[Year]

Communications and Networking for Public Safety

Communications and Networking Technology for Public Safety
An IEEE Public Safety Technology Initiative Report

Communications and Networking Technology for Public Safety: An IEEE Public Safety Technology Initiative Report

Table of Contents

List of Figures

INTRODUCTION

This IEEE Public Safety Technology Initiative report discusses **communication and networking technologies** that can be leveraged to **improve public safety**. The report explores various use cases and scenarios, examining their benefits, challenges, and enabling technologies.

- The **Aerial Base Stations** use case involves using aerial vehicles like drones and balloons as **rapidly deployable communication infrastructure** in disaster scenarios where terrestrial connectivity is damaged or absent. Enabling technologies include 3GPP, ETSI MEC, and IEEE standards, and potential challenges include power provisioning and adapting to different coverage needs.
- The **IoT Communications for Public Safety** use case explores how data from diverse IoT domains can enhance **situational awareness and decision-making** during emergencies. Challenges include ensuring reliable broadband access for first responders within hazardous environments and enabling secure access to external IoT domains. 5G networks, deployable nodes, and satellite systems are key enabling technologies.
- The **RIS-aided UAV Communications for Public Safety** use case proposes using **reconfigurable intelligent surfaces (RIS) and unmanned aerial vehicles (UAVs)** to enhance communication reliability and security in public safety scenarios. Potential challenges include optimizing RIS and UAV placement, trajectory design, and resource allocation, especially considering UAV payload and energy limitations.
- The **5G O-RAN and Prioritization of Public Safety Traffic** use case discusses **prioritizing public safety traffic in 5G networks using O-RAN specifications**. Key challenges include verifying the effectiveness of prioritization rules and ensuring sufficient radio resources for public safety during network congestion.
- The **Trust and Physical Layer Security for 6G Cyber-Physical Systems** use case emphasizes the need for **adaptive, AI-enabled security solutions** in 6G networks to address challenges like low latency requirements, quantum resistance, and adversarial AI. The emergence of sensing and high-precision localization in 6G also raises privacy concerns.
- The **Energy-efficient Indoor Communications for Public Safety** use case proposes using **RF backscatter communication and visible light communication** to improve energy efficiency and reliability for wearable devices used by first responders in indoor environments. Challenges include signal penetration, attenuation, and interference.

The report also discusses **standardization efforts and provides conclusions and recommendations** for advancing communication and networking technologies for public safety. The document emphasizes the importance of collaboration between industry, academia, and government to address the challenges and realize the potential of these technologies to enhance public safety and emergency response.

WHITE PAPER

1. Aerial Base Stations

Major disasters are typically followed by power and communications infrastructure failures making it difficult for first responders and volunteers to reach and deliver care to the victims who require immediate assistance [1] [2]. The success of disaster relief operations depends on the efficiency of the coordination efforts, which, in turn, depend on how well information is acquired and shared among all stakeholders including first responders and decision-makers involved in the relief operations. Typically, numerous organizations engage in disaster relief operations. Emergency scenarios exemplify the complex processes (communications, coordination, information acquisition and sharing, and decision-making) that take place on the ground. Disaster relief operations require effective coordination among the first responders and decision-makers so that resources can be allocated quickly and optimally [3] [4]. Current technologies and tools used by the emergency management personnel are not capable of meeting the desired levels of performance set by the Department of Homeland Security (DHS) [5]. This chapter describes the knowledge gaps by presenting the processes that take place during disaster relief operations. It outlines how these processes can be streamlined and improved through the support of advanced emergency communication solutions.

This article includes a discussion of complex interactions that take place among the individuals (first responders, and decision-makers) and organizations (government, utilities, transportation and volunteer) during disaster relief operations in order to inform technology solutions for streamlining these processes with an overall objective of improving the efficiency, effectiveness, and speed of disaster relief operations. It includes the abstraction and analysis of information flows within the human network during disaster relief operations that will ultimately lead to systems and tools for communications, information acquisition and sharing, and decision-making. The overall vision is to equip local communities with state-of-the-art tools to effectively coordinate disaster relief operations [6]. It also includes the challenges to realizing this vision in terms of fundamental and cross-disciplinary research problems and solutions [7].

1.1. Use Case Scenario

Providing a reliable communication infrastructure in presence of emergency scenarios is characterized by the following specific challenges:

- Absence or limited availability of terrestrial connectivity: several disaster situations are characterized by partial or complete destruction of the terrestrial communication facilities (e.g., mobile network base stations or Wi-Fi access points), or their isolation from the core network infrastructure;
- Absent or limited power provisioning: similar to the previous point, potential damage can introduce losses or unavailability of power provisioning through the energy grid;
- Need for adapting to different coverage scenarios: disruption of the area subject to the disaster might generate unexpected distribution of potential users, or unpredictable mobility patterns;

- Need for providing at least two levels of service: (i) reliable and low latency for emergency responders, and (ii) public connectivity for the persons in the area subject to the emergency;
- Need for interconnecting with other available networks, e.g., to enable to increase context awareness by collecting sensor information (e.g., video from public cameras, etc.).

Figure 1 illustrates a use case scenario for a rapidly deployable communication system. In this use case, the stakeholders who would benefit from a rapidly deployable system are identified.

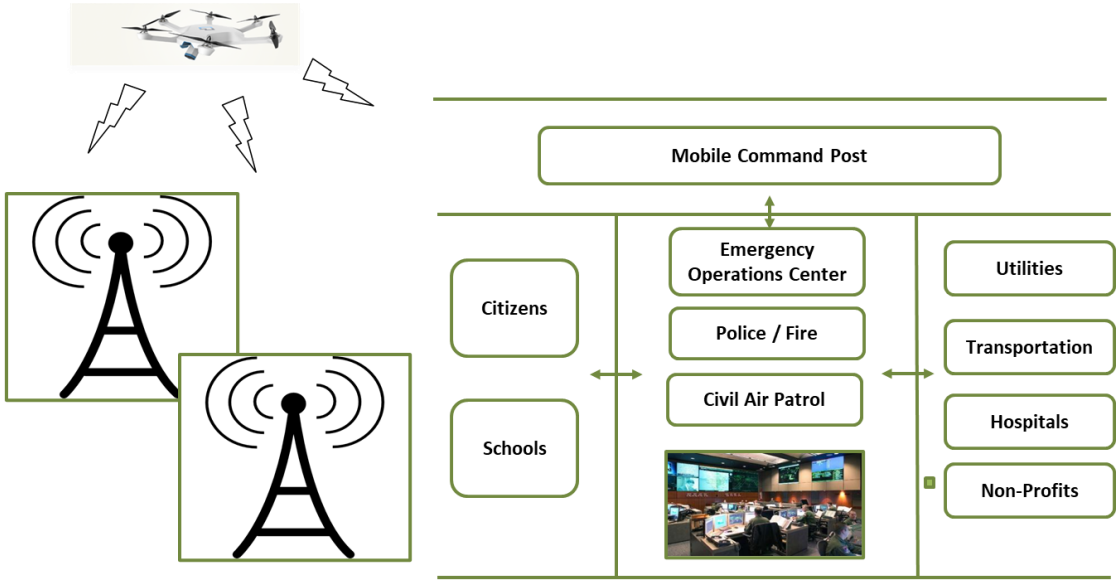

Figure 1 Rapidly deployable communication systems: A use case scenario in which emergency responders are provided with connectivity.

1.2. Preconditions and Assumptions

Deploying aerial base stations (ABS), such as drones or balloons equipped with communication technology, can be a game-changer in disaster relief operations. However, successful deployment hinges on several pre-conditions and assumptions.

One key precondition is understanding the specific communication needs in the disaster zone . This includes identifying the types of users who need access (first responders, civilians, etc.), the required coverage area, and the necessary data rates. Additionally, airspace regulations and safety protocols must be considered before deploying ABS. Obtaining necessary permissions from aviation authorities and establishing clear flight paths to avoid collisions with other aircraft are crucial . Furthermore, the availability of suitable launch sites and infrastructure for operating and maintaining the ABS is essential. This includes having trained personnel, ground control stations, and logistical support for refueling or battery replacement.

1.3. Challenges Specific to the Use Case Scenario

Deploying ABS for disaster relief presents various challenges. All of these challenges can be overcome with appropriate planning and collaborations with the local and regional stakeholders.

Regulatory hurdles: Obtaining necessary flight permissions and coordinating with aviation authorities can be complex and time-consuming, especially in emergency situations.

Logistical complexities: Setting up ground control stations, ensuring reliable power sources for sustained operation, and managing logistics for maintenance and refueling can be challenging.

Environmental factors: Severe weather, terrain obstacles, and electromagnetic interference can significantly impact ABS performance and flight stability.

Integration and interoperability: Ensuring seamless integration with existing communication infrastructure and ground-based networks can be technically challenging.

Performance limitations: Factors like limited payload capacity, battery life, and communication range can restrict the effectiveness of ABS in certain scenarios.

Security concerns: Protecting ABS from cyberattacks and ensuring data security is crucial, especially when handling sensitive information in disaster situations.

1.4. Proposed Solution

The solution to address the challenge is to provide connectivity and communication services to terrestrial users and first responders through the deployment of one or more Aerial Base Stations. Aerial Base Stations or Flying Towers are aerial vehicles that can be easily and rapidly deployed as a substitute or complement to existing communications infrastructure. Drones or balloons can be used to achieve this goal, but also High Altitude (Aerial) Platforms (HAPs). Basically, the aerial vehicles operate as substitutes for the terrestrial base stations and need to be equipped with proper computational power to implement the Radio Unit (RU) and Base Band Unit (BBU) functionalities. Moreover, in case of absence of terrestrial infrastructure, the aerial vehicles should be capable of acting as relays by exploiting the connectivity provided by satellite links. In this framework, balloons can be preferable due to the longer flight time, even if drones (or swarms of drones) have higher maneuverability.

1.5. Insights and Discussions

- **Disaster preparedness is crucial:** Organizations with well-defined disaster recovery plans and trained personnel are better equipped to handle emergencies effectively. This includes having procedures for requesting and coordinating external assistance, such as deploying ABS.
- **Collaboration is key:** Effective disaster response often involves collaboration between various agencies and organizations. This highlights the importance of interoperability between ABS and existing communication infrastructure to ensure seamless information sharing.

- **Learning from past events:** Analyzing past disaster responses and incorporating lessons learned is essential for improving future preparedness. This includes evaluating the effectiveness of different technologies and strategies, such as ABS deployment, in various disaster scenarios.
- **Addressing specific needs:** Disaster recovery efforts should consider the unique needs of affected communities and prioritize equitable access to resources. This includes ensuring that ABS deployment strategies address the communication needs of diverse user groups.

Figure 2 Deploying a standalone aerial base station.

1.6. Enabling Technologies

Existing Technologies

- 3GPP Rel. 17 and beyond provide a wealth of information on non-terrestrial networking solutions.

New Technologies/Standards

Current standardization efforts include:

- ANSI Standards Roadmap for Drones
- ANSI Unmanned Aircraft Systems Standardization Collaborative (UASSC): https://www.ansi.org/standards_activities/standards_boards_panels/uassc/overview

- ASTM Standard Specification for Remote ID and Tracking: https://www.astm.org/Standards/F3411.htm
- IEEE P1920.1 and IEEE P1920.2 Standards working Groups (Jointly sponsored by IEEE ComSoc and VTS):
    - P1920.1 – Aerial Communications and Networking Standards: https://standards.ieee.org/project/1920_1.html
    - P1920.2 – Standard for Vehicle to Vehicle Communications for Unmanned Aircraft Systems: https://standards.ieee.org/project/1920_2.html
    - P1954 – Standard for Self-Organizing Spectrum-Agile Unmanned Aerial Vehicles Communications.
- 3GPP UAV activities: https://www.3gpp.org/uas-uav
- 3GPP non-terrestrial initiative: https://www.3gpp.org/news-events/1933-sat_ntn
- GSMA and GUTMA joint initiative to help define the future of Aerial connectivity: https://www.gsma.com/iot/news/gutma-and-the-gsma-announce-collaboration-to-help-define-the-future-of-aerial-connectivity/

1.7. Conclusions

It's important to note that the specific challenges and lessons learned from ABS deployments can vary depending on the type of disaster, the environment, and the technology used. Further research and case studies are needed to gain a more comprehensive understanding of the effectiveness of ABS in different disaster situations.

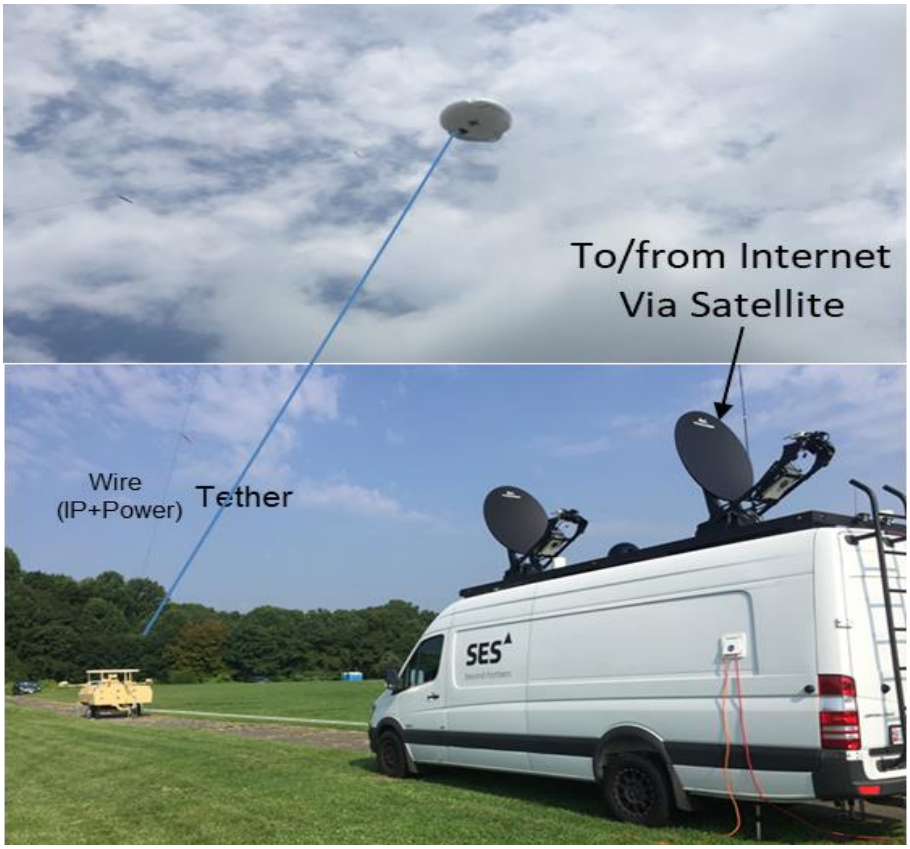

Figure 3 Internet connectivity provided through satellite connectivity.

2. IoT Communications for Public Safety

The Internet of Things (IoT) is expected to foster significant developments of new capabilities for public safety by enhancing data-driven situational awareness, thus improving the ability to mitigate, respond and recover from natural and human-caused incidents. It is expected that public safety will draw on many sources of data in order to develop a meaningful situational portrait to assist in life-critical decision-making. The data will likely be from disparate sources pertaining to different administrative domains and operators. Thus, public safety must be able to accommodate different data formats and ontologies and join the data into a common operating picture.

2.1. Use Case Scenario

A use case that describes one of many ways that IoT can be used to support public safety is the case of a structure fire that presents hazardous conditions for first responders and civilians. Data would be collected from different domains in order to launch the mission and to monitor progress as it unfolds. Various sensors in the structure provide information on the temperatures, state of containment of hazardous materials, and stress exerted on conduits and other physical infrastructure. As well, the structure contains flow control devices, door locks and other devices that can be actuated from a local operations center or remotely. Environmental sensors can detect the presence of hazardous materials in the air and in the municipal drainage system. Traffic and emergency signage can be remotely controlled to prioritize the routing of emergency vehicles and limit access to civilians in neighboring areas if the possibility of a hazardous gas leak is a concern. Valves in the drainage system can prevent hazardous materials from propagating in the sewer system. The public safety agency uses sensors to monitor the safety of the firefighters, such as their vital signs, air pressure in their Self-Contained Breathing Apparatus (SCBA), and their locations. Heads-up display capability in the face masks of the firefighters can guide them to the possible locations of persons trapped in the structure using augmented reality (AR). Artificial intelligence can help the incident commander decide on the best route that accounts for the hazards and other information that is collected by the various sensors. The figure below illustrates the multiple IoT domains that are implicated in the use case with emphasis on the transformation of disparate data into actionable intelligence.

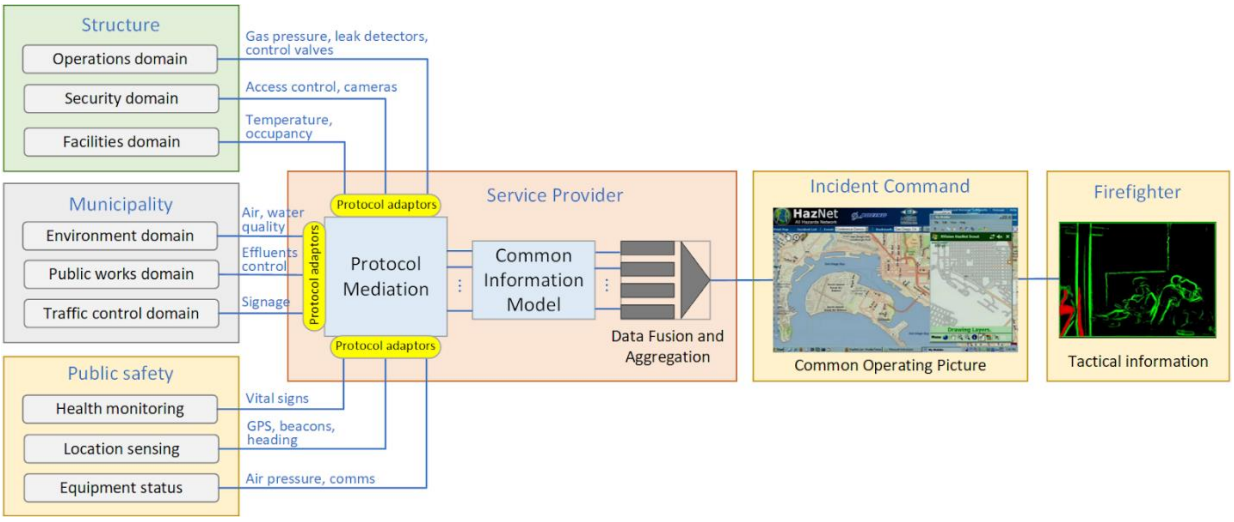

Figure 4 Example of public safety system architecture.

2.2. Preconditions and Assumptions

- Public safety agencies are authorized to access the sensors and actuators in the other domains during emergencies.
- A public safety agency can deploy a temporary base station to improve the communications reliability for firefighters inside structures.
- A 5G mobile broadband network serves the area where the event is located.
- The public safety agencies and the serving mobile broadband network operator can coordinate the use of deployable base stations by a public safety agency during emergencies.
- Protocol mediation, data fusion and aggregation is provided as a service to public safety agencies and the operators of the IoT domains.
- The firefighters are equipped with facemasks that can project images as a heads-up display from data that they receive over a wireless broadband network.

2.3. Challenges

The challenges that are encountered in this use case span several planes. At the most fundamental level, it is necessary for the firefighters to be able to connect to wireless broadband services while they are in the structure. It is not uncommon for power to be intentionally shut off during a structure fire to prevent a potential electrical hazard for firefighters. Furthermore, communications networks such as Distributed Antenna Systems, small cells or WLAN inside the structure may suffer damage from the fire or from the actions of the firefighters in trying to suppress the fire. The AR applications are intended to allow firefighters to navigate within a darkened or smoke-obstructed environment. If the structure is at the edge of a mobile broadband cell or the structure is composed of highly absorptive or reflective materials at radio frequencies, then the signal level inside the structure may be attenuated to the point of not being useful for public safety.

Another important challenge is for public safety to be able to access the various IoT domains that are outside their own. Normally, access to sensors and actuators for any specific domain is restricted to authorized personnel only. During an emergency, access to those IoT objects that are appropriate for establishing situational awareness should be granted to public safety. Assuming such access privileges can be securely granted, public safety must be able to communicate with the IoT objects or their gateways. There are several industry standards for the data formats and protocols for IoT systems and it is a significant challenge for public safety to be able to accommodate the myriad standards. It would be infeasible for mobile command centers to have monitoring stations for each and every possible IoT domain. Furthermore, situational awareness is best achieved by merging all relevant information into a common operating picture. Even if all the IoT domains can be accessed by public safety, another challenge is to remain up to date with the changes that the operators of the IoT systems would inevitably undertake during the operational life of their IoT systems. This may be less of a technical challenge than an administrative challenge. But nevertheless, it presents an important operational barrier.

It is imperative that public safety trust the information that it uses to inform its mission plans and actions. In the case where information is sourced from outside its security domain, public safety must be able to ascertain its trustworthiness. The challenge for public safety is to be able to know whether an IoT object can accurately sense its environment (e.g., functioning, calibrated to a

traceable source), that it is cyber-protected (e.g., can detect physical tampering, updated to latest security patch, type of encryption, can detect and repudiate attempts to alter its data), and that it is a legitimate IoT object and not an imposter, among other trust attributes.

2.4. Proposed Solutions

Generally, firefighters do not know a priori if the structure they will enter is adequately served with broadband communications. As described in the scenario of this use case, the indoor communications infrastructure may be inoperable. Therefore, for greater confidence, firefighters should bring temporary infrastructure with them. Deployable base stations can be set up in the vicinity of the event and they must be operational within a very short time after they arrive on-scene. Such systems must not interfere with, or be interfered by, the macro cellular network. In addition, the firefighters' communications devices must be able to act as relays to minimize the possibility of having isolated firefighters. The latency and data rate of the communications service inside the structure must be adequate to support the applications that the firefighters will use, especially real-time AR. 5G is specified to support high data rates and have very low latency. It can also be used to backhaul the deployable node to cloud-based servers where data processing and rendering is performed. Backhaul can also be provided via emerging non-terrestrial networks such as a low earth orbiting (LEO) platforms or aerostats as long as the bandwidth and latency can satisfy the performance requirements for the applications.

In order for public safety to access IoT objects that are outside their operational domains the owners of those domains must allow it. There should be a pre-established agreement that will stipulate when and how such access will be permitted and by whom. The agreement would also require the domain owners to provide public safety with a level of assurance concerning the degree of trustworthiness of the data that it provides. In effect, the agreement would signify mutual trust between the parties prior to an event. Having one-to-one agreements between many parties is unwieldy and costly to administer and maintain. A third-party trust service provider could manage the agreements between all the parties and standardize the attributes that each party should adhere to in order to participate in a trusted community. In this way, even parties that are unknown to each other can be part of the trusted community.

The usual flow of information between public safety and external IoT domains would be through the application servers and the broadband network connecting public safety responders. However, there is a direct path that can be considered between the IoT object itself and the responder's device. For example, both the IoT object and the device may be able to connect via Bluetooth. However, they would both need to authenticate each other. Pre-shared keys could be used to establish the connection. The responder's device could present recognizable credentials to the IoT object, and the object could present its security state to the responder's device that could be assured via a distributed ledger system. However, in order for the communication to proceed, other layers in the communications stack must be implemented at both ends.

To use data from disparate sources in a common operating picture requires that all the streams of data be merged such that the aggregated information may be presented in a meaningful and actionable way. For example, the location of firefighters, location of hot spots, and the potential locations of trapped persons should be shown onto a representation of the structure's blueprints. Data fusion combines data from multiple sensors and related information from associated databases to achieve improved accuracy and more specific inferences than could be achieved by

the use of a single sensor alone. All the information is collected from different sources and are presented in a common operating picture. A possible approach to achieving this is to mediate the protocols and ontological meanings of every independent data stream into a common information model (CIM), which describes a collection of related objects in terms of classes, attributes and relationships and provides unique names and definitions to each object.

2.5. Enabling Technologies

A 5G non-private network (NPN) can serve as a deployable node under the administrative authority of a public safety agency. It can contain a local data network that would host incident-specific applications such as an AR rendering of the environment. However, the data from the sensors and the protocol adaptation would likely be remotely hosted relative the NPN node. Therefore, the NPN node would need a backhaul connection to the application servers that mediate the IoT protocols and aggregate the data. The backhaul can be provided by a mobile broadband network where the NPN node would be a stand-alone NPN (SNPN) access network to a macro 5G network via the latter's N3 Interworking Function (N3IWF) [8]. Starlink or other LEO communications system can provide local access to the Internet for backhaul, but there would need to be some QoS assurances. LEO backhaul would impart moderate latency and may not be suitable for real-time AR applications.

Interference between the macro network and the NPN would need to be avoided. Assuming a backhaul connection between them exists, then the two networks can coordinate the assignment of radio resources via the Xn reference point. Dynamic spectrum management (DSM) techniques such as context-aware DSM and cognitive-radio based DSM are intended to avoid interference. Successive interference cancellation is a technique that can be used to suppress interference.

A responder can access an IoT object either through the cloud or directly in device-to-device connection. In the former case, the responder's device would connect to the IoT server by virtue of its data plane being routed to the 5G Data Network Name (DNN) that is associated with the IoT server. Access controls would be needed to protect the IoT object and its data. Direct device-to-device connection can be established using Bluetooth and Secure Simple Pairing to establish the link with a pre-shared key. The Bluetooth standard specifies the link layer. The Internet, transport and application layers also need to be implemented at both ends of a communications link.

Data interoperability is a key pre-requisite in being able to analyze and extract the value within heterogeneous data sets. Protocol mediation consists of adapting the different data protocols into a CIM. Several industry associations promote their standards for a CIM. DMTF, formerly known as the Distributed Management Task Force, is a standards organization that creates standards related to the interoperability of management information across disparate technologies. Its Web-Based Enterprise Management (WBEM) specifications define how resources are modeled using the DMTF CIM, such that they can be discovered, accessed and processed. The OASIS Data Exchange (DEX) specification is intended to standardize the information models that are specific to particular business processes. The DEX specification is a subset of the ISO 10303-239 Product Life Cycle Support (PLCS) information model. It provides guidance for how to use and combine entities and data in the exchange between systems. oneM2M is a standards development organization whose goal is to develop technical specifications for a common machine-to-machine (M2M) service layer for the exchange and sharing of data among applications, which can be readily embedded within various hardware and software and can be relied upon to connect myriad IoT

devices with M2M application servers. It proposes a CIM referred to as the 'Home Domain Abstract Information Model'. The Connectivity Standards Alliance produced a standard for an IoT data protocol, referred to as Matter, which is oriented towards residential IoT devices, such as door locks, light switches, garage door openers, and thermostats, among many other uses.

A COP is produced by combining the different data streams into a single composite view, although the view can consist of different layers. A prerequisite is that the datasets adhere to a common information model and common semantics. The World Wide Web Consortium (W3C) has defined two key standards that underpin semantic interoperability – Web Ontology Language (OWL) and Resource Description Framework (RDF). RDF provides a data-modelling vocabulary. OWL is a semantic Web language that represents rich and complex knowledge about things, groups of things and relations between things. The Open Geospatial Consortium (OGC) refers to the W3C standards to base its recommendations for semantic sensor network ontology to describe sensors and the data that is collected, the procedures involved in sensing, the features of interest in the data set, the samples used in the data set, and the observed properties of the data. The ontology also applies to actuators. A standardized ontology allows data from various sources to be integrated in higher level processes and facilitates the interpretation of the data. The oneM2M base ontology leverages OWL and is intended to provide semantic interoperability between oneM2M systems and external systems.

There is no one industry standard specification for data fusion, as the field encompasses a variety of techniques and approaches that are used in different contexts and industries. But some organizations have defined data fusion models that can have general applicability. For example, the U.S. Joint Directors of Laboratories (JDL) developed a data fusion model [9] for military applications. Other applications can use the JDL model by suitably defining measurement systems, resource planning procedures, hypotheses, tasks, reports and other parameters of the model.

Trustworthiness is an essential attribute in determining whether an IoT object or a public safety user can be a useful actor in this use case. Trust service providers fulfill an important role in determining the trustworthiness of an actor. A trust service provider operates a trust framework that provides a common set of agreed upon standards (i.e., trust marks) for disparate entities such that any entity can determine the degree of trustworthiness of any other entity. To support this use case, the public safety agency and the owners of the IoT objects could subscribe to a trust service provider that has established a trust framework with trust marks that apply to public safety and trust marks that apply to IoT objects. The trust service provider quantities the level of trustworthiness but every party decides what is an acceptable level of trustworthiness to allow access to the requesting party.

2.6. Insights and Discussions

The technologies that that are involved in enabling the capabilities that are described in this use case span numerous disciplines. Connecting the responders with the IoT objects is the most fundamental technical prerequisite. Of the approaches that are posited in the previous section, the direct device-to-device connection requires the implementation of TCP/IP layers that must be continually coordinated and managed across multiple agencies and IoT domains. This approach is administratively burdensome and presents an increasing risk of incompatibility over time. Using deployable nodes to augment capacity and/or coverage when needed has been adopted by some public safety agencies (e.g., U.S. FirstNet, New South Wales - Public Safety Network, Germany -

Federal Agency for Public Safety Digital Radio) and is supported by the vendor community with a variety of offerings. LEO communications satellites offer the possibility to backhaul traffic from an incident area with moderate latency and bandwidth. This approach would likely be coupled with edge/fog computing. The cloud processing would be performed for latency-tolerant applications such as a COP, but processing the data needed for an AR application would be performed locally.

Granting public safety access to IoT objects that are outside its administrative domain and under what circumstances is the purview of the operators of the IoT domains. Each IoT gateway could be configured with a secure port that is assigned to public safety. Access privileges would be enabled or disabled according to the terms of presumed agreements between the operators of the IoT domains and public safety agencies. The agreements could be managed by a third-party trust service provider within the context of a trust framework that is designed for this purpose. There are numerous applications of trust frameworks in health care, finance, governments and other industries. However, a trust framework that is tailored to the needs of public safety is not known to have been commercialized, apart from pilot initiatives. One such initiative is the Trustmark Framework that is sponsored by the U.S. Department of Homeland Security and led by the Georgia Tech Applied Research Center [10]. Yet, while this initiative is intended for public safety, it has not defined a Trustmark that can apply to IoT objects. There are some IoT Trustmark initiatives that can potentially be adapted for use in a public safety IoT trust framework. For example, the IoT Security Trust Mark™ framework sets out the principles and basis for third-party conformity assessment to cyber security requirements for IoT devices.

There are several CIMs that are backed by influential standards organizations. As such, there is no lacking for a standard that can serve as the basis to implement a CIM for this use case. However, only one CIM should be used in the ecosystem to avoid having to support and adapt the data protocols to multiple CIMs. As with any solution that integrates multiple technologies and spans multiple domains, it will be necessary to maintain and manage the on-going changes that are made by every party over the lifetime of the solution. Part of the burden of managing an integrated CIM solution can be alleviated by using a standardized data protocol for industrial IoT.

Fusing data from multiple sensors would improve the situational awareness of the incident by using multiple inputs to generate a more reliable result. As there is no known standard for this function, an implementation of a data fusion engine would likely be either a point solution developed by a systems integrator specifically for this purpose, or a hosted solution by a value-added provider of such services. There is no such entity that is known to offer this service.

2.7. Conclusions

Data will provide an unparalleled enhancement in situational awareness for public safety that will translate into more effective strategies and tactics to mitigate, respond and recover from events, as will the ability for public safety to remotely initiate certain actions via controllable actuators. In order for the benefits to be realized many pre-requisites must be satisfied. Among them is the ability to communicate with the sensors and actuators. The Internet of Things has networked the sensors and objects via a communications standard that can be integrated with other communications technologies. 5G cellular networks, WLAN, deployable communication systems, and satellite systems all have a role in connecting public safety with IoT objects. By understanding

their capabilities and limitations these technologies can be applied thoughtfully since no one technology can satisfy the needs of public safety all the time.

It is expected that data will be sourced from different types of sensors and from different operator domains. The various streams of data would need to be aggregated into a format that can provide a common operating picture to the incident command team and that can be rendered useful for responders. As such, the different formats of data would be adapted into a common information model. Several influential standards organizations such as OASIS, oneM2M and W3C have each proposed their own model. Some organizations such as the Connectivity Standards Alliance have proposed standardizing the sensor data format itself, which would alleviate the effort to manage the CIM. Fusing data from multiple sources would improve the accuracy of the information that is derived from various sensors. However, there is no standardized data fusion model that can be applied to public safety, but the JDL model that was developed for military applications may be a candidate model that could be adapted for public safety.

Cyber-security is an important consideration in most disciplines and especially in public safety. It is necessary for public safety to be able to trust the information that it relies on. As public safety becomes more dependent on sensor-derived data, it is imperative that the information is trustworthy, which includes trusting the sensor itself. An emerging actor in the IoT communications ecosystem is the trust service provider. Although some trust frameworks are in commercial use for IoT such as the IoT Security Trust Mark™ and one is under development for public safety interoperability by DHS and Georgia Tech Applied Research Center, none are directly applicable to ensuring mutual trust between IoT objects and public safety users.

3. RIS-aided UAV Communications for Public Safety

The integration of reconfigurable intelligent surfaces (RIS) with unmanned aerial vehicles (UAVs) has been proposed as a promising solution for enhancing communication reliability, improving security, and extending coverage in future wireless networks. RIS is a cutting-edge technology that consists of artificially engineered meta-atoms with various functionalities, such as beam shaping, signal splitting, reflection, absorption, and polarization. This opens up new opportunities for integrating RIS into UAV networks, where UAVs equipped with RIS can move freely in 3D space to manipulate signals, while UAV users can benefit from available RIS in their environment to communicate securely and efficiently. This integration is seen as a crucial enabler for critical public safety services, as it provides highly resilient, reliable, secure, and low-latency communications.

Specifically, several practical public safety use cases can be envisioned with the interplay of RIS and UAV technologies.

3.1. Use Case Scenarios

3.1.1. RIS-assisted UAV for Public Safety Networks

Assisting UAVs with RIS may lead to several benefits including extended coverage, higher capacity, and flexible spectrum sharing for public safety services. For instance, by using multiple RIS components along the travelling path between a base station (BS) and a controlled UAV, the operational range of the UAV can be significantly expanded, leading to more prompt and effective responses to emergencies in the targeted area. In such as case, the UAV can be used to relay emergency calls, video streaming for situation assessment, surveillance, etc., in a multi-hop fashion between RISs.

Figure 5 RIS-assisted UAV communication for surveillance (A surveillance UAV is connected in a multi-hop fashion to its serving BVLoS BS, through RISs).

3.1.2. RIS-equipped UAV for Public Safety Networks

Another potential use case is to mount RIS on a UAV, called RIS-UAV. By doing so, the flying RIS-UAV can be flexibly positioned to forward signals between a cellular base station and first responders within an occluded or under-covered area. The use of RIS on the UAV allows the latter to relay signals at a lower energy consumption level and low payload than using energy-greedy active transceiver components.

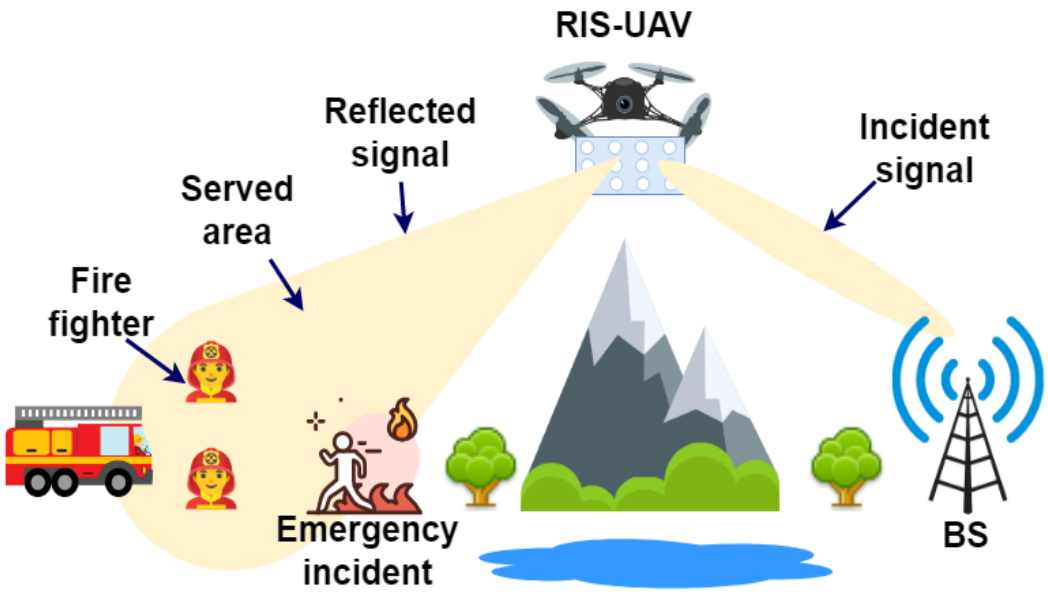

Figure 6 RIS-UAV assisted communication for search and rescue (A RIS-UAV reflects communication signals between a BS and fire fighters in a non-served area).

3.2. Preconditions and Assumptions

3.2.1. RIS-assisted UAV for Public Safety Networks

Currently, RIS development is still in its early stages, meaning that there is no large-scale deployments. Nevertheless, related system modelling has been developing very fast. The main assumptions to operate RIS-assisted UAVs are:

- Multiple RISs deployment within the environment
- Adjustment of the sizes, locations, orientation, and operation mode (active or passive) of RISs
- Prior full or partial knowledge of the base station, RIS, and UAV locations and channel state information (CSI) conditions

3.2.2. RIS-equipped UAV for Public Safety Networks

Mounting an RIS on a UAV is not straightforward and would require a careful analysis about how the mounting can be achieved. Current assumptions include:

- Adjustment of the size and operation mode of the RIS conditioned on the UAV's payload
- RIS is typically installed at the bottom of the UAV
- UAVs either hover or fly in a continuous path
- UAVs may be equipped with an antenna to ensure their own remote control through visual line-of-sight (VLoS) or beyond visual line-of-sight (BVLoS)

3.3. Challenges

There are several challenges than need to be addressed either for the RIS to assist the UAV's communications or to mount it on a UAV.

3.3.1. RIS-assisted UAV for Public Safety Networks

Due to the UAV's mobility and given the number of RISs involved several challenges may be raised:

- How many, how large, and where to place the RISs in order to improve communication quality to the supported UAVs?
- Which trajectories UAVs should follow to improve the quality of the RIS-assisted communication?
- How to configure the BSs and RISs to support the UAV's mobility?
- How to configure the RISs to guarantee secure communication to/from the UAVs?

3.3.2. RIS-equipped UAV for Public Safety Networks

Similarly, to the previous use case, the mobility of users to serve, e.g., deployed first responders, may have an impact on the communication's quality. Moreover, the payload of the UAV is a limiting factor of the RIS's efficacy. Hence, relate3d challenges would include:

- How large an RIS can be to be mounted on a UAV?
- How to place or which trajectory the RIS-UAV should follow to guarantee service quality for deployed first responders?
- How to configure the RIS in order to improve the communication's quality?
- What is the impact of RIS characteristics (size, operating frequency, etc.) on the UAV's payload, loitering time, and power consumption?

3.4. Proposed Solutions

3.4.1. RIS-assisted UAV for Public Safety Networks

Several works started investigating the aforementioned challenges. For instance, some studied the analytical model of the RIS-assisted communication system and derived outage performance and

bit error rate expressions [11]. In other [12] [13], authors investigated the joint trajectory design and RIS phase shifting to maximize data rate of ground users. An extension to user scheduling has been proposed [14]. For security purposes, authors optimized the UAV trajectory, RIS phase shifts, and legitimate users transmit powers, aiming to improve the secrecy rate, i.e., maximizing the data rate of legitimate users while reducing the one of attackers [15].

3.4.2. RIS-equipped UAV for Public Safety Networks

A link budget analysis for RIS-UAV systems has been conducted [16], which has shown the dependence of the received power at ground users on several parameters, including operating frequency, BS/user antenna gain, and RIS-UAV location. Also, authors investigated BS beamforming and RIS phase shifting to maximize the worst user received signal-to-noise ratio (SNR) [17]. From the security perspective, some [18] jointly optimized the UAV location and RIS configuration to maximize the secrecy rate, while others [19] extended the optimization to the UAV trajectory, user association and transmit power in order to maximize the secrecy energy efficiency instead.

3.5. Enabling Technologies

For RIS-enabled UAV system to operate efficiently, it is required to rely on efficient approaches and technologies.

Channel Modelling: For UAV-to-ground channel modelling, large-scale and small-scale models have been extensively discussed in the literature, for both near-field and far-field scenarios. Nevertheless, available models still lack comprehensive expressions. In particular, most of them focused primarily on characterizing large-scale and small-scale fading under unrealistic conditions. As a consequence, we need a comprehensive framework to demonstrate RIS-enabled UAV channel modelling in practical scenarios, which would involve UAV high mobility and wobbling. Wobbling is a major challenge on the design of accurate channel models, since it impacts the quality of the UAV-RIS link to ground users.

Machine Learning: To accomplish resilient public safety services using RIS-enabled UAV networks, a sophisticated level of organization is required in order to coordinate UAV paths, flying times, energy consumption, and RIS configuration. In this context, machine learning is deemed as a vital enabler. Particularly, advanced machine learning algorithms can be developed and exploited to orchestrate the operations of RIS-enabled UAVs for public safety. Such a topic is still in its infancy, thus representing a potential future research direction.

Physical Layer Security: Physical layer security (PLS) is becoming critical in highly dynamic networks, such as UAV networks. Consequently, it is mandatory to design enhanced PLS schemes for RIS-enabled UAV systems, aiming to fulfill the security requirements of public safety networks. The latter are vulnerable to several physical layer attacks, particularly jamming and spoofing attacks, resulting on serious damages, e.g., humans' death. As a consequence, novel PLS mechanisms should be introduced to guarantee reliable and secure public safety communications via RIS-enabled UAV systems.

3.6. Insights and Discussions

The integration of RIS into UAV system is presenting a tremendous potential to support public safety operations, however the performance of this novel paradigm is currently constrained by several factors. First, although a higher number of RIS reflecting elements (REs) implies batter performance and improved coverage, due to the UAV's limited size and supported payload particularly in turbulence scenarios, the size of RIS mounted on UAVs should be limited. Moreover, the relatively high mobility and wobbling effect of UAVs requires frequent CSI acquisition and, thus, continuous RIS reconfiguration is needed. Such a situation would lead to an increased overhead, which would impose new challenges on the deployment of on-demand and fast RIS-enabled UAV systems for public safety networks. In addition, joint trajectory design and resource allocation optimization represents a challenging factor in the implementation of RIS-enabled UAVs. Specifically, this joint optimization is required to ensure maximized coverage while maintaining high energy efficiency to meet the needs of public safety networks under the limitations imposed by the constrained UAV capabilities. Finally, the emergence of the space-air-ground integrated network (SAGIN) concept as a serious enabler to connect the unconnected motivates its use to realize reliable and secure public safety communications. Yet, the adoption of SAGIN with RIS introduces novel challenges, pertaining to the heterogeneity and dynamicity of SAGIN systems.

3.7. Conclusions

The integration of RIS into UAV networks to provide public safety services is presented here. We exposed two use cases, where RIS-assisted communications or RIS-equipped UAVs are needed. Such systems face several challenges to become fully operational, which will require cooperative efforts from both the scientific and industrial communities.

4. 5G O-RAN and Prioritization of Public Safety Traffic

This section discusses the methods available in the open radio access network (O-RAN) specifications for prioritizing public safety traffic in a 5G RAN. It also discusses the challenges and limitations of these methods and potential approaches to addressing them. The O-RAN specifications can be considered as an extension of 5G RAN disaggregation by 3rd generation partnership project (3GPP). The 5G RAN disaggregation involved splitting the next generation NodeB (gNB) into three components, i.e., radio unit (RU), distributed unit (DU), and centralized Unit (CU). The RAN disaggregation allowed deploying each component hierarchically in different geographical locations, scaling the components independently, and supporting a multi-vendor RAN. The 3GPP standards provided the specifications only for the user-plane interfaces between the components, i.e., F1 and enhanced common public radio interface (eCPRI). The O-RAN specifications address the deficiencies in the 3GPP standards and add support for management and network optimization functions that work across RAN components from multiple equipment vendors.

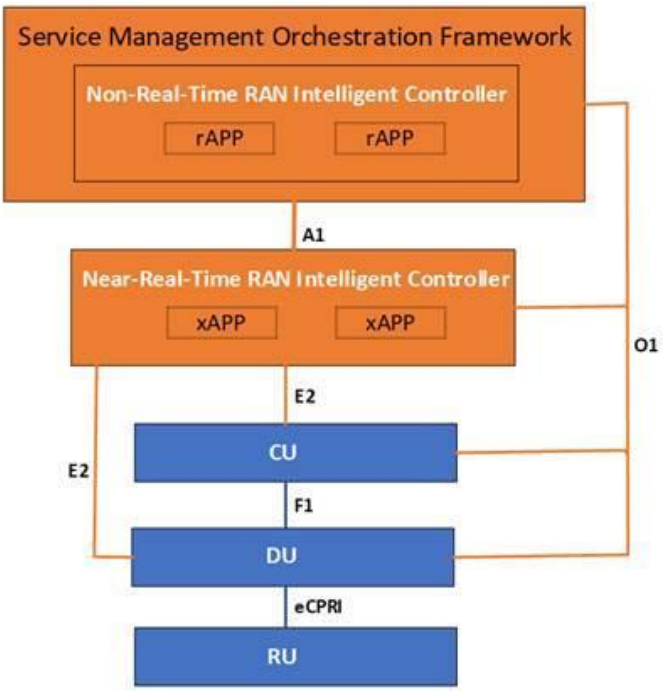

Figure 7 O-RAN Architecture.

Figure 7 illustrates the high-level O-RAN architecture. The orange boxes and lines represent the components and interfaces introduced by O-RAN. The service management and orchestration (SMO) framework hosts the non-real time RAN intelligent controller (non-RT RIC) function. The Non-RT RIC performs optimization of RAN in non-real-time, i.e., in greater than one-second intervals, by pushing performance targets to near-RT RIC via the A1 interface. The rAPPs residing in the non-RT RIC compute performance targets from the RAN performance metric. In contrast to the non-RT RIC, the near-RT RIC performs the optimization of RAN in real-time, i.e., in less

than one-second intervals, by providing policies to CU and DU via the E2 interface. The xAPPs situated in the near-RT RIC derive the policies from the RAN performance metric and performance targets. The policies pushed by the near-RT RIC to CU and DU are generally RAN configuration parameters defined by 3GPP. The SMO framework performs the management of RICs, CU, and DU via the O1 interface.

4.1. Use Case Scenario

It is expected that communication service providers (CSPs) will deploy a network slice dedicated to public safety and thereby ensure priority treatment and improve service availability of public safety-related services especially when the mobile network is congested. Among the various use cases identified in the O-RAN Use Cases and Deployment Scenarios [20] white paper, the RAN Slice SLA Assurance use case is important from the service availability perspective of the public safety slice. The white paper states that the non-RT RIC and near-RT RIC can fine-tune RAN behavior to assure RAN slice service level agreement (SLA) dynamically.

4.2. Preconditions and Assumptions

The GSMA Generic Slice Template [21], the standard for specifying slice requirements by a network slice tenant, allows the slice tenant to stipulate the slice requirements such as availability, area of service, delay tolerance, downlink throughput per network slice, and mission-critical support. The standard also provides a template or network slice type (NEST) with a recommended minimum set of attributes and their suitable values for public safety communication, e.g., availability as very high (>99.999%), and mission-critical support as supported. The O-RAN SMO framework receives those slice attributes applicable to the RAN from the network slice subnet management function (NSSMF). Also, the O-RAN Slicing-Architecture [22] states that the 5G system shall enable the network operator to define a priority order between different network slices in case multiple network slices compete for resources on the same network. It is expected that CSPs will configure public safety slices with higher priority than non-public safety slices. Furthermore, the public safety authority may want to ensure that CSPs assign a reasonably high priority to the public safety slices. The non-RT-RIC is expected to honor the attribute values of the public safety slice even when the RAN is extremely congested. For this purpose, non-RT-RIC is expected to downgrade the performance targets of non-public safety slices to maintain the service level of the public safety slices in congestion scenarios. Examples of slice performance targets are the maximum number of user equipment (UEs), guaranteed downlink (DL) throughput, and maximum DL throughput. The near-RT RIC will translate these performance targets to radio resources for each slice, e.g., a public safety slice is expected to receive a larger percentage of RAN resources such as physical resource blocks (PRBs) when RAN resources are in high demand.

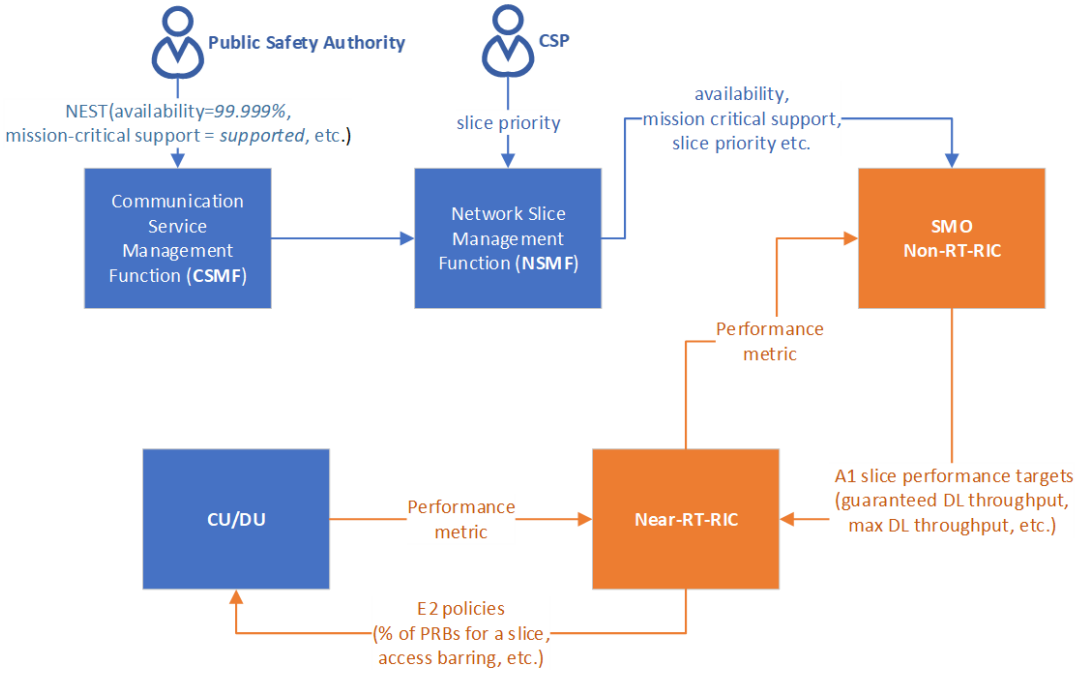

Figure 8 Network Slicing - End-to-End Configuration Flow.

Figure 8 depicts the information flow of network slice-related configuration from the slice template to the CU and DU.

4.3. Challenges Specific to the Use Case Scenario

As discussed in the previous paragraphs, service availability of the public safety network slice is most important particularly when the network is congested. The rules that generate the A1 performance targets and E2 policies can be developed manually or using AI/ML algorithms. In either case, the behavior of these rules should be verified before an extreme congestion event occurs.

4.4. Proposed Solutions

The public safety authority must work with CSPs and ensure that public safety slices are configured with sufficiently high-priority values. The ability of A1 targets and E2 policies to maintain the service level of public safety slice can be verified by emulating highly loaded RUs or upper-PHY layer of the DU in a lab. It is important to match the functionality and configuration of the rest of the components including RICs, CU, and DU with the field deployments. The public safety authority may request the CSPs to share the relevant test results periodically. If it is not practical to replicate the field deployment in a lab, modeling may be used to assess the ability of A1 targets and E2 policies to maintain the service continuity of public safety slices.

4.5. Enabling Technologies

The E2 interface pushes policies to CU and DU and its specifications are written considering the normal network load scenarios. However, supporting additional attributes in this interface may help the CU and DU to handle extreme congestion scenarios better so that the service level of public safety network slices can be maintained. A few examples of such desirable E2 attributes not listed in the Near-Real-time RAN Intelligent Controller E2 Service Model (E2SM), RAN Control [23] are identified below.

Choice of scheduling algorithms (e.g., proportional fair) and their configuration: A public safety slice may want to preserve the quality of service (QoS) of voice calls on the cell edge at the cost of the data throughput of cell center users in extreme congestion by allocating more percentage of PRBs to the cell edge UEs.

Alpha for fractional power control: Optimal power control for physical uplink shared channel (PUSCH) in extreme loads may not have the same characteristics as the busy hour. The RAN may want to maintain the PUSCH signal-to-interface noise ratio (SINR) more aggressively in extreme congestion scenarios.

4.6. Conclusions

The existing GSMA slice template, 3GPP network slicing architecture, and O-RAN architecture together are adequate to ensure priority of the public safety communication, particularly during congestion scenarios.

The public safety authority must work with CSPs and execute the following steps to ensure service continuity of public safety network slices in extreme network congestion scenarios.

- Configure public safety slices with sufficiently elevated priority values.
- Perform periodic testing and verify that public safety network slices will get enough radio resources to maintain service level.
- If testing in a lab is not practical, model gNB including O-RAN components with functionality and configuration matching field deployments.

It may be possible to improve CU's and DU's ability to use network resources more efficiently in extreme network congestion by supporting more attributes on the E2 interface.

5. Trust and Physical Layer Security for 6G Cyber-Physical Systems

In the fifth generation (5G) of wireless, the introduction of public key encryption-based authentication for private 5G networks, brought wireless security protocols even closer to those predominantly used in the core network. At the same time, new use cases were introduced to accommodate emerging verticals, such as smart factories, autonomous vehicles, and smart cities. The introduction of massive machine type communications (mMTC) and of critical Internet of things (IoT) applications under the umbrella of ultra-reliable low latency communications (URLLC), were in fact the precursors of a new wave of intelligent devices and (sub)networks that will be part of the 5G and beyond. Autonomous agents such as robots, drones, vehicles, etc., loaded with sensors and running advanced artificial intelligence (AI) algorithms (embedded or on the edge) to drive their autonomous operation. In this new emerging reality, the fiber of networking also changes, moving towards a network of subnetworks. In view of these fundamental changes, the question arises: in this emerging reality of dynamic, largely decentralized, heterogeneous systems of intelligent agents and things, will the standard, static, crypto-based security controls of previous generations be the way forward?

5.1. New challenges and Opportunities in 6G

5G security enhancements present a significant improvement with respect to long-term evolution (LTE), with the use of public key encryption (PKE) based protocols for authentication and key agreement (AKA), in addition to message integrity checks, etc. However, as the complexity of the application scenarios increases with the introduction of URLLC, mMTC and more generally intelligent IoT related verticals, novel security challenges arise that seem difficult to address with the classic complexity-based cryptography. Below, we attempt to provide an overview of the challenges as well as the opportunities ahead and comment on some of the potential emerging paradigms.

5.2. Low Latency, Low Footprint, Scalable Security

Operating under aggressive latency constraints, in massive connectivity regimes, with low energy footprint and low computational effort, while providing explicit security guarantees for networks of autonomous agents, is challenging. Persistently, the massive scale deployment of low-end IoT nodes, often manufactured with non-homogeneous production processes, poses pressing questions on the long-term IoT security (note that IoT traffic is largely unprotected).

5.3. Quantum Resistance

Furthermore, future-proof security systems will necessarily rely on quantum-resistant primitives and schemes. With respect to the recently standardized post-quantum cryptographic algorithms by NIST [24] [25], computational complexity remains substantial for very simple devices (low-end IoT) – despite the fact that the chosen lattice-based algorithms are among the alternatives with the shortest key lengths. There is a clear need for novel, lightweight quantum-resistant solutions oriented specifically to low-end IoT devices.

5.4. Artificial Intelligence and Machine Learning

At the same time, the extensive introduction of AI and ML will further increase the attack surface of 6G systems; it is currently understood that defenses are needed against adversarial AI (e.g., to protect against data-poisoning), the energy footprint needs to be contained to sustainable levels (green AI), the outputs of AI algorithms need to be explainable and unbiased (XAI) [26]. Hand in hand with these challenges, new opportunities arise, for example with respect to decentralized and democratized learning and computing (e.g., using federated learning) and the possibility to perform context and semantics distillation that can enable the use of new technologies, such as physical layer security, as discussed below.

5.5. Quality of Security (QoSec)

Looking at the big picture, a sustainable and secure future calls for adaptivity to make the most out of limited resources. In this direction, adaptive security algorithms and protocols can be envisioned, that dynamically adjust their configuration and parameters according to inputs from several layers and more generally from semantics and contexts. To provide scalable solutions for massive IoT and networks of cyber-physical systems, QoSec could provide a flexible security framework for future networks, introducing different security and trust levels.

5.6. Physical Layer Security

In the framework of adaptive, AI-enabled security, it is envisioned that physical layer security (PLS) solutions [27], which exploit physical phenomena to provide security, can complement post-quantum cryptographic schemes and strengthen the overall trust and resilience of 6G. PLS can be used to provide keyless exchange of confidential or private messages, as well as to generate and distribute symmetric keys by exploiting the propagation characteristics of the wireless channel. In 6G, channel engineering and controllability (e.g., with the use of meta-surfaces, drones for multi-hop networks and very narrow beamforming) will allow to exploit such opportunities in a systematic manner. In addition, authentication at PHY and hardware layers, e.g., using physical unclonable functions and localization as a second factor of authentication, can be introduced to enable a quick and potentially continuous verification of legitimate user, even without upper layer processing.

5.7. The Introduction of Sensing and High Precision Localization in 6G

In 6G, positioning and radar sensing will be the default services [28]. On one hand, this provides novel opportunities for the use of positioning and sensing for integrity / consistency checks and anomaly detection accounting for the physical behavior devices. Such a processing can be generalized with the use of distributed statistical inference. Positioning and sensing integrity will be of great importance; currently, angle of arrival (AoA) in conjunction to ranging, camera depth estimations, etc., are studied to render positioning unforgeable. Several protocols have already been proposed that incorporate positioning information as a second soft authentication factor, while Sybil cyberattacks in robotic systems have been identified using AoA [29]. Overall, positioning will be an important parameter for evaluating the trustworthiness of autonomous agents in 6G. At the same time, privacy concerns arise.

5.8. Privacy in 6G

As mentioned above, radar sensing will be omnipresent. It can be used to count the number of people in a room (e.g., by identifying heartbeat) or other related physiological signs. At the same time, the use of wide frequency bands (available at mmWave and sub-THz bands) can allow resolving multipath components and reaching cm-level localization precision with radio frequency signals. As a result, serious concerns arise with respect to privacy of individual users. While federated learning and approaches targeting differential privacy i.e., relying on rate-distortion theory, are promising, there is still a lot of work in terms of privacy preserving sensing and privacy by design. The trade-off between utility and privacy is potentially a key research topic in 6G security.

5.9. Trust and Trustworthiness

As a whole, the overall behavior of the devices, agents and systems should be accounted for when building trust and evaluating trustworthiness. For a trustworthy 6G, multiple layers of trust must be assured. While related discussions are still unfolding, it is common sense that building a trustworthy 6G network necessitates trusting the AI brains and the infrastructure body of the 6G network (including the sensing, the communication links and the processing). At a very abstract level, the first anchors of trust can be boiled to trusting (in a very abstract manner):

- The sensing (radar, RF, camera, lidar, etc.,) that collects raw or processed data (of particular importance in 6G is high precision localization information) and drives actuation;
- The computation and processing platforms (including for learning and optimization) at different parts of the network (on device, edge, core network);
- The communication links that carry the data exchanged and authenticate agents and devices, providing confidentiality, integrity, authentication and availability guarantees;
- The AI algorithms that determine the behavior of the autonomous agents, devices and systems based on the received data and sensing inputs.

5.10. Conclusions

The sixth generation of wireless will be the first AI native generation and will interconnect intelligent and autonomous cyberphysical systems (robots, vehicles, platoons), will bring to life digital twins of physical objects and the metaverse. The anticipated fusion of the physical, digital and human worlds marks the beginning of a new era in which the physical properties of interconnected systems are crucial for security. Research into areas such as AI, distributed statistical inference, physical layer security are, among others, pivotal to enable smart, adaptive security protocols.

6. Energy-efficient Indoor Communications for Public Safety

During emergencies, the success of first response depends on different factors: some of them concern individual competence and ability, while others pertain to organization and management of the safety operations. In this sense, an effective information sharing with the decision support structures may significantly contribute to develop situational awareness and, consequently, improve the response's timeliness [30].

Recent proliferation of smart portable and wearable devices, also driven by the development of flexible electronics, has opened new opportunities towards that end. This technology, indeed, can be used to track where responders are on the scene, facilitating real-time information transmission to the core structure in the decision-making process. Moreover, it can be used to automatically monitor wearer's physiological parameters, such as temperature or heart rate, to discover, for example, whether responders have been exposed to dangerous substances.

Energy supply is a great issue for this kind of small devices: even if battery technology is mature and several power management strategies are deployed to prolong battery life, the exclusive use of replaceable batteries to power the wearable sensors may limit their flexibility as well as their possibility to be kept safely powered.

6.1. Use Case Scenario

In some cases, emergency responders and other public safety (PS) personnel are required to operate in indoor environments, including hospitals, schools, train and subway stations, airports, shopping malls, or government buildings.

The newly introduced technology of portable and wearable devices can assist responders to exchange information with the central control unit and complete complex operations. These devices, indeed, allow for real-time communication and location tracking, making it easier for teams to stay in contact and respond to emergencies quickly and efficiently. Wearable devices typically consist of a small computer or microcontroller, a communication module, and a power source. The computer or microcontroller is responsible for processing data and controlling the device's functions, while the communication module allows for real-time communication with other devices or a central control center. Usually, replaceable batteries are employed as power source for such a portable equipment.

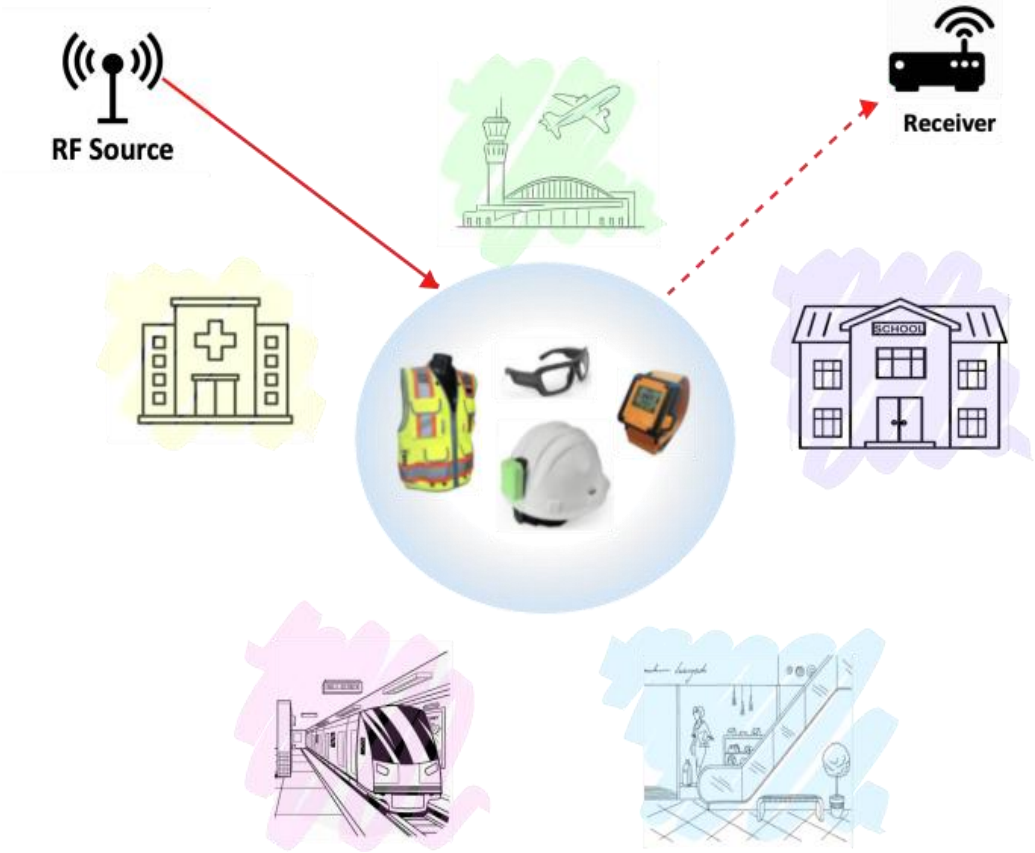

Figure 9 Examples of indoor environments where wearable devices can communicate through RF backscatter communications.

6.2. Challenges

From a communication perspective, indoor scenarios are rather challenging, since they usually contain different structures that can interfere with traditional forms of wireless communication, complicating, thus, the information sharing among PS officers. The main challenges that can arise in these environments are represented by the limited signal penetration, high signal attenuation, and interference. The physical characteristics of objects in indoor environments, such as building materials, furniture, openings, and partitions, can significantly hinder the signal penetration, especially as frequency grows [31], and, consequently, reduce the link quality. This can be particularly demanding in large buildings, such as shopping malls or airports, where there are many floors and rooms. In addition, reflection, diffraction, and scattering from nearby objects result in multipath fading, which can severely degrade the performance of indoor wireless communication systems. Moreover, indoor environments can experience a high level of interference from other wireless devices, such as Wi-Fi routers and Bluetooth devices, which can make it difficult for emergency responders to communicate with each other.

A limited wireless connectivity may increase the power consumption of portable equipment, restricting its operating time and affecting its usability. Power source represents a significant challenge for wearable sensors, which are usually powered by replaceable batteries, whose rigid

characteristics limit their overall flexibility. Further, due to the small form factor of wearable sensors, batteries are small and, consequently, have limited energy storage capacity.

The main requirements of power supply for portable equipment targeted at PS personnel are the following ones:

- power supply needs to be easily portable and accessible, allowing officers to quickly move from one location to another;
- it must provide sufficient power to guarantee a constant and reliable communication;
- it must be safe, avoiding the use of risky chemicals for PS officers.

6.3. Proposed Solution to Address the Challenges

Self-powered technology can represent a possible solution for the power supply issue in portable and wearable systems. In this case, a device can perform its own operations by harvesting energy from the surrounding environment, without an external supply. Different types of energy can be exploited to this aim, such as mechanical energy [32] [33], thermal energy [34], solar energy [35], or chemical energy [36].

In indoor environments, the principle of radiofrequency (RF) backscatter communication can constitute an alternative solution. RF backscatter communication is a wireless communication technique that allows devices to transmit their own data by backscattering towards the receiver, after modulating it, a portion of the received electromagnetic wave. A recent evolution of this technology is represented by ambient backscatter communication (AmBC) [37] [38], which leverages existing RF signals, like cellular, TV, or Wi-Fi ones. This paradigm eliminates the need for a dedicated power source, making it a perfect solution for low-power and battery-less devices.

One of the key advantages of RF backscattering for public safety communications is its ability to provide communication in environments, like those indoor, wherein cellular or satellite networks are unavailable or unreliable.

Another advantage is its low power requirements, i.e., it can be used to power small, wearable devices that can be worn by emergency responders, providing, thus, real-time location tracking and communication.

Additionally, backscatter communication can be used to create a mesh network, where devices can communicate with each other and relay information to a central control center. This can be particularly useful in areas, where there is little or no infrastructure, allowing emergency responders to stay connected and coordinate their efforts.

RF technology is certainly the enabler of choice for wireless communication, but long-term exposure to RF electromagnetic fields could result in adverse human health effects. For this reason, optical communication (OWC), and especially visible light communication (VLC), may represent a promising candidate to provide wireless access to wearable devices, also thanks to its energy efficiency and security, as well as the availability of high bandwidth in the visible light spectrum and the inherent insensitivity to RF interference. In VLC systems, data is transmitted by modulating the intensity of light emitted by a light emitting diode (LED), which allows one to utilize the existing lighting infrastructures for communication. The backscatter principle can be applied to optical communications, giving rise to the visible light backscattering (VLB) paradigm, wherein the incident light is reflected after optical modulation.

6.4. Enabling Technologies

RF backscatter communication (BC) can be divided into three categories based on their architecture: monostatic BC (MBC), bistatic BCs (BBC), and AmBC.

MBC systems comprise a backscatter transmitter (or tag) and a reader. The reader generates the RF signal that activates the tag, whereas the tag first modulates the received RF signal with its own data and then reflects it towards the reader. This architecture, wherein the reader represents, at the same time, the RF source and backscatter receiver, may suffer from round-trip path loss and doubly near-far problem [39], which can be particularly severe if the tag is far from the reader. For this reason, MBC is mainly used for short-range applications.

In BBC systems, on the contrary, the RF source (carrier emitter) and the backscatter receiver are physically separated and, thus, the round-trip path-loss problem affecting MBC systems is avoided. Differently from MBC, the coverage area of BBC systems can be significantly increased by optimally placing the carrier emitters.

Unlike bistatic backscatter systems, ambient backscatter systems do not require a dedicated carrier emitter, but utilize existing or legacy RF signals, such as cellular, TV, radio, or Wi-Fi. In particular, the reference architecture is composed by a legacy system and a backscatter transmitter that wishes to transmit information symbols to its intended recipient. The backscatter transmitter is a passive device that communicates using the power harvested from the RF signals of the legacy system. The backscatter and legacy receivers, in this framework, can be spatially separated nodes or they can be placed on the same device.

When the electromagnetic wave reaches the backscatter transmitter, its antenna is excited, and the RF power is converted to direct current power through a power harvester. Once sufficient RF power is harvested from the legacy signal, the backscatter transmitter will be activated, and the harvested DC voltage is used to modulate the reflected electromagnetic wave and to power the digital logic units on the device. The backscatter transmitter performs digital modulation, i.e., it maps its bit sequence onto RF waveforms, by properly varying the load impedance of the antenna. The reflection coefficient is given by:

$$\Gamma_i = \frac{Z_i - Z_a^*}{Z_i - Z_a}$$

where Za is the antenna impedance, Zi is the load corresponding to the i-th switch state (i =1,2) and * is the complex conjugate operator. By choosing Z1 or Z2, the reflection coefficient switches from the absorbing to the reflecting state and, consequently, a forward or a backward wave is generated. Such a mechanism is generally referred as load modulation.

The principle of visible light backscattering is similar to RF backscattering [40]: its simplest architecture includes a LED acting as light source and an active transmitter, and a passive tag, equipped with a retroreflector device which reflects the light back towards the source, after modulating it with its own data. An optical retroreflector (ORR) is a device that reflects light back in the direction from which it came, regardless of the angle of incidence. There are two main types of ORR: corner-reflectors and cat's eye retroreflector. Corner-reflectors are made up of three mutually perpendicular reflecting surfaces, while cat's eye retroreflectors consist of a curved reflecting surface and a small aperture. By controlling the reflection mechanism through micro-

electromechanical systems (MEMS) or multiple quantum wells (MQW) technologies, it is possible to employ a retroreflector as an optical modulator.

In VLB systems, optical modulation can be realized by means of LCD shutter devices. They work by using liquid crystal material to control the polarization of light passing through it, allowing light to pass through or blocking it based on the applied electrical signal.

The natural evolution of backscattering is represented by the recently emerged technology of reconfigurable intelligent surfaces (RISs), which can work both at RF and optical frequencies.

They consist of two-dimensional nanostructured materials used to control the phase, amplitude, polarization, and direction of the incident signal. In particular, RISs are composed by sub-wavelength metal/dielectric structures, referred as meta-atoms, which can be independently controlled via software to switch among different reflection amplitude and phase responses. A key aspect of such a technology is its reconfigurability, which provides a high level of flexibility and adaptability.

6.5. Discussion

Backscatter communications represent a better choice with respect to conventional radio communications for public-safety applications in indoor environments, given their peculiarities in terms of operating distance, data-rate requirements, and power availability. In the first proposed architectures, backscatter devices communicate with passive receivers by reflecting either ambient signals or a dedicated wave source (tag-to-tag communication), ensuring in this way ultra-low power consumption. However, the poor sensitivity of passive receivers limits the operating distance range. To account for this, different system solutions have been considered wherein the passive receivers are replaced by radio ones, which exhibit sensitivities much lower than passive receivers, allowing thus for a significant operating distance extension. Therefore, recent research efforts seek to address the design of backscatter indoor systems where tags transmit data which can be received, for example, on a commodity smartphone, without modifying the existing infrastructure [41].

A further development in backscatter communications consists in multi-hop and mesh networking. Traditional peer-to-peer communication among backscatter devices ensures satisfactory communication rates over relatively short distances [8]: a great enhancement could be achieved by implementing multi-hop backscatter systems, which is still an open problem. Recently, research activity on backscatter communications is focusing on millimeter-wave (mmWave) bands, which can largely boost the transmission data rates. At these frequencies, a significant antenna miniaturization is possible, which allows for system implementation with additive manufacturing technologies (AMTs) and direct integration with wearable and flexible electronics [42].

6.6. Conclusions

Information sharing among PS officers can significantly improve the success probability of safety operations. In this sense, smart portable and wearable devices represent useful tools to track where PS officers are on the scene, facilitating real-time information transmission to the core structure during the decision-making process. Since energy supply is a great issue for this kind of small devices, energy-efficient communication strategies have been discussed in relation to indoor

scenarios. Particularly, we have focused our attention on the recent paradigm of backscatter technology that enables communication by reflecting RF or optical signals, leveraging dedicated carrier emitters or existing ambient waves. Its working principle has been illustrated, presenting the main enabling technologies, the advantages, and some open problems, which need to be addressed to make the technology more effective.

7. Private AI for Preserving Public Safety Concerning Data and AI Services in Next Generation Networks

The realization and standardization of 5G has paved the way for increased research concerning sixth generation (6G) communication systems. The popular use cases of 5G systems include ultra-reliability and low-latency communications (URLLC), massive machine type communications (mMTC), and enhanced mobile broadband (eMBB). In contrast to 5G that uses artificial intelligence (AI) as a service, 6G considers AI as an enabling technology to realize the improved services. It is to be believed that the synergy of 6G and AI would explore new paradigms in terms of research, usability, services, and resource optimization [43]. One of the applications that benefits from 5G, and next generation networks is the public safety for critical operations. Current mission critical operations are limited to voice-based services, however, 6G in conjunction with AI would enable video services, augmented reality based haptic feedback systems, remote controlled drones, and healthcare monitoring [44]. The popularity of public safety services via mobile network providers can be measured by the requests received from the governments, which include AT&T and FirstNet based nationwide public safety networks in United States, BT/EE and Home Office alliance-based mission critical communication systems for emergencies in United Kingdom, and Erillisverkot's public safety and mission critical networks in Finland [45].

With the technological improvements, security concerns have also been on the rise, especially concerning the data that is used for the public safety networks. Federated learning was introduced as a potential solution to preserve data privacy; however, differential privacy attacks have proven to bypass the federated learning-based defenses as it directly attacks models [46] [47]. It is, therefore, necessary to design methods and strategies that not only preserve the data privacy but also secure the model parameters in order to maintain the compliance with General Data Protection Regulation (GDPR) guidelines. One of the potential solutions to the aforementioned issues is the use of Private AI. Initially, Private AI term was coined to secure the data by using encrypted data for end-to-end processes [48]. Recently, the proposal of Private AI was extended to model security as well [46]. Therefore, leveraging the Private AI framework for preserving data and model for public safety application when using next generation networks and AI services seems to be one of the immediate solutions.

7.1. Use Case Scenario

The proposed use case scenario explored in this paper is shown in Figure 1. The selection of the use case scenario is in compliance with public safety and mission critical applications. The selection of use case has been motivated by the recent internal displacement of people to refugee camps and tents due to flood situation in Pakistan and aftermath of earthquakes in Turkey. The communication for such camps needs to be set via a remote drone and portable 5G cell site equipment, which relays the information to centralized 5G core / mobile edge computing (MEC) framework. Such network deployment is possible through EC's 5GINFIRE platform [49] and has been used for verifying its support in the context of public protection and disaster relief [50]. This experimentation facility is referred to as public protection drone (PPDrone). This facility is composed of a cloud radio access network (C-RAN), software defined radio (SDR), backend infrastructure from OpenStack-based Internet as a Service (IaaS), and flexible configuration options. Remote Radio Head (RRH) was implemented as distributed unit to deploy public protection drone, base band unit (BBU) was implemented as control unit, evolved packet core

(EPC), and a monitoring dashboard with IoT Gateway. Through the aforementioned facility, a base of operations can be set on the emergency site as well as the area where refugee camps are being set. On the edge side, industrial grade gateway was used to provide backhaul connectivity, monitoring dashboard, tactical command base, and the components used in portable cell site. Further details on the deployment along with spectrum access and power usage can be found [50]. The assumption is that the base of operations is set to monitor the physical and mental health conditions of the people dealing with the aftermath of the disaster and losing either their home or loved ones.

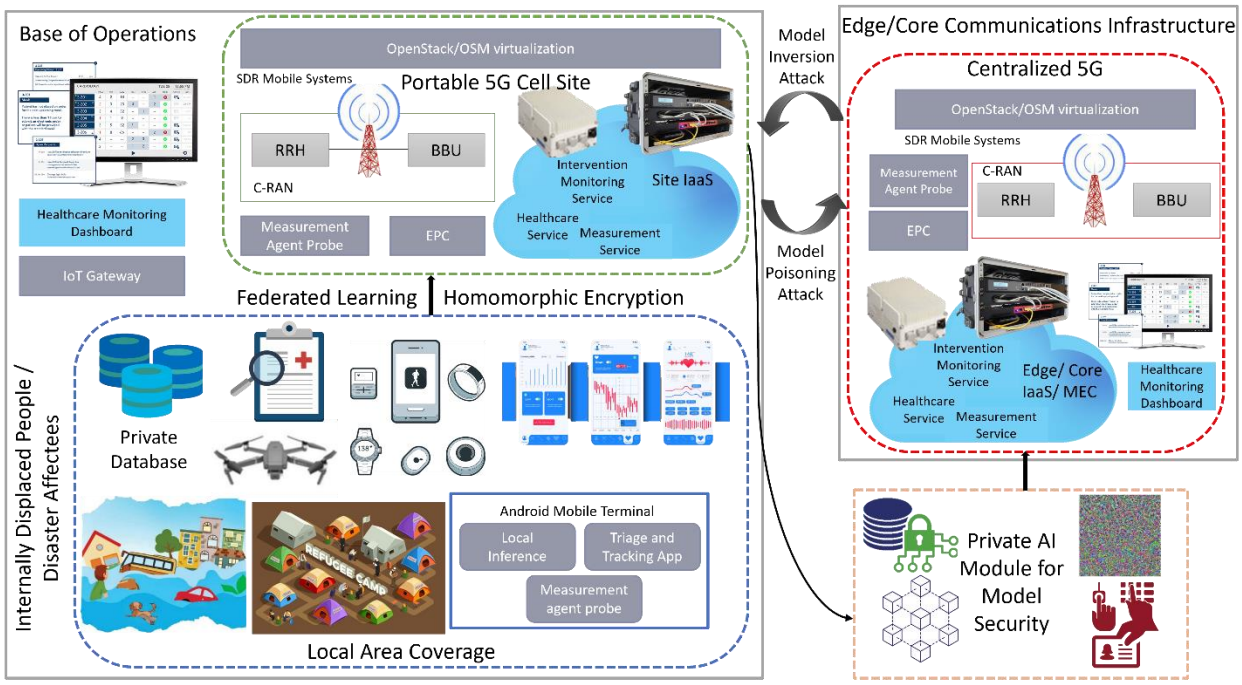

Figure 10 Proposed use case scenario for public safety and mission critical application deployment using next generation networks.

7.2. Preconditions and Assumptions

The main aim and purpose of this work is to highlight the importance of Private AI for public safety and mission critical applications in connection to next generation networks. With respect to the aforementioned scenario shown in Figure 1, we make some assumptions considering the base of operations, portable 5G cell site, availability of equipment, wearable sensors, integration of monitoring dashboard at the base of operations and security vulnerabilities. Considering that a disaster has occurred, government is carrying out a rescue operation and meanwhile, a refugee camp has been set to transfer the disaster affectees. Facing such type of disaster not only incurs physical health issues but also the mental ones. Following are the preconditions related to the communication networks.

- A Portable 5G cell site along with drones for providing network coverage is available.
- A healthcare monitoring dashboard is set to monitor the conditions in real-time.

- The portable cell site is connected with the centralized 5G systems to provide healthcare services.

Following are the assumptions related to the aforementioned scenario.

- Affectees have access to smart phones and wearable sensors.
- The smartphones are equipped with android mobile terminal and necessary APIs.
- Wearable sensors can connect to the smartphone.
- Smartphones are able to access the communication services.
- Malicious users trying to access the data or model with data and model related attacks.

We assume that the users' health care (physical and mental) is being monitored by the continuous access to data through the smartphones. We consider both the scenarios where the data is sent to portable site and then to centralized 5G systems for providing relevant services or the trained model is sent to the centralized station via portable site using federated learning technique. A malicious attacker wants to access the data or the model to malign the privacy of the users' data, accordingly.

7.3. Proposed Solutions to Address the Challenges

The data gathered by the wearable sensors or smartphones are considered to be quite personal and requires privacy preservation respectively. Usually, inertial measurement units (IMUs) are used for monitoring physical activities and related anomalies, for example, fall detection. Physical activity monitoring along with vital signs are the first stage to identifying emergencies [51]. Subsequently, mental anomalies such as stress, anxiety, depression, despair, can be recognized and monitored using heart rate, heart rate variability, galvanic skin response, electrodermal activity, and blood volume pulse, respectively. The security of such data is critical as it can be used against an individual. At the data level, if the data is being sent to portable base station and then to the cloud, it may be intercepted. Similarly, the data can also be retained from model inversion attacks when sending an update to the users from the cloud. Model poisoning attacks can infiltrate the weights; thus, the monitoring dashboard will be compelled to show false positives or false negatives.

The proposal leverages the concept of Two-Tier Private AI that not only protects the data but also preserves model privacy. Private AI framework suggests that private databases should be added, in this case, smartphones that can train the model locally instead of sending the data to the cloud. Alternatively, if the data needs to be sent, it should be sent either over the private network to the trusted party and then stored in private databases or should be sent in encrypted form (homomorphic encryption). This step will preserve the data privacy. For the model privacy, we consider two attacks, i.e., model poisoning and model inversion. For both the attacks, the portable cell site should first send the model to Private AI module for model security for taking necessary measures and then to the cloud. Different strategies are used for model security in Private AI setting that include homomorphic encryption, initialization of intentional attack, adding noise, intentional label perturbations, and so forth. The two-tier security framework not only helps in retaining acceptable level of data privacy and security but also reduce the chances for the affectees to suffer more mental distress, if the data gets stolen.

7.4. Enabling Technologies

In the context of public safety, the base technologies that help in realizing real-time mission critical applications are 5G, AI, and Internet of Things (IoT). However, we have entered into an era where geo-political crisis, climate change calamities, street crimes, and cybercrimes have been a norm. In order to tackle the aforementioned challenges, the base technologies need to be combined with emerging ones for providing better security and response measures. Following are some of the enabling technologies that would help in improving the public safety services.

7.4.1. Internet of Everything

Most of the institutions dealing in public safety are considering smartphones as one-stop shop for every tool they require such as e-citation devices, voice recorders, and cameras. Furthermore, different software packages can also pay a key role in reducing cultural and language barriers in the form of translation and wellness applications. However, public safety is not just limited to crimes rather it also has mandate of looking after healthcare, which includes monitoring of data from real-time body worn sensors. Furthermore, current technologies are limited to geolocation searching of patrol cars rather than individuals. Internet of Everything allows users, caregivers, and patrol officers a chance to speed up the communication processes for providing timely and reliable services, respectively.

7.4.2. Blockchain

Existing technologies mostly use conventional encryption strategies or authentication schemes to protect the data privacy. With recent advancement in technology and evolution of machine learning based strategies, it is hard for those conventional encryption methods to keep up while preserving the data privacy. Recently, researchers have moved to blockchain systems for data privacy and security issues. Blockchain creates a distributed ledger systems which is hard to manipulate, thus, provides an edge to the systems dealing with sensitive data such as public safety applications. In the proposed framework, the blockchain systems can be used for both data and model security modules. For data security, the transactions can be monitored for the changes, while the model security module can benefit from blockchain in terms of securing model parameters, which can be used to re-engineer the data. Model poisoning can also be diagnosed with blockchain systems as manipulation in any transaction is either recorded or denied if minimum number of nodes do not agree with it.

7.4.3. 6G Systems

5G has been a big boost to public safety networks but still there is room for improvement in terms of super-fast data transfer, support for real-time applications, and livestream for body worn cameras. The 6G technology promises the services and speed that can realize public safety and mission critical applications to its true potential. 6G technology will allow moving vehicles to have real-time location awareness for facilitated traffic flows, empower decision makers by providing real-time video feeds at base of operations, emergency response by observing real-time feed via body worn cameras, and medical assistance through virtual meetings or even virtual robot assistant remotely controlled by the surgeon.

7.4.4. Metaverse

Metaverse is a conceptual world where a human transform itself into a digital being and realizes physical world in digital form, respectively. The use of metaverse has already been started in the context of public safety, for instance, West Midlands police has taken an initiative through their website that interacts with humans into the digital world and let them asks "what if" questions to get updates and information. Another such example is the virtual courts that brings the virtual avatars of all the stakeholders in a digital place to roll out the justice system. In order to provide an immersive experience virtual reality, augmented reality, and extended reality is used at great lengths.

7.5. Existing Technologies

To the best of our knowledge, Private AI, specifically that provides two-tier security has not been explored in the context of public safety domain. Existing works focus on either security model, i.e., data or model. Conventionally, priority is given to data security as many of the communication systems still collect the data and send it to the cloud server for service activations. Over the recent years, perception has been started to change for adopting distributed technologies such as federated learning, which transmits the trained model rather than data. With the adoption of federated learning strategies, the attack paradigm has been shifted to the model's privacy rather than the data itself. Recent studies [52] [53] on the public safety domain do consider next generation networks, conventional authorization schemes, lightweight security modules, and private keys to protect the data, however, very limited discussion has been carried out to model privacy. We believe that the data concerning public safety applications is quite sensitive, specifically the health-related data as shown in Figure 10. Therefore, providing two-tier security, i.e., data and model, is not just a priority but rather a necessity.

7.6. Proposed New Technologies

The proposed use case and concept of adapting Private AI has been built upon our series of works [54], where both the data and model privacy has been given equal importance. The private AI framework relies upon three modules, which are private database, private AI for data security, and private AI for model security, respectively. In the given scenario, most of the encryption techniques and privacy methods would work well if the private database were with the user in the smartphone. Therefore, the private database module is not discussed at length here.

For a service to get activated in public safety environment as shown in Figure 1, there are two ways to go. The first is the transmission or raw data and the second is the use of Federated learning approach. The former needs security measures as it can be sent to a trusted or third-party services. The private AI framework suggests that the data should be sent in an encrypted form over the transmission channel. The encryption should have at least two to three layers, suggesting that the first layer is a secret key that is shared with the trusted party, along with encryption algorithm and addition of noise. The addition of noise as well as decryption mechanism is assumed to be in line with the current practices. However, if the data is sent to third party services, it is suggested to perform the operations on the data in an encrypted form. This process is referred to as homomorphic encryption. The latter way trains the model locally with the user and transmits the

trained model over the transmission channel, which again reduces the problem of data privacy to an acceptable threshold.

The use of federated learning approach does provide privacy preservation to the data, but it is quite vulnerable to differential privacy threats associated with the model and the parameters [54]. In the proposed scenario, we mostly address model poisoning and model inversion attacks. Both attacks assume that the data is either compromised or reengineered by the attacker mainly using generative adversarial networks (GANs). To date, GANs has been adopted in most of the works that address model inversion and model poisoning attacks. Similar to the previous one, Private AI for model security module is open for different prevention strategies such as addition of noise to model parameters, intentional initialization of attack to the data itself, or label perturbations. These strategies have shown certain degree of resilience to differential privacy threats.

7.7. Challenges Specific to the Use Case Scenario

The proposed Private AI framework for public safety applications might face many challenges from both the technical and financial point of views. In this paper, we are highlighting some technical challenges that have greater impact concerning the use case shown in Figure 10. Following are some of the challenges associated:

7.7.1. Speed and Bandwidth

Although the current iteration of communication technology (5G) has leaps and bounds ahead of previous iteration, it has still limitations for the provision of speed and bandwidth that is required for real-time healthcare services, such as live streaming of body worn cameras, real-time navigation, real-time remote controlling of medical robot for performing procedures on patients, and so forth. Nevertheless, 5G has still potential to provide near real-time services and public safety networks can benefit largely from the current iteration, accordingly.

7.7.2. Communication Footprint and Scalability

In the proposed scenario, we assumed that the portable 5G cell site is deployed with a drone that is able to provide communication services within the said area. The assumption holds for a limited number of affectees and refugees along with a limited land area. As the number of people requiring communication services increase along with the number of devices and associated land area, it would require extension of communication footprint and scalability. One of the recent works showed a way to extend the footprint via distributed services and device to device communication but the work is still theoretical, and a practical realization is yet to be implemented. In the current scenario, both the drones and portable 5G cell sites needs to be increased to accommodate the increasing number of users, devices, and land area, respectively.

7.7.3. Homomorphic Encryption and Blockchain

Both of the techniques have been used extensively in the field of data security and privacy, yet some issues still need to be solved in their respective domains. The homomorphic encryption is considered to be quite effective for preserving data privacy, however, studies have shown that it

can degrade recognition and classification performance. To design homomorphic encryption methods that are secure while maintaining an acceptable level of tradeoff in terms of service performance is an open research problem. Similar is the case with blockchain. Recent studies have extensively committed themselves and suggested the use of blockchain technology, but it is no exception to the security vulnerabilities. The security challenges associated with blockchain include 51% attacks, phishing attacks, routing attacks, blockchain endpoint vulnerabilities, and sybil attacks have shown to degrade the overall performance of the said system. Researchers are striving for continual improvement of blockchain technology to cope with the aforementioned attacks.

7.7.4. Resource Constrained Devices

In the proposed use case, there are many resources constrained devices in use ranging from smartphones, wearable sensors, IoT devices, to drones that provide communication service. Continuous data transmission has been shown to have a major impact on battery constraint devices while the computationally intensive applications directly affect the memory constraint devices. For provision of near real-time services, techniques to reduce the communication while striving to maintain the service performance is still a challenge to many of the service providers. The same goes for the design of AI and encryption algorithms that require extensive computations to be performed such as training models on the smartphones and using multi-level encryption techniques. Both the operations have the capability drain memory as well as battery from resource constrained devices.

7.8. Insights and Discussion

Private AI field is gaining a lot of interest in the research community, specifically due to the consideration of model security. With the rising threats concerning cybersecurity it is essential for any application that uses AI as a service to deploy security measures. However, designing defense strategies require the information of how the attacks can be carried out. So far there are some methods that have been proposed such as deep leakage from gradients [55] and its improved version [56] as state-of-the-art methods. Some studies have recently proposed the simulation of attack methods in the context of communication systems and vehicular technology systems [54]. Some of the key insights from the works from model related attacks and defense are as follows:

- Private databases reduce the latency but increases the cost of capital.
- Using encrypted form of data to perform operations would reduce the privacy risks by more than 76%.
- Using GANs and sophisticated methods such as deep leakage from gradients, the success rate of reengineering data is more than 50%.
- Adding noise or intentional adversarial attacks can reduce the attack success rate by 38%.
- Using just one attacker node the model poisoning attack can cause degradation of model performance by 29%.
- Combining deep leakage from gradients for data reengineering and model poisoning attacks can reduce the degradation of model performance by 45%.
- Encrypting model parameters can reduce the attack success rate by 42%, however it also reduces the performance of the system by 12%.

It should be noted that the model related privacy vulnerabilities and attacks are still a new concept, and many studies have started working on the concept, i.e., evolving the attack strategies so that efficient methods for the defense can be designed. Over the years, the key insights we gathered might change with the advancement in the either of the technologies, i.e., attack or defense, respectively.

7.9. Conclusions

The climate change has provoked natural disasters in a significant way, which has resulted in natural calamities. The response to such disaster events requires active public safety and support for mission critical applications. For responsiveness measures to be effective, fast, reliable, and secure communication services need to be provided to the public safety personnel. Next generation networks such as 5G communication network meets the necessary communication requirement to some extent, however, the data, model, and services remain vulnerable to security threats. We propose Private AI network to address the security issues for public safety applications in next generation networks. The data transmitted while performing activities to maintain public safety and mission critical applications is quite sensitive as discussed in the proposed use case. In this regard, Private AI is a natural choice as it provides security to not only users' data but also the model that is the basis for service activation and provisioning. We further highlight challenges that are specific to use case scenario and provide some insights based on our previous studies, experiments, and gathered data, respectively. We believe that the use of Private AI reduces the attack success rate by 20 – 30% on both the data and the model. The synergy between Private AI and public safety would provide a secure platform to the users and safety personnel to carry out the operations in a swift manner.

8. Coordination in Serious Games Scenarios Leveraging on Dishomogeneous PSN

The interest in the resilience of the Critical Infrastructures (CIs) has a well-established history in European Union (EU). The history roots are in the Directive [57] and specific actions date to the 2008 Directive on European Protection of Critical Infrastructure Program [58]. The currently founded Horizon 2020 Projects PRECINCT and PRAETORIAN examine the approaches to attain resilience in complex interdependent crisis scenarios, involving CIs and First Responders (FRs). The Projects identify a set of related CIs that are impacted because of a major incident. Cascading effects affecting the CIs are structured in an analysis framework. The aim is to train the CIs and FRs operators at cooperating to recover since the earlier phases of the incident. The Projects devise an Ecosystem Platform for connecting stakeholders of interdependent CIs and Emergency Services to collaboratively and efficiently manage security and resilience by sharing data, Critical Infrastructure Protection models, and related new resilience services. Real world, Scenarios Simulation and Demonstration (also known as, Serious Games [59]) provide a means of identifying vulnerabilities as well as testing and validating new detection and mitigation models and associated services in a real-time real-life context. The coordinated use of different PPDR radio networks in a crisis scenario has been identified by the two Projects as a gap to overcome. The models and tools developed by the two Projects are proposed as an opportunity to increase the resilience of interconnected PPDR communications networks. The intention is to contribute to a field of interest of ITU, ECC, EU and European National and International bodies since a long time.

8.1. Use Case Scenarios

The Projects intend to develop a market-ready technology of a set of already established technological practices. End users of the technology (CI operators and FRs) and technical developers work alongside to develop tools tailored to the needs of the operators. The interaction of the operators and the tools is tested on “urban / sub-urban crisis” use case scenarios. Some of the operators participating in the use case scenarios (the Ljubljana, Bologna, and Zagreb ones) have developed the discussion about the current state, the expectations in critical situations and the current gaps to be overcome about PPDR radio networks. The discussion has raised the awareness that the nature of the Scenarios Simulations and Demonstrations as enablers to develop consequences mitigation could be effectively used in preparation to deploy an inhomogeneous PPDR radio networking scenario. Consequence mitigation could be achieved via short term and long-term enhancements of the single converging radio networks involved in a major incident, resulting from the identification of short- and long-term measures that improve resilience. This opportunity was not in the original premises of the Projects, but the approach appears promising.

8.2. Preconditions and Assumptions

The aim of the Projects is to increase the CIs resilience in the selected use case scenarios, which is the ability of interdependent CIs and First Responders / Public authorities in a territorial context to plan for, prevent, absorb, recover, and adapt efficiently and effectively to the effects of cyber-physical and hybrid threats / attacks as well as impede their cascading effects. In the Projects, the collaborative part, and the governance model that enable the resilience take place in the CIs

Coordination Centers (3Cs). Each 3C links CIs, FRs and other CI stakeholders into a common security and resilience management framework, ultimately harmonizing CIs emergency processes with command structures and data sharing with Emergency Services, thus enabling the quantification and management of resilience. In order to maintain a high level of abstraction, the technical aspects of the 3C have not been defined, except for some assumptions made in the use case scenario of Ljubljana. Progresses still need to be made in a number of topics, and operational definitions are required, e.g.: on the extension of 3C area of responsibility (national, regional, etc.); whether 3Cs are physical or logical entities; how 3C is connected to the operators; what kind of information is exchanged and in what format; how protocols, services, and operators' inter-work. The differences found among the 3Cs communications capabilities constitute a gap to overcome in order to define a future 3Cs communications network model that enables coordination irrespective of the actual crisis scenario. In the Projects terms, the 3C itself can be treated as the user of multiple critical infrastructures (the communications ones operated by the different CIs and FRs). Therefore, in line with the spirit of the Projects, we proposed and discussed an approach about how the resilience of a 3C communications infrastructure can be improved.

8.3. Challenges Specific to the Use Case Scenario

In each Scenario, proper coordination happens and is positively assessed when sensitive information is transferred in a secure way, for enabling common situational awareness. Scenario simulations can show the importance and emerging issues of information sharing and collaboration between CI. In the PPDR context, the main challenge is the establishment and maintenance of a communications framework that promotes the collaboration within each 3C. The support of the operators in the field mandates the focusing on mobile radio resources as means to support cooperation during incidents. It is common, in Europe, that each CI as well as each FR had deployed and maintains its own radio infrastructure. This situation may vary to a degree in different countries. It constitutes one of the aspects that has to be dealt with when setting the expectations for a prompt relief from a crisis. Under these premises, the discussion around the challenges to address in future, as well as the opportunity to improve the 3Cs resilience within the scenarios has highlighted some themes. The characteristics of the individual networks involved in a scenario may be largely different, because of different planning requirements. At the physical layer, the coverage might have been designed for different purposes: for specific areas, for specific minimum field strength, or for desired Quality of Service as well as Grade of Service or Level of Service. Still at physical layer, the different radio access interfaces might have been configured to provide different levels of protection of the information. In a similar way the different networks may or may not provide standardized link and routing layer. At operational level, there might be the need of specific hardware configurations, to provide case-by-case solutions to attain the interoperation between networks. The need to convey a control channel may be satisfied at different degrees by the different radio systems. At the payload level, the different grade of security of the individual networks raises concerns related to the need of confidentiality, identifiability and authenticity of the information exchanged in an inhomogeneous context of technologies. Analogously, at the control level, the interoperability during the crisis period shall not become a potential threat by flooding the channel, either intentionally or unintentionally. An additional concern has been raised with respect to the EU studies and national regulations related to the protection of CIs information. Almost all the concerns discussed have raised the interest of the ITU [60]. This Report describes the studies carried in the field of PPDR communications and confirms the outcomes within the

Projects. However, it was rather interesting that the confidentiality issue in conjunction with the control of the unwanted traffic has arisen as a specific outcome of the discussion within the Projects.

8.4. Proposed Solutions

The relevance of the Projects lies in their contribution to put in operation an approach to the general problem of resilience itself. To address the challenges posed to the 3C communications by the scenarios, the proposed way is the modelling of the 3C communications networks as a CI and therefore exploiting its testing by means of Scenarios Simulation and Demonstration. The Projects define the pathway to develop an effective Scenarios Simulation and Demonstration of 3Cs. It takes the moves from the definition of Critical Infrastructure Protection Blueprints (CPBs). CPBs are a combination of one or more AI models with all their dependencies, required libraries and application components (e.g., AI/ML libraries, data processing, streaming & analytics applications, visualization tools, etc.) necessary for their execution, extended with Quality of Service requirements (e.g., scaling policies to minimize costs and optimize execution time, expected deadlines for completion, required security and data privacy settings). Then, the joint set of CPBs and Organizational and Governance Models promoting public-private collaboration in CIs Coordination Centers can be used in Digital Twins (DTs) and Scenarios Simulation and Demonstration of 3C inhomogeneous communications networks.

8.5. Enabling Technologies

As an additional step towards the interoperability, ITU-R has promoted IMT for BB-PPDR [61]. In its studies, the proposed models take into consideration various approaches, ranging between the self-standing network, and the integration within the public network. The last opportunity foresees a sliced network, to offer services to CIs and FRs. Currently, the former opportunity (self-standing, but not IMT) is most deployed. In addition, to allow the design of proper PPDR networks, the Report [60] provides guidance both for the understanding of the requirements of PPDR, and for the key results to attain in terms of objectives and requirements of PPDR systems. These design guidelines offer the opportunity to define the CPBs required to develop both the DTs and the Scenarios Simulation and Demonstration of the 3Cs communication service. These Mobile Network DTs, and Scenarios Simulation and Demonstration would both provide elements for increasing the efficient use of the radio resources, specifically, by 3Cs (e.g., establishing the already mentioned short-term and long-term objectives and requirements that enhance resilience), and provide insight in the development of novel PPDR solutions. Then, these solutions could be modelled as CPBs to iterate the process. The Scenario Simulation and Demonstration would provide a means of testing and validating new detection and mitigation approaches in present day real-life 3Cs contexts. Scenarios Simulation and Demonstration would be used as an innovative vulnerability assessment tool for the complex multi-system cascading effects in the coordinated networks, thereby supporting focused development of new resilience enhancement services. DT models would benefit from the collection of intelligence during incidents. ML and AI Libraries could provide the analysis tools to extract additional modelling parameters (e.g., uprising of commercial traffic is a well-established phenomenon during crisis: the development of analytics of this specific kind of traffic could add instruments both in the preparation and in the recovery phase, enabling what if analysis to support coordination choices). Given the motivation for the

intelligence data collected an open data approach to their distribution could / should be considered. This opportunity adds a possible topic to be discussed in the context of confidentiality.

8.6. Insights and Discussions

From the point of view of available spectrum resources, the ECC Decision [62] provides the harmonized technical conditions and frequency bands for the implementation of Broadband Public Protection and Disaster Relief (BB-PPDR) systems in the 700 MHz and 400 MHz bands. This decision follows the outcomes of the ITU-R Res.646-2019, that indicated the range of frequencies where those services may be operated and protected. Nevertheless, as already noticed, the implementation is inhomogeneous. Additionally, it seems that, the availability of spectrum does not necessarily lead neither to the establishment of an interoperable approach among different spectrum users nor to the use of the spectrum under a common approach. Within its Radiocommunication Study Groups, ITU-R (ensuring the effective use of the radio-frequency spectrum and studies concerning development of radiocommunication systems) continues its commitment at studying the development of radiocommunications systems used in disaster mitigation/relief operations [63]. From the use cases scenarios point of view, the technology openness does not produce any valuable effect if the implementation is not interoperable, and presently, the deployed technology is deemed successful when attaining the objective of exchanging messages. The process of increasing the resilience of inhomogeneous network appears to require a regulatory approach. This intervention should consider both the proposed models for the deployment of more interoperable network and the cost of the Recurring Administrative Costs. The latter aspect is relevant, as, usually, CIs costs are only in part reduced in the view of their use for emergency purposes. As a conclusive remark, in general, the benefits of increasing resilience of 3Cs communications network by means of its architectural modelling could lead to more resilient PSN network: in fact, FRs network may benefit of CIs network, regardless of the latter involvement in a specific crisis scenario.

8.7. Conclusions

In analogy with the [64], due to the need and nature of seamless and borderless communications networks, it must be expected that PSN coordination could and should consolidate into a significant international endeavor level to the development and delivery of future and resilient networks.

As highlighted by the already mentioned publications from ITU-R, it appears unreasonable that the burden of a joint approach to the resilience of the 3C communications may be in charge of any single 3C. This appears to be true even considering National level 3C. An international effort is required. Under this provision, additional advantages may be attained at the National level, recognizing that joining the capabilities of different CI, and FR networks may be beneficial because of an availability and need coordination, rather than a register and activate coordination, under the supervision of the 3C itself.

Finally, the Simulations Scenarios and Demonstrations may offer elements to plan a real world 3C by providing simulated yet controlled performance of the abstract models.

9. Integrated Sensing and Communications for Public Safety

It is expected that over 70% of the global population will have mobile connectivity, only North America will constitute to 5 billion networked devices/connections, and internet-of-things (IoT) technology with massively connected devices will be the fastest growing mobile device category, all by 2023 [65]. The fifth generation (5G) subscriptions are estimated to reach 5 billion by 2028, and around 420 million subscriptions only in North America [66]. In order to enable anytime, anything and anywhere IoT connectivity, mobile service providers would require intelligent connectivity solutions that can deploy multi-function architectures in the next generation wireless communication standards. In situations of natural calamities such as earthquakes, volcanoes, floods, hurricanes and landslides, there is severe disruption to existing wireless infrastructure in the disaster-affected regions, and as a result, we require intelligent and multi-function solutions that can assist in disaster management effectively. Intelligent and multi-function systems such as integrated sensing and communication (ISAC) technology can enable low latency and hyper-connectivity for public safety operations, and the deployment of such multi-function cost-effective solutions can also tackle the issue of climate change.

The ISAC technology provides a highly potential solution towards efficient use of hardware and spectral resources, while decongesting the crowded sub-6 GHz spectrum currently used for most of the mobile communications. It unifies sensing and communications operations on a single hardware and use of same spectral resources, where sensing collects and extracts information, such as target detection, and using radio waves for tracking movement, while communication possesses transfer of information [67] [68]. A special case of ISAC technology is joint radar-communications (JRC) system which performs radar sensing and communication operations. The JRC systems are classified into three categories [67]: one is communication-centric JRC which implements radar sensing as the secondary function of the existing communication system, second is radar-centric JRC which integrates wireless communication as the secondary function of the existing radar system, and third is joint JRC that offers tunable trade-off between both the operations. Unlike radar-communication coexistence (RCC) systems which require effective co-ordination between radar and communication units, JRC systems perform simultaneous target detection and communication by using the same hardware and signal for both the operations.

9.1. ISAC for Public Safety: Trends and Challenges

For ISAC designs, there have been recent technical advancements in terms of achieving energy and hardware efficient systems and optimal waveform designs [69] [70] [71] [72], which are useful in carrying out fast and all-time wireless connectivity required for public safety operations. Besides energy and hardware efficient designs of JRC systems, there has been recent attention on spectral efficiency maximization [73] where interference and hardware distortion parameters are taken into account. The implementation of ISAC also addresses the fundamental challenges in realizing sustainable communications for 5G Advanced and sixth generation (6G) wireless networks, through tackling ever-increasing resource demand problems of future networks and providing efficient yet cost-effective solutions. Moreover, the ISAC technology aligns with many of the United Nations (UN)'s sustainable development goals (SDGs) such as "affordable and clean energy", "sustainable cities and communities", and "industry, innovation and infrastructure" [74].

Hybrid beamforming-based energy and hardware efficient designs incorporated with massive multiple-input multiple-output (MIMO) antenna setup can effectively achieve high degrees-of-

freedom (DoF) while achieving low-cost outcomes for ISAC transmission [75]. Such MIMO-ISAC systems, by sharing the functionalities of sensing and information communication on a single hardware, reduce the overall power consumption, system size and information exchange latency during public safety operations, especially in the response and recovery tasks of post-disaster situations. However, advanced signal processing strategies are required to truly realize the benefits and improve trade-off scenarios of MIMO-ISAC systems. Furthermore, high frequency millimeter wave (mmWave) frequencies above 30 GHz range can be deployed for ISAC systems. In the case of JRC, with few multipath components in the mmWave band, radar echo may experience less clutter interference in comparison to the sub-6 GHz bands [76]. It is expected that mmWave technology will equip favorable sensing functionality which may be applied to vehicular communication scenarios [77] [78], e.g., 77 GHz will be used for automotive radar in driverless cars which can be used to detect speed and range of objects in the vicinity of the car. Automotive radar can be categorized into short-range radar and long-range radar.

At high frequency channel modelling such as at mmWave and terahertz (THz), short-range sensing is better supported since such high frequencies are prone to high path loss, however the use of MIMO-ISAC or massive MIMO-ISAC antenna setups can overcome this issue. Nevertheless, fast and all-time global connectivity is quite crucial in public safety operations which can be enabled using dual-function ISAC technology efficiently irrespective of the channel model. In terms of the standardization, IEEE 802.11bf Wi-Fi or wireless local area network (WLAN) sensing standards are considering the specification that will turn Wi-Fi devices into object sensors to perform enhanced sensing operations in frequency bands between 1 and 7.125 GHz, and above 45 GHz [4]. In the following, we present a special case of implementing ISAC setup in a non-terrestrial network (NTN) which can assist in sensing and communication operations over a disaster-affected region.

9.2. ISAC-Assisted NTNs for Public Safety

Besides spectrum and hardware sharing in ISAC technology, NTNs such as the use of low-Earth orbit (LEO) satellites and unmanned aerial vehicles (UAVs) can truly provide anytime, anything, anywhere connectivity, where these flying platforms can act as relays and help transceivers build reliable communication links with remote areas such as over the disaster-affected regions. The overview, use cases, deployment scenarios and various architectures on 5G-envisioned NTNs are provided [79]. NTN technology has attracted significant attention in 5G research and development indicating a considerable inclusion in the future of wireless standards [80].

In terms of the Third Generation Partnership Project (3GPP) progress on evolution of the 5G technologies, there has been a recent focus on NTNs for their latest release, i.e., Release-18, which highlights satellite backhaul, UAV, IoT NTN and New Radio (NR) NTN as some of the key technology enablers for the 5G wireless standard [81]. Furthermore, 3GPP has been consistently addressing NTN related technologies as important in last releases such as Release-17 [82]. In terms of public safety operations, for instance NTNs can be used for multiple applications in disaster management including monitoring, surveillance, forecasting, early warning predictions and notifications, logistics and evacuation support, search and rescue missions, providing medical aid, and supporting infrastructure and communication systems. We consider intertwining of the NTNs with ISAC technology for fast wireless communications and effective response time, where NTNs

are equipped with dual-function ISAC capabilities which can efficiently assist in disaster management operations.

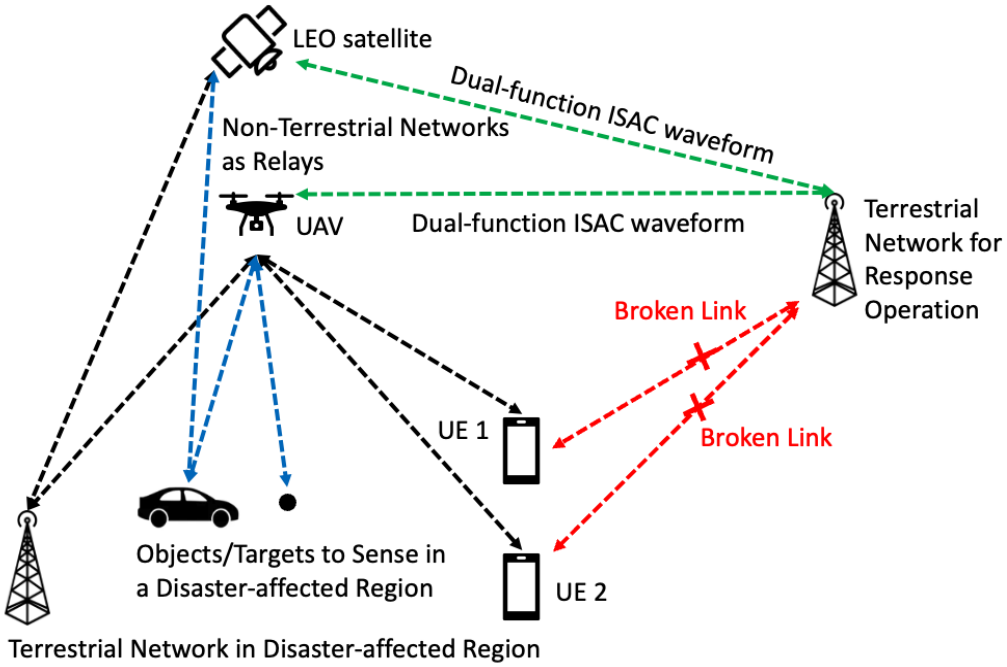

Figure 11 Illustration of ISAC-assisted NTNs for public safety operations.

Figure 11 shows a hyper-connected network of ISAC-assisted LEO satellite and UAV, which are equipped with multi-function ISAC setup that can sense objects and simultaneously communicate with the terrestrial network units in disaster-affected regions, which otherwise are unable to communicate with an external control unit responsible for response operation. NTN units, i.e., LEO satellite and UAV, equipped with ISAC can act as relays which will sense/communicate information with the terrestrial network in disaster-affected region and transmit dual-function ISAC waveform to the external control unit which can provide fast response and equally an effective connectivity since it involves sharing of both spectral and hardware resources through the ISAC-assisted NTN system.

9.3. RIS-Aided ISAC Technology

The reconfigurable intelligent surfaces (RIS) technology has attracted wide attention in communication systems, due to their low complexity and higher energy efficiency [83] [84]. RIS technology leverages smart radio surfaces with high number of small antennas or metamaterial elements based on a programmable structure that can be used to control the propagation of electromagnetic waves. The reflection of EM waves makes RIS technology highly compatible with the transceiver antenna setup which can provide high capacity and coverage while benefitting from its energy-efficient characteristics, fulfilling both public safety as well as net zero objectives. RIS can be employed in an ISAC setup for public safety, in the case of NTNs or otherwise, where dual-

function ISAC waveforms can be steered intelligently into the desired direction. There have been recent advances in RIS-assisted ISAC designs such as maximizing spectral efficiency using dynamic beamformer for the ISAC system [85] [86] [87].

In conclusion, all deployment configurations and use cases of ISAC technology such as ISAC with NTNs (UAVs and LEO satellites), reconfigurable ISAC with RIS, etc., will tend to be key technology enablers in public safety operations as well as the next generation wireless communication standards. Furthermore, the energy and hardware efficient ISAC system design will majorly contribute towards the objective of net-zero and coping up with the issue of climate change. The recent trends and benefits of implementing ISAC indicate an upwards trajectory in regard to the growth of fast and all-time wireless connectivity.

10. Communications Interoperability for Public Safety

Mutual aid between public safety agencies is frequently required when the severity or nature of an incident surpasses the ability for a local agency to respond to it. The procedures for invoking mutual aid and the way it is provided are governed by agreements between agencies. Among numerous aspects, the agreements refer to how communications equipment will be configured and how the participating agencies' responders will use the equipment to communicate with each other. Normally, the responders are arranged into talk groups, also referred to as service groups. Interoperability within and between talk groups composed of responders from different agencies is essential.

Every mode of communication, i.e., voice, video and data, is used by responders. Video and data modes allow responders to access and share information that is rich in content. However, voice remains as the de facto mode for communicating urgently among each other and with the dispatcher or the incident commander during life- or safety-critical circumstances, including when a connection to the base station is not available. Land mobile radio technology defined the push-to-talk (PTT) paradigm for how voice communications is to be conducted and continues to persist with today's mobile broadband services.

10.1. Use Case Scenario

This use case presents a scenario where responders from different public safety agencies respond to an incident and are organized according to their roles rather than the agencies to which they pertain. A complicating factor for communications interoperability is if the agencies are subscribed to different mobile network operators. This is illustrated in the figure below where responders A1, A2 and A3 are subscribed to the network operator designated as PLMN-A, and responders B1, B2 and B3 are subscribed to the network operator designated as PLMN-B. In this case the network operators have overlapping coverage of the incident area. All the firefighters, regardless of which agency they belong to, are assigned to talk group TG-1 and all the law enforcement officers are assigned to TG-2. One law enforcement officer and one firefighter are also assigned to a separate inter-service talk group, TG-3, to help coordinate the actions between the two services. Responders A3 and B3 are in a radio coverage dead-zone and are not able to attach directly to either network. However, responder A3 is in proximity to A2 and responder B3 is in proximity to A3. By virtue of the sidelink capability of their devices, they are able to connect to their respective talk TGs. When A3 or B3 re-emerge into the service area of one of the networks, their devices will attach to it. The active communications sessions are un-interrupted during the transition from off-network state to on-network state and vice-versa.

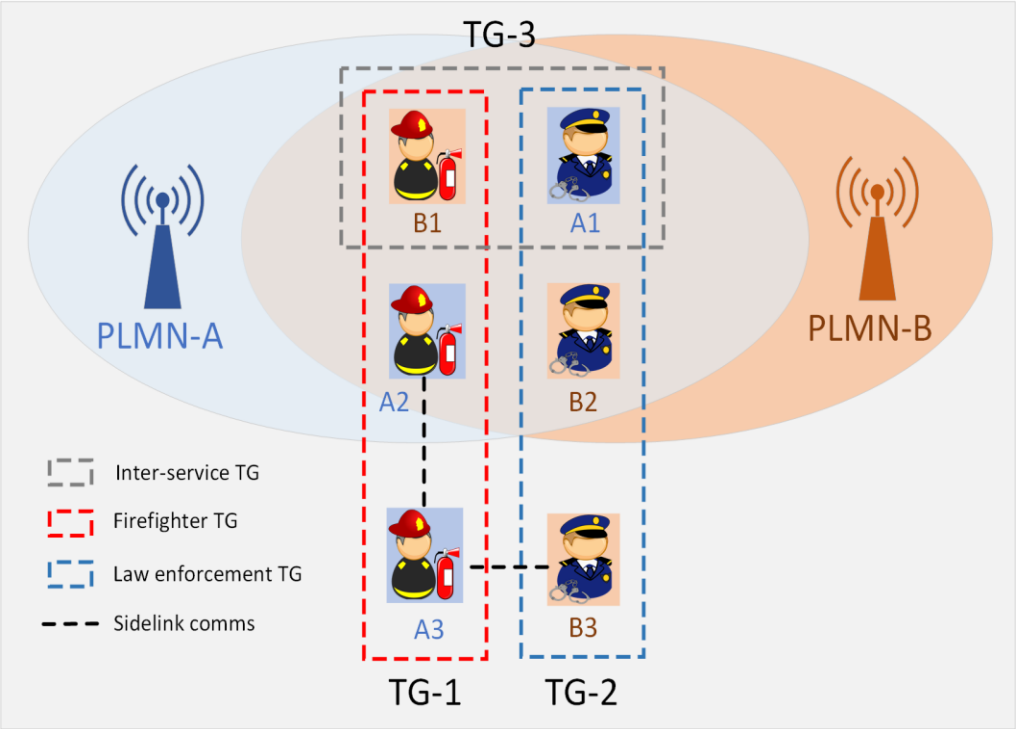

Figure 12 An example of interoperability of firefighters and law enforcement communication systems.

10.2. Preconditions and Assumptions

We list the preconditions and assumptions as follows:

- PTT communications is enabled with mobile broadband networks.
- The operators of the mobile broadband networks have implemented 5G technology.
- The public safety agencies have a mutual-aid agreement between them that establishes the principles and procedures that govern when and how to instantiate inter-agency talk groups.
- The voice communications among the responders is encrypted for confidentiality.
- The responders' devices can support direct D2D communications.

10.3. Challenges

Achieving communications interoperability among responders that pertain to different agencies entails technical and non-technical challenges. These challenges are exacerbated when the agencies are subscribed to different mobile network operators. Under these circumstances the incident commander must be able to assign responders to various talk groups on-the-fly, including those responders that are not attached to any network, but are nevertheless still reachable via devices that assume the role of device-to-network relay. Furthermore, the communications sessions must not be interrupted as the responders transit between on-network and off-network states.

Mobile network operators must configure their networks to treat public safety communications in a similar manner with regards to priority and quality of service (QoS), including the ability to pre-

empt lower priority traffic, in order to deliver a similar experience regardless of what type of device is used, what agency the responders pertain to, and which network the devices are served by. An important public safety requirement is to dynamically adapt the priority and QoS profiles as an incident unfolds and evolves. It is a challenge to enable an incident commander to adjust the configurations for end-to-end priority and QoS for responders from one agency that are subscribed to one network, let alone multiple agencies and networks.

Each participant in the incident is expected to be assigned a unique identity by the hosting network operator that will be used to determine access privileges and roles (e.g., for role-based priorities). The identities must be shared between agencies and network operators so that the participants can be assigned to various talk groups. A challenge is to ensure confidentiality of the identities of the subscribers among the network operators.

Another challenge lies in ensuring that all responders are able to communicate using encrypted sessions regardless of which agency they belong to, or which network they are subscribed to. This applies when the responders' devices are on-network as well as off-network, i.e., disconnected from any base station. It is a challenge to coordinate the configuration parameters across multiple networks and devices that belong to different agencies.

10.4. Proposed Solutions

Communications interoperability is as large a subject as communications itself. This use case focuses on a specific type of communication – one that is preferred by public safety for communicating among responders during emergencies. That is, push-to-talk voice where talk groups can be established flexibly and securely among responders that may pertain to different agencies. It is common practice in these circumstances for the hosting agency to either lend land mobile radios to the visiting agency or to configure the visiting agency's land mobile radios to be able to interoperate with the host agency. However, many public safety organizations are converging their voice communications with video and data using mobile broadband services. The challenges noted herein, as a minimum, should be addressed in order to attain that goal.

One approach to addressing some of the challenges relies on establishing partnerships between mobile broadband operators that allow MCPTT users to migrate between their networks. The public safety agencies would need to have the ability to configure the user profiles and the QoS and priority configuration levers of the network, which is not commonly permitted by mobile network operators. Therefore, there would need to be an agreement between the MNOs and the public safety agencies that allows dynamic re-configuration of QoS and priority parameters under certain conditions that would minimize the impact on the MNOs' commercial services. To this end, FirstNet in the U.S. proposed a "QoS Priority and Pre-emption Framework" [88] that examines the conditions under which QoS and priority configurations should be adapted and how that can be accomplished. But even this extra-ordinary scope of allowing public safety to access some configurable parameters of the network would only impact the access network. End-to-end QoS and priority under dynamic conditions requires real-time orchestration of service levels in the transport network as well.

A possible approach for connecting responders would be for all participating agencies to subscribe to a PTT hosting service or to an over-the-top PTT application. This would require that the public

safety agencies entrust one or more third-party application providers with critical information about their users and the security of their communications.

When a device is off-network the first step in establishing direct D2D communications with other off-network devices, or with an on-network-off-network relay node, is to discover those other devices and for itself to be discoverable by other devices. Enabling communications follows the discovery step. The configurable parameters for discovery and communications are set by the network operator.

Each approach entails advantages and disadvantages, which are examined below.

10.5. Enabling Technologies

The 3GPP has defined PTT and direct device-to-device (D2D) capabilities using 5G mobile broadband services with specifications for Mission Critical PTT (MCPTT) [2] and Proximity Services [89]. Notably, the specification for MCPTT is agnostic as to the radio access network. As such, the devices can be mobile broadband devices, referred to by the term 'User Equipment' (UE) or they can be of a different technology altogether, e.g., Wi-Fi. Therefore, there is the possibility to have MCPTT interoperability with different radio access technologies when served by 5G networks. In order for MCPTT talk groups to be established, the participating members' devices must have the MCPTT client installed on their devices which must be affiliated to an MCPTT server. The device is initially configured via a bootstrapping procedure, which includes the connection information to an MCPTT server. It should also be configured with information concerning other MCPTT servers that the devices may affiliate to. This would allow the MCPTT service to be migrated from one server to another server. An MCPTT client can only affiliate to one server at a time. As such, if a mobile network operator hosts the MCPTT service, then all the MCPTT clients must affiliate with it regardless of which agency they pertain to or which network operator they are subscribed to. Migration is made possible by implementing low-latency interconnectivity between the MCPTT servers of their respective mobile networks. If a third-party provides the interconnection service, then suitable security measures would be required.

The 3GPP proposes a model for mission-critical services – where the MCPTT services are offered by a trusted third-party MC service provider, to which the MNOs and the public safety agencies would subscribe. The MC service provider would control the application plane of the MC services, and the MNO would retain control of the signaling plane. This approach may facilitate inter-network interoperability of MCPTT but requires delegating the management of MCS user identities to the third-party. The BroadWay project's SpiceNet-HUB [90] is an example of a third-party MC service provider. The Broadway project demonstrated secure, broadband communications interconnectivity between responders from different agencies and different countries. A key objective was to achieve cross-border operational mobility providing an uninterrupted service when public safety users passed from the domain of one broadband network to the domain of another network, even between networks of different technologies or functioning in different frequency bands.

For priority and QoS, the 3GPP has proposed standardized values of 5G QoS Identifier (5QI) = 65 and 69 for MCPTT user plane and signaling traffic, respectively. 5G access identity level = 2 is proposed for mission critical services. For Wi-Fi radio access networks, the network operator should configure an Access Category, as defined by the IEEE, to provide similar priority treatment

as the 5G access network. For instance, AC_VO can be used to prioritize voice traffic on the Wi-Fi network.

Aligning 5G and 802.11 priority settings is not sufficient to ensure end-to-end priority treatment for MCPTT traffic since a transport network is most likely also part of the ecosystem. Assuming an IP-based transport, then the operator of the transport network should configure one or more Differentiated Services Code Point (DSCP) values that provide priority treatment for the MCPTT packets. The IETF [91] recommends mapping the AC_VO user traffic to Expedited Forwarding (DSCP value = 46) and signaling traffic to Class Selector 5 (DSCP value = 40). The 3GPP does not offer any recommendations for mapping 5QI values to DSCP values, instead deferring to service level agreements between operators. The GSM Association [92] offers QoS mapping guidance for IP Exchange (IPX) operators. It recommends using DSCP Assured Forwarding (DSCP value = 34) for PTT applications.

Several organizations have proposed solutions to achieving end-to-end real-time service orchestration in virtualized network environments, as in 5G networks. The TM Forum proposes the "Zero-touch Orchestration, Operations and Management (ZOOM)" network and operations management architecture that addresses the seamless interaction between physical and virtual components that can dynamically instantiate customized services and the coupling of intelligent policy management to OSS that emphasizes automation and real-time responsiveness. Real-time service orchestration using the ZOOM architecture has been demonstrated on the Géant network [93]. ETSI proposes the "Management and Orchestration (MANO)" architecture for enabling real-time instantiations of network slices in virtualized networks. Either architecture could serve as the foundation for enabling public safety to have secure and trusted access to certain sensitive network functions that affect the end-to-end QoS and priority configurations.

FirstNet proposes the implementation of a "Dynamic Controller" function in a mobile broadband network that can access information such as network utilization, user profile data and user location. The Dynamic Controller would override default settings for QoS and priority, including pre-emption capability. The Dynamic Controller could use the principles of Applications Based Network Operations [94], as described by the IETF, in order to coordinate the changes across all the implicated functions in the access and transport networks.

Some land mobile radio vendors offer over-the-top (OTT) PTT applications that work on mobile broadband devices and can interoperate with their land mobile radios. However, interoperability can only be achieved if all the devices use the same client application. Therefore, multi-vendor interoperability is lacking.

10.6. Insights and Discussions

Achieving communications interoperability requires the confluence of several technical and non-technical measures. The use case under scrutiny here describes a scenario that requires inter-agency and inter-operator interoperability. Inter-agency interoperability is predicated on the mutual aid agreements and ensuring a degree of commonality with respect to the devices that they assign to their responders. Whereas OTT applications can provide interoperability between LMR and mobile broadband network devices, OTT falls short on inter-agency interoperability due to its dependency on which vendors the agencies choose. The 3GPP -based MCPTT solution is anchored on industry-accepted standards. Thus, there is less dependency on the vendor, but the agencies

need to ensure that their devices are configured to support the MCPTT standards. Inter-operator interoperability is more difficult to achieve. Although the 3GPP standards provide a possible path towards achieving interconnectivity, MNOs must trust each other with commercially sensitive information such as the identities of each other's public safety subscribers. Expecting this level of trust between commercial competitors may be unfeasible as is evidenced by the lack of MCPTT interoperability between subscribers of FirstNet and Verizon Wireless in the U.S. [95]. Perhaps in anticipation of this possibility, the 3GPP proposed an implementation model that introduces a third-party mission-critical services service provider to which the mobile network operators would delegate the identity management and key management functions. The MNOs would still be required to implement certain MC server functions within their networks. A successful demonstration of inter-operator MCPTT "operational mobility" was achieved by the Broadway project. A key lesson from the project is that interoperability is predicated on business relationships between the participating service delivery entities and the entity that hosts common MC services.

Maintaining connectivity is an essential prerequisite to interoperability, but achieving a familiar quality of experience, regardless of which is the serving network, is also an important ingredient for interoperability. The quality of experience is underpinned by how the network responds to the user under various conditions. For example, when a user initiates an emergency call or signals "imminent peril", those events should be treated with high priority at any time and at any location. Therefore, the MNOs need to align their priority and QoS policies, including an equivalent configuration of the transport networks. By having standards already defined for MCPTT traffic, the MNOs can independently adhere to them. The only known instance where a mobile network operator allows one of its subscriber communities to dynamically adjust QoS and priority configurations of its network is AT&T allowing FirstNet to selectively elevate the priority level of responders to a pre-determined state during an event. The impact is limited to the local access network since there is no consideration for inter-operator interoperability. To apply the same principle to an end-to-end MCPTT service using software-defined instantiations of virtualized functions would require real-time orchestration and life-cycle service management that would need to account for impacts on other services and subscribers.

10.7. Conclusions

It is common for public safety agencies to assist each other when the severity of an event surpasses the ability for any one agency to respond adequately. During these events it is essential that the responders from all the implicated agencies are able to communicate with each other. Hence, the devices that the responders use must be able to interoperate. An important mode of communications used by responders is by voice using PTT, also referred to as MCPTT to emphasize this vital capability. The 3GPP standards provide a way to achieve interconnectivity for devices of different access technologies, when devices migrate between networks and when devices are off-network. The standards also propose an implementation model where a third-party service provider undertakes the role of providing mission-critical services to public safety agencies on behalf of subscribing mobile network operators.

Maintaining connectivity under different and changing conditions is a necessary prerequisite for interoperability but is not sufficient. Interoperability also implies that the responders are familiar with the MCPTT service and as such, they expect a consistent quality of experience regardless of which mobile network operator is the serving network. When MCPTT traffic traverses more than

one network the notion of end-to-end QoS applies. Therefore, the configurable points of all the networks that carry the traffic must be provisioned to process it in a similar manner and the functions that orchestrate the MCPTT service must span all the implicated technologies. In 5G networks, an MCPTT service may be instantiated as a network slice using virtualized network functions. The TM Forum and ETSI, among other standards organizations, propose operations, management and service orchestration architectures for such networks with real-time responsiveness.

At the time of writing, there is no known implementation of an MCPTT service that is interoperable between networks that encompasses, persistent connectivity for on-network and off-network states, dynamically adaptable end-to-end QoS and priority, and real-time service orchestration in a virtualized environment. However, elements of a solution exist, and some have been demonstrated.

11. STANDARDIZATION LANDSCAPE

Standards organizations including ANSI, IEEE, ITU, and 3GPP have been contributing immensely towards the developing standards for communications and networking. However, industry lacks communications and standards for public safety applications. This whitepaper provides a foundation for such activity.

12. CONCLUSIONS AND RECOMMENDATIONS

This whitepaper is focused on the need for communications and networking applications for public safety. The ten use cases presented in this whitepaper is a collective effort from the subcommittee on “communications and networking” established by the IEEE Public Safety Technology Initiative. It is intended to promote research, development, education, outreach, and industry standards in the IEEE community and beyond.

13. REFERENCES

[1] *Federal Emergency Management Agency. Robert T. Stafford disaster relief and emergency assistance act, as amended, and related authorities, 2007. http://www.fema.gov/about/stafact.shtm.*

[2] *FCC. Katrina panel report and recommendations, 2006.http://transition.fcc.gov/pshs/advisory/hkip/index.html.*

[3] *Federal Emergency Management Agency. Homeland security exercise and evaluation program, 2013. http://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.*

[4] *Texas Task Force 1. Urban search and rescue response system, 2014. http://usar.tamu.edu/Pages/Default.aspx.*

[5] *Department of Homeland Security. S&T pilot aimed at improving first responder situational awareness, 2015. https://www.dhs.gov/science-and-technology/frg-iot-pilot.*

[6] *Federal Emergency Management Agency. Whole community concept, 2010. http://www.fema.gov/whole-community.*

[7] *The IEEE Public Safety Technology Task Force. Public safety technology gaps and opportunities. https://publicsafety.ieee.org/publications, May 2021.*

[8] *3GPP TS 23.501, "System architecture for the 5G System (5GS)," V17.3.0, 2021-12.*

[9] *A. N. Steinberg and C. L. Bowman, "Revisions to the JDL Data Fusion Model," in Handbook of Multisensor Data Fusion, Second Edition: Theory and Practice, 2 ed., J. Llinas, D. L. Hall and M. E. Liggins, Eds., CRC Press, 2009, pp. 45-67.*

[10] *U.S. Dapertment of Homeland Security - Science and Technology Directorate, "DHS S&T Selects Georgia Tech Group to Improve Info Sharing & Safeguarding for Public Safety Comms," 21 January 2020. [Online]. Available: https://www.dhs.gov/science-and-technolog.*

[11] *Yang L, Meng F, Zhang J, Hasna MO, Renzo MD (2020) On the performance of RIS-assisted dual-hop UAV communication systems. IEEE Trans. Veh. Technol. 69(9):10 385–10 390.*

[12] *Li S, Duo B, Yuan X, Liang Y-C, Di Renzo M (2020) Reconfigurable intelligent surface assisted UAV communication: joint trajectory design and passive beamforming. IEEE Wireless Commun. Lett. 9(5):716–720.*

[13] *Li J, Liu J (2020) Sum rate maximization via reconfigurable intelligent surface in UAV communication: phase shift and trajectory optimization. In: Proc. IEEE/CIC Int. Conf. Commun. in China (ICCC), pp 124–129.*

[14] *Jiang L, Jafarkhani H (2021) Reconfigurable intelligent surface assisted mmwave UAV wireless cellular networks. In: Pro. IEEE Int. Conf. Commun. (ICC), pp 1–6.*

[15] *Li S, Duo B, Di Renzo M, Tao M, Yuan X (2021) Robust secure UAV communications with the aid of reconfigurable intelligent surfaces. IEEE Trans. Wireless Commun., 20(10):6402-6417.*

[16] *Alfattani S, Jaafar W, Hmamouche Y, Yanikomeroglu H, Yongaçoglu A (2021) Link budget analysis for reconfigurable smart surfaces in aerial platforms. IEEE Open J. Commun. Soc. 2:1980-1995.*

[17] *Mursia P, Devoti F, Sciancalepore V, Costa-Pérez X (2021) RISe of flight: RIS-empowered UAV communications for robust and reliable air-to-ground networks. IEEE Open J. Commun. Soc. 2:1616–1629.*

[18] *Tang X,Wang D, Zhang R, Chu Z, Han Z (2021) Jamming mitigation via aerial reconfigurable intelligent surface: passive beamforming and deployment optimization. IEEE Trans. Veh. Technol. 70(6):6232–6237.*

[19] *Long H, Chen M, Yang Z,Wang B, Li Z, Yun X, Shikh-Bahaei M (2020) Reflections in the sky: joint trajectory and passive beamforming design for secure UAV networks with reconfigurable intelligent surface. In: Proc. IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, 1-6.*

[20] *O-RAN Use Cases and Deployment Scenarios, https://www.o-ran.org/resources.*

[21] *GSMA Generic Network Slice Template, https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v8.0-1.pdf.*

[22] *O-RAN.WG1.Slicing-Architecture, https://orandownloadsweb.azurewebsites.net/specifications.*

[23] *Near-Real-time RAN Intelligent Controller E2 Service Model (E2SM), RAN Control, https://orandownloadsweb.azurewebsites.net/specifications.*

[24] *R. Avanzi et al., "CRYSTALS–Kyber: Algorithm Specification and Supporting Documentation.", NISTPQC Round, 2019, 2(4).*

[25] *S. Bai et al., "CRYSTALS–Dilithium: Algorithm Specification and Supporting Documentation." 2021.*

[26] *V. Belle and I. Papantonis, "Principles and practice of explainable machine learning," Frontiers in Big Data, vol. 4, 2021.*

[27] *M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, Physical Layer Security: Authentication, Integrity, and Confidentiality. Cham: Springer International Publishing, 2021, pp. 129–15.*

[28] *3GPP (2022), Technical Report TR 22.837, "Study on Integrated Sensing and Communication", www.3gpp.org.*

[29] *S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, "Guaranteeing spoof-resilient multi-robot networks," Autonomous Robots, vol. 41, pp. 1383–1400, 201.*

[30] *G. Baldini, S. Karanasios, D. Allen and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety," in IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 619-641, Second Quarter 2014, doi: 10.1109/SURV.2013.082713.00034.*

[31] *Carneiro de Souza L, de Souza Lopes CH, de Cassia Carlleti dos Santos R, Cerqueira Sodré Junior A and Mendes LL (2022) A Study on Propagation Models for 60 GHz Signals in Indoor Environments. Front. Comms. Net 2:757842. doi: 10.3389/frcmn.2021.757842.*

[32] *Xia, K. et al. (2018) Painting a high-output triboelectric nanogenerator on paper for harvesting energy from human body motion. Nano Energy 50, 571–580.*

[33] *Mondal, S., Paul, T., Maiti, S., Das, B. K. & Chattopadhyay, K. K. (2020) Human motion interactive mechanical energy harvester based on all inorganic perovskite- PVDF. Nano Energy 74, 104870.*

[34] *Nozariasbmarz, A. et al. (2020) Review of wearable thermoelectric energy harvesting: from body temperature to electronic systems. Appl. Energy 258, 114069.*

[35] *Hashemi, S. A., Ramakrishna, S. & Aberle, A. G. (2020) Recent progress in flexible-wearable solar cells for self-powered electronic devices. Energy Environ. Sci. 13, 685–743.*

[36] *Bandodkar, A. et al. (2017) Soft, stretchable, high power density electronic skin- based biofuel cells for scavenging energy from human sweat. Energy Environ. Sci. 10, 1581–1589.*

[37] *D. Darsena, G. Gelli and F. Verde (2017) Modeling and Performance Analysis of Wireless Networks with Ambient Backscatter Devices," in IEEE Trans. Commun., 65(4) 1797-1814.*

[38] *D. Darsena, G. Gelli and F. Verde (2019) Cloud-Aided Cognitive Ambient Backscatter Wireless Sensor Networks," in IEEE Access, 7:57399-57414.*

[39] *N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang and D. I. Kim (2018) Ambient Backscatter Communications: A Contemporary Survey," in IEEE Commun. Surv. Tuts., 20(4) 2889-2922.*

[40] *M.H. Ullah, G. Gelli, F. Verde (2022) Visible light backscattering with applications to communication and localization in healthcare: A survey," in Procedia Compu. Sci., 203:745-752.*

[41] *V. Talla, J. Smith, and S. Gollakota (2020) Advances and Open Problems in Backscatter Networking, GetMobile: Mobile Comp. and Comm. 24(4)32–38.*

[42] *J. Kimionis, A. Georgiadis and M. M. Tentzeris (2017) Millimeter-wave backscatter: A quantum leap for gigabit communication, RF sensing, and wearables, In: Proc. IEEE MTT-S Int. Microw.*

Symp. (IMS), Honololu, HI, USA, 812-815.

[43] *Dev, K., Khowaja, S.A., Sharma, P.K., Chowdhry, B.S., Tanwar, S. and Fortino, G., (2022) DDI: A novel architecture for joint active user detection and IoT device identification in grant-free NOMA systems for 6G and beyond networks, IEEE IoT J. 9(4)2906-2917.*

[44] *Khowaja, S.A., Dev, K., Khuwaja, P., Pham, Q.V., Qureshi, N.M.F., Bellavista, P. and Magarini, M. (2022) IIFNet: A Fusion-Based Intelligent Service for Noisy Preamble Detection in 6G, IEEE Netw., 36(3)48-54.*

[45] *Li, J., Nagalapur, K.K., Stare, E., Dwivedi, S., Ashraf, S.A., Eriksson, P.E., Engström, U., Lee, W.H. and Lohmar, T., (2022 5G New Radio for public safety mission critical communications, IEEE Commun. Stand. Mag. 6(4) 48-55.*

[46] *Khowaja, S.A., Dev, K., Qureshi, N.M.F., Khuwaja, P. and Foschini, L. (2022) Toward industrial private AI: A two-tier framework for data and model security, IEEE Wireless Commun. 29(2) 76-83.*

[47] *Khowaja, S.A., Lee, I.H., Dev, K., Jarwar, M.A. and Qureshi, N.M.F. (2022) Get your foes fooled: Proximal gradient split learning for defense against model inversion attacks on IoMT data, IEEE Trans. Netw. Sci. and Engineer.*

[48] *Lauter, K. (2022) Private AI: machine learning on encrypted data. In Recent Advances in Industrial and Applied Mathematics, Springer International Publishing, 97-113.*

[49] *Silva, F., Rosa, P., Hrasnica, H. and Gravas, A. (2019) 5GINFIRE: Enabling an NFV based experimentation of vertical industries in the 5G context. In Anais do X Workshop de Pesquisa Experimental da Internet do Futuro, 64-69.*

[50] *Volk, M. and Sterle, J., 2021. 5G experimentation for public safety: Technologies, facilities and use cases. IEEE Access, 9:41184-41217.*

[51] *Khowaja, S.A., Prabono, A.G., Setiawan, F., Yahya, B.N. and Lee, S.L. (2018) Contextual activity based Healthcare Internet of Things, Services, and People (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors. Computer Netw.*

[52] *Suomalainen, J., Julku, J., Vehkaperä, M. and Posti, H. (2021) Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. IEEE Op.*

J. of the Commun. Soc., 2:1590-1615.

[53] *Deebak, B.D., Memon, F.H., Khowaja, S.A., Dev, K., Wang, W., Qureshi, N.M.F. and Su, C. (2022) Lightweight blockchain based remote mutual authentication for AI-empowered IoT sustainable computing systems. IEEE IoT J..*

[54] *Khowaja, S.A., Khuwaja, P., Dev, K. and Antonopoulos, A., 2022. SPIN: Simulated Poisoning and Inversion Network for Federated Learning-Based 6G Vehicular Networks, arXiv preprint arXiv:2211.11321.*

[55] *Zhu, L., Liu, Z. and Han, S. (2019) Deep leakage from gradients. Advances in neural information processing systems, 32.*

[56] *Zhao, B., Mopuri, K.R. and Bilen, H., (2020) IDLG: Improved deep leakage from gradients, arXiv preprint arXiv:2001.02610.*

[57] *96/82/EC, Council Directive of 9 December 1996 on the control of major-accident hazards involving dangerous substances (EU Seveso-II Directive).*

[58] *2008/114/EC, Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.*

[59] *Soroudi, M., Ko, I., Gordan, M., & McCrum, D. (2022) A Sustainable GIS-Based Serious Game Approach to Improve Railways Resilience.*

[60] *ITU-R (2017) Report M.2237-1 Radiocommunication objectives and requirements for Public Protection and Disaster Relief. Nov. 2017, M Series - Mobile, radiodetermination, amateur and related satellite services.*

[61] *ITU-R (2021) Report M.2291-2 The use of International Mobile Telecommunications (IMT) for broadband Public Protection and Disaster Relief (PPDR) applications. Dec. 2021, M Series - Mobile, radiodetermination, amateur and related satellite services.*

[62] *16(02), ECC Decision. On harmonised technical conditions and frequency bands for the implementation of broadband public protection and disaster relief (BB-PPDR) systems.*

[63] *ITU-R (2019) Res.55-3 Studies of disaster prediction, detection, mitigation and relief. 2019.*

[64] *ITU-T (2020) Network 2030 a blueprint of technology, applications and market drivers towards the year 2030 and beyond.*

[65] *Cisco Annual Internet Report 2018-23 White Paper, (2020) [Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html].*

[66] *Ericsson Mobility Report 2022 (2022), 1-40, [Available: https://www.ericsson.com/4ae28d/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-november-2022.pdf].*

[67] *J. A. Zhang et al., (2021) An Overview of Signal Processing Techniques for Joint Communication and Radar Sensing, IEEE J. of Select. Top. in Sig. Process. 15(6)1295-1315.*

[68] *J. Wang et al. (2022) Integrated Sensing and Communication: Enabling Techniques, Applications, Tools and Data Sets, Standardization, and Future Directions," IEEE IoT J. 9(23) 23416-23440.*

[69] *O. Dizdar et al. (2022), Energy efficient dual-functional radar-communication: Rate splitting multiple access, low-resolution DACs, and RF chain selection, IEEE Op. J. of the Commun. Soc. 3:986-1006.*

[70] *A. Kaushik et al. (2021), Hardware efficient joint radar-communications with hybrid precoding and RF chain optimization, Proc. IEEE Int. Conf. Commun. (ICC) 1-6.*

[71] *A. Kaushik et al (2022), Green joint radar-communications: RF selection with low resolution DACs and hybrid precoding, Proc. IEEE Int. Conf. Commun. (ICC), 1-6.*

[72] *A. Kaushik et al. (2022), Waveform design for joint-radar communications with low complexity analog components, Proc. IEEE Int. Symp. Joint Commun. and Sens. 1-5.*

[73] *A. Kaushik et al. (2022), Towards 6G: Spectrally efficient joint radar and communication with RF selection, interference and hardware impairments, IET Sig. Process. 16(7) 851-863.*

[74] *UN's sustainable development goals (SDGs). [Available: https://sdgs.un.org/goals].*

[75] *E. Vlachos and A. Kaushik (2023), Covariance-based hybrid beamforming for spectrally efficient joint radar-communications, Proc. IEEE Int. Conf. Commun. (ICC), 1-6.*

[76] *H. Wymeersch et al. (2017), 5G mmWave positioning for vehicular networks, IEEE Wireless Commun., 24(6) 80-86.*

[77] *J. A. Zhang et al. (2019), Multibeam for joint communication and radar sensing using steerable analog antenna arrays, IEEE Trans. Veh. Technol. 68(1) 671-685.*

[78] *S. H. Dokhanchi et al. (2019), A mmWave automotive joint radar-communications system, IEEE Trans. Aeros. and Electro. Syst. 55(3)1241-1260.*

[79] *5G Americas White Paper: 5G & Non-Terrestrial Networks (2022), 1-35 [Available:https://www .5gamericas.org/wp-content/uploads/2022/01/5G-Non-Terrestrial-Networks-2022-WP-Id.pdf].*

[80] *A. Kaushik and M. Z. Shakir (2022) Non-Terrestrial Networks: Have We Found that Ultimate Catalyst for Global Connectivity in 6G?, IEEE ComSoc Technol. News (CTN).*

[81] *3GPP Release 18 [Available: https://www.3gpp.org/specifications-technologies/releases/release-18].*

[82] *3GPP Release 17 [Available: https://www.3gpp.org/specifications-technologies/releases/release-17].*

[83] *M. Di Renzo et al. (2022), Communication models for reconfigurable intelligent surfaces: From surface electromagnetics to wireless networks optimization, Proceed. of the IEEE, 110(9) 1164-1209.*

[84] *R. Singh et al. (2024), Indexed multiple access with reconfigurable intelligent surfaces: The reflection tuning potential, IEEE Commun. Mag. 62(4)120-126.*

[85] *X. Wang, et al. (2021), RIS-assisted spectrum sharing between MIMO radar and MU-MISO communication systems, IEEE Wireless Commun. Lett. 10(3)594-598.*

[86] *E. Vlachos and A. Kaushik (2023), Subset selection based RIS-aided beamforming for joint radar-communications, Proc. IEEE Wireless Commun. Network. Conf. Wrkshp., 1-6.*

[87] *Y. Li and A. Petropulu (2022), Dual-function radar-communication system aided by intelligent reflecting surfaces, Proc. IEEE Sensor Array and Multichanne Sig. Process. Wrkshp (SAM), 126-130.*

[88] *FirstNet, CTO Whitepaper (2015), Nationwide Public Safety Broadband Network (NPSBN) QoS Priority and Preemption (QPP) Framework, Version 0.9 draft, 18 Nov. 2015.*

[89] *3GPP TS 23.304, Proximity based Services (ProSe) in the 5G System.*

[90] *Broadway, SpiceNet Reference Architecture, [Available: https://www.broadway-info.eu/spicenet/].*

[91] *IETF, RFC 8325 (2018), Mapping Diffserv to IEEE 802.11.*

[92] *GSM Association (2021), IR.34, V 17.0, 18 May 2021.*

[93] *J. Sobieski and I. Golub (2018), Deliverable D8.8 Integrated Services Framework and Network Services Development Roadmap – Follow-Up, GÉANT Assoc.*

[94] *IETF, RFC 7491 (Informational) (2018), A PCE-Based Architecture for Application-Based Network Operations.*

[95] *Mission Critical Communications (2018), Colorado Group Asks FCC to Ensure FirstNet Supports Interoperability, [Available: https://www.rrmediagroup.com/Features/FeaturesDetails/FID/854].*

14. COMMITTEE MEMBERS AND CONTRIBUTORS

1. Kamesh Namuduri (Lead)
2. Periklis Chatzimisios (Lead)
3. Wael Jaafar (Lead)
4. Abbas Omar
5. Aishwarya Roy
6. Anastasios Papazafeiropoulos
7. Arsenia (Ersi) Chorti
8. Aryan Kaushik
9. Claudio Lucente
10. Cristiano Passerini
11. David Moura
12. Donatella Darsena
13. Abbas Omar
14. Eapen Kuruvilla
15. Fabrizio Granelli
16. Fernando Luis
17. Hichan Moon
18. Iwan Adhicandra
19. Jiang (Linda) Xie
20. Jinwei Liu
21. Kapal Dev
22. Kaustubh Ranjan Singh
23. Ko Chung Wong
24. Lincoln Unruh
25. Luc Samson
26. Nitin Gupta
27. Paul Spicer
28. Peter Zidar
29. Ranga Rao Venkatesha Prasad
30. Saim Ghafoor
31. Sunder Ali Khowaja
32. Tamara Hadjina
33. Tariq Umer
34. Tom Henderson
35. Vladimir Orlic
36. Yasir Saleem