Project Title	Virtual Presence in Moving Objects through 5G
Project Acronym	PriMO-5G
Grant Agreement No	815191
Instrument	Research and Innovation Action
Topic	The PriMO-5G project addresses the area of “a) Focus on mmWave and super broadband services” in the call “EUK-02-2018: 5G” of the Horizon 2020 Work Program 2018-2020.
Start Date of Project	01.07.2018
Duration of Project	36 Months
Project Website	https://primo-5g.eu/

D1.3
SPECTRUM OPTIONS AND ECONOMIC STUDY

Work Package	WP1, Scenarios, architecture, economic and regulatory analysis
Lead Author (Org)	Ki Won Sung (KTH)
Contributing Author(s) (Org)	Anders Nordlöw (EAB), Ulrika Engström (EAB), SeHoon Yang (KT), Irshad Ahmad Meer (KTH), Ki Won Sung (KTH), Seunghwan Kim (YU), Sujin Kook (YU), Sihun Baek (YU), Seong-Lyun Kim (YU)
Due Date	31.12.2020, M30
Date	31.12.2020
Version	1.0

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

The work described in this document has been conducted within the project PriMO-5G. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 815191. The project is also supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00170, Virtual Presence in Moving Objects through 5G). The dissemination of results herein reflects only the author’s view, and the European Commission, IITP and MSIT are not responsible for any use that may be made of the information it contains.

Disclaimer

PriMO-5G has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 815191. The project is also supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00170, Virtual Presence in Moving Objects through 5G). The dissemination of results herein reflects only the author's view, and the European Commission, IITP and MSIT are not responsible for any use that may be made of the information it contains.

Table of Contents

List of Tables

List of Figures

Executive Summary

The main aim of the PriMO-5G project is to demonstrate an end-to-end 5G system providing immersive video services for moving objects. To achieve this, PriMO-5G chose the public safety communications, particularly smart firefighting assisted by unmanned aerial vehicles (UAVs), as the main use case. because it is an area where immersive video services with moving objects can make a substantial improvement in the safety and efficiency of the operations. The usage of UAVs for firefighting can be divided into three categories. The first category is preparatory actions for the fast collection of information. Second, the drones can provide visual information to the first responder and the incident commander. Third, the drones can gather sensory and measurement data of the fire scene and surroundings.

In this deliverable, we investigate the regulatory and economic aspects of the PriMO-5G use cases. This deliverable focuses on mission critical services and UAVs since these are the two main features of the PriMO-5G use cases. Regarding mission critical services, the contents include spectrum demand estimation for mission critical services, spectrum availability for public safety communications, feasibility of mission critical services in commercial mobile networks, and private networking via non-public network. As for UAVs, the deliverable discusses current regulation on drones, a novel scheme for low-latency spectrum access, and coexistence of drones with other services.

Mission critical services

Public safety communications providing mission critical services are moving from a voice-centric paradigm to a data-centric paradigm enabled by Long-Term Evolution (LTE), 5G, and the ongoing 3rd Generation Partnership Project (3GPP) evolution. When we consider emerging mission critical applications, the estimated amount of required spectrum far exceeds the currently allocated spectrum dedicated for public safety. This is one of the reasons that more safety agencies are now considering prioritized access to mobile network operator (MNO) spectrum for providing advanced mission critical services. Licensed spectrum is strongly recommended for mission critical communications. According to Report ITU-R M.2377, the license-exempt spectrum does not meet, among others, the priority access requirements of Public Protection and Disaster Relief (PPDR).

The challenges of establishing the next generation public safety communications are not only to satisfy per performance requirements but also to achieve economic viability. Therefore, an important question is who will establish and operate the public safety communications system. Some countries, such as Norway, the UK, and the USA, have decided to utilize the commercial mobile networks for the mission critical services. Various models under this category exist, and the selection of a model depends on cost estimation and performance requirements specific to each country.

The PriMO-5G project has been working on technical enablers and architecture components that can contribute to mission critical services. Particularly, the network slicing and moving base station have potential to lower the cost of public safety communication networks, and thus they should be considered in the cost calculation. The moving base stations can be coupled with the equipment of public safety professionals, e.g., fire brigade, and thus it necessitates a new model for network establishment and operation. Non-public network can be an element of such a model. It is a physical or virtual cellular network that is deployed for special or private use by governments, public safety agencies, or companies. The market for non-public network is expected to grow steadily, making it an industry that surpasses the current public cellular market.

Use of UAVs

Currently, license-exempt spectrum is typically used for the control of UAVs in line-of-sight (LOS) situations because Wi-Fi standards or similar protocols have been the first protocols of implementation from the UAV control vendors. Each country has own regulations for maximum transmission power in

the license-exempt band, which is a primary factor in determining the flying distance of UAVs. If a UAV is in the urban area and the transmission power of the control signal is restricted to low power, the control signal may experience harsh interferences, which makes a control of the UAV flight difficult. In this case, using cellular networks such as 4G and 5G will be an effective solution for reliable control of UAVs. 3GPP networks can provide reliable and trustworthy communication for control of UAVs in beyond visual LOS (BVLOS) situations.

As for the communications among UAVs in the context of mission critical services, low-latency access is one of the key requirements. 3GPP has standardized solutions for the low-latency access, and thus licensed spectrum provides better control of QoS for mission critical services. License-exempt spectrum for mission critical communications has been technically down-prioritized because the listen-before-talk and back-off mechanisms would need to be employed by the systems such as Wi-Fi. As a consequence, unpredictable behavior and potentially large delay may occur, especially under large load. Hence, there are research opportunities to exploit whether a new medium access control (MAC) mechanism in the license-exempt spectrum has feasibility to achieve low-latency access. Non-orthogonal random access which utilizes a non-orthogonal signal decomposition technique is a promising direction.

If UAVs are served by terrestrial cellular networks, coexistence with other types of users is one of major concerns. From the perspective of adjacent channel interference, introducing UAVs in a frequency band does not affect the performance of ground users or UAVs in an adjacent channel. However, satellite-based services, e.g., complementary ground component, is influenced considerably in the uplink when UAVs are flying above their base stations.

List of Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
5G	Fifth-Generation Mobile Network
ACIR	Adjacent channel interference ratio
AMRS	Aeronautical Mobile Radiocommunication Service
AMSRS	Aeronautical Mobile-Satellite Radiocommunication Service
BS	Base Station
BVLOS	Beyond Visual Line of Sight
CGC	Complementary Ground Component
CNPC	Control and Non-Payload Communications links
CSMA/CA	Carrier-sense multiple access with collision avoidance
DoA	Description of Action
ECC	Electronic Communications Committee
eMBB	Enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GSD-ST	Geometric Sequence Decomposition with k-Simplexes Transform
IMT	International Mobile Telecommunications
ISM	Industrial, Scientific, and Medical
ITU	International Telecommunication Union
LBT	Listen Before Talk
LOS	Line of Sight
LTE	Long-Term Evolution
MAC	Medium Access Control
MEC	Multi-access Edge Computing
mMTC	Massive Machine Type Communications
MNO	Mobile Network Operator
MSS	Mobile-Satellites Services
No-INFRA	Non-orthogonal interference-free radio access

Acronym	Definition
NPN	Non-public Network
OFDM	Orthogonal Frequency Division Multiplexing
PLMN	Public Land Mobile Network
PNI-NPN	Public Network Integrated Non-public Network
PPDR	Public Protection and Disaster Relief
RAN	Radio Access Network
SNPN	Stand-alone Non-public Network
SNR	Signal-to-noise ratio
SRD	Short Range Devices
TETRA	Terrestrial trunked radio
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UE	User Equipment
URLLC	Ultra-Reliable Low-Latency Communications
VR	Virtual Reality
XR	Extended Reality
WP	Work Package
WRC	World Radiocommunication Conference

1 Introduction

1.1 Purpose and Scope

The main aim of the PriMO-5G project is to demonstrate an end-to-end 5G system providing immersive video services for moving objects. In this deliverable, we investigate the regulatory and economic aspects of the use cases defined in the deliverable D1.1 of the project [PRI19-D11]. Since the use of UAVs[1] and public safety communications are two distinct features of the PriMO-5G use cases, this deliverable considers these two areas. With regard to the use of UAVs, the contents of the deliverable include the current regulation on drones, a novel scheme for low-latency spectrum access, and coexistence of drone and other services. As for the public safety communications, the deliverable addresses spectrum demand estimation for mission critical services, spectrum availability for public safety communications, feasibility of mission critical services in commercial mobile networks, and non-public network.

1.2 Structure of the document

This deliverable is organized as follows. Section 2 presents a brief review of the PriMO-5G use cases. In Section 3, we discuss regulatory issues including the current regulation on drones, spectrum demand estimation for mission critical services, and spectrum availability for public safety communications. Section 4 introduces a novel scheme for low-latency spectrum access and a result of coexistence study for drone with other services. In Section 5, economic issues are discussed. Specifically, feasibility of mission critical services in commercial mobile networks and non-public network are considered. Finally, Section 6 provides concluding remarks.

1.3 Relationship to other project outcomes

The study of regulatory and economic aspects will complement the technical works conducted in WP2-WP5 of the project. Furthermore, the findings of this deliverable will influence the exploitability of PriMO-5G developments in WP6.

[1] In this deliverable, UAV and drone are used interchangeably.

2 PriMO-5G use cases

The PriMO-5G project chose the public safety, particularly firefighting, as the main use case because it is an area where immersive video services with moving objects can make a substantial improvement in the safety and efficiency of the operations.

Fires are a growing challenge for modern society [SDB+20]. The dynamic nature of fires makes firefighting operations complex, high risk, and demanding in terms of the required firefighting resources and technologies. The use of public safety communications systems and aerial support systems is now critical for enhancing the safety and efficiency of firefighting operations. Communications technologies provide significant enhancements in situational awareness for the emergency first responders and their effectiveness in managing hazards by enabling immersive services and reducing constraints on operational data sharing. As a concrete example, we envisage that the use of UAVs, particularly drones, will make the firefighting much safer and more efficient if it is combined with 5G communications.

The usage of drones for firefighting can be divided into three categories. The first category is preparatory actions. Drones can be dispatched to the fire scene faster than fire trucks to gather the overall situational information. Furthermore, the drones can interact with the people around the scene to evacuate them to the safe area. Second, the drones can provide visual information to the first responder and the incident commander. The use of immersive video services, i.e., virtual reality (VR) and augmented reality (AR), is a key to this enhancement. Third, the drones can gather sensory and measurement information of the fire scene and surroundings and report it to the firefighters and the incident commander. This will help the firefighters locate the people to rescue, identify toxic substances, and detect the possible explosion or collapse.

We divide the scenarios of the drone-assisted firefighting into the rural and urban cases as discussed in the subsequent sections. More detailed description of the PriMO-5G use cases can be found in [PRI19-D11] and [SMJ+19].

2.1 Rural and forest firefighting

Assume that a fire breaks out in a rural forest. Fire trucks have difficulties in reaching the fire scene due to the inadequate road condition. Firefighting equipment is too heavy for human firefighters to carry. Fallen trees are dangerous obstacles in the scene. Fire can expand quickly at any time, which may risk the safety of firefighters. We envisage that UAVs can play a significant role in such circumstances. UAVs are mainly expected to perform a supporting role. The duties of the UAVs would be to gather visual and location information of the fire scene and to facilitate communications between the actors. A UAV can be either user equipment (UE) or base station (BS), or both depending on the situation and its computational power. In addition, a fire truck can act as a BS as well as an multi-access edge computing (MEC). The rural and forest firefighting scenarios is illustrated in Figure 2-1.

In this scenario, the lack of existing infrastructure is a challenge to overcome. It is possible that the fire area is out of the reach of existing mobile network except for traditional voice and low data rate services. Therefore, fast deployment and setup of communications between the firefighters, incident commander, drones, and control centre is a key requirement for the smart firefighting operations. Moving terrestrial and aerial BSs can be a technical solution to address this challenge.

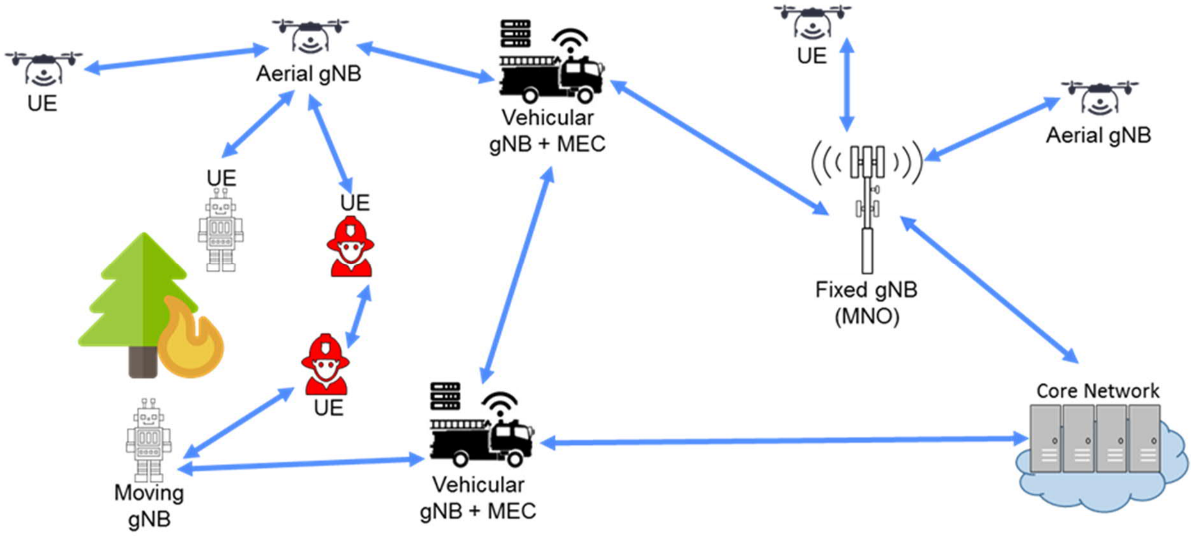

Figure 2-1: An illustration of the rural firefighting. (source:[PRI19-D11]]

2.2 Urban firefighting

Rapid industrialization caused unplanned and haphazard urbanization. In the same manner, the roads were constructed carelessly and loosely to meet the needs of rapidly growing urban population. So, the streets tend to be very complicated with the lack of standardization. The traffic congestion of a big city limits the mobility of fire engines, and the sudden appearance of a fire engine is unpredictable to drivers. This may cause a belated action of drivers which prevents the fire engines from reaching the scene on time. Moreover, in industrialized cities, flammable materials are used anywhere which can cause secondary accidents. Those situations are highly risky to densely populated areas. Fortunately, UAVs are capable of approaching the critical areas much faster than the fire engines and firefighters. Thus, UAVs are predicted to be increasingly helpful for firefighting in urban area.

While the firefighting equipment and human firefighters are on their way, fleets of UAVs can reach the fire scene first as they can travel straight through the air space. The air fleets can take preparatory measures, such as evacuation of people, search for persons to be rescued, and surveillance of dangerous materials to prevent secondary accidents in the near fire area. The drones can actively lead the evacuation procedure by telling (e.g., the evacuation instructions and warnings from the commander), showing (e.g., the evacuation path to the victims and the spectators), and providing (e.g., masks and other safety equipment). In addition, the aerial view from high altitudes can also assist the fire engines to take faster actions and firefighters by navigating the optimal route to the area. The urban firefighting scenario is depicted in Figure 2-2.

A crucial aspect of an urban setting that we must account for is its density, i.e., population, network nodes, and traffic. Concentrated population around the site, both victims and passers-by, further intensifies the threat of a fire accident and increases the complexity of countermeasures that have to be taken. In addition, traffic congestion of automobiles makes it difficult for the fire engines to arrive before the critical time, commonly known as the “golden time” of the operation. Finally, diverse and abundant network nodes, which aid us in our normal lives, could hinder the operation at its critical moment. Nevertheless, we consider this setting advantageous for our proposed scenario. Network slicing is one of the key technologies to address the requirements for the urban environment.

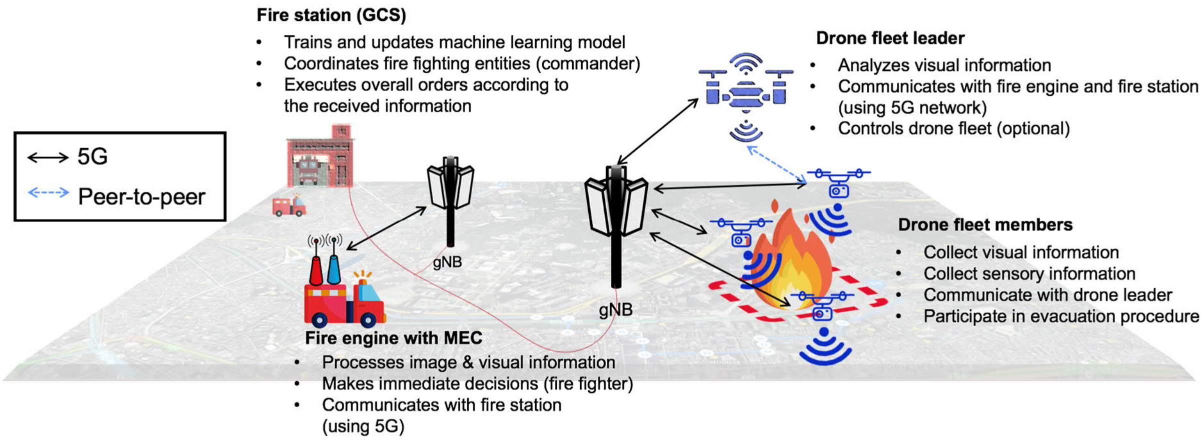

Figure 2-2: An illustration of the urban firefighting. (source: [PRI19-D11])

3 Spectrum options for PriMO-5G

This section provides an overview of spectrum options for PriMO-5G. We focus on mission critical services and drones because these are the two main features of PriMO-5G use cases. Specifically, we investigate the spectrum regulations for Unmanned Aircraft Systems (UAS)[2], spectrum demand for mission critical services, and current spectrum availability of public safety communications. A prerequisite for critical communications is full control of the spectrum. Today, only licensed spectrum guarantees control over spectrum usage by the system, making it a preferred option for critical communications [ERI19].

3.1 Current spectrum regulation for UAS

In this section, we give an overview of global 5G spectrum status. Then, we focus on the spectrum regulations for UAS.

3.1.1 Global 5G spectrum status

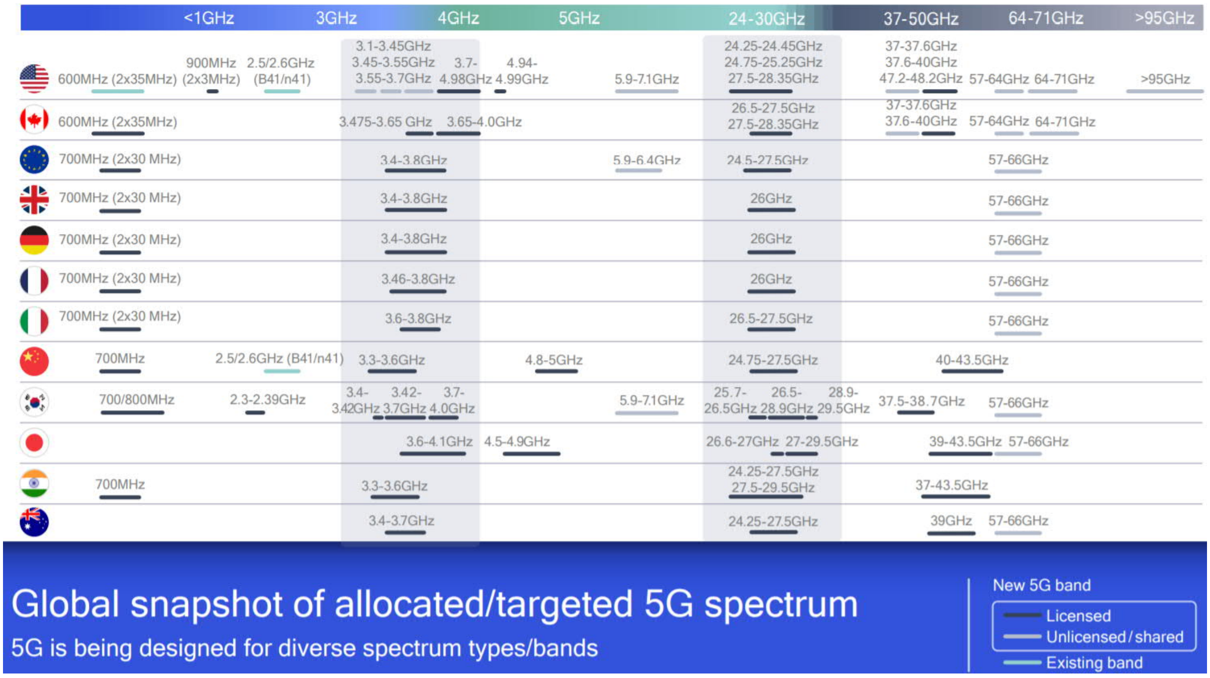

Figure 3-1: Global snapshot of 5G spectrum. (source: [BRE20])

As is well known, according to IMT-2020, the vision of 5G is defined according to three scenarios: enhanced mobile broadband (eMBB), massive machine type communications (mMTC), and ultra-reliable low-latency communications (URLLC) [IMT15]. In order to satisfy the manifold requirements, 5G is defined by using a wide band of frequencies in various ways. It supports channel sizes ranging from 5 MHz to 100 MHz for bands sub-6 GHz, and channel sizes from 50 MHz to 400 MHz in bands above 24 GHz (mmWave). Global snapshots of allocated and targeted 5G spectrum are summarized in Figure 3-1.

Since each frequency band has a different spectrum characteristic that cannot be physically overcome, the frequencies used for the 5G communication are roughly divided into low, mid, and high bands

[2] UAS includes a UAV, a ground-based controller, and a system of communications between these.

[HUA20]. Accordingly, there are national/regional regulations for each band. Figure 3-1 above shows the frequency allocation by major countries.

The key focus is on new mobile bands including spectrum in the 3.5 GHz range (3.3 ~ 3.8 GHz) that has been assigned in numerous countries, however other bands are also being considered. For instance, several countries plan to use frequency spectrum in the 4.5 ~ 5 GHz range for 5G, such as China and Japan and so on. A growing number of countries are considering the 3.8 ~ 4.2 GHz range, 5925 / 6425 ~ 7125 MHz, 2.3 GHz and 2.5 / 2.6 GHz bands for 5G.

The fastest throughputs depend on milli-meter wave (mmWave) bands, which is above 24 GHz. At WRC-19, countries supported a globally harmonised identification of 26 GHz, 40 GHz and 66 GHz bands.

At the other end of the spectrum, which is low-bands, Europe has prioritised the 700 MHz band for wide area 5G deployments and the US has already licensed the 600 MHz band. Prime 5G mid-bands (e.g., 3.5 GHz) and mmWave bands (e.g., 26 GHz and 28 GHz) suits dense 5G small cell networks in urban hotspots where additional capacity is vital.

3.1.2 Spectrum regulations for UAS

In the use cases of PriMO-5G, UAS including drone is actively utilized to carry out public safety missions. Controlling the UAS can be remotely controlled via 5G communication. Nevertheless, in general, using a separate control signal should be considered as a baseline. Therefore, it is necessary to understand the status of the maneuvering frequencies for each country separately from the frequency of 5G.

3.1.2.1 Use cases of frequency bands for UAS control

The frequency bands for UAS can be classified into using a licensed band and an license-exempt band as follows.

- License-exempt band: ISM band
  - 2.4GHz or 5.8GHz are used.
  - It has requirements of the maximum allowed output power to prevent the radio interference.
  - License-free ISM applications and bands are defined at the ITU level. Uses, power level, or field strength, duty cycle, modulation and other restrictions are defined by FCC 47CFR15 [FCC20-1] and 47CFR18 [FCC20-2] regulations in the USA and under the CEPT/ECC ERC/REC 70-03 recommendation in Europe [ERC20].
- SRDs (short range devices) bands (Europe)
  - The bands for SRDs are license-free in Europe with a few exceptions, following recommendation ERC/REC 70-03 [ERC20] and several ETSI standards. In general, SRDs refer to Radio-Frequency Identification (RFID) applications, fire, security and social alarms vehicle, and so on. 868 MHz SRD band in Europe is dedicated to specific applications or for “Non-specific SRDs”. Non-specific SRDs can cover for telemetry, telecommand, alarms and data transmission. For reliable, robust, and flexible radio links for drones in Europe, one must take SRD regulation and uses into consideration.
- Radio amateur bands (ham radio)
  - Many of the amateur radio bands share license-exempt ISM or SRD bands. The objectives of Amateur Radio, also known as “ham radio”, were to allow for the non-commercial exchange of messages, wireless experimentation, self-training, private recreation, radio sport, contesting, and emergency communication. 433 MHz is a ham radio band. It is an ISM band in Europe, but not in the USA. A 420-450 MHz band for RC can be used with reaching transmit powers of 1 W for model aircraft. 1.3GHz band (1.24-1.30 GHz) is an amateur band available both in Europe and the US.
- Licensed band: dedicated frequency of control for UAS
  - 5,030-5,091MHz band has an Aeronautical Mobile Radiocommunication Service

(AMRS) allocation for terrestrial Control and Non-Payload Communications links (CNPC) for UAS and also an Aeronautical Mobile-Satellite Radiocommunication Service (AMSRS) allocation for satellite Beyond Visual Line-Of-Sight (BVLOS) CNPC by WRC-12.
- 12.2~12.75GHz and 29.5~30GHz can be used to control UAS by satellite, according to WRC-15.

3.1.2.2 Status of UAS frequency band regulations by country

There are no international radio link industry standards for UAS. The main reason is that the Wi-Fi standard (IEEE 802.11 family) has been so widely used for UAS radio links. Instead, the signaling power limitation is regulated when the control device is authenticated. Table 3-1 below represents the transmission power limitations for one controller when using the ISM band by country. The controller's output power is a primary factor in determining the capability of UAS's flying distance. If a drone included in a UAS is located in the urban area and the transmission power of the control signal is restricted to low power, the control signal experiences harsh interferences, making direct control of the drone flight difficult. In this case, using a previously deployed cellular network such as 4G and 5G is an effective solution for drone control.

Table 3-1: Limitations of transmission power by country.

Frequency	South Korea	The United States	Europe	Japan
2.4GHz	1W	4W	0.1W	1W
5.8GHz			0.025W	unknown

The spectrum regulations for UAS control signals are different by country because the assigned usages for each spectrum band are different. Below is an identified list of major countries' UAS controlling spectrum regulations.

Europe and the USA

For most toy drones, only 2.4 GHz ISM band is used while following the Wi-Fi standards. For more expensive commercial drones, both 2.4 GHz and 5.8 GHz ISM bands are used. For control and command (C2) signalling, the 2.4 GHz band is utilized for the wide coverage area. At the same time, for first-person view (FPV) video transmission, 5.8 GHz band is utilized for the link capacity. They still follow the Wi-Fi standard. There is another option to divide the C2 signal into different ISM bands. For example, in Europe, 433 MHz band can be utilized for telemetry (one part of the C2 signal) while 2.4 GHz band is still utilized for radio control signal (another part of the C2 signal). In the case of the US, 915 MHz band is utilized for telemetry instead of 433 MHz band of Europe. Likewise, the ham radio (1.3 GHz) is exploited for video transmission mitigating link-load of 5.8 GHz band.

South Korea

There is a lack of the UAS dedicated frequency and specific standardization work. Currently, most of the drones released by South Korea are using only ISM band (2.4GHz or 5.8GHz).

China

According to the regulations of PRC, the frequency bands of 840.5-845 MHz, 1430-1444 MHz, 2408-2440 MHz are approved for UAS. The 1430-1438 MHz is applied for video transmission of police unmanned aircraft and helicopter.

Japan

Recently, a new regulation for designations of frequency in the ranges of 2.4GHz and 5.7GHz for specific use by drones are created. Japan's new legislation would be to increase the limit of power to 1W allowing transmission of images to around 5km. It enables the transmission of high-quality video for a variety of applications such as construction and engineering. Like Korea, there are insufficient regulations related to other drone control frequencies.

Utilizing ISM bands for UAS control is commonplace. The ISM bands take advantage of international versatility, however, the harsh interference from other interferers everywhere. Especially in urban areas, a single malfunctioning of a UAS occurred by a signalling error, can cause a disastrous result when the UAS acts as a mission-critical player in the public safety mission. Besides, it is expected that when we consider only the ISM band for video transmission, the wireless capacity would be insufficient to achieve virtual presence in the flying drone. The most possible alternative to this is to actively use cellular networks for UAS. Using the 5G network for control signalling as well as video transmission will maximize the utility of UAS so that we can think of manifold usages for UAS in public safety missions.

3.2 Spectrum demand estimation for mission critical services

In this section, we present methodology and result of a spectrum demand estimation for mission critical (MC) services.

3.2.1 MC spectrum demand estimation methodology

The methodology presented here is used for estimating the spectrum demand for the following MC services: MC Push-to-talk (PTT), MC Data, MC Video, and a hypothetical MC AR. The methodology is generic, and can be applied for various parameters, e.g., different number of users. To specify the considered MC services, we employed the data rate and service requirements defined by 3GPP (see the following subsections). A rather demanding public safety scenario of MC forest fighting has been investigated with the following assumptions:

- Users per cell: 50 for MCPTT, 10 for MC Data, 10 for MC Video, and 5 for MC AR.
- Spectral efficiency (0.5 and 1.5 bps/Hz/cell).

The traffic per cell is calculated as:

$$Traffic\ per\ cell\ =\ Users\ per\ cell\ \times\ traffic\ per\ user\ (or\ data\ rate\ per\ user).$$

Therefore, the resulting required spectrum is given by

$$Required\ spectrum\ = \frac{Traffic\ per\ cell}{Spectral\ efficiency}.$$

3.2.1.1 MC Service Requirements: 3GPP MCPTT

The requirements for MCPTT is taken from [3GPP-22179]. The UL transmission from UE A to the gNB is done via unicast with one UL talker (e.g., UE A) and many DL listeners (e.g., UEs B, C, and D). For the DL transmission from gNB to all the listeners within the group (UEs B, C and D), the transmission can be done by either of following two methods:

- Unicast communications (each listener is assigned with its own dedicated RBs but with higher spectrum efficiency) which generally requires higher bandwidth.
- Multicast communications (the same RBs are used for all listeners but with lower spectrum efficiency; the spectrum efficiency value depends on the UE that has the worst DL link budget) which generally lower bandwidth.

In practice, there can be multiple groups of first responders using MCPTT simultaneously. Data rates can differ between 20 kbps to 70 kbps depending on the codec and PTT implementation.

3.2.1.2 MC Service Requirements: 3GPP MC Data

According to [3GPP-22282], the MCData service has the following requirements:

- The MCData service shall provide a Short Data Service (SDS) feature for conveyance of limited size, and variable content and messages.
- The MCData service shall provide a file distribution capability.
- The MCData service shall provide a data streaming capability.
- The MCData service shall enable an MCData user to initiate transport of IP data towards a server in the network or another MCData user.

3.2.1.3 MC Service Requirements: 3GPP MC Video

In 3GPP, the service requirements for the MCVideo are defined in [3GPP-22281]. The MCVideo service shall support video resolution at least from 320 x 240 at 10 frames per second up to and beyond 1280 x 720 at 30 frames per second. The required data rate varies significantly with the quality of the video.

For a 720p HD video resolution of 1280 x 720 at 30 frames per second, the required data rate is calculated as follows:

- Pixels per second = 1280x720x30 → 27,648,000 pixels/second
- Quality Factor (QF) = 1/b bits/pixel (bpp) = 1/8 = 0.125 for a H.264 video stream
- Video bit rate for a HD video = bpp x pixel/Second =~3.6 Mbps
- Assuming a good stereo sound audio bit rate of 192 Kbits/s
- Data rate = (Video bit rate + Audio bit rate) x 1.5 =~ 5Mbps

For a 240p video resolution of 320 x 240 at 10 frames per second, the data rate is as below:

- Pixels per second = 1280x720x30 → 768,000 pixels/second
- Quality Factor (QF*) = 0.03 for a poor-quality video
- Video bit rate for a HD video = bpp x pixel/Second =~23 Kbps
- Assuming a mono sound audio bit rate of 64 Kbits/s
- Data rate = (Video bit rate + Audio bit rate) x 1.5 =~ 0.15 Mbps

3.2.1.4 MC Service Requirements: MC Remote AR

Remote AR is a hypothetical MC service where robots and vehicles are controlled remotely. It is expected to be useful in many public safety needs such as firefighting. It needs fast and high-resolution UL, and thus the required data rate can be calculated as follows:

- 1 Byte/pixel x 100 codec compression gain
- Full HD (1920*1080 pixels/frame)
- 20.7KB/frame after compression
- 17ms frame interval from 60Hz FPS
- Assuming 3 ms DL and UL radio latency
- 20.7KB/3ms=55.3Mbps in UL and DL
- Note: Peak/burst data rates used instead of Average data rate.

Service requirements of a 5G system including AR are described in [3GPP-22261].

3.2.2 Result of MC spectrum demand estimation

Here, the result of MC spectrum demand estimation is presented, assuming unicast communication.

Recall that we consider the bandwidth estimation for a rather demanding PS scenario of MC forest firefighting. The bandwidth has been estimated assuming cellular uplink/downlink.

A summary of the assumed service requirements is shown in Figure 3-2 below.

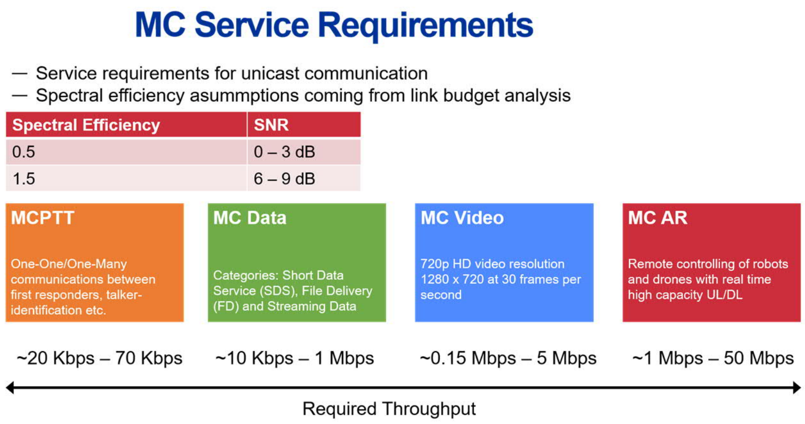

Figure 3-2: MC Service requirements. The data-rates are shown as intervals due to min and max (peak) rates.

For a spectrum efficiency of 0.5 bps/Hz, the resulting bandwidth estimates are shown in Figure 3-3 below.

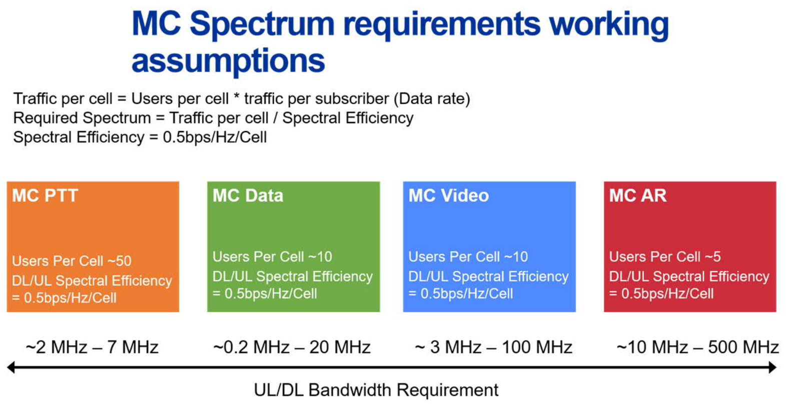

Figure 3-3: Spectrum estimate, for the described MC service example, for a spectrum efficiency of 0.5 bps/Hz.

Therefore, the sum of the bandwidth requirement for this MC scenario ranges between 15 and 627 MHz.

For a spectrum efficiency of 1.5 bps/Hz/cell, which is a rather good spectrum efficiency, the resulting bandwidth estimates are shown in Figure 3-4 below.

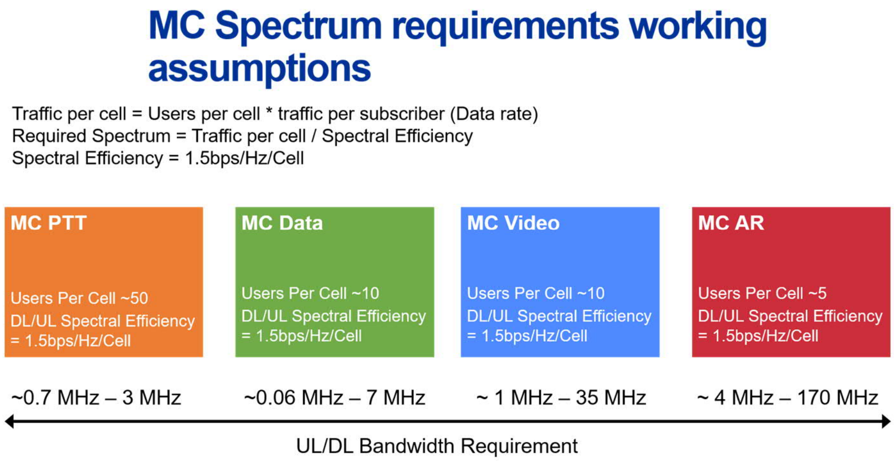

Figure 3-4: Spectrum estimate, for the described MC service example for a spectrum efficiency of 1.5 bps/Hz.

This means that the sum of the bandwidth requirement under the assumption of a good spectral efficiency is in the interval of 6 and 215 MHz.

3.2.3 *Summary and discussion*

The key results of the spectrum demand estimation are summarized as follows:

- The poorer spectrum efficiency (SE), the larger bandwidth need.
- For the considered MC forest firefighting use case, the estimated spectrum requirement is 15 - 627 MHz (for SE of 0.5 bps/Hz) and 6 - 215 MHz (for SE of 1.5bps/Hz), respectively, given the assumptions described earlier. Larger bandwidths are needed for the more advanced MC Video and hypothetical MC AR services.
- Depending on the extent of demand, e.g., the number of users and required data rates, the bandwidth requirement will differ.

It is noteworthy that, in practice, the allocated spectrum dedicated for public safety agencies around the globe is about 10 MHz or less. Looking at the lowest value of spectrum estimation, support for the basic MC services may be enough. However, supporting evolved public services with high-capacity and low-latency requirements needs significantly more spectrum. More and more public safety agencies are now considering prioritized access to MNO spectrum for providing advanced MC services.

3.3 Spectrum options for public safety

Basically, there are two spectrum options available for public safety: licensed spectrum and license-exempt spectrum. As operators many times are the main owners of national communication infrastructure, the Public Safety authorities will reuse the operator infrastructure and complement the operator infrastructure with temporary networks, if needed. Operators mainly use licensed spectrum for the infrastructure.

The reasons that operators use licensed spectrum are twofold: 1) to secure capacity to subscribers, 2) to secure QoE to subscribers. In an uncongested license-exempt situation an operator can satisfy 1) but cannot guarantee 2). In a congested licensed-exempt spectrum an operator can neither guarantee 1) or 2). That is why governmental bodies will build public safety solutions based on licensed spectrum with licensed-exempt spectrum as complement. On top of this, there may also be technical limitations between technologies used in licensed and licensed exempt spectrums.

3.4 Spectrum band availability for public safety

In this section, we provide an overview of the currently available spectrum for public safety in Europe and USA. Here, the focus is on the 700 MHz band because it is typically used by the public safety agencies.

The 700 MHz European harmonized PPDR band plans are shown in Figure 3-5 below. As shown in the figure, option B is the most popular option considered by PPDR agencies.

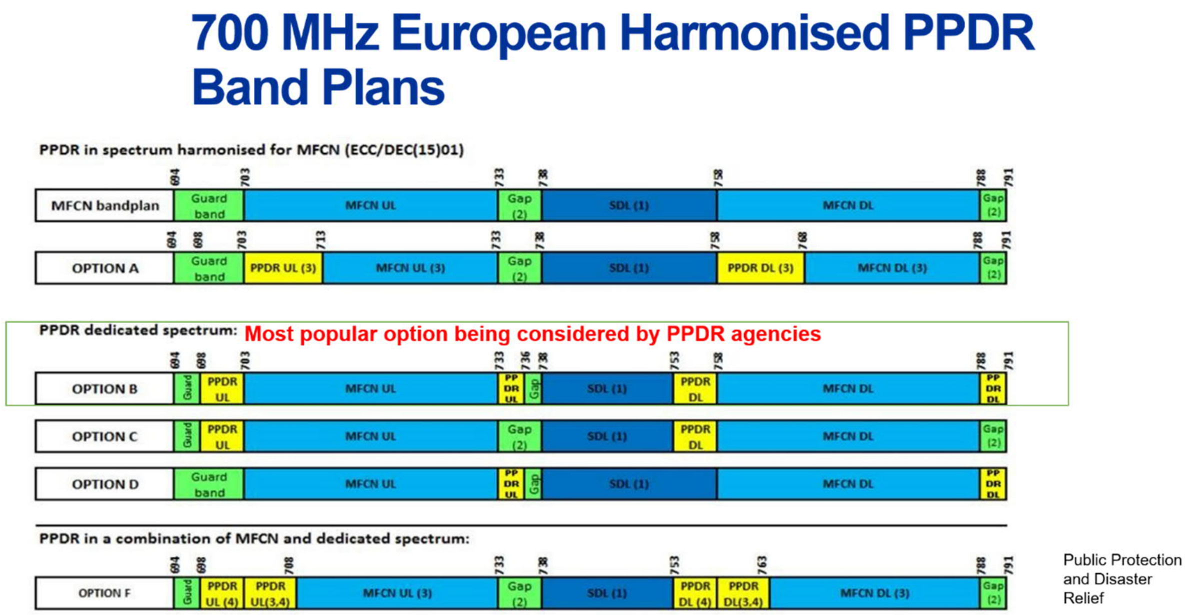

Figure 3-5: 700 MHz European Harmonized PPDR band plan. (source: [ECC15])

Figure 3-5 above shows options for frequency arrangements in CEPT. It refers to ECC Decision ECC/DEC/(15)01 (approved 6 March 2015) [ECC15], but there is also ECC Decision ECC/DEC/(16)02 (Approved 17 June 2016; Amended 8 March 2019) [ECC16].

This can be compared to the frequency arrangements in Recommendation ITU-R M.2015-2 [ITU18]. Table 3-2 below is a quote of the part pertaining to CEPT that includes references to the ECC Decisions in the Clause 1-1.1 “Harmonized frequency arrangements within the frequency range 698 to 791 MHz in accordance with the CEPT harmonization measure ECC/DEC/(16)02 for broadband PPDR” from [ITU18].

Table 3-2: A quote from [ITU18] on PPDR spectrum.

Frequency arrangements for broadband PPDR in the 698-791 MHz frequency range

<table>
<tr><th rowspan="2">Frequency arrangement (options)</th><th colspan="4">Paired arrangements</th><th rowspan="2">Notes</th></tr>
<tr><th>Mobile station TX (MHz)</th><th>Centre gap (MHz)</th><th>Base station TX (MHz)</th><th>Duplex separation (MHz)</th></tr>
<tr><td>a)</td><td>698-703</td><td>50</td><td>753-758</td><td>55</td><td>LRTC specified in Annex 1 of ECC/DEC/(16)02</td></tr>
<tr><td>b)</td><td>703-733</td><td>25</td><td>758-788</td><td>55</td><td>LRTC specified in ECC/DEC/(15)01</td></tr>
<tr><td>c)</td><td>733-736</td><td>52</td><td>788-791</td><td>55</td><td>LRTC specified in Annex 1 of ECC/DEC/(16)02</td></tr>
</table>

Detailed description of the frequency arrangement

<table>
<tr><th>698-703 MHz</th><th>703-708</th><th>708-713</th><th>713-718</th><th>718-723</th><th>723-728</th><th>728-733</th><th>733-736 MHz</th><th>736-753</th><th>753-758 MHz</th><th>758-763</th><th>763-768</th><th>768-773</th><th>773-778</th><th>778-783</th><th>783-788</th><th>788-791 MHz</th></tr>
<tr><td>PPDR a)
uplink</td><td colspan="6">PPDR b)
uplink (MFCN)</td><td>PPDR c)
uplink</td><td></td><td>PPDR a)
downlink</td><td colspan="6">PPDR b)
downlink (MFCN)</td><td>PPDR c)
downlink</td></tr>
<tr><td>5 MHz</td><td colspan="6">30 MHz (6 blocks of 5 MHz)</td><td>3 MHz</td><td></td><td>5 MHz</td><td colspan="6">30 MHz (6 blocks of 5 MHz)</td><td>3 MHz</td></tr>
</table>

Channelling arrangement for option b)

Channel number	Mobile station transmit Channel centre frequency (MHz)	Base station transmit Channel centre frequency (MHz)	Channel bandwidth (MHz)
N = 1 to 6	$f_N = 703 - 2.5 + N \times 5$	$f_N = 758 - 2.5 + N \times 5$	5

Administrations requiring 2 × 10 MHz for broadband PPDR, as calculated in Report ITU-R M.2377-0 and ECC Report 199, and authorizing the full 2 × 30 MHz in option b) for commercial mobile/fixed communications networks (MFCN) can no longer identify 2 × 10 MHz for dedicated broadband PPDR networks within the 700 MHz band. These administrations may therefore need to use the remaining part as shown in option a) and c) and additionally use the 400 MHz range.

For further information on broadband PPDR usage in CEPT please see ECC/DEC/(16)02 ("Harmonised technical conditions and frequency bands for the implementation of Broadband Public Protection and Disaster Relief (BB-PPDR) systems") and the relevant ECC Reports mentioned therein. For international coordination Resolution **749 (Rev.WRC-15)** and Resolution **760 (WRC-15)** are applied as appropriate. For the frequency range 698-791 MHz ECC/REC/(16)03 ("Cross-border coordination for Broadband Public Protection and Disaster Relief (BB-PPDR) systems in the frequency band 698-791 MHz") is relevant within CEPT.**"**

In the USA, the term FirstNet has come to refer to both the actual national wide public safety broadband network being built, and the public-private partnership between the FirstNet Authority and AT&T. Band 14 has been authorized to FirstNet as follows:

- UL: 788 MHz – 798 MHz
- DL: 758 MHz – 768 MHz

According to the decisions made by USA governments, AT&T can use public safety spectrum capacity for its commercial operations as long as the capacity is not required by PS operations. In addition, it allows immediate usage of AT&T's commercial network for FirstNet subscribers to kick-start the operational phase as well as to provide good redundancy. (see, e.g., [ATT18])

In conclusion, public safety frequency bands are expanding both when it comes to enable spectrum sharing for dedicated and commercial bands as well as providing bands for non-terrestrial networks. 5G also provides opportunities for migrating LTE bands.

4 Innovative spectrum usage

In this section, we discuss some issues related to spectrum usage for UAVs, particularly in the context of mission critical services. Firstly, we explore the feasibility of an innovative spectrum usage in license-exempt spectrum band. Here, the objective is the investigate whether a low-latency access is achievable in license-exempt band. Secondly, we address the coexistence between aerial users (e.g., drones) and other services (e.g., ground users, other aerial users, or satellite) both connected to a terrestrial cellular system on licensed spectrum. Our study is focused on the use of adjacent channels by the aerial users and other services.

4.1 Feasibility of utilizing license-exempt band

In order to minimize or even eliminate external interference, it is important to have control of the spectrum used for over-the-air transmission. In most countries, spectrum is treated as a natural resource, with usage controlled by national authorities which allocate resources according to the country's needs. Spectrum is divided into several frequency bands. Bandwidths are specified by authorities and depend on the needs of the user and of others competing for the same resource. Some spectrum is aligned with international standard bands, as in 3GPP. Spectrum can be either licensed, which means that the license holder is the only authorized user of that spectrum range, or license-exempt, which means that anyone who wants to use the spectrum can do so, such as for Wi-Fi [ERI19].

License-exempt spectrum can be used by anyone, anytime. As a result, it can be unused and support very good service quality, or it can be completely congested and therefore insufficient for supporting good service quality for even simple applications. It is not possible to know the status at any point in time, and thus it is generally believed that license-exempt spectrum is not a good choice for critical communications with predictable deterministic performance. A prerequisite for critical communications is full control of the spectrum. Today, only licensed spectrum guarantees control over spectrum usage by the system, making it a preferred option for critical communications. Furthermore, 3GPP has standardized solutions for the low-latency access. License-exempt spectrum for mission critical communications has been technically down-prioritized because the listen-before-talk and back-off mechanisms employed by Wi-Fi standards incur latency and poor service quality particularly in the congested traffic situation. Therefore, there are research opportunities to exploit whether a new medium access control (MAC) mechanism in the license-exempt spectrum has feasibility to be used or to complement licensed spectrum for non-critical communications.

4.1.1 Problem definition

URLLC is an essential component of the 5G communication networks. However, with the wide variety of services being offered by telecommunication networks, the limited spectrum available to them is already saturated. In addition to the terrestrial users in the network, aerial users (e.g., drones) are also being connected to the cellular networks. Drones with autonomous operations require URLLC for the command and control between them. This astronomical growth in the users and limited available spectrum has motivated us to look for some innovative way of sharing the spectrum. Therefore, in this work, we investigate the use of license-exempt spectrum for URLLC.

As the name suggests URLLC communications are extremely delay sensitive and require protocols that prioritize minimizing the latency. URLLC requires reliable transmission of time sensitive information between nodes. The license-exempt bands with current MAC like in Wi-Fi suffer from high latency. Listen Before Talk (LBT) and back-off mechanisms that are employed in license-exempt bands hinder the use of URLLC services in these bands. Therefore, in order to use URLLC services in license-exempt bands, one of the main challenges is to design a new MAC that enables low latency access in license-exempt bands. To further reduce the size of the problem, we design the MAC for the pairwise random network. In this section, we focus only on the latency. Reliability, e.g., security issues with license-exempt spectrum, is beyond the scope of the section.

4.1.2 *Proposed solution approach*

4.1.2.1 System model

In this work we consider a random pair-wise network where a transmitter and a receiver in a pair are pre-determined. This ensures that there is no conflict within the pair. All the individual pairs are autonomous and are not coordinated by a centralized entity. This makes the MAC design a distributed approach for the random access. The channel model considered is the free space model with extension to include the air to ground channel for the aerial users. Figure 4-1 illustrates the concept of random pair-wise network. The red circle in the figure indicates the collision region of the node in the center.

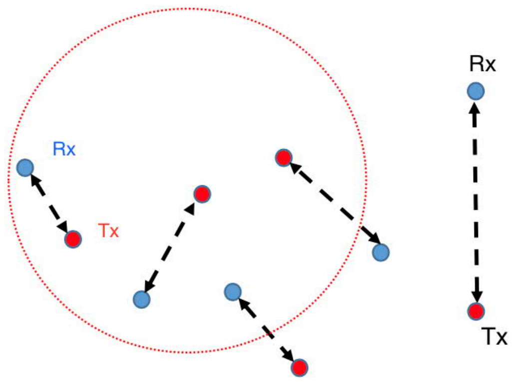

Figure 4-1: An illustration of pair-wise random network.

4.1.2.2 Solution Approach

We use a novel approach to design a random access that uses a non-orthogonal signal decomposition technique, which is Geometric Sequence Decomposition with k-Simplexes Transform (GSD-ST) [LLS20]. With GSD-ST, we have a possibility of many users sharing a limited bandwidth and thus giving us the ability to utilize the spectrum more efficiently. Non-orthogonal interference-free radio access (No-INFRA) which uses GSD-ST to enable collision-free reception of uncoordinated signals [LLS20] can be used for access in our new MAC. Therefore, we develop a synchronized slotted system that utilizes No-INFRA for access and conventional schemes like Orthogonal Frequency Division Multiplexing (OFDM) for data transmission. The collision of the grant and request messages is resolved by using the GSD-ST and with message size of the access messages very small, a small bandwidth is required.

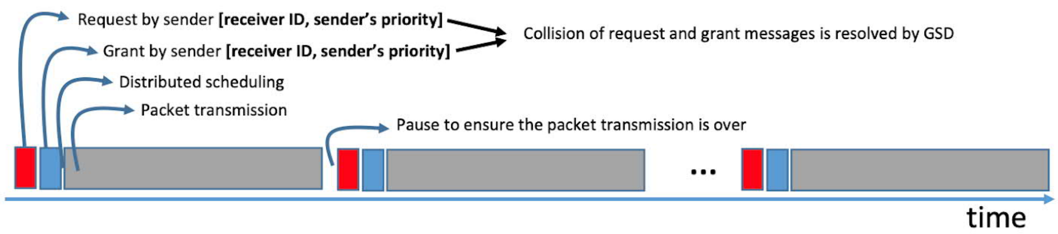

Figure 4-2: Concept of proposed low-latency MAC.

Using the non-orthogonal signal decomposition technique allows all users to send access requests simultaneously which can be resolved by the receivers. This allows receivers to grant or deny access to their corresponding transmitters according to the priority of the requests received by them. A transmitter then sends data only if it is granted access by the intended recipient. This approach removes the need for LBT, congestion windows and back off. The resulting improvement in latency makes it viable for delay sensitive URLLC applications. This system also overcomes commonly encountered problems of multi-access channels like the hidden and exposed node problems. The concept of proposed low-latency MAC is depicted in Figure 4-2.

To begin with, we consider pairwise random networks where the transmitter receiver pairs are pre-defined. We can then extend our results to more general topologies. As long as the transmitters set and the receivers set are predefined, the results can be easily extended. In order to compare the performance of the proposed scheme, it is important to compare it with the already existing schemes like carrier-sense multiple access with collision avoidance (CSMA/CA) that are commonly used for medium access in license-exempt bands. Therefore, we start with the application of the CSMA/CA in our system model. We investigate the latency and throughput using the CSMA/CA. We focus on the time lost in the LBT and the back-off of the CSMA/CA. We can then conduct analysis and simulations to assess the performance of the proposed protocol in comparison to the CSMA/CA [HTC+09].

4.1.2.3 Performance metric

We define our performance metric as follows:

- Efficiency: The ratio of the number of slots a node is transmitting the data to the total number of slots where the node has data to send. Because of the random access the nodes will not always be successful in transmitting the data because of the priority in granting access to different nodes and also the error in receiving the request message or grant message. In case of the CSMA/CA, because of the wait before send, collisions and the back-off, we lose the time slots. In CSMA/CA, we also define efficiency as the ratio of the number of slots a node is transmitting the data to the total number of slots where the node has data to send.

$$Efficiency = \frac{Transmission\ Time}{Transmission\ Time\ + Time\ lost\ in\ waiting\ +\ Time\ lost\ in\ error}$$

We investigate performance of our No-INFRA based solution to a benchmark CSMA/CA scheme where carrier sensing is used and nodes start transmitting the data only after sensing the channel is idle. Once the transmission starts, the data packets are sent in their entirety. In this scheme, the node when sense that the channel is being used will wait for a period of time (usually random) for the channel to be free before listening again for a free communications channel. Thus, the node loses time when it actually wants to send the data. Also, when the collision happens in the transmission, the node goes into a back-off procedure for a binary exponential random period before attempting to retransmit. Thus, again wasting the time when the node wants to transmit the data. Our scheme is different from the benchmark as we do not have to wait for the channel to be free for obtaining the access. Based on the priority of the node, we can transmit our request to the target nodes and if given a grant, all the others will not transmit.

4.1.3 Numerical results

We consider a time slotted common collision area with a number of nodes-pairs ranging from one to four. Our focus is to compare the MAC performance of our scheme with the benchmark. We use MATLAB to compare the MAC performance of our new No-INFRA based scheme with the benchmark CSMA/CA scheme. In implementing the No-INFRA based MAC, we use the SNR range of 5 to 60 dB. The error probability in transmitting the request and grant messages is considered in the range of 0.001 to 0.1. The error probability is the function of the SNR of the link and the number of node pairs transmitting at the same time. We assume an ideal error-free transmission for the data. For the traffic, we consider a Poisson arrival traffic model for the nodes.

We provide the simulation results to show performance of our new No-INFRA based MAC scheme by changing the number of nodes, data rates, and SNR values in the system. We also compare our scheme with the CSMA/CA.

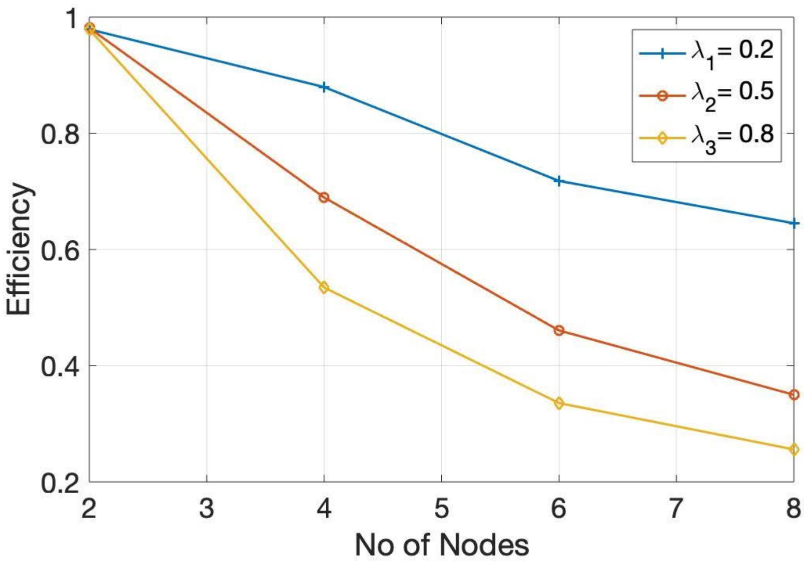

Figure 4-3: Efficiency according to the number of nodes in the system.

In order to investigate the effect of increased number of nodes in the system on the efficiency in time for the nodes to transmit the data, we changed the number of node-pairs from one to four. As can be seen from the Figure 4-3, an increase in the number of nodes decreases the efficiency. This is because of the two main reasons. First, as the number of nodes increase in the system, more time will be wasted in waiting for the channel to be free. Second, the error probability in transmitting/receiving the request and grant message is the function of number of simultaneously transmitting node pairs. As the node-pairs increase the error probability increases and we lose time. We have defined three traffic loads, low load ($\lambda_1 = 0.2$) means we have two new data packets per ten time slots. For moderate traffic load ($\lambda_2 = 0.5$), we have 5 data packets per ten time slots and for high traffic load ($\lambda_3 = 0.8$), we have 8 data packets per ten time slots. We see traffic loads affecting the efficiency, the higher traffic load makes the nodes wait more for them to transmit. A relatively low traffic load at four nodes in a system performs better than the system having only two nodes but with a higher traffic load.

The error probability in transmitting/receiving the request and grant message is a function of the SNR of the link. High SNR regime represents LOS available among the UAVs. This can be seen from Figure 4-4, as the SNR increases and the channel quality increases, the efficiency also increases. For different numbers of node-pairs in the system, we can see an increase with the increase in SNR but the increase with three node-pairs in the system is steep as compared to two and four node-pairs. This can be explained by the fact that with lower number of node-pairs, the channel efficiency is at its highest and cannot be improved much while with higher number of node-pairs, the main reason for loss of time slots is the channel being busy while other nodes are transmitting.

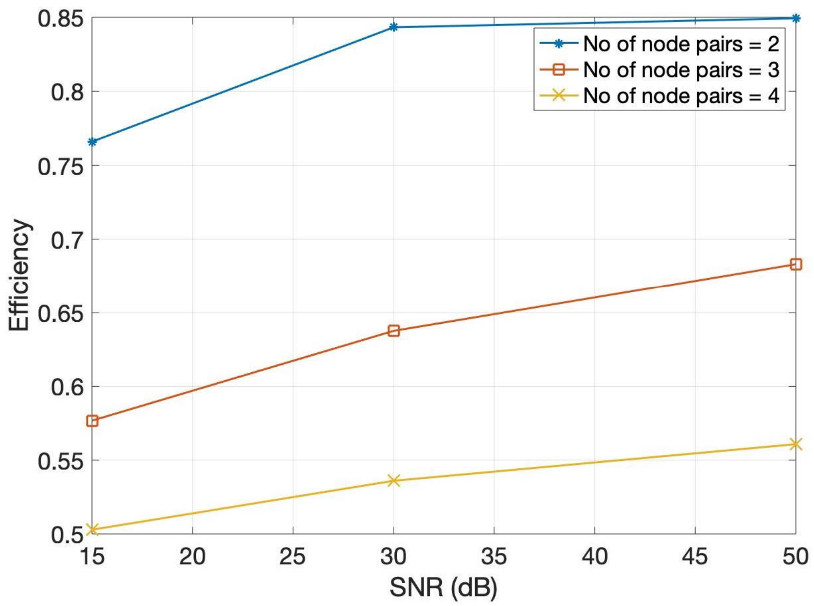

Figure 4-4: Efficiency according to SNR ($\lambda_2 = 0.5$).

In order to see if our proposed scheme is performing better, we need to compare it with the bench-mark scheme. In this case, we compare the performance of our scheme with the CSMA/CA. As can be seen from the Figure 4-5, our system performs better than the CSMA/CA even at the higher number of simultaneously transmitting node-pairs and even much better at the lower number of node-pairs. Our scheme is 50% more efficient than the CSMA/CA in terms of the time efficiency. Thus, making it a perfect candidate for the low latency communication in the license-exempt bands.

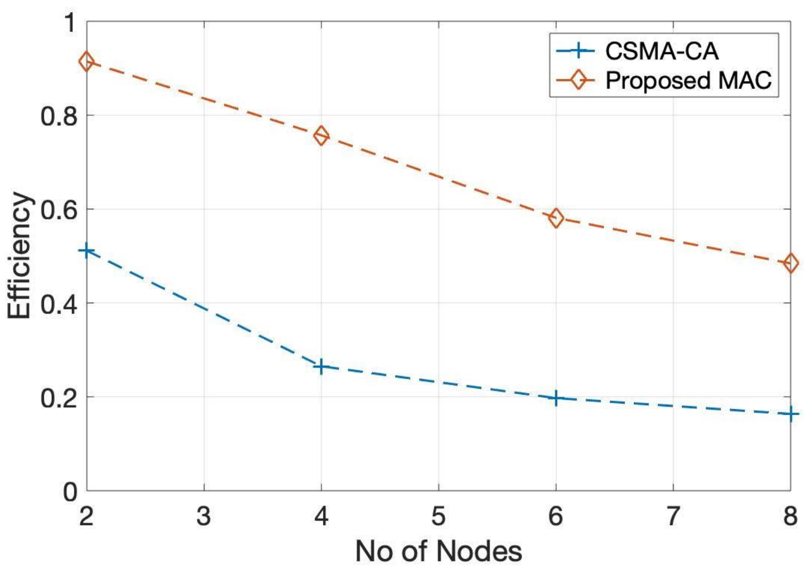

Figure 4-5: A comparison of the proposed MAC and CSMA/CA ($SNR = 30dB$, $\lambda_2 = 0.5$).

The last phase of this work will involve further extensions to unpaired random networks. Such networks present several new issues that need to be studied further and resolved. The solution strategies for these networks are not immediately clear.

4.2 Coexistence of aerial users and other services in adjacent channel

This section focuses on analysing the impact of the introduction of drones on their host or own network operating in the same frequency and the potential coexistence issues with another cellular networks and/or services, e.g., Complementary Ground Component (CGC), operating in an adjacent frequency in licensed spectrum. To this end, in the first step, the impact of including drones in an LTE network towards an adjacent or neighbouring LTE network, both operating at 2.6 GHz, is studied. The next step covers the impact of including drones in an LTE network towards the adjacent services such as satellites at 2.1 GHz.

In this study, the drones are depicted as the UEs and not the BSs. From this perspective, the main difference that distinguishes drones from the ground users in a cellular network is the height. In the simulations carried out in this study, it is assumed that the ground users are at a fixed height of 1.5 m above the ground, whereas the drones can fly in the height range between 1.5 m and 300 m above the ground. Furthermore, CGC is a ground-based infrastructure in a satellite network which contains the CGC base station as well as the airplanes equipped with the aeronautical terminals which can communicate with the CGC base stations and the Mobile-Satellites Services (MSS) [3GPP-38901]. In this subsection, we are only interested in the terminals transmitting toward the CGC base stations at 2.1 GHz band. Simulation parameters for both macro and CGC networks are listed in Table 4-1.

Table 4-1: Simulation parameters.

Network parameters		
	Macro and UAV	CGC
Cell layout	Inter-side distance of 500 m	Cell radius 150km
BS antenna height	25 m	25m
Duplex	FDD	FDD
BS transmit power	46 dBm	47 dBm per polarization
Bandwidth	10 MHz	10MHz
Drone heights	Range of 1.5 m – 300 m	
Propagation	Uma model for macro [1], UAV model for drones [2]	Free space
Aircraft coordinate		(150km,150km,13km) assuming CGC BS is at origin
ACIR	0-60dB	30dB

The scenarios used for the simulations to understand the coexistence behaviour are summarized in Table 4-2. Since the main interest is in the impact of adding drones, the scenarios with their associated baselines are the ones without drones in the network. In addition, in each scenario and its corresponding baseline, two networks namely the victim and the aggressor exist. To understand the coexistence behaviour, the victim network performance metrics, DL/UL average network throughput loss and interference levels, are evaluated [3GPP-36777].

Table 4-2: Simulation scenarios.

Baseline 1	LTE @2.6 GHz serving ground UEs (Victim) vs LTE @2.6 GHz serving ground UEs (Aggressor)

Scenario 1	LTE @2.6 GHz serving ground UEs (Victim) vs LTE @2.6 GHz serving ground UEs + UAVs (Aggressor)
Baseline 2	LTE @2.6 GHz serving ground UEs + UAVs (Victim) vs LTE @2.6 GHz serving ground UEs (Aggressor)
Scenario 2	LTE @2.6 GHz serving ground UEs + UAVs (Victim) vs LTE @2.6 GHz serving ground UEs + UAVs (Aggressor)
Baseline 3	LTE @2.1 GHz with CGC base stations serving users in the aircraft (Victim) vs LTE @2.1 GHz serving ground UEs (Aggressor)
Scenario 3	LTE @2.1 GHz with CGC base stations serving users in the aircraft (Victim) vs LTE @2.1 GHz serving ground UEs + UAVs (Aggressor)

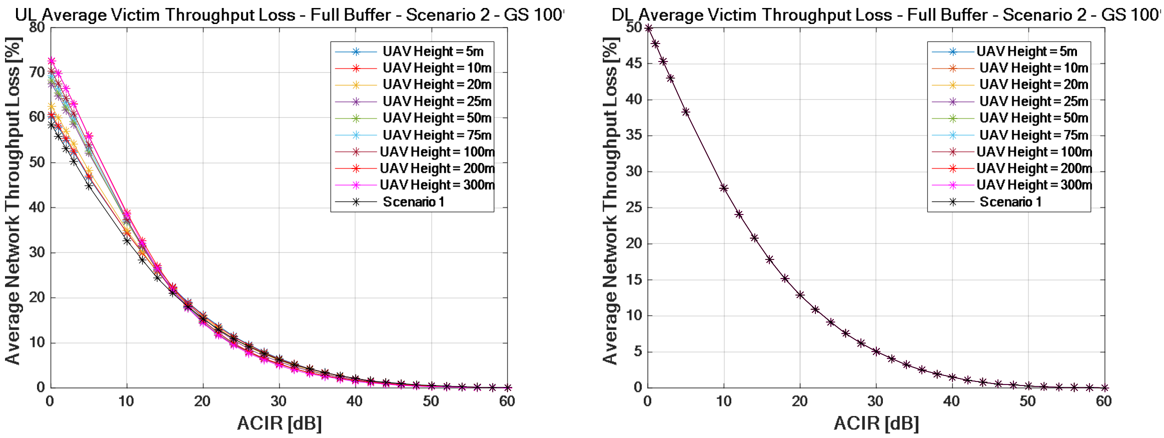

Figure 4-6: UL/DL Average Victim Throughput Loss vs ACIR

Figure 4-6 illustrates the UL/DL average victim network throughput loss as a function of adjacent channel interference ratio (ACIR) for Scenario 1. In baseline 1 (i.e., no drones in the aggressor network) the UL throughput loss in the victim network is the lowest compared to the scenario 1 (i.e., with drones in the aggressor network). In addition, when drones fly higher up in altitude, the throughput loss becomes higher. However, in all cases the 5% of the average victim network throughput loss value is similar. This leads to the conclusion that both networks in scenario 1 can coexist with the same ACIR requirements on the BS as in baseline 1. In the DL, there is no impact on the victim network when drones are introduced in the aggressor network.

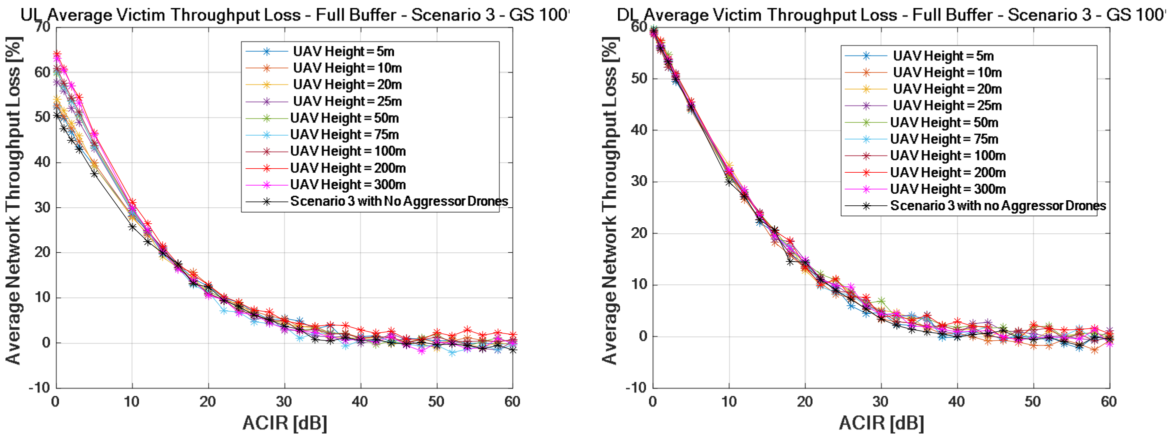

Figure 4-7 : UL/DL Average Victim Throughput Loss vs ACIR

For the scenario 2, the UL/DL average victim network throughput loss as a function of ACIR is shown in Figure 4-7. It can be seen that in Baseline 2 (black curve), where there are no drones in the aggressor network, the UL throughput loss in the victim network is the lowest compared to having uniformly distributed drones in the aggressor network. In this setup the drones are always present at a fixed height above the ground in the victim network and the impact on this victim network is studied. In addition to that, it can also be seen that when the drone goes high up in altitude in the victim network, the throughput loss becomes higher. However, in all cases the 5% average network throughput loss value is similar which again concludes that both these networks can still coexist with the same ACIR requirements on the base station receiver as before when no drones were introduced in the aggressor network. However, in the DL, there was no impact on the victim network when adding drones in the aggressor network.

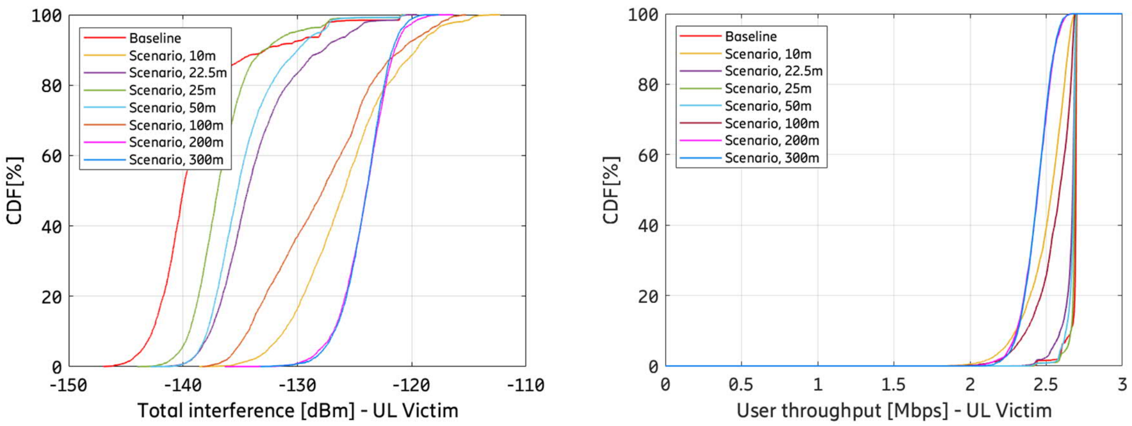

Figure 4-8: UL Victim Interference and User Throughput.

The results of coexistence with CGC network are presented in Figure 4-8. It shows that when drones are flying below the base station height, the higher they are, the less interference in the victim network they generate. However, once they pass the base stations, the higher, the more interference. In addition, the user throughput gets better when drones are still below the base stations height of 25 m and gets worse when above it while flying higher. It is also observed that although the interference can never be as small as the base line interference, the user throughput can become very close when drones are flying in vicinity of the CGC base station.

Introducing UAVs in the adjacent operator network does not really affect the performance of the victim network without UAVs and victim network with UAVs. Hence no additional suppression is required in terms of ACIR. In addition, for a better coexistence performance, the operators might want to have a min-distance between aggressor drones and victim BS because higher min-distance will lead to a better performance.

Presence of UAVs in an LTE system adjacent to the satellite service (CGC system) is increasing the aggregated total interference toward the CGC base station which is communicating with the aircraft. Such an increase is also observed in the user throughput results for the CGC system in the UL. The impact of the altitude of drones above the base station is as follows: higher the drones from the ground, higher is the interference. However, if UAVs are flying below the base station, the behaviour is different: higher altitude UAVs cause less interference.

The overall conclusion of this study is that the introduction of drones causes negligible impact on adjacent channels, whereas on adjacent satellite service, the impact is considerable mainly in the UL.

5 Economic and business aspects of PriMO-5G

In this section, we touch upon the economic and business aspects on fulfilling PriMO-5G use cases. Firstly, we investigate operational models for public safety communication systems. Particularly, viability of providing mission critical services in commercial networks is discussed in Section 5.1. Then, in Section 5.2, we consider non-public network as an option for enriching the ecosystem of public safety communications.

5.1 Viability of mission critical services in commercial networks

Public safety communications are moving from a voice-centric paradigm to a data-centric paradigm [PRI19-D12]. The public safety agencies and industries have used dedicated networks with specialized technologies such as terrestrial trunked radio (TETRA) [ON20]. While TETRA has proven itself to be reliable, resilient, and secure, it is a narrowband technology mainly providing voice services. As we discussed in Section 3.2, emerging mission critical services require data-centric systems that are capable of broadband applications. Therefore, the future of public safety communications will be enabled by LTE, 5G, and the ongoing the 3GPP evolution.

Many countries are currently faced with the challenge of establishing the next generation public safety communications. The challenge is not only to satisfy the requirements for performance, reliability, and security, but also to achieve the economic viability from the economies of scale and making best use of available technologies.

In this light, an important question is who will establish and operate the public safety communications system. In principle, this can be roughly rephrased as follows: whether a dedicated (also state-owned in most cases) PPDR mobile network should be established or existing commercial mobile networks should be strengthened and utilized. In practice, however, there are various options in detail. Note that this also includes access to spectrum, e.g., dedicated public safety spectrum or shared spectrum, e.g., prioritized access to MNO spectrum. In [LK18], four different models are suggested. Quoting [LK18], these four models are as follows:

- **State-owned network with commercial fallback (State MNO)**. The state establishes and owns a dedicated PPDR network and signs one or more roaming agreements with commercial networks for added coverage and robustness.
- **Single commercial network (One RAN)**. The state buys access to PPDR services from a single commercial operator only, and relies on the coverage and reliability of that network. ESN (UK) and FirstNet (USA) both fall into this category, albeit with quite different contractual arrangements.
- **Primary network with fallback (Primary RAN)**. One commercial operator is the main PPDR supplier, but a second mobile network is used as backup when the primary network is not available.
- **Multiple equal networks (Equal RAN)**. The PPDR network is based on two or more commercial mobile networks that have the same role in the solution design.

Regarding the technical feasibility of the public safety communications through commercial networks, [NEC20] claims that commercial networks are not an option for public safety because only dedicated networks can provide the reliability and performance required for the critical services. It is widely agreed that commercial networks can be used for mission critical purposes if the networks are hardened [FHB14]. As for the cost, commercial networks are expected incur much lower cost than the dedicated option [FHB14, LK18, KL18]. According to [LK18], the State MNO option obviously shows the highest expected cost, while the costs of the three options for the commercial networks are similar and the best option may differ depending on specific requirements and the market situation in the specific country, as illustrated in Figure 5-1.

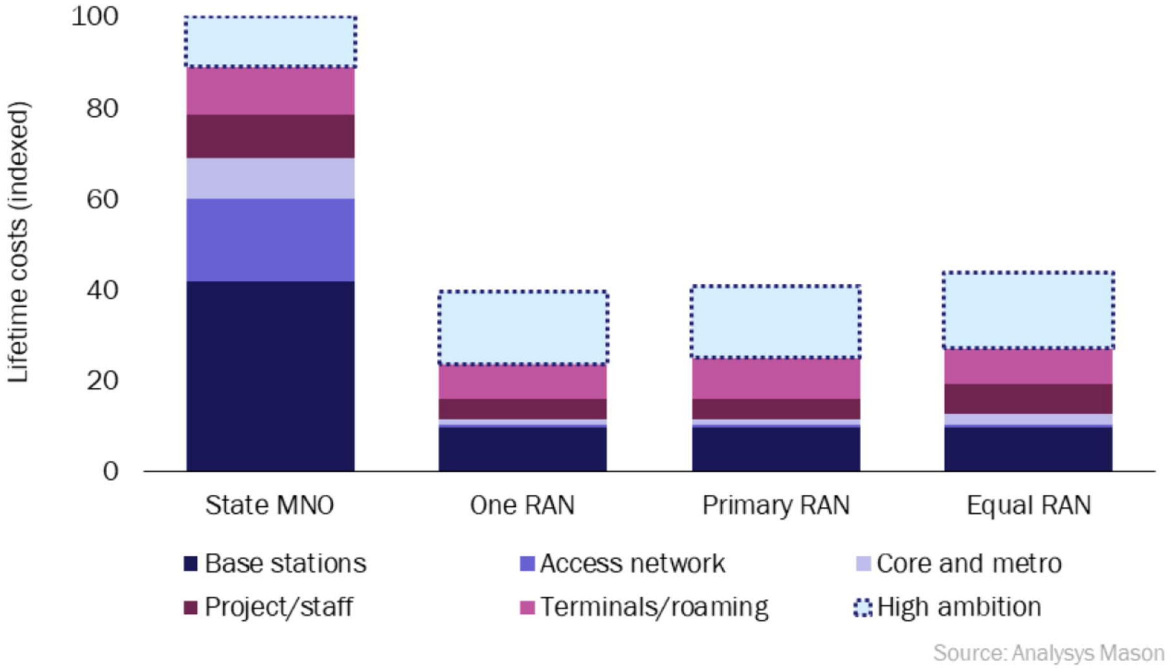

Figure 5-1: Cost comparison of the four models (source: [LK18]).

Some countries, such as Norway, the UK, and the USA, have decided to utilize the commercial mobile networks for the mission critical services. In the year 2018, the Norwegian government published a white paper about three alternatives for providing mission critical services in commercial networks [DSB18]. According to [DSB18], the three alternatives are as follows:

- **Secure MVNO**: The State acquires its own core network and service platform and enters into agreements with preferably all mobile operators for use of their radio access networks. With this model, the State will be responsible for the end-to-end functionality and performance.
- **A single turnkey provider**: A single operator provides the communication services through a turnkey contract, and there is no need for any state-owned network infrastructure. The preferred operator will be responsible for the end-to-end functionality and performance.
- **Several competing turnkey providers**: This model is an extension to the turnkey model, where two or all three of the operators in Norway can offer the services and compete to attract the users. Each operator will be responsible for the end-to-end functionality and performance of the services for their own subscribers only, but have to co-operate to ensure that services work across the networks.

In [DSB18], the advantages and disadvantages of the three models are summarized as shown in Table 5-1 below.

Table 5-1: A summary of the three alternatives (source: [DSB18]).

	Model 1 State-owned MVNO	Model 2 A single turnkey provider	Model 3 Several, competing turnkey providers
Main concept	A dedicated, state-owned NGN core network using radio resources in preferably	NGN implemented inside a single commercial network. Roaming to back-up	NGN implemented independently inside several commercial networks. Full NGN

	Model 1 State-owned MVNO	Model 2 A single turnkey provider	Model 3 Several, competing turnkey providers
	all three commercial networks.	radio access network(s) as an option.	service interoperability and national roaming across the networks.
Main benefit	Governmental control of the core network and user data. Minimum impact on the mobile market competition.	One main responsible, simplest technical and contractual structure.	Enables competition for NGN services. Less impacts on the mobile market competition.
Main challenge	Technically and contractually complex. Many involved parties, need for several contracts. The State must take the end-to-end responsibility.	Hardening the network of the selected operator may result in lock-in and market-inefficiencies.	Continuous risk of service incompatibility and malfunctioning between the networks. Many involved parties, need for several contracts.
Responsibilities and contractual relations	The State is responsible for establishing, updating and operating the core network. Requires separate agreements with the operators for connection to, and use of their radio access networks.	One main contract between the State and a single overall responsible operator.	Separate contracts between the State and the qualified operators. End-to-end responsibility governed by the operators through interconnect-agreements. Public Safety organisations can choose what NGN operator to use.

PriMO-5G project has been working on technical enablers and architecture components that can contribute to the realization of the use cases. These technical enablers would play an important role in the selection of the aforementioned models. Two of the most relevant enablers are network slicing and moving base station, which are explained below.

- *Network slicing*: According to GSMA, a network slice is defined as an independent E2E logical network that runs on a shared physical infrastructure, capable of providing a negotiated service quality [GSMA20]. It is the one of the key features of 5G. From the perspective of mission critical services, network slicing enables the public safety agencies to establish a logically dedicated network although the physical configuration is more complex [ON20].
- *Moving terrestrial and aerial base stations*: In the use case scenarios developed in [PRI19-D11], fire truck is equipped with gNB and can act as a base station near the incident site. The moving terrestrial base station can serve both terrestrial and drone user equipment and can include application servers as well. In addition, some UAVs can act as aerial base stations to cover dead spot due to obstacles and to serve a swarm of UAVs. With these base stations, the network can provide the required coverage and capacity quickly after an incident happens without the need for keeping high network density in remote areas [FAN+16].

The network slicing and moving base station have potential to lower the cost of public safety communication networks, and thus they should be considered in the cost calculation. Furthermore, it is noteworthy that the moving terrestrial and aerial base stations are coupled with the equipment of public safety professionals, e.g., fire brigade, which necessitates a new model for network establishment and operation. Non-public network, which will be discussed in the next section, can be considered to be an element of such a model.

5.2 Non-public networks

A new generation of private 5G networks is emerging to address critical wireless communication requirements in infrastructure, industry, and potentially public safety deployments. These private networks are physical or virtual cellular systems that have been deployed for private use by governments or companies. Non-public network (NPN) is the term adopted by 3GPP for such networks. Critical capabilities are network features and services that are needed to serve mission-critical or business-critical use cases. Mission-critical functions are vital to an organization's or society's operation, such as public safety services and electricity. Critical capabilities target the fulfillment of multiple key performance indicators (KPIs) in a 3GPP cellular connectivity solution. Private networking is related to the degree of control that the given industry has over the provided service. The main critical capability requirements for private networking are illustrated in Figure 5-2 [ERI19].

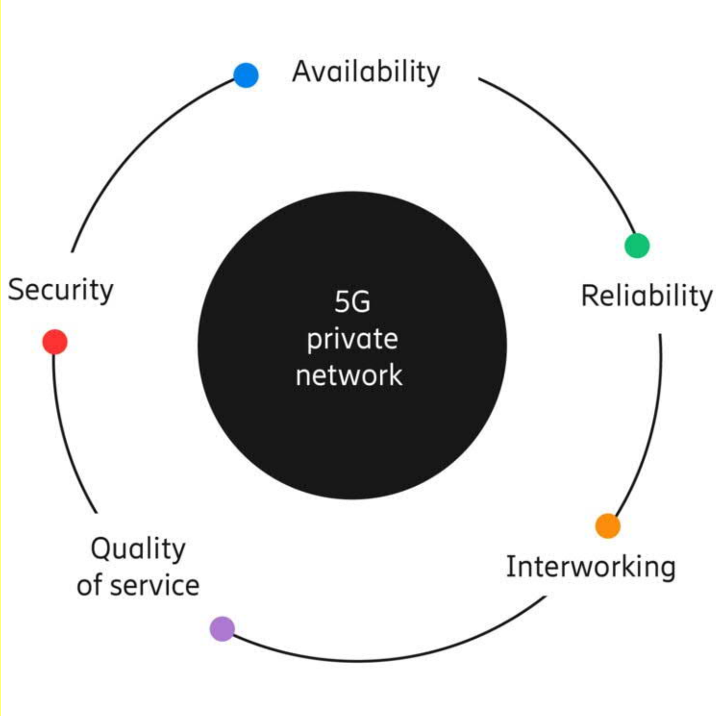

Figure 5-2: Main capability requirements for private networks. (source: [ERI19])

Although a wide variety of IoT use cases can be run over private networks, most use cases' similar connectivity needs are covered by standardized critical 3GPP functions. Mobile technologies before, and including, 4G were designed to support voice and best-effort services and were not initially considered for mission- or business-critical communications. However, standardization efforts to better serve such use cases were ramped up with 3GPP Rel-12. In the mission-critical domain, public safety was an early 3GPP critical communications requirement driver, with several features introduced in LTE Rel-12. 5G is designed to handle critical communications from the start. A set of critical capabilities are included as intrinsic components in the first 3GPP standard for 5G, Rel-15, in the URLLC feature set [ERI19].

From the perspective of PriMO-5G use cases, when a disaster occurs, some damages to the nearby infrastructure may be incurred. If communication-related facilities (such as BSs) are damaged, the communication failures make it difficult to use several communication services including emergency calls. In South Korea, a roaming system for disaster situations is established to maintain communication services such as phone calls and text messages. In the disaster roaming system, data communication other than phone calls or messaging is restricted due to problems such as an overload of data. Under this circumstance, it is difficult to ensure a stable communication environment for utilizing equipment such as drones and robots. NPN can be used to satisfy communication requirements for mission-critical use cases such as public safety use cases. Self-contained cores and networks enable stable communication and support better performance. If it is used with mobile BSs, 5G communication can be easily supported even in disasters in suburban and remote areas where 5G supply is insufficient. In short, NPN enables dedicated 5G communication in public safety situations, further increasing the utilization of equipment requiring high-capacity, real-time data transmission.

5.2.1 Status of Non-public Networks

NPNs are considered by many companies and countries due to their advantages such as mobility, broadband, low latency, and massive communication over traditional wired LANs, Wi-Fi LANs. Countries such as Japan (local 5G) and Germany are pushing for the introduction of NPNs by allocating dedicated frequencies as summarized in Table 5-2. If NPNs are introduced, new stakeholders may emerge in existing MNOs and a small number of vendor-oriented markets.

Table 5-2: Frequency Allocation Status for NPN.

Country	Bandwidth	Range
Japan	100MHz	28.2 – 28.3GHz
Germany	100MHz	3.7 – 3.8 GHz
U.K.	390MHz 2.25GHz (indoor only)	3.8-4.2 GHz 24.25 – 26.5 GHz
Hong Kong	400MHz	27.95 – 28.35 GHz
Finland	20MHz	2.3 – 2.32 GHz

5.2.1.1 Deployment methods of Non-public Networks

The deployment methods of NPN are largely divided into two categories: SNPN (Stand-alone NPN) and PNI-NPN (Public Network Integrated NPN) [3GPP-23501]. SNPN is the method operated by an NPN operator and not relying on network functions provided by a PLMN. PNI-NPN method is deployed with the support of a PLMN. Details of how to deploy a Non-Public Network are described in Section 5.5 of [PRI19-D12]. In this section, we will discuss the case where another agency has credential based on the NPN deployment models.

5.2.1.2 Requirements of Non-public Networks: 3GPP

According to [3GPP-22261], requirements of NPNs can be summarized as follows:

- The 5G system enables the standalone operation of NPNs, enabling the operation of NPNs without the dependency of PLMN.
- If there is agreement between the operators and service providers, the operator should provide the support for NPN subscribers with the following:

- o Access to subscribed PLMN services via the NPN
- o Access to selected NPN services via a PLMN
- o Seamless service continuity for subscribed PLMN services and NPN services between a NPN and a PLMN.

5.2.1.3 How to support SNPN with separate subscriptions from SNPN

Supporting SNPN using subscriptions provided by other entities is essential. This enables some of the main use cases of Non-Public Networks. In particular, it can support the moving scenarios, including service continuity, of the UE. It also enables simultaneous data services with other networks (e.g., PLMN) [3GPP-23700].

- Visited-SNPN (V-SNPN): SNPN to which the UE does not have a credentials for that SNPN, but provides access.
- Home Service Provider (Home SP): SNPN, which is separate from the existing SNPN, but has the subscription information of the UE.

The entity that provides the data services can be the serving SNPN or the Home SP. The connection between SNPN and Home SP is similar to roaming, but it is not necessary to follow the roaming interface. At this time, the UE has an “Equivalent Home Service Provider” list and/or an “Service Provider Controlled Network Selector” list and/or “User Controlled Network Selector” list for network selection.

5.2.2 Economic Impact of Private 5G Networks

Private networks are gaining momentum across a number of industries that require use cases of new telecommunications services for many enterprise environments such as IoT, automation and AR/VR. The telecommunications market for private networks is likely to grow into a multi-billion-dollar industry over the next decade. In addition, the private network market is expected to increase steadily, making it an industry that surpasses the current public cellular market. [5GA20, ABI20]. Figure 5-3 shows the expected CAPEX of cellular 5G networks with regard to the type of operations.

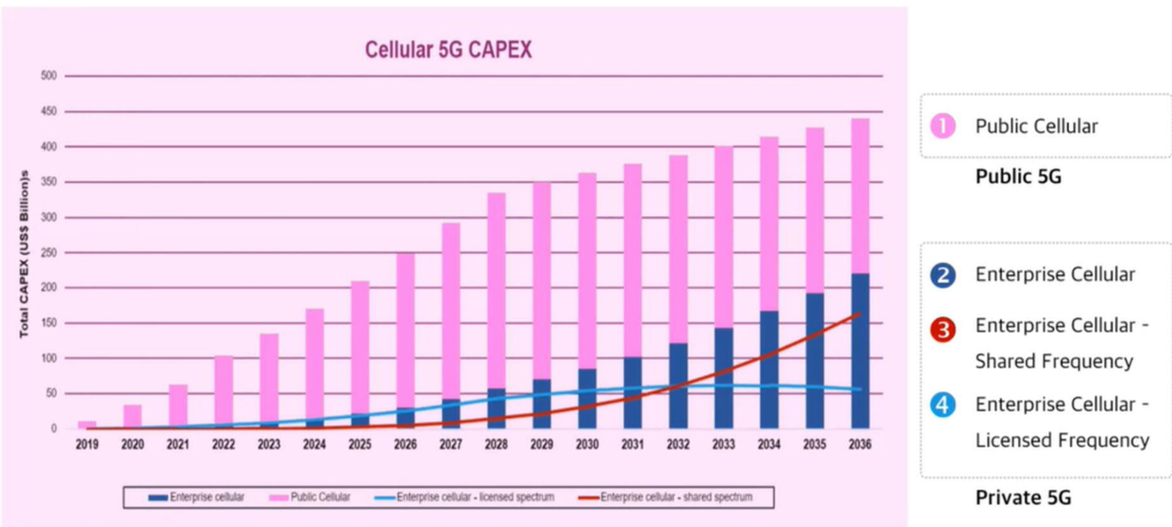

Figure 5-3: Cellular 5G CAPEX. (source: [ABI20])

The increase in the share of private network market is affected by several reasons. First, a growing number of companies are trying to connect a variety of devices (4K/8K CCTV, AR/VR devices, AVG), which have different communication connection requirements, to the private 5G network and control it using edge clouds. Features of 5G technology play a part in this. For example, there are eMBB, URLLC, mMTC, Network Slicing, MEC, Virtualization and Cloud Native. In addition, appearance and diffusion of local 5G frequency is also affecting. For another reason, the use of Open technology is reducing the cost of 5G equipment. In addition, 5G RAN and core can be deployed hardware through virtualization and software. This make 5G RAN and core deployable through servers and software. Lastly, companies have increased their desire to build and operate own networks themselves by NPN. If they build their own network, they enable the speed control of uplink/downlink in private 5G network regardless of mobile network provider, and also, enable the company to define their own security policies. At this time, there are limitations to the Ethernet and WLAN technologies currently used in private network. Wired Ethernet is expensive to build wiring, WLAN technology has the disadvantages of unstable communication and security.

Companies focus on three key areas of network management: "coverage and control," "performance and reliability," and "operational flexibility and integration." These three have different needs depending on the characteristics of the companies. Private network allows companies to customize their networks to suit their own characteristics. For example, in environments such as remote surgery, a very small URLLC environment needs to be met, but it may not be necessary to have a wide coverage. In other industries, eMBB functions can be used primarily to use vast amounts of video data.

6 Conclusions

In this deliverable, we investigated the regulatory and economic aspects of the PriMO-5G use cases. We focused on the two main features of the use cases. When it comes to the use of UAVs, we discussed the current regulation on drones, a novel scheme for low-latency spectrum access, and coexistence of drone and other services. With regard to the public safety communications, we addressed spectrum demand estimation for mission critical services, spectrum availability for public safety communications, feasibility of mission critical services in commercial mobile networks, and NPNs.

Considering data-centric mission critical applications enabled by LTE, 5G, and ongoing 3GPP evolution, we performed a spectrum demand estimation. The results suggest that the estimated amount of required spectrum far exceeds the currently allocated spectrum dedicated for public safety. Therefore, more safety agencies are now considering prioritized access to mobile network operator (MNO) spectrum for providing advanced mission critical services. Licensed spectrum is strongly recommended for mission critical communications.

The challenges of establishing the next generation public safety communications are not only to satisfy per performance requirements but also to achieve economic viability. An important question is who will establish and operate the public safety communications system. Some countries, such as Norway, the UK, and the USA, have decided to utilize the commercial mobile networks for the mission critical services. Various models under this category exist, and the selection of a model depends on cost estimation and performance requirements specific to each country. The PriMO-5G project has been working on technical enablers and architecture components that can contribute to mission critical services. Particularly, the network slicing and moving base station have potential to lower the cost of public safety communication networks, and thus they should be considered in the cost calculation. The moving base stations can be coupled with the equipment of public safety professionals, e.g., fire brigade, and thus it necessitates a new model for network establishment and operation. NPN can be an element of such a model. The market for NPN is expected to grow steadily, making it an industry that surpasses the current public cellular market.

Currently, license-exempt spectrum is typically used for the control of UAVs in LOS situations because Wi-Fi standards or similar protocols have been the first protocols of implementation from the UAV control vendors. Each country has own regulations for maximum transmission power in the license-exempt band, which is a primary factor in determining the flying distance of UAVs. If a UAV is in the urban area and the transmission power of the control signal is restricted to low power, the control signal may experience harsh interferences, which makes a control of the UAV flight difficult. In this case, using cellular networks such as 4G and 5G will be an effective solution for reliable control of UAVs. 3GPP networks can provide reliable and trustworthy communication for control of UAVs in BVLOS situations.

As for the communications among UAVs in the context of mission critical services, low-latency access is one of the key requirements. 3GPP has standardized solutions for the low-latency access, and thus licensed spectrum provides better control of QoS for mission critical services. License-exempt spectrum for mission critical communications has been technically down-prioritized because the listen-before-talk and back-off mechanisms employed by Wi-Fi standards incur latency and poor service quality particularly in the congested traffic situation. Therefore, there are research opportunities to exploit whether a new medium access control (MAC) mechanism in the license-exempt spectrum has feasibility to achieve low-latency access. Non-orthogonal random access which utilizes a non-orthogonal signal decomposition technique is a promising direction.

If UAVs are served by terrestrial cellular networks, coexistence with other types of users is one of major concerns. From the perspective of adjacent channel interference, introducing UAVs in a frequency band does not affect the performance of ground users or UAVs in an adjacent channel. However, satellite-based services, e.g., complementary ground component, is influenced considerably in the uplink when UAVs are flying above their base stations.

References

[3GPP-22179] 3GPP Technical Specification 22.179, Mission Critical Push to Talk (MCPTT); Stage 1, Release 13.

[3GPP-22261] 3GPP Technical Specification 22.261, Service requirements for the 5G system, Release 15, 2016.

[3GPP-22281] 3GPP Technical Specification 22.281, Mission Critical (MC) video, Release 14, 2016.

[3GPP-22282] 3GPP Technical Specification 22.282, Mission Critical (MC) data, Release 14, 2016.

[3GPP-23501] 3GPP Technical Specification 23.501, System architecture for the 5G System (5GS), Release 15, 2016.

[3GPP-23700] 3GPP Technical Report 23.700-07, Study on enhanced support of Non-Public Networks (NPN), Release 17, 2019.

[3GPP-36777] 3GPP Technical Report 36.777, Enhanced LTE support for aerial vehicles, Release 15, 2017.

[3GPP-38901] 3GPP Technical Report 38.901, Study on Channel Model for Frequencies from 0.5 to 100 GHz, Release 14, 2017.

[5GA20] 5G Americas, 5G Technologies in Private Networks, 5G Americas white paper, October 2020, https://www.5gamericas.org/wp-content/uploads/2020/10/InDesign-5G-Technologies-for-Private-Networks-WP.pdf

[ABI20] ABI Research, 5G And Private Networks: The Key for Enterprise Business Continuity, July 2020, https://go.abiresearch.com/lp-5g-and-private-networks-enterprise-business-continuity

[ATT18] AT&T, FirstNet Momentum: Band 14 Added to More Than 2,500 Sites Across the Country, First FirstNet Dedicated Deployable Assets Available, available at https://about.att.com/story/firstnet_increases_network_coverage_as_band_14_is_added.html

[BRE20] D. Brener, Global update on spectrum for 4G and 5G, Qualcomm Presentation, June 2020, https://www.qualcomm.com/media/documents/files/5g-spectrum-update-for-mipi-alliance.pdf

[DSB18] Norwegian Directorate for Civil Protection, Alternatives for mission-critical services in public mobile networks in Norway, 2018, https://www.nodnett.no/globalassets/ngn/20180503-conceptual-models-for-ngn-v1.0.pdf

[ECC15] ECC, ECC Decision (15)01 Harmonised technical conditions for mobile/fixed communications networks (MFCN) in the band 694-790 MHz including a paired frequency arrangement, March 2015, https://docdb.cept.org/download/837045c3-e8c4/ECCDEC1501.PDF

[ECC16] ECC, ECC Decision (16)02 Harmonised technical conditions and frequency bands for the implementation of Broadband Public Protection and, Approved June 2016, Amended March 2019, https://docdb.cept.org/download/1cadc836-23e4/ECCDEC1602.pdf

[ERI19] Ericsson, Critical capabilities for private 5G networks, Ericsson White Paper, December 2019, https://www.ericsson.com/4af9b6/assets/local/reports-papers/white-papers/criticalcapabilities5g.pdf

[ERC20] ERC, ERC recommendations (70-03): Relating to the use of Short Range Devices (SRD), October 2020, https://docdb.cept.org/download/25c41779-cd6e/Rec7003e.pdf

[FAN+16] R. Favraud, A. Apostolaras, N. Nikaein and T. Korakis, "Toward moving public safety networks," IEEE Communications Magazine, vol. 54, no. 3, pp. 14-20, March 2016, doi: 10.1109/MCOM.2016.7432142.

[FCC20-1] FCC, Federal Regulations, Title 47: Telecommunication, PART 15—RADIO FREQUENCY DEVICES, November 2020, https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/rules-regulations-title-47

[FCC20-2] FCC, Federal Regulations, Title 47: Telecommunication, PART 18—INDUSTRIAL, SCIENTIFIC, AND MEDICAL EQUIPMENT, November 2020, https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/rules-regulations-title-47

[FHB14] S. Forge, R. Horvitz, and C. Blackman, Is Commercial Cellular Suitable for Mission Critical Broadband?, A study prepared for the European Commission DG Communications Networks, 2014. doi: 10.2759/54788

[GSMA20] GSMA White Paper, An Introduction to Network Slicing, Jan. 2020, https://www.gsma.com/futurenetworks/resources/an-introduction-to-network-slicing-2/

[HTC+09] J. He, Z. Tang, H. Chen and Q. Zhang, "An accurate and scalable analytical model for IEEE 802.15.4 slotted CSMA/CA networks," in IEEE Transactions on Wireless Communications, vol. 8, no. 1, pp. 440-448, Jan. 2009, doi: 10.1109/T-WC.2009.080277.

[HUA20] Huawei, 5G Spectrum: Public Policy Position, Huawei White Paper, February 2020, https://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_position_5g_spectrum.pdf

[ITU-15] ITU, Recommendation M.2083-0, IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Approved, September 2015.

[ITU17] ITU, Report ITU-R M.2377-1, Radiocommunication objectives and requirements for Public Protection and Disaster Relief, Approved, November 2017.

[ITU18] ITU, Recommendation M.2015-2 Frequency arrangements for public protection and disaster relief radiocommunication systems in accordance with Resolution 646 (Rev.WRC-15), Approved January 2018,

[KL18] A. Kvalbein and H. W. Lie, Critical communications for public protection and disaster relief, Analysis Mason White Paper, 2018.

[LK18] H. W. Lie and A. Kvalbein, Four different models for next-generation emergency networks using commercial mobile technologies, Analysis Mason White Paper, 2018, https://www.analysysmason.com/about-us/news/newsletter/next-generation-emergency-networks-jul18/

[LLS20] W. -H. Lee, J. -H. Lee and K. W. Sung, "Geometric Sequence Decomposition with k-simplexes Transform," IEEE Transactions on Communications, 2020. doi: 10.1109/TCOMM.2020.3028876.

[NEC20] NEC White Paper, The case for dedicated public safety networks, 2020, https://www.nec.com/en/global/solutions/pdf/the_case_for_dedicated_public_safety_networks.pdf

[ON20] A. Othman and N. A. Nayan, "Public Safety Mobile Broadband System: From Shared Network to Logically Dedicated Approach Leveraging 5G Network Slicing," IEEE Systems Journal, doi: 10.1109/JSYST.2020.3002247.

[PRI19-D11] PriMO-5G Deliverable D1.1, PriMO-5G use case scenarios, February 2019, https://primo-5g.eu/download/357/

[PRI19-D12] PriMO-5G Deliverable D1.2, End-to-end PriMO-5G network architecture, June 2020, https://primo-5g.eu/download/609/

[SDB+20] J. San-Miguel-Ayanz, et al., Forest Fires in Europe, Middle East and North Africa 2019, EUR 30402 EN, Publications Office of the European Union, Luxembourg, 2020.

[SMJ+19] K. W. Sung, et al., PriMO-5G: making firefighting smarter with immersive videos through 5G, in proc. IEEE 2nd 5G World Forum (5GWF), 2019.

[AUG20] http://www.auggmed-project.eu/

[CPRI13] Common Public Radio Interface (CPRI); Interface Specification v6.0, available at http://www.cpri.info/downloads/CPRI_v_6_0_2013-08-30.pdf