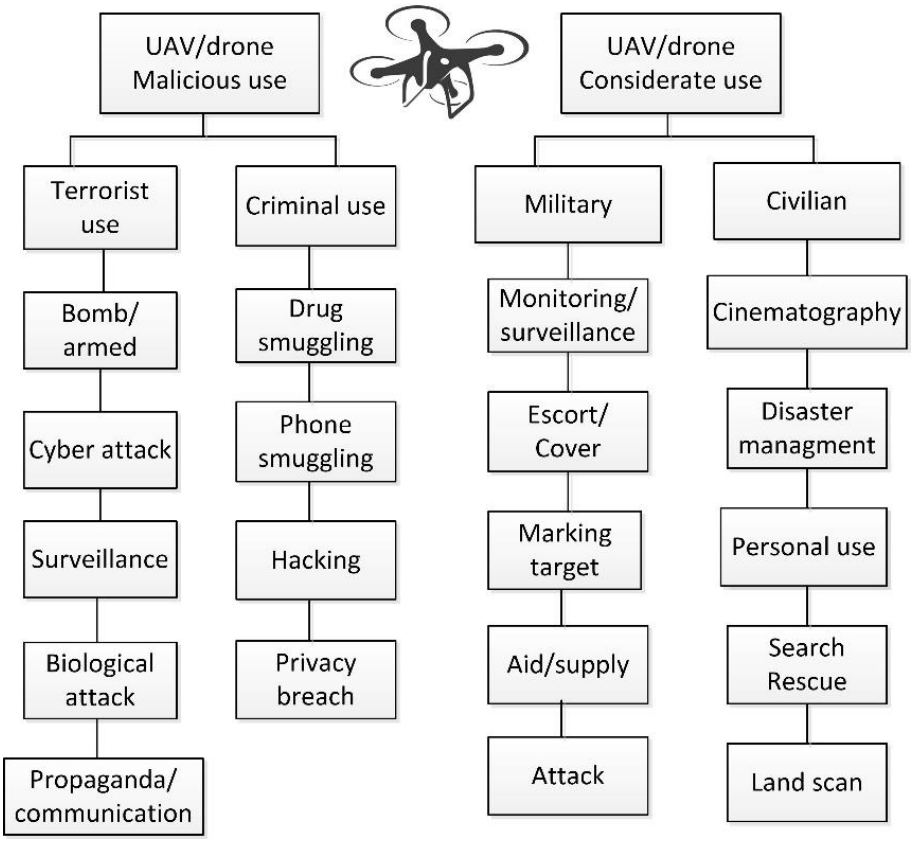

Figure 6. Drone/UAV application based domain classification

6. Drone/UAV security vulnerabilities and threats

Drones/UAVs offer numerous benefits that have kept increasing with technological progress. However, some of them have limited operating resources and others create diverse security, privacy, and safety concerns [34,35]. Licensing, regularization, and various measures (over-sight) should be adopted to limit unnecessary of nepharious UAV-based photography. Authorities all over the world should ensure that the adoption of surveillance-regulating measures and regulations are a priority. As regards network security and risk analysis, network coverage provided by a UAV is not similar to any Wireless Sensor Network (WSN) or Mobile Ad-hoc Network (MANETs) [36]. This is due to resource constraints as UAV-based coverage is wider and broader as compared to WSN and MANETs. Concerning AAA (Authorization Authentication Accounting), the following guidelines can be effective for UAVs:

- *Authorization:* Assigning privileges to the controller of the UAV to avoid any hostile takeover with administrative rights.
- *Authentication*: There must be a rigid authentication method for UAVs to avoid unauthorized access and control.
- *Accounting:* In case of any illegal activity by a UAV/drone, the owner can be tracked down.

Mischievous or criminal entities can use drones/UAVs for conducting illegal surveillance, cyber-attacks, and initiating privacy threats individuals and organizations because of the ease of accessibility. Various mechanical and operational capabilities of drones/UAVs are being exploited for conducting malicious activities [37]. Such events make UAV/drone growth a double-edged sword, the effort to make them more secure and rigid also makes them more effective for malicious activities.

6.1. Security concerns

Due to their portability, low cost, availability, maintenability, and maneuverability UAVs are a perfect choice for criminal activity. For example, terrorists and criminals use UAVs to conduct harmful activities and sabotage. The ability to carry a wide range of attachments makes UAVs effective couriers for harmful chemicals or explosive items. Additionally, their ability to reach places where humans cannot, makes them useful. They can carry anything, unnoticed or stealthily [38].

6.2. Safety concerns

Security is not the only concern for drones/UAVs. Any drone flying over populated areas or property can malfunction and crash. Such crashes can be harmful to buildings and can injure people [39]. Such incidents have been reported all over the world. Human injuries due to a UAV/drone are unfortunately common. In April 2016, a UAV hit a passenger jet (British AirwaysBA727). Due to these accidents, a few public safety measures can be considered:

- *Safety Feature:* There is a high probability that a UAV/drone can be hacked or go out of control due to strong winds. Under such circumstances, there should be an option to shut it down or to regain control again.
- *Weak Signal or jamming*: Signal jamming makes UAVs/drones venerable to hacking and hijacking as part of a cyber-attack.
- *Design/Architecture safety*: Most of the UAV/drones that are easily accessible to the public are rotary-based types as shown in Figure 7.

Figure 7. Commonly available types of drone/UAV.

These drones can have additional safety features as shown in some products in Figure 8. Understandably adding such measures affects the architecture and may introduce some performance concerns, but safety must be a higher priority. A standard should be introduced regarding safety measures for publically available drones/UAVs. Such standards should also include crash avoidance features.

Figure 8. UAVs/drones with additional safely measure.

6.3. Privacy concern

Privacy concerns are rife due to the ease with which anyone can procure UAVs with high-definition cameras and gadgets. People can be easily recorded or observed within their private property without their knowledge. Per Canadian Public Safety (CPS), UAVs have generated quite a few safety, security, and privacy concerns [40]. Taking pictures or recording people without their consent has resulted in blackmail and other criminal activities. Legal policies regarding taking private photos or videos without consent using UAVs, flying through premises, or hovering at window level should be introduced to help regulate UAV operations.

7. Existing threats for drones/UAVs

Due to a lack of standardization, several UAVs currently in the market have considerable design issues. One of the most concerning of these issues is the unavailability of wireless security [41].

Table 5. Common Threads/Vulnerability of UAVs/drones.

Thread/Vulnerability	Details
Malware Infection	Most of the UAV controllers are based on a cellphone, remote control, laptop, or wireless remote control. These techniques are not secure [42], as they enable hackers to generate a reverse-shell TCP payload, which can be injected into UAV memory. This can result in the stealthy installation of harmful malware on the UAV controller.
Spoofing	The exploration of configuration and remote controllers of UAVs/drones' rotor-based models, expose some vulnerability issues. These issues are associated with the communication link (via serial port connections), which are usually not encrypted [43]. Experiments highlight that by GPS spoofing; information can be taken, altered, or even injected into the UAVs.
Manipulation	As most of the drones/UAVs follow pre-programmed flying routes, manipulation of those routes can be implemented [44]. Such manipulation can help steal precious cargo and can even direct a drone to attack a target.
Natural concern	While flying, the UAV/drone can face many natural issues. Strong wind, lightning, overheating due to surrounding temperature, etc. . Some predator birds can also cause issues for any lightweight and small UAV/drone [45].

Continued on next page

Thread/Vulnerability	Details
Technical Problems	Several drones/UAVs encounter technical issues both hardware and software-based. Glitches and technical issues are a part of every system. UAV's suffer issues which may include battery problems, crashes due to wing or rotor malfunction, remote controller communication issues, etc.
Attack on sensors	Drones/UAVs rely on different sensors to perform their task and to operate. Son Y. et al. [46] experimented and showed how ultrasonic waves can be used to perform an attack on MEMS gyroscope. They showed how certain frequencies could destroy a UAV's gyroscope.
Wi-Fi security	Some drones/UAVs can be remotely piloted using smart devices through Wi-Fi, which is a security risk. In an experiment [47] in which two Wi-Fi connection software's Mavic and Spark from the same company were used, it was observed that the connection to the UAV was disrupted with the help of another software, requesting UAV control.
ADS-B security	Automatic Dependent Surveillance-Broadcast (ADS-B) is one of the aircraft's operation monitoring technology, which is based on GPS and is used for communication. Aircraft are equipped with both ADS-B in and out, while a UAV is only equipped with ADS-B in. ADS-B broadcast is intended for all aircraft and is not encrypted, which means any criminal can use a UAV and GPS spoofing device to disrupt such broadcasts and cause harm to aircraft traffic [48].
Zero-Day Vulnerability	Zero-Day vulnerabilities are one of the common bugs in software and firmware. These bugs are unknown by the time of product release but with time vendors release patches to overcome these bugs. Attacks through such vulnerabilities were successfully experimented on in a UAV control stream [49] using Parrot Bebop.
De-authentication attack	De-authentication attacks target the control stream between the controller and the UAV. There are software such as 'SkyJack', which can be used to conduct such attacks on vulnerable UAVs [50].
Video-Replay attack	These attacks are quite harmful and target the Operation Control Unit (OCU). These attacks puzzle the controller by changing the live feed to some other video. While a human operator might be able to notice the difference, an autonomous UAV might find this attack difficult to handle [51].

Some researchers also conducted different types of cyber-attack on UAVs in a controlled environment to test the effects and vulnerability [49]. Such experiments include:

- *DoS Attack:* Researchers used parallel requests for controlling UAVs. The high amount of requests overloaded the response and crashed the UAV system.
- *Buffer-Overflow:* In such an attack, the researchers modified the packet request for controlling the drone/UAV and crashed the system responsible for controlling the drone/UAV.
- *ARP Attack:* In Address Resolution Protocol (ARP) attack, the researcher used the cache-poisoning approach and it resulted in the disconnection of the UAV from its controller.

Other than communication links or attacks on ground control, a different aspect of cyber-attack on UAV is the attack on the operating system (OS) or micro-controller unit of a UAV. In most cases, these OS for UAVs are very similar to smartphones OS. Due to this similarity, several attacks that are

effective against smartphone OS are also useful on UAV systems [52]. With the advancement of technology and UAV, attack vectors on UAVs are on the rise. The probability of attack types can be unlimited in the current era of technology. Figure 9 shows the attacks that are being reported or being conducted successfully for educational purposes [49,50,53–57]. Among the attacks highlighted in the section, GPS spoofing is one of the most common cyber-attack on UAVs/drones. Among the most common type of GPS attacks, include signal jamming, de-authentication, and zero-day attacks.

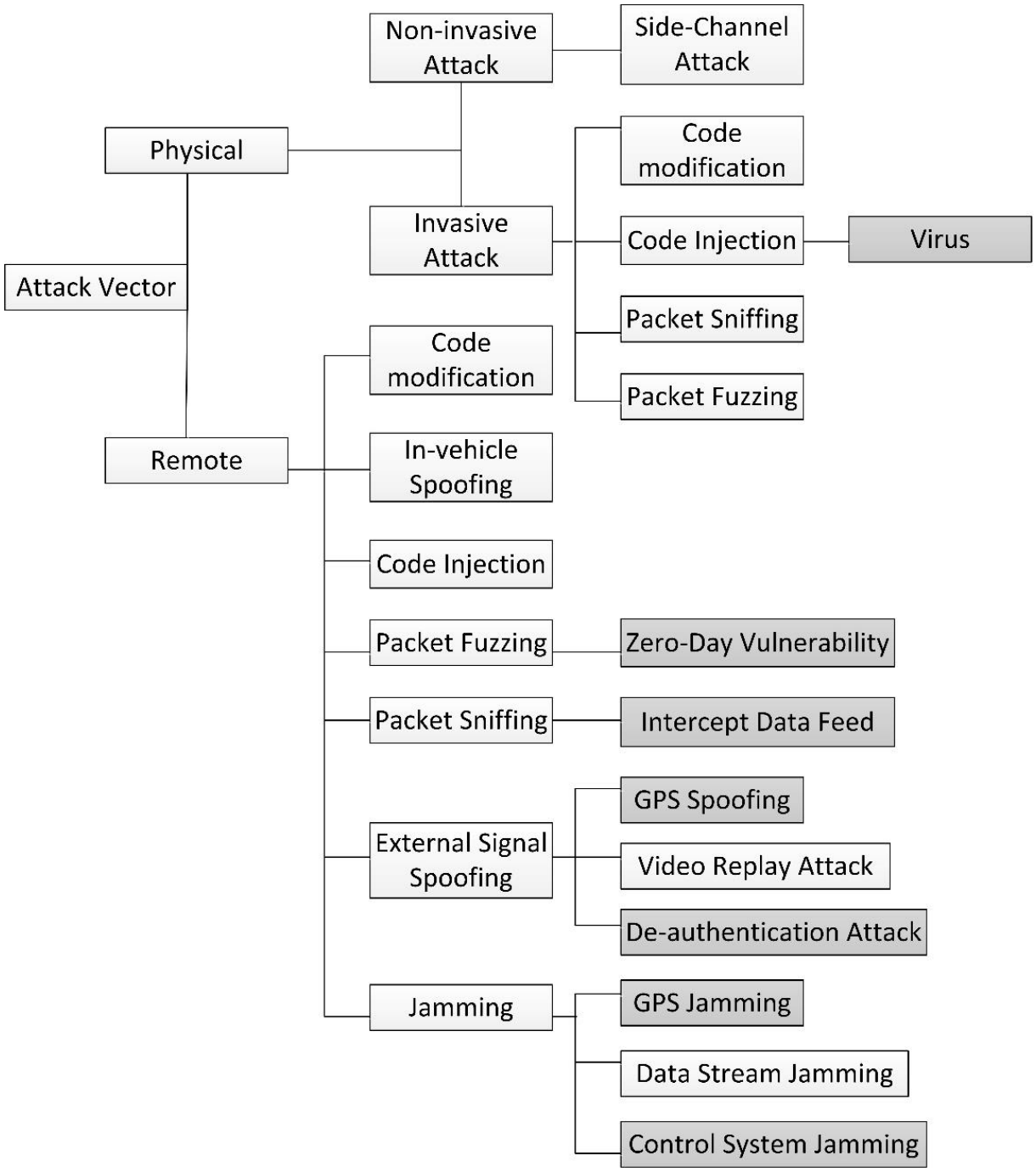

Figure 9. Drone/UAV Attack Vector with reported incidence or educational purpose in grey.

8. Existing solutions and counter measures for UAV/Drone security

The first counter-measure for resolving security threats on drones/UAV is classifying the attacks types, intended target, and objective of the attack. Table 6 shows some of the most proponent cyber-attacks conducted against UAVs/drones. The table also highlights the nature of the attack and some security measures against the attacks [57]. Most of the attacks highlighted in Table 6 target the authentication process of a UAV/drone. This highlights the need for improvement in the authentication method of a UAV/drone.

8.1. Current countermeasures

The wireless-based communication network suffers from numerous security issues and threats. In recent times, machine learning (ML) based intrusion detection systems (IDS) have been quite successful against network threats. As machine learning-based solutions require higher resources, several researchers are working on how resources can be managed in ML-based IDS [58]. Blockchain is also among the most effective approach for UAV/drone security and privacy [11].

Table 6. Cyber-attack types and counter in UAV/drones.

Attack	Nature	Target	Security Measure
Malware	Infection	Privacy, Integrity, Data confidentiality, Availability, Authentication	Light-weight IDS, control Access policies, multi-factor authentication, system integrity
Injection/Modification	Exploitation	Privacy, Integrity	ML-based IDS, time stamping, message authentication, digital signature
Eavesdropping	Interception	Privacy, Data confidentiality	Secure communication, secure connection
Man in the middle	Authentication	Privacy, Data confidentiality, Integrity	Light hybrid IDS, multi-factor authentication, lightweight but strong cryptography authentication methods
Wi-Fi Air crack	Cracking	Authentication	Physical layer lightweight IDS, Strong & periodic password, strong encryption
Wi-Fi Jamming	Jamming	Authentication	Frequency hopping, frequency range variation, Strong & periodic password, strong encryption
De-Authentication	Jamming	Authentication	Frequency hopping, frequency range variation
Replay attack	Jamming	Authentication	Frequency hopping, time-stamping

Continued on next page

Attack	Nature	Target	Security Measure
Buffer Overflow	Jamming	Authentication	Frequency hopping, frequency range variation
DoS	Jamming	Authentication	Frequency hopping, frequency range variation
ARP attack	Jamming	Authentication	Frequency hopping, frequency range variation
GPS Spoofing	Jamming	Authentication	Return-to-base function or protocol, frequency range variation

8.1.1. UAV/Drone communication network security

Keeping up with the current requirements of network security ML-based IDS are among the most successful tools. Generally, IDS are categorized into three types:

- *Rule-Based:* These types of IDS are used in the UAV domain [59] and the objective is to identify false data-injection attacks, specifically those who target signal strength between UAV and ground control. Rule-based IDS can be effective against known attack patterns and techniques. Conversely, these types of IDS cannot detect the new or complex types of attacks and require human interaction to counter such attacks.
- *Signature-Based:* Some researchers have also used signature-based IDS on UAV. In a paper [60], the authors used a bio-inspired cyber-attack method that attacks air-born networks. Like rule-based IDS, signature-based IDS are also not good against unknown and complex attacks.
- *Anomaly-Based*: These types of IDS are used against jamming attacks in UAV networks [61]. Jamming attacks include DoS, DDoS, triggering malfunction, and sensors-based attacks. The only major issue for anomaly-based ML IDS is the high resource requirement.

As the number of UAVs/drones increase, quite a lot of different solutions for UNV communication network are proposed. Some papers [62] identified the physical layer issues in UAV communication network and proposed iterative algorithm based on optimizing methods showed an improved detection rate of attacks. Similarly, other papers have looked into ADS-B issues, line of sight issues, air-to-ground, eavesdropping, and air-to-air wireless communications. Some of the solutions proposed by researchers include using modulation, dual antenna, game theory-based algorithm, or Q-learning-based approaches. In addition to these methods, encryption for secure UAV communication is also an important aspect. Researchers have been looking to encryption methods that are not resources hungry. Since traditional encryption, methods do not consider resources and delay as an important factor [63]. Encryption can not only provide secure communication but can also be very effective in the authentication process of a UAV/drone.

8.1.2. Data security

Data captured by a UAV/drone is aggregated onboard the UAV before it is transmitted out. This aggregation plays an important part in minimizing network traffic. However, this aggregation and encrypting data creates other issues. The symmetric cipher is not secure enough to counter advance attack methods and asymmetric cipher requires high computation and high resources. Asymmetric cipher also requires additional storage overhead. Due to these constraints, researchers are looking to secure, yet lightweight encryption methods for UAV/drone data security.

8.1.3. Forensic approaches

Digital forensics can plan a vital role in identifying and countering different types of UAV attacks. In paper [64] authors presented a generic framework for NF (Network Forensics). The framework analysis data traveling through firewalls or IDS to identify any anomaly. The goal of the framework is not only to identify the anomaly but also to track back the source of the activity. Another paper [65] has suggested an NF framework involving DIP (Digital Investigation Process) with multiple hierarchical digital investigation methods. The approach presented in this paper follows two-tiers. The first tier involves assessment, countermeasure, data collection and analysis, the incident report, and event closure. Second-tier is an object-based sub-phase [66]. In addition, a UAV/drone forensic process can be broken down into three main steps as shown in Table 7 [67].

Table 7. UAV/drone forensic process steps.

Steps	Details
1. Preparation	a. Identify the chain of command b. Identify any fingerprint or identity of UAV c. Offensive process of tracking down the owner using time, date, location, and identity found on the UAV.
2. Examination	a. Accessing and inspecting data on the UAV i.e., audio, video, pictures, etc. b. Finding communication method and port
3. Analysis and Report	a. After extracting all the information from the UAV, compiling and analyzing them to identify the culprit, its location, or method of attack.

Similarly, several other researchers have proposed different methods to use forensic methods to counter complex and advanced attacks. The reason for highlighting the forensic method is that with time the type and objective of attacks are more complex and difficult to identify [68]. With the help of forensic, both perpetrator and method of attack can be identified. With the identification of attack type, appropriate countermeasures can be implemented to avoid any future incident.

Table 8. Physical countermeasures against UAV/drones.

Counter Measure	Details
Drone catcher [70]	Bulky drone/UAV are equipped with a net. The net can be shot to capture drones/UAVs.
Drone defender [71]	Drone defender (Dedrone) is a radio wave gun that is used to drop drones/UAVs down from the sky.
Electric Fences [72]	These are invisible fences and work as a virtual prohibition or wall against UAV/drones. Cloud technology is used to implement them so that every drone in the area can identify and avoid these areas.
Unconventional methods [73]	These methods include training birds of prey i.e., eagles to hunt down any drone/UAV in the area. However, these methods include the danger of animals being injured by the UAV/drone.

9. Physical and logical attacks countermeasures

As per the survey [69], 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 cyber-attacks 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 illegal use of UAVs would likely proliferate. Civilian or domestic UAV countermeasures are divided into physical and local countermeasures. Physical countermeasures against UAVs can be seen in Table 8.

Keeping in view that logical countermeasure for urban use against UAVs is not high-end tech and limited in range and functionality. Table 9 outlines the logical countermeasures against UAV/drones in an urban environment.

Table 9. Logical countermeasures for UAV/drone in an urban environment.

Counter Measure	Details
Wi-Fi jamming [74]	Wi-Fi-based drone/UAV operates using a 2.4 GHz frequency. A conventional jammer can jam these frequencies within a limited range and can be used for privacy purposes.
Wi-Fi Aircrack [75]	Although it is an attacking method, it can be used to take control of any illegal or privacy-invading UAV/drone.
Three-way handshake [76]	Although it is also an attacking method, it can be used to de-authorize or even jam communication between the UAV/drone and the controller.
DoS [77]	Websploit Wi-Fi jammer can be an effective method to jam or de-authenticate UAV from its controller. However, to conduct DoS based attack, some knowledge about the communication channel is required.
GPS Spoofing [78]	Encryption of civilian-based equipment is very costly and making it vulnerable to GPS spoofing attacks.

9.1. Military and government Counter-measure techniques

When it comes to military-based countermeasures, resources availability is often not in question. As discussed earlier, the use of UAVs/drones is not limited to surveillance, but they are capable of conducting attacks or used to pinpoint locations for an attack, making them dangerous tools on the battlefield. Some of the well-known drone/UAV countermeasures can be seen in Figure 10.

Militaries all around the globe are well equipped to handle UAV/drone-based threats. Figure 10 only highlights some of the well-known and publically available information on anti UAV/drones weapon systems. Military and Government based organizations use different methods to detect drones. They (UAV/drone) can be detected using audio, video, motion, thermal, radio, and RF-based methods. All these methods have their own merits and demerits.

Table 10 gives a brief overview of different UAV/drone detection methods [79–81]. UAV/drone

can be detected based on audio, video, motion, thermal, radio, and RF-based methods. All these methods have their own merits and demerits as highlighted in Table 10.

Figure 10. Some well-known military anti UAV/drone systems.

Table 10. UAV/drone detection methods.

Method	Range	Accuracy	Pros	Cons
Radio Frequency	60–430 meter	Good/Average	Can detect signal and location of drone/UAV	Can be countered by using signal interference.
Audio	8–10 meter	Not consistent	Detect drones based on the sound it makes	Can only detect in the short-range and have noise interference concerns.
Video	77 meter	Average/Bad	High resolution and image	The high false detection rate
Thermal	77 meter	Good/Bad	Good in detecting fix-winged UAV/drone	Mini/Micro drone does not have a high heat signal so thermal-based detection have difficulty detecting them.
Motion	16–46 meter	Fair	Can identify drones easily	Works for a very short range
Radar	46–457+ meter	Good/Average	Highly accurate in detection and locating UAV/drone	Concerns over detecting and locating mini/micro drones

10. Security implementation limitations

Several limitations still exist in adopting and implementing rigid security methods for UAVs/drones. Table 11 highlights some of the main issues for UAV/drone security limitations [82–84]. Most of the mentioned limitations can be overcome by standardizing UAV/drone design, communication protocols, and basic factory default security suits.

Table 11. UAV/drone security limitations.

Limitation	Details
Availability	UAV/drones are easily accessible for everyone to purchase. There is no owner registration or license registration for purchasing a UAV/drone.
Design issue	Due to the absence of standardization, manufacturers are failing to comply with necessary requirements i.e., safe design, factory authentication, etc.
Policies	Standardization and policies are absent for UAV/drone operations and operators. In some countries, policies are defined for UAV/drones flying in proximity of sensitive areas. However, a general set of operating policies for a UAV/drone are still not available.
Non-real-time countermeasures	Due to a lack of standardization for design and operational software, the current UAV/drones do not have real-time protection during flight. If a UAV/drone is compromised during flight it cannot be retained by the original owner.
Limited testing	Due to limited testing, the available control and communication units are vulnerable to several types of attacks.
Forensic limitations	In case of a harmful event, the limited availability of forensic tools and methods makes it difficult to identify the malicious operator of UAV/drones involved in the dangerous act.
Unreliable security	Based on the hostile operational environment of UAV/drones, the default security measures are not suitable. Due to the harsh operating environment of UAV/drones, a robust security protocol is necessary. But due to design and resource limitations, improving security measures is very challenging.
Authentication	Based on recent events as shown in Table 6, the currently employed authentication methods for UAV/drone can easily be compromised. Except for the UAV/drones operated for defense purposes as they have trailered software to cope with the requirements.
Limited Frequency bands	The UAV/drones are being operated within a limited range of frequencies. Making them an easy target for jamming-based attacks.

11. Open research areas

Based on the earlier sections, it is clear that a lot of work is still needed in improving UAV/drone security. Some of the areas that are open for research are listed in Table 12. Research areas listed in Table 12 can play an integral part in solving several UAV/drone security concerns [85,86].

Table 12. Open Research areas for UAV/drones.

Area	Description
Path loss	Path loss and channel model to facilitate higher carrier frequencies are a concern. Specifically in areas that are surrounded by tall concrete buildings and have a high number of wireless equipment operating in the vicinity.
Latency	Keeping up with the latency requirement of less than 1 millisecond is still an ongoing concern. Future cellular technology needs to ensure improved facilitation in terms of latency for UAV/drones in emergencies.
Reliability	Ultra-reliable communication is among the most important area related to UAV/drone communication. With the exponential increase of UAVs/drones, reliable communication will be quite challenging.
Battery Life	UAV/drones, which rely on battery power need long-lasting batteries or power sources that are not only light but can also, provide long flight ability.
Collision Avoidance	Mobility and the ability to avoid collision are still areas that researchers are looking to improve for UAV/drones.
AI integration	AI can play an integral role in the future of UAVs/drones. AI cannot only assist UAVs in terms of security but can also provide improvement in terms of collision avoidance, data analysis, and security. However, due to high computational requirements, AI-based solutions need further research and improvements.

Table 13. Recommendations for improving UAV/drone security and privacy.

Measure	Description
Licensing	Every UAV/drone should be registered and licensed. Such measures will make it easy for the authorities to identify the owner of any harmful drone/UAV.
Flying Permit	A flying permit similar to a driving license should be issued with a registered drone/UAV. Such regulation would limit UAV/drone-based illegal or harmful activity.
Education	The public should be educated on the harmful or illegal use of UAV/drones.
Laws	Based on harmful and illegal events, laws should be introduced for the misuse of UAV/drones.
Restricted zones	Areas that are classified or could pose a danger to drones/UAVs should be marked. Map-based public applications should also indicate areas that are no-fly zones for UAV/drones.
Non-lethal measures	Non-lethal tools to counter drones/UAVs should be publically available. Such tools can play an important role in urban areas.
Machine Learning	Security tools such as ML-based IDS can vastly improve the security architecture of drones/UAVs.
Multi-factor authentication	Rigid authentication methods can help in stopping several common security threats.

12. Recommendations and summary

Some recommendations to improve security and privacy for UAV/drones are shown in Tables 13 and 14. In Table 13 general recommendations which could help in improving UAV security and privacy are mentioned. While Table 14 enlist the most recent block-chain-based solutions for UAV security and privacy. Further, the authorities and industry need to put a combined effort into regularizing and standardizing UAVs/drones to counter security and privacy-related issues [84,87–89].

Table 14 represent UAV's privacy and security solutions based on blockchain. Blockchain can provide very effective and enhanced security for UAVs/drones [90]. The only concern for blockchain-based solutions is the requirement of additional computational resources [91]. On the contrary, the enhancement in terms of security and privacy due to blockchain is more than adequate. The blockchain-based solution can be a very suitable option for UAVs specifically designed for defense and government usage.

Table 14. Blockchain-based proposed solutions for improving UAV/drone security and privacy.

Reference	Description
[92]	The authors in this paper proposed a novel pairing-free certificate less scheme that used the blockchain and smart contract to develop a novel, secure, reliable, and efficient certificate-less signature (CLS) scheme. The proposed model in this paper can be very useful for UAV/drone security against many common attack methods.
[93]	This paper presents a solution for identity authentication issues. The authors proposed an efficient authentication protocol based on blockchain, dynamic Join-and-Exit mechanism, Elliptic Curve Cryptography (ECC), and batch verification.
[94]	In the paper, the authors propose a covert communication model which can be an effective method for secure communication in UAV/drones. The proposed model uses smart contracts to model covert communication under the blockchain to solve the concerns of traditional covert communication.
[95]	In this paper, an improved method for data processing and sharing is proposed. The proposed method can be very useful for UAV/drone secure communication and data sharing process. The proposed approach in the paper can be represented by three main stages. First, the proposed model employs a group-agent strategy based on trust computing to improve transmission efficiency. Second, to improves resource allocation in each edge device the authors proposed a stacked task sorting and ranking mechanism. Third, the model adopts used symmetric searchable encryption (SSE) for a secure and efficient content model.
[96]	In this paper, the authors proposed a computationally efficient method for data integrity and authenticity. The proposed model is designed especially for devices with limited resources i.e UAV/drones, IoT, etc. The proposed method provides a secure and efficient data sharing and storage scheme for mobile-edge computing based on blockchain. The model uses a unique signature private key approach to achieve data integrity and authenticity.

Table 15 highlights the areas discussed in this paper and a comparison with some recent survey papers on UAVs/drones. In Table 15 the first column represents all the topics discussed in the paper and the first row represents the recent survey papers reference. To highlight the significance of this paper, Table 15 shows the topics discussed in other survey papers by a black dot in contrast with the eleven topics covered in this paper.

Table 15. Topic comparison with recent survey papers on UAV/drone security and privacy concerns.

	Topics	[4]	[20]	[32]	[47]	[57]	[76]	[82]
1.	Regulation		●					
2.	Classification	●	●	●			●	
3.	Architecture and communication methods	●		●	●	●	●	
4.	Applications	●		●			●	●
5.	Security Vulnerabilities and Threats			●	●	●	●	●
6.	Existing Threats			●	●	●	●	●
7.	Existing Solutions and Counter Measures		●	●	●	●	●	
8.	Physical and Logical Attacks countermeasures			●				
9.	Security Implementation Limitations			●			●	●
10.	Open Research Areas	●	●	●			●	●
11.	Recommendations		●	●	●	●		

13. Conclusions

The trend and exponential growth in the use of UAV/drones are giving birth to an era of autonomous aerial vehicles. UAV/drones offer numerous advantages to both civilian and military-based domains. However, this increase in use and easy availability has raised serious security and privacy-related concerns. Due to the flexibility, low cost, ease of deployment, and portability of these devices, they have become very useful tools for mischievous activities. Despite the availability of several countermeasures against the malicious use of these vehicles (UAV/drone), they are still very effective for carrying out harmful activities. Privacy issues with UAV/drones are also very significant. In this technological age, privacy is a major concern for individuals and organizations. This paper presented a comprehensive study of these (security and privacy) concerns including an overview of factors driving these concerns alongside with possible counter-measures. Different recommendations were also made in the paper including existing solutions based on blockchain. These solutions can provide UAV/drones with improved data integrity, authenticity, and accessibility.

Conflict of interest

The authors declare no conflict of interest.

References

1. M. K. Bombe, 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 from: https://www.meticulousresearch.com/download-sample-report/cp_id=5086.
2. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, T. R. Gadekallu, G. Srivastava, SP2F: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles, *Comput. Netw.*, **14** (2021), 107819. https://doi.org/10.1016/j.comnet.2021.107819
3. S. Hayat, E. Yanmaz, R. Muzaffar, Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications View point, *IEEE Commun. Surv. Tut.,* **18** (2016), 2624–2661. https://doi.org/10.1109/COMST.2016.2560343
4. K. Chan, U. Nirmal, W. Cheaw, Progress on drone technology and their applications: a comprehensive review, *AIP Conf. Proc. 2030*, **020308** (2018). https://doi.org/10.1063/1.5066949
5. S. C. Hartmann K, The vulnerability of UAVs to cyber, in Cyber Conflict (CyCon) 2013 5th International Conference, Tallinn, Estonia, 2013.
6. S. O'Donnell, Consortiq. Available from: https://consortiq.com/short-history-unmanned-aerial-vehicles-uavs/.
7. D. Ekramul, First successful Air-raid in history, 22 August 2019. Available from: https://www.daily-bangladesh.com/english/First-successful-Air-raid-in-history/27424.
8. T. R. Berg, Air Space Mag, 10 January 2020. Available from: https://www.airspacemag.com/daily-planet/first-map-compiled-aerial-photographs-180973929/.
9. Q. A. Abdullah, Introduction to the Unmanned Aircraft Systems, Available from: https://www.e-education.psu.edu/geog892/node/643.
10. M. Bowden, How the Predator Drone Changed the Character of War, Smithsonian Magazine, November 2013. Available from: https://www.smithsonianmag.com/history/how-the-predator-drone-changed-the-character-of-war-3794671/.
11. A. Miah, Drones: The Brilliant, the Bad and the Beautiful (Societynow), London: Emerald Publishing Limited, 2020. https://doi.org/10.1108/9781838679859
12. S. Wright, Ethical and safety implications of the growing use of civilian drone, UK Parliament Website (Science and Technology Committee), 2019.
13. C. Lowbridge, Are drones dangerous or harmless fun?, *BBC News*, 5 October 2015. Available from: https://www.bbc.com/news/uk-england-34269585.
14. Federal Aviation Authorities, Recreational Flyers & Modeler Community-Based Organizations, 18 February 2020. Available from: https://www.faa.gov/uas/recreational_fliers/.
15. U. Coach, Master List of Drone Laws (Organized by State & Country), Available from: https://uavcoach.com/drone-laws/.
16. M. Aljehani, M. Inoue, A. Watanbe, T. Yokemura, F. Ogyu, H. Iida, UAV communication system integrated into network traversal with mobility, *SN Appl. Sci.*, **2** (2020), 1057. https://doi.org/10.1007/s42452-020-2749-5
17. A. Professionals, Drones and remotely piloted aircraft (UAS/RPAS) - frequencies and radio licenses, Traficom, 17 July 2021. Available from: https://www.traficom.fi/en/transport/aviation/drones-and-remotely-piloted-aircraft-uasrpas-frequencies-and-radio-licences.
18. C. Carnahan, ISO/TC 20/SC 16 Unmanned aircraft systems, 2014. Available from: https://www.iso.org/committee/5336224.html.

19. Pilot, What's the Difference Between Drones, UAV, and UAS? Definitions and Terms, Pilot Institute, 22 March 2020. Available from: https://pilotinstitute.com/drones-vs-uav-vs-uas/.
20. A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, et al., Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges, *IEEE Commun. Surv. Tut.*, **21** (2019), 3417–3442. https://doi.org/10.1109/COMST.2019.2906228
21. J. Irizarry, M. Gheisari, B. Walker, Usability Assessment of Drone Technology as Safety Inspection Tools, *Electron. J. Inf. Technol. Constr.*, **17** (2012), 194–212.
22. M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, M. Debbah, A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems, *IEEE Commun. Surv. Tut.*, **21** (2019), 2334–2360. https://doi.org/10.1109/COMST.2019.2902862
23. K. Nagpal, Unmanned Aerial Vehicles (UAV) Market, Q Tech Synergy, 24 December 2016. Available from: https://defproac.com/?p=2041.
24. E. Pastor, J. Lopez, P. Royo, A Hardware/Software Architecture for UAV Payload and Mission Control, *2006 IEEE/AIAA 25TH Digital Avionics Systems Conference*, Portland, 2006, 1–8. https://doi.org/10.1109/DASC.2006.313738
25. J. VanZwol, Design Essentials: For UAVs and Drones, Batteries are Included, Machine Design, 4 April 2017. Available from: https://www.machinedesign.com/mechanical-motion-systems/article/21835356/design-essentials-for-uavs-and-drones-batteries-are-included.
26. A. Sharma, P. Vanjani, N. Paliwal, C. M. Basnayaka, D. N. K. Jayakody, H.C. Wang, et al., Communication and networking technologies for UAVs: A survey, *J. Netw. Comput. Appl.*, **168** (2020), 102739. https://doi.org/10.1016/j.jnca.2020.102739
27. H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, M. Cuevas, 5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases, *IEEE Access*, **7** (2019), 37251–37268. https://doi.org/10.1109/ACCESS.2019.2905347
28. C. Luo, W. Miao, H. Ullah, S. McClean, G. Parr, G. Min, Unmanned aerial vehicles for disaster management, *Geological Disaster Monitoring Based on Sensor Networks*, Singapore, Springer, 2018, 93-107. https://doi.org/10.1007/978-981-13-0992-2_7
29. N. Hosseini, H. Jamal, D. W. Matolak, J. Haque, T. Magesacher, UAV Command and Control, Navigation and Surveillance: A Review of Potential 5G and Satellite, IEEE Aerospace Conference March 2019, MT, USA, 2019. https://doi.org/10.1109/AERO.2019.8741719
30. IvyPanda, Unmanned Aerial Vehicles Essay, 13 January 2020. Available from: https://ivypanda.com/essays/unmanned-aerial-vehicles-essay/. (Accessed 20 December 2020).
31. K. P. Valavanis, G. J. Vachtsevanos, UAV Applications: Introduction, in Handbook of Unmanned Aerial Vehicles, Dordrecht, Springer, 2015, pp. 2639–2641. https://doi.org/10.1007/978-90-481-9707-1_151
32. H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, et al., Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges, *IEEE Access*, **7** (2019), 48572–48634. https://doi.org/10.1109/ACCESS.2019.2909530
33. K. L. B. Cook, The Silent Force Multiplier: The History and Role of UAVs in Warfare, in 2007 IEEE Aerospace Conference, MT, USA, 2007.
34. M. A. Siddiqi, M. Khoso, A. Aziz, Analysis on Security Methods of Wireless Sensor Network (WSN), in SJCMS 2018, Sukkur, Pakistan, 2018.

35. A. Cavoukian, Privacy and Drones: Unmanned Aerial Vehicle, Ontario: Information and Privacy Commissioner, Ontario, Canada, 2012.
36. M. A. Kafia, Y. Challal, D. Djenouri, M. Doudou, A. Bouabdallah, N. Badache, A Study of Wireless Sensor Networks for Urban Traffic Monitoring: Applications and Architectures, *Procedia Comput. Sci.*, **19** (2013), 617–626. https://doi.org/10.1016/j.procs.2013.06.082
37. K. Mansfield, T. Eveleigh, T. H. Holzer, S. Sarkani, Unmanned aerial vehicle smart device ground control station cyber security threat model, *2013 IEEE Int. Conf. Technol. Homel. Secur. (HST)*, Walthan, USA, 2013. https://doi.org/10.1109/THS.2013.6699093
38. K. W. Smith, Drone Technology: Benefits, Risks, and Legal Considerations, *Seattle J. Environ. Law (SJEL)*, **5** (2015), 291–302.
39. J. Eyerman, K. Hinkle, C. Letterman, D. Schanzer, W. Pitts, K. Ladd, et al., Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns, Institute of Homeland security and solutions, 2013.
40. N. Syed, M. Berry, Journo-drones: a Flight over the Legal Landscape, American Bar Association, Chicago, Illinois, United States, 2014.
41. M. F. B. A. Rahman, Smart CCTVS for Secure Cities: Potentials and Challenges, S. Rajaratnam School of International Studies (RSIS), Singapore, 2017.
42. A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge, Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, *Aerospace Research Central*, (2012), 2438. https://doi.org/10.2514/6.2012-2438
43. Y. Zeng, R. Zhang, T. J. Lim, Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges, *IEEE Commun. Mag.*, **54** (2016), 36–42. https://doi.org/10.1109/MCOM.2016.7470933
44. P. R. Soria, R. Bevec, B. C. Arrue, A. Ude, A. Ollero, Extracting Objects for Aerial Manipulation on UAVs Using Low Cost Stereo Sensors, *Sensors*, **16** (2016), 700. https://doi.org/10.3390/s16050700
45. M. Erdelj, E. Natalizio, Drones, Smartphones and Sensors to Face Natural Disasters, *4th ACM Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, France, 2018, 75–86. https://doi.org/10.1145/3213526.3213541
46. Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, et al., Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors, in 24th USENIX Security Symposium, Washington, D.C, 2015.
47. Y. Zhi, Z. Fu, X. Sun, J. Yu, Security and Privacy Issues of UAV: A Survey, *Mobile Netw. Appl.*, **25** (2019), 95–101. https://doi.org/10.1007/s11036-018-1193-x
48. M. Strohmeier, M. Schäfer, V. Lenders, I. Martinovic, Realities and challenges of nextgen air traffic management: the case of ADS-B, *IEEE Commun. Mag.*, **52** (2014), 111–118. https://doi.org/10.1109/MCOM.2014.6815901
49. M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, et al., Securing commercial wifi-based UAVs from common security attacks, *MILCOM 2016-2016 IEEE Military Communications Conference*, 2016, 1213–1218. https://doi.org/10.1109/MILCOM.2016.7795496
50. E. Rivera, R. Baykov, G. Gu, A Study On Unmanned Vehicles and Cyber Security, in Rivera 2014 ASO, Texas, USA, 2014.
51. I. N. Junejo, H. Foroosh, GPS coordinates estimation and camera calibration from solar shadows, *Comput. Vis. Image Underst.*, **114** (2010), 991–1003. https://doi.org/10.1016/j.cviu.2010.05.003

52. K. Hartmann, K. Giles, UAV Exploitation: A New Domain for Cyber Power, *2016 8th Int. Conf. Cyber Conflict*, Tallinn, Estonia, 2016, 205–221. https://doi.org/10.1109/CYCON.2016.7529436
53. C. Currier, H. Moltke, Spies in the sky, The Intercept, New York, USA, 2016.
54. E. Yadereli, C. Gemci, A. Z. Akta, A study on cyber-security of autonomous and unmanned vehicles, *J. Def. Model. Simul.*, **12** (2015), 369–381. https://doi.org/10.1177/1548512915575803
55. Y. S. Lee, Y. J. Kang, S. G. Lee, H. Lee, Y. Ryu, An overview of unmanned aerial vehicle: Cyber security perspective, in IT Convergence Technology 2016, Korea, 2016.
56. L. Wu and X. Cao, Geo-location estimation from two shadow trajectories, in Computer Vision and Pattern Recognition (CVPR), San Francisco. USA, 2010.
57. C. G. Leela Krishna, R. R. Murphy, A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles, *2017 IEEE Int. Symposium on Safety, Security and Rescue Robotics (SSRR)*, Shanghai, China, 2017, 194–199. https://doi.org/10.1109/SSRR.2017.8088163
58. M. A. Siddiqi, W. Pak, Optimizing Filter-Based Feature Selection Method Flow for Intrusion Detection System, *Electronics*, **9** (2020), 2114. https://doi.org/10.3390/electronics9122114
59. M. Strohmeier, V. Lenders, I. Martinovic, Intrusion Detection for Airborne Communication Using PHY-Layer Information, *Int. Conf. Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, Cham, 2015, 67–77. https://doi.org/10.1007/978-3-319-20550-2_4
60. S. G. Casals, P. Owezarski, G. Descargues, Generic And Autonomous System For Airborne Networks Cyber-Threat Detection, *2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC)*, IEEE, 2013. https://doi.org/10.1109/DASC.2013.6712578
61. C. Rani, H. Modares, R. Sriram, D. Mikulski, F. L. Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks, *J. Def. Model. Simul.*, **13** (2016), 331–342. https://doi.org/10.1177/1548512915617252
62. G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing UAV Communications via Joint Trajectory and Power Control, *IEEE Trans. Wireless Commun.*, **18** (2019), 1376–1389,. https://doi.org/10.1109/TWC.2019.2892461
63. Y. S. Lee, E. Kim, Y. S. Kim, D. C. Seol, Effective Message Authentication Method for Performing a Swarm Flight of Drones, *Emergency*, **3** (2015), 95–97.
64. E. S. Pilli, R. Joshi, R. Niyogi, A Generic Framework for Network Forensics, *International J. Comput. Appl.,* **1** (2010), 1–6. https://doi.org/10.5120/251-408
65. N. L. Beebe, J. G. Clark, A hierarchical, objectives-based framework for the digital investigations process, *Digit. Investig.*, **2** (2005), 147–167. https://doi.org/10.1016/j.diin.2005.04.002
66. U. Jain, M. Rogers, E. T. Matson, Drone forensic framework: Sensor and data identification and verification, *2017 IEEE Sensors Appl. Symp. (SAS)*, 2017, 1–6. https://doi.org/10.1109/SAS.2017.7894059
67. A. Roder, K. K. R. Choo, N. A. Le-Khac, Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone As A Case Study, *arXiv preprint arXiv:1804.08649*, 2018.
68. M. A. Siddiqi, N. Ghani, Critical Analysis on Advanced Persistent Threats, *Int. J. Comput. Appl.*, **141** (2016), 46–50. https://doi.org/10.5120/ijca2016909784
69. G. Wild, J. Murray, G. Baxter, Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters, *Aerospace*, **3 (**2016), 22. https://doi.org/10.3390/aerospace3030022
70. M. Goodrich, Drone Catcher: "Robotic Falcon" can Capture, Retrieve Renegade Drones, Michigan Tech, 7 January 2016. Available from: https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html.

71. M. McNabb, Dedrone Acquires the Anti Drone Shoulder Rifle, Batelle's Drone Defender, Drone life, 9 October 2019. Available from: https://dronelife.com/2019/10/09/dedrone-acquires-the-anti-drone-shoulder-rifle-batelles-drone-defender/.
72. E. Capello, M. Dentis, L. N. Mascarello, S. Primatesta, Regulation Analysis and New Concept for a Cloud-based UAV Supervision System in Urban Environment, *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, IEEE, (2017), 90–95. https://doi.org/10.1109/RED-UAS.2017.8101649
73. R. Joglekar, 4 strategies for stopping 'rogue' drones from flying in illegal airspace, ABC news, 23 December 2018. Available from: https://abcnews.go.com/Technology/strategies-stopping-rogue-drones-flying-illegal-airspace/story?id=59973853.
74. S. Friedberg, A Primer on Jamming, Spoofing, and Electronic Interruption of a Drone, Dedrone, 19 April 2018. Available from: https://blog.dedrone.com/en/primer-jamming-spoofing-and-electronic-interruption-of-a-drone.
75. T. E. O. Cyber, How To Crack WPA/WPA2 Wi-Fi Passwords Using Aircrack-ng, Medium, 5 November 2019. Available from: https://medium.com/@TheEyeOfCyberBuckeyeSecurity/ how-to-crack-wpa-wpa2-wi-fi-passwords-using-aircrack-ng-8cb7161abcf9.
76. J. P. Yaacoub, H. Noura, O. Salman, A. Chehab, Security analysis of drones systems: Attacks, limitations, and recommendations, *Internet Things*, **11** (2020), 100218. https://doi.org/10.1016/j.iot.2020.100218
77. C. A. T. Bonilla, O. J. S. Parra, J. H. D. Forero, Common Security Attacks on Drones, *Int. J. Appl. Eng. Res.*, **13** (2018), 4982–4988.
78. J. Gaspar, R. Ferreira, P. Sebastião, N. Souto, Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms, *Wireless Pers. Commun.*, **115** (2020), 2729–2754. https://doi.org/10.1007/s11277-020-07211-7
79. M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, I. Guvenc, Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques, *2019 IEEE Aerospace Conf.*, IEEE, (2019), 1–13. https://doi.org/10.1109/AERO.2019.8741970
80. A. Digulescu, C. Despina-Stoian, D. Stanescu, F. Popescu, F. Enache, C. Ioana, et al., New Approach of UAV Movement Detection and Characterization Using Advanced Signal Processing Methods Based on UWB Sensing, *Sensors*, **20** (2020), 5904. https://doi.org/10.3390/s20205904
81. I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis, *IEEE Commun. Mag.*, **56** (2018), 106–111. https://doi.org/10.1109/MCOM.2018.1700340
82. G. Choudhary, V. Sharma, T. Gupta, J. Kim, I. You, Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives, in MobiSec 2018: The 3rd International Symposium on Mobile Internet Security, Cebu, Philippines, 2018
83. H. N.Noura, O. Salman, A. Chehab and R. Couturier, DistLog: A distributed logging scheme for IoT forensics, *Ad Hoc Netw.*, **98** (2020), 102061. https://doi.org/10.1016/j.adhoc.2019.102061
84. R. S. Cohen, The Drone Zappers, Air Force Magazine, 22 March 2019. Available: https://www.airforcemag.com/article/the-drone-zappers/.
85. M. A. Siddiqi, H. Yu, J. Joung, 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices, *Electronics*, **8** (2019), 981. https://doi.org/10.3390/electronics8090981

86. G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing UAV communications via joint trajectory and power control, *IEEE Trans. Wireless Commun.*, **18** (2019), 1376–1389. https://doi.org/10.1109/TWC.2019.2892461
87. K. Mizokami, Air Force Downs Several Drones With New ATHENA Laser Weapon System, Popular Mechanics, 8 November 2019. Available from: https://www.popularmechanics.com/military/research/a29727696/athena-laser-weapon/.
88. Federal Aviation Administration, Become a Drone Pilot, Become a pilot, May 19, 2021. Available from: https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot/.
89. Transport Canada, Where to fly your drone, Drone safety, February 19, 2021. Available from: https://tc.canada.ca/en/aviation/drone-safety/where-fly-your-drone.
90. R. Ch, G. Srivastava, T. R. Gadekallu, P. K. Maddikunta, S. Bhattacharya, Security and privacy of UAV data using blockchain technology, *J. Inf. Secur. Appl.*, **55** (2020), 102670. https://doi.org/10.1016/j.jisa.2020.102670
91. Sinha Satyajit, Securing IoT with Blockchain, Counterpoint, 11 May 2018. Available from: https://www.counterpointresearch.com/securing-iot-blockchain/.
92. W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, C. Su, Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices, *IEEE Trans. Ind. Inform.*, 2021. https://doi.org/10.1109/TII.2021.3084753
93. W. Wang, H. Huang, L. Zhang, and C. Su, Secure and efficient mutual authentication protocol for smart grid under blockchain, *Peer-to-Peer Netw. Appl.*, **14** (2020), 2681–2693. https://doi.org/10.1007/s12083-020-01020-2
94. L. Zhang, Z. Zhang, W. Wang, Z. Jin, Y. Su, H. Chen, Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment, *IEEE Syst. J.,* 2021. https://doi.org/10.1109/JSYST.2021.3057333
95. L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, H. Chen, Resource allocation and trust computing for blockchain-enabled edge computing system, *Comput. Secur.*, **105** (2021), 102249. https://doi.org/10.1016/j.cose.2021.102249
96. L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, H. Chen, Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing, *Trans. Emerging Telecommun. Technol.*, (2021), e4315. https://doi.org/10.1002/ett.4315

AIMS Press