drones

MDPI

Review

A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics

Fazal Noor [1], Muhammad Asghar Khan [2,*], Ali Al-Zahrani [1], Insaf Ullah [2] and Kawther A. Al-Dhlan [3]

[1] Faculty of Computer Science and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia; mfnoor@iu.edu.sa (F.N.); a.alzahrani@iu.edu.sa (A.A.-Z.)
[2] Department of Electrical Engineering, Hamdard University, Islamabad 44000, Pakistan; insaf.ullah@hamdard.edu.pk
[3] Department of Computer Science and Information, University of Hail, Ha'il 55425, Saudi Arabia; k.aldhlan@uoh.edu.sa
* Correspondence: m.asghar@hamdard.edu.pk; Tel.: +92-336-5276465

Received: 6 September 2020; Accepted: 28 September 2020; Published: 30 September 2020

Abstract: Unmanned aerial vehicles (UAVs), also known as drones, once centric to military applications, are presently finding their way in many civilian and commercial applications. If national legislations permit UAVs to operate autonomously, one will see the skies become populated with many small UAVs, each one performing various tasks such as mail and package delivery, traffic monitoring, event filming, surveillance, search and rescue, and other applications. Thus, advancing to multiple small UAVs from a single large UAV has resulted in a new clan of networks known as flying ad-hoc networks (FANETs). Such networks provide reliability, ease of deployment, and relatively low operating costs by offering a robust communication network among the UAVs and base stations (BS). Although FANETs offer many benefits, there also exist a number of challenges that need to be addressed; the most significant of these being the communication one. Therefore, the article aims to provide insights into the key enabling communication technologies through the investigation of data rate, spectrum type, coverage, and latency. Moreover, application scenarios along with the feasibility of key enabling technologies are also examined. Finally, challenges and open research topics are discussed to further hone the research work.

Keywords: UAVs; FANETs; Bluetooth; ZigBee; 5G; 6G; security; privacy; blockchain; energy harvesting

1. Introduction

Unmanned aerial vehicles (UAVs) have gained recognition for their variety of applications in different domains such as surveillance, agriculture, health care, traffic control, inspections, and public safety [1]. Moreover, in comparison to a stand-alone UAV, multiple small UAVs can be effectively combined to execute assigned tasks in autonomous ways [2]. Thus, advancing from a single UAV to multi-UAVs results in the emergence of a new clan of networks named flying ad-hoc networks (FANETs) [3]. Smaller interconnected UAVs can exchange data with each other and with base stations (BS) in a FANET system [4]. FANETs possess advanced features such as high mobility, fast deployment, self-configurations, low cost, scalability, and others. However, such specific features demand a set of guidelines that need to be addressed for effective implementation. Particularly, when

selecting a FANET system for real-time communication, Quality of Service (QoS) should be guaranteed [5]. In addition, for the exchange of information between UAVs and a BS, the network must have incorporated an efficient and secure wireless connection.

FANETs can be deployed either individually or incorporated into traditional cellular infrastructures. The subject has attracted the interest of both industry and academic experts. Most related research studies seek to integrate FANETs with or without traditional networks in a manner that upholds the QoS, security, and reliability requirements of small UAVs [6]. Therefore, the detection and identification of vulnerabilities in the current systems are important for developing solutions that enable high-throughputs and reliable data communications. The popular short-range wireless networking technologies such as Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), and others can be utilized to incorporate a FANET system independently. Such technologies not only provide wireless networking in the immediate vicinity, but also provide spectrum-free bands [7]. In the following two scenarios, they are a good choice: in the event of failure due to the deterioration of existing communication networks, and in remote areas, where problems do not enable installation and deployment immediately. Additionally, they can step up rescue operations by maintaining effective UAV communications. In addition, the low altitude of UAVs due to short-distance wireless communication significantly improves the performance of networks in terms of QoS.

The Fifth-Generation (5G) technologies are projected to offer improved services in terms of data rates and coverages in linking FANETs to existing cellular networks [8]. Moreover, 5G provides multi-access edge computing (MEC), incorporating cloud computing capabilities. MEC prevents resource-affected UAVs from performing compute-intensive tasks in a UAV environment and provides offloading facilities to the edge of the network. Hence, 5G has many benefits for high-altitude UAVs equipped with cameras, sensors, and GPS receivers. In addition, 5G has made it possible to envision cellular networks beyond 5G (B5G) and sixth-generation (6G) is capable of incorporating autonomous services as well as emerging developments to be envisioned [9]. The main issues are the safe usage of these technologies and the provision of privacy in small UAVs in future wireless networks. The design considerations of small UAVs rarely address the security concerns [10]. Small UAVs also suffer from security vulnerabilities due to limited and insufficient onboard computing and energy capabilities [11,12]. Such constraints prevent UAV deployment for longer periods of time and for safer operations. Significant attempts have been made to resolve the underlying technical problems in order to take advantage of the wider benefits of the multi-UAV networks [13]. Figure 1 shows a diagram summarizing the communication scope in FANETs, their involvement with recent technological advances, and their combined applications. Therefore, it is essential to have adequate wireless technologies and lightweight security schemes that can significantly stabilize battery life, have minimal computational costs, and encourage better connectivity. In comparison, in this review, key enabling technologies are addressed that manifest themselves as the paradigms needed to effectively deploy FANETs in the future. It also highlights the main challenges and provides guidance for future research work.

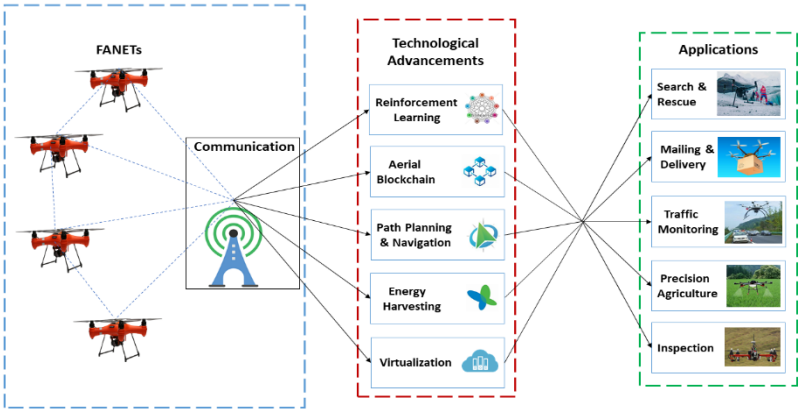

Figure 1. Scope of communication with technological advancements for various applications in FANETs.

The rest of the paper is organized as follows. Section 2 describes the key enabling wireless technologies; Section 3 elaborates on applications; in Section 4, the challenges are discussed; Section 5 highlights the future work, and finally Section 6 contains the conclusions.

2. Key Enabling Wireless Technologies

The choice of appropriate wireless communication technologies for FANETs depends on the type of an application and the nature of the mission involved. Unlicensed wireless technologies such as Wi-Fi, ZigBee, and Bluetooth are widely used for fast deployment and small- to medium-scale applications [6,7]. Licensed wireless technologies such as 5G/6G, on the other hand, are used to satisfy the requirements of broadband access everywhere, high device mobility, and integration of a massive number of UAVs in an ultra-reliable way [14]. Based on the spectrum type (licensed/unlicensed), the most suitable wireless technologies for FANETs are categorized in Table 1. To provide wireless connectivity in the immediate vicinity, unlicensed or short-range wireless technologies have the ability to offer off-the-shelf, lightweight, and cost-effective wireless connectivity. Unlicensed technologies offer information transfer in the instant vicinity ranging from millimeters to a few hundred meters.

The most suitable short-range wireless technologies are Wi-Fi, Bluetooth, and ZigBee, which can be used for medium and low data rate applications of FANETs. Wi-Fi provides a set of specifications for the implementation of wireless local area networks (WLANs) with radio bands of 2.4, 3.6, 5, and 60 GHz, respectively. IEEE 802.11a/b/g/n/ac is the first choice of variants for many FANET applications to provide the required throughput for transmitting medium size data such as video and images [15]. The standard Wi-Fi system has a transmission range of approximately 100 m. A multi-hop networking scheme may expand the transmission range to kilometers. However, it cuts down the lifetime of the network from hours to minutes. An alternative to Wi-Fi is the use of low-cost and low-power radios like Bluetooth and ZigBee. Bluetooth (IEE 802.15.1) is a possible candidate for the deployment of FANETs at low cost and low power manners. It operates in an unlicensed frequency band of 2.4 GHz with a contact range of 10 to 100 m and uses a distributed frequency-hopping transmission spectrum. Bluetooth technology, with data rate ranging from 1 to 3 Mbps and a capacity of 24 Mbps, can be used in three different models. The new version of Bluetooth core specification is Bluetooth 5 [16]. The primary focus of Bluetooth 5 is to improve data rate, coverage, energy efficiency, and coexistence with other technologies. Given the major improvements, Bluetooth 5 appears to be a possible candidate for implementing future FANET systems at low cost and low power manners. Similarly, ZigBee technology is widely used in applications that require long battery life, low data rates, and secure networking. It ranges from 10 to 100 m and is less expensive and convenient than proprietary communication technologies such as Bluetooth and Wi-Fi.

Low-power wide area networks (LPWAN) can be another good option that consumes less energy and offers a wide range of connectivity for UAVs [17–20]. LPWAN allows transmitting data for a longer duration of time and without much loss of energy resources. LoRaWAN has been designed as a convention explicitly for the management of low energy consumption transmissions when Internet of Things (IoT) devices on LPWAN [21,22]. For IoT users, LoRaWAN uses a novel network paradigm for bidirectional connectivity, localization, and mobility management services [23]. It provides a new framework for LPWAN execution for long-range communications. It has the potential to operate over the ISM band (868 MHz and 900 MHz) with data rates ranging from 0.3 kbps to 50 kbps and network coverage from 5 to 15 km [24–26]. Sigfox, similar to LoRaWAN, is a low-speed but low-power and long-range solution for UAVs. It uses the same ISM band as LoRaWAN. One of the advantages of Sigfox is that it supports open-sight up to 30 km of range.

If the unlicensed wireless technologies are not capable of meeting the UAV throughput requirements, traditional cellular communications can be used as a backhaul for providing data transmission services in two sights. Narrow band Internet of Things (NB-IoT) is a LPWA standard technology designed to provide connectivity and access to new services for a wide range of the latest IoT devices. NB-IoT, especially in deep coverage, significantly improves user device power consumption, system capacity, and spectrum efficiency. Moreover, as the later proposals in 5G have made it conceivable to conceptualize cellular systems beyond 5G (B5G) and sixth-generation (6G), able of unleashing the complete potential of copious, past-including autonomous administrations as well as emerging trends. They give capacity extension methodologies to resolve the issue of gigantic connectivity and give ultra-high throughput, indeed in extraordinary or crisis circumstances where there may be shifting framework densities, transmission capacity as well as traffic pattern. These technologies can moreover be valuable to FANETs by empowering UAVs to communicate specifically with each other and at the same time with a fixed communication framework. Within the same setting, the limited onboard processing capacity of small UAVs, storage, and battery imperatives raises a number of concerns over the effective execution of complex assignments. Leveraging the cloud storage facility offered by 5G to offload both computation and storage-intensive activities from resource-constrained UAVs to remote cloud servers is an effective technique to overcome these limitations. Furthermore, the deployment of UAVs as a flying base station (BS) with other physical layering mechanisms such as massive MIMO, cognitive radios, mmWave, and others as a prerequisite, is a promising approach to achieve data-hungry services [27].

The above discussions led to the conclusion that depending on the range and throughput requirements, Bluetooth, ZigBee, Wi-Fi, LoRaWAN, and Sigfox can be considered, depending on the range and throughput requirements [28]. 5G and 6G can be a more suitable choice if the coverage area is large, together with high throughput demands. However, these technologies require the existing telecommunications infrastructure.

Table 1. Comparison between the various communication technologies for FANETs.

Communication Technology	Standard/Service Category	Spectrum Type	Frequency/Medium	Device Mobility	Theoretical Data Rate	Range Indoor-Outdoor	Latency
Wi-Fi	802.11	Unlicensed	2.4 GHz IR	Yes	Up to 2Mbps	20–100 m	<5 ms
	802.11a	Unlicensed	5 GHz	Yes	Up to 54Mbps	35–120m	
	802.11b	Unlicensed	2.4 GHz	Yes	Up to 11Mbps	35–140m	
	802.11n	Unlicensed	2.4/5 GHz	Yes	Up to 600Mbps	70–250 m	
	802.11g	Unlicensed	2.4 GHz	Yes	Up to 54Mbps	38–140 m	
	802.11ac	Unlicensed	5 GHz	Yes	Up to 866.7Mbps	35–120 m	
ZigBee	802.15.4	Unlicensed	2.4 GHz	Yes	Up to 25Kbps	10–100 m	15 ms
Bluetooth V5	802.15.1	Unlicensed	2.4 GHz	Yes	Up to 2Mbps	10–200 m	3 ms
LoRaWAN	IEEE 802.15.4g	Unlicensed	868 MHz, 915 MHz	Yes	Up to 50 kbps	05–15 km	Device Class Dependent
Sigfox	-	Unlicensed	868 MHz, 902 MHz	Yes	Up to 100 bps	03–30 km	2 s
NB-IoT	• LTE Cat NB1 • LTE Cat NB2	licensed	200 KHz	Yes	Up to 250 kbps	10–35 km	1.6–10 s
5G	• mMTC • URLLC • eMBB	licensed	• Sub-6 GHz • MmWave for fixed access	Yes	Up to 1 Gbps	Wide Area	1 ms
B5G	• mMTC • URLLC • eMBB • Hybrid (URLLC + eMBB)	licensed	• Sub-6 GHz • MmWave for fixed access	Yes	Up to 100 Gbps	Wide Area	1 ms
6G	• MBRLLC • mURLLC • HCS • MPS	licensed	• Sub-6 GHz • MmWave for mobile access • Exploration of higher frequency and THz bands (above 300 GHz) • Non-RF (e.g., optical, VLC, etc.)	Yes	Up to 1 Tbps	Wide Area	<1 ms

3. Applications and Feasibility of the Wireless Technologies

The use of small UAVs for multiple insurgents, civilian, and commercial applications is expected to produce good results when it comes to providing accurate and reliable data transfer. As shown in Figure 2, some of the areas where FANETs can be used are search and rescue, mail and delivery, traffic monitoring, precision agriculture, reconnaissance, and others.

3.1. Search and Rescue (SAR)

SAR missions are amongst the most popular aerial robotics driving applications. This is largely due to UAVs' unique features such as versatility, flexibility, and scalability in contrast with human vehicles [29]. Furthermore, the UAVs are able to fly autonomously, access difficult terrain, and perform tasks of data collection, which are impossible for human vehicles. The advent of FANETs has further increased UAV participation in active search and rescue operations [30]. In the event of unexpected natural disasters, hazardous gas intrusions, wildfires, avalanches, and the rapid identification of missing persons, FANETs will serve as the first line of protection. In such scenarios, FANETs could be deployed in the affected areas, in exchange for sending humanitarian aid that could be at risk. UAVs were first used during the 2005 Hurricane Katrina search and rescue missions and later in the 2011 Fukushima and 2015 Nepal earthquake, respectively [31].

In [32], the authors proposed a modern search and rescue operations (SARO) strategy to search for survivors following major disasters on the assumption that wireless communication network cells are partly functional while taking advantage of the UAV-based network. These SAROs are based on the notion that nearly all survivors should be equipped with handheld remote gadgets called User Equipment (UEs), which function on the ground as human-based sensors. The control messages in SAR operations include the exchange of task assignment, position and heading, and map information, while the data messages involve either images or video streaming, requiring a minimum data rate of 1 Mbps and 2 Mbps, respectively. In addition, the delay limits for these operations is about 50 ms and 100 ms and covers small- to medium-sized areas. Thus, keeping these parameters in mind, unlicensed (i.e., Wi-Fi and Bluetooth 5) technologies can be used for limited coverage areas and a fewer number of nodes, whereas cellular technologies can be used for large coverage areas and mass deployment of UAVs.

3.2. Mailing and Delivery

Package delivery is one of the most enticing UAV applications supported by major courier companies for quick, cost-effective and efficient transportation of packages that weigh less than a UAV maximum bearing load [33]. For example, Amazon reports that 83 percent of its packages weigh less than 2.5 kg [34], while the average FedX package weighs less than 5 kg [35]. Moreover, the adoption of UAVs is increasing rapidly due to the growing trend of online ordering in congested cities, especially in the retail sector. Many major retailers and logistics companies are stepping up efforts to integrate small UAVs into their transport systems to solve the problem of "last mail" delivery. The authors in [36] illustrated the plans of large retailers and logistics companies as follows: DHL launched its drone delivery service for express and emergency products and began the first automated drone delivery to Juist Island in 2014; later on, DHL successfully made more than 100 deliveries in the Bavarian Alps in early 2016 through its Parcelcopter 3.0 drone; UPS tested the delivery of a successful automated drone in Florida in 2017 from the roof of a company electric vehicle; and through securing a U.S. patent, Amazon created major competition to legalize its UAV distribution project called "Prime Air." Patent and Trademark Office are dropping packages from drones to consumers through the use of parachutes.

Mailing and delivery operations require low throughputs for trajectory planning, however, the coverage areas may be large. The communication range of unlicensed technologies is limited, so it is therefore possible to use any appropriate licensed technology for mailing and delivery operations.

3.3. Traffic Monitoring

Roadway traffic surveillance is also a possible application where FANETs can replace the laborious and complex infrastructures used for observations. UAVs are less costly than traditional traffic control devices used on the roadside such as loop detectors, video surveillance cameras, and microwave sensors [37]. Moreover, data obtained from detector technology is somewhat statistical in nature and does not provide precise tracking of the individual vehicle path within the stream of traffic. It limits the use of data obtained in the study of calibration, human driving behaviors, and simulation models [38]. Additionally, disasters can easily damage the fixed structures located along the road side used for computing, communications, and electrical systems. Such shortcomings result in a complete lack of the transport network capacity to track and gather data [39]. Alternatively, the FANETs that can track and record accidents or perform traffic management statistics are an economically and socially viable choice because of their 3D movement, high speed, and wide coverage.

In traffic monitoring, UAVs are involved in transmitting images and video streaming to the control center in real-time; thus, licensed technologies will be a better choice. In addition, licensed technologies make use of existing communication infrastructures, particularly in urban areas and can operate without line-of-sight.

3.4. Precision Agriculture

Management of agriculture production includes the monitoring of crop health. Despite manned aerial vehicles having been used in this sector over the decades, however, the new concept of autonomous UAVs is considered more beneficial as they conduct field operations with greater precision on smaller as well as wider fields [40]. High-resolution crop images can be taken with the aid of small UAVs. The captured images are processed in order to produce relevant information, which can then be used for future decision-making. Crop health is defined using data obtained from the color imaging mapping of the normalized vegetation difference index (NDVI) [41]. These color images are usually obtained through a multispectral high-definition camera installed on the UAVs. NDVIs are counted as separating healthy from unhealthy plants, which is achieved by calculating the level of chlorophyll in crops. It takes advantage of the knowledge to identify the area under greater stress. The decision support engine (DSE) is responsible for taking the appropriate steps to process the task.

The coverage area in precision agriculture can be small or medium in size. Short-range wireless technologies, particularly Wi-Fi, can be the most appropriate choice to meet the requirements in terms of coverage, latency, and throughput in crop health monitoring.

3.5. Reconnaissance

For a long time, UAVs have been used for surveillance applications. However, with the advent of FANETs, the idea of surveillance is supposed to be more revolutionized. UAV plays a key role in reducing human intervention in patrolling a particular geographic location. Aerial surveillance tasks may involve collecting battlefield information, mapping areas affected by earthquakes, and monitoring law enforcement activities. Taking photographs of items distributed over large regions and areas of interest can also be used in surveillance work. For example, a border surveillance UAV group can detect not only unplanned humanitarian problems including weapons and drugs, but illegal border crossings [42]. The collected information can then be analyzed and transferred directly to the Intelligence Control Centers. However, data sensitivity calls for high precision and accuracy for immediate intervention. All such surveillance missions are complex in nature and are usually intolerant to false alarms.

Similar to search and rescue operations, in reconnaissance, unlicensed (i.e., Wi-Fi and Bluetooth 5) technologies can be used for cases of limited coverage areas and fewer number of nodes connectivity, whereas licensed technologies can be used for large coverage areas and mass deployment of UAVs.

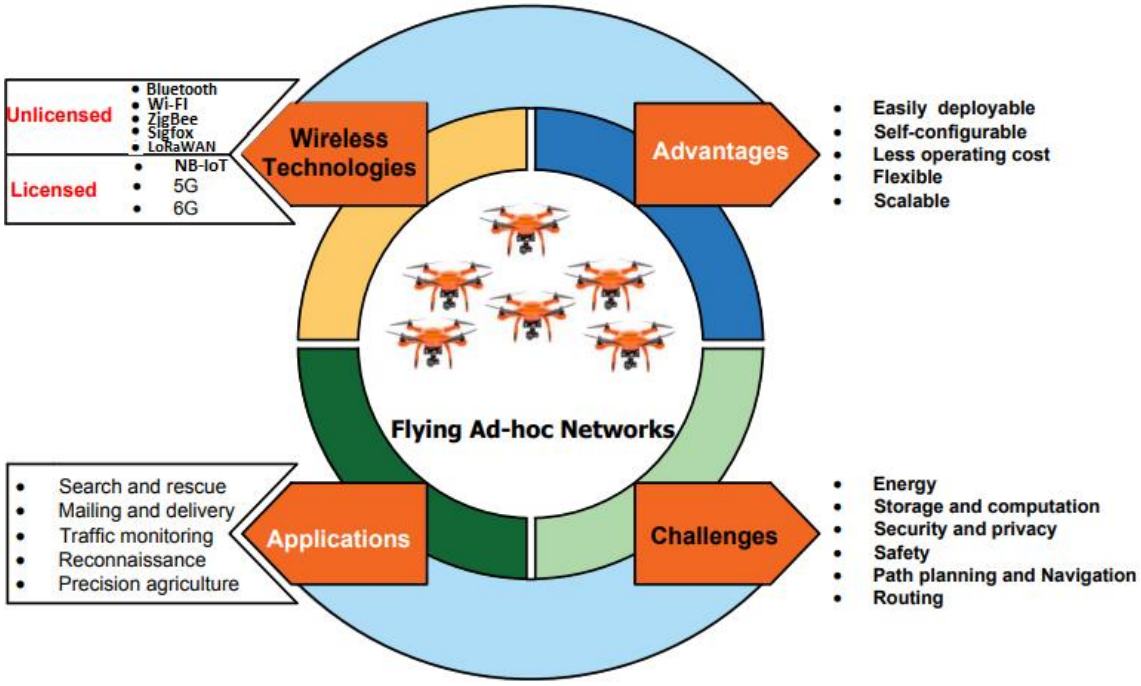

Figure 2. Advantages, key wireless technologies, applications, and challenges of flying ad-hoc networks.

4. Challenges

4.1. Security and Privacy

The design consideration of small UAVs rarely addresses the security considerations [7]. This vulnerability could adversely affect the network security and privacy, resulting in colossal damage to the information exchange operations within the network. An intruder intending to harm the FANET system has many options for carrying out malicious intentions. For example, the attacker can transmit plenty of reservation requests, eavesdrop the control messages, and/or forge the information. UAVs connected with Wi-Fi are considered to be more unsecure as opposed to cellular networks due to unreliable links and poor security mechanisms [43]. The authors in [44], ascertained that Wi-Fi-based UAVs were vulnerable to fundamental security attacks. Someone with an appropriate transmitter could attach to a UAV and embed commands into a progressing session, making it easy to interpret any UAV. In addition, UAVs can become a luring target for physical attacks in the event that it hovers over a hostile environment, which is another aspect of security concern in the UAV network [45–48]. In such instances, an attacker dissembles the captured UAV to gain access to retrieve internal data via common interfaces or ports such as a USB.

Global positioning system (GPS) spoofing [49–54] is another major security threat affecting the privacy of small UAVs in which UAV GPS signals are manipulated by an intruder. An adversary generally transmits fake GPS signals to an intended UAV with a slightly higher power than the actual GPS signals in this attack in order to trick the UAV into thinking that it is at another location. This technique can therefore be used by the attacker to send the UAV to the desired predetermined area where it can be effortlessly captured [55]. The attack environment used to exploit the GPS spoofing vulnerability of the commercial drone of the 3D Robotics firm is presented in Figure 3. A laptop with a virtual machine and a Linux operating system equipped with Ubuntu 14.04 and BladeRF X40 are required to exploit the particular vulnerability of transmitting fake coordinates. This can, however, be possible only if the necessary libraries have been designed to work with the BladeRF [56]. The cooperative localization system must use the actual positions of neighboring UAVs and their associated distances in order to avoid the GPS spoofing attack to help UAVs determine their desired location.

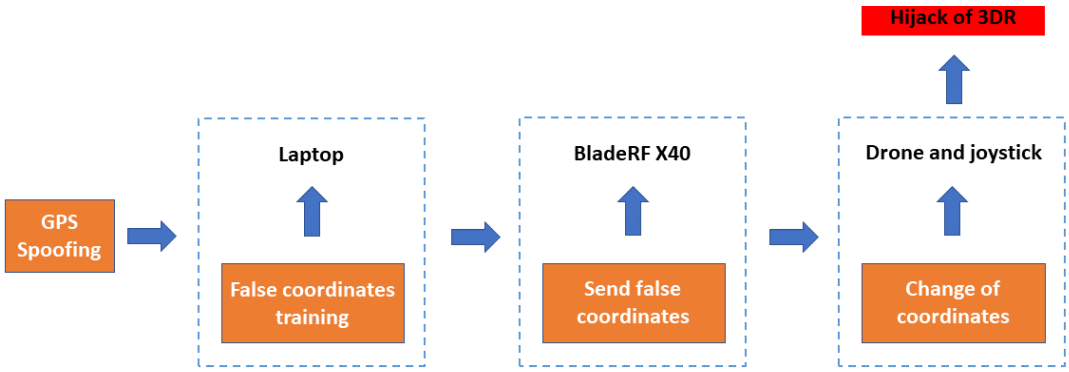

Figure 3. Global positioning system (GPS) spoofing vulnerability for the commercial drone of the company 3D Robotics [52].

4.2. Safety

FANETs deployed for various applications raise major safety issues, for example, crashing UAVs could cause tremendous damage to property or humans on the ground. This could be the result of a mid-air collisions, technological malfunction, or misuse by its operator [57,58]. Extreme weather conditions such as turbulence, lightning, battery life, and lifting capability have caused public property concerns about the failure of UAVs. In addition, there is also a significant risk of airborne accidents, leading to widespread devastation due to the sharing of airspace with other passenger planes in larger cities.

4.3. Energy Limitations

Limited onboard energy is one of the main limitations impeding the development of small UAVs. The key issue with small UAVs is flight time, because small UAVs of the general domain use standard onboard batteries that have a finite life time [59]. Additionally, it is hard to swap UAV batteries during the flight. Completing the resource-hungry applications for the FANET system in a timely fashion, is therefore a crucial task.

4.4. Storage and Computation Restrictions

The limited storage and computing capabilities mounted on small UAVs do not allow for computational-intensive tasks to be performed locally [45]. Moreover, the data aggregated by the small UAVs could be too large for the same UAV to process and store it onboard, as it engages in the monitoring task [46]. It also requires high computing and storage capacity. In addition, performing computationally intensive assignments may result in slower response times, which in turn can impede the overall performance of FANETs.

4.5. Routing

Routing allows for the UAVs to collaborate and coordinate amongst themselves and set up an optimal route for data transmission. Routing is the most challenging job in FANETs due to the unique attributes of UAVs such as high mobility, 3D movement, and rapid topology changes [60–63]. In addition, highly sensitive applications need FANETs to provide accurate, stable, and efficient data transfer. To make the applications and services more persistent and active, it is therefore important to develop and choose suitable routing protocols for FANETs. Network efficiency in terms of throughput and response time are important parameters, which is based on the potency of the algorithm running within the routing protocol.

4.6. Path Planning and Navigation

Unless UAVs collide with each other and with moving objects that appear stable or dynamic in the flying space, FANETs cannot guarantee safe operation. Thus, path planning and navigation of multiple UAVs have become a prime concern to efficiently accomplish the assigned task [64]. To prevent a possible collision and ensure the safety of the whole system, a predictive method must be established for path planning and navigation in order to find the best way to avoid collisions.

5. Open Research Topics

The research on FANETs is still in its infancy. As a flying platform, a UAV network may further contribute to various services. For more guidance in the study, some open research topics are mentioned below.

5.1. Aerial Blockchain

An emerging trend for adaptive security of privacy preferences in UAV communication networks supported by 5G, B5G, and 6G is expected to be the aerial blockchain. The privacy and integrity of data collected by UAVs can be assured using an aerial blockchain approach [65]. Furthermore, the integration of blockchain and 5G/6G technologies make the UAV communication more secure against cybersecurity vulnerabilities [66]. Blockchain-enabled UAV softwarization can also be used to provide UAV network communication services with flexible, dynamic, and on-the-fly decision capabilities [67]. Although numerous research efforts have been devoted to blockchain technology in UAV networks, researchers have not yet explored blockchain-enabled UAV network softwarization [67].

5.2. High-Speed Backhaul Connectivity

To support high data rate services, backhaul networks in 6G need to manage the huge amount of data to integrate the UAV networks with the core network. For high-speed backhaul connectivity, optical fiber and FSO networks can be a potential solution here; however, any increase in the performance of these networks is challenging due to the demand for exponential data growth [68].

5.3. Deep Reinforcement Learning

Since cellular technology is a key enabler for providing high-speed data communication services to the swarm of UAVs in the sky, however, it enforces challenges like supporting mobility [69]. Deep-reinforcement learning techniques can be used to refine handover decisions dynamically to ensure stable communication. In addition, deep-reinforcement learning methods may also be used to find the optimal way to avoid collisions during real-time path planning and navigation [70,71].

5.4. Energy Harvesting Technologies

Limited battery power and limited weight restrictions with a short flight duration time of UAVs is still a key factor in preventing the involvement of FANETs in a wide range of applications. Charging UAVs using energy harvesting technologies can overcome the short flight duration problem [72].

5.5. Virtualization of Unmanned Aerial Vehicles (UAV)-Enabled 5G Networks

UAVs can potentially be integrated into the Internet to leverage the cloud computing facility, web technologies, and service-oriented infrastructures for enabling smart IoT applications [73]. Within the same settings, UAV resources can be virtualized and integrated into an interconnected environment with other network resources. Therefore, in the future, efficient methods for the virtualization of UAV-enabled 5G networks need to be developed.

6. Conclusions

A flying ad-hoc network (FANET) is a flying platform that controls the autonomous dynamic movement of numerous UAVs, simply called drones. However, wireless communication systems that connect multiple UAVs to a FANET system have the potential for further improvements. Wireless communication systems that can be deployed quickly to functional FANETs in challenging environments are currently in high demand. In addition, for long transmission range and high data rate applications, traditional cellular communication systems can be used as a backhaul link. The inclusion of 5G and 6G technologies will make UAV networks ultra-reliable and ubiquitous. However, challenges such as security and privacy, limited onboard energy and restricted computational capabilities confine the participation of FANETs in a wide range of applications. A perfect balance between communication technologies, security schemes, and energy harvesting methods are required to provide secure and efficient communication links with long flight times and minimal communication latencies for different real-time applications. Therefore, in this article, key enabling technologies, applications, challenges, and open research problems were thoroughly investigated.

Author Contributions: Conceptualization, M.A.K. and F.N.; Methodology, M.A.K. and F.N.; Software, M.A.K. and F.N.; Validation, M.A.K., F.N., and I.U.; Formal analysis, M.A.K., F.N., and I.U.; Investigation, M.A.K. and F.N.; Resources, M.A.K. and A.A.-Z.; Data curation, M.A.K. and K.A.A.-D.; Writing—original draft preparation, M.A.K.; F.N., K.A.A.-D., and A.A.-Z.; Writing—review and editing, M.A.K., A.A.-Z., and K.A.A.-D.; Visualization, M.A.K., A.A.-Z., and K.A.A.-D.; Supervision, F.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

Abbreviations

The following abbreviations are used in this manuscript.

UAV	Unmanned Aerial Vehicle
FANETs	Flying Ad-Hoc Networks
IMU	Inertial Measurement Unit
GPS	Global Positioning System
BS	Base Station
FSO	Free Space Optics
DSE	Decision Support Engine
NDVI	Normalized Vegetation Difference Index
6G	Sixth-Generation
B5G	Beyond Fifth-Generation
mmWave	Millimeter Wave
SAR	Search and Rescue
LPWAN	Low-Power Wide Area Networks
MEC	Multi-Access Edge Computing

References

1. Shakoor, S.; Kaleem, Z.; Baig, M.I.; Chughtai, O.; Duong, T.Q.; Nguyen, L.D. Role of UAVs in Public Safety Communications: Energy Efficiency Perspective. *IEEE Access* **2019**, *7*, 140665–140679.
2. Yanmaz, E.; Yahyanejad, S.; Rinner, B.; Hellwagner, H.; Bettstetter, C. Drone networks: Communications, coordination, and sensing. *Ad Hoc Netw.* **2018**, *68*, 1–15.
3. Sharma, V. Advances in Drone Communications, State-of-the-Art and Architectures. *Drones* **2019**, *3*, 21.
4. Oubbati, O.S.; Atiquzzaman, M.; Lorenz, P.; Tareque, M.H.; Hossain, M.S. Routing in Flying Ad Hoc Networks: Survey, Constraints, and Future Challenge Perspectives. *IEEE Access* **2019**, *7*, 81057–81105.
5. Guillen-Perez, A.; Cano, M.-D. Flying Ad Hoc Networks: A New Domain for Network Communications. *Sensors* **2018**, *18*, 3571.

6. Khan, M.A.; Qureshi, I.M.; Khanzada, F. A Hybrid Communication Scheme for Efficient and Low-Cost Deployment of Future Flying Ad-Hoc Network (FANET). *Drones* **2019**, *3*, 16.
7. Khan, M.A.; Khalid, A.; Khanzada, F. Dual-Radio Dual-Band Configuration for Flexible Communication in Flying Ad-hoc Networks (FANET). In Proceedings of the International Conference on Communication Technologies (ComTech'2019), Rawalpindi, Pakistan, 20–21 March 2019.
8. Marchese, M.; Moheddine, A.; Patrone, F. IoT and UAV Integration in 5G Hybrid Terrestrial-Satellite Networks. *Sensors* **2019**, *19*, 3704.
9. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *arXiv* **2019**, arXiv:1902.10265.
10. Lin, C.; He, D.; Kumar, N.; Choo, K.-K.R.; Vinel, A.; Huang, X. Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Commun. Mag*. **2018**, *56*, 64–69.
11. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and Privacy Issues of UAV: A Survey. *Mobile Netw. Appl.* **2019**, *25*, 95–101.
12. Hassanalian, M.; Abdelkefi, A. Classifications, applications, and design challenges of drones: A review. *Prog. Aerosp. Sci.* **2017**, *91*, 99–131.
13. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.W.; Jayakody, U.N.K.; Wang, H.-C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 02739.
14. Zhang, S.; Zhang, H.; Song, L. Beyond D2D: Full Dimension UAV-to-Everything Communications in 6G. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6592–6602.
15. Van den Bergh, B.; Chiumento, A.; Pollin, S. Ultra-Reliable IEEE 802.11 for UAV Video Streaming: From Network to Application. In *Advances in Ubiquitous Networking 2. UNet 2016*; El-Azouzi, R., Menasche, D., Sabir, E., De Pellegrini, F., Benjillali, M., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2016; Volume 397.
16. Bluetooth Core Specification, Bluetooth Special Interest Group (SIG). 2016. Available online: https://www.bluetooth.com/specifications/bluetooth-core-specification (accessed on 1 September 2020).
17. Sharma, V.; You, I.; Pau, G.; Collotta, M.; Lim, J.D.; Kim, J.N. LoRaWAN-Based Energy-Efficient Surveillance by Drones for Intelligent Transportation Systems. *Energies* **2018**, *11*, 573.
18. Neumann, P.; Montavont, J.; Noël, T. Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study. In Proceedings of the 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, USA, 17–19 October 2016; pp. 1–8.
19. Bardyn, J.P.; Melly, T.; Seller, O.; Sornin, N. IoT: The era of LPWAN is starting now. In Proceedings of the 42nd European Solid-State Circuits Conference (ESSCIRC Conference 2016), Lausanne, Switzerland, 12–15 September 2016; pp. 25–30.
20. Sanchez-Iborra, R.; Gamez, J.S.; Santa, J.; Fernandez, P.J.; Skarmeta, A.F. Integrating LP-WAN Communications within the Vehicular Ecosystem. *J. Internet Serv. Inf. Secur*. **2017**, *7*, 45–56.
21. Garcia, D.; Marin, R.; Kandasamy, A.; Pelov, A. LoRaWAN Authentication in RADIUS Draft-Garcia-RadextRadius-Lorawan-03. 2 May 2017. Available online: https://www.ietf.org/archive/id/draft-garcia-radextradius-lorawan-03.txt (accessed on 26 December 2017).
22. Garcia, D.; Marin, R.; Kandasamy, A.; Pelov, A. LoRaWAN Authentication in Diameter Draft-Garcia-DimeDiameter-Lorawan-00. 30 May 2016. Available online: https://tools.ietf.org/html/draft-garcia-dimediameter-lorawan-00 (accessed on 26 December 2017).
23. LoRa Alliance Technology. Available online: https://www.lora-alliance.org/technology (accessed on 25 January 2018).
24. Casals, L.; Mir, B.; Vidal, R.; Gomez, C. Modeling the Energy Performance of LoRaWAN. *Sensors* **2017**, *17*, 2364.
25. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Enhancing the security of the IoT LoraWAN architecture. In Proceedings of the International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), Paris, France, 22–25 November 2016; pp. 1–7.
26. Sornin, N.; Luis, M.; Eirich, T.; Kramp, T.; Hersent, O. *LoRaWAN Specification V1.0.2*; Technical Report; LoRa Alliance: Beaverton, OR, USA, 2016.
27. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360.

28. Hayat, S.; Yanmaz, E.; Muzaffar, M. Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Commun. Surveys Tutor.* **2016**, *18*, 2624–2661.
29. Półka, M.; Ptak, S.; Kuziora, Ł. The use of UAV's for search and rescue operations. *Procedia Eng.* **2017**, *192*, 748–752.
30. Zafar, W.; Khan, B.M. Flying Ad-Hoc Networks: Technological and Social Implications. *IEEE Technol. Soc. Mag.* **2016**, *35*, 67–74.
31. Allmer, T.; Fuchs, C.; Kreilinger, V.; Sevignani, S. Social networking sites in the surveillance society. In *Media, Surveillance, and Identity: Social Perspectives*; Jansson, A., Christensen, M., Eds.; Peter Lang: New York, NY, USA, 2014; pp. 49–70.
32. Alsaeedy, A.A.R.; Chong, E.K.P. 5G and UAVs for Mission-Critical Communications: Swift Network Recovery for Search-and-Rescue Operations. *Mob. Netw. Appl.* **2020**, 1–19.
33. Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of drones. *IEEE Access* **2016**, *4*, 1148–1162.
34. Gross, D. Amazon's Drone Delivery: How Would it Work? 2013. Available online: http://www.cnn.com/2013/12/02/tech/innovation/amazon drones-questions/ (accessed on 14 August 2020).
35. FedEx Corporation. Q1 Fiscal 2015 Statistics. 2015. Available online: http://investors.fedex.com/files/doc downloads/ statistical/FedEx-Q1-FY15-Stat-Book v001 t195uu.pdf (accessed on 14 August 2020).
36. Khan, M.A.; Alvi, B.A.; Safi, A.; Khan, I.U. Drones for Good in Smart Cities: A Review. In Proceedings of the International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC), Tamil Nadu, India, 28–29 January 2018.
37. Ke, R.; Li, Z.; Kim, S.; Ash, J.; Cui, Z.; Wang, Y. Real-time bidirectional traffic flow parameter estimation from aerial videos. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 890–901.
38. Guido, G.; Gallelli, V.; Rogano, D.; Vitale, A. Evaluating the accuracy of vehicle tracking data obtained from unmanned aerial vehicles. *Int. J. Transp. Sci. Technol.* **2016**, *5*, 136–151.
39. Leitloff, J.; Rosenbaum, D.; Kurz, F.; Meynberg, O.; Reinartz, P. An operational system for estimating road traffic information from aerial images. *Remote Sens.* **2014**, *6*, 11315–11341.
40. Tsouros, D.C.; Bibi, S.; Sarigiannidis, P.G. A review on UAV-based applications for precision agriculture. *Information* **2019**, *10*, 349.
41. Shafi, U.; Mumtaz, R.; García-Nieto, J.; Hassan, S.A.; Zaidi, S.; Iqbal, N. Precision Agriculture Techniques and Practices: From Considerations to Applications. *Sensors* **2019**, *19*, 3796.
42. Berrahal, S.; Kim, J.H.; Rekhis, S.; Boudriga, N.; Wilkins, D.; Acevedo, J. Border Surveillance Monitoring Using Quadcopter UAV-Aided Wireless Sensor Networks. *J. Commun. Softw. Syst.* **2016**, *12*, 67–82.
43. Zeng, Y.; Zhang, R.; Lim, T.J. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Commun. Mag.* **2016**, *54*, 36–42.
44. Hooper, M.; Tian, Y.; Zhou, R.; Cao, B.; Lauf, A.P.; Watkins, L.; Robinson, W.H.; Alexis, W. Securing commercial Wi-Fi-based UAVs from common security attacks. In Proceedings of the Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016.
45. Khan, M.A.; Ullah, I.; Nisar, S.; Noor, F.; Qureshi, I.M.; Khanzada, F.; Khattak, H.; Aziz, M.A. Multi-access Edge Computing (MEC) Enabled Flying Ad-hoc Networks with Secure Deployment Using Identity Based Generalized Signcryption. *Mob. Inf. Syst.* **2020**, *2020*, 8861947.
46. Khan, M.A.; Ullah, I.; Qureshi, I.M.; Noor, F.; Khanzada, F. An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-Hoc Network. *IEEE Access* **2020**, *8*, 36807–36828.
47. Khan, M.A.; Qureshi, I.M.; Ullah, I.; Khan, S.; Khanzada, F.; Noor, F. An Efficient and Provably Secure Certificateless Blind Signature Scheme for Flying Ad-Hoc Network Based on Multi-Access Edge Computing. *Electronics* **2020**, *9*, 30.
48. Jiang, B.; Yang, J.; Song, H. Protecting Privacy From Aerial photography: State of the Art, Opportunities, and Challenges. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 799–804.
49. Guo, Y.; Wu, M.; Tang, K.; Tie, J.; Li, X. Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6557–6564.
50. Eldosouky, A.; Ferdowsi, A.; Saad, W. "Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet Things J.* **2020**, *7*, 2840–2854.
51. Krishna, C.G.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199.

52. Arteaga, S.P.; Hernández, L.A.M.; Pérez, G.S.; Orozco, A.L.S.; Villalba, L.J.G. Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. *IEEE Access* **2019**, *7*, 51782–51789.
53. Feng, Z.; Guan, N.; Lv, M.; Liu, W.; Deng, Q.; Liu, X.; Yi, W. Efficient drone hijacking detection using onboard motion sensors. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Lausanne, Switzerland, 27–31 March 2017; pp. 1414–1419.
54. Wang, J. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends. *arXiv* **2020**, arXiv:2008.12461.
55. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636.
56. Kang, W.C.; Aimin, S.P. Time and position spoong with open source projects. *Proc. Black Hat Eur*. **2015**, *148*, 1–8.
57. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442.
58. Bolkcom, C.; Bone, E. Unmanned aerial vehicles: Background and issues for congress, report for congress, congressional research service. In *Library of Congress*; UNT Digital Library: Washington, DC, USA, 2003.
59. Li, B.; Fei, Z.; Zhang, Y. UAV communications for 5G and beyond: Recent advances and future trends. *IEEE Internet Things J.* **2018**, *6*, 2241–2263.
60. Sang, Q.; Wu, H.; Xing, L.; Xie, P. Review and Comparison of Emerging Routing Protocols in Flying Ad Hoc Networks. *Symmetry* **2020**, *12*, 971.
61. Khan, M.A.; Khan, I.U.; Safi, A.; Quershi, I.M. Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols. *Drones* **2018**, *2*, 27.
62. Lakew, D.S.; Sa'ad, U.; Dao, N.-N.; Na, W.; Cho, S. Routing in Flying Ad Hoc Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1071–1120.
63. Khan, M.A.; Qureshi, I.M.; Safi, A.; Khan, I.U. Flying Ad-Hoc Networks (FANETs): A Review of Communication architectures, and Routing protocols. In Proceedings of the 2017 First International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT), Karachi, Pakistan, 15–16 November 2017; pp. 692–699.
64. Ashraf, A.; Majd, A.; Troubitsyna. E. Online Path Generation and Navigation for Swarms of UAVs. *Sci. Program.* **2020**, *2020*, 8530763.
65. Li, B.; Fei, Z.; Zhang, Y.; Guizani, M. Secure UAV communication networks over 5G. *IEEE Wirel. Commun.* **2019**, *26*, 114–120.
66. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538.
67. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. A taxonomy of blockchain-enabled softwarization for secure UAV network. *Comput. Commun.* **2020**, *161*, 304–323.
68. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions. *arXiv* **2019**, arXiv:1909.11315.
69. Chen, Y.; Lin, X.; Khan,T.; Mozaffari, M. Efficient Drone Mobility Support Using Reinforcement Learning. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea, 25–28 May 2020; pp. 1–6.
70. Challita, U.; Saad, W.; Bettstetter, C. Deep Reinforcement Learning for Interference-Aware Path Planning of Cellular-Connected UAVs. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
71. Liu, Q.; Shi, L.; Sun, L.; Li, J.; Ding, M.; Shu, F. Path Planning for UAV-Mounted Mobile Edge Computing With Deep Reinforcement Learning. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5723–5728.
72. Liu, Q.; Li, M.;Yang, J.; Lv, J.; Hwang, J.; Hossain, A.S.; Muhammad, G. Joint power and time allocation in energy harvesting of UAV operating system. *Comput. Commun.* **2020**, *150*, 811–817.
73. Sekander, S.; Tabassum, H.; Hossain, E. Multi-tier drone architecture for 5G/B5G cellular networks: Challenges, trends, and prospects. *IEEE Commun. Mag.* **2018**, *56*, 96–103.