Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques

Vinay Chamola*,a,b, Pavan Kotesha, Aayush Agarwalb, Narenb, Navneet Guptaa, Mohsen Guizanici

a Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, 333031, India
b APPCAR, BITS-Pilani, Pilani Campus, 333031, India
c Department of Computer Science and Engineering, Qatar University, 2713 Doha, Qatar

ARTICLE INFO

Keywords:
UAV
Drone
Attacks
Neutralization
Jamming

ABSTRACT

Unmanned Aerial Vehicles (UAV) have revolutionized the aircraft industry in this decade. UAVs are now capable of carrying out remote sensing, remote monitoring, courier delivery, and a lot more. A lot of research is happening on making UAVs more robust using energy harvesting techniques to have a better battery lifetime, network performance and to secure against attackers. UAV networks are many times used for unmanned missions. There have been many attacks on civilian, military, and industrial targets that were carried out using remotely controlled or automated UAVs. This continued misuse has led to research in preventing unauthorized UAVs from causing damage to life and property. In this paper, we present a literature review of UAVs, UAV attacks, and their prevention using anti-UAV techniques. We first discuss the different types of UAVs, the regulatory laws for UAV activities, their use cases, recreational, and military UAV incidents. After understanding their operation, various techniques for monitoring and preventing UAV attacks are described along with case studies.

1. Introduction

Unmanned Aerial Vehicles are becoming popular and are being used for various applications at an accelerating rate [1,2]. UAVs are deployed across various sectors including logistics [3,4], agriculture [5], remote sensing [6], wireless hotspot services [7], smart city applications [8] and disaster management [9]. Notably, UAVs are being used for crowd surveillance, public announcements, and sanitizing public places to help in managing the COVID-19 pandemic [10]. Techniques are also being developed to employ legitimate UAVs for tracking and surveillance of suspicious UAVs [11]. According to the latest Goldman Sachs report, by 2020 there would be 7.8 million consumer UAV shipments and USD 3.3 billion in revenue, versus only 450,000 shipments and USD 700 million in revenue in 2014 in the commercial UAV segment [12]. The market is anticipated to register a Compound Annual Growth Rate (CAGR) of 56.5% from now till 2025 [13]. UAVs are expected to play a huge role in upcoming 5G networks by supporting flexible deployment and backhaul connectivity operations [14,15]. Blockchain and other distributed ledger technologies are expected to enable trusted and transparent sharing of UAVs across different commercial enterprises [16–20]. UAVs are also being used for various military applications such as surveillance, target tracking, air-to-ground combat among many others. The US military spending on UAVs is estimated to be around USD 17 billion from 2017 to 2021 [12]. For such critical applications, the security of wireless UAV-UAV and ground-UAV communications is a must. Security schemes and techniques to ensure essential security features such as mutual authentication and privacy protection, and methods to analyze security vulnerabilities in UAV networks are also being developed [21–26]. There is little doubt that UAVs will play a crucial role in our future societies.

Despite all the advantages of UAVs, they are not free from security vulnerabilities. Even professional UAVs, which are used for critical and sensitive applications such as police operations and enemy surveillance have been shown to possess several security vulnerabilities [27]. When compromised, they can be used by criminals and terrorist organizations for illegal surveillance and unmanned attacks. They may be turned off...
remotely, hijacked, flown away or stolen. [28]. Recent incidents of UAV attacks provide an indication of how devastating they can be. Take, for example, the attack on Saudi Arabia’s biggest oil refinery, Saudi Aramco. In this attack, UAVs targeted one of Saudi Aramco’s facilities and successfully damaged it declining the production by about 5.7 million barrels of oil a day which is about 5 percent of the global production of oil [29]. All this clearly indicates the need for Anti-UAV technologies.

Anti-UAV refers to the process of prevention of potential UAV attacks by either capturing the UAV or jamming its communication channel to disrupt its flight pattern, possibly bring it to a halt on the ground. In this paper, we present a literature review of various anti-UAV techniques. This paper is structured such that we first analyze the classification of UAVs in order to better understand the methods of attacking UAVs. Then we present case studies of deliberate UAV attacks to get more insights into how the UAVs caused damage and how it could have been prevented. Next, we present methods of monitoring UAVs and successively counterattacking them including jamming their communication networks, neutralizing their autopilot software, and more. An overview of the outline of this paper is shown in Figure 1.

2. Classification of UAV

The UAV industry is extensive with a broad diversity. In this section, we have classified UAVs based on various parameters to give the reader an acquaintance with various parameters used for comparing UAVs. This will help in giving the reader a perspective through the rest of the paper. They have been classified on the basis of weight, altitude, and range, wings and rotors, and their application. There does not exist a single classification standard throughout the industry. However, we have provided our classification based on the guidelines set by the Indian Government [30,31].

2.1. Based on Weight

- Nano: UAVs with weight less than 250 gm
- Micro: UAVs with weight greater than 250 gm and less than 2 kg
- Small: UAVs with weight greater than 2 kg and less than 25 kg
- Medium: UAVs with weight greater than 25 kg and less than 150 kg
- Large: UAVs with weight greater than 150 kg

2.2. Based on Altitude and Range

- Hand-held: UAVs that can fly at altitudes of less than 600 m and have a range of less than 2 km.
- Close: UAVs with an altitude of less than 1500 m and range less than 10 km.
- NATO: UAVs with an altitude of less than 3000 m and range less than 50 km.
- Tactical: UAVs with an altitude of less than 5500 m and range less than 160 km.
- MALE (Medium Altitude Long Endurance): UAVs with an altitude of less than 9100 m and range less than 200 km.
- HALE (High Altitude Long Endurance): UAVs with altitude more than 9100 m and indefinite range.
- Hypersonic: UAVs with altitude around 15200 m and range greater than 200 km.

Table 1 summarizes the classification of UAVs based on their altitude and range.

2.3. Based on Wings and Rotors

- Fixed Wing: UAVs that resemble an aeroplane design with fixed wings.
- Single Rotor: UAVs that resemble a helicopter design with one main rotor and another small one at the tail.
- Multi-rotor: UAVs that have more than one rotors. The most commonly found are tricopters, quadcopters, hexacopters and octacopters.
- Fixed-Wing Hybrid VTOL: Hybrid UAVs with longer flight time. They have the stability of fixed-wing UAVs as well as the ability to hover, take off and land vertically. Here, VTOL refers to vertical takeoff and landing.

Table 2 presents a comparison and typical use cases.

| Type of UAV | Altitude | Range |
|-------------|----------|-------|
| Hand Held   | <600 m   | <2 km |
| Close       | <1500 m  | <10 km|
| NATO        | <3000 m  | <50 km|
| Tactical    | <5500 m  | <160 km|
| Medium Altitude Long Range | <9100 m | <200 km |
| High Altitude Long Range | >9100 m | NA |
| Hypersonic  | <15200 m | >200 km|

Figure 1. Outline of this paper
2.4. Based on Application

- **Personal:** Used for applications such as videography and entertainment.
- **Commercial:** Used for applications such as infrastructure monitoring, product delivery, and aerial imaging.
- **Government and Law enforcement:** Used for applications such as firefighting and patrolling.
- **Military:** Used for application such as surveillance and combat attacks.

3. UAV Regulations

As UAV technology is advancing, it has become easily approachable and affordable. Many recreational and commercial UAV pilots are entering the commercial sectors where UAVs are extensively used (e.g., real estate, film making, journalism). As the ecosystem of UAVs is evolving quickly, many countries have come up with laws to regulate the usage of UAVs for various kinds of users. The regulations have evolved with advancements in UAV technology. Certain countries have established certification authorities to certify the usage of a UAV in their air space. In this section, we provide an overview of UAV regulations in various countries as of September 2020.

3.1. United States of America

It is legal to fly UAVs in the United States of America, but one must register their device with the Federal Aviation Authority (FAA) on the FAADroneZone [33] website if the UAV weighs over 0.55lbs (250g). To fly a UAV for commercial purposes, one must obtain certification from the FAA and follow the commercial rules set by the FAA which is discussed briefly below. Our discussion is limited to a few important rules which are applicable in many states in the USA, but there are specific laws for individual states.

Pilots are allowed to fly their UAVs in Class G airspace. According to the United States airspace classification, Class G airspace is airspace from ground to 1,200 feet (i.e., 365 m or less), often referred to as uncontrolled airspace. To fly in controlled airspace, one needs to apply for special permission from airspace authorization authorities.

3.1.1. Recreational/Hobbyist Regulations

If one is flying for hobbies or recreational purposes, they can fly within visual line-of-sight and should not do side jobs or in-kind work. The UAV owner is entitled to follow the community-based guidelines programmed by nationwide organizations like the Academy of Model Aeronautics (AMA). The weight of the UAV cannot exceed 55lbs (25kg), ie., only Nano, Micro and Small UAVs as referred in Section 2.1, can be used for recreational/hobby purposes. To use medium and large UAVs, one needs to get certified by a community-based organization. One cannot fly their UAV near emergency response efforts and can fly only in Class G airspace.

3.1.2. Commercial Regulations

For commercial flying, one is required to acquire a Remote Pilot

---

Table 2: Comparison of different UAVs based on wings and rotors, adapted from [32]

| Type          | Pros                              | Cons                              | Typical Use                      |
|---------------|-----------------------------------|-----------------------------------|----------------------------------|
| Fixed Wing    | Longer flight times at faster speed giving more area coverage | Takeoff and recovery needs large space and no VTOL or hover | Pipeline and Power line inspection, Aerial mapping |
| Multi-rotor   | Easy to use even in confined areas, support VTOL and hover, giving good camera control | Short flight times and small payload capacity | Video inspection and Aerial photography |
| Single Rotor  | Longer flight times with VTOL and hover support, higher payload capability | More dangerous, harder to fly, more training needed, expensive | Aerial LIDAR scanning |
| Fixed-Wing Hybrid VTOL | VTOL and longer flight times | Not perfect at either forward flight or hovering | Delivery through UAVs |

Fig. 2. Classification of UAV based on wings and rotors.
Certificate issued by the FAA. The UAV must fly in class G airspace within visual line-of-sight and weigh less than 55lbs (25kg), including payload, at takeoff. The pilot should ensure that the UAV does not cross a speed limit of 100 miles per hour (160 km/h), an altitude of 400 feet (120 m), and the flight should take place only during daylight or civil twilight. The UAV should not fly directly over people and should not be operated from a moving vehicle. Except for the weight and airspace regulations, there is a provision to waive off the rest of the rules for commercial UAV flights by applying for a special waiver.

3.2. European Union (EU)

As per European Union Aviation Safety Agency regulations [34], if a UAV operator wishes to fly UAV in European Union, they must register if the UAV weighs more than 250 grams or has an attached camera. Every operator who is registering must complete training to receive a certificate, which is valid in other EU countries as well. The regulation number needs to be displayed with a sticker on all the UAVs you own including those privately built.

The pilot should always keep the UAV in line of sight, and shouldn’t fly higher than 120 meters altitude, close to other objects, airports, or above groups of people. The UAV operator cannot intrude anyone’s privacy by capturing photographs or videos without their permission. EU has released new rules for UAV operators which will be effective from December 31, 2020. As per the new system, the UAVs will be categorized under the specified 3 categories (Open, Specific, and Certified). The category is based on the risk of the flight. This risk is determined by the weight of the UAV and the location of the flight. Depending on the flight category a remote pilot may need certain permits or certificates.

3.3. Australia

It is legal to fly UAVs in Australia. As per Australia’s Civil Aviation Safety Authority (CASA) regulations [35], the pilot should fly the UAV only during the day and keep it within a line of sight, i.e., the UAV should be visible within the line of sight of the naked eye and not through any device. The pilot should ensure that the UAV does not fly above an altitude of 120 m and the UAV should always be at 30 m distance from people or objects. One should avoid flying the UAV near emergency operations, over gatherings and densely populated areas. A single pilot can fly only one UAV at a time and cannot fly over people, including sports events, beaches, etc. If the UAV weighs more than 100 g, one must keep at a distance of 5.5km from aviation airfields, commercial airports, and airbases of the military. Violating anyone’s privacy makes the pilot come under the purview of state laws. CASA also released an official mobile application, “Can I fly there?” to determine whether one can fly a UAV in a particular area for recreational or commercial purposes.

3.3.1. Commercial Regulations

Those flying devices weighing over 2kg (4.5 lbs) for commercial purposes, has to inform CASA and apply for an aviation reference number and fly within the standard operating conditions. To fly outside the CASA listed standard operating conditions which are described in the previous paragraph, one needs to acquire a RePL (Remote Pilot License) and fly with a certified pilot.

3.4. United Kingdom

As per the Civil Aviation Authority of the UK (CAA) regulations [36], one should always keep the UAV in direct visual sight, to avoid any collision, especially with other aircraft. All UAVs, irrespective of their weight, should not fly 122 m above the surface. There are further regulations for those UAVs with an attached camera. The pilot shouldn’t operate the UAV anywhere near populated areas or assembly of 1000 persons by maintaining a minimum distance of 150 m from these areas.

The pilot should avoid flying the UAV within 50 m of any person or object which is not under his/her control. The pilot should not operate the UAV within a 5km radius of an airbase, be it the commercial airport or military airbase. One should not attach any payload that can cause damage by dropping it over anyone or anything on the ground.

3.4.1. Commercial Regulations

To perform Commercial UAV operations in the UK one needs to take permission from the CAA. CAA makes it mandatory for all commercial UAV operations to have insurance. For foreign operators to carry out commercial work, CAA will normally be able to grant permission, with the pre-condition that they are ready to meet the basic safety requirements that are necessary for the regular U.K based UAV operators.

3.5. Norway

As per the Civil Aviation Authority of Norway (CAAN) regulations [37], the UAV pilot must maintain visual contact with the aircraft throughout the operation. UAVs cannot fly over festivals, near accident areas, military areas, sporting events, and cannot go near the 5 km radius of any airport. They should also avoid flying near traffic, people, and buildings. The pilot should ensure that the UAV does not cross an altitude of 394 feet (120 m) above the ground. The pilot is liable for action if found disturbing others’ privacy by taking photographs or videos.

3.5.1. Commercial Regulations

To perform any commercial UAV operations in Norway, one should register themselves with the CAAN. Norway has divided the regulations for commercial operators, referred to as RO (Remotely Piloted Aircraft Systems Operators), into three categories: RO 1, RO 2, and RO 3. Table 3 shows the regulations for each of these categories. RO 1 and RO 2 regulations apply to Nano, Micro, and Small UAVs. RO 3 regulation applies to Medium and Large UAVs.

3.6. India

As per India’s national aviation authority regulations [38], foreigners are currently not allowed to fly UAVs in their country. India uses the classification of UAVs based on the weight mentioned in Section 2.1, namely, Nano, Micro, Small, Medium, and Large during their official registration. Except the Nano UAVs, all others need to acquire Unique Identification Number (UIN) by registration. The pilot should always maintain a visual line of sight and shouldn’t fly the UAV 400 feet (120 m) above ground level. UAVs are restricted to fly over no-fly zones like airports, borders, military bases etc. The aviation authority prescribes specific mandatory features for UAVs (excluding Nano category) like Global Positioning System (GPS), Return-to-Home (RTH), anti-collision light, identification (ID plate), a controller with flight data logging, radio frequency identification (RFID) and Subscriber Identity Module (SIM). Every UAV that fly in India should have these prescribed features.

3.6.1. Commercial Regulations

To fly UAV for commercial purposes in India, one should hire an Indian entity who can operate their UAV and that entity needs to obtain the Unique Identification Number from the Directorate General of Civil Table 3
Norwegian Remotely Piloted Aircraft Systems operators regulations

| Category  | Max mass | Max speed | Acceptable Line of Sight          |
|-----------|---------|----------|----------------------------------|
| RO 1      | Up to 2.5 kg | 60 knots | Visual line of sight            |
| RO 2      | Up to 25 kg  | 80 knots | Extended line of sight           |
| RO 3      | 25 kg or more | 80 knots | Beyond visual line Of sight      |

1 knot = 1.85 kilometers per hour
Aviation (DGCA). Except for Nano category flown below 50 feet and Micro category flown below 200 feet, every commercial operation with a UAV in India should be executed only after obtaining a permit from DGCA.

3.6.2. No Permission No Takeoff Policy (NPNT)
Having registered on [39] platform, all pilots should request permission before every flight through their mobile app. Based on the acceptance or rejection from the platform, one can proceed with their flight.

4. Recreational UAVs and Malpractices

UAVs find applications in various industries like logistics, structural monitoring, automation, and agriculture [40]. They reduce the cost and provide simpler solutions to problems like generating climate data, monitoring borders, watering of crops, airborne inspection of structures like pipes, etc [12]. Some of the major manufacturers of UAVs in the field are DJI, Yuneec, Parrot, and Sensfly. Table 4 presents a list of popular UAVs and their specifications. Unfortunately, unlike military UAVs, these solutions do not always undergo vigorous security testing, because the implementation of security features increases the product development time and costs, thereby decreasing revenue for the manufacturing company. Additionally, enhanced security measures might make it difficult for general consumers to operate the UAV. The Internet of Things (IoT) ecosystem has its own set of security challenges [41–43]. There is a possibility that UAV-IoT ecosystems providing aerial IoT services [44] might inherit the same security challenges. Several security vulnerabilities like the possibility of hijacking, jamming of a UAV in flight, disabling the UAV, etc. have been reported for many of the popular UAVs available in the market [45]. Since the vulnerabilities are publicly available, this type of UAVs has a high possibility of misuse. Cyber attacks on industrial facilities are not very uncommon [46]. With UAVs expected to be an integral part of the industrial workforce, it becomes necessary to ensure high levels of security to ensure smooth industrial operations.

Generally, hobby-level UAVs (Micro and Small UAVs, Section 2.1) have 0.3 to 2 kg of payload capacity. These UAVs can carry a payload, which can be lethal objects like explosives and biological hazards. Even the UAV itself can be rammed into objects to cause damage. Although various countries have set up regulations to prevent such misuses, their enforcement is difficult. In many cases, it may not be possible to identify the owner or UAV operator who may have been operating the UAV from a remote location. Hence, having anti-UAV systems, which are discussed in Section 9, are very important and need to be widely deployed.

The following subsections discuss various malpractices using hobby, commercial, and personal UAVs which have been classified as in Figure 3. Reference [47] provides a list of incidents and intrusions from around the world using hobby, commercial, and personal UAVs. Additionally, Table 5 presents the risks posed due to UAVs in airports, rescue operations, prisons, offices, residences, and patrols.

4.1. Disruption by Collision

According to the United States National Inter-agency Fire Center, aerial firefighting efforts were shut down a minimum of nine times, and a minimum of twenty UAV incursions had hindered firefighting capabilities within the US from January to October in the year 2019. Even though a bill was passed in 2015 by the US legislature, allowing firefighters to neutralize UAVs that interrupted their efforts to handle fires, and also imposing and creating penalties for UAV pilots who interrupted with firefighters, the UAV appearances in such rescue operations have continued to exist [48].

Beyond firefighting efforts, UAVs are known to interfere with airport traffic. Despite being small, UAVs they can cause expensive disasters if they come in collision with a large aircraft. Collisions with an engine, wing or any part of an airplane can cause severe damage. In 2017, a small UAV collided with a commercial airplane flying towards Quebec City in Canada. Although the plane landed safely, this incident introduced concerns about the collisions between unmanned aerial vehicles with commercial aircraft, following which the regulation of UAVs has increased [49].

A 2017 Federal Aviation Administration (United States) study [50] found that UAVs colliding with large aircraft can cause more damage than birds, a threat which the industry has long faced. Unlike the soft

| Company       | Country | UAV Model          | Flight Time | Weight | Max Resolution | Price*  |
|---------------|---------|--------------------|-------------|--------|----------------|---------|
| Parrot        | France  | Bebop 2            | 25 mins     | 500 g  | 1080p@30fps    | USD 599 |
| DJI           | China   | Phantom 4 Pro V2   | 30 mins     | 1375 g | 4K@60fps       | USD 1599|
| DJI           | China   | Mavic Air 2        | 34 mins     | 570 g  | 4K@60fps       | USD 799 |
| Yuneec        | China   | Typhoon H3         | 25 mins     | 1965 g | 4K@60fps       | EUR 299 |
| 3D Robotics   | USA     | H520-G             | 28 mins     | 1645 g | 4K@60fps       | USD 599 |

* Prices as of 1st August 2020
There have been multiple instances where UAVs were used to deliver contraband like narcotics, ammunition, and cell phones into prisons by flying over the walls. In March 2019, a UAV along with contraband was discovered at the Collins Bay Institution correction facility in Ontario, Canada. The regional president for the Union of Canadian Correctional Officers also stated that similar practices were being carried out at other facilities as well. The countermeasures to prevent these further were not made public to prevent exploitation [52]. There have been similar incidents in London, Ohio, New York, and many more. UAV detection technologies like audio, video, and radio monitoring, which are discussed in later sections have been deployed across prisons to prevent such incidents [53].

4.3. Cyber Attacks

UAVs can be modified and additional components can be added to use it as a mobile hacking tool. In [54], a single board computer with a 3G connection and a WiFi packet injector was added to an Parrot AR Drone to create a botnet. Weakly protected WiFi networks were detected by the UAV, their information was sent to the cloud over a 3G network. This has been misused a lot for several operations [51].

4.4. Spying

Many UAVs have a high definition camera attached to it for transmitting live footage to the user. This has been misused a lot for several illegal activities. In December 2016 in Orem, Utah, United States of America a UAV was recovered with video captured of several people in their homes [56]. It has also been reported that UAVs are used to track law enforcement officials to anticipate their movement, find windows, and plan crimes (especially robberies). Similarly, at national borders, they have been used to track border patrols so that they can be avoided while crossing [57].

4.5. Terrorist activities

4.5.1. Caracas Drone Attack

Two UAVs carrying explosives were detonated near Avenida Bolívar in Caracas, Venezuela where Nicolás Maduro, the President of Venezuela was giving commemorations in the middle of a speech to the Bolivarian National Guard on August 4, 2018. The UAVs were reported to be the DJI M600 model loaded with C4 plastic explosives and gun powder. Though the president was unharmed, some National Guard soldiers were injured. Later, a terrorist group made posts on social media claiming responsibility for the attack [58]. This shows that UAVs are available without regulation and they can be easily used as tools for terrorism.

4.5.2. Abqaiq - Khurais Attack

A group of 10 UAVs launched from Yemen, attacked Saudi Aramco oil facilities at Abqaiq and Khurais on 14th September 2019 in Eastern Saudi Arabia. The UAVs attacked the refineries and caused large fires, which were put out several hours later. Due to this, both the refineries were shut down and Saudi Arabia lost half of the oil production (5% of the total supply of oil in the world). Due to this shortage, the international crude oil prices rose by more than 12% the following day. A terrorist group claimed responsibility for this attack. Samad 1, an autopilot fixed-wing type Kamikaze (suicide) UAV was used in this attack to carry explosives. Saudi Arabia’s missile defense systems in Abqaiq were designed against high flying targets and hence could not detect these UAVs which flew at lower altitudes [59].

5. UAVs in Military Attacks

Military have been using aerial attacks for more than 150 years. Such attacks were first observed in 1849 in besieged Venice when the Austrians attempted to drop bombs over the city by attaching them to balloons with a time fuse. After that, during World War I, the American military developed the earliest prototypes which are modified versions of aeroplane that can hit specific enemy targets.

Advancement in Radio control allowed the UAVs to be operated in real-time. American designed Curtiss F-5L is the first aircraft [61] controlled remotely which made its successful takeoff, maneuver, and landing in September 1924 completely guided in real-time. Using similar radio control technology, US Navy conducted a torpede attack using Curtiss TG-2 in April 1942 during a test strike on practice warship.

In 1970, the Ryan Aeronautical Company produced a new UAV named BGM-34A, which was developed based on their early 1960s reconnaissance UAV model. This UAV became the first Unmanned Combat Aerial Vehicle (UCAV) [62] which successfully launched air to surface guided missile hitting the target. In the later part of this section, some of the recent attacks using such UAVs have been discussed in depth.

UAVs are used for a wide variety of military applications like reconnaissance/scouting (the military observation of a region to locate or ascertain enemy forces), surveillance, and intelligence. UAVs are extensively used in reconnaissance missions because of the high degree of risk involved in manned missions. Although traditionally UAVs were used only for reconnaissance and surveillance purposes, they are now being used for conducting strikes, rescue missions, and for other miscellaneous applications in the military. Table 6 shows the details of top military UAVs based on payload capacity and weapons on board. With recent improvements in IMUs (inertial measurement units), cameras, and flight control systems, UAVs find a variety of military applications and are fast replacing manned aircraft and satellites [63].

Till date, more than ten countries have conducted UAV strikes. Figure 5 shows a map of various countries that have already conducted UAV strikes. Many other countries, including Saudi Arabia, India, and China, among others, maintain armed UAVs in their arsenals. Figure 4 shows a map of countries that have acquired armed UAVs. References [64-66] provides some insights into military UAV attacks conducted on countries like Pakistan, Afghanistan, Yemen, Iraq, Syria, Somalia etc.

The USA, UAE, Israel, UK, Italy, and Greece were some of the first countries to develop armed UAVs [60]. Figure 6 shows various countries that have now developed armed UAVs. USA and Israel are the largest producers and sellers of UAVs. America’s leading UCAV is the MQ-9 Reaper (manufactured by General Atomics), which has served operations around the world for more than a decade. The MQ-1 Predator, which served the United States Air Force for more than 21 years retired in 2018. Israel’s leading UCAV is IAI Heron and is the largest UAV exporter in the world, accounting for 41% of UAV exports from 2001 to 2011. Along with their popular model CH-3, China also developed the CH-4 and CH-5 models. India is a major UAV importer. It accounted for 22.5 percent of all UAV imports from 1985 to 2014. Also, India has its very own Rustom range of UAVs. The Rustom has 3 variants, namely, Rustom-I, Rustom-H, Rustom-II (or TAPAS-BH-201). Rustom-I has been tried and tested several times (on at least 15 different occasions) and has had several successful flights. Rustom-II has been designed to conduct reconnaissance and surveillance roles for the Indian Armed Forces.
5.1. Damadola Attack

This attack was carried out on Jan 13, 2006. It involved four Central Intelligence Agency operated unmanned MQ-1L Predator UAVs that launched AGM-114 Hellfire missiles into the Pakistani village of Damadola about 7 km from the Afghan border. The attack purportedly targeted the leader of a terrorist group, who was suspected to be in the village [67].

5.2. Miramshah Airstrike

This attack was carried out in 2008 September in Miramshah in North Waziristan, Pakistan. This was targeted at militants and carried out by the United States Air Force UAV named Predator B (MQ 9-Reaper) capable of high-altitude surveillance, air-to-ground missiles, and laser-guided bombs. The missile released by the UAV hit two buildings and killed militants [68].

5.3. Makin Airstrike

The 2009 Makin airstrike is one of the deadliest UAV attacks since such operations were started by military forces. It was conducted by a US military UAV targeting militants in a funeral procession in the Makin city of South Waziristan, Pakistan, killing several militants [69].

5.4. Hmeymim Air Base

Hmeymim Air Base operated by Russia has been under multiple UAV attacks. It is located near Latakia in Hmeimim, Latakia Governorate, Syria, which is very close to the Bassel Al-Assad International Airport. On September 27, 2019, a Russian Defense Ministry spokesman said that the air defense and electronic warfare systems deployed at the Hmeimim airbase shot down or disabled 118 unmanned UAVs during terrorists’ attempted attacks on the military facility over the previous two years. The first attack on this airbase was on January 6, 2018 when 13 combat fixed-wing UAVs attacked the base. For some of these UAVs, the control signals were overpowered and control was obtained, while others had to be destroyed by short-range Pantsir-S1 anti-aircraft missiles [70]. Radars for detection and a combination of short-range and long-range missiles were used [71].

6. Preliminary Background of Wireless Communication

In this section, we provide a preliminary background of wireless communications necessary to understand UAV operations, UAV monitoring, and UAV neutralization techniques. We begin by discussing spread spectrum which is the concept targeted throughout the rest of the paper.

6.1. Spread Spectrum

There are several basic modulation techniques such as frequency modulation, amplitude modulation and digital modulation. However, such modulation of the original message signal on a fixed carrier wave makes the resultant signal wave vulnerable to tampering and jamming. Such a modulated wave can also be demodulated by anyone to get the...
original message signal. Spread spectrum is a modulation technique which protects the message signal from interference, environmental noise, and jamming. It also ensures secure communication and reduces the probability of signal detection. In spread spectrum techniques, the original narrow-band message signal is modulated with an independent wide-band code signal. The resultant signal thus has a higher bandwidth and the original message signal is "spread" over a wide range of frequencies. At the receiver end, the same wide-band code signal is used to "de-spread" the transmitted signal to get back the original narrow-band message signal, as shown in Figure 7. In the following discussion, we briefly explain four major variants of spread spectrum techniques which are often used in wireless UAV communications: Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum, Time Hopping Spread Spectrum and Chirp Spread Spectrum.

6.1.1. Direct Sequence Spread Spectrum (DSSS)

DSSS is the most fundamental form of spread spectrum techniques. In this type, the message or signal wave is spread by modulation using a wide band code known as the Pseudo Noise (PN) code. This PN code consists of a radio pulse with a very short duration and thus higher bandwidth when compared to the signal wave. Figure 8 shows how the signal wave gets spread by the PN code.

Spreading on the PN code results in the original signal wave getting distributed over a much wider range of frequency bands and causes the modulated signal to have a bandwidth almost identical to the PN code. The smaller the duration of the PN code, the larger the bandwidth over which the data signal gets modulated, and thus higher the system resistance to outside interference. DSSS systems generally employ an additional modulation through Binary Phase Shift Keying (BPSK) modulation or Quadrature Phase Shift Keying (QPSK) modulation. Phase shift keying is a modulation technique by which the data bits are expressed as phases in the signal wave. BPSK expresses each 0 or 1 in the data as 0° or 180° phase shifts in the carrier wave, respectively, whereas in QPSK two bits are considered at once and expressed as 0°, 90°, 180° or 270° phase shifts. To summarize, in DSSS the data signal first gets modulated with the PN code followed by phase shift keying over a carrier wave.

6.1.2. Frequency Hopping Spread Spectrum (FHSS)

In FHSS communication systems the data signal is modulated onto a carrier signal, whose frequency is rapidly switched among different channels. A pseudo-random sequence generator passes a sequence to a frequency synthesizer that generates the frequency of the carrier wave used for spectrum spread. The frequency of the carrier wave is increased (upchirp) or decreased (downchirp), respectively, whereas in MFSK two bits are considered at once and expressed as 0°, 90°, 180° or 270° phase shifts. To summarize, in DSSS the data signal first gets modulated with the PN code followed by phase shift keying over a carrier wave.

6.1.3. Time Hopping Spread Spectrum (THSS)

In THSS, the input signal is not sent continuously. Instead, it is broken into fragments and sent in pulses and 2M discrete pulses are used as carrier signals to transmit k bits/pulse. A transmission window of duration x is divided into n segments and the signal is sent in one of the n segments (which varies with time). Figure 11 presents the discrete signal pulses, over a period of time. The resistance to interference is achieved by randomly varying the transmission time by pseudo-randomly changing the carrier pulse period and duty cycle. In a strict sense, time hopping in itself does not introduce any spread spectrum characteristics. Hence it is generally used in the hybrid spread spectrum with FHSS.

6.1.4. Chirp Spread Spectrum (CSS)

CSS, unlike DSSS or FHSS, does not employ any pseudo-code generator. Instead, CSS relies on its unique way for varying the frequency of the carrier wave used for spectrum spread. The frequency of the carrier wave is increased (upchirp) or decreased (downchirp)
according to various mathematical functions. The chirp spread spectrum utilizes the entire bandwidth allocated to transmit a signal and hence achieves robust performance against interference. Figure 12 shows an upchirp CSS whose frequency increases linearly with time.

6.2. Processing Gain

The higher bandwidth achieved by the transmitted signal in spread spectrum gives it resistance against interference. The ratio of the bandwidth of the modulated signal to that of the original data signal is referred to as the Processing Gain ($G_p$) of the system. This gives a quantifiable measure to the system’s resistance to interference.

The basic idea behind this is that by increasing the bandwidth of the signal we are making it inefficient for a malicious jammer to interfere with the signal. Since there is limited power in the hands of a jammer, it will have to distribute the fixed power for transmission of the interference over a wide range of frequencies, thus introducing very little interference in a particular section of the signal. On the other hand, if the jammer transmits all its power on a particular section of the signal, the rest of the signal remains free of any interference.

6.3. Jamming Margin

The level of interference that a spread spectrum system can handle and still be able to perform at par with a specified level of performance is measured with the help of the jamming margin. It depends on the processing gain, system implementation losses and the minimum SNR ratio required at the receiver for error-free information transmission.

7. UAV Operation

In this section, we present a discussion of the various aspects of UAV operation such as the modes, flow of control, systems for navigation, and also review some of the most common commercial transmission protocols.

7.1. Mode of Operation

Depending upon their mode of operation, UAVs can be classified as manual, partially autonomous, and fully autonomous.

7.1.1. Manual

Most traditional applications of UAVs involve manual remote radio control over the flight of the UAV and its traversed path. In this, the pilot tunes the flight controller parameters to adjust stability and maneuverability. The most common method of doing so is by using a PID (Proportional Integral Derivative) control loop which provides three parameters described in Table 7. Error refers to the difference between the actual and intended values.

Applications based on manual operation occasionally involve the transmission of payload signals such as video feedback or positional information. UAVs in such scenarios can be detected and neutralized using different RF spectrum jamming techniques which are discussed in Section 9.

7.1.2. Full and Partial Autonomous

As the complexity of operations performed using UAVs increases, many tasks are being offloaded to the onboard flight controller. In the case of a partially autonomous system, the controller takes care of the low-level tasks of the mission such as collision detection and altitude control. The high-level mission constraints and parameters such as way-points are controlled by a human operator. Thus, instead of human or manual control, the system uses different sensors such as inertial measurement units, pressure sensors, etc. to determine the current state of the system and maintain properties such as altitude of the UAV. On the other hand, a fully autonomous system application would involve a completely autonomous execution of the mission, without necessarily involving the transmission/reception of RF signals to/from the ground station. A typical example would involve a pre-programmed flight route.

In most of these autonomous applications, it is necessary for the UAV to track its current location in order to facilitate the higher level mission objectives. This is done with the help of a global navigation satellite system (GNSS) receivers such as GPS. Such systems can be identified and neutralized using GNSS/GPS jamming.

For certain, in the cases of fully autonomous applications, it is possible that there is no transmission of signals with the UAV, or it becomes difficult to analyze the RF frequency spectrum reliably. In such cases, radar-based techniques are used to detect unauthorized UAVs.

7.2. Basic Working Mechanisms

Major components of an UAV include propellers, motors, frame, sensors, speed controllers, flight controller, receiver, and battery pack. Besides the UAV, the ground station and intermediaries needed for communication also play a vital role. Figure 13 shows the various components of UAV along with their interaction with each other.

The frame of the UAV is a simple, lightweight, aerodynamically efficient and stable platform with limited space for on-board electronics. The material and structure of the frame is very important as defects in it

| Parameter     | Purpose            | Effect                                                                 |
|---------------|--------------------|------------------------------------------------------------------------|
| Proportional  | Deals with present error | Increasing this parameter increases sensitivity of the UAV. Too high a value can make it difficult to control the UAV. |
| Integral      | Deals with past errors | Increasing this decreases wobbling of the UAV. Too high a value can make the UAV too rigid. |
| Derivative    | Deals with future errors | Increasing this counteracts the over-sensitivity caused due to the proportional gain parameter preventing sudden movements. Too high a value can cause vibrations in the UAV leading to overheating. |
can disrupt the UAV’s operation in several ways. A heavy frame decreases the payload capacity, and a skewed frame will create problems in the stability of its flight. UAV frames are constructed mostly using carbon/graphite fibers or thermoplastics such as polyethylene, polystyrene and polyether-ether-ketone (PEEK). A manual UAV receives commands from the pilot through a transmitter and receiver working over various technologies like radio, Wi-Fi, and Zigbee based on various radio protocols like DSMx, A-FHSS, etc. After receiving the signal from the radio transmitter, the radio receiver converts them to electrical signals in Pulse Width Modulation (PWM) or Pulse position modulation (PPM) format. These signals are interpreted by the flight controller whose commands are converted into specific actions for controlling the UAV. For rotor based UAVs, the Electronic Speed Controller (ESC) takes the signal from the flight controller and power from the battery and adjusts the speed of the motors to control the flight. For fixed-wing UAVs, servo motors are used to precisely control the angle of the wings which in turn controls the flight. Besides the commands, there is an additional transmitter-receiver pair that transmits crucial information like battery voltage reading and radio signal strength to the ground station, termed as telemetry. A ground station is the control center that facilitates the human control of UAVs.

An autonomous UAV has a predefined flight route based on GNSS systems like GPS or environment checkpoints which can be detected by the camera. The UAV can roughly track its position relative to its initial position by using onboard IMU sensors. It corrects its position based on visual checkpoints and GPS confirmation.

7.3. Systems for UAV Navigation

UAVs operating in different modes follow different principles for their navigation. Manual UAVs usually receive signals from the pilot, partially autonomous from the pilot, GNSS system, and sensors, whereas completely autonomous ones have capability for flight without pilot intervention.

1. Direct radio for remote control:
   This type of communication method involves a human operating a radio transmitter/receiver, a smartphone, a tablet or a computer as a ground station to control the flight path of the UAV. UAVs using this type of communication can fly only in the line of sight of the operator, and hence, these types of UAVs are generally short-ranged.

2. Satellite Navigation:
   This type of communication involves UAVs communicating with a GNSS system. UAVs using this type of communication are generally long-ranged. A very common GNSS system is GPS. GPS navigation is provided using more than 30 satellites continuously revolving in their fixed orbits around the earth. Each satellite has a stable atomic clock which is synchronized with others and to a base station which updates the time with respect to the ground. For knowing the position accurately, a signal from at least 4 satellites needs to be received. The navigational message includes the Almanac data and Ephemeris data. The Ephemeris data has information regarding the location and time of each satellite in the orbit. Almanac message include data regarding the entire constellation of satellites. Hence, these messages from satellites are used by the GNSS receiver to find its location and time using the trilateration method.

3. Relay:
   In system, another aircraft that is always in a definite range of the UAV serves as a relay to give flight control. Sometimes, the other aircraft can itself be a UAV which is controlled through either satellite navigation or remote control. This type of relay communication is witnessed in swarms of UAVs. Swarms are a very upcoming topic which can implement secure communication using blockchain over technologies like Software Defined Networking which give secure flexibility to the network architecture [73–80].

4. Sensors:
   Various sensors such as ultrasonic, LiDARs and cameras are used for sensing distance from the objects in the environment whereas IMUs are used to track the orientation of the UAV over 9 degrees of freedom. Barometers are also used to track altitude of the UAV. All of these sensors are used in combination to give feedback to the flight controller for stable flight. These sensors are used to implement localization through Simultaneous Localization and Mapping (SLAM) algorithms or deep learning approaches [81–84].

7.4. Popular Transmission Protocols

Transmission (Tx) protocols are implemented in the wireless communication between the transmitter and the receiver. A transmission protocol is defined by the structure of its data packets, and the type of spread spectrum and encryption scheme it uses. Some major UAV manufacturers implement the same protocols across all of their UAVs. These are of utmost concern for the security analysis of a UAV. Some of
the most popular Tx protocols include MAVLink, Digital Signal Modulation (DSM), Automated Frequency Hopping Digital System (AFHDS) and Futaba Advanced Spread Spectrum Technology (FASST). Table 8 presents a list of popular transmission protocols used for UAVs. The organisations that use these protocols generally use the same Radio Frequency Integrated Circuit in their implementations. This documentation of these RFICs can be looked into for vulnerabilities like default passwords and behavior on disconnection. It is worth noting that MAVLink is an Open Source Tx protocol and thus has been thoroughly explained in literature whereas descriptions of other protocols are not readily available. This makes MAVLink easier to analyze compared to other protocols.

7.4.1. MAVLink

The Micro Aerial Vehicle (MAV) Link protocol is a very lightweight messaging protocol used to carry telemetry, and to command and control multiple UAVs. MAVLink follows a modern hybrid publish-subscribe and point-to-point design pattern. In the publisher-subscribe model, we have a central broker that manages various topics to which clients either subscribe (listen to messages) or publish (pass messages). When a particular message is published on a topic, all subscribers receive that message. On the other hand, in the point-to-point model, messages are sent directly between the sender and the receiver. Therefore, in MAVLink, message data packet has just 14 bytes of overhead as shown in Figure 14 [85].

Table 8
List of Popular Transmission Protocols

| Manufacturer | Protocol    |
|--------------|-------------|
| Spektrum     | DSM2        |
|              | DSMX        |
| Futaba       | S-FHSS      |
|              | FASST       |
| FrSky        | ACCST       |
| FlySky       | AFHDS2      |
| Syma         | SymaX       |
| DJI          | DESST       |
| Walkera      | Devo        |

7.4.2. Digital Signal Modulation 2

The Spektrum DSM2 technology operates in the 2.4GHz band and uses wideband DSSS. DSM2 uses DualLink technology that is based on the use of two channels. The DualLink technology assists recovery from polarization blind spots and reflected signal fading. Upon switching on, the DSM2 based transmitter scans for two free channels in the 2.4GHz band. On finding them, the transmitter transmits it’s distinct Globally Unique Identifier (GUID) in these channels. Subsequently, on receiving the GUID, the receiver locks on to these two free channels [87]. In case one of the channels is noisy, the other channel acts as a backup. This lowers the chance of disconnection of the signal significantly. However, if both channels become unusable, the connection might be lost [88]. Hence, the DSM2 signal provides additional resistance to noise, interference and other transmitters transmitting on the same frequency.

7.4.3. Digital Signal Modulation X

The Spektrum DSMX is based on DSM2 and is a successor to it. DSM2 and DSMX transmitter receiver pairs are compatible with each other. Firstly, an important feature of DSMX, similar to DSM2, is the wide-band signal which compared to the narrow-band signal of other 2.4GHz transmitters, is more resistant to interference and a has a higher SNR.

Secondly, unlike DSM2, DSMX employs Frequency Hopping Spread Spectrum. DSMX transmitters have their own unique frequency shift pattern calculated using their GUID and each pattern uses just 23 channels in the 2.4GHz spectrum. Lastly, it uses DualLink technology as well [89].

7.4.4. Automatic Frequency Hopping Digital System

The Flysky Automatic Frequency Hopping Digital System (AFHDS) is a digital protocol that ensures two or more transmitters can operate at the same time without interfering with each other’s respective communication. AFHDS 2A is the second generation of the system that added duplex communication capability and telemetry capabilities [90]. AFHDS-2A supports up to 14 channels and requires manual-binding. It offers options to change the reception (Rx) protocol for the receiver, servo frequency, the Link Quality Indicator output (an indication of the quality of the data packets received by the receiver based on the receiver signal strength), and the fine-tuning of the operational frequency [91]. AFHDS 3 is the latest generation of the protocol and allows automatic frequency hops in the range of 2.402GHz to 2.481GHz. However, depending on the outcome of the initial transmitter-receiver pairing, the frequencies actually in use and hopping algorithm change. Moreover, each time the system is powered on, the frequencies and hopping algorithm change as a security measure.

7.4.5. Futaba Advanced Spread Spectrum Technology

Futaba Advanced Spread Spectrum Technology (FASST) is the Tx protocol of the Japanese company Futaba and is used not only in the RF products of Futaba, but also as a part of products made by other manufacturers, such as the DJI Phantom 2. It uses the 2.4-2.485 GHz frequency band with the minimum bandwidth of the channels as 1.1 MHz and sidebands of up to 2 MHz. FASST implements frequency hopping, Gaussian frequency-shift keying, and sometimes a combination with DSSS which significantly increases resistance against interference or jamming. It also has different modes of usage providing 7, 8 or 14 transmit control channels. It’s successor FASSTEST also employs duplex communication [92].

8. UAV monitoring

There are various methods for monitoring the presence of UAVs and plan counter attacks. It is an important field that is growing with the rapid increase in UAVs. Both industry and academia are working on the
implementation of available methods and coming up with new ones. UAV monitoring has mainly four operations:

1. **Detection**: Sensing the presence of a UAV.
2. **Identification**: Verification and analysis of the UAV and its properties.
3. **Localization**: Tracking the position of the UAV.
4. **Responding**: Taking actions like broadcasting a warning, neutralizing or alerting.

Not all of the various approaches for UAV monitoring can efficiently do all the aforementioned operations. Approaches for detection, identification and localization are discussed in this section which can be classified as in Figure 15 and summarized in Table 9 at the end of this section. Implementation of neutralization as a method for responding is discussed in Section 9.

### 8.1. Radar

Radar-based techniques are usable in the case of partial or completely autonomous UAVs where no radio communication takes place. For detection by radar, generally, radio waves are transmitted, which on reflection from an object undergo reflection and change in place. For detection by radar, generally, radio waves are transmitted, properties such as polarization. Based on the properties of received waves, information about the presence of an object can be calculated. Doppler radars are able to detect motion, specifically speed differences within moving objects. As UAVs have major moving parts like propellers which create a large spectrum of linear speed differences, this is a good approach. Millimeter-wave radars, ultra-wideband radars, and non line-of-sight radars are some of the applicable radar technologies [93,94].

### 8.2. Radio Frequency Analyzers

In this method, the RF waves coming from the UAV are intercepted. Generally, a manually operated UAV communicates with the ground station (GS) and a GNSS for its operation. Both of these may be absent for an autonomous UAV working solely based on on-board sensors.

Methods like FHSS are often applied for the communication between the GS and the UAV. However, for most commercial UAVs, an AI-based classification algorithm can be implemented which analyzes the spectrum using Software Defined Radio (SDR) and based on features such as the hopping sequence, predicts the presence of a UAV along with details about it [95–97]. Also, based on the signal strength, it is possible to track and localize the UAVs. Besides these, the UAV may be transmitting information about itself like its coordinates and video feed which can be intercepted and analyzed for localization.

These methods have a good detection range depending on the transmit power of the UAVs. However, they tend to be expensive. Software defined radio is a recent technology that will reduce the cost of this approach [98].

### 8.3. Video Surveillance

Another approach for detecting and monitoring UAVs is by using computer vision. Video surveillance from strategically placed cameras in an area can be passed though deep learning models trained to detect and track UAVs. These deep learning models are trained with datasets of images and videos of UAVs from which they eventually extract the features which help in distinguishing and tracking UAVs. The models could be based on either identifying the appearance of UAVs or their motion. Multiple cameras with a varying field of views can be used for faster detection [99,100]. For situations when the ambient light is low, it is hard for normal systems to carry out detection due to a lack of contrast and features. In such scenarios, thermal imaging can be used [101].

### 8.4. Audio Surveillance

In this approach, the various sounds made by a UAV due to its moving parts like motors, propellers, and chassis vibration are analyzed using machine learning and deep learning classification approaches to detect its presence. UAV sounds can be recorded in control environments to make datasets that can further be augmented using noisy environments to simulate real environments. With these augmented datasets, various models based on support vector machines (SVM) and neural networks can be developed for UAV detection [102-104]. Besides these, fundamental audio processing approaches such as audio fingerprinting may also be used [105]. It is also possible to track the position of UAVs by using multiple microphones with methods like triangulation.

Better results can be availed by combining two or more of the aforementioned methods, such as cameras along with microphones assisting each other in their operation. A system can be designed which uses the acoustic sensors to identify UAVs by audio fingerprinting along with identifying the direction of the source, after which the camera can rotate to spot the target [106,107].

Once the UAV is successfully detected and localized, the next step is to take the appropriate response action. The response action depends on the extent to which it is detected, identified, and localized.

### 9. UAV Neutralizing Techniques

Based on the mode of operation (i.e., manual, full, and partially autonomous), different situations necessitate different approaches for neutralization. For a manual or semi-autonomous UAV, the RF radio communication between the ground station and UAV happens over
various protocols with fixed packet structure. These packets can be intercepted and decoded to obtain the packet architecture and hence a spoofing attack can be launched. RF jammers which transmit large amounts of energy towards the UAV can also be used for disrupting communication. This can lead to the UAV activating its fail-safe which may be to make a safe landing in its current position, return to a preset base location, or fly haphazardly and crash. For an autonomous UAV, the sensor values can be corrupted. The GNSS signals specifically can be jammed as well as spoofed. Besides these, there are some other physical attacks that are possible as well. Figure 16 presents a table listing all the techniques discussed in this section. Additionally, a Table 12 reviews some of the state of the art solutions against UAVs available in the industry.

### 9.1. Jamming

In the case of RF radio communication between the UAV and the ground control, RF jamming techniques are used to increase the level of noise interference at the RF receiver, in this case, the UAV or the UAV. This reduces the SNR at the receiver. This in turn prevents the receiver from responding to the commands from the sender, and thus, neutralizes its operation. Hence, the signals from the pilot or satellite systems can be jammed to disrupt the operation of manual and autonomous UAVs that depend on these. However, some UAVs that operate solely using other sensors such as IMUs and cameras are immune to this jamming technique.

Different UAVs may employ different spread spectrum and modulation techniques. To reduce the effectiveness of jamming, various methods have also been developed based on software defined networks [108]. Hence, depending upon these situation, different RF jamming

---

**Table 9**

| Technique       | Pros                                      | Cons                                      | Related Works |
|-----------------|-------------------------------------------|-------------------------------------------|---------------|
| Radar           | Long range                                | Very costly                               | [93,94]       |
|                 | Constant tracking which can handle hundreds of targets simultaneously | Range depends on UAV size                |               |
|                 | Accurate positioning                      | Needs extra support to distinguish between birds and UAVs |               |
|                 | Independent of autonomous UAVs, weather conditions | Requires licensing                      |               |
| RF Analyzers    | Low Cost                                  | Cannot detect autonomous UAVs            | [95–97]       |
|                 | Can detect, identify and triangulate multiple UAVs and transmitters | Short ranged                            |               |
|                 | Not affected by weather                   | Needs multiple instances to position      |               |
| Video Surveillance | No licensing required                    | Not that effective in RF noisy environments | [99–101]     |
|                 | Visuals on the UAV can be used for identification and forensics | Short Range and directional              |               |
|                 | Low Cost                                  | Depends on ambient light                  |               |
|                 | Can operate in dark with IR support       | Multiple needed for positioning           |               |
| Audio Surveillance | Medium Cost                              | Public privacy may be a concern          | [102–105]    |
|                 | No licensing needed                       | Inefficient in noisy environments         |               |
|                 | Based on acoustic signatures, can identify and detect autonomous UAVs | High False Positives                     |               |
|                 | Omni-directional beyond line of sight     |                                           |               |

**Table 10**

| Technique       | Pros                                      | Cons                                      | Related Works |
|-----------------|-------------------------------------------|-------------------------------------------|---------------|
| Noise           | Applied to a small portion of the spectrum with required power | Requires too much power to be effective | [112]         |
|                 | Is the simplest form of jamming           | No dynamic analysis of signal, hence can be easily mitigated |               |
|                 | Effective against localisation radars used by UAVs such as SAR | Effective against DSS |               |
| Tone            | Applied to a single or multiple tones     | Performance depends on placement of tones | [113]         |
|                 | Provides fine control                     | Performs poorly against FHSS systems      |               |
| Swept           | Covers a wide spectrum with less power    | As both the jamming and signal tones keep changing in case of FHSS, performance can be unreliable | [114, 115]   |
|                 | Provides fine control                     | Mitigation strategies are already being developed |               |
| Follower        | Effective against FHSS                    | Analysis of entire spectrum takes additional resources | [116]         |
| Smart           | Power efficient and effective             | Prior knowledge about target signal is needed | [117]         |
|                 | Is most reliable compared to other methods against FHSS and DSS | Analysis needs to be done by technologies such as SDR |               |

Fig. 16. Methods for Neutralizing UAVs.
Table 12
List of a few Commercial Anti-UAV Products in Market

| Product             | Technology                        | Vendor               | Host Country |
|---------------------|-----------------------------------|----------------------|--------------|
| Advanced Test High  | High energy laser                 | Lockheed Martin      | USA          |
| Energy Asset (ATHENA)| blast                            |                      |              |
| AUDS Anti-UAV       | Radar, Video Tracker and RF inhibitor| Blighter Surveillance Systems Ltd | UK          |
| Defence System (AUDS) |                                 |                      |              |
| Anti RPAS           | Radar, RF detectors and infrared cameras | Indra Company | Spain        |
| Multisensor System | Disrupts navigation transmission | Droneless            | Spain        |
| SkyFence            | Jamming the signal between drone and pilot | DroneShield | Australia   |
| Drone Gun           |                                   |                      |              |
| Coyote UAS          | Physical attack                   | Raytheon Technologies | USA         |
| Skywall Auto,       | Long Ranged Physical Capture      | Openworks Engineering | UK          |
| Skywall 100         |                                   |                      |              |

Techniques will be more efficient for effectively introducing interference at the RF receiver. The different types of RF jamming techniques available in literature [109-111] are discussed in this section. In addition to these, GNSS jamming has been discussed as a subsection due to its relevance to the subject (although it is not a different type of jamming and a specific case of the preceding types). Table 10 presents a comparative analysis of the various jamming techniques discussed.

9.1.1. Noise Jamming

Also known as Barrage Jamming, it is the simplest form of jamming in which a noise signal is applied to a small portion or the entire spectrum of the wideband modulated signal. This form of jamming directly affects and reduces the channel capacity of the system. It reduces the SNR value at the receiver, thereby reducing the channel capacity and increasing the information error rate. Noise jamming affects FHSS systems especially by introducing background interference during clock synchronization and tracking that is required between the sender and the receiver in between each transmission. Figure 17 shows a visual representation of how the RF spectrum is jammed using noise jamming.

Synthetic Aperture Radar (SAR) is a special radar used for two dimensional and three-dimensional spatial mappings and is often employed in UAVs to provide autonomy to the UAV by using methods such as Simultaneous Localization and Mapping (SLAM). Noise jamming can be used against such systems since the radio interference generated by it is sufficient to hide echoes, thereby rendering the SAR system futile [112].

9.1.2. Tone Jamming

In this type of jamming one or more tones in the spectrum are jammed strategically to introduce interference. The jamming performance depends on the placement of the tones in the spectrum and the transmission power. The transmission power is directly proportional to the interference on the tone. This technique is dependent on being able create sufficient interference in order to overcome the jamming margin, which requires a lot of power as multiple tones are targeted.

Fig. 17. Noise, tone and swept jamming.

Tone jamming can be of two types: either on a single tone (mono-tone) or on multiple tones (multi-tone). Both perform poorly against FHSS systems due to the variable nature of the transmission spectrum. Monotone jamming performs poorly since the overall performance of the system is not affected by one channel being absent. Even in multi-tone jamming, to be able to introduce significant interference, the adversary has to jam enough channels in the spectrum. The performance of single-tone jamming against DSSS systems has been analyzed in [113] and compared against narrow-band barrage jamming. With the correct placement of the tone, tone jamming performs fairly well against DSSS systems. Figure 17 shows a visual representation of how the RF spectrum is jammed using tone jamming.

9.1.3. Swept Jamming

In swept jamming, a relatively narrow-band signal, sometimes even a pulse or tone, is scanned in time across the frequency spectrum of interest. At a particular time instant, only a single frequency is targeted. However, over a period of time, the jammer covers a range of frequency bands by sweeping the target frequency. Hence, it is a mixture of noise and tone jamming in its application. Similar to noise jamming, it focuses on a single tone, but by sweeping, it also emulates tone jamming. Unlike noise or tone jamming, sweeping the jamming waveform ensures that it covers the entire set of hop frequencies of the data signal in the entire spectrum. Figure 17 shows a visual representation of how the RF spectrum is jammed using swept jamming.

Swept jamming performs well against DSSS systems since the data frequency bands are stationary, unlike FHSS systems where the frequency bands hop periodically in a pseudo-random fashion. Swept jamming finds most applications against GPS enabled systems due to weak strength of the GPS signals [114]. Ways of safeguarding GNSS to swept jamming are also constantly being actively developed and analyzed [115].

9.1.4. Follower Jamming

A follower jammer always tries to locate the new frequency hop that an FHSS system went to and then locates the target signal. Once confirmed, it then tries to jam the located frequency. To locate the target FHSS system frequency, it requires that the jammer measure the spectrum for energy losses and gains. An energy gain in the spectrum indicates a new signal entering whereas energy loss indicates a signal leaving the band. However, even then it is important to accurately identify whether a particular energy variation corresponds to the target signal or not, for which analysis needs to be carried out [116].

9.1.5. Smart Jamming

This type of jamming is applicable when the target signal properties are known previously from sources such as the Radio Frequency Integrated Circuit (RFIC) specifications. In smart jamming, only the necessary signals are attacked to deny successful communication, and hence they are power efficient and effective. This can be achieved by analyzing the data that is being transmitted and identifying critical points. Protocol-aware jamming techniques can be developed using Software Defined Radios. After analyzing the target signal, a jamming signal similar to it in terms such as hopping patterns (FHSS systems), PN code data rate (DSSS systems), and modulation techniques can be generated. Literature on implementations of such systems present the energy-efficient jamming performance as compared to other jamming techniques in terms of bit error rate (BER) introduced in the system. It is found to outperform other techniques in successfully jamming the target signals both in DSSS and FHSS systems but relies on the analysis of the target signal [117].

9.1.6. GNSS Jamming

Today, almost all UAV applications involve an autopilot functionality. That is, they are either partially or fully autonomous in their mode of operation. They house numerous sensors and onboard hardware to
estimate the current properties of the UAV such as orientation, location, and acceleration. One of these is the GNSS module such as GPS, which provides signals for localization. GPS signals are generally vulnerable in nature due to weak signal strength and are highly susceptible to noise and outside interference [118,119]. The implementation of GNSS jamming is an active field since although it is being used as a technique to disable UAVs in this context, the same methods can be used to disable GNSS systems in other critical applications such as navigation. Different jamming techniques for GPS signals have been studied, analyzed, and evaluated based on spectral efficiency, energy efficiency, and complexity. Based on this, protocol aware jamming or smart jamming was found to be the most efficient [120]. GPS jamming is very prevalent as such and jammers are easily available in the market [121]. A study in 2013 by Chronos Technology supported by the United Kingdom Technology Strategy Board investigated the prevalence of such vectors by setting up several monitoring stations across the UK. Results showed that some stations even recorded 5-10 jamming instances in a day [122].

Research has also been done to prevent GNSS jamming due to the financial and strategic importance that this technology holds for all countries. Various methods to mitigate GNSS jamming, such as using antenna arrays (which improve the overall SNR ratio) have also been proposed [123–125].

9.2. Spoofing

9.2.1. Sensor Spoofing

The autonomous UAV auto-pilot application relies heavily on the onboard sensors such as LIDARs, SONARs and optical flow sensors for localization and navigation. These sensors interact with the environment and provide valuable data for the auto-pilot computer to optimally guide the autonomous UAV system. In a sensor spoofing attack, the attacker transmits false sensor values to the flight controller which are in contrast to the actual values. The feedback loops get triggered and in order to correct the destabilized false values, the UAV orientates itself to stabilize, which in turn destabilizes it. Since many sensors share data for actuation, this can even lead to complete loss of control of the system, since one can gain access to the on-board actuator sensors or simulate false values. Simulations of sensor spoofing attacks on optical flow sensors found on UAV systems have proven this vulnerability [126].

In order to throttle the rising number of such attacks, control invariants have been introduced into the system which are able to detect differences between the perceived state and actual state. Such control invariants are derived from physical dynamics and control systems [127]. For instance, the data of GPS and optical flow sensors can be used to validate against other sensor data to detect inconsistencies to detect such attacks [133].

9.2.2. Signal Spoofing

In contrast to jamming which involves bombarding the receiver with noise signals, spoofing involves the generation of plausible counterfeit input signals with enough power to fool the receiver into believing this to be the original legitimate signal. Spoofing of the Tx protocol is difficult and requires reverse engineering to understand the structure. GPS signals tend to fluctuate in power due to the position of the satellites in the space as well as the weather conditions. Most modern-day GPS receivers implement an Automatic Gain Control (AGC) to compensate for these widespread fluctuations in the GPS signal strength. However, this also leaves the system more vulnerable to spoofing attacks [128]. A fake GNSS signal can be broadcast in an area making the UAV in that area perceive as if it is located in a different position, giving virtual control of the UAV to the spoofer [129,130].

- **Meaconing:**

Spoofing can be achieved simply by meaconing which involves the interception and re-transmission of the original signal with higher power to the receiver. It is the preferable vector when the targeted signals are encrypted since it does not rely on reverse-engineering the signal. In case of military bands, it is difficult to implement such an attack since retransmitting the signals need costly resources due to the much larger PN modulation and difficulty to predict the frequency hop pattern. However, in 2011, Iranian military captured a Lockheed Martin produced RQ-170 sentinel UAV using meaconing, among various other techniques [131].

- **Security Code Estimation and Replay (SCER):**

Similar to meaconing, it is used in systems where the GPS signal is protected with cryptography. In this attack, each symbol of the secret code is separately estimated by observing the received signal in the corresponding symbol interval. The symbol estimate is continuously updated by observing the received signal and simultaneously used in the spoofed signal, trying to replicate the secret code as faithfully as possible. Then, the spoofed signal is sent with some delay to the original signal. Methods such as likelihood ratio testing and its derivatives can help protect against this vector [132,134].

Table 11 presents a comparative analysis of the various spoofing techniques that have been discussed in this subsection.

9.3. Physical

- Nets can be used for capturing the UAV without severely damaging it as in other methods. This allows forensics on the UAV as well as identification of the owner. The nets can be deployed from another UAV system or ground launchers through turret or gun like structures. However, as nets are bulky and large the system may be inaccurate, need long reload-time and are short-ranged [135].
- Projectiles like missiles and explosives can also be used for neutralizing the drone [136].
- Aerial systems such as defense UAVs and birds of prey can be used to crash into the hostile UAV or destroy it by using offensive mechanisms such as claws and remote weaponry. [137].
- High Power Microwave (HPM) devices disrupt electronics by generating an Electromagnetic Pulse (EMP). The high voltage and current spikes that EMP creates in electronics circuits interfere with the radio links and disrupt or even destroy the electronic circuitry within range. As UAVs are based on electronics, HPMs are an effective solution. However as they are not specific and target all electronics in general they risk high collateral and are also very costly.
- High energy laser systems have a source of energy which excite electrons in atoms which on relaxing, release photons. These photons are focused using lenses hence producing a highly focused beam
which can destroy objects it collides with due to high energy density. Recent technological breakthroughs have made this approach feasible. However, they are very costly and risk collateral damage as they are not specific to UAVs [138].

9.4. Other Methods

- The flight controller and GC are electronics and hence are vulnerable to hardware and software Trojans. Trojans can be either designed in the system itself or planted in it later. For instance, a hacker can tap into the power rails of the primary processor, and extract the security key required to hack that UAV, possibly obtaining knowledge about how the authentication occurs. This technique targets a device and plants malicious software on it temporarily reducing the voltage of the power supply to a chip, hijacking the I2C bus that most voltage regulators communicate on, assert a new master and send messages from there. By momentarily under-volting a chip at precise timings, an attacker can cause the chip to make errors while executing processes that use confidential data. Hence, these errors can be exploited to get sensitive information such as cryptographic keys or biometric data. With such security bypassed, the attacker may update the UAV with modified firmware and could expose the whole network to serious damage and vulnerability.

- The data sent from the UAV to the GS over telemetry has information like video feed, sensor values, and battery levels. Details about the telemetry structure and control protocols can be obtained by reverse engineering. Jamming or spoofing these can manipulate the operation commands which can change the flight plan and sent it back or crash.

- Deauthentication attacks can be done on UAVs to disconnect the actual pilot, and this may lead to fail-safe activation of the UAV, as well as providing a window where the attacker may be able to connect to the UAV instead. WiFi is specifically vulnerable to such attacks and is used commonly found in consumer UAVs as most users have devices like their mobile phones that support WiFi.

10. UAV Neutralization Case Studies

This section provides specific cases when researchers and hobbyists have tried implementing anti-UAV technologies. Vulnerabilities in the software or communication system were identified and exploited. The presented cases are classified on the basis of attack vectors such as malware, GPS spoofing, WiFi attacks, reverse engineering, and spoofing. Table 13 summarizes all the cases we have discussed in this section.

10.1. Malware

10.1.1. Maldrone

Maldrone is a software malware that overrides the UAV’s autopilot and allows the attacker to take over control remotely. It can be used against any ARM based UAV running on Linux like AR Parrot and DJI Phantom. It opens a backdoor which gives access to sensors and drivers to the hacker. The developer of Maldrone, Rahul Sasi, tested it on a Parrot AR drone in 2015. The Parrot AR Drone, revealed at the International CES 2010 in Las Vegas, is a quadcopter that can be controlled by a smartphone or tablet over WiFi.

A binary named program.elf that manages the AR drone has not been made open-source. However, this could be reverse-engineered by using software like IDA which can convert asm code to pseudo C code. This gave sufficient information about the UAV’s operation. Maldrone injects itself like a proxy, thus enabling the injection of the desired values for both flight controller and sensor communication [139].

10.1.2. SkyJack

SkyJack has been developed for searching and hijacking UAVs that are in WiFi communication range. It gave the SkyJack pilot the ability to take control over the hijacked UAV and also view the camera.

SkyJack’s developer, Samy Kamkar, used a Raspberry Pi with a WiFi Packet injector installed with SkyJack to hack an AR Parrot 2 drone in 2015. The AR Parrot 2, like its predecessor, works over WiFi and can be controlled by a smartphone or tablet. The AR Parrot 2 hosts its wireless network which is how the pilot of the UAV connects. SkyJack first runs aircrack-ng (open source) to run monitor mode to find the UAVs and UAV owners in its vicinity. The MAC addresses of the UAVs owned by the Parrot company can be detected over any wireless connections from MAC addresses as they can be found online in the IEEE Registration Authority’s organizationally unique identifiers. After that aireplay-ng (open source) is used to de-authenticate the actual pilot of the UAV. Once unauthenticated, the attacker can connect as the UAV is not connected to any pilot. Finally, node-ar-drone is used to control the newly enslaved UAV via Javascript and node.js [140]. SkyJack does have its limitations, however, since it can only select targets within a predefined range of MAC addresses on an unsecured network.

10.2. GPS Spoofing

10.2.1. DJI Matrice 100

A Software Defined Radio along with an Open Source GPS-SDR-SIM repository is used to broadcast fake GPS signals [141]. The attacker supplies a GPS broadcast Ephemeris file for specifying the GPS satellite constellation. The Ephemeris files are used to generate the simulated pseudo-range and Doppler for the GPS satellites in view. After this, the simulated range data is used to generate the digitized I/Q samples for the GPS signal. Further, the SDR converts the I/Q to RF waves which are received as stronger signals than the real GPS by the UAV. Almost all UAVs that are dependent on GPS are vulnerable to this kind of attack owing to the very nature of unencrypted civilian GPS signals.

10.2.2. IIT Madras

In February 2020, students at the Indian Institute of Technology, Madras designed a UAV that can detect other UAVs visually, along with a GPS spoofing mechanism for neutralizing the operation of GPS dependent UAVs in the vicinity. It uses a deep learning model to detect motion in order to spot other UAVs even in the absence of light. It also uses an SDR approach to broadcast stronger GPS signals for GPS spoofing. Mathematical models of the time differences with the target UAV are used to generate the spoofed GPS packets. With multiple time differences, eventually the target UAV calibrated its clock to the spoofed signals. When there is a large variance in the actual GPS position and spoofed position, the target UAV’s fail-safe is activated that disrupts its operation. This was tested against various civilian GPS receivers used in the UAV industry such as Ublox and DJI in-house GNSS. The students were able “to take down the UAVs almost instantaneously” [144].

10.3. WiFi Attacks

The Parrot Bebop was tested against various attacks by a research
team and they were able to discover three vulnerabilities [142]. The first is a denial of service attack where about 1000 requests were made to the UAV rapidly, each trying to connect as controller. The UAV’s processor and memory could not handle this and therefore, it shut down. This sent the UAV into what the team referred to as “an uncontrolled landing”. Next, a buffer overflow attack where a very large data packet was transmitted to the UAV, which exceeded the maximum capacity of the buffer in the system. This also caused the UAV to crash. Lastly, fake packets claiming the sender to be the UAV’s controller were sent repeatedly from a laptop. This claim was made by spoofing the IP address. Soon the UAV accepted the sender as hence its own contact with UAV was severed. This led to an emergency landing of the UAV.

10.4. Reverse Engineering and Spoofing

The Digi XBee 868LP RF Modules provide wireless connectivity to end-point devices in mesh networks. It was used for telemetry between the UAV and ground station for a UAV, which was exploited by Nils Rosdady and presented in the Black Hat Asia Conference 2016 [145]. By referring to the instruction manual of the chip, an API mode was discovered which allowed the user to fabricate their own custom packets for transmission. A broadcast mode was also discovered which allowed pinging all chips in the range and getting their addresses from acknowledged frames. The chip also had a feature where its address, used for packet transmission, can be changed remotely by another chip. Hence, the attacker introduced another chip in the system besides the ones in the ground station and UAV, switched to API mode, and then broadcast to get the addresses of the GS and UAV chips. After that, they modified the addresses such that all packet were sent through the attacker chip. Hence, he got access to reading and writing information on the channel but was still unaware of the data packet structure. For this, he reverse-engineered the Android application in the GS and then used trial and error to list all operation packets. After getting the templates, he could rebroadcast those packets to spoof itself as the UAV GS.

11. Conclusion

UAV misuse has led to the formation of regulations and regulatory bodies in various countries. So, in this paper, we highlighted the need for research and implementation of measures to counteract the misuse of UAVs. Having provided the current situation of UAVs from a security perspective, the current global scenario of UAVs in the military and commercial usage, existing regulations in various countries, we reviewed and discussed popular transmitter protocols and presented some detecting and neutralizing methods for UAVs. We emphasized the RF communication used by the UAV as it seems to be the most reliable method which can be deployed on a wide scale, owing to new technologies like SDRs, which reduce the cost dramatically. In the latter part, we presented case studies that specifically talk about how different kinds of commercial UAVs can be hacked and thus can be misused. With the growing popularity of UAVs in various fields, UAVs are soon going to be employed in our day to day life and there is a need for research addressing all the security concerns to accelerate this process securely.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Y. Liu, H.-N. Dai, Q. Wang, M.K. Shukla, M. Imran, Unmanned aerial vehicle for internet of everything: Opportunities and challenges, Computer Communications (2020).
[2] S. Vashish, S. Jain, G.S. Aujla, Mac protocols for unmanned aerial vehicle ecosystems: Review and challenges, Computer Communications (2020).
[3] J.P. Skrinjar, P. Skorput, M. Furdic, Application of unmanned aerial vehicles in logistics processes, in: I. Karabegovic (Ed.), New Technologies, Development and Application, Springer International Publishing, Cham, 2019, pp. 255–266.
[4] V. Hantija, V. Chamola, V. Gupta, S. Jain, N. Guzani, A survey on supply chain security: Application areas, security threats, and solution architectures, IEEE Internet of Things Journal (2020).
[5] V. Unapoom, N. Dusadee, R. Ramaraj, Modern Agriculture Drones The Development of Smart Farmers 2018, Maejo University, pp. 13–19.
[6] H. Shakkather, A.H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Oshman, A. Kheirehah, M. Guzani, Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges, IEEE Access 7 (2019) 48572–48634.
[7] S.A. Hoseini, J. Hassan, A. Bokani, S.S. Kanhere, Trajectory optimization of flying energy sources using q-learning to recharge hotspot uavs, arXiv preprint arXiv:2003.12258 (2020).
[8] P. Garg, A. Srinivasan, M. Mandial, P. Narang, V. Chamola, M. Guzani, Idenet: AI-enabled instance segmentation of aerial scenes for smart cities, ACM Transactions on Internet Technology.
[9] A. Restas, Drone applications for supporting disaster management, World Journal of Engineering and Technology (2013) 316–321, https://doi.org/10.4236/wjet.2015.31C047.
[10] V. Chamola, V. Hantija, V. Gupta, M. Guzani, A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact, IEEE Access (2020) 90225–90265.
[11] K. Li, R.C. Voicu, S.S. Kanhere, W. Ni, E. Tovar, Energy efficient legitimate wireless surveillance of uav communications, IEEE Transactions on Vehicular Technology 68 (3) (2019) 2283–2293.
[12] Drones: Reporting for work, [Online]. Available: https://www.goldmansachs.com/investors/technology-driving-innovation/drones/.
[13] Drones Market Size (2019-2025) Application, [Online]. Available: https://www.adroitmarketresearch.com/industryreports/drones-market.
[14] M. Gapeyenko, V. Petrov, D. Molchchanov, S. Andreev, N. Hinayat, V. Kocheryavy, Flexible and reliable uav-assisted backhaul operation in 5g mmwave cellular networks, IEEE Journal on Selected Areas in Communications 36 (11) (2018) 2486–2496.
[15] B. Li, Z. Fei, Y. Zhang, Uav communications for 5g and beyond: Recent advances and future trends, IEEE Internet of Things Journal 6 (2) (2018) 2241–2263.
[16] T. Alladi, V. Chamola, N. Sahu, M. Guzani, Applications of blockchain in unmanned aerial vehicles: A review, Vehicular Communications (2020) 100249.
[17] M. Singh, G.S. Aujla, R.S. Ball, Otol: One drone one block based lightweight blockchain architecture for internet of drones. IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2020, pp. 249–254.
[18] V. Hantija, V. Chamola, D.N.G. Krishna, M. Guzani, A distributed framework for energy trading between uavs and charging stations for critical applications, IEEE Transactions on Vehicular Technology 69 (5) (2020) 5391–5402.
[19] A. Braeken, M. Liyanage, S.S. Kanhere, S. Dixit, Blockchain and cyberphysical systems, Computer 53 (9) (2020) 31–35.
[20] V. Hantija, V. Saxena, V. Chamola, Scheduling drone charging for multi-drone network based on consensus time stamp and game theory, Computer Communications 149 (2020) 51–61.
[21] T. Alladi, Naren, G. Baner, V. Chamola, M. Guzani, Secautharya: A novel authentication scheme for uav-ground station and uav-uav communication, Accepted for publication, IEEE Transactions on Vehicular Technology.
[22] M. Wazid, A.K. Das, N. Kumar, A.V. Vasilakos, J.J. Rodrigues, Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment, IEEE Internet of Things Journal 6 (2) (2018) 3572–3584.
[23] Z. Lv, S. Zhang, W. Xiu, Solving the security problem of intelligent transportation system with deep learning, IEEE Transactions on Intelligent Transportation Systems (2020).
[24] T. Alladi, V. Chamola, Naren, N. Kumar, et al., Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks, Computer Communications (2020).
[25] Z. Ali, S.A. Chaudhry, M.S. Ramzan, F. Al-Turjman, Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles, IEEE Access 8 (2020) 43711–43724.
[26] S. Garg, G.S. Aujla, N. Kumar, S. Batra, Tree-based attack-defense model for risk assessment in multi-uav networks, IEEE Consumer Electronics Magazine 8 (6) (2019) 35–41.
[27] N.M. Rosdady, R.d.O. Schmidt, A. Pras, Exploring security vulnerabilities of unmanned aerial vehicles, NOMS 2016-2016 IEEE/SPIF Network Operations and Management Symposium, IEEE, 2016, pp. 993–994.
[28] T. Alladi, V. Chamola, B. Sikkadar, K.-R.R. Choo, Consumer iot: Security vulnerability case studies and solutions, IEEE Consumer Electronics Magazine 9 (2) (2020) 17–25.
[29] Houthi drone attacks on 2 Saudi Aramco oil facilities spark fires, [Online]. Available: https://www.aljazeera.com/news/2019/09/droneshit-saudi-aramco-oil-facilities-fires-190914051900472.html.
[30] DGCA RPAS Guidance Manual, [Online]. Available:https://public-prd-dgca.s3-ap-south-1.amazonaws.com/InventoryList/headerblock/drones/DGCA%20Guidance%20Manual.pdf.
[31] The we enable flight for India’s unmanned aircraft, [Online]. Available:https://dig india-gov-duty.gov.in/
V. Chamola et al.

Vinay Chamola received the B.E. degree in electrical and electronics engineering and master’s degree in communication engineering from the Birla Institute of Technology and Science, Pilani, India, in 2010 and 2013, respectively. He received his Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016. In 2015, he was a Visiting Researcher with the Autonomous Networks Research Group (ANRG), University of Southern California, Los Angeles, CA, USA. He also worked as a post-doctoral research fellow at the National University of Singapore, Singapore, where he worked in the area of Internet of Things. He is currently Assistant Professor with the Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus where he heads the Internet of Things Research Group / Lab. He has over 50 publications in high ranked SCI Journals including more than 33 IEEE Transaction and Journal articles. His works have been published in Journals like IEEE Transactions on Communications, IEEE Transactions on Vehicular Technology, IEEE Journal on Selected Areas in Communications, IEEE Communications Magazine etc. Furthermore, his works have been accepted and presented in reputed conferences like IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, IEEE PerCom to name a few. His research interests include IoT Security, Blockchain, 5G network management and addressing research issues in VANETs and UAV networks. He has served as a reviewer for several IEEE/Elsevier Journals. He is a Guest Editor in Computer Communication, Elsevier. He serves as an Associate Editor for the Ad Hoc Networks journal, Elsevier, IET Networks Journal, IET Quantum Communications and Frontiers in Communications and Networks. He is a senior member of the IEEE.

Pavan Kotesh is M.Tech Software Systems Graduate from Birla Institute of Technology and Science, Pilani, India. He has completed his B.E from the same university. Working in a software company based out of Bangalore in the last 6 years, he has worked and deployed several cryptography projects, websites and mobile applications. He has worked on Internet of Drones and security in his M.Tech thesis and continue to pursue his interest in research areas like Internet of Drones, Security in IoT, Cryptography and Blockchain.

Aayush Agarwal is currently pursuing his B.E. in Electronics and Instrumentation at Birla Institute of Technology and Science, Pilani. He has also been as a Teaching Assistant to a course on Internet of Things at National University of Singapore. He has worked on several projects and actively participates in competitions demonstrating skills spanning in different domains such as Web Development, IoT and Augmented Reality. His research interests include architecture design in IoT and Cloud, communication protocols and penetration security.

Navneet Gupta is currently Associate Professor in Department of Electrical and Electronics Engineering at BITS-Pilani, Rajasthan, India. Prof. Gupta received his Master’s degree in Science with specialization in Advanced Electronics from H.N. Birla Institute of Technology and Science (BITS-Pilani), Rajasthan, in 1995 with first rank in the University and was awarded Gold Medal. He received M.Tech in Materials Technology in 1998 from Indian Institute of Technology (IIT-BHU)-Varanasi. He completed his Ph.D in the field of Semiconductor Devices Modelling from HNBGU in 2005. His current research interests are in the areas of Modeling of Micro/Nano Electronic Devices, Flexible and Wearable Electronics, Computational Material Science and Electromagnetics. He has published 123 research papers in international and national journals and conferences. He has written text books published by Oxford University Press (Foundations of Electrical Engineering) and New Age International Publishers (Electromagnetic Field and Waves). He is Fellow of The Institution of Engineers (India), Senior member of IEEE and life members of other professional bodies. He is expert reviewer of many reputed International Journals including IEEE, Springer, Elsevier and IE (I).

Mohsen Guizani (S’85-M’89-SM’99-F’09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor at the Computer Science and Engineering Department in Qatar University, Qatar. Previously, he served in different academic and administrative positions at the University of Idaho, Western Michigan University, University of West Florida, University of Missouri-Kansas City, University of Colorado-Boulder, and Syracuse University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is currently the Editor-in-Chief of the IEEE Network Magazine, and the Founder and Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 500 publications in refereed journals and conferences. He received the 2017 IEEE Communications Society WTC Recognition Award as well as the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and Ad-Hoc Sensor networks. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer. He is a Fellow of IEEE and a Senior Member of ACM.