

SPECTRUM POLICY CHALLENGES OF UAV/DRONES

MICHAEL J. MARCUS

There is growing interest around the world in unmanned aerial vehicles (UAVs), often called “drones,” for both military and civil use. In International Civil Aviation Organization (ICAO) jargon they are called remotely piloted aircraft (RPA), while in the International Telecommunication Union (ITU) they are called unmanned aeronautical systems (UAS). The civil use includes both commercial use as well as noncommercial use (e.g., a new platform for photography). Indeed, a major U.S. newspaper reported recently, “The next time you go to a wedding, be sure your hair is done, your lipstick is on, and your underwear isn’t sticking out of your pants. You never know if a drone is lurking in the sky about to zoom in and take your picture [1].”

UAVs range in size from military units with mass of over 1000 kg to much smaller consumer units with mass of up to a few kilograms. Similarly, the range and endurance time of these units vary significantly from minutes to hours. While autonomous UAVs without radio links are theoretically possible, for a variety of reasons radio links are generally used for vehicle control and often used to downlink information such as imagery or video in real time.

The spectrum needs of UAVs have been under consideration in ITU deliberations for more than a decade. A 2009 ITU-R report [2] found that “Communications are key in UAS systems due to the remote nature of human presence. Safety-of-flight is the driving factor when the seamless flight of UAS within civilian air traffic is at stake. In the end, safe operation of UAS relies on communications which represents a critical step in enabling UAS operations in non-segregated airspaces.”

The report listed a wide variety of applications for UAVs, including:

- Movie making, sports games, popular events like concerts
- Cargo planes with reduced man power (one-man cockpit)
- Inspections for industries such as oil fields, oil platforms, oil pipelines, power line, and rail lines
- Provision of airborne relays for cell phones in the future
 - Commercial agricultural services like crop dusting
 - Earth science and geographic missions (e.g., mapping and surveying, aerial photography), biological and environmental missions (e.g., animal monitoring, crop spraying, volcano monitoring, biomass surveys, livestock monitoring, tree fertilization)
- Coastline inspection, preventive border surveillance, drug control, anti-terrorism operations, strike events, search and rescue of people in distress, and national security
- Public interest missions like remote weather monitoring, avalanche prediction and control, hurricane monitoring, forest fire prevention surveillance, insurance claims during disasters, and traffic surveillance

•Famine relief, medical support, aid delivery; search and rescue activities

Note that this long 2009 list from ITU-R includes neither the military use of UAVs, which has become a regular news item, nor wedding photography.

The same report estimated the spectrum needs for UAVs to be “34 MHz for terrestrial systems (and) 56 MHz for satellite systems.” However, in view of the rapid recent changes in UAV technology, it is not clear if these 2009 estimates are still adequate.

Next year, ITU WRC-15 Agenda Item 1.5 will consider “the use of frequency bands allocated to the fixed-satellite service ... for the control and non-payload communications of unmanned aircraft systems (UAS) in non-segregated airspaces, in accordance with Resolution 1533 (WRC-12)” [3, 4].

But while formal reallocations are being considered, the “marketplace” is making way for rapidly expanding private sector UAVs use, utilizing existing spectrum in ways that might cause long-range pragmatic problems. In particular, unlicensed (“licence exempt” in European jargon) spectrum and cellular land mobile spectrum are both readily, if not formally legally, used for modest UAV applications such as photography for weddings, and marketing houses and land for sale. Already one U.S. cellular carrier has announced the marketing of a UAV controlled from smartphones via a Bluetooth link [5]. Whether this is a brilliant marketing decision or an event that “opens Pandora’s box” remains to be seen. Why? Illegal jamming of both cellular spectrum and GPS spectrum is an unfortunate growing trend in industrialized countries. While the sociology of this jamming is complex, a key motivator appears to be perceptions in society that some of today’s wireless technology of which we are so proud is seen by others in our communities as invading personal privacy. (Jamming motivated by direct personal gain, on the other hand, appears to be rare.)

“Peeping drones” are a growing concern about UAVs that provide imagery from locations previously thought private such as bedroom windows and backyards [6]. Public perception of UAV use as privacy invasion could escalate interest in illegal, but hard to suppress, jamming of the spectrum supporting the imagery.

While ITU and national spectrum allocations provide for the Aeronautical Mobile Service that is planned for communications to/from airborne systems, cellular and unlicensed bands are not similarly planned for transmitters well off the ground. Thus, transmitters in UAVs at more than 50–100 m altitude can impact the band used much more than terrestrial users since height has a great impact on propagation loss and effective signal range. Widespread use of imagery transmission from UAVs in cellular or unlicensed spectrum may congest that spectrum much more than the expected terrestrial use for which the systems in

those bands were designed. For example, in a cellular system in an area with dense base stations, a drone using cellular spectrum at several hundred meters could cause significant power flux density at a large number of base stations and decrease system capacity much more than terrestrial users anticipated in system planning.

Thus, poorly planned use of cellular and unlicensed spectrum for UAV imagery might have adverse impacts on both cellular and unlicensed/"license exempt" spectrum hosting the transmission. WRC-15 deliberations on UAV/UAS use will be a forum to approach this issue in a deliberate way, but might not be timely enough for the rapid growth of this sector. National regulators will probably have to deal with UAV spectrum issues for private sector users independent of the pending WRC-15 agenda item since UAV use is growing on a faster timescale than ITU deliberations.

REFERENCES

- [1] "Bird? Plane? No, It's the Wedding Photographer," *New York Times*, Aug. 2, 2014; <http://nyti.ms/1tEi6YC>.
- [2] ITU-R M.2171, "Characteristics of Unmanned Aircraft Systems and Spectrum Requirements to Support Their Safe Operation in Non-Segregated Airspace," Dec. 2009; http://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000A0007PDFE.pdf.
- [3] ITU, "The Use of Frequency Bands Allocated to the Fixed-Satellite Service Not Subject to Appendices 30, 30A and 30B for the Control and Non-Payload Communications of Unmanned Aircraft Systems in Non-Segregated Airspaces" WRC-12 Resolution 153; https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000A0007PDFE.pdf.
- [4] ITU, "WRC-15 Agenda and Relevant Resolutions"; http://www.itu.int/dms_pub/itu-r/oth/12/01/R1201000014A01PDFE.pdf.
- [5] "Sprint Offers Smartphone-Controlled Drones," *Kansas City Business Journal*, July 21, 2014; <http://www.bizjournals.com/kansascity/news/2014/07/21/sprint-smartphone-controlled-drones.html>.
- [6] "Regulatory Vacuum Exposed after 'Peeping Drone' Incident," *Seattle Times*, July 5, 2014; http://seattletimes.com/html/localnews/2024002284_drones.xml.html; "Peeping Drone 'an Invasion of Privacy,' B.C. Homeowner Says," *CBC News*, Aug. 28, 2014; <http://www.cbc.ca/news/canada/british-columbia/peeping-drone-an-invasion-of-privacy-b-c-homeowner-says-1.2749365>.

BIOGRAPHY

MICHAEL J. MARCUS [S'66, M'72, SM'01, F'04] (mjmarcus@marcus-spectrum.com) is director of Marcus Spectrum Solutions, Cabin John, Maryland, adjunct professor at Virginia Tech's Department of Electrical & Computer Engineering, and was 2012–2013 chair of the IEEE-USA Committee on Communication Policy. He retired from the Federal Communications Commission in 2004 after nearly 25 years in senior spectrum policy positions. While at FCC, he proposed and directed the policy developments that resulted in the bands used by Wi-Fi, Bluetooth, ZigBee, and unlicensed millimeter wave systems. He was an exchange visitor to the Japanese Ministry of Posts and Telecommunications, and has been a consultant to the European Commission and the Singapore regulator. In 2013 he was awarded the IEEE ComSoc Award for Public Service in the Field of Telecommunications. He received S.B. and Sc.D. degrees from the Massachusetts Institute of Technology.

CALL FOR PAPERS

IEEE WIRELESS COMMUNICATIONS MAGAZINE

QUALITY-OF-EXPERIENCE (QOE) AND QUALITY-OF-PROTECTION (QOP) PROVISIONS IN EMERGING MOBILE NETWORKS

BACKGROUND

Mobile networks have gained tremendous momentum in recent years due to both the wide proliferation of mobile devices such as smartphones and tablets as well as the ubiquitous availability of network services. Mobile networks allow the mobile users to discover the new friends, and share their pictures, videos and other information among their common interest friends, which have been witnessed by the super popularity of representative smart phone applications.

Although the recent years have seen major and remarkable developments in the field of mobile networking technologies, Quality-of-Experience (QoE) and Quality-of-Protection (QoP) issues in mobile networks have attracted less attention so far. QoE is a new concept related to but differs from Quality-of-Service (QoS) perception. It combines user perception, experience, and expectations with non-technical and technical parameters such as application- and network-level QoS. In other words, QoE is a subjective measure of a customer's experiences with a service focusing on the entire service experience, and is a more holistic evaluation. Further, security and privacy are essential for services provisions in emerging mobile networks and Quality-of-Protection (QoP) is an important concept for measuring the security benefits provided by the security approaches including: authentication, confidentiality, availability as well as the privacy guarantees. The challenge of achieving QoP in emerging mobile networks is that it will incur extra security overheads (e.g., processing time, bandwidth and energy consumption), which will inevitably affect the users' experience. Therefore, QoE and QoP are closely coupled concepts, which are expected to describe the tradeoff of service utility and the security in emerging mobile networks. To ensure the QoE and QoP guaranteed services delivery in emerging mobile networks, there is a critical need for research into new designs and implementations that can make mobile networks more reliable and secure from a system point of view.

SCOPE OF CONTRIBUTIONS

The goal of this special issue is to seek original articles examining the state of the art, open challenging research issues, new research results and solutions in QoE and QoP issues in emerging mobile networks. All submissions should contain substantial tutorial contents and be accessible to a general audience of researchers and practitioners.

SCHEDULE FOR SUBMISSIONS

Manuscript Submission: December 1, 2014
 First round of reviews to author: March 15, 2015
 Notification of Acceptance: May 1, 2015
 Final Manuscript Due: June 15, 2015
 Publication Date: August 2015

For manuscript preparation and submission, please follow the guidelines in the Author Guidelines and Paper Submission Guidelines section at the IEEE Wireless Communications web page, <http://www.comsoc.org/wirelessmag>. A paper should have no more than 4500 words, no more than 6 tables/figures, and its abstract should have no more than 250 words. Any submission that fails to comply with the guidelines will be rejected without review. Papers must be submitted in PDF format to the Manuscript Central <http://mc.manuscriptcentral.com/ieee-wcm>.

Prof. Haojin Zhu
 Shanghai Jiao Tong Univ., China
zhu-hj@cs.sjtu.edu.cn

Prof. Wenbo He
 McGill Univ., Canada
wenbohe@cs.mcgill.ca

Prof. Kuang-Hao (Stanley) Liu
 National Cheng Kung Univ., Taiwan
khliu@mail.ncku.edu.tw

Prof. Kaoru Ota
 Muroran Inst. of Technol, Japan
ota@csse.muroran-it.ac.jp