IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 21, 2018, accepted May 7, 2018, date of publication May 18, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2838062

Antenna and Propagation Considerations for Amateur UAV Monitoring

NAN ZHAO[1], XIAODONG YANG[1], (Senior Member, IEEE), AIFENG REN[1], ZHIYA ZHANG[1], WEI ZHAO[2], FANGMING HU[1], MASOOD UR REHMAN[3], (Senior Member, IEEE), HAIDER ABBAS[4], (Senior Member, IEEE), AND MEHRAN ABOLHASAN[5], (Senior Member, IEEE)

[1]School of Electronic Engineering, Xidian University, Xi'an 710071, China
[2]School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China
[3]Centre for Wireless Research, University of Bedfordshire, Luton LU1 3JU, U.K.
[4]National University of Sciences and Technology, Islamabad 44000, Pakistan
[5]School of Computing and Communications, University of Technology Sydney, Ultimo, NSW 2007, Australia

Corresponding author: Xiaodong Yang (xdyang@xidian.edu.cn)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant JB180205, in part by the National Natural Science Foundation of China under Grants 61671349, 61301175, and 61601338, and in part by the International Scientific and Technological Cooperation and Exchange Projects in Shaanxi Province under Grant 2017KW-005.

ABSTRACT The broad application spectrum of unmanned aerial vehicles is making them one of the most promising technologies of Internet of Things era. Proactive prevention for public safety threats is one of the key areas with vast potential of surveillance and monitoring drones. Antennas play a vital role in such applications to establish reliable communication in these scenarios. This paper considers line-of-sight and non-line-of-sight threat scenarios with the perspective of antennas and electromagnetic wave propagation.

INDEX TERMS UAV, surveillance drones, amateur monitoring, antenna and propagation.

I. PRIMER

Unmanned Aerial Vehicles (UAVs) have gone through a long history of technological development, almost as long as the invention of the airplane by the Wright brothers. Like their manned counterparts, the earliest UAVs belonged to the military and used for training, spying or eliminating a target. The UAVs have always been part of the aviation history though buried in oblivion in the yesteryears in contrast to the flying heroes with chest full of medals telling their glorious deeds [1]. Recent years have seen them grow significantly in technology as well as commercial usage [2].

UAVs can fly a few meters from the ground, which can fill the gap between the low-resolution satellite images and data acquisition vehicles that rely on the weather effectively. A specially designed camera on the platform combined with data cloud can have applications ranging from data acquisition, surveillance and monitoring, transportation, emergency relief, infrastructure develop-ment, agriculture and scientific research [3]. The UAVs enable the construction enterprises to quantify engineering progress in real time, allow road network data collection in all directions, help forest fire fighting, enable fast courier service, allow farmers to continuously monitor crop growth and allow mining owners to obtain accurate individual digging information. Energy and infrastructure companies can thoroughly inspect pipelines, roads and cables by using the UAVs. Humanitarian organizations can use the UAVs to quickly assess the affected zone, adapt to refugee and provide effective relief based on the collected data. A transport UAV with a load capacity can take off and land near a building or a human settlement, enabling developing countries to achieve rapid logistics even without adequate road infrastructure, release the convenience of e-commerce and development of the national economy quickly. In developed countries, transport UAVs can help to achieve better quality of service in crowded or remote areas.

An UAV with inspection function may fly in a confined space to assist the fire or emergency unit assessing the level of danger by finding building cracks, road hazards, situation of bridges and tunnels faster and safer. The UAVs can cross the complex terrestrial environment easily that is a huge obstruction for ground robots. For telecom companies, the UAVs can act as a mobile and temporary private network base station. Some groups use UAVs instead of manned helicopters to study volcanic eruptions eliminating the risks of volcanic eruption and loss of life with obvious advantage [3].

Rapid maturity of microelectronics and materials industry along with novel miniaturization techniques hasresulted in unlimited potential for the UAVs. Today, a wide variety of

	Endurance Time	Flying Distance	Load Capacity	Frequency	Power Source	Convenience	Hover Time
 Airship	●●●●○	●●●●○	●●●●○	Infrared 2.4/5 GHz	Hybrid Power	●○○○○	●●●●●
 Fixed Wing	●●●○○	●●●○○	●●○○○	2.4/5 GHz	Hybrid Power	●●○○○	●○○○○
 Helicopter	●●○○○	●●○○○	●●●○○	2.4/5 GHz	Single Power	●●●○○	●●●○○
 Four Rotor	●○○○○	●●○○○	●●○○○	2.4/5 GHz	Single Power	●●●●○	●●●○○

	External Sensor	Calculate Ability	Staff Supervision Required	Current Level	Deployment Platform
Sensory	None or few	Little	Yes	Deployed	All types
Reactive	Few and sparse	Medium	Little	Partly deployed	Fixed wing, rotorcraft and flapping wing
Cognitive	Several and high density	High	None	Not yet deployed	Mostly rotorcraft

FIGURE 1. Common aircraft types and their autonomous control requirements.

drones are in operation to open an era of sharing the sky with traditional sky owners, the airplanes. Aviation regulations around the world are being updated or supplemented to accommodate this great change. According to the federal aviation administration, there will be 10,000 UAVs soaring in the United States skies alone by 2020, bringing huge benefits to social economy [4].

II. TYPES OF UAVs

There are various types of amateur drones available in the market, weighing from a few hundred grams to kilograms [5]. The most common types include fixed-wing, rotor aircraft, and flapping wing based on the bionic structure [3]. They are usually powered by batteries or fuel engines. The electrically driven UAVs are generally low in requirements, are more reliable and quieter than the one using the fuel engines but have very short flight distance. Fixed-wing drones are easy to design, they are cost effective, and they can quickly and efficiently fly, but usually are very difficult to hover. They are able to fly longer distances by having larger fixed wings. A larger wing also increases the load capacity at the expense of higher takeoff requirements. Helicopters are generally portable and require less space for take-off. The rotorcraft can be hovered well, but they are less efficient on forward flight. The bionic flapping wing provides a possible compromise, but the fluid mechanics and control problems are more challenging than the first two categories.

Due to the distrust on human operation, many studies are trying to achieve a complete autonomous UAV where the UAV itself judges the next action and follows the set target. In order to achieve this goal and in ensure that the UAV completes the task in a particular space or near the ground, the existing mechanical and electronic design will be completely updated and requires complying with the autonomic control logic (Fig. 1) [3]. These scene positioning signals and remote control are often not accurate enough or difficult to reach. Some preliminary conclusions, such as underwater electromagnetic wave 3D positioning studies have been reported [6]. This is a promising direction, but it requires continuous efforts.

III. STANDARDIZATION REQUIREMENTS

Everything looks good and thriving for the UAVs until public safety issues are considered due to their small size [7]. Many UAVs are only about 1 meter in size making them difficult to be spotted by the airplane pilots. Larger number of drone

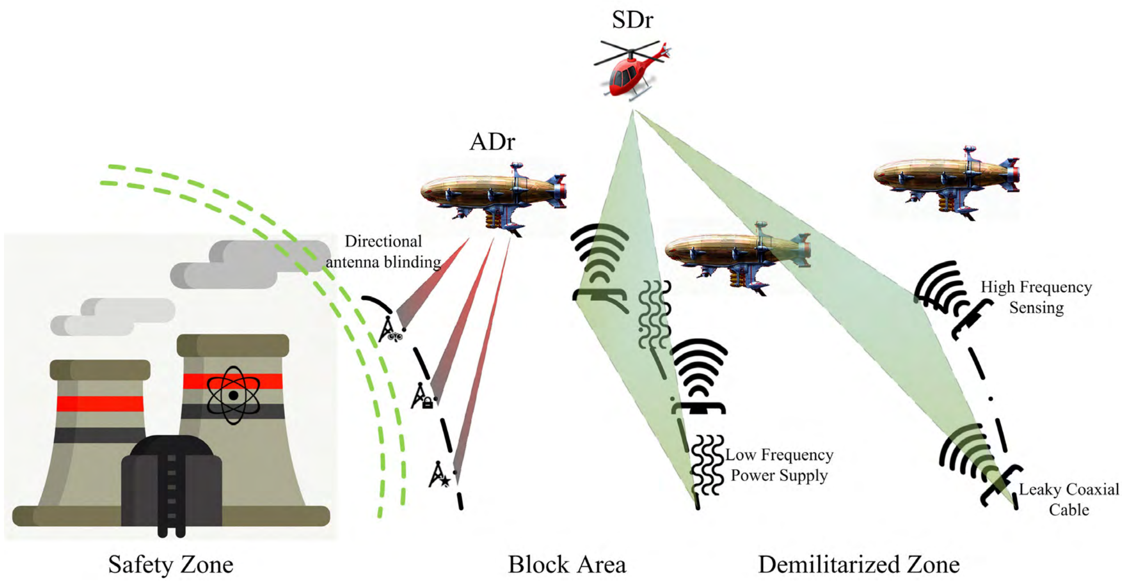


FIGURE 2. Concept of a regulated UAV system based on leaky wave cable and directional antennas to cooperate with SDr to realize the discovery and control of ADr.

usage also brings serious challenges in air traffic control. Collision avoidance of the UAVs with other drones and legacy air traffic is a challenging task. Visible or infrared cameras provide a cheap and effective technical solution, but the clouds in the sky limit their scope of application. Breach of people's privacy is another major concern by the use of high-resolution cameras, infrared detectors, and even faces recognition software on the UAV terminal [8]. Some government regulations require amateur drones to fly within the operator's vision, but this rule ignores the fact that today's drones allow you to see their location through mobile phones or computer screens and even virtual reality devices.

There are huge safety concerns surrounding the UAVs. Combined with a sharp blade, even a 500g UAV will generate enough potential energy to cause a permanent damage to the fragile human body in the event of an accident or failure. The US Federal Aviation Administration published a roadmap in 2013 [3], stating that by 2028 civilian unmanned aircraft could fly out of the operator's line of sight and gradually integrate into the national airspace management system. Likewise, the British regulations permit flying a UAV weighing less than 20 kilograms in the crowded area, within the operator's line of sight. Although we cannot see that there is a huge technical barrier to the community to accept more independent research or commercial UAV control in the next five years, as a result of the possible changes in government policy, an autonomous UAV's flight in the actual environment may be illegal until 2028 in the United States and Europe.

The 21st century will be in many ways a century of robotics where the UAVs must and will play an important role. It is important to address the legal challenges posed by the development of unmanned air vehicles, including privacy and airspace safety. Improvements and additions to airspace management may make UAV flights more orderly, but privacy and airspace security issues that rely on the law alone may not be enough, the key is how to implement. Survey [9] proposed guidelines for privacy protection related models, it can be used in UAV related research. In the absence of concrete regulations and standards, commercial usage of the drone technology is severely daunted.

Due to the lack of regulatory techniques, some too harsh regulations were introduced. Beginning in 2014, DJI, one of the world's leading amateur UAVs manufacturers, began to update their UAV firmware (the UAV's brain), in collaboration with the local authorities, airport and the seat of government to standardize the UAV operation and set boundaries for the UAV flight [10]. In case the UAV operators decide to ignore the restricted airspace warning and continue the flight (either malicious or just curious), the firmware will make the UAV unmoved. Some of regulations consider auxiliary means of scientific research as "illegal" [11]. Amateur drones are generally banned from commercial airspace [5]. In fact, the current management has established a double standard, entertainment users can use the UAVs (often inexperienced), but trained researchers cannot. Some researchers have to use other alternative means, for example, a large kite to carry the camera to collect data, but such a compromise has obvious shortcomings, no wind no data. Concept of a regulated drone system is illustrated in Fig.2. The electronic fence is consisting of the ground leaky cable and the air surveillance drones (SDr) that collectively monitor the possible intruders in the airspace. The nuclear power plant in the Safety Zone represents the target needed to be protected from unauthorized drone flights. Three directional antennas placed in Block Area represent use of directional beam blinding the incoming UAVs that could invade the Safety Zone of amateur drone (ADr). The mooring cable in Demilitarized Zone has a dual frequency attribute, where low frequency waves are

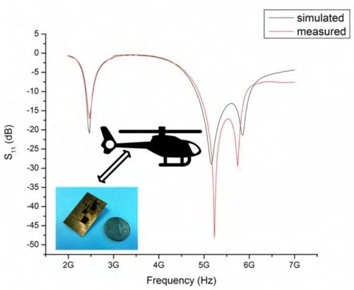
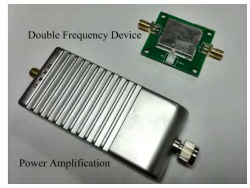
Dual Frequency PIFA Antenna	Directional Antenna	Angle Reflector	Double Frequency Device Power Amplification
			
Using a dual-band antenna on SDr, which can receive 2.4 / 5 GHz signal	Concentrated power, directional blinding antenna	Increase radar echo, enemy identification	Increase the power and frequency

FIGURE 3. Useful microwave devices for the UAV detection system.

collected for SDr energy, and high frequency constitutes an electronic fence to detect possible intrusion. The details of each antenna and radio wave propagation unit are given in the following sections.

IV. ADr SURVEILLANCE WITH ANTENNA DEVICES

Large majority of existing commercial ADr control works at a single frequency band of 2.4/5 GHz due to cost issues. For better perception of suspicious ADr control signal, it is practical to have a dual-band operation for the SDr using a dual-band antenna. As shown in the Fig. 3, a dual-band PIFA antenna operating at 2.4/5 GHz is designed to increase the sensitivity at 5 GHz as this band is more susceptible than 2.4 GHz. Dual-band PIFA is an omni-directional antenna that can be a good monitor of incoming threats in all directions. Combined electromagnetic noise in the sky is cleaner. Its low profile design also makes the antenna cost-effective and easy to integrate. The antenna is embedded in the lower part of the fuselage in order to better receive the control signal from the ground. This could be own flight control signal or possible intruder signal. Antenna has to fulfill three key tasks; facilitate own communication, perceive suspected signal in the same airspace, and establishment of the electronic fence on earth and sky.

Self-communication, as the eye in the sky, requires the control of the ground station, as the autonomous controlled aircraft in Fig. 2 remains in the laboratory phase for the time being. Suspicious command monitoring through monitoring the ADr's own flight control signal can be useful to find suspicious objects, rather than using image segmentation identification or other feature recognition. Stable and significant characterized flight control signals are easier to identify than image segmentation. Sky and earth integrated electronic fence is achieved through the electromagnetic waves to form an invisible wall (as shown in Fig. 2). Under normal circumstances, the airspace is clear and the electronic fence is not much of interference. But when there is foreign invasion, especially non-biological, will produce a reflection or scattering of electromagnetic waves disturbing the system to expose itself.

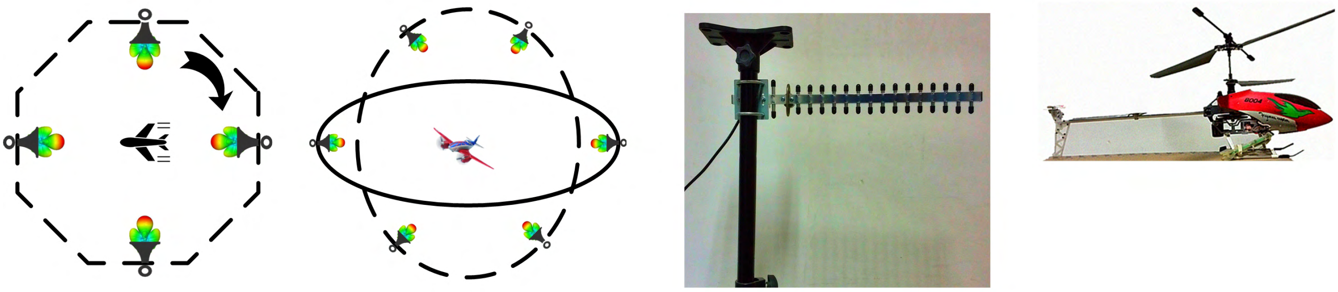
In Fig.2, the system uses directional Yagi antenna (25 dBi 16 units) as a deterrent to blind the attacking ADr into the block area. Use of the Yagi antenna with high gain and narrow beam helps to form multiple beams with a high energy density ‘‘black barrier’’. To cut off the link between the ADr and its controller, the ‘‘black barrier’’ makes the background noise power effectively equal to the command's SNR so that the command of the intrusion operator is submerged in the background noise. Multi beam synthesis can be a good block to the ADr, but also impacts the other objects in the sky minimum resulting in the SDr to perform its duties properly.

Angle reflector is a smart low profile device that improves the radar echo and when integrated in the SDr, achieves effective enemy identification. The aircraft generally considers airflow line dynamics. For the flying

objects, accuracy of the image resolution is inversely proportional to the distance, and it is obvious that the distance is too far to be seen. Corner reflectors can amplify SDr echo characteristics as well as the echo of a mid-size intruding aircraft. It helps to distinguish between the SDr and ADr, and it is convenient for directional antennas to aim at targets that should be aligned.

Power amplifier and frequency multiplier are basic RF devices. Amplifiers are used to enhance the background noise power level. If high background noise can be implemented in a certain region, the command of ADr operator is less effective. Maximum working power of the power amplifier is 8 W, which can cover the whole UAV remote control band. Frequency multiplier is being used as a frequency doubler enabling the SDr to interfere with two frequency bands simultaneously using a single signal source.

The proposed antenna system's usability is established through measurements of the ADr data. Multi-angle acquisition of the spectral data in two-dimensional plane is noted



(a) (b) (c)

FIGURE 4. Acquisition of electromagnetic spectrum characteristics of UAV from plane to three-dimensional space.

using DEVISER E8000 Spectrum Analyzer and rotating the directional antenna clockwise as shown in Fig.4 (a). The rotor is started but not took off in this configuration. The data for three-dimensional motion of the aircraft in the air, as shown in Fig.4 (b), is acquired next for experimental repeatability. The aircraft started the rotor and simulated the free flight state but cable bound. The measurement photos are shown in Fig.4 (c). The measured data has exhibited poor reproducibility and correlation especially with change of angles. It is inferred that since the UAV has its own movement, the acquisition system also has relative movement. Different angles, distances, and different environmental backgrounds have a random effect on the data. High frequency rotor, which is the source of aircraft power, is different from the natural environment, so it is more feasible to identify the electromagnetic characteristics of the whole aircraft and then to capture the ADr. At the same time, it is proved that the SDr monitoring ADr flight control command is an effective early warning method. The control command characteristics are obvious, and the working frequency band is known making the data collection and observation simple. After preliminary tests, the electromagnetic spectrum parameters of different brand or types of drones are very different. However, the control frequency band is highly similar, except that the coding is done to avoid collisions.

V. NLoS AND LoS THREAT COUNTERMEASURES

The existing UAV attack modes can be summarized as non-line-of-sight (NLoS) and line-of-sight (LoS). In NLoS attacks, the attacker sets the target and ADr will fly according to the given coordinates. Such threats are easy to implement, and the operator may have left the location of takeoff location. The ADr itself does not contain redundant information and acts as a pawn to implement the threat or a terrorist attack. In LoS mode, the ADr attacks being within the range of the operator's vision. Due to the limitations of amateur ADr console power and state regulations, amateur drones mostly fly within a limited range. There is no malicious but curious threat likely to occur in this mode. Such threats are often more intelligent because of the presence of human controllers. The NLoS threat has a long history. There were balloon bombs during the world wars, setting the initiation time and taking off from the upper airside. Though blind but can make panic because you do not know where ADr will go next. For such threats, the main countermeasures are surveillance and misleading.

We try to deal with a shadow noise (war fog). The setup is shown in Fig. 5 (a) where a GPS antenna is erected in the target area (blue grid), the real target area is covered from the GPS signal emitted by the satellite, and the local coordinates are projected to other regions (time-variation). NLoS ADr cannot reach the target area according to the instruction. Because the coordinates are always changing, the wandering behavior of itself (irregular, multiple transformation direction of flight) has become the intrusion detection feature. Intrusion detection is divided into logical or practical, a forward-looking WSN intrusion detection logic is presented in [12]. Because civilian GPS does not take certification [2], such strategies can be deployed at a small cost. The embedded development board and a sufficiently long GPS antenna to implement the response (a long enough GPS antenna can ensure that the "war fog" affects the sky rather than other normal services on the ground) are shown in Fig.5 (b). A spectrum analyzer adjusted to the GPS mode is monitoring the GPS signal from the satellite, confirming that the deployed projection noise does not affect ground services.

The LoS threat can cause trouble more accurately. Technical means can fool large number of low-level ADr attacks but not carefully prepared malicious attackers. As shown in Fig. 2, the SDr monitors the 2.4/5 GHz flight control signal in the Demilitarized Zone. If any strange signal is broadcasted, it is certain that there is new UAV launch (set as an ADr). At the same time, the leaky cable lies on the ground and launches high frequency electromagnetic wave. The SDr acts as an air base station receiving the electromagnetic wave. Due to a certain direction, the electromagnetic wave will become an electromagnetic wall. An object reaching near to this wall or passing through it will have a great impact on the channel condition as discussed earlier. Considering the SDr is a very important air hub, the airtime will greatly affect the performance of the whole system. Through the SDr carries a large capacity rechargeable battery itself,

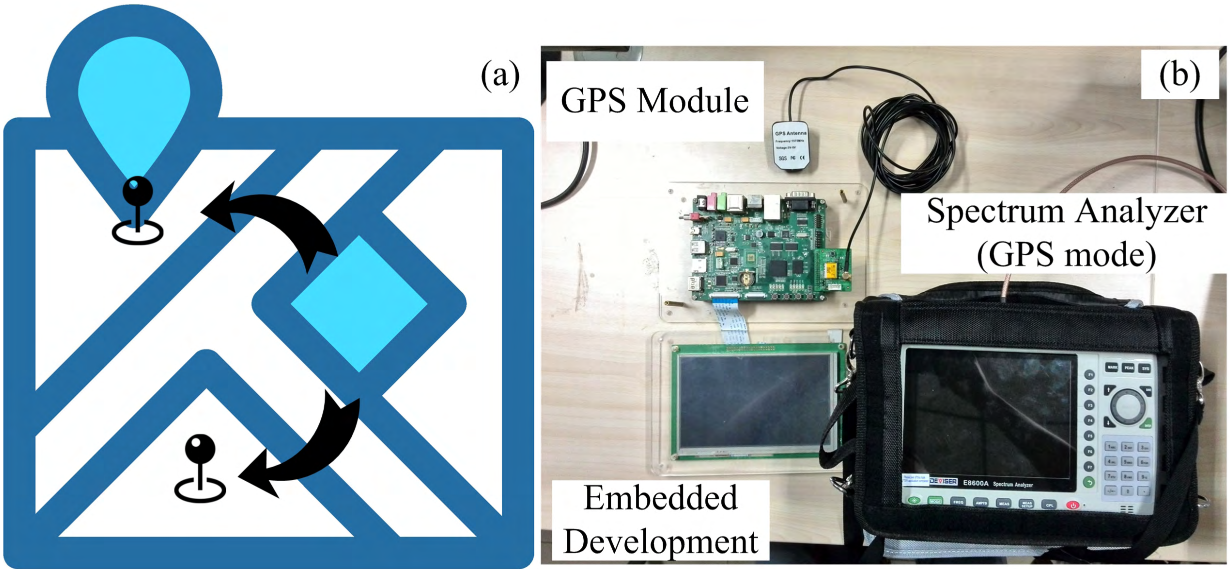


FIGURE 5. War fog, GPS coordinate mapping changes over time.

a hybrid approach having low-frequency radio wave energy harvesting can achieve remote non-contact energy supply to increase the airtime significantly and enhance the effectiveness of amateur drone surveillance. Although, the application scenario is not completely same, the SDr energy harvesting can follow principles as laid out for wireless body area networks [13].

VI. CONCLUSION AND FUTURE WORK

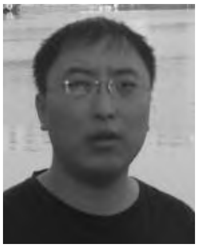
The rise of unmanned aerial vehicles will bring a brighter future, but need careful consideration of safety, privacy and regulatory issues, which will gradually, perfected as the technology matures.

This paper introduces a regulated drone surveillance system based on the antenna and radio wave propagation. In fact, from this point of view, the UAVs still have a lot of work worth doing such as analysis of UAV spectrum data and effective interference mitigation are all open issues. Military or specially designed drones are not within the scope of this article due to non-availability of data. It is experimentally observed that in contrast to the 2.4/5 GHz crowded frequency band, high frequency bands (60 GHz or even higher) seems more suitable for commercial UAV control because the air itself can bring high path loss, can limit UAV flight area, almost cannot be out of sight (which is enough for entertainment applications). The enduring UAV can be open to universities, research institutions and certified users to avoid a lot of air management problems.

REFERENCES

[1] J. Villasenor, "'Drones' and the future of domestic aviation [point of view]," *Proc. IEEE*, vol. 102, no. 3, pp. 235–238, Mar. 2014.
[2] K. Wesson and T. Humphreys, "Hacking drones," *Sci. Amer.*, vol. 309, no. 5, p. 54, 2013.
[3] D. Floreano and R. J. Wood, "Science, technology and the future of small autonomous drones," *Nature*, vol. 521, pp. 460–466, May 2015.
[4] S. C. P. Williams, "Studying volcanic eruptions with aerial drones," *Proc. Nat. Acad. Sci. USA*, vol. 110, no. 27,p. 10881, Jul. 2013.
[5] N. Stafford, "Spy in the sky," *Nature*, vol. 445, no. 7130, p. 808, 2007.
[6] M. F. Hossain, M. B. Wali, K. S. Munasinghe, and A. Jamalipour, "Three dimensional (3D) underwater sensor network architectures for intruder localization using EM wave," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Doha, Qatar, Apr. 2016, pp. 1–6.
[7] D. Pogue, "Unclear for takeoff," *Sci. Amer.*, vol. 312, no. 4, pp. 35–35, 2015.
[8] "The spies above your backyard," *Sci. Amer.*, vol. 308, no. 4, p. 12, 2013.
[9] J. M. de Fuentes, L. González-Manzano, and O. Mirzaei, "Privacy models in wireless sensor networks: A survey," *J. Sensors*, vol. 2016, 2016, Art. no. 4082084.
[10] J. Hsu, "Cloudy with a chance of drones," *Sci. Amer.*, vol. 313, no. 3, p. 20, 2015.
[11] H. Ledford, "US drone research hits regulatory turbulence," *Nature*, vol. 512, no. 7514, pp. 239–240, Aug. 2014.
[12] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2006, pp. 640–644.
[13] F. Akhtar and M. H. Rehmani, "Energy harvesting for self-sustainable wireless body area networks," *IT Professional*, vol. 19, no. 2, pp. 32–40, Mar./Apr. 2017.

NAN ZHAO is currently pursuing the Ph.D. degree with Xidian University.



XIAODONG YANG (SM'17) has authored over 50 peer-reviewed papers in highly ranked journals. His research interests include body area networks, antennas and propagation, 5G, information security, wireless sensing, radar, millimeter-wave technology, terahertz technology, nanocommunications, biomedical nanoimaging, biomedical communications, visible light communications, calibration of vector network analyzer, and machine learning. He has a global collaborative research network in the field of antennas and propagation, wireless communications, health informatics, information security, microwave techniques and Internet of Things. He received the Young Scientist Award from the International Union of Radio Science in 2014. He is on the editorial board of several IEEE and IET journals, including the IEEE Journal of Electromagnetics, RF and Microwave in Medicine and Biology.

AIFENG REN received the B.S. degree in automatic control and the M.S. degree in circuit and system from Xidian University, Xi'an, China, and the Ph.D. degree in information and telecommunication engineering from Xi'an Jiaotong University. He is currently an Associate Professor with the School of Electronic Engineering, Xidian University. He has authored many papers in some leading journals and conferences. His research interests include signal and image processing, complex brain network, and embedded wireless sensor networks.

ZHIYA ZHANG received the B.S. degree in electrical engineering and the Ph.D. degree in electromagnetic field and microwave technology from Xidian University, Xi'an, China, in 2007 and 2012, respectively. He is currently an Associate Professor with the National Key Laboratory of Antennas and Microwave Technology, Xidian University. His current research interests include broadband antennas, millimeter-wave antennas, and antenna arrays.

WEI ZHAO received the B.S. and M.S. degrees in measurement science and instruments from Xidian University, Xi'an, China, in 2005 and 2008, respectively, and the Ph.D. degree in communication and information system from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011. In 2011, he joined Xidian University, where he is currently a Lecturer with the School of Electro-Mechanical Engineering. His research interests include microwave measurement techniques, particularly the calibration technique for multiport vector network analyzer and computational electromagnetics.

FANGMING HU is currently a Professor with Xidian University.

MASOOD UR REHMAN (SM'16) received the B.Sc. degree in electronics and telecommunication engineering from the University of Engineering and Technology, Lahore, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees in electronic engineering from the Queen Mary University of London, London, U.K., in 2006 and 2010, respectively. He was a Post-Doctoral Research Assistant with the Queen Mary University of London till 2012. He joined the Centre for Wireless Research, University of Bedfordshire, University Square, Luton, U.K., as a Lecturer. He involved in a number of projects supported by industrial partners and research councils. He has authored or co-authored four books, seven book chapters, and over 75 technical articles in leading journals and peer-reviewed conferences. He has contributed to a patent. His research interests include compact antenna design, radiowave propagation and channel characterization, satellite navigation system antennas in cluttered environment, electromagnetic wave interaction with human body, body-centric wireless networks and sensors, remote health care technology, millimeter wave and nanocommunications for body-centric networks, and D2D/H2H communications. He is a fellow of The Higher Education Academy (U.K.), a member of the IET, and part of the technical program committees and organizing committees of several international conferences, workshops, and special sessions. He is an Associate Editor of the IEEE Access. He is the lead guest editor of numerous special issues of renowned journals. He also serves as a reviewer for book publishers, IEEE conferences, and leading journals.

HAIDER ABBAS (SM'15) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from KTH, Sweden, in 2006 and 2010, respectively. He is currently associated with the National University of Sciences and Technology, Pakistan, as an Associate Professor. He is the Cyber Security Professional, who took professional trainings and certifications from the Massachusetts Institute of Technology, USA; Stockholm University, Sweden; IBM; and EC-Council. He is also the Principal Advisor for several graduate and doctoral students with King Saud University; the National University of Sciences and Technology, Pakistan; and the Florida Institute of Technology, USA. He received many awards and several research grants for ICT related projects from various research-funding authorities from U.S., EU, KSA, and Pakistan. He is an Associate Editor or on the editorial board of a number of international journals.

MEHRAN ABOLHASAN (M'01–SM'11) received the B.E. degree in computer engineering and the Ph.D. degree in telecommunications from the University of Wollongong, Wollongong, NSW, Australia, in 1999 and 2003, respectively. He is currently an Associate Professor and the Deputy Head of the School for Research and School of Computing and Communications, University of Technology Sydney, Ultimo, NSW, Australia. He has been leading several major research and development projects in various areas of wireless communications since 2003. He received more than U.S. $1 million in research funding. He has authored over 60 international publications. His current research interests include wireless mesh, fifth-generation cooperative networks, and body area/sensor networks.