Ericsson white paper
GFMC-18:000526
November 2018

ERICSSON

Drones and networks: Ensuring safe and secure operations

Mobile networks are well suited to support low-altitude drone communication and to be integrated with drone traffic management systems to enhance the safety and security of drone operations. The licensed mobile spectrum serves as the foundation for mobile networks to provide wide-area, high-quality and secure connectivity that can enable cost-efficient drone operations beyond visual line-of-sight range. Current mobile networks are capable of serving drones in the low-altitude airspace. Specific performance enhancements can optimize LTE/5G connectivity toward more effective and efficient connectivity for connected drones while maintaining the performance of mobile devices on the ground.

Introduction

Commercial drone applications are becoming increasingly common, with recent forecasts indicating that drones represent a $100 billion market opportunity over the coming years [1]. Drones are already widely used for newsgathering (photography and videography, for example), and for inspection and mapping in industrial applications. They are also being tested in agricultural and logistics deployments. **Figure 1** provides an overview of several 5G use cases in which drones are expected to play an instrumental role.

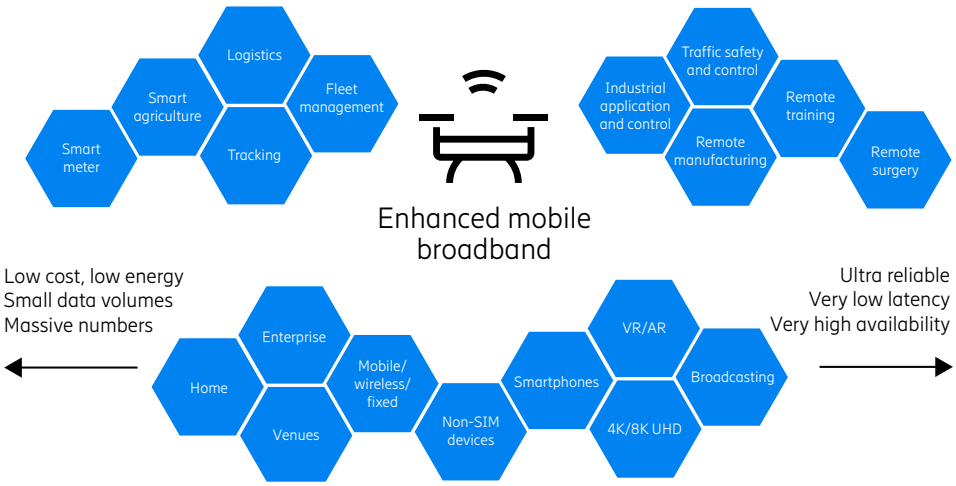

Figure 1: 5G use cases in which drones are expected to play a significant role

The potential of drone technology will only truly be unleashed when both technological capabilities and regulations allow for autonomous operation beyond visual line of sight. Wide-area secure wireless network connectivity is required to safely expand drone operations and unlock the potential of drone technology for commercial applications. At Ericsson, we believe that mobile networks are well suited to provide the necessary connectivity. To make sure that reliable airborne communication is possible, we have studied the radio link performance of terrestrial mobile networks, as well as identifying additional capabilities that mobile networks can provide for drone operations and management.

The challenge

The forecasted significant growth and widespread application of drones present a major safety challenge for regulators around the world. This includes both safety on the ground (to prevent drones from falling to earth and injuring people and/or damaging property) and safety in the air (to prevent mid-air collisions).

Current regulations limit low-altitude operations (below 400ft or 120m) to the visual line of sight of a human pilot who is always in control of the drone. Nonetheless, many enterprises in a wide variety of industries are currently exploring the potential of autonomous drone activity – that is, both beyond visual line of sight and without the direct control of a pilot. Examples of such applications include parcel delivery, medical supply delivery, remote and large-scale infrastructure monitoring, and surveillance. In fact, autonomous drone operations are already gaining traction for precision monitoring and mapping applications. **Figure 2** illustrates the main drone operation modes.

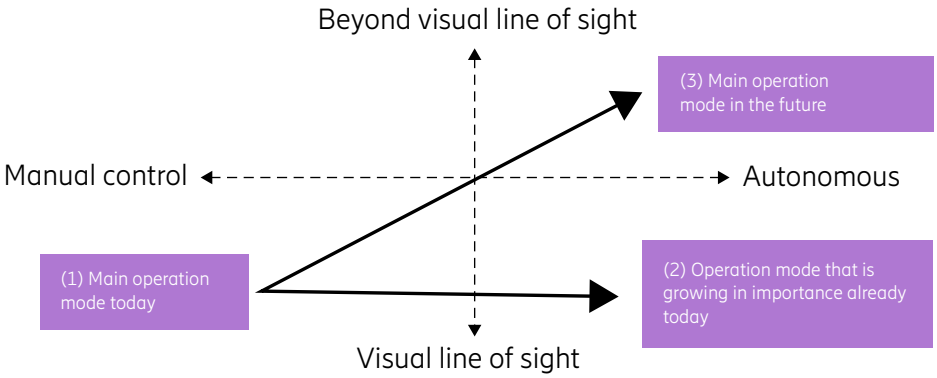

Figure 2: Drone operation modes

Aviation authorities around the globe have initiated programs to define the rules of drone operation, in an effort to address the safety issues regarding commercial use of drones. This includes mandating drone traffic management systems similar to the air traffic control systems of manned aviation. For example, Unmanned Aircraft Systems Traffic Management (UTM) is the system under definition by NASA and FAA [2], while a similar concept called U-Space is under development in a joint project of the European Union [3].

Architecture for drone traffic management

The overall architecture envisioned for drone traffic management and operations is depicted in **Figure 3.** The drone traffic management system handles drone flight approvals and deconflicts drone flights. In addition, it is also responsible for coordinating with manned aviation and its air traffic control systems, as well as for ensuring compliance with low-altitude airspace restrictions. Supplemental data services such as weather services, for example, can feed information to the drone traffic management system to aid decision making. Drone operators will connect to the drone traffic management system to seek flight approval and periodically report the status of drone flights. This can be facilitated, for example, by providing telemetry reports to aid the drone traffic management system in keeping an up-to-date status of the airspace.

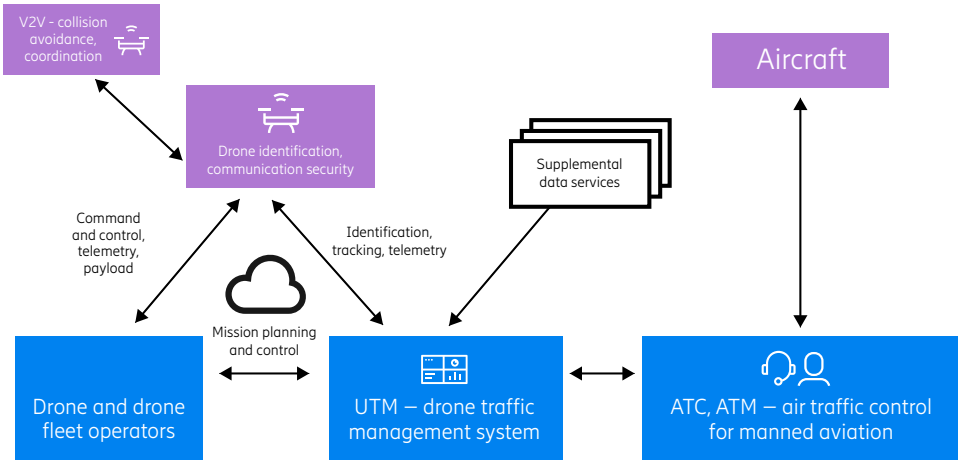

Figure 3: System elements supporting drone operations

Drone identification

Authorities require mechanisms to uniquely identify each drone and eventually its operators as well. This identification needs to be secure and tamper resistant. Beyond visual labeling, two main categories for drone identification are being considered. Local solutions rely on a broadcast signal that is sent from the drone and can be read in the area where the drone is operating. Network publishing solutions rely on using network connectivity to publish data on a remote server, potentially to the drone traffic management system.

Wireless communication options

Drones are inherently mobile and therefore rely on wireless connectivity to support their communication needs. Communication is needed for management to support authentication and authorization. Command and control communication is needed to operate the drone. Finally, payload data transmission is needed to support the applications onboard the drone, such as high bandwidth video streaming for news gathering. For collision avoidance, drones may require means to communicate with other nearby drones in a vehicle-to-vehicle (V2V) manner.

Wireless drone communication can potentially be provided over licensed and unlicensed spectrum. Unlicensed spectrum is shared spectrum in which users do not receive exclusive access to channels. This spectrum is intended to facilitate innovation and, for this purpose, it includes light regulations. Therefore, this spectrum is more prone to interference than licensed spectrum, as the latter requires exclusive licenses that include regulatory requirements to fulfill.

There are essentially three options for providing drone communication over licensed spectrum: satellite technology over satellite spectrum, deployment of a dedicated drone terrestrial network over licensed spectrum, or use of the existing terrestrial mobile network over licensed mobile spectrum. Satellite technology might provide good outdoor coverage, however the drawbacks are high latency, low throughput and higher cost. The drawbacks of deploying a dedicated terrestrial network also include increased costs, as well as the time it takes to build out a system that has adequate coverage for drones.

The existing terrestrial mobile network already has significant coverage with low latency, high throughput and low cost. Further, communication over mobile networks has been proven to be secure and robust. Therefore, while different technologies may be used, we at Ericsson believe that the existing terrestrial network is the most cost-efficient and reliable alternative for drone communication.

The solution

Mobile networks can provide a proven and flexible communication channel to support the various requirements of drone use cases from low latency to high bandwidth scenarios. At the same time, the use of licensed bands and encrypted communication increases the safety of drone applications. 4G LTE and the upcoming 5G networks support a variety of capabilities that fit well with drone requirements. For reliable command and control communication, mobile networks can provide flexible differentiated QoS matching the needed reliability, latency and throughput.

Communication security is already inherent within the architecture of mobile networks and provided at many levels from encryption on the radio link to higher layer security mechanisms. For collision avoidance and drone identification, the sidelink capability provides a secure mechanism to exchange broadcast type messages to nearby entities in addition to network connectivity. Drone tracking is supported by the mobile positioning service and can be queried from the mobile network and integrated into the drone traffic management systems. Industry forums, like GSMA and CTIA have prepared position papers to highlight the potential of mobile networks for drones [4][5].

Regulations and standards

In Europe, the European Conference of Postal and Telecommunication Administrations (CEPT) has identified existing Mobile Fixed Communications Network (MFCN) bands as a potential means to provide connectivity to UAS via existing LTE mobile networks for command and control links [6]. It is also evaluating the current regulatory framework for MFCN bands for this use case.

In the USA, based on a review of various communication technologies, the Radio Technical Commission for Aeronautics (RTCA) Drone Advisory Committee has identified LTE and its successors as promising technologies for both drone command and control, as well as drone identification [7]. The Technical Advisory Committee of the Federal Communications Commission is also evaluating the spectrum requirements for drones. It has determined that cellular networks fulfill all the communications requirements for low-altitude drones, due to their ability to support long distances and provide an integrated solution.

A work item on LTE Support for Aerials Vehicles has been finalized as part of 3GPP Rel-15. The 3GPP study concludes that the existing mobile LTE networks targeting terrestrial usage can offer wide-area wireless connectivity to the drones [8].

Radio coverage considerations

Empirical measurements have shown that aerial radio channels exhibit different propagation characteristics compared to the terrestrial radio channels. One distinct feature of the aerial radio channels is the higher likelihood of line-of-sight propagation due to the absence of obstacles in the sky. In general, as the altitude increases, the propagation becomes closer to free space transmission [9].

The existing mobile networks are optimized for terrestrial broadband communication with the antennas of base stations being down-tilted to optimize the ground coverage and reduce the inter-cell interference. With down-titled base station antennas, drones flying in the sky may be served by the sidelobes of base station antennas that have smaller antenna gains than the main lobes' antenna gains. However, the higher likelihood of line-of-sight propagation can make up for antenna gain reductions, and in some scenarios may lead to even stronger received signal strengths. This fact has been verified by field measurements [10].

Figure 4 shows the cell association patterns based on maximum received power at ground level, and heights of 50m, 100m, and 300m in a simulated rural macro LTE network. Devices in the areas marked by the same color are associated with the same site. It can be seen that the cell association patterns change dramatically with height. At a height of 300m the pattern of the sidelobes of the antenna are clearly visible in the cell association pattern.

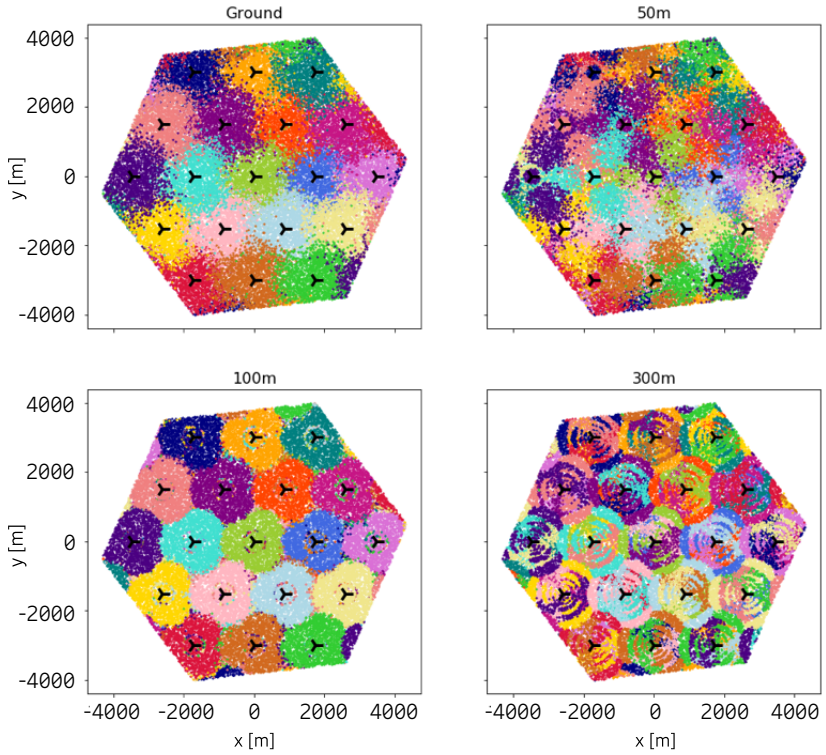

Figure 4: Cell association patterns at different altitudes

The existing terrestrial LTE networks can provide good mobility support to the initial deployment of a small number of drones. New mobility management challenges may arise for higher drone densities or more difficult radio environments. As shown by simulation and field trial results documented in the 3GPP technical report [8], in some scenarios the mobility performance of drone user equipment is worse compared to a terrestrial user equipment. Two main problems have been identified: (1) When drones move through the sidelobe nulls of base station antennas, the default mobility procedures might be too slow for successful execution; (2) drones experiencing line-of-sight propagation conditions to many neighbor cells that cause comparably high interference levels may have difficulty in establishing and maintaining connection to the network.

Performance enhancing solutions can be used to optimize mobile connectivity to provide improved performance for the drones while maintaining the performance of ground mobile devices. Next generation 5G networks will have higher capacity in providing connectivity services to both terrestrial and aerial devices. New advanced technologies have been introduced in 5G networks [11]. At Ericsson, it is our goal that 5G networks will be evolved to achieve ubiquitous mobile broadband coverage both on the ground and in the sky.

Drone identification and drone tracking

Authorities are evaluating different solutions for the identification and tracking of drones. A reliable and secure solution for drone identification is essential to ensure safe operation. Drones need a tamper resistant unique identifier, that is used for flight approvals and can be retrieved in the field to allow law enforcement to take immediate action. The identification may include information about the drone owner and responsible pilot to add further context to flight missions and ensure that responsibility and liability are established. In fact, the FAA's ARC committee (Aviation Rulemaking Committee) [12] has recognized cellular networks as a potential candidate to fulfil the broadcast identification and network tracking capabilities.

Mobile networks can assist with drone identification, authorization, and geo-fencing. Mobile networks are equipped with a variety of tools to identify and authorize users and devices that can access the networks. The International Mobile Equipment Identity (IMEI) is used to identify the mobile device, and the International Mobile Subscriber Identity (IMSI) is used to identify the user in a mobile network. The subscriber and connectivity provider profiles are embedded in the SIM card, or dynamically provisioned on demand to the embedded SIM (eSIM) or embedded Universal Integrated Circuit Card (eUICC). This ensures a tamper resistant solution for drone identification. On the other hand, IMEI and IMSI can be utilized to support other drone identification solutions, providing a robust and secure way to bootstrap certificate-based solutions to identify, authenticate and authorize drones, pilots, and individual drone operations.

There are two main solution categories for drone identification: local broadcast solutions and network publishing solutions. Mobile networks can support both. Local broadcast can utilize the LTE sidelink V2X communication capabilities that can be integrated into mobile chipsets, while network publishing solutions are inherently supported by the data connectivity provided to mobile subscribers. One of the benefits of using mobile technology for both identification modes is that communication is encrypted and uses a secure channel for both local broadcast as well as network publishing mechanisms. A key advantage of cellular solutions is that enabled smartphones can be used to access both the broadcast and network publishing information so that specialized receivers are not required.

In addition to identifying drones, their positions over time need to be monitored as well. This is important to ensure that drone traffic management systems have up-to-date information about the locations of individual drones as well as to be able to locate any drone in the airspace.

An important component of drone tracking solutions is the use of GNSS systems. Drones retrieve their positional information from GNSS readings and then, to support tracking, they communicate this information to a central server, a component of the drone traffic management system. The shortcoming of this self-reporting solution is that the telemetry data provided by a drone can be easily altered by a malicious user without detection by the drone traffic management system.

Mobile systems also provide an independent location tracking mechanism. The cellular mobile positioning system (MPS) can be used both to validate and act as a backup to the drones' self-reported location information. The MPS system can provide a location estimate with tens of meters of accuracy. This precision is enough to validate the telemetry data. In addition, the MPS positioning information can also be used if the drone fails to report telemetry because of, for example, a malfunction. In this case, MPS positioning information may be used to continue monitoring no-flight zone violations, or even to detect potential crash landings along with an approximate position of the incident.

Detecting uncertified use of mobile devices

From the mobile network operator perspective, it is important to detect uncertified use of mobile devices and subscriptions. One such use is when a regular mobile phone is mounted on a drone and is used, for example, for video streaming. This usage may cause significant interference to the network. As soon as such an operation is detected, mitigation techniques can be initiated, for instance, to throttle the subscriber's data communication traffic. Detection may be done by monitoring radio link characteristics and mobility patterns.

Machine learning can be utilized to identify the uncertified use of a mobile device mounted on a drone. The radio link characteristics and mobility patterns are different for devices in the sky and devices on the ground. For example, a drone device operating at a high altitude is expected to have a close to line-of-sight propagation environment that leads to low variance of Reference Signals Received Powers (RSRP) of the strongest cells. Similarly, the Received Signal Strength Indicator (RSSI) statistics of drone devices are different from those of regular ground devices because a mobile device mounted on a drone may receive signals from multiple cells with similar strengths. Therefore, radio link characteristics such as RSPR and RSSI may be selected as features to be fed into a machine learning classification model that identifies the uncertified use of a mobile device mounted on a drone [13].

Co-locating systems to support the safety of drone operations

Safe drone operations require physical infrastructure across cities and throughout a country. Mobile infrastructure is widely and relatively evenly distributed infrastructure that may be used to co-locate additional systems, like the ones introduced below, to support drone operations.

While the previously introduced solutions using mobile technology for identification and tracking of drones apply to drones using cellular communication, to protect from malicious users we need to be prepared for drones that use other technologies for communication, or for drones that do not emit radio signals to evade detection. Different technologies are being developed to detect drones based on radio emission, low altitude radar, video or audio detection combined with triangulation. All these technologies need to be deployed throughout the area they are protecting. Installing these devices along with mobile infrastructure is a cost-effective way to roll out drone detection systems.

Mobile infrastructure locations provide installation options for the hardware devices as well as power and reliable network connection. Similar to detection systems, drone defense solutions need to be deployed to act upon a rogue drone that poses a public safety risk. Drone defense devices need the same infrastructure – that is, physical installation, power and reliable network connectivity.

Regular drone operations also require services such as weather sensors, charging stations and safe emergency landing locations. These services can be co-located with mobile infrastructure – for example, on rooftops or within a secured area along mobile infrastructure in rural areas.

Conclusion

Wide-area network coverage is needed to safely expand low-altitude drone operations for beyond visual line-of-sight missions. Mobile networks provide wide-area secure wireless connectivity, utilizing proven technology based on mobile licensed spectrum and global standards. We have evaluated the performance of mobile networks for airborne drone communication and found that already today, LTE networks are capable of supporting the initial deployment of low-altitude drones. The significantly improved capabilities of 5G networks will provide more efficient and effective mobile connectivity for large-scale drone deployments with more diverse applications. Further, we believe that in addition to wireless communication, drone traffic management systems should utilize the sophisticated and proven identity management and tracking capabilities of mobile networks. Ericsson will continue to work actively in the relevant forums to align mobile network capabilities with drone communication and traffic management requirements.

Glossary

UTM	Unmanned Aircraft Systems Traffic Management
UAV	Unmanned Aerial Vehicle
FAA	Federal Aviation Administration
FCC	Federal Commission Communication
RTCA	Radio Technical Commission for Aeronautics
NASA	National Aeronautics and Space Administration
TAC	Technical Advisory Committee
ARC	Aviation Rulemaking Committee
GNSS	Global Navigation Satellite System
RSRP	Reference Signals Received Powers
RSSI	Received Signal Strength Indicator
MPS	Mobile Positioning System
MFCN	Mobile Fixed Communications Network
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

References

1. Drones reporting for work, Goldman Sachs, available at: https://www.goldmansachs.com/our-thinking/technology-driving-innovation/drones/

2. UTM, available at: https://utm.arc.nasa.gov/index.shtml

3. U-Space, available at: https://www.sesarju.eu/U-space

4. Commercial Wireless Networks: The Essential Foundation of the Drone Industry, CTIA white paper, available at: https://api.ctia.org/wp-content/uploads/2017/11/Droner_WhitePaper_FINAL.pdf

5. Mobile-enabled unmanned aircraft, GSMA white paper, available at: https://www.gsma.com/iot/wp-content/uploads/2018/02/Mobile-Enabled-Unmanned-Aircraft-web.pdf

6. Technical and Regulatory Aspects and the Needs for Spectrum Regulation for Unmanned Aircraft Systems (UAS), ECC Report 268, available at: https://www.ecodocdb.dk/document/1034

7. Drone Access to Airspace: Report of the Drone Advisory Committee, November 2017, RTCA, available at: https://www.rtca.org/sites/default/files/dac_tg2_final_reccomendations_11-17_update.pdf

8. Enhanced LTE Support for Aerial Vehicles, 3GPP TR 36.777, available at: ftp://www.3gpp.org/specs/archive/36_series/36.777/36777-f00.zip

9. The Sky is Not the Limit: LTE for Unmanned Aerial Vehicles, IEEE Communications Magazine, vol. 56, no. 4, pp. 204-210, April 2018, available at: https://www.researchgate.net/publication/318670906_The_Sky_is_Not_the_Limit_LTE_for_Unmanned_Aerial_Vehicles

10. Mobile Networks Connected Drones: Field Trials, Simulations, and Design Insights, Ericsson, January 2018, available at: https://arxiv.org/ftp/arxiv/papers/1801/1801.10508.pdf

11. 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology, Ericsson, June 2018, available at: https://arxiv.org/ftp/arxiv/papers/1806/1806.06898.pdf

12. UAS Identification and Tracking Aviation Rulemaking Committee Recommendations, Final Report, September 2017, available at: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf

13. Rogue Drone Detection: A Machine Learning Approach, Ericsson Research, 2018, available at: https://arxiv.org/abs/1805.05138

Further reading

- Drone communication and traffic management over mobile networks, video available at: https://www.youtube.com/watch?v=AVUHKZTkvmw&t=172s
- Managing drone air traffic with network services, Ericsson Research blog, available at: https://www.ericsson.com/research-blog/managing-drone-air-traffic-with-network-services/
- How mobile networks can support drone communication, Ericsson Research blog, available at: https://www.ericsson.com/research-blog/how-mobile-networks-can-support-drone-communication/
- LTE for unmanned aerial vehicles, presentation at Texas Wireless Summit 2017 (starts at ~24:30), available at: https://www.youtube.com/watch?v=AwvL17WZ2I8
- Standardization aspects of LTE/NR connected drones, CEPT Workshop on Spectrum for Drones, available at: https://cept.org/files/20153/A2-2%20Helka-Liina%203gpp%20MFCN.pdf
- Interference Mitigation Methods for Unmanned Aerial Vehicles Served by Cellular Networks, available at: https://arxiv.org/abs/1802.00223
- Mobility Support for Cellular Connected Unmanned Aerial Vehicles: Performance and Analysis, available at: https://arxiv.org/abs/1804.04523
- An Overview of 3GPP Release-15 Study on Enhanced LTE Support for Connected Drones, available at: https://arxiv.org/abs/1805.00826
- A Telecom Perspective on the Internet of Drones: From LTE-Advanced to 5G, available at: https://arxiv.org/ftp/arxiv/papers/1803/1803.11048.pdf

Contributors

The contributors to Ericsson's opinion on this topic are Attila Takacs, Xingqin Lin, Stephen Hayes and Erika Tejedor.

Attila Takacs
Attila Takacs is Director of Innovation, heading the Ericsson Garage in Silicon Valley. He also serves as venture advisor at SkyDeck, the start-up accelerator of UC Berkeley. Prior to his current role he was Engineering Director of Networking and Cloud Research and was instrumental in specifying software defined networking (SDN) and network function virtualization (NFV) for telecommunications. Takacs joined Ericsson in 2001 and since then has held various roles within the CTO organization. He holds an M.Sc. in computer science from the Budapest University of Technology and Economics in Hungary, and an MBA from the Central European University Business School.

Xingqin Lin
Xingqin Lin joined Ericsson in 2014 and currently serves as a Senior Researcher. He leads 4G/5G research and standardization in the areas of drones and satellites. He is a highly experienced telecom professional with expert knowledge in wireless communications and technology strategy. Lin has published more than 50 refereed journal and conference papers, and holds numerous patents. His publications have been cited over 2,000 times according to Google Scholar. He is a frequent speaker, panelist, and technical contributor at numerous conferences and workshops. He holds a Ph.D. in electrical and computer engineering from The University of Texas at Austin, USA.

Stephen Hayes
Stephen Hayes is Director of Standards for Ericsson in North America. He has worked on various cellular issues over the last 20 years and been heavily involved in the evolution of the 3GPP family of technologies. His current focus includes the ATIS committees and 3GPP. He also chairs the FCC TAC group on UAS systems and standards and serves as the vice-chair of 3GPP TSG-RAN. Hayes also serves as the chair of both the 3GPP group on working procedures and the Rapporteur group on Standardization Strategy within ITU-T.

Erika Tejedor
Erika Tejedor is currently a Master Researcher at Ericsson, where she leads the technical work toward spectrum regulations. She is involved in the ITU-R preparations for WRC-19 as well as in CEPT and FCC regulatory work. Tejedor has also taken an active role in the 3GPP RAN4 standardization process for 3G and 4G. She joined Ericsson in 2008 after receiving her Master's degree in wireless communications from the University of Zaragoza, Spain.