IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 September 2022, accepted 16 October 2022, date of publication 26 October 2022, date of current version 10 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3217223

SURVEY

A Survey on Security Approaches on PPDR Systems Toward 5G and Beyond

FLORIANO NETO, JORGE GRANJAL, (Member, IEEE), AND VASCO PEREIRA
CISUC, Department of Informatics Engineering, University of Coimbra, 3030-290 Coimbra, Portugal

Corresponding author: Floriano Neto (fdneto@dei.uc.pt)

This work was supported by the FCT—Foundation for Science and Technology, I.P./MCTES, through the National Funds (PIDDAC) through CISUC Research and Development Unit under Grant UIDB/00326/2020 and Grant UIDP/00326/2020.

ABSTRACT The present survey seeks to contribute to the existing discussion about the changing of current Public Protection and Disaster Relief (PPDR) networks (TETRA, TETRAPOL, P25, and DMR) to commercial cellular networks (4G and 5G). The availability and robustness of these commercial networks are challenging current PPDR networks and creating opportunities for a successful transition of existing systems to commercial cellular networks. Specifically, 5G networks aim to support a massive number of heterogeneous devices while providing ultra-reliable low latency communications, higher mobility, and the capability of customised support of applications via network slicing, thus providing a natural contribution to mission critical systems. This survey details the essential mission requirements of security of PPDR systems, describes the state of the art of the most used technologies and discusses their evolution to 4G and 5G cellular networks. Furthermore, it analyses future research directions that may contribute to a successful transition of current systems to the newer cellular networks.

INDEX TERMS 4G, 5G, DMR, LTE, P25, PPDR, public safety, security, TETRA, TETRAPOL.

I. INTRODUCTION

The Public Protection Disaster Relief (PPDR) agencies play a very significant role in society. Their main purposes are to maintain law and order, protect life and property, and respond to emergencies. Notwithstanding, in disaster relief situations, their objective is also to respond to catastrophes that endanger human life, society, or the environment [1]. Due to specific operation scenarios, PPDR operations demand mission-critical systems, where every component must always be available, operating continuously and uninterrupted. Security services have a vital role in this scenario, assuring the authenticity, confidentiality, and integrity of these networks' critical information. Historically, public safety organisations such as police, firefighters, and emergency services, have been using Land Mobile Radio (LMR) systems to support mission-critical voice communications. LMR systems are professional push to talk systems. They typically consisted of mobile radios, fixed base stations, and supporting network infrastructure. which provided a two-way radio communication system that allows users, who share the same range of frequencies, to communicate. These systems migrated from the original basic analogue systems to digital systems that supported voice and data and ultimately to digital trunked systems. While the first digital systems required manual selection of channels that were exclusively used by a group of users continuously during a critical event, trunked systems allow for the sharing of media, with automatic assignment of frequency channels, providing more efficient use of the available spectrum. Many digital trunked radio technologies were launched in the market, such as Terrestrial Trunked Radio (TETRA), TETRAPOL, Project 25 (P25), and Digital Mobile Radio (DMR) [2]. These systems proved sufficient to fulfil initial PPDR requirements, which focused on voice services and valued the availability, security, and reliability of calls. However, the demand for enhanced data services required by today's public safety first responders requires new approaches. The new requirements include access to data from several sources, including database access and real time video streaming, sensor

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

data collection, and Internet of Things (IoT) device management. PPDR agencies pursued the Long-Term Evolution (LTE), commercially called 4G or 4G LTE, to the transition. The initial goal was to pair existing narrowband LMR networks for voice with broadband networks for high speed data before transitioning to an entire LTE network. However, due to the specific needs of public safety agencies, the support of mission-critical services over 4G presented several technical challenges [3]. These challenges included spectrum coverage, service availability, prioritised communication, and interoperability. Some of these handicaps have already been addressed by 3rd Generation Partnership Project (3GPP), and there were initiatives to enable the transition from current PPDR networks to commercial 4G broadband networks around the world. The introduction of the 5th generation of cellular networks (5G), will further enhance critical services support, featuring the possibility of having many heterogeneous devices, ultra-reliable low latency communications, and higher mobility, combined with the capability of customised support of application requirements via network slicing. All these characteristics resulted in an increasing interest from PPDR agencies in the transition to cellular networks [4]. As current PPDR systems have voice services as a priority, the security of these systems was focused on mechanisms such as mutual authentication, air interface encryption, and end-to-end encryption, not correctly addressing the security of data communications. With the introduction of 4G commercial networks in PPDR environments, data security emerges as a solid aspect to be considered in response to the increased number of services that use data communications. The introduction of 5G with support for mission critical systems further extends the security concerns. To deal with a greater volume of data, potentiated by the higher transmission rates and an exponential increase in devices, security aspects such as privacy and reliability become critical. Some security features are already included in 5G, but further research on security mechanisms is required. This survey presents the state of the art of current PPDR systems and details the requirements for the next generation, focusing on communications security. Current technologies included in current standards (usually closed patterns) are compared to new security technologies included in 4G and 5G to provide a critical comparison and provide insights on the viability of the transition from PPDR systems to these new networks. The main contributions of this survey are:

- A description of the evolution of requirements of mission-critical PPDR systems, with a special focus on security requirements;
- A review of the state of the art of PPDR systems, including their standards and security services, addressing the most used LMR systems: TETRA, TETRAPOL, P25, and DMR;
- Analysis of the transition from current systems to cellular networks, focusing on their security requirements and challenges;
- Analysis of what has been done to implement PPDR systems in 4G networks and what are the possibilities that 5G provides;
- A comparison between 4G and 5G security proposals for PPDR systems;
- A discussion on the future research directions needed to fulfill the security requirements of future PPDR systems.

How we find at the moment, our survey is the first with the goal of analysing PPDR systems in the light of mission-critical requirements, in the context of the transition from legacy PPRD network towards commercial 4G and 5G communication environments.

The remainder of the paper is organised as follows: Chapter II introduces the security requirements of mission-critical and PPDR systems. Chapter III presents the state of the art of the current PPDR systems: TETRA, TETRAPOL, P25, and DMR. In addition, it describes the services and security mechanisms of each system. Chapter IV analyses the transition from current PPDR systems to 4G cellular networks and introduces 5G and its benefits to PPDR systems. Also, it compares 4G to 5G in their provided security. Chapter V discusses future resource directions concerning security in PPDR systems based on 4G and 5G networks, and finally, Chapter VI concludes the paper.

All the acronyms used in the paper are enlisted in Table 1.

II. SECURITY REQUIREMENTS OF PPDR SYSTEMS

The 3GPP TR 22.862 [8] includes PPDR systems in mission-critical services. Their description is defined with an operation of first responders, classified as ''Ultra-reliable communications''. To enable services requiring this communication, a minimum level of reliability and latency is required to guarantee the user experience or initially enable the critical service. According to 3GPP, Mission-critical communication services require preferential handling when compared to normal telecommunication services. Public Safety requires preferential handling of its traffic and the ability to support dynamic allocation of quality of service, priority, and pre-emption parameters.

However, the main concern and a critical requirement for the transition of current PPDR communications to commercial networks is the traffic disputed between a typical cell phone user and a PPDR agent. For example, in an emergency, such as a fire, a firefighter cannot have the message or call interrupted or delayed by a typical user. For this reason, there is a need to prioritise PPDR voice and data communications over commercial networks.

Furthermore, the preferential access based on 4G networks is approached in Multimedia Priority Service (MPS) specified by 3GPP in ''Enhancements for Multimedia Priority Service'' [43]. According to the standard, the decision on the appropriate settings of an Evolved Packet System (EPS) bearer's Quality of Service (QoS) parameters, such as Access Class (AC), Aggregate Maximum Bit Rate (AMBR), Quality of Quality of Service Class Identifier (QCI), Guaranteed Bit Rate (GBR), Allocation and Retention Priority (ARP), and

TABLE 1. Acronyms used in the paper.

Acronyms	definition
3GPP	3rd Generation Partnership Project
AC	Access Class
AF	Application Function
AIE	Air Interface Encryption
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
ANSI	American National Standards Institute
APCO	Association of Public Safety Communications Officers
ARP	Allocation and Retention Priority
AUSF	Authentication Server Function
BS	Base Station
DMO	Direct Mode Operation
DMR	Digital Mobile Radio
DN	Data Network
DSCP	Differentiated Services Code Point
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
eMBB	Enhanced Mobile Broadband
eNB	Evolved NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
FP7	Framework Program 7
FS	Fixed Station
GBR	Guaranteed Bit Rate
GEK	Group Encryption Key
IIoT	Industrial Internet of Things
IoLST	Internet of Life-Saving Things
IoT	Internet of Things
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
KEK	Key-Encryption Key
KFD	Key Fill Device
KMF	Key Management Facility
KVL	Key Variable Loader
LBT	Listen Before Talk
LMR	Land Mobile Radio
LS	Line Station
LT	Line Termination
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCVideo	Mission Critical Video
MDBV	Maximum Data Burst Volume
MDT	Mobile Data Terminal
MFBR	Maximum Flow Bit Rate
MoU	Memorandum of Understanding
MPS	Multimedia Priority Service
MRs	Mobile Radios
MS	Mobile Station
MT	Mobile Termination
NAS	Non-Access Stratum
NFV	Network Function Virtualization
NGMN	Next-Generation Mobile Network
NR	New Radio
NR-U	New Radio Unlicensed
NSSF	Network Slice Selection Function
OTAR	Over-The-Air Rekeying
P25	Project 25
PABX	Private Automatic Branch Exchange
PCF	Policy Control Function
PDN	Public Data Networks
PDO	Packet Data Optimized
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PPDR	Public Protection Disaster Relief
ProSe	Proximity-Based Services
PSTN	Public Switched Telephone Network
QCI	Quality of Service Class Identifier
QFI	Quality of Service Flow ID
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RT	Radio Terminal
SAGE	Security Algorithm Group of Experts
SDN	Software-Defined Networking
SDR	Software Defined Radio
SDS	Short Data Service
SIM	Subscriber Identity Module
SMF	Session Management Function
SSC	Security Service Chaining
ST	System Terminal
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SwMI	Switching and Management Infrastructure
TAAs	TETRA Authentication Algorithms
TE	Terminal Equipment
TEI	TETRA Equipment Identity
TETRA	Terrestrial Trunked Radio
TIA	Telecommunications Industry Association
TSCC	Trunk Station Control Channel
UDM	Unified Data Management
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
URC	Ultra-Reliable Communication
URLLC	Ultra-reliable and Low Latency Communications
UTRA	Universal Terrestrial Radio Access
V2X	Vehicle-to-Everything

TABLE 2. QoS parameters. (Adapted from 3GPP TS 23.203 [44].)

QCI	Resource Type	Priority Level	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100 ms	10^{-2}	Conversational voice
2		4	150 ms	10^{-3}	Conversational video (Live streaming)
3		3	50 ms	10^{-3}	Real-time gaming, V2X messages
4		5	300 ms	10^{-6}	Non-conversational video (Buffered streaming)
65		0.7	75 ms	10^{-2}	Mission critical user plane Push-to-talk voice (e.g., MCPTT)
66		2	100 ms	10^{-2}	Non-Mission critical user plane Push-to-talk voice
75		2.5	50 ms	10^{-2}	V2X messages
5	Non-GBR	1	100 ms	10^{-6}	IMS signalling
6		6	300 ms	10^{-6}	Video (Buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p, file sharing, progressive video)
7		7	100 ms	10^{-3}	Voice, Video (Live streaming), Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p, file sharing, progressive video)
9		9			
69		0.5	60 ms	10^{-6}	Mission critical delay sensitive signalling (e.g., MC-PTT signalling)
70		5.5	200 ms	10^{-6}	Mission critical data (example services are the same as QCI 6/8/9)
79		6.5	50 ms	10^{-2}	V2X messages

Differentiated Services Code Point (DSCP) has handled the PPDR agency. In this case, the network operator policy is used. The inputs for the PPDR agency decisions can consist of subscription-related information like the MPS priority level, in the context of one or more of the special access class categories used in 4G networks to prevent an overload of the radio interface control channels by restricting access attempts from some users [30].

The 3GPP standard TS 23.203 establishes different QoS and example services to be used in 4G networks. Table 2, extracted from [44], shows in the columns the aspects of EPS settings and in the lines the respective value of priority of the service.

QoS control mechanisms are used to assign priority, and resource management, which is performed using three algorithms, as introduced by [24] according to 3GPP standard 22.011 [44], which are:

TABLE 3. 5G additional QoS parameters. (Adapted from 3GPP TS 23.501 [98].)

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Max Data Burst Volume	Default Averaging Window	Example Services
80	Non-delay critical GBR	68	10 ms	10^{-6}	N/A	N/A	Low latency eMBB applications, Augmented reality
82	Delay-critical GBR	19	10 ms	10^{-4}	255 bytes	2000 ms	Discrete automation
83		22	10 ms	10^{-4}	1354 bytes	2000 ms	Discrete automation, V2X messages
84		24	30 ms	10^{-6}	1354 bytes	2000 ms	Intelligent transport systems
85		21	5 ms	10^{-6}	255 bytes	2000 ms	Electricity distribution high voltage, V2X messages
86		18	5 ms	10^{-4}	1354 bytes	2000 ms	V2X messages

- Access Priority: is used to control congestion and access to services, and is significant when, in an emergency, a PPDR agent needs access to the network's resources. Each common device (e.g., cellphone of popular users) is assigned a specific class, numbered from 0 to 9. Special class numbers, from 11 to 15, can also be given, each allocated to specific high priority users (the enumeration is not meant as a priority sequence) [44]:
  - Class 15: Public Land Mobile Network (PLMN) Staff;
  - Class 14: Emergency Services;
  - Class 13: Public Utilities (e.g., water/gas suppliers);
  - Class 12: Security Services;
  - Class 11: For PLMN Use.

  It is essential to inform that class 10 is used for emergency calls. In this case, this algorithm is responsible for defining the priority of each device and controlling access to the environment.
- Admission Priority: As mentioned at the beginning of this chapter, the following service level QoS parameters are defined: QCI, ARP, GBR, and MBR. According to [24] extracted from [45]. At the same time, non-GBR, GBR, and MBR are related to the throughput of the carriers that have been established. The ARP and QCI parameters will define the corresponding QoS level by the ARP parameter. The decision to establish or not a carrier, in other words, the admission protocol, is made through the ARP parameter, which respects the priority levels, defined in 15 levels, where level 1 has the highest priority, as mentioned in the previous protocol.
- Data Plane QoS Configuration: According to [24], the last process after the bearer is established is that through the QCI parameter, the treatment of packets by network nodes will be defined. In Table 2 we can see that there is a correspondence between the QCI parameter and the type of service.

These three protocols mentioned above are responsible for defining, controlling, and admitting the access priority of devices on the LTE network. More details of each algorithm

are detailed in 3GPP standard 22.011 [44]. To support the additional service requirements of 5G, 4G QoS parameters (shown in Table 2) were extended and are shown in Table 3. Two new columns, "Maximum Data Burst Volume (MDBV)" and "Averaging Window", were added. Another difference was the conversion of QCI nomenclature for the 5G QoS Identifier (5QI). There are several standardised 5QI values in Table 3 from 3GPP TS 23.501, which provides the mapping from 5QI to QoS characteristics. Maximum Data Burst Volume, according to 3GPP, each GBR QoS Flow with Delay-critical resource type shall be associated with a MDBV. The MDBV denotes the most significant amount of data that the 5G is required to serve within a period. In this sense, each GBR QoS Flow shall be associated with an Averaging window that represents the duration over which both Guaranteed Flow Bit Rate and Maximum Flow Bit Rate (MFBR), are calculated. While in 5G, QoS is implemented at the flow level, 4G QoS is enforced at the EPS bearer level, where each bearer is assigned a specific ID. 5G uses QoS Flows, each identified by a Quality of Quality of Service Flow ID (QFI). As with 4G, both non-GBR flows and GBR flows are supported in 5G, along with a new delay-critical GBR. 5G also introduces a new concept - Reflective QoS. The QoS flow is the finest level granularity within the 5G system and is where policy and charging are enforced [98]. One or more Service Data Flows can be transported in the same QoS flow if they share the same approach and charging rules (similar to an EPS bearer in 4G). All traffic within the same QoS flow receives the same treatment. It is important to remember that Table 3 extends Table 2. Thus, the two Figures are complementary, re-evaluating the content presented with the introduction of 5G.

In mission-critical systems, a secure communication network is an important aspect of providing a high availability system, which asserts that a computer system is available or accessible by an authorised user whenever needed. To implement secure systems are necessary aspects of Confidentiality, Integrity, Authentication, Non-Repudiation, and Availability [23].

- Confidentiality: protects information from being accessed by unauthorised parties. In other words, only the people who are authorised to do so can gain access to sensitive data.
- Integrity: is the maintenance of and the assurance of the accuracy and consistency of data over its life cycle and is a critical aspect of the design, implementation, and usage of any system that stores, processes, or retrieves data. Integrity refers to ensuring the authenticity of information—that information is not altered and that the source of information is genuine. However, only authorised users should be able to modify the information being exchanged.
- Authentication: is the process of verifying the identity of a person or device. A typical example is entering a username and password when logging in to a system. Entering the correct login information lets the system know 1) who you are and 2) that it is you accessing the system. In other words, the sender's identity can be verified by the receiver.
- Non-repudiation: is the assurance that someone cannot deny the validity of something (e.g. message authorship).
- Availability: it is the time of service available and is typically associated with reliability and system up-time. It ensures authorized users have timely and reliable access to resources when needed. Critical systems have a high order of availability to ensure that the system operates as expected when needed.

3GPP presents quantitative and qualitative security requirements to characterise PPDR systems that prioritise traffic. PPDR systems are characterised by communications that have to be treated with a higher priority compared to regular communications in the network [8], such as:

- support a low end-to-end latency (10 ms);
- support high uplink and downlink data rates (10 Mbps per device) in a dense environment;
- support high throughput (10 Mbps);
- support very high reliability (99,999 % or higher);
- support service continuity;
- support high availability (approximately 100 % of the time on the road);
- support optimised signalling for prioritised users and traffic;
- can provide a real-time dynamic control function that adapts the prioritised access, QoS, and policies based on various criteria such as user status, service data, and incident or other dynamic data;
- supports different levels of protection for users and traffic;
- support different levels of resilience, availability, coverage, and reliability to offer different levels of guaranteed communications.

In this context, this survey has a focus on the security aspects of PPDR systems from current systems towards 4G and 5G commercial systems, considering the requirements of security in mission-critical networks mentioned.

III. CURRENT PPDR SYSTEMS

PPDR systems rely on old and well-tested protocols and solutions because they offer a high level of confidence and resilience. As these systems tend to have closed standards and update slowly, they do not easily allow the integration with new technologies and the extension or update of the current services. They mainly rely on voice communication and radio transmission systems, using protocols not designed to transmit other data types, such as video.

This survey describes four current systems: TETRA, TETRAPOL, P25, and DMR. These systems are used around the world and exemplify the current used PPDR technologies. TETRA is the most used system in Europe. However, France, Belgium, and other countries mainly use TETRAPOL. P25 is the primary system in North and South America. The DMR

TABLE 4. Technical comparison among current PPDR systems.

	TETRAPOL	TETRA	P25 - Phase 1	P25 - Phase 2	DMR
Release Date	1980	1995	1995	2010	2005
Responsible Organisation	Airbus	ETSI	TIA	TIA	ETSI
Modulation	GMSK	4-DQPSK	C4FM	C4FM	4FSK
Access Method	FDMA	TDMA (4 slots)	FDMA	TDMA (2 slots)	TDMA (2 slots)
Frequency (MHz)	VHF, UHF, or 800	VHF, UHF, or 800	VHF, UHF, 700, 800 or 900	VHF, UHF, 700, 800 or 900	VHF, UHF or 800
Channel Bandwidth (KHz)	12.5	25	12.5	6.25	12.5
Data Rate (Kbps)	8	28.8	9.6	9.6	9.6

system was the last introduced and is usually used by small PPDR agencies requiring low implementation costs.

All technologies presented in this survey are still in use, for example, Motorola Solutions announced in 2019 during an interview with IWCE's Urgent Communications that the company has participated in the initial commercial deployment phase of 3.5 GHz Citizens Broadband Radio Service (CBRS) technology. In this announcement, Motorola presents its MOTOTRBO Nitro system that provides private LTE voice and data services [122].

Table 4 makes a technical comparison between all currently used systems of PPDR agencies. We compared the mechanisms PPDR systems implement to provide security with others that 4G and 5G offers. This comparison is presented in the next section.

A. TETRA

TETRA is created by European Telecommunications Standards Institute standard (ETSI). It operates in the frequency range from 150 MHz to 900MHz and can achieve a bit rate of 28.8 kb/s. TETRA systems have been built and operate in more than 100 nations, and the first version was published in 1995. Originally conceived for use by the European Union government and public safety agencies, it was later adopted as the worldwide standard for digital radio communications systems.

1) TETRA OVERVIEW

TETRA implements a high-end solution for small private systems up to large public networks, while preserving characteristics and advantages of private land mobile radio systems, such as fast call set-up and group calls. The TETRA service uses 3 types of operating modes:

- Circuit mode (Voice plus Data), which provides circuit-switched speech and data transmission;
- Packet Data Optimized (PDO), which provides data traffic based on packet switching;
- Direct Mode Operation (DMO), which provides voice transmission between two terminals is used without using a network.

The Functional Components of a TETRA Network are defined by the Mobile Station (MS), Line Station (LS), Switching and Management Infrastructure (SwMI), and Gateways. MS comprises the subscriber's physical equipment, a Subscriber Identity Module (SIM) and a TETRA Equipment Identity (TEI) specified for each device. TEI is attributed by the operator, similar to Personal Identification Number (PIN) in mobile devices, which means what can disable a stolen device immediately. LS has a similar structure as a mobile station but with the SwMI connected over Integrated Services Digital Network (ISDN). It provides the same function and services as a mobile station. SwMI contains base stations that establish and maintain communication between MS and LS over ISDN. It allocates channels, switches calls, and includes databases with subscribers' information. The Network Management unit provides local and remote management functionality. Gateways interconnect a TETRA network with a non-TETRA network such as Public Switched Telephone Network (PSTN), ISDN, and Public Data Networks (PDN). Translation or conversion of information formats and communication protocols might be necessary.

2) TETRA SECURITY

TETRA has been designed with the requirements of public safety in mind. This means that security is a critical requirement. TETRA provides the following mechanisms to fulfill the security requirements:

- Authentication: to ensure trusted access of radios to the TETRA infrastructure and vice-versa (mutual authentication);
- Encryption: Air Interface Encryption (AIE) to encrypt the voice, data, and signalling over-the-air, is fundamental to provide high confidentiality and End to End Encryption of voice and data;
- Enable and Disable: to allow remote disabling of TETRA radios when the radio is lost or stolen;
- Key Management: for managing dynamic keys over the air.

In a similar form to GSM and the 3G systems, the fundamental security service in TETRA is based on strong authentication. Authentication is the process of validating the identity of the parties in the communication. When using symmetric-key cryptography, one can only trust parties that share the same secret, and only with the same secret can they communicate. The authentication in TETRA is based on proving knowledge of the same secret shared between an MS and the Authentication Center. In the TETRA context, all authentication is between the terminal and the infrastructure, never terminal to terminal, and not directly infrastructure to

user. Each device contains a shared secret 128-bit encryption key directly inside the terminal or on a SIM card [11] to provide integrity.

The TETRA authentication algorithms (TAAs) are a set of algorithms used as the basis of authentication and encryption key derivation. The full specification of the standard algorithm TAA1, is available from the TETRA Memorandum of Understanding (MoU) [10], [11]. The algorithms were developed for the TETRA-MoU [121] by the Security Algorithm Group of Experts (SAGE), a group formed by ETSI members set up to design algorithms for various ETSI standards. For example, the TETRA encryption algorithm (TEA) protects the user data over the air interface. TEA is a stream cipher with an 80-bit key. The full specification of several possible algorithms is available from the TETRA-MoU, each directed to a particular commercial objective:

- TEA 1: European commercial use;
- TEA 2: EU public safety organisations;
- TEA 3: Public safety organisations outside EU;
- TEA 4: Commercial organisations outside EU.

TETRA end-to-end encryption is a standard of the TETRA system. An end-to-end encrypted voice service operates between terminals without any intervention by the infrastructure other than its role as a bit carrier. It removes the need for a user to trust the network to maintain the confidentiality of the data in transit. All required of the network is that it acts as a transparent pipe and delivers the same sequence of bits to the receiving terminal. The TETRA standard is designed to support end-to-end encrypted voice service. It offers the necessary transparency and a small amount of signalling support that allows terminals to achieve and maintain cryptographic synchronisation quickly.

While TETRA was designed as a secure system in its original concept, commercial pressures made mandatory security features optional. As a result, the basic level of security offered by practical TETRA systems is defined by three different security classes:

- class 1: No encryption;
- class 2: Static Cipher Key encryption;
- class 3: Dynamic Cipher Key encryption.

An essential element of any cryptographic system is key management. The TETRA Key Management is the approach of the standard mentioned in Recommendation 02 of the TETRA-MoU. It reserves a particular identifier in the Short Data Service (SDS) for end-to-end encryption key management messages. It is similar to the standard TETRA security in that each terminal holds an embedded secret, the Key-Encryption Key (KEK). This secret must be directly loaded into the terminal by the key management protocol. The KEK is expected to be unique to a terminal. It minimises the management overhead if the terminal is lost or there is a suspected compromise of its key. After that, all other keys may be loaded over-the-air using the SDS. The key used in the hierarchy is the Group Encryption Key (GEK). The GEK is expected to be shared across a group of terminals that are managed identically. Using a shared key allows a bandwidth-efficient broadcast method to distribute Traffic Encryption Keys. This are the keys that are used to encrypt the voice traffic. The available management messages include commands that allow end-to-end keys to be deleted from the terminal.

In any system that uses cryptography, the fundamental security of the system lies in the cryptographic keys and in how they are generated, distributed, used, and protected. There can be high operational costs in the day-to-day management of these keys. TETRA minimises these costs by using the Over-The-Air Rekeying (OTAR) service. Delivering key material removes the need for terminals to be returned at intervals to a central point to be filled with new keys. It also enables the system to handle scheduled and unscheduled key changes without disrupting the users.

B. TETRAPOL

TETRAPOL is an open, digital, purpose-built PPDR technology designed to suit the most demanding users. From public safety agencies and the military to utility and transport operators, professionals around the world rely on Tetrapol to provide secure, reliable voice and data communications [13].

1) TETRAPOL OVERVIEW

TETRAPOL was developed by Matra Communication (today AIRBUS), France. The first users of TETRAPOL were the Gendarmerie (mid-1992) and then the police (early 1995) in France. Today the TETRAPOL technology is supported and further developed by two organisations: TETRAPOLForum (mainly manufacturer) and the User's club. The primary users of the TETRAPOL system are closed user groups, such as transport services (e.g., taxi, state railway, and local transport companies), airports, energy companies, and public security agencies [14]. TETRAPOL provides a secure and robust voice and data communication in critical situations. TETRAPOL is proven worldwide, with 85 networks in around 30 countries. In TETRAPOL network communications, three working modes are considered [15]: Network mode, Direct mode and Repeat mode. In Network mode, the terminals connect and are controlled by a base station (a fixed infrastructure). The communication between two MS always runs through the Base Station (BS). Two or more mobile stations communicate directly in a direct mode without coordination by a base station. This so-called *walkie-talkie mode* can also work in areas where the base station cannot cover (e.g., in a tunnel or basement of a building). The communication is transmitted through a repeater in Repeat mode, relaying the signal and does not have any coordination functions. The mobile stations can communicate at a longer distance than in Direct mode. According to TETRAPOL standard [13], a general TETRAPOL System Terminal (ST) is the service access reference point provided to the user by the system. It may be defined by a Line termination (LT) or Mobile Termination (MT).

The User Data Terminal, also known as Terminal Equipment (TE), is connected to the LT or MT. MT is also known

as a Radio Terminal (RT). Each may have a SIM. Internally, an MT or LT can be split into the following entities described in the TETRAPOL Publicly Available Specifications (PAS) [13]:

- Encryption entity for voice and data end-to-end encryption;
- CODEC for voice coding and decoding;
- A chipset includes an ASIC (ARM and digital signal processors) and a Radio Frequency (RF) part.
- An authentication entity for authentication of the MT to the network.

The network architecture defined in TETRAPOL is used for critical communications and presents the necessary support for security services. The TETRAPOL network architecture will be described below.

2) TETRAPOL SECURITY

TETRAPOL provides several security mechanisms, described in [12]:

- End-to-end encryption: prevents third parties from accessing data while it is transferred from one end system or device to another; The data is encrypted on the sender's system or device, and only the recipient can decrypt it;
- Mutual authentication: a security process in which entities authenticate each other before actual communication occurs;
- Signaling protection: to prevent traffic analysis, a temporary identity allocated by the network is used instead of the real subscriber address;
- Encryption diversity: multiple algorithms are permitted for end-to-end encryption;
- Automatic re-keying: key management without the need for user involvement;
- Automatic network reconfiguration: for increasing service availability, provisioning redundant critical components;
- Remote Enable/Disable: to remotely disable or enable compromised devices;
- Access control: this feature controls access to the equipment by smart cards or passwords.;
- Subscriber Identity Module: a SIM card can be used with a PIN code control and authentication; other configurations are possible if public keys are used.

The security services presented provide TETRAPOL reliability, secure authentication, and communication encryption to attend PPDR systems' requirements.

C. P25

P25 is a set of standards for digital mobile radio communications, fundamentally created for use by PPDR agencies and users. The first implementation was in North America, and after in New Zealand, Australia, and Canada, which extended to South America, mainly in Brazil.

1) P25 OVERVIEW

The P25 protocols were designed by an international consortium of vendors and users centred in the United States. The protocols are coordinated by the Association of Public Safety Communications Officers (APCO), jointly administered and with its standards documents published by the Telecommunications Industry Association (TIA) and the American National Standards Institute (ANSI). Work on the protocols started in 1989, and the first version was published in 1995, with new protocol features continuing to be refined and standardised on an ongoing basis and improving equipment interoperability from different manufacturers.

The Mobile Radios (MRs) are either hand-portable or vehicle-mounted and paired with a Mobile Data Terminal (MDT) for accessing data services. The Fixed Station (FS) fulfils the roles of a base station, Key Management Facility (KMF), trunking controller, and repeater. The FS may also provide data services, gateways to the public switched telephone network, automatic branch exchanges, and other radio systems [17]. In the existing P25 standard, the Common Air Interface (CAI) traffic is exchanged at 9600 bps using either 4-level frequency-shift keying (FSK) modulation in a 12.5 kHz half-duplex channel or π_4 differential quadrature phase-shift keying (DQPSK) modulation in a 6.125 kHz half-duplex channel. However, to accommodate the limited data rate, voice transmissions employ the IMBE vocoder to encode voice traffic into compressed voice codewords, where each 88-bit codeword represents 20ms of uncompressed speech. In the structure of voice transmission, each voice transmission begins with a header data unit (HDU), followed by several voice superframes which carry the compressed voice traffic. That is followed by a terminator data unit (TDU). Each superframe is composed of alternating Logical Data Unit 1 (LDU1) and Logical Data Unit 2 (LDU2) frames, each of which contains nine IMBE compressed voice codewords and differs only in the meaning attached to the non-voice payload of each frame [17].

2) P25 SECURITY

The TIA-102 standard [112] provides several standardized security services that have been adopted for implementation in P25 systems. P25 provides several security mechanisms:

- End-to-End Voice Encryption;
- Data CAI Encryption;
- AES or 3DES Encryption;
- OTAR;
- Multiple Keys;
- Subscriber Validation;
- Key Fill Device (KFD) and KMF Interfaces;
- Link-Layer Encryption.

As P25 is a digital protocol, it is technically straightforward to encrypt voice and data traffic, which is far more difficult in the analogue domain systems it is designed to replace. However, encryption is an optional feature, and even radios equipped for encryption can operate in clear mode. In the

encryption mode, keys may be manually loaded into mobile units or updated at intervals using the OTAR protocol.

P25 provides options for traffic confidentiality using symmetric-key cyphers, which can be implemented in software or hardware. The DES, 3DES, and AES cyphers are identified for usage in the standard and the null cypher for cleartext. The standard also provides for the use of vendor-specific proprietary algorithms (such as 40 bit RC4 for radios aimed at the export market) [10]. However, pre-shared symmetric keys are used for all traffic encryption.

The system requires a key table traditionally located in each radio mapping unique Key ID and Algorithm ID tuples to particular symmetric cypher keys stored within the unit. This table may be keyed manually or using an OTAR protocol. A group of radios can communicate in encrypted mode only if all radios share a standard key (labelled with the same Key ID). The KFD and KMF are responsible for integrity management.

A technician may do cryptographic keying of P25 radios manually with a particular key loading device, called a Key Variable Loader (KVL), or perform remotely via the OTAR protocol. The OTAR protocol relies on each mobile having pre-shared unit-specific keying material (key encrypting keys) that permits a remote KMF to securely add, update, and remove elements of the radios' traffic key tables [18].

D. DMR

DMR is an open digital mobile radio standard defined in ETSI Standard TS 102.361 parts 1–4 [21] and used in commercial products around the world.

1) DMR OVERVIEW

DMR was designed with three tiers. DMR tiers I and II (conventional), the first published in 2005, and DMR III (Trunked version) was published in 2012, with manufacturers releasing products within a few years of each publication. The Digital Mobile Radio Association define the tiers as [19]:

- Tier I: products are open source and used in the 446MHz band. It grants a lack of consumer and low-power commercial applications, utilising a maximum of 0.5 Watt of Radio Frequency power.
- Tier II: this technology is made to cover licensed conventional radio systems, mobile devices, and hand portables operating in the frequency bands from 66 to 960MHz, basically used for PPDR systems.
- Tier III: is prepared to cover a trunking operation in frequency bands from 66 to 960MHz, to satisfy the PPDR spectrum. Also, it supports packet data services in various formats, that include IPv4 and IPv6 protocols which represents a requirement for future PPDR networks.

The primary goal of the standard is to specify a digital system with low complexity, low cost, and interoperability across brands. Therefore, radio communications purchasers are not locked into a proprietary solution.

The DMR network design is scalable from one site to an extensive, wide area network with multiple node controllers controlling hundreds of sites. Open standard protocols are implemented to provide gateways to non-DMR base stations/repeaters and digital or analog dispatch console equipment. Radio networks of different manufacturers and technologies can also be connected through DMR networks, creating a simple migration path or large-scale communication systems.

There are some key elements of the network in the DMR architecture [16]:

- A Linking infrastructure, or the IP backbone, interconnects the various elements of the DMR network.
- DMR site equipment, such as base stations or repeaters, provides the RF path to and from the mobile and portable radios for voice or data communications.
- DMR nodes control the call setup, generate and store call records and raise alarms.
- Network gateways provide an audio interface to equipment and systems outside the DMR system.
- Telephone gateways support direct communications between radios and external telephones through the PSTN/Private Automatic Branch Exchange (PABX).
- DMR mobile and portable subscribers communicate between radio users and other network-connected devices.

The DMR architecture recognises a standard of the other technologies that cover the spectrum of PPDR networks traditionally based on this architecture is a robust security system for DMR networks will be presented below.

2) DMR SECURITY

According to ETSI, one primary objective of the DMR Tier III standard is to provide interoperability at the Air Interface between equipment of different origins. The standard defines only the over-the-air signalling and imposes minimum constraints on system design. The DMR air interface security services enable a Trunk Station Control Channel (TSCC) to authenticate an MS using the standard RC4 algorithm. If the TSCC wishes to authenticate an MS, it sends a random number in a PDU, defining the challenge. The MS calculates the response to the challenge using a 56-bit authentication key programmed into each MS during manufacture. Similarly, an MS may authenticate a TS using the TSCC key [21].

The DMR encryption is not ETSI standardised yet, but it is the manufacturer's choice. Motorola MOTOTRBO™ terminals perform two levels of encryption, one ''basic'' with low security (255 non-dynamic keys) and the other using an ''advanced'' algorithm that assures a higher level of reliability. The vocoder implemented in Motorola MOTOTRBO™ terminals is the AMBE II+™ (Advanced Multi-Band Excitation) which is a proprietary speech coding standard. The use of the AMBE standard requires a license [20].

Motorola first started to develop so, making it a standard. Probably the following actors should follow Motorola's protocols and vocoder because it is already in use. On the other

hand, Motorola is interested in creating an open standard due to the commercial power of a multi-vendor environment.

IV. EVOLUTION AND INTEGRATION OF PPDR SYSTEMS IN THE CONTEXT OF 4G AND 5G

As shown in the previous sections, the current PPDR networks play an essential role in the critical environment of PPDR systems, mainly in voice communication. Unlike ordinary voice communications with some flexibility, PPDR networks support voice communications in highly efficient security, efficiency, and availability. Besides, PPDR agencies use specific functionalities and applications that are linked to voice services; for example, push-to-talk function, dispatch services, priority and group communications, and off-network communications are used for peer-to-peer devices, DMO or talk-around, group call and group management.

However, other security functions are being adopted by the PPDR systems, such as ciphering, OTAR, and supplementary security services. Therefore, many other features and functionalities define PPDR services and separate them from the typical consumer services over commercial 4G networks [22].

In this sense, the demand for broadband communications in PPDR networks was born with the necessity for devices that use the broadband communication of data to search databases and exchange messages, photos, and videos with the central control, in addition to other functionalities such as video calls and live video streaming. All these demands are growing and fulfil an essential role in the PPDR scenario. For instance, sending live video streaming to the central control will help PPDR agents to accurately evaluate the disastrous situation, allowing the mobilisation of agents in a timely fashion and with precision.

The current massive advancement of 4G technologies was considered a great promising candidate to support the specific and critical requirements of PPDR networks [9], taking into account the demand for high-speed broadband and low latency for video transmission. In this sense, according to [30], the introduction of 4G networks was intended to complement, not replace, the current PPDR networks. However, there is a consensus on using commercial network technology to replace the current PPDR networks [3], [28] [30], [31]. According to the [23], the first step toward mission-critical mobile broadband networks has been implemented, the standards are in place, and the functionalities required for 4G are defined. However, the replacement of current public safety networks for 4G will not be immediate. Notwithstanding, there are projects worldwide that lead us to believe in this reality. Next, some examples of implementation and academic proposals will be presented.

The FirstNet is an independent authority within the U.S. Department of Commerce. Authorised by Congress in 2012, its principal mission is to develop, build and operate the nationwide broadband network that equips first responders for public protection and disaster relief of U.S. communities [48], [49]. It is possible to say that the USA is one of the first countries that initiated the transition to critical mobile broadband networks [23]. In the same context, according to the Britain Government [50] the new Emergency Services Network (ESN), a critical communications system, will replace the current Airwave service used by the emergency services in Great Britain [51]. In Belgium, to provide broadband data services to PPDR users, ASTRID initiated the Blue Light Mobile project. In other words, Belgium started a hybrid network. The TETRA was used before as an interoperable extension to Blue Light Mobile broadband project [52]. In South Korea, is implemented Korea SafeNet [53] is a single communication network on a national scale supporting one channel of command and control and integrated response at disaster sites. It adopts 4G for Disaster and Safety management.

In this same context, some European projects helped collect requirements for the transitioning from current PPDR networks to commercial networks. In addition to designing future networks with their challenges and necessities. Some examples are introduced, such as Framework Program 7 (FP7) HELP this project describes a new approach to wireless communication systems in the PPDR domain, which explores the capabilities of new technologies and concepts like 4G. In the results report of the FP7 HELP project, several projects in the area of PPDR wireless communications sponsored by the FP7 project are mentioned [28], such as EULER [54] which applied the Software Defined Radio (SDR) technology to intend to mitigate the lack of interoperability of the agencies in the operational PPDR scenarios. FP7 DITSEF [55] (Digital and Innovative Technologies for Security and Efficiency of First responder operations) was introduced to supply a self-organising and robust ad-hoc communication network with location information that can be used in critical infrastructures. FP7 INFRA - Innovative and Novel First Responders Application [56] aims to research and develop new technologies for personal digital support systems as part of an integral and safe emergency management system.

The SALUS project [57] has a proposal of robust, reliable, and secure mobile broadband communications system solutions for a wide variety of PPDR applications and services on PPDR broadband networks, including the ability of inter-system, inter-agency and cross-border operations with emphasis on interoperability between users in current PPDR networks and 4G/5G.

Another relevant project in this sense is BROADMAP [58] which takes the first steps towards future procurement of interoperable next-generation broadband radio communication systems for public safety and security to improve PPDR service to European citizens and enhance interoperability across borders.

The security requirements were summarised as traffic prioritisation, low latency to the transmission of video streaming, end to end encryption, and short mobility and flexibility for mobile devices. With the commercial deployment of 5G networks, new possibilities for PPDR systems can be

considered, which add new requirements to the previously set defined for 4G. The new scenarios include heterogeneous environments, a high number of devices, IoT support and enhanced data capabilities such as high definition live streaming video. These will require higher levels of speed, lower latency, privacy, flexibility, energy awareness, and mobility support.

Next, 4G and 5G will be detailed and their security mechanisms compared.

A. PPDR OVER 4G

4G is a worldwide deployed standard, adopted by an increasing number of commercial networks, that due to its characteristics can facilitate the implementation of new PPDR services. Prerequisites in PPDR networks are the low set-up time in call establishment, high availability, and broad coverage. 4G complies with all these items and supplies high outdoor and indoor covering, a competitive advantage. Another important aspect is security in PPDR networks, which have complex mechanisms of authentication and encryption [24]. 4G architecture also has implemented security mechanisms, as defined by 3GPP System Architecture Evolution Specification [25] which will be presented in the subsection IV-A3.

1) 4G OVERVIEW

In Dec. 2004, the 3GPP launched a new technology called 4G to improve requirements for a new air interface called Evolved Universal Terrestrial Radio Access (E-UTRA), an evolution of Universal Terrestrial Radio Access (UTRA), or 3G. It is possible to identify that LTE and E-UTRA are synonymous, and will usually be defined in the literature as E-UTRA. The results and requirements of this work can be founded in Rel-7 3GPP TR 25.913 available in [26], and as summarised as:

- Considerably increased peak data rates: 100 Mbps in downlink and 50 Mbps in uplink;
- Increased bitrates at the edge of cells assuming current site locations;
- Improved spectrum efficiency: 2-4 times (available in Rel-6);
- Lower latency;
- Scalable bandwidth for greater flexibility in frequency allocations;
- Reduced capital and operational expenditure, including backhaul;
- Acceptable system and terminal complexity, cost and power consumption;
- Support for inter-working with existing 3G systems and non-3GPP specified systems;
- Efficient support of the various types of services, especially from the PPDR domain (e.g., Voice over IP, and Push To Talk);
- Optimized for low mobile speed but supporting high mobile speed (up to 500 km/h).

After that, in the same context of the definition of the LTE requirements, the same Rel-7 study produced posteriorly a 3GPP TR 25.912 available in [27] to introduce radio functionalities. According to the normative of LTE, the work followed from Sep. 2006 until March 2009 in Rel-8 specifications. The first specification for 4G based on PPDR systems started in Rel. 11 [32], which was activated from 2010 to 2013, but public safety specifications were not as widespread in this report. Soon after the versions, Rel. 12 [33], and 13 [34] were launched, which were developed in the range from 2011 to 2016, which contain many specifications for PPDR over 4G, but still, very scarce [23]. Now is available the Rel. 14 [35] and the recent version of Rel. 15 [36], which includes grounded standards related to PPDR systems.

The general work developed by 3GPP for PPDR over 4G can be classified on Rel. 15 in four main areas:

- MCCORE, available in TS 22.280 [37]: This standard provides the service requirements that are common across the mission-critical services, which can be used for PPDR systems and help the definitions of the principal requirements. Further development of mission-critical services beyond Mission Critical Push To Talk (MCPTT), such as Mission Critical Video (MCVideo) and Mission Critical Data (MCData), created an opportunity to re-use base functionality documented in the Stage 1 requirements for MCPTT. For example, the ability to communicate mission-critical information to groups of users is a common need regardless of the service type. For this reason, the MCCORE was created.
- MCPTT, available in 3GPP TS 22.179 [38]: This standard provides the service requirements for the operation of the MCPTT. This service is essential to PPDR operations and present in all current systems. Furthermore, a Push To Talk service implements an arbitration method utilised by two users or more who may interlock in communication. This service is popular and entirely accepted in PPDR current systems and is most practical to use in critical situations according to PPDR agents in the field.
- MCData, available in 3GPP TS 22.282 [39]: This standard provides the service requirements for the operation of the Mission-Critical Data service, which can be used in PPDR systems. Multiple services can be built using the generic capacities and use cases defined in the standard.
- MCVideo, available in 3GPP TS 22.281 [40]: This standard provides the service requirements for the operation of the Mission-Critical Video service. MCVideo defines a solution for Mission Critical video communication using 3GPP transport networks.

Another important functionality of 3GPP related to the requirements of PPDR systems is Proximity-Based Services (ProSe) [41]. ProSe Direct Communication enables the establishment of communication paths between two or more ProSe-enabled devices in the direct communication range. The ProSe Direct Communication path can use 4G or WLAN. This functionality is to compensate for the DMO requirement

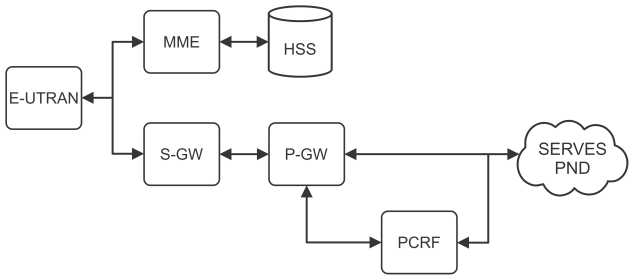


FIGURE 1. 4G network architecture adapted from [96].

of current PPDR networks. A PPDR user enabled with the ProSe service can communicate with another user who has the ProSe service enabled, even if the 4G network is not available. In other words, the devices communicate without interference or network operation. This technology has an essential role in disasters located in remote areas or in devastated structures. More information on the security aspects of ProSe is defined in TS 33.303 [42].

The benefits of 4G led to the publication of many works that endorse the transition of current PPDR networks to this new standard. Many of these works also propose additional improvements in terms of security, performance and availability to complement the existing ones [3], [9], [22], [23], [24], [28], [29], [30], [31], [77], [78], [81], [82], [83], [84], [85].

Also, the work related to Rel. 15, ''Removal of 'over LTE' limitation from Mission Critical Specifications'', opens space for the arrival of 5G, dropping this nomenclature to open a pass to new developments.

2) 4G NETWORK ARCHITECTURE

As specified by 3GPP, 4G networks are defined as two main parts: E-UTRAN and Evolved Packet Core (EPC). In this sense, in the 4G network explained in Figure 1, the radio access network consists only of the base stations Evolved NodeB (eNB) (the E-UTRAN can be composed of one or more eNBs). The EPC is considered the main component of the 4G network and consists of these services: Home Subscriber Server (HSS), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), MME (Mobile Management Entity), and Policy and Charging Rules Function (PCRF) [9]. However, in 4G infrastructures, the S-GW is the central part of the EPC and is the support point among the E-UTRAN and the EPC. For more information, the principal 4G logical network components definition can be found in [96].

In this context, the access network of 4G, E-UTRAN, consists of a network of eNBs. For several user traffic, as traditionally opposed to broadcast, there is no centralised controller in E-UTRAN.

3) 4G MISSION-CRITICAL SECURITY

The security developed in 4G technology is considered in the rel. 3GPP TS 33.401 [100]. This report distributes the security architecture into five different groups or domains. This division is convenient for describing the distinct security features of EPS since each domain can have its own set of security threats and solutions.

- 1 - Network access security to provide secure access to the service by the user.
- 2 - Network domain security protects the network elements and secures the signalling and user data exchange.
- 3 - User domain security provides control of the mobile stations' security access.
- 4 - Application domain security, used to establish secure communications over the application layer.
- 5 - Visibility and security configuration, allowing the user to check if the security features are in operation.

The mentioned domain of Network access security focuses on the security features that provide a user with secure access to the EPS. This domain includes mutual authentication besides privacy features, protection of signalling traffic, and User Plane traffic. An important aspect to remember is that protection may provide confidentiality and integrity protection. However, Network domain security refers to the features that allow these network nodes to securely exchange data and protect against attacks on the network between the nodes. The User domain security refers to the set of security features that secure access to terminals. The only defined user domain security feature is related to the PIN or PIN Unlock Key (PUK) code before becoming capable of accessing the device. Application domain security consists of the security features used by applications. For example, HTTPS provides end-to-end security between the application in the terminal and the peer entity providing the service. In another way, the previous security features listed provide hop-by-hop security, meaning they apply to a single link in the network only. Finally, the Visibility and configuration of security are defined as the set of features that allows the user to learn whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature. In most cases, the security features are transparent to the user, and the user is unaware that they are in operation.

B. INTRODUCTION OF PPDR OVER 5G

5G is the next generation of mobile internet networks, designed to provide advanced mobile broadband services with higher data rates, lower latency, more capacity, and enormous potential for new value-added wireless services. However, 5G systems are characterised by advanced flexibility and upgradeability. For example, Network slicing or Network Function Virtualization (NFV) provides seamless global mobility (500km/h) [61] in heterogeneous environments and supports multiple radio access technologies. The 5G technology will bring several new improvements to mobile communication systems, namely in what concerns bandwidth, latency, and scalability, besides opening doors to new concepts and techniques. This makes 5G a severe candidate for use in new areas and contexts where mobile communications are not usually used. One of these contexts is the Mission-critical systems. These systems require strict

performance and security requirements. Mobile communications like 4G did not fully satisfy all necessities in these environments, leading to the deploying of dedicated closed networks with increased cost. Shifting such systems to 5G networks means that systems usually using closed and reliable transmission systems will be using open ones. Moreover, current protocols used in such areas may not contain security mechanisms to prevent cyber-attacks on available systems.

1) 5G OVERVIEW

5G networks aim to respond to the new challenges imposed by new mobile and strongly connected society, by supporting a new set of applications and scenarios, whose requirements were defined within the scope of the International Mobile Telecommunications-2020 (IMT-2020 Standard) by the ITU Radiocommunication Sector (ITU-R) [59]. However, according to ETSI [60], ITU-R has defined the following main usage scenarios for IMT for 2020 and beyond in their Recommendation ITU-R M.2083 [61]:

- Enhanced Mobile Broadband (eMBB) to deal with hugely increased data rates, high user density, and very high traffic capacity for hotspot scenarios as well as seamless coverage and high mobility scenarios with still improved used data rates;
- Massive Machine-type Communications for the IoT, requiring low power consumption and low data rates for large numbers of connected devices;
- Ultra-reliable and Low Latency Communications (URLLC) to cater for safety-critical and mission-critical applications.

In the same context, the requirements were provided in ITU-R M.2410 [62]. For example, the minimum requirements are classified into 1-4, and other requirements are 5 and 6, as follows:

- 1 - Peak data rate: 20Gb downlink, 10Gb uplink;
- 2 - Peak spectral efficiencies: 30 bit/s/Hz downlink, 15 bit/s/Hz uplink;
- 3 - User plane latency: 4 ms for eMBB, 1 ms for URLLC;
- 4 - Control-plane latency: 10-20ms;
- 5 - Maximum aggregated system bandwidth: at least 100 MHz, up to 1GHz in higher frequency bands (above 6GHz);
- 6 - Mobility: up to 500km/h in rural eMBB.

With Release 15 of the 3GPP specifications, the first milestones towards IMT-2020 were accomplished. Besides introducing the first version of 5G, Release 15 specified a new Radio Access Technology, the 5G New Radio (NR), which was designed to be the global standard for the air interface 5G networks. After that, release 16 was completed on July 3, 2020. The Rel-16 specifies the second version of 5G and a variety of topics: MPS, Vehicle-to-Everything (V2X) application layer services, 5G satellite access, Local Area Network support in 5G, wireless and wireline convergence for 5G, terminal positioning and location, communications in vertical domains and network automation and novel radio techniques. In the same context, Rel-16 became the foundation for deploying 5G in New Radio Unlicensed (NR-U) spectrum in the unlicensed 5GHz and 6GHz bands. The standard employs the same contention-based Listen Before Talk (LBT) protocol used in 802.11 to ensure equal access to available channels. This enables NR-U operating in or above the 6 GHz frequency range to be unencumbered by the strict LBT protocols adopted for harmonious coexistence in the 5 GHz bands. Category 4 (CAT4) LBT is the baseline for 5 GHz operation, forcing severe backoff following Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) procedures. NR-U can employ CAT1 LBT in and above the 6 GHz range, where channel access is immediate and requires no LBT [119]. Therefore, this technique leads to increased interference. In critical scenarios, interference is one key factor affecting the QoS and thus decreasing the security efficiency of the network [120]. In this sense, the security protocols used in NR-U are the same. The difference is in the mechanism of access to the spectrum. However, more 5G system enhancements are defined to follow in Release 17 with a new schedule approved by 3GPP in [63].

According to the 3GPP, most PPDR services are currently identified as emerging services for 5G [79]. 5G aims to provide flexible systems to support different services with divergent requirements in their unique structure. However, integration of current PPDR systems in the 5G system should bring main advantages, such as, for example, better interoperability and coordination with civil networks and emerging services related to connected objects, but also cost reduction [80]. The advent of the 5G mobile broadband standard introduces additional sophisticated technologies that may further benefit PPDR agencies [64], [71]. The 5G system is expected to support diverse service portfolios and multiple service providers on the same infrastructure with network slicing. The closed nature of modern networking equipment prevents mobile operators to tests and deploying new features and consequently makes them unable to respond to quickly changing PPDR agency's needs. To solve these shortcomings. Software-Defined Networking (SDN) and NFV are considered to be some of the key technologies to realize the future 5G networks [71], [73], [74], according to the opinion of public-private consortiums 5G-PPP group [72]. These technologies are described as follows:

- Network slicing is responsible to enables the creation of logical networks with appropriate isolation, resources, and optimised topology to be implemented in a particular use case [64], and a slicing concept is described in [65]. A study on future business requirements is conducted by the Next-Generation Mobile Network (NGMN) alliance from the perspective of network operators. It describes the necessity for a flexible mobile system with modular network functions to optimise resource usage while providing scalable and cost-efficient solutions. Network slicing allows mobile operators to supply customised logical networks to third-party customers or tenants that can be business vertical or virtual operators with their subscribers.

Critical communications for public safety with rigid requirements in terms of network reliability and resiliency in all conditions are one of the use cases described by NGMN [66].

- NFV to support network slicing, the 5G system must offer flexibility in terms of network function chain composition, placement, and allocation of related resources. However, ETSI created a specification group for NFV [69], [70]. The main objective of NFV is to allow the implementation of network functions as software modules running on commodity hardware. Furthermore, virtualisation technology allows network function software to be virtualised and dynamically chained to provide a network service [67], [68]. For PPDR networks, current mobile systems extensively rely on hardware-based network functions that run on specialised hardware. NFV became a provider of mobility and resilience in this context.
- SDN architecture offers a new solution that decouples the control plane from the data plane, which is traditionally coupled together. Network functions typically obtained in specific hardware can now be separated and virtualised on any equipment. A split between control and data path nodes is performed, so a centralised controller has a global view of the network. In contrast, the data plane includes devices that simply forward packets following rules expressed by the controller. In this sense, to communicate between these two layers, an open standard protocol is employed to introduce communication between these two layers. This division between the two layers simplifies network management and helps program network control [75]. In the context of PPDR networks, the combination of SDN and NFV technologies is emerging as the principal solution to provide a flexible, dynamic, and adaptive way of managing PPDR services with effective communication capabilities [73].

According to [76], SDN and NFV could contribute to meeting the main requirements of mission-critical emergency communication networks, as follows:

- The logical centralisation of control functions in a physically distributed system can contribute to satisfying the high availability, reliability, resiliency, and robustness of mission-critical networks. However, with the virtualisation of network functions, it is possible to build logically centralised control planes that preserve good concentration properties without reducing the robustness of the whole system. In this sense, NFV can also contribute to the migration of network functions from one device to different parts of the network or supporting infrastructure that is disabled in the same disaster that creates the PPDR requirement.
- The employment of NFV could facilitate the rapid ad hoc networks reconfiguration and reallocation of available network capacity (up to the level of disposed size) to provide the incidental necessities of PPDR emergency without physical intervention on the device.
- For special services, for example, group calling, or device-to-device (D2D) messaging is more natural to provision and configure with SDN than with a traditional network.
- In SDN using OpenFlow, network decisions are decided on a flow basis for arbitrary flow definition and implemented in rules with priority levels. What can treat flows differently based on policies implemented by the controller, and as the controller has a full view of the network, it ensures strict respect for the plans. However, in PPDR networks, the decomposition of control planes and data planes could potentially enable or facilitate the application of fine-grained and sophisticated rules priority management to traffic flows.

Many papers proposed the transition from current PPDR networks to 5G (see in ''Comprehensive comparison over 4G and 5G security for PPDR systems''), due to the requirement to exchange data, images, and videos, not only voice.

The next step for PPDR systems over 5G is the Release 17 of 3GPP with more 5G system enhancements. The main work in this version is Mission Critical Services over 5G. It specifies the use of the 5G considering regular functional architecture, procedures, and information flows needed to support mission-critical services encompassing the usual services core architecture [94].

2) 5G NETWORK ARCHITECTURE

teThe network architecture of standalone 5G NR was developed by 3GPP with complete standardisation in June 2018 with Release 15 phase 2, which supports subscriber data management, control plane functions, and user plane functions. In this sense, 5G systems separate the User Plane functions from the Control Plane functions, allowing independent scalability, evolution, and flexible deployments, e.g., centralised location or distributed (remote) location. However, the 3GPP 5G network is referred to as reference point representation starting with the letter 'N' in rel. TS 23 501 [98]. Initially, these were assigned 'NG' for next-generation. Nevertheless, presently, the term has been shortened to just read 'N' [99]. The 5G System architecture consists of the following Network Functions (NF):

- User Equipment (UE)
- Authentication Server Function (AUSF)
- Unified Data Management (UDM)
- Access and Mobility Management Function (AMF)
- Session Management Function (SMF)
- Policy Control Function (PCF)
- Application Function (AF)
- Network Slice Selection Function (NSSF)
- Radio Access Network (RAN)
- User Plane Function (UPF)
- Data Network (DN)

The network architecture of 5G, represented in Figure 2, consists of a core AMF, a SMF, PCF, AF, and NSSF. The NSSF is responsible for selecting which core network instance is to accommodate the service request from a UE,

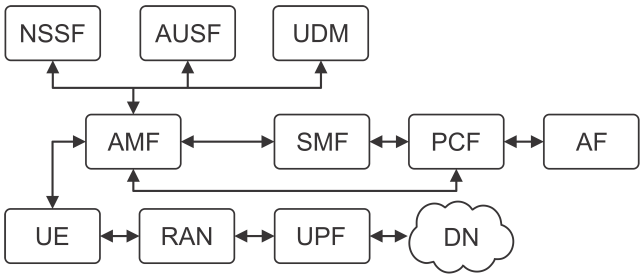


FIGURE 2. 5G network architecture adapted from [99].

by taking into account the subscription of UE devices and any specific parameters [98], [99].

The user plane functions start with the UE, which may be a smartphone or a new form terminal, probably fixed rather than mobile for those aspects. In this context, the connects via the RAN to the UPF and on to a DN. However, the DN may be the Internet, a corporate Intranet, or an internal services function within the mobile network core of the operator, for this reason including content distribution networks [98].

The UE connects to the RAN via the air interface, which in previous releases of 3GPP technologies, has been known as the Non-access stratum (NAS). This is a peer-to-peer control plane communication between the UE and core network. Furthermore, the connection between the RAN and the core network is commonly known as mobile backhaul. The connectivity between the UPF and any internal or external networks or service platforms is done via the air interface. This interface will include connectivity to the public Internet and therefore contain the necessary Internet-facing firewalls and other smarts associated [99].

3) 5G MISSION-CRITICAL SECURITY

Starting with 3GPP Release 13, mission-critical communications are delivered as a core network service, especially mission-critical Push-to-Talk, supporting critical services such as the ones used by police, firefighters and emergency medical personnel. In 5G Networks, first responders will go far beyond basic Push-to-Talk to add Push-to-Video, video sharing, group chat, file sharing, location sharing and much more. All with the prioritization of mission-critical traffic. It is important to note that while 5G networks are still in the early design stages, many services, such as Mission-Critical Communications, are already available in the LTE networks, as specified in the 3GPP Release 13 and above. Using Mission-Critical Communications over LTE, we can already greatly enhance the communication capabilities of first responders. Even if the tower becomes unavailable, a mobile network can be provided via the antenna on any truck, drone, emergency vehicle or backpack. Such private LTE networks will support all first responders' communication capabilities. Firefighters can share a live video of a disaster site among team members and receive videos from drones, surveillance cameras, planes and satellites in real-time. They will also be able to share their location, significantly improving teamwork and team communication.

According to [91], the expectation for the security features in the further evolution of 5G security were be high. New features will be introduced, including security support for reduced-capability NR devices referred to also as NR-Light, enhanced Non-Public Network, proximity services (considering commercial services such as a new generation of sensors (V2X) and PPDR applications), Multimedia Broadcast Multicast Service (MBMS), National Trends Networks (NTNs), and Unmanned Aerial Vehicles (UAVs), for example for identification, control, and tracking, and new features to increase the security of Virtual Network Functions (VNF). Besides, it is expected that UE will be prepared to support the legitimacy of base stations before attempting to connect, which should make the deployment of fake base stations more difficult. With security assurance specifications for all 5G nodes, operators and regulators can be guaranteed the security compliance of the 5G system. In the security aspects, 5G networks guarantee the privacy of their users, confidentiality, protection, integrity of the traffic transported, and assurance protection against attacks that can affect availability, the integrity of the network, and confidentiality of stored data.

The 3GPP improved the requirements in the Rel-15, besides introducing a broad range of security features aligned with the general 5G architecture evolution principles. Based on the Rel-15 security framework, new security features in Rel-16 support multiple segments, including PPDR. Support for Non-Public Networks with new authentication schemes will drive 5G adoption in PPDR environments. Security features for IoT communications will improve massive IoT appropriation. With authentication based on the slice and primary authentication, slice holders gain increased access control and security isolation between slices. Network Slice Selection Assistance Information (NSSAI) for slice access can be protected if necessary. Security for duplicated transmissions (for URLLC) is expected to provide support for new applications such as medical imaging. Integrity protection in the user plane will prevent packet injection and manipulation of user packets [91]. The following are some of the key security features specified in Rel-15 and Rel-16 [36], [91]:

- Improved subscriber privacy;
- Improved Security for Radio Resource Control (RRC);
- Centralized authentication framework and access to agnostic authentication;
- Increased home control, for example, authentication and steering of roaming;
- Support for user plane integrity protection (covering all three use case domains, for example, eMBB, URLLC, and massive IoT);
- Primary and secondary authentication in public and non-public networks (including support for a slice-specific authentication);
- Security for interworking between the 5GS and the EPS of 4G;
- Secure service-based architecture and interconnection with current PPDR networks, and NAS signaling.

TABLE 5. Classification of papers related to the security of PPDR networks based on commercial networks.

Security Aspect	Technology	References
Confidentiality	4G	[3], [23], [24], [74], [77], [85]
	5G	[4], [71], [76], [85], [89]
Integrity	4G	[9], [23], [24], [77], [84], [85], [86]
	5G	[76], [85], [88], [90], [91], [92], [93]
Authentication	4G	[3], [23], [24], [28], [77], [78], [82]
	5G	[85], [90], [91], [92], [93]
Non-repudiation	4G	[3], [23], [24], [77]
	5G	[85], [90], [91], [92], [93]
Availability	4G	[9], [22], [28], [29], [30], [31], [78], [81], [82], [83], [84], [85], [86], [87]
	5G	[4], [64], [71], [73], [74], [76], [80], [85], [88], [89]

In Release 17 [63], some items of mission-critical is considered. Isolated Operation for Public Safety (IOPS) over 5G systems introduced initially in 3GPP Release 13 is being defined in Release 17. The introduction of mobile broadband with low latency combined with edge computing opens new possibilities for deploying command and control capabilities. Usage of Augmented Reality (AR) and Virtual Reality (VR) will reduce the amount of desk space used by multiple display screens and allow emergency organisations to equip workers with wearable solutions like smart glasses to access data at the scene of an event. Also, security improvements are planned for mission-critical Release 18 [123] (scheduled for 2023), mainly in Security, Privacy, Application Enablement, and Critical Communication Applications.

C. COMPREHENSIVE COMPARISON OVER 4G AND 5G SECURITY FOR PPDR SYSTEMS

As introduced in chapter II, mission-critical systems have high-security requirements and require comprehensive coverage of critical security aspects. PPDR systems classified as essential are also included in this necessity. In this section, we will compare 4G and 5G systems previously mentioned in chapters IV-A and IV-B, considering the security aspects of each associated and previously classified article. The security requirements presented for the classification are:

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Availability

The articles are classified and analysed in Table 5 for more helpful visualisation, and scrutiny of the proposals presented, according to the security classification presented.

After the emergence of smart mobile devices, and following the need for greater bandwidth, there was a consensus on the transition of PPDR networks to broadband networks. This move created new security requirements and challenges, such as greater confidentiality and integrity, more robust authentication, and the need of non-repudiation. In 4G networks, confidentiality and integrity are main security features, user and signaling data are considered sensitive and they should be protected between the UE and the serving network. Furthermore, in contrast with Universal Mobile Telecommunications Service (UMTS) where the data confidentiality and integrity had been ensured only in the air interface, normally between UE and Radio Network controller (RNC), these features in the EPS have been implemented in different levels to ensure more data security. 4G depends on using regular updating of the authentication process by exchanging sequence numbers in the messages of encryption mechanisms. The IPsec protocol and tunnels are also used for asserting the confidentiality of the user's data while transmitting traffic between 4G nodes. 4G end-to-end security involves availability with Authentication and Key Agreement (AKA). The foundation of 4G security is authenticating the UEs and wireless networks. This can be accomplished using the AKA process which asserts that the serving network authenticates the identity of a user and the UE certifies the network signature. The AKA creates encryption and integrity keys applied for originating various session keys for ensuring 4G security and privacy.

Confidentiality in 4G is covered in several works. Article [3] covers interoperability with legacy narrow-band systems and 4G networks and presents security challenges in confidentiality, authentication and non-repudiation. In [23] the authors presents a hybrid model approach to ensure a seamless transition from TETRA to LTE for Norway's public safety network, besides mentioning confidentiality, integrity, authentication and non-repudiation. In [24] the authors discuss an overview of communications for PPDR and its way towards the 4G commercial networks and introduces the security aspects of this process, referring to confidentiality, integrity, authentication and non-repudiation. [77] presents an evolution of TETRA systems to 4G commercial networks, besides to focused on network elements and allowing for low latency infrastructures and PMR encryption algorithms for user-to-network security and end-to-end encryption. In [85] the authors discuss PPDR operations by securely connecting the services run on their legacy networks to the 4G and 5G infrastructures and presents a framework of the security model with integrity, availability and confidentiality for PPDR agencies to this transition.

Regarding works on 4G integrity, article [9] highlights the history of LMR systems, presents the architecture of 4G for PPDR agencies, and provides deployment and migration solutions, besides mentioning requirements and security aspects like integrity and availability. The work in [84] introduces the 4G LTE, LTE-R, and LTE-M for PPDR networks focused on user priority-based resource allocation schemes to resolve significant challenges, such as co-channel interference, mission-critical user requirements, and QoS prioritization, besides mentioning security aspects how integrity and availability. In [86] the authors discuss mission-critical communications and 4G technology for a video service platform for first responders, besides mentioning QoS aspects, integrity and availability.

Authentication and non-repudiation in 4G was also researched in many works. Article [28] describes a new approach for exploiting the capabilities of new technologies and concepts of 4G for PPDR agencies, spectrum sharing

and cognitive radio in the FP7 Project, besides mentioning authentication, non-repudiation and availability. The work presented in [78] provides a strategy of evolution for PPDR over 4G networks and contributes towards Smart City evolution, besides mentioning authentication, non-repudiation and availability. Article [82] proposes a network architecture based on the integration of satellite and 4G networks and provides field operators and people in distress with transparent accessibility, coverage guarantees and broadband performance to expand their coverage, capacity and availability, besides mentioning authentication and non-repudiation.

Finally, availability is also addressed in many works. [22] examines the capability of 4G to provide requirements for PPDR systems and identifies possible future developments to enhance the ability of 4G to provide the necessary service, besides mentioning availability in the security aspects. In [29] the authors discuss the performance of 4G base stations deployed on airborne platforms, which provide coverage for first responders during emergencies, and concludes that 4G communication capabilities are up-and-coming candidates for robust communication links during emergency relief operations, besides mentioning availability as a crucial security aspect. Article [30] proposes a system architecture solution for PPDR and 4G commercial networks in a secure and interoperable manner and ensures through the dynamic management of prioritization policies, besides mentioning the availability as a critical security aspect. [31] analyzes the extension of the LTE/LTE-advanced (LTE-A)for PPDR agencies, and an overview of the technical features expected to turn the LTE standard into a mission-critical-capable technology is first provided, besides mentioning availability in field use cases. In [81] the authors discuss a detailed technical overview of the IOPS specifications and identifies several research prospects and development perspectives opened up by IOPS, and present a relatively novel concept in the 4G networks, besides mentioning availability in the security aspects. Article [83] presents a performance analysis and feasibility assessment of 4G when used to support a diverse set of emerging IoT applications ranging from mission-critical applications with a focus on devices with latency and availability requirements. Authors in [87] introduce the present works in 4G related to mission-critical communication and a future vision of 5G, besides mentioning availability with a requirement of this transition.

After that, with the introduction of IoT, 4G networks were unable to support initiatives such as Industrial Internet of Things (IIoT) and Internet of Life-Saving Things (IoLST). In 4G, different nodes perform different functions. One of the limitations of 4G is speed. Infrastructure nodes act as access points, while mobile nodes can only pass data to infrastructure nodes. 4G clients cannot pass data directly or communicate directly with another 4G client device without first talking to the infrastructure (a cell location), then to a switch, and vice versa. This makes 4G sufficient for delay-tolerant applications, such as intelligent metering. Still, it lacks the agility to support real-time IIoT platforms, such as Machine-to-Machine (M2M) communications or autonomy. Another limitation shown by 4G is flexibility and scalability. The 4G infrastructure does not adapt well to rapid increases in customer density. A cell phone station has a fixed number of connections that it can support, making it easier to overload the infrastructure's connection capacity. The 4G infrastructure also has elaborate static configurations that are not adaptable. The expansion of 4G networks requires the installation of new large and expensive towers. Besides, 4G networks have static structures and support only a limited number of simultaneous connections. Finally, there is a reliability limitation. A network that depends on infrastructure nodes creates points of failure. If an infrastructure node goes down, the mobile clients cannot access the network. In addition, the infrastructure and mobile nodes access only their respective dedicated frequencies, and the loss of line of sight can create connectivity challenges. There is no ideal way to get around signal blocking or interference. 5G networks have become developed to introduce more speed, low latency, security, and availability. In IoT environments that are more heterogeneous and require flexibility and scalability, functions such as SDN, NFV, and network slices, make 5G the appropriate technology for this scenario. Confidentiality and Integrity is guarantee in 5G networks, Subscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed Subscription Permanent Identifier (SUPI). The UE generates a SUCI using a protection scheme with the public key of the Home Network (HN) that was securely provisioned to the User SIM during the User SIM registration. Only the Mobile Subscriber Identification Number (MSIN) part of the SUPI gets concealed by the protection scheme while the home network identifier Mobile Country Code (MCC) and Mobile Network Code (MNC) gets transmitted in plaintext.The authentication and non-repudiation in 5G networks is provided by Service-based architecture (SBA), this service has been proposed for the 5G core network. Consequently, new entities and new service requests have also been defined in 5G. However, some of the new entities are relevant to 5G authentication as shown: The Security Anchor Function (SEAF), AUSF, UDM, and The Subscription Identifier De-concealing Function (SIDF). Similar to 4G, 5G authentication is carried out using the AKA method, in addition, they have introduced three new authentication methods: 5G-AKA, EAP-AKA', and EAP-TLS. Furthermore, Reliability is introduced in 5G networks as Ultra-Reliable Communication (URC), URC refers to the provision of a certain level of communication service almost 100% of the time. For example, URC applications include reliable cloud connectivity, critical connections for industrial automation and PPDR systems, and reliable wireless coordination between vehicles. In table 6, it is possible to verify the comparison between the PPDR systems approached in this survey, current, 4G, and 5G concerning these security requirements.

Confidentiality in 5G is addressed in [4], which introduces the feasibility, requirements and design challenges of 5G for mission-critical environments, besides mentioning security

TABLE 6. Coverage of security requirements in PPDR systems.

	Confidentiality	Integrity	Authentication and Non-Repudiation	Reliability
TETRA	End-to-end Encryption, AIE, Key Management, Over-the-air rekeying (OTAR)	Secret key K	Mutual authentication TETRA authentication algorithms (TAAs)	Self-recovery mechanisms (SDH/SONET), Voice + Data Communication, Direct Mode Operation (DMO)
TETRAPOL	End-to-end Encryption, Encryption diversity, Automatic rekeying	Access control	Mutual authentication, Signaling protection, Subscriber Identity Module	Voice + Data Communication, Direct Mode Operation (DMO)
P25	End-to-End Voice Encryption, Data CAI Encryption, AES or 3DES Encryption, OTAR, Multiple Keys, Link-Layer Encryption	KFD and KMF Interfaces, Key ID+Algorithm ID	Mutual authentication, Subscriber Validation	Voice + Data Communication, Direct Mode Operation (DMO)
DMR	End-to-end Encryption, Over-the-air encryption, Multiple Keys	SIM Card	Mutual authentication	Voice + Data Communication, Direct Mode Operation (DMO)
4G	Cipher algorithm EEA, Cipher key agreement, Encryption/Decryption of user, and signaling data	Integrity algorithm (EIA), Integrity key (IK) agreement, Data integrity feature	Mutual authentication, 4G EPS-AKA	IP Multimedia Subsystem (IMS), MCPTT, MCDATA, MCVIDEO, ProSe (Proximity Services)
5G	Subscription Concealed Identifier (SUCI), radio resource control (RRC) signaling, NR encryption algorithm (NEA)	MACs, Integrity protection algorithm (NIA)	Mutual authentication, 5G-AKA, EAP-AKA', and EAP-TLS	MCPTT, MCDATA, MCVIDEO, ProSe (Proximity Services), Ultra Reliable Low Latency Communication (URLLC), Network Slicing, Software-Defined Networking (SDN), Virtual Network Functions (VNF)

aspects like confidentiality and availability. [71] introduces a SDN-based network of 5G for both downlink and uplink transfers in order to provide public safety operators with broadband network capabilities and improved availability, besides mentioning confidentiality. In [76] authors discuss the application of SDN/NFV technology as a complement to 5G's network sharing between PPDR agencies and commercial mobile operations, mentioning the security aspects. [89] discusses the impact of the satellite channel characteristics on 5G communications, besides mentioning security challenges involving availability and confidentiality.

Integrity on 5G is addressed in many works. Article [88] provides an overview of the features of the 3GPP in 5G and introduces wearable devices and the concept of the IoLST, besides mentioning security aspects, e.g. integrity and availability. Authors in [90] introduce the PPDR network with satellite backhaul to ensure communication on the move with interoperability with 5G, besides mentioning security aspects, e.g. integrity, authentication and non-repudiation. In [91] the authors discuss the 5G evolution in Rel-15 and Rel-16, including security aspects such as integrity, authentication and non-repudiation. The work in [92] provides a practical framework for immersive aerial monitoring for PPDR agencies, focusing on 5G network performance on UAVs, besides mentioning security aspects. The work [93] provides an agile SDR broadband downlink system using 5G, including security aspects.

Availability on 5G is discussed on [64], where authors discuss the functionalities to meet the rigid requirements of PPDR use cases in terms of network slice reliability, resiliency, and security. [73] reviews PPDR services using 5G to deploy virtualized emergency services dynamically, besides mentioning the security aspects. In [74] the authors discuss the 5G ESSENCE project using SDN and NFV in 5G networks with flexible slices for dedicated mission-critical PPDR applications at the network's edge, also addressing availability. [80] presents the COHERENT project which focuses on developing an innovative programmable control and coordination framework that is aware of the underlying network topology, mentioning availability.

V. OPEN RESEARCH ISSUES AND OPPORTUNITIES

We proceed by identifying and discussing future research directions regarding the transition from current PPDR networks to 4G and future 5G networks. Furthermore, it presents the security challenges related to the context of 5G networks for PPDR systems.

The deployments and approaches for the 4G networks have already been executed and scrutinized over time, many authors have observed the requirements and challenges of the 4G network since its proposal in 2004 [3], [9], [22], [23], [24], [28], [29], [30], [31], [77], [78], [81], [82], [83], [84], [85]. In addition, there is already a consensus for the deployment of PPDR networks based on 4G, and many authors analyzed

this transition. The introduction of 5G, composed of a set of new characteristics such as URLLC and adaptable networks, created a high expectation on PPDR agencies regarding a possible transition. This chapter will focus on the main security challenges encountered.

A. CONFIDENTIALITY AND INTEGRITY

IoLST does not have a solid academic definition yet, but it is a recurring theme on the Internet and mainly on FirstNet in the USA. By definition, according to [88], the IoLST technologies are similar to the general meaning of the IoT, a network of devices that collect data and use various communication technologies to share it in real-time. Its purpose is specific and consists of improving PPDR responses to emergencies and disasters. The IoLST represents an extension of the current PPDR systems and PPDR over 4G capabilities, which are mainly targeting the connection of computing devices to the Internet. Furthermore, IoLST solutions extend the PPDR use cases into new types of applications, including, but not limited to, real-time video using body-worn cameras, traffic system control with sensor-equipped vehicles, temperature and gas exposure measurement based on smart helmets, healthcare, and vital sign monitoring of first responders, and drone surveillance systems. However, IoLST use cases involve a variety of devices, among which wearables are gaining the attention of the PPDR community, such as in proposals [88], [95]. As has been seen, security in mission-critical IoT environments is a relevant concern, and it is even more in IoLST. Authentication and encryption are crucial aspects of security in IoT environments, and key management becomes a vital security requirement in this regard. Many articles mention key management for IoT, and with the increase in devices and challenges in heterogeneous networks, a dynamic key management is essential. Finally, the use of IoT devices based on 5G networks is an excellent opportunity for future research, taking into account the creation of the IoLST networks and the investigation of requirements, limitations, performance, and security using 5G networks in mission-critical systems. There is a lack of papers regarding the dynamic keys management of IoLST devices for PPDR based on 5G networks, thus building a great opportunity for future research. Key management can be defined as a set of processes and mechanisms that support the key establishment and the maintenance of ongoing keying relationships between valid parties according to a security policy. Key management is a core mechanism to ensure network services and application security. In this sense, reliable distribution and management techniques of these keys are vital for safety in the IoT environment. Depending on the ability to update the cryptographic keys of devices during their runtime (rekeying), these schemes can be classified into two different categories: static and dynamic. In dynamic key management, the code keys of a device in the network's lifetime are updated, and the processes of updating the keys are conducted either periodically or based on requests. The rekeying process increases the resilience and resistance of the nodes to the attacks and consequently elongates the lifetime of a network. In new PPDR environments based on 5G, with the introduction of IoT devices, dynamic key management is essential to provide secure end-to-end encryption. Besides, the interconnection of Dynamic key management with ''Adaptive Security'' will be an excellent opportunity for future resources. The concern with the need for adaptive security comes from the case of different algorithms with different power requirements. Although some of them are connected to how exemplary and optimised, the actual implementation is, a considerable part is intrinsic to the specific algorithm. Therefore, when analysing authentication and encryption, a longer key is bound to produce higher requirements, even though it should also increase the complexity of cryptanalysis and the robustness of ciphertext. For this reason, when energy is a significant concern, having to commit to a specific algorithm will be a decision to be made. The concept of Adaptive Key Management is an excellent opportunity to be introduced in the PPDR networks based on 5G due to the lack of proposals in this sense. The improving the high security and energy efficiency that the proposal presents potential this essential security function for the new PPDR networks based on 5G.

B. AUTHENTICATION AND NON-REPUDIATION

Satellite communications (SatCom) refers to a wide range of systems operating in various frequency bands allocated by the International Telecommunication Union (ITU) to respectively Broadcast Satellite Services (BSS), Fixed Satellite Services (FSS), or Mobile Satellite Services (MSS). With the introduction of 5G technologies, the interoperability with SatCom is more attractive for PPDR agencies due to various technology integration initiatives. According to [89], 3GPP recognized the added value of SatCom and initiated several items of study and work on the implementation of 5G. There is an expectation in the interoperability between 5G networks and satellite networks, which would bring several benefits as a complement to 5G services in limited or underserved areas. It would improve 5G communications reliability and serve for M2M, IoT devices and Mission Critical services. In this sense, according to [71], it is impossible to guarantee acceptable properties of QoS, to field PPDR operators for data communication, without an interoperable structure between 5G and satellite communications, especially during major events, which networks are very congested and, in disaster situations that can damage or even destroy existing infrastructure. However, satellite communications also have inherent limitations: high propagation delay and low data rates. Some papers introduce a security architecture or a proposal on these security issues [107], [108], [109], but there is a lack of papers specifically concerning PPDR systems. [110] presents a reliability solution for PPDR systems, but not a complete security and interoperability solution. It is important to remember that rel 22.822 [111] of 3GPP does not yet present the security requirements for Satcom communications in 5G. Authentication and non-repudiation

are two core concepts in information security regarding the legitimacy and integrity of data transmission. When we transmit data, it is essential to verify the sender's origin (authentication) and ensure that during transmission, the data was not intercepted or altered in any way (integrity). When having both authenticity and integrity, the legitimacy of the data cannot be denied, and therefore, all parties can be confident in their data security (non-repudiation). Therefore, given the lack of standardization, non-repudiation is crucial to review in critical communications in SatCom for future work combined with authentication.

C. AVAILABILITY

Availability is an essential requirement for critical networks. For PPDR networks, mainly in the field, it is a central challenge for the system's proper functioning. 5G networks and their interoperability introduced better conditions for this environment. Adaptive security and virtualization are examples for future work in this direction.

1) ADAPTIVE SECURITY

Adaptive security is based on adjusting security measures according to the context. It concerns applications in which changes may occur in data sensitivity to security or in the threat level of the environment where the security service is deployed. Indeed, the application of adaptive security is directly related to the deployment environment. It requires the availability, at runtime, of information about threats or data sensitivity so that it can adjust the security level without compromising the security. Adaptive security reduces energy by adjusting security measures rather than systematically considering the worst case. This can be done by making parametrical or structural changes in the security protocols or simply by calling the protocol only when required.

Some articles mention adaptive security in IoT environments.

In the [113], the authors propose a scheme with self-and context-awareness in addition to a holistic view of security services at each layer of the communication stack. The proposed method uses distributed agents and intrusion detection systems to monitor the security threats and then dynamically adapts its security level by jointly considering several dimensions.

In the [114], authors describe a risk-based adaptive security framework for IoT devices in eHealth that estimates and predicts risk damages and future benefits using game theory and context-awareness techniques.

In the [115], the authors propose a game-based model for adaptive security in IoT devices, with an emphasis on eHealth applications. Furthermore, the authors use the trade-off between security-effectiveness and energy efficiency to evaluate adaptive security strategies.

However, there is a gap in articles on adaptive key management and mainly related to PPDR systems.

In the [116], the authors propose an adaptive solution that structures group members into clusters according to the application requirements in terms of synchronization and the membership change behaviour in the secure session. Furthermore, the authors made tests and presents an efficient solution in terms of security.

In the [117], the authors present an adapting key management process, this proposal adapts to the membership frequency during the multicast session. This protocol is called AKMP and tries to mitigate the inefficient solutions for real multicast sessions.

In the [118], the authors propose a privacy-preserving aggregation (PARK) scheme with adaptive key management and revocation, to preserve identity in the smart grid. Furthermore, the authors propose an adaptive key management mechanism with effective cancellation, where users can automatically update their encryption keys if no user joins or departs from the system. In this paper, the energy-awareness could be considered how validation of the proposal.

Despite all the research already done, adaptative security is not yet a reality and more work is needed especially for mission-critical scenarios. The lack of adaptative key management proposals is one example.

2) VIRTUALIZATION

Network Slicing, NFV, and SDN technologies, as introduced in chapter IV-B1, provide greater flexibility, robustness, and scalability to 5G networks, which makes them highly useful for PPDR systems. In the security context, the interest in SDN networks is evident, especially in IoT environments, not only related to the issue of dedicated hardware when SDN has multiple resources, but in the flexibility and scalability that SDN networks produce. It can maintain a global view of the network state and can be used to programmatically configure forwarding flow tables in the switches, thus enabling the NFV orchestration. NFV proposes to move the packet processing from hardware middleboxes toward software, thus providing possibilities for network optimization and cost reduction. Some papers show the combination of SDN and NFV to ensure more security in IoT environments [102],[103], [106], [107].

The dynamic Security Service Chaining (SSC) is one of the most typical use cases which are enabled by SDN and NFV. At the moment, dynamic SSC technology is still in its infancy [102]. However, the optimal SSC composition is one of the most challenging problems in the SDN and NFV enabled networks. Dynamic or Adaptive security is a topic extensively discussed in the IoT environment [104], [105], and therefore of interest to PPDR agencies, which can adapt their level of security according to the environment, situation, or the type of agency such as police, fireman, and emergency rescue. In this sense, for future research, this survey presents the idea of creating an IoT network for PPDR systems, which helps in the daily tasks of PPDR agencies, and which can be adaptive in several aspects, such as performance, security, and energy awareness using 5G networks and SDN and NFV features.

Adaptive security using SDN and NFV is a promising line of research in 5G networks, specially considering PPDR requirements.

VI. CONCLUSION

Current PPDR systems were designed to fulfil security requirements in a scenario focused on voice services. However, the enhanced data services required by today's public safety first responders, such as data and video transmission, are challenging for narrowband network communication technologies. As a result, current systems cannot provide the necessary bandwidth, speed, and performance to support the new required services. With the introduction of commercial broadband services and mobile devices, digital mobile solutions became available to complement and enhance traditional voice focused solutions, leading to a consensus between PPDR agencies on the need to transition to commercial 4G networks [3], [28] [30], [31]. The addition of a new set of devices to PPDR scenarios, and the adoption of IoT, together with new requirements of high speed, very low latency, scalability, and flexibility, is now demanding new approaches not fully addressed by 4G that 5G is trying to fulfil. Being a key moment to evaluate the existing systems and the new possibilities, this survey presents the evolution of PPDR system's requirements and technologies, focusing on security, from LMR systems to the last available generation of cellular networks. A discussion of the open research issues and opportunities needed to fulfil the security requirements of future PPDR systems is also provided.

REFERENCES

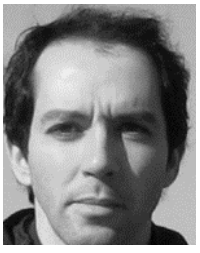
[1] A. R. Jamieson. (2004). *Radiocommunication for Public Protection and Disaster Relief*. (Jun. 19, 2022). [Online]. Available: https://www.itu.int/itunews/manager/display.asp
[2] K. Kunavut, "An overview of digital trunked radio: Technologies and standards," *J. Ind. Technol.*, vol. 10, pp. 111–121, May 2014.
[3] K. C. Budka, T. Chu, T. L. Doumi, W. Brouwer, P. Lamoureux, and M. E. Palamara, "Public safety mission critical voice services over LTE," *Bell Labs Tech. J.*, vol. 16, no. 3, pp. 133–149, Dec. 2011, doi: 10.1002/bltj.20526.
[4] O. N. C. Yilmaz, Y.-P.-E. Wang, N. A. Johansson, N. Brahmi, S. A. Ashraf, and J. Sachs, "Analysis of ultra-reliable and low-latency 5G communication for a factory automation use case," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 1190–1195, doi: 10.1109/ICCW.2015.7247339.
[5] R. Ferrus and O. Sallent, *Public Protection and Disaster Relief Communications in Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*. Hoboken, NJ, USA: Wiley, 2015, pp. 1–48, doi: 10.1002/9781118831243.ch1.
[6] T. Aven, "Identification of safety and security critical systems and activities," *Rel. Eng. Syst. Saf.*, vol. 94, no. 2, pp. 404–411, Feb. 2009, doi: 10.1016/j.ress.2008.04.001.
[7] M. Hinchey and L. Coyle, "Evolving critical systems: A research agenda for computer-based systems," in *Proc. 17th IEEE Int. Conf. Workshops Eng. Comput. Based Syst.*, Mar. 2010, pp. 430–435, doi: 10.1109/ECBS.2010.56.
[8] M. Kanerva, "Feasibility study on new services and markets technology enablers for critical communications," 3GPP, Tech. Rep. 22.8624, 2016.
[9] A. Jarwan, A. Sabbah, M. Ibnkahla, and O. Issa, "LTE-based public safety networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1165–1187, Jan. 2019, doi: 10.1109/COMST.2019.2895658.
[10] S. Duan, S. F. Mjølsnes, and J. K. Tsay, "Security analysis of the terrestrial trunked radio (TETRA) authentication protocol," Tech. Rep., 2013.
[11] D. W. Parkinson, "TETRA security," *BT Technol. J.*, vol. 19, no. 3, pp. 81–88, 2001, doi: 10.1023/a:1011942300054.
[12] SALUS. (2014). *Security and Privacy Analysis of TETRA/TETRAPOL PPDR, LTE and Wi-Fi Networks*. (Jun. 16, 2022). [Online]. Available: https://www.sec-salus.eu/wp-content/uploads/2014/05/SALUSD5.1v1.01.pdf
[13] (Jun. 16, 2022). *TETRAPOL*. [Online]. Available: http://tetrapol.com
[14] *TETRAPOL Digital Professional Mobile Radio*, WAVECOM, 2014.
[15] *Part 1: General Network Design*, TETRAPOL Specifications, 1999.
[16] (Aug. 22, 2019). Tait Radio Academy. *Radio Academy: Free Courses for Critical Communications. Tait Radio Academy | Free Educational Content about Critical Communications*. (Jun. 19, 2022). [Online]. Available: https://www.taitradioacademy.com/
[17] M. Rajarajan, F. Piper, H. Wang, and G. Kesidis, *Security and Privacy in Communication Networks*. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). 2012, doi: 10.1007/978-3-642-31909-9.
[18] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (special agent) Johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system," in *Proc. 20th USENIX Secur. Symp.*, 2011, pp. 1–16.
[19] (Jun. 19, 2022). Digital Mobile Radio Association. *Digital Mobile Radio Association | Supporting over 15 Million DMR Users worldwide*. [Online]. Available: https://www.dmrassociation.org/
[20] (Jun. 19, 2022). *Web Designer: Angelica Ayala Per Cléim*. Radio Activity Srl. Radio Activity. [Online]. Available: http://www.radioactivity-tlc.it/entutorials.html
[21] *Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Digital Mobile Radio (DMR) General System Design*, Standard ETSI TR 102 398, 2018.
[22] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, "LTE for public safety networks," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 106–112, Feb. 2013, doi: 10.1109/MCOM.2013.6461193.
[23] S. Milan. (2016). *Public Safety Networks Towards Mission Critical Mobile Broadband Networks*. [Online]. Available: http://hdl.handle.net/11250/2406853
[24] P. Silva and F. Velez, "Communications for public protection and disaster relief overview and vision towards the future," Tech. Rep., 2016.
[25] *3GPP System Architecture Evolution (SAE); Security Architecture*. document TS 33.922, V1.0.0, 3GPP, Oct. 2018.
[26] *Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)*, document 25.913, 3GPP, Release 7, V9.0.0, 2009.
[27] *Feasibility study for evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)*, document 25.912, Release 7, V16.0.0, 3GPP, 2020.
[28] G. Baldini, R. A. Ferré, J. O. Roig, P. Hirst, S. Delmas, and R. Pisz, "The evolution of public safety communications in Europe: The results from the FP7 HELP project," Tech. Rep., 2012.
[29] K. Gomez, T. Rasheed, L. Reynaud, and S. Kandeepan, "On the performance of aerial LTE base-stations for public safety and emergency recovery," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1391–1396, doi: 10.1109/GLOCOMW.2013.6825189.
[30] R. Ferrus, O. Sallent, G. Baldini, and L. Goratti, "LTE: The technology driver for future public safety communications," *IEEE Commun. Mag.*, vol. 51, no. 10, pp. 154–161, Oct. 2013, doi: 10.1109/MCOM.2013.6619579.
[31] R. Ferrus and O. Sallent, "Extending the LTELTE—A business case: Mission- and business-critical mobile broadband communications," *IEEE Veh. Technol. Mag.*, vol. 9, no. 3, pp. 47–55, Sep. 2014, doi: 10.1109/MVT.2014.2333695.
[32] (2014). 3GPP. *3GPP Release 11*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/specifications/releases/69-release-11
[33] (2015). 3GPP. *Release 12*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/specifications/releases/68-release-12
[34] (2015). 3GPP. *Release 13*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/release-13
[35] (2018). 3GPP. *Release 14*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/release-14
[36] (2018). 3GPP. *Release 15*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/release-15
[37] *Mission Critical Services Common Requirements (MCCoRe)*, document TS 22.280, V17.4.0, 3GPP, 2020.

[38] *Mission Critical Push to Talk (MCPTT)*, document TS 22.179, V17.0.0, 3GPP, 2019.
[39] *Mission Critical (MC) Data*, document TS 22.282, V16.4.0, 3GPP, 2018.
[40] *Mission Critical (MC) Video*, document TS 22.281, V16.0.0, 3GPP, 2018.
[41] *Proximity-Based Services (ProSe)*, document TS 23.303, V16.0.0, 3GPP, 2020.
[42] *Proximity-based Services (ProSe); Security Aspects*, document TS 33.303, V16.0.0, 3GPP, 2020.
[43] *Enhancements for Multimedia Priority Service (MPS)*, document TR 23.854, V11.0.0, 3GPP, 2011.
[44] *Policy and Charging Control Architecture*, document TS 23.203, V16.2.0, 3GPP, 2019.
[45] R. Hallahan and J. Peha, "Policies for public safety use of commercial wireless networks," Tech. Rep., 2010.
[46] *Report on Collective Use of Spectrum (CUS) and Other Spectrum Sharing Approaches*, Radio Spectrum Policy Group, 2011.
[47] R. Ferru, O. Sallent, G. Baldini, and L. Goratti, "Public safety communications: Enhancement through cognitive radio and spectrum sharing principles," *IEEE Veh. Technol. Mag.*, vol. 7, no. 2, pp. 54–61, Jun. 2012.
[48] (Jun. 19, 2022). FirstNet. *First Responder Network Authority*. [Online]. Available: https://firstnet.gov/
[49] *GSC Task Force on Emergency Communications (GSC-EM)*, Standard ITU-R WP5A-AR, 2014.
[50] (Jun. 19, 2022). ESN. *Emergency Services Network: Overview*. [Online]. Available: https://www.gov.uk/
[51] (Jun. 19, 2022). *EE*. [Online]. Available: https://ee.co.uk/
[52] (Jun. 19, 2022). *ASTRID*. [Online]. Available: https://www.astrid.be/en
[53] (Jun. 19, 2022). Korea Safe-Net. *Disaster and Safety Communications Network*. [Online]. Available: https://www.mois.go.kr/
[54] G. Baldini, O. Picchi, M. Luise, T. Sturman, F. Vergari, C. Moy, T. Braysy, and R. Dopico, "The Euler project: Application of software defined radio in joint security operations," *IEEE Commun. Mag.*, vol. 49, no. 10, pp. 55–62, Oct. 2011, doi: 10.1109/MCOM.2011.6035818.
[55] (Jun. 19, 2022). DISTEF. *Digital and Innovative Technologies for Security and Efficiency of First Responders Operation*. [Online]. Available: https://cordis.europa.eu/project/id/225404
[56] (Jun. 19, 2022). FP7 INFRA. *Innovative and Novel First Responders Applications*. [Online]. Available: https://cordis.europa.eu/project/id/225272
[57] (Jun. 16, 2022). SALUS. *Security and Interoperability in Next Generation PPDR Communication Infrastructures*. [Online]. Available: https://www.sec-salus.eu/salus/
[58] (Jun. 16, 2022). BROADMAP. *Mapping Interoperable EU PPDR Broadband Communication Applications and Technology*. [Online]. Available: http://www.broadmap.eu/
[59] (Jun. 19, 2022). ITU. *ITU: Committed to Connecting the World*. [Online]. Available: https://www.itu.int/en/Pages/default.aspx
[60] (Jun. 19, 2022). ETSI. *ETSI: European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/
[61] *IMT Vision—Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, Standard ITU-R M.2083-0, 2015.
[62] *Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s)*, Standard ITU-R M.2410-0, 2017.
[63] (2019). 3GPP. *Release 17*. (Jun. 19, 2022). [Online]. Available: https://www.3gpp.org/release-17
[64] A. Othman and N. A. Nayan, "Public safety mobile broadband system: From shared network to logically dedicated approach leveraging 5G network slicing," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2109–2120, Jun. 2021, doi: 10.1109/JSYST.2020.3002247.
[65] *Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)*, 3GPP, 2018.
[66] *NGMN Alliance*, 5G White Paper, V1.0, 2015.
[67] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.
[68] (Jun. 19, 2022). ETSI. *Network Functions Virtualisation: Introductory White Paper*. [Online]. Available: http://portal.etsi.org/NFV/NFVWhitePaper.pdf
[69] *Network Functions Virtualisation (NFV); Architectural Framework*, Standard ETSI GS NFV 002, V1.1.1, 2013.
[70] *Network Functions Virtualisation (NFV); Management and Orchestration*, Standard ETSI GS NFV-MAN 001, v1.1.1, 2014.
[71] M. Casoni, C. A. Grazia, and M. Klapez, "A software-defined 5G cellular network with links virtually pooled for public safety operators," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 3, p. e3092, Mar. 2017, doi: 10.1002/ett.3092.
[72] (Jun. 19, 2022). 5G PPP. *The 5G Infrastructure Public-Private Partnership*. [Online]. Available: https://5g-ppp.eu/
[73] M. G. Perez, A. H. Celdran, F. J. G. Clemente, and G. M. Perez, "Review and open challenges of public safety networks to manage emergency settings in 5G," in *Proc. 17th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, Jun. 2020, pp. 555–558, doi: 10.1109/ECTI-CON49241.2020.9158213.
[74] M. R. Spada, J. Perez-Romero, A. Sanchoyerto, R. Solozabal, M. A. Kourtis, and V. Riccobene, "Management of mission critical public safety applications: The 5G ESSENCE project," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2019, pp. 155–160, doi: 10.1109/EuCNC.2019.8802026.
[75] A. B. Letaifa, "SSIM and ML based QoE enhancement approach in SDN context," in *Advances in Computers*. 2019, pp. 151–196, doi: 10.1016/bs.adcom.2019.02.004.
[76] J. S. Marcus and G. Molnar, "Network sharing and 5G in Europe: The potential benefits of using SDN or NFV," *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3007398.
[77] M. Steppler, *Evolution of TETRA, White paper, P3 Communications*, 2011.
[78] A. Raza, "LTE network strategy for smart city public safety," in *Proc. IEEE Int. Conf. Emerg. Technol. Innov. Bus. Practices Transformation Societies (EmergiTech)*, Aug. 2016, pp. 34–37, doi: 10.1109/EmergiTech.2016.7737306.
[79] *Study on New Services and Markets Technology Enablers*, document TR 22.891, V14.2.0, 3GPP, 2016.
[80] A. Kostopoulos, G. Agapiou, F.-C. Kuo, K. Pentikousis, A. Cipriano, D. Panaitopol, D. Marandin, K. Kowalik, K. Alexandris, C.-Y. Chang, N. Nikaein, M. Goldhamer, A. Kliks, R. Steinert, A. Mammela, and T. Chen, "Scenarios for 5G networks: The COHERENT approach," in *Proc. 23rd Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–6, doi: 10.1109/ICT.2016.7500421.
[81] J. Oueis, V. Conan, D. Lavaux, R. Stanica, and F. Valois, "Overview of LTE isolated E-UTRAN operation for public safety," *IEEE Commun. Standards Mag.*, vol. 1, no. 2, pp. 98–105, Jul. 2017, doi: 10.1109/MCOMSTD.2017.1600875.
[82] M. Casoni, C. A. Grazia, M. Klapez, N. Patriciello, A. Amditis, and E. Sdongos, "Integration of satellite and LTE for disaster recovery," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 47–53, Mar. 2015, doi: 10.1109/MCOM.2015.7060481.
[83] A. Hassebo, M. Obaidat, and M. A. Ali, "Commercial 4G LTE cellular networks for supporting emerging IoT applications," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, Feb. 2018, pp. 1–6, doi: 10.1109/ICASET.2018.8376832.
[84] I. Ahmad and K. Chang, "Mission-critical user priority-based cooperative resource allocation schemes for multi-layer next-generation public safety networks," *Phys. Commun.*, vol. 38, Feb. 2020, Art. no. 100926, doi: 10.1016/j.phycom.2019.100926.
[85] D. Kim, D. H. Gu, and H. K. Kim, "Beyond PS-LTE: Security model design framework for PPDR operational environment," 2020, *arXiv:2009.12116*.
[86] C. A. García-Pérez, A. Rios, P. Merino, K. Katsalis, N. Nikaein, R. Figueiredo, D. Morris, T. O'Callaghan, and P. Rodriguez, "23 Q4 health: Mission critical communications over LTE and future 5G technologies," Tech. Rep., 2016.
[87] F. Bader, L. Martinod, G. Baldini, F. Frantz, S. Kandeepan, and O. Sallent, "Future evolution of public safety communications in the 5G era," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 3, p. e3101, Mar. 2017, doi: 10.1002/ett.3101.
[88] S. Saafi, J. Hosek, and A. Kolackova, "Cellular-enabled wearables in public safety networks: State of the art and performance evaluation," in *Proc. 12th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2020, pp. 201–207, doi: 10.1109/ICUMT51630.2020.9222459.
[89] A. Guidotti, S. Cioni, G. Colavolpe, M. Conti, T. Foggi, A. Mengali, G. Montorsi, A. Piemontese, and A. Vanelli-Coralli, "Architectures, standardisation, and procedures for 5G satellite communications: A survey," *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107588, doi: 10.1016/j.comnet.2020.107588.

[90] F. Völk, R. T. Schwarz, M. Lorenz, and A. Knopp, "Emergency 5G communication on-the-move: Concept and field trial of a mobile satellite backhaul for public protection and disaster relief," *Int. J. Satell. Commun. Netw.*, vol. 39, no. 4, pp. 417–430, Jul. 2021, doi: 10.1002/sat.1377.
[91] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019, doi: 10.1109/ACCESS.2019.2939938.
[92] S. Seo, S. Kim, and S.-L. Kim, "A public safety framework for immersive aerial monitoring through 5G commercial network," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2020, pp. 1–6, doi: 10.1109/WCNCW48565.2020.9124805.
[93] O. Font-Bach, N. Bartzoudis, X. Mestre, D. Lopez-Bueno, P. Mege, L. Martinod, V. Ringset, and T. A. Myrvoll, "When SDR meets a 5G candidate waveform: Agile use of fragmented spectrum and interference protection in PMR networks," *IEEE Wireless Commun.*, vol. 22, no. 6, 56–66, Dec. 2015, doi: 10.1109/MWC.2015.7368825.
[94] *Mission Critical Services over 5G System*, document TS 23.289, V0.3.0, 3GPP. 2021.
[95] (Jun. 19, 2022). *5G Mobilizer Project Consortium*. [Online]. Available: https://5go.pt/
[96] R. Nossenson, "Long-term evolution network architecture," in *Proc. IEEE Int. Conf. Microw., Commun., Antennas Electron. Syst.*, Nov. 2009, pp. 1–4, doi: 10.1109/COMCAS.2009.5385947.
[97] S. Nashwan, "SAK-AKA: A secure anonymity key of authentication and key agreement protocol for LTE network," *Int. Arab J. Inf. Technol.*, vol. 14, pp. 790–801, Sep. 2017.
[98] Standard ETSI TS 123 501, V15.3.0, 2018.
[99] A. Sutton, "5G network architecture," *ITP J.*, vol. 12, no. 1, pp. 9–15, 2018.
[100] document TS 33.401, 3GPP, version 15.7.0, Release 15, 2019.
[101] Y. Liu, Y. Lu, W. Qiao, and X. Chen, "A dynamic composition mechanism of security service chaining oriented to SDN/NFV-enabled networks," *IEEE Access*, vol. 6, pp. 53918–53929, 2018, doi: 10.1109/ACCESS.2018.2870601.
[102] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, Aug. 2019, doi: 10.1109/COMST.2018.2862350.
[103] L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, "A self-adaptive deep learning-based system for anomaly detection in 5G networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018, doi: 10.1109/ACCESS.2018.2803446.
[104] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy efficiency in security of 5G-based IoT: An end-to-end adaptive approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6589–6602, Jul. 2020, doi: 10.1109/JIOT.2020.2974618.
[105] D. Ageyev, O. Bondarenko, W. Alfroukh, and T. Radivilova, "Provision security in SDN/NFV," in *Proc. 14th Int. Conf. Adv. Trends Radioelecrtronics, Telecommun. Comput. Eng. (TCSET)*, Feb. 2018, pp. 506–509, doi: 10.1109/TCSET.2018.8336252.
[106] I. Farris, J. B. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Sep. 2017, pp. 169–174, doi: 10.1109/CSCN.2017.8088617.
[107] H. Saarnisaari and C. M. de Lima, "5G new radio in SATCOM: An overview of physical and medium access layer issues," in *Proc. 22nd Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2020, pp. 1–4, doi: 10.1109/ICTON51198.2020.9203099.
[108] K. Bernsmed, C. Froystad, P. H. Meland, and T. A. Myrvoll, "Security requirements for SATCOM datalink systems for future air traffic management," in *Proc. IEEE/AIAA 36th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2017, pp. 1–10, doi: 10.1109/DASC.2017.8102083.
[109] A. Knopp, R. T. Schwarz, and B. Lankl, "Secure MIMO SATCOM transmission," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2013, pp. 284–288, doi: 10.1109/MILCOM.2013.56.
[110] H. Gierszal, E. Sdongos, L. Kiedrowski, D. Korzeniowki, K. Plucinski, L. Brajer, P. Tyczka, P. S. Antonio, M. Tsagkaropoulos, N. McCrone, and J. Jackson, "Reliability of SATCOM transmission for PPDR usage," in *Proc. IEEE 12th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2016, pp. 1–4, doi: 10.1109/WiMob.2016.7763172.
[111] *Study on using satellite access in 5G*, document TR 22.822, V16.0.0, 3GPP, 2018.
[112] *Project 25 Digital Land Mobile Radio—Security Services Overview*, document TIA 102, 2018.
[113] E. Nigussie, A. Hakkala, S. Virtanen, and J. Isoaho, "Energy-aware adaptive security management for wireless sensor networks," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2014, pp. 1–4, doi: 10.1109/WoWMoM.2014.6919023.
[114] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 269–275, doi: 10.4108/icst.bodynets.2012.250235.
[115] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 920–925, doi: 10.1109/ICC.2014.6883437.
[116] Y. Challal, H. Bettahar, and A. Bouabdallah, "SAKM," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 55–70, Apr. 2004, doi: 10.1145/997150.997157.
[117] H. Bettahar, A. Bouabdallah, and Y. Challal, "AKMP: An adaptive key management protocol for secure multicast," in *Proc. 11th Int. Conf. Comput. Commun. Netw.*, Oct. 2004, pp. 190–195, doi: 10.1109/ICCCN.2002.1043065.
[118] K. Zhang, R. Lu, X. Liang, J. Qiao, and X. S. Shen, "PARK: A privacy-preserving aggregation scheme with adaptive key management for smart grid," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2013, pp. 236–241, doi: 10.1109/ICCChina.2013.6671121.
[119] (2022). 3GPP. *Release 16*. (Jun. 16, 2022). [Online]. Available: https://www.3gpp.org/release-16
[120] A. M. Voicu, L. Simić, and M. Petrova, "Survey of spectrum sharing for inter-technology coexistence," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1112–1144, 2nd Quart., 2018.
[121] (Jun. 19, 2022). Tetra-MOU. *TETRA Memorandum of Understanding (MOU)*. https://www.tetramou.com/.
[122] (Jun. 19, 2022). *IWCE's Urgent Communications Magazine*. [Online]. Available: https://urgentcomm.com/2019/09/13/motorola-solutions-announces-plans-to-deploy-mototrbo-nitro-commercially-in-3-5-ghz-cbrs-band/
[123] (2022). 3GPP. *Release 18*. (Jun. 16, 2022). [Online]. Available: https://www.3gpp.org/release-18

FLORIANO NETO is currently pursuing the Ph.D. degree with the Department of Informatics Engineering, Faculty of Science and Technology, University of Coimbra, Portugal, through the Doctoral Program in Information Sciences and Technologies Computer Science. He has worked in national and international companies generally in the area of information technology, focusing on computer networks and SQL databases. He is also in the academic area as a Professor, a Content Creator, a Scientific Researcher, and a Consultant in innovation and startups.

JORGE GRANJAL (Member, IEEE) received the Ph.D. degree, in 2014. He is currently an Assistant Professor with the Department of Informatics Engineering, Faculty of Science and Technology, University of Coimbra, Portugal. He is also a Researcher with the Laboratory of Communication and Telematics, Centre for Informatics and Systems, University of Coimbra. His current research interests include computer networks, network security, and wireless sensor networks. He is also a member of the ACM Communications Groups.



VASCO PEREIRA received the Ph.D. degree in informatics engineering from the University of Coimbra (UC), in 2016. He is currently an Assistant Professor at the Department of Informatics Engineering, UC, and the Vice-Coordinator of the bachelor's degree in informatics engineering. He is also a Senior Researcher at the Centre of Informatics and Systems, UC. His research interests include computer networks, network security, QoS, the IoT, and 5G networks. For more information visit the link (http://www.uc.pt/go/vasco).