

Received February 5, 2022, accepted March 9, 2022, date of publication March 16, 2022, date of current version March 28, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3160193

A Survey on LPWAN-5G Integration: Main Challenges and Potential Solutions

YU CHEN^{ID}, (Student Member, IEEE), **YUSUF A. SAMBO**^{ID}, (Member, IEEE),
OLUWAKAYODE ONIRETI^{ID}, (Senior Member, IEEE), AND
MUHAMMAD A. IMRAN^{ID}, (Senior Member, IEEE)

James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.

Corresponding author: Yu Chen (y.chen.5@research.gla.ac.uk)

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) Global Challenges Research Fund—the DARE Project under Grant EP/P028764/1.

ABSTRACT The popularity of Internet of Things (IoT) has resulted in increased deployments of Low Power Wide Area (LPWA) technologies for both commercial and private services due to their performance and cost advantages. Although Low Power Wide Area Networks (LPWANs) have the advantages of low power consumption, wide coverage, low-cost and scalability, they generally have lower data rates and lower reliability, thus limiting their suitability for a wider range of industrial use cases such as process control and high data rate multimedia applications. To overcome this, LPWA technologies can be integrated into 5G, a flexible, scalable, agile and programmable mobile communication system. In this paper, we provide a survey on LPWAN-5G integration focusing on the main integration challenges and potential solutions. We firstly compare popular licensed and unlicensed LPWA technologies, and then introduce the 5G architecture and enabling technologies for LPWAN-5G integration. Finally, we discuss in detail the challenges and potential solutions of LPWAN-5G integration, covering all the important aspects including hybrid architecture, security, mobility, interoperability between LPWANs, and coexistence with other wireless technologies. From our analysis, it can be seen that LPWAN-5G integration tends to evolve from access network to core network.

INDEX TERMS 5G, cellular, converged core network, the Internet of Things, low power wide area network.

I. INTRODUCTION

Digital connectivity has changed the world by bridging the distance between people and making it a global village. Compared to previous generations, 5G is a flexible, scalable, agile and programmable communication system that can support integration with other technologies [1]. The authors in [2] argue that 5G will complement other wired and wireless technologies, and propose a general model for the integration of 5G into industrial Ethernet systems. This kind of integration can be applied to some industrial production scenarios such as connected homogeneous islands, virtualized controller, and versatility with virtualization and remote site [3]. The trend in Industry 4.0 [4] is to replace wired technologies with wireless technologies wherever

possible, given the advantages of wireless networks such as flexibility, mobility and ease of deployment. Moreover, the Industry 4.0 paradigm will be driven by the Internet of Things (IoT), which will support machine-to-machine (M2M) communications [5].

IoT applications can be segmented into four categories: Massive IoT, Broadband IoT, Critical IoT and Industrial Automation IoT [6]. Given that these categories have unique requirements, the 3GPP defines three application scenarios for IoT: 1) massive Machine Type Communication (mMTC) for massive IoT, 2) enhanced Mobile Broadband (eMBB) for Broadband IoT, 3) Ultra-Reliable and Low-Latency Communications (URLLC) for both Critical IoT and Industrial Automation IoT [7]. Characterized by low data rate, low power consumption and wide-area coverage, Low-Power Wide Area (LPWA) technologies, such as Narrowband Internet of Things (NB-IoT) [8], Long Range Wide Area

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau^{ID}.

Network (LoRaWAN) [9] and SigFox [10], are an important class of alternatives to 5G networks for Massive IoT applications [11], [12].

The global IoT connections increased by 9% to 12.3 billion in 2021 according to IoT Analytics [13] and are forecasted by GSMA to reach 25 billion by 2025 [14]. The popularity of IoT has resulted in increased deployments of LPWA technologies for both commercial and private services due to their performance and cost advantages. In 2021, Low Power Wide Area Networks (LPWANs) became the main driver for the growth of the IoT connections globally and are expected to replace most 2G/3G IoT connections in the future [15]. With the rapid increase of end devices, billions of machines need to be connected to the network. A single cellular network cannot offer ubiquitous coverage and is hard to support substantial connectivity [16]. With the capability of processing huge data traffic, LPWANs are expected to bring great evolution into 5G ecosystem [17]. This paper will comprehensively survey the integration of LPWAN and 5G.

A. MOTIVATION BEHIND LPWAN-5G INTEGRATION

The two main motivations behind LPWAN-5G integration are discussed as follows:

1) As one of the three application scenarios of 5G, mMTC can provide connectivity for billions of IoT end devices with a density of 1 million/km². Given the substantial number of connections, key requirements for end devices are low cost, low power consumption and wide coverage, and these cannot be supported by cellular technologies alone. LPWANs can provide a trade-off between the limitations of current cellular technologies and current mMTC requirements [18].

2) Although LPWANs have the advantages of low power consumption, wide coverage, low-cost and scalability, they generally have lower data rates and lower reliability, thus limiting their suitability for a wider range of industrial use cases such as process control and high data rate multimedia applications. To overcome this, industrial operators often deploy both cellular networks and LPWAN to support industrial use cases. Unfortunately, this dual deployment model is complex, and expensive to deploy and manage. Commercial 5G systems have been deployed progressively since 2018. Due to its boundary stretching performance metrics, the 5G system can provide the backbone connectivity and management functions for LPWANs, which can significantly reduce complexity, cost and improve the resilience of LPWANs deployment.

B. CONTRIBUTIONS

Given their popularity, LPWANs have received considerable attention from the research community with a sizeable number of surveys and tutorials published. The authors in [19] discuss the cause of the diversity of LPWA technologies and argue the need of interoperability between them. The authors in [20] identify interoperability between various wireless technologies, including LPWANs and 5G, as one of the main challenges of 5G networks. Although the two surveys

mention LPWAN-5G integration, they do not discuss the integration in detail as they have relatively wider topics, i.e. 5G networks for IoT, and enabling technologies of LPWANs respectively. An in-depth survey of the security challenges of integrating LPWAN into 5G has been provided in [21]. Although security is an important factor, the survey does not cover other aspects of LPWAN-5G integration. Moreover, it does not compare different LPWANs and especially the difference between licensed and unlicensed LPWANs is not discussed.

In this paper, we provide a survey and tutorial on LPWAN-5G integration for hybrid networks. To be specific, we present an overview of 5G and LPWANs, and evaluate five important aspects of LPWAN-5G integration, including hybrid architecture, security, mobility, interoperability between LPWANs and coexistence of LPWAN with other wireless technologies. We further discuss the challenges and propose potential solutions towards achieving LPWAN-5G integration. The comparison with other related LPWAN surveys is shown in Table 1.

The rest of this paper is structured as follows. In Section II, we introduce and compare nine popular LPWAN technologies which are classified into licensed LPWANs and unlicensed LPWANs. In Section III, 5G network architecture and enabling technologies are introduced. In Section IV, we discussed the five challenges of LPWAN-5G integration, followed by the potential solutions for these challenges in Section V. Finally, we conclude the paper and discuss the future research directions in Section VI.

II. LPWAN TECHNOLOGIES

LPWAN [25] is a class of communication technologies characterized by low power consumption, low data rate, and wide-area coverage, which are perfectly suitable for most IoT applications such as smart cities, smart agriculture, connected industries, etc. As a promising solution for IoT and M2M communication, LPWAN can provide billions of connections at a lower cost than conventional cellular systems.

LPWAN can be classified into two types: cellular LPWAN and non-cellular LPWAN. Cellular LPWAN technologies, such as NB-IoT, enhanced Machine Type Communication (eMTC) and Extended Coverage Global System for Mobile Communication IoT (EC-GSM-IoT), are introduced by 3GPP, operating in licensed cellular frequency bands. They are designed to seamlessly integrate with cellular networks and rely on the infrastructure of the cellular network. Unlike cellular LPWAN, non-cellular LPWAN technologies, such as LoRaWAN, SigFox and Random Phase Multiple Access (RPMA), are designed independently of cellular systems. Working in unlicensed bands (mostly in sub-GHz ISM bands), non-cellular LPWAN technologies are run by both public and private operators. In this section, we will introduce and compare nine popular LPWAN technologies including NB-IoT, eMTC, EC-GSM-IoT, LoRaWAN, SigFox, RPMA, DASH7, Weightless and Telensa. Their key performance indicators (KPIs) are listed in Table 2.

TABLE 1. Comparison with related survey works.

	LPWAN-5G integration	Comparison of LPWANs	5G Architecture	Integrated architecture	Security	Mobility	Interoperability among LPWANs	Coexistence with other technologies
[21]	✓	×	✓	×	✓	×	×	×
[20]	✓	✓	×	×	✓	×	×	×
[19]	✓	✓	×	×	✓	×	✓	✓
[22]	×	✓	×	×	✓	✓	✓	✓
[23]	×	✓	×	×	✓	×	✓	×
[24]	×	✓	×	×	×	✓	✓	✓
This paper	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 2. Comparison of cellular and non-cellular LPWANs [26]–[28].

	NB-IoT	eMTC	EC-GSM-IoT	LoRaWAN	SigFox	RPMA	DASH7	WEIGHTLESS-W	WEIGHTLESS-N	WEIGHTLESS-P	TELENSA
Licensed Cellular	YES	YES	YES	NO	NO	NO	NO	YES	NO	YES/NO	NO
Standardization group	3GPP	3GPP	3GPP	LoRa Alliance	SigFox	Ingenu	DASH7 Alliance	Weightless SIP	Weightless SIP	Weightless SIP	Telensa
Frequency (MHz)	700-900	700-900	800-900	EU 868, EU 433, US 915, CN 490, AS 923, etc.	EU 868, EU 433, USA 915	2400	433, 868, 915	TV whitespace (470-790)	EU 868, US 915	Sub-GHz (169/433/470/780/868/915/923MHz or licensed)	EU 868, US 915, Asia 430
Bandwidth (Hz)	180k or 200k	1.08M	200k	125k, 250k, 500k	200k (100k each)	1M	200k	5M	200	12.5k	100k
Range (km)	1 (urban), 10 (rural)	<11	<15	2-5 (urban), 10-20 (rural)	3-10 (urban), 30-50 (rural)	5 (urban), 15 (rural)	0-5	5	2	5	3 (urban), 8 (rural)
Security	3GPP based	3GPP based	3GPP based	Two-layer AES-128b	AES-128b	AES-256b	AES-128b	AES-128b	AES-128b	AES-128b/256b	/
Modulation	BPSK, QPSK	QPSK, 16QAM	GMSK/8PSK	CSS	BPSK	DSSS for UL, FSK for DL	GFSK	16-QAM, offset-BPSK	DBPSK	GMSK and offset-QPSK	UNB 2-FSK
Adaptive data rate	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO
Payload (bytes)	1600	/	/	0-243	12 (UL), 8 (DL)	6-10k	20	>10	20	>10	65k
Data rate (bps)	200k	1M	70k/240k	300-50k	100 or 600	20k	200	1k-10M	200-100k	30-100k	62.5 (UL), 500 (DL)
Network Topology	Star	Star	Star	Star	Star	Star/Tree	Tree/Star	Star	Star	Star	Star/Tree

A. LICENSED LPWAN

1) NB-IoT

NB-IoT [29] was standardized by 3GPP in Release 13 [30] in 2016. Based on Long Term Evolution (LTE), NB-IoT is introduced to achieve M2M communication with the demand of low cost, low power, long-distance and massive capacity [31]. Due to these characteristics, NB-IoT can be classified as a LPWAN technology. Facilitating radio network evolution and efficient coexistence with Mobile Broadband (MBB), NB-IoT can share the same infrastructure as LTE [32]. NB-IoT can be deployed in three operation modes including standalone mode, in-band mode and guard band mode. In standalone mode, NB-IoT operates in a dedicated band re-farmed from Global System for Mobile Communication (GSM) with a bandwidth of 200 kHz. In in-band mode, NB-IoT is allocated a LTE carrier with a

bandwidth of 180 kHz. In guard band mode, NB-IoT utilizes the unused guard band (180 kHz) of LTE which is located at the edge of the LTE band. The collision and interference between LTE and NB-IoT may occur when NB-IoT operates in in-band mode or guard mode even though their power spectrum density is restricted [33]. NB-IoT is currently operated by many cellular operators in their 4G systems.

2) EMTc

In addition to NB-IoT, 3GPP Release 13 also introduces eMTC which is an amendment of the LTE-Machine-to-Machine (LTE-M) [34] standard. Compared with Machine Type Communication (MTC) in 3GPP Release 12, eMTC can provide extended coverage (less than 11 km) with lower device complexity, lower power consumption [35]. Compared with other LPWAN technologies, eMTC can

provide a comparatively high data rate of 1 Mbps at the cost of occupying a relatively wider frequency bandwidth of 1.08 MHz within LTE band. Utilizing Power Savings Management (PSM) and extended Discontinuous Reception (eDRX), the battery life of eMTC can be extended to over 10 years [36]. However, due to the relatively extended coverage and higher data rate, the cost of eMTC end devices is increased, making it have no price advantage [37].

3) EC-GSM-IoT

2G cellular network is the first global digital mobile network that has extensive coverage in the world. So, utilizing GSM, 3GPP introduced EC-GSM-IoT [38] for IoT application. Operating in the GSM frequency band with a narrow bandwidth of 200 kHz, EC-GSM-IoT can provide long-range communication of up to 15 km. However, GSM is not specifically designed for IoT applications, resulting in the relatively higher power consumption of EC-GSM-IoT. The battery life of EC-GSM-IoT is shorter than other LPWAN technologies due to the relatively high transmitting power of GSM end devices.

B. UNLICENSED LPWAN

1) LoRaWAN

LoRaWAN is one of the most popular LPWA IoT networks [39]–[42]. With regard to 5G mMTC use cases especially those without time-critical requirements, LoRaWAN is a potential complementary solution for the 5G network. It can achieve around 10% of the 5G mMTC connection density objective in the uplink [43]. LoRaWAN is a Medium Access Control (MAC) layer standard based on LoRa (Long Range) Physical layer standard proposed by Semtech [44] and promoted by the LoRa Alliance [39]. LoRa operates in unlicensed Industrial, Scientific and Medical (ISM) bands with a bandwidth of 125 kHz. According to the Regional Parameters [45] proposed by LoRa Alliance, nine different ISM bands are specified for different regions. In the EU, there are two available bands including EU 863-870MHz ISM band and EU 433MHz ISM band. The key technology of LoRa is the Chirp Spread Spectrum (CSS) modulation which will generate a chirp signal for every single bit of data in the same time duration. This kind of modulation enables long-range end-to-end communication which can usually reach 2-5 km in urban areas and 15 km in suburban areas. In [46], the authors conduct a practical experiment using EU 868 MHz ISM band and 14 dBm transmit power, showing the maximum communication range of LoRa is 15 km on the ground and close to 30 km on water. However, due to the CSS modulation, LoRa is only suitable for low data rate communication.

Benefiting from the feature of LoRa, LoRaWAN is designed in MAC layer level to achieve long-range, low power and low data rate communication which is perfectly suitable for IoT networks. As shown in Figure 1, LoRaWAN has a star topology with multiple gateways supporting end devices, LoRaWAN servers and application servers. For the uplink, the packets from an end device should be received

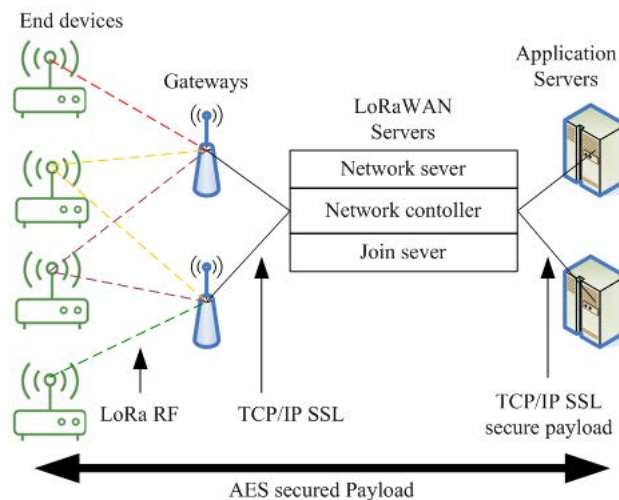


FIGURE 1. The architecture of LoRaWAN.

and forwarded by all the gateways that can receive the packets. The gateways then forward the packets to the LoRaWAN servers including the network server, the network controller and the join server. These servers are responsible for controlling the network and determining the network parameters. Specifically, the Adaptive Data Rate (ADR) is a key function realized by these servers which specify a minimum transmitting power for each end node by adjusting its data rate in the range of 300 to 50k bps. In doing so, the lowest power consumption of the whole network can be achieved. Finally, LoRaWAN servers also send the frame payloads of the message to application servers for a variety of use cases.

For the downlink, LoRa Alliance defines three kinds of end nodes including class A (baseline), class B (beacon) and class C (continuous) in the LoRaWAN specification [39]. Class A end devices can receive message only in two short downlink receiving windows following every uplink transmission. Compared with class A, class B end devices can open an extra periodic receiving window for downlink message reception. Class C end devices keep the receiving window open all the time. The three kinds of end devices can be chosen for different use cases to achieve the lowest power consumption. A well-configured LoRaWAN end device powered by a battery of 2400 mAh can achieve a 6-year lifetime when communicating infrequently [47]. In terms of security, LoRaWAN adopts Message Integrity Code (MIC) and two-layer Advanced Encryption Standard (AES) secured encryption. Each frame and each MAC layer message have a MIC to ensure the integrity of each packet. Further, the application session has a different encryption key from the network session. In doing so, the network operator cannot decrypt the payload data of each application, ensuring the privacy of application users.

2) SigFox

SigFox [48] is a typical LPWA technology proposed by its operator which is also named SigFox. Based on Low

Throughput Network (LTN) [49], SigFox has similar star network architecture to LoRaWAN. The packets sent from objects, i.e., the end nodes of SigFox, can be received by any base stations in the range. Then all the packets are forwarded to the SigFox Cloud to be processed and subsequently, the application payload would be transmitted to the corresponding application server. Unlike LoRaWAN in which the network infrastructure is operated by several independent operators having joined the LoRa Alliance, the infrastructure of SigFox is operated by SigFox itself.

Operating in unlicensed bands such as EU 433 MHz, EU 868 MHz and USA 915 MHz, SigFox adopts Binary Phase Shift Keying (BPSK) [50] modulation in ultra-narrowband which is 100 Hz wide for each message. The message payload is confined within 12 bytes for uplink transmission and 8 bytes for downlink transmission, which is very limited but enough for many sensor data transmissions such as GPS location, temperature and speed. Unlike the ADR of LoRaWAN, the data rate of SigFox is fixed to 100 or 600 bps depending on the region. Given that the bandwidth, payload size and data rate are limited, SigFox can achieve long-distance communication [51], [52] and low power consumption [53]. In rural areas, SigFox can cover a range of 30-50 km while in urban areas the distance is reduced to 3-10 km. Due to low power consumption, the battery life can be significantly extended which is predicted to be over 10 years.

3) RPMA

RPMA [54] is a proprietary LPWAN technology proposed and operated by Ingenu which is an American company founded in 2008. Unlike other LPWAN technologies that use different sub-GHz frequency bands in different regions, RPMA adopts a unified unlicensed 2.4 GHz ISM band all over the world, which is beneficial for roaming across regions. The bandwidth of RPMA reaches 1 MHz, which is also much wider than other LPWAN technologies. In the physical layer, Direct Sequence Spread Spectrum (DSSS) is employed as the modulation method for uplink transmission and a single time slot can be shared by multiple transmitters [55]. In the downlink transmission, RPMA adopts the Frequency Shift Keying (FSK) modulation technique [56]. This physical layer standard has been made to comply with IEEE 802.15.4k, which is a low-power critical infrastructure monitoring networks standard. RPMA can cover a range of 15 km in rural areas and 5 km in urban areas with a payload size of up to 10 kB [57]. In terms of security, RPMA adopts AES-256b based encryption.

4) DASH7

Stemming from ISO 18000-7 Radio-frequency Identification (RFID) [58], DASH7 [59], [60] is an open-source LPWAN standard proposed by DASH7 Alliance. With the modulation technique of Gaussian Frequency Shift Keying (GFSK) [61], DASH7 operates in the sub-GHz ISM bands including 433 MHz, 868 MHz and 915 MHz. It is designed for

ultra-low-power sensor-actuator applications where sensors can report data and actuators can receive commands typically within a latency of 1 second but only consuming 30 uA on average. Offering data rates up to 200 kbps, DASH7 can cover a range of 0-5 km.

5) WEIGHTLESS

Weightless [62] is an open LPWAN technology operated in sub-GHz frequency bands and managed by Weightless Special Interest Group (Weightless SIG). This technology consists of three types of standards including Weightless-W, which operates on licensed bands, and Weightless-N and Weightless-P that both operate on unlicensed bands. They have similar network architecture but the coverage and power consumption of the three stands are different to meet the demands of different use cases.

Based on LTN, Weightless-N [63] is the second standard released by Weightless SIG. With the Differential Binary Phase Shift Keying (DBPSK) modulation scheme, Weightless-N operates in ISM Sub-GHz bands including EU 868 MHz and US 915 MHz with an ultra-narrow bandwidth. To relieve spectrum collision, a special frequency hopping method is used by Weightless-N to randomly select a channel for each transmission [64]. Weightless-N can cover a range of 2 km with 20 Bytes payloads. The main disadvantage of Weightless-N is the one-way communication from nodes to the base station.

To conquer the disadvantage of Weightless-N, Weightless-P [65] is proposed to achieve bidirectional communication at the cost of consuming more energy. Adopting Gaussian Filtered Minimum Shift Keying (GMSK) and offset Quadrature Phase Shift Keying (QPSK) modulation scheme, Weightless-P operates in sub-GHz bands such as 433 MHz and 868 MHz or licensed bands with a bandwidth of 12.4 kHz.

6) TELENESA

Telensa [66] provides LPWAN IoT solutions and infrastructure for smart city buildings, especially smart street lighting [67]. With the Ultra Narrow Bandwidth (UNB) 2-FSK modulation scheme, Telensa operates in unlicensed ISM band including EU 868 MHz, US 915 MHz and Asia 430 MHz. Although the source is not open, Telensa is trying to standardize its technology to comply with ETSI LTN.

III. 5G ARCHITECTURE

5G was initially standardized by 3GPP from Release 15 in 2018 [7] and shortly afterward, deployments by both public and private network operators commenced. For example, Verizon and AT&T released their first 5G service in the USA at the end of 2018. The early commercial systems of 5G are deployed in the Non-standalone Architecture (NSA) mode in which only the 5G New Radio (5G NR) is utilized and the 4G core network, Evolved Packet Core (EPC), remains as the core network. This architecture provides only eMBB service. However, subsequent Releases of 5G provide

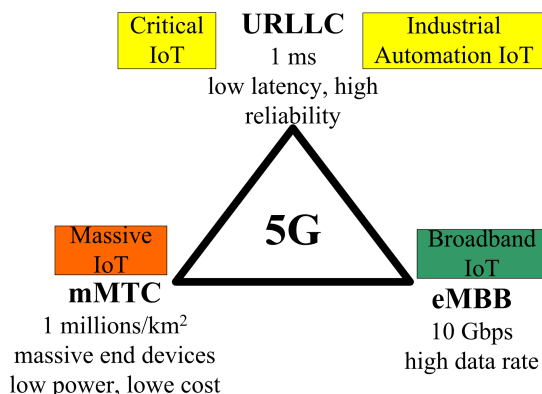


FIGURE 2. Applications scenarios of 5G.

URLLC service and mMTC service to support varieties of IoT applications. As shown in Figure 2, the requirements of the three application scenarios are distinct from each other. For eMBB, 5G is required to provide communication with a high data rate of up to 10 Gbps. For URLLC, 5G should provide mission-critical communication with a latency of less than 1 ms. For mMTC, 5G is expected to enable ultra-dense connection (1 million per km²). The KPIs of the three application scenarios are too strict to be met simultaneously. Fortunately, most practical use cases do not require 5G to meet all the KPIs. For example, some mission-critical applications require URLLC to function properly but a lot of these applications have low data rate requirements.

5G has been designed with evolved network architecture and a set of enabling technologies, such as Software Defined Network (SDN), Network Function Virtualization (NFV) and Network Slicing, are utilized to support its stringent requirements. Before 5G, cellular technologies are designed by the hardware-based method. SDN, a network paradigm evolved from work done at UB Berkeley and Stanford [68], can replace this method with software-driven network design, which can make the network more flexible and programmable [1]. NFV can be the complement to SDN for 5G. It enables the functions of the 5G core to work in general-purpose hardware rather than dedicated hardware, which can reduce the operators' cost and make the network more scalable and agile. Due to the distinct scenarios that 5G should be applied to, a physical 5G network is expected to incorporate multiple logical networks with different Quality of Service (QoS). Network Slicing can achieve this goal to provide different network topologies and parameters configuration for different services.

There are two methods to describe and visualize the architecture of 5G: reference point representation and service-based representation. In both representations, each network element is called a function and the acronyms of these functions are described in Table 5. As shown in Figure 3, reference point representation is a traditional method that describes the logical interfaces between two functions. In 5G, the interaction between two functions

is regarded as a service provisioning process in which one function serves as the service provider and the other one serves as the service user [69]. Thus, service-based representation, shown in Figure 4, can describe this notion better. Moreover, the control plane and user plane are completely separated in 5G. Compared with 4G, there are three noticeable features in the 5G network architecture. First, some 4G entities are separated into several logical functions in 5G. For example, Home Subscriber Server (HSS) in 4G can achieve user equipment (UE) authentication while in 5G the subscription information stored in Unified Data Repository (UDR) [70] should be retrieved by Authentication Server Function (AUSF) through Unified Data Management (UDM). This kind of separation can simplify the deployment and management of the functions even when the network scales up in size. Second, new functions have been introduced to provide more services. For example, Network Slicing Select Function is introduced to achieve Network Slicing. Third, unlike 4G, the entities in 5G are called functions because they are just logical functions that may run in the same physical general-purpose hardware by NFV.

It can be seen from Sections 2 and 3 that the requirements of the mMTC scenario can be met by LPWAN and with 5G being a flexible, scalable, agile and programmable network platform, it is the opportunity to integrate LPWAN into 5G network to create a hybrid ecosystem for IoT [1]. The authors in [71] introduce the 5G Test Network (5GTN) in Oulu, Finland, which has a highly heterogeneous architecture including IEEE 802.11, Bluetooth Low Energy, LoRa, NB-IoT, Ultra-wideband (UWB) and LTE evolutions like LTE-M and LTE-U. The 5GTN demonstrates the feasibility of unlicensed LPWAN-5G integration, but there are still many challenges.

IV. INTEGRATION CHALLENGES

Cellular LPWAN technologies are designed to be compatible with cellular networks, but they operate in licensed cellular bands, which results in significant initial capital investment. Non-cellular LPWAN technologies, operating in unlicensed bands with low power consumption, wide coverage, low-cost and scalability, are expected to complement 5G networks to support a variety of applications. By integrating unlicensed LPWAN into 5G, the capital and operational expenditures of the operator can be significantly reduced through a hybrid network with a unified management entity. However, there are several challenges for the integration of non-cellular LPWAN and 5G, including hybrid architecture, security, mobility, interoperability between LPWAN technologies and coexistence of LPWANs with other wireless technologies.

A. HYBRID ARCHITECTURE

5G and unlicensed LPWAN have their own infrastructures which are different from each other. For operators that require both 5G and LPWAN, it could be costly and inefficient to deploy and manage two network infrastructures

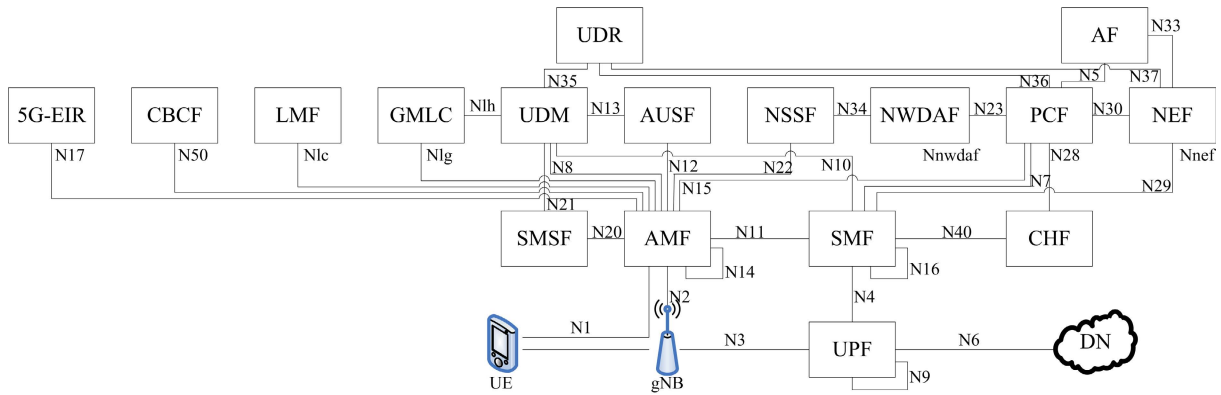


FIGURE 3. Reference-point network architecture of 5G.

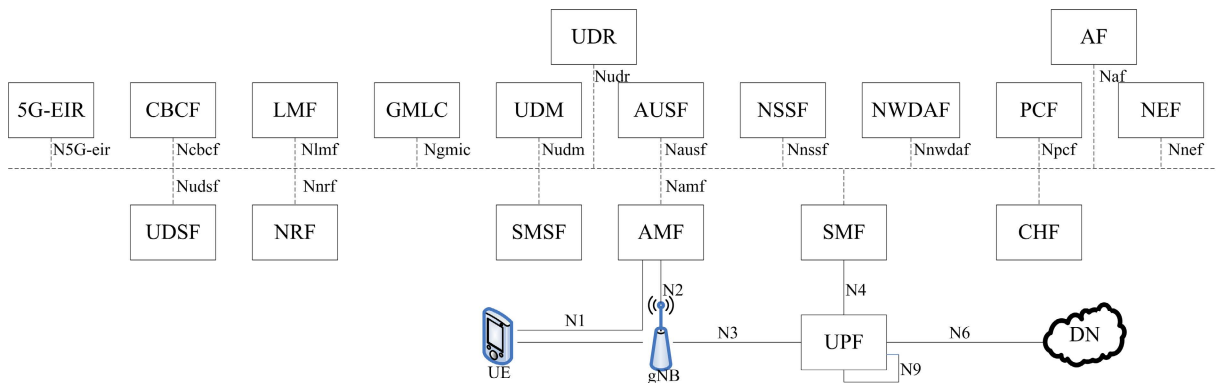


FIGURE 4. Service-based network architecture of 5G.

simultaneously. Thus, there is an urgent need for a hybrid architecture that can support and manage LPWAN end devices through 5G infrastructure. Unfortunately, it is challenging to design such hybrid architecture for both access and core networks. As shown in Figure 1, LoRaWAN has a simple architecture that is distinct from the much more complicated architecture of 5G shown in Figure 3. In terms of access networks, LoRaWAN end devices transmit each packet over the air to all the gateways that can receive the signal, and then these gateways will forward the copies of the packet to the network server without processing. In contrast, 5G UE will select the best gNB to transmit packets, and then only the serving gNB will transmit the packets to the core network. Moreover, LoRaWAN and 5G have distinct radio access technologies that are only suitable for their own use cases and cannot be applied to each other.

In terms of core networks, emerging enabling technologies, including network slicing, NFV and SDN, provide the possibility of implementing LoRaWAN servers within 5GC. The control plane and the user plane are separated entirely in 5GC for scalability and easy management [72]. By contrast, all the signals, including both signaling and user data, are transmitted to Network Server in LoRaWAN. Hence, LoRaWAN packet routing has to be carefully designed in the converged core network for seamless interoperability.

B. SECURITY

As expected, 5G and LPWAN adopt different security schemes. Compared with 5G, the security schemes of LPWAN are simplified due to the requirements of low cost and low power consumption of end devices. However, this results in three notable security challenges for LPWAN-5G integration, which are identity protection, key derivation and encryption, and unified authentication procedure. First, to protect UE identities, 5G adopts Subscription Concealed Identifier (SUCI) to conceal the permanent UE identifier, i.e. Subscription Permanent Identifier (SUPI), which is not transmitted over the air in plain text at any time [73]. By contrast, LPWANs do not meet the requirements of identity protection of 5G [74]. For example, LoRaWAN end devices will send join-request, containing Devices Extended Unique Identifier (DevEUI) and Join Extended Unique Identifier (JoinEUI), to the gateways over the air without encryption [45]. DevEUI and JoinEUI are 64-bit MAC addresses that identifies LoRaWAN end devices and Join Servers respectively. The Join-request in plain text would undermine the security of the LPWAN-5G integrated network [75]. In terms of the privacy of LPWAN users, their DevEUI could be captured by illegitimate gateways, resulting in position exposure and/or the crisis of replay attack [76]. In terms of the security of the integrated core network, JoinEUI would expose the address of the function dealing

with the join-request, which could lead to Denial-of-Service (DoS) [77]. Thus, identity protection is one of the challenges when designing secure LPWAN-5G integrated networks.

Second, it is difficult to integrate the different key hierarchies and encryption methods of LPWANs and 5G. From the root key K to the radio key K_{gNB} , 5G adopts 6-level key hierarchy and AKA-based encryption. By contrast, LPWANs generally adopt 2-level key hierarchy and AES-based encryption as shown in Table 2. To enhance the efficiency of the hybrid network and benefit from the integrated infrastructure, the keys of LPWANs can be derived from the keys of 5G. However, it is challenging to design an exchange mechanism to send 5G keys to LPWANs without posing any threats to the security of the 5G network.

Third, LPWANs adopt diverse authentication methods and it is difficult to design a unified authentication method for all kinds of the LPWAN end devices in the hybrid network. 5G adopts three bidirectional authentication methods including 5G-Authentication and Key Agreement (5G-AKA) [78], Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) [79] and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) [80]. EAP-TLS is used to provide key services in specific IoT circumstances [81]. Due to the constraints on end devices such as low power and low cost, LPWANs tend to adopt unidirectional authentication methods i.e., only end devices need to be authenticated by the network [82]. When different types of LPWANs end devices connect to the hybrid network, a network-independent authentication method should be used for these end devices to reduce the network complexity and ease management. However, given the diversity of LPWANs and the requirement of compatibility with 3GPP's specification, it is hard to design a unified authentication method for these LPWAN end devices. Hence, special care must be taken when designing a LPWAN-5G hybrid network to ensure that the security of both technologies is not compromised.

C. MOBILITY

In most cases, both cellular and non-cellular LPWANs only consider fixed connected things and the mobility of end devices is not the strength of LPWANs, which limits the range of their suitable use cases [83]. For example, as two major drivers of the expected IoT growth in the next few years, smart transportation and logistics tend to adopt IEEE 802.11p-based technologies instead of LPWANs mainly due to their mobility [84]. Although roaming and high mobility are not supported by most LPWAN standards, mobility is one of the key features of 5G systems [85]. In the hybrid network of LPWAN-5G integration, the mobility and roaming ability of LPWANs is expected to be significantly enhanced by virtue of the strong mobility and roaming ability of 5G. However, there are three challenges that should be addressed to enhance the mobility and roaming ability of LPWANs by 5G. First, the interface between the data management entities of LPWAN and 5G should be designed

carefully. As shown in Figure 3, 5G adopts UDM to manage subscription data stored in UDR [70]. By contrast, LPWANs employ different entities to manage data. For example, as shown in Figure 1, Join Server is the the entity that manages the subscription information of LoRaWAN users [86]. The different data management entities need to communicate with each other through an interface when 5G network is utilized to authenticate the roaming or moving end devices of LPWANs. The interface must be designed carefully as important data, such as encryption keys and subscription information, would be transmitted through it, which has an impact on the network security and privacy.

Second, it is challenging to map from the 64-bit MAC address of LPWANs end devices to SUPI of 5G. According to 3GPP specifications, all the data of 5G, including subscription data, policy data, structured data for exposure, application data and group ID mapping data, converged in an UDR, instead of multiple databases [87]. In the hybrid network of LPWAN-5G integration, the subscription data of LoRaWAN should be transferred to UDR for both mobility enhancement and compatibility with 5G standards. However, as shown in Figure 5, user equipment Identifier (ueId) serves as the identifier to structure the subscription data in UDR for 5G. The ueId of 5G is referred to as SUPI that is no more than 15 digits consisting of Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscription Identification Number (MSIN). By contrast, LPWANs generally use 64-bit MAC addresses as the identifiers of their end devices. To keep UDR compliant with 3GPP, the long MAC addresses need to be mapped to the short SUPI, which is a challenge.

Third, designing a unified charging and billing policy for LPWANs in 5G system needs to be considered. Emerging enabling technologies allow 5G networks to achieve multitenancy, multi-network slicing and multi-level services, resulting in the increasing complexity of charging and billing system [88]. From release 15, service-based charging and billing systems are introduced by 3GPP, merging the message commands, chargeable events and charging information in the Charging Function (CHF) [89]. On the other hand, the charging and billing policies of LPWANs usually depend on the operators and are highly diverse. Thus, to enhance the mobility of the hybrid network, we need to carefully design a hybrid core that can support both the highly diverse charging policies of LPWANs and the highly converged and complex charging policies of 5G.

D. INTEROPERABILITY BETWEEN LPWAN TECHNOLOGIES

In the Internet of Everything era, a single technology cannot meet the demands of all kinds of use cases. Multiple LPWAN technologies may be deployed in the same area or even in the same hybrid ecosystem. However, most non-cellular LPWAN technologies operate in unlicensed ISM frequency bands that are close to each other or even in the same bands, resulting in interference and collisions [90]. For example, both operating in EU 868 MHz and EU 434 MHz, LoRaWAN and SigFox

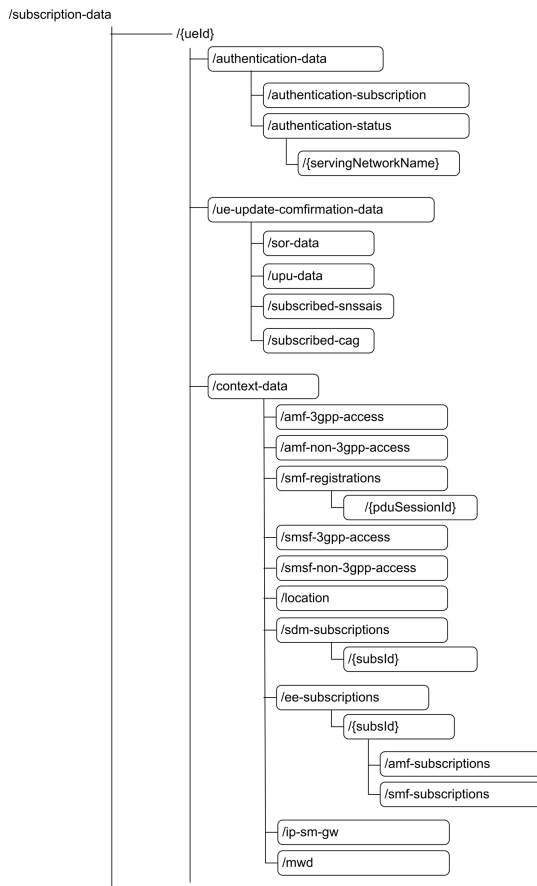


FIGURE 5. Architecture of subscription data in UDR (extracted from [87]).

may interfere with each other in Europe [91]. Thus, the main challenge of interoperability between LPWANs is to mitigate interference of radio signals. Moreover, although LPWANs have the advantages of wide coverage, low cost and low power consumption, their weaknesses are also noticeable, such as low mobility, low reliability and low security. It is important to overcome their weaknesses through interoperability between multiple LPWAN technologies.

E. COEXISTENCE WITH OTHER WIRELESS TECHNOLOGIES

Although LPWANs have the advantages of low power consumption, wide-area coverage, low-cost and scalability, they generally have lower data rates, lower reliability and higher latency, and can only meet the demands of mMTC. For other types of IoT requirements like URLLC, LPWANs are not suitable. In order to meet the demands of all kinds of use cases, a hybrid 5G-based ecosystem with various wireless technologies including but not limited to LPWANs is needed. Given the distinct features of these different wireless technologies, designing a coexistence scheme for the 5G-based ecosystem is a great challenge. Thus, we should also consider the existence of LPWANs with other wireless technologies when designing the scheme of LPWAN-5G integration.

As shown in Table 3, the challenges of LPWAN-5G integration are summarized and linked with corresponding potential solutions that will be discussed in next section.

V. POTENTIAL SOLUTIONS

In this section, we will discuss the potential solutions to address the five challenges mentioned above.

A. ARCHITECTURE OF UNLICENSED LPWAN-5G INTEGRATED NETWORKS

The authors in [93] investigate how to seamlessly integrate LoRaWAN into 5G and propose four potential integration options, i.e. 1) via 3GPP access network, 2) via non-3GPP untrusted access network, 3) as a part of eNodeB, and 4) virtually as a part of the core network. In Option 1, the LoRaWAN gateway has access to eNodeB by installing Universal Mobile Telecommunications System Subscriber Identity Module (USIM) and IP stack in the gateway. Then, by the eNodeB connected with EPC through the S1 interface, LoRaWAN can access the core of the cellular network. This option is easy to be implemented and has already been realized in the 5G Test Network of the University of Oulu, Finland in 2017 [93]. Moreover, currently, there are also available commercial LoRaWAN gateways in the market for this Option, like the Wirnet iFemtoCellevolution LoRaWAN gateway [143] produced by Kerlink. In Option 2, the LoRaWAN gateway is also required to have an IP stack. Moreover, the evolved packet data gateway (ePDG) configured in 5G Core Network (5GC) can create Internet Protocol Security (IPSec) tunnel for untrusted non-3GPP access network [144], which makes it possible for the LoRaWAN gateway to be connected with 5GC through one non-3GPP technology like WiFi. In Option 3, the LoRaWAN gateway is incorporated into eNodeB which is expected to support multiple LPWAN technologies in the future, enabling LPWAN end devices to have access to eNodeB directly. This will increase the complexity of eNodeB and at the stage of deployment, the operators have to modify many eNodeB which they have already deployed before. In Option 4, utilizing NFV and OpenStack cloud platform, the LoRaWAN server will be installed in the cloud as a part of 5GC and the LoRaWAN functionality will be available in some virtual instances.

Similar to option 3, the integrated architecture proposed by [18], named as Option 5 in our survey, is to implement the virtual base station function of eNodeB protocol stacks into LoRaWAN gateways, which enables the gateway to deliver signaling and data message through 5GC. In both Option 3 and Option 5, the integration is achieved at the RAN level by incorporating LoRaWAN gateways with eNodeB, but their incorporating directions are opposite. In Option 5, only the LoRaWAN gateway needs to be modified, while the end device, LoRaWAN server and 5GC infrastructure remain standard. Consequently, both 5G and LoRaWAN security are maintained. Furthermore, from the cellular operators' perspective, Option 5 is better than Option 3 considering the

TABLE 3. Challenges and potential solutions.

Aspects	Challenges	General efforts	Potential solutions	Status ¹
Architecture	Access network design	Actility, Simfony	[18], [92]–[96], Kerlink	✓
	LoRaWAN packet routing in the converged core		None	×
Security	Identity protection	5G: [97]–[106]	None	×
	Key derivation and encryption	LPWANs: [19], [22], [23], [107]–[112]	[18], [92]	✓
	Unified authentication procedure	Integration: [21]	[113], [114]	✓
Mobility	Interface design between data management entities	5G: [22], [24], [115]–[122]	[92]	✓
	Mapping from MAC address to SUPI	LPWANs: [123]–[129]	None	×
	Charging and billing policy design	Hybrid network: [130]	None	×
Interoperability between LPWANs	Interference between LPWANs	None	[91], [90]	✓
	Overcoming weaknesses by interoperability		[130]–[132]	✓
Coexistence with other wireless technologies	designing a coexistence scheme for a hybrid 5G-based ecosystem	None	[33], [133]–[142]	✓

¹ ✓ denoting that the challenge has not yet been completely solved even though some work has been done, and × denoting that no work has been done to address the challenge

cost of deployment as there is no need to modify a great number of eNodeB which have already been deployed before. Therefore, Option 5 has advantages over Option 3 in terms of security [18] and deployment costs.

In [92], the LoRa end device is equipped with components required in 5G UE, which consequently has the capability of 5G communication. We denote the architecture as Option 6 in the survey. When adopting Option 6, the roaming end device can be authenticated in a visited LoRaWAN network by virtue of 5GC, which enhances the mobility and roaming ability of LoRaWAN. There are two authentication methods in Option 6. Method A does not require 5G coverage but deviates from the standard authentication procedures of 5G and LoRaWAN. By contrast, method B almost follows the standard authentication procedures of 5G and LoRaWAN but requires 5G coverage and pre-authentication. Although the roaming ability is enhanced, Option 6 is not suitable for many common use cases, especially in cases where the end device does not need roaming, making this option expensive since the end device has dual connection capability.

Other researchers employed architectures of these options to investigate other issues of cellular-LoRaWAN integration. Employing Option 1, an LTE-LoRaWAN integrated network is adopted in [94] to evaluate two use cases, i.e., terrestrial vehicular and unmanned aerial vehicles. Specifically, LTE serves as a backhaul network while LoRaWAN is used to deliver the data collected in sensors. In doing so, the cellular infrastructure that the operators have deployed can be employed to support the LoRaWAN network. With the architecture of Option 1, [95] utilizes LTE as the backhaul to deliver packets from the gateway to the network server and the LoRaWAN gateways are replaced by multiple intermediate gateways which can receive packets from end devices and then forward them to eNodeB. Copies of the same uplink packets from an end device are likely to be transmitted to multiple gateways and then to be forwarded to LTE. To reduce the load of LTE, [95] proposes a traffic management method to select a suitable eNodeB and a gateway for each uplink traffic. Also focused on traffic management, [96], however,

adopts Option 5 instead of Option 1. It proposes a routing and packet scheduling mechanism in the integrated network, which allows multiple LoRa gateways to coexist and forward packets through EPC to the application server. Actility [145] and Simfony [146] announced in April 2021 that they will cooperate on developing a multi-technology IoT platform that can provide Mobile Network Operators (MNOs) and Mobile Virtual Network Operators (MVNOs) an integrated solution for the management of LoRaWAN and Cellular IoT networks.

The hybrid architectures of the 6 options are illustrated in Figure 6, and the comparison among them is concluded in Table 4. Most of the options, including Option 1, 2, 3 and 5, are only considering access-level integration and only utilize cellular network as backhaul. Although Option 6 works at core network level, it is only suitable for very limited use cases due to the requirement of dual connection. Option 4 focuses on core network for most use cases, but its authors do not provide any methods to achieve it.

B. AUTHENTICATION, SECURITY AND PRIVACY

Security is an important aspect of both 5G and LPWANs. Significant research [97]–[103] has been carried out to generally analyze 5G security including its technologies, challenges, threats and solutions. Given that 5G provides substantial support for IoT, some research works, such as [104]–[106], focus on 5G security in IoT application scenarios. Although LPWANs simplify their security mechanism to achieve low cost, low complexity and low power consumption, security is still an essential aspect especially when considering network integration. As mentioned in Subsection C of Section 1, some surveys [19], [22], [23] on LPWANs analyze the security mechanisms of LPWANs. Other works focus on one specific LPWAN technology, such as [107] and [108] on NB-IoT, [109] and [110] on LoRaWAN, and [111] and [112] on SigFox.

In terms of LPWAN-5G integrated networks, there are also some published works aiming at addressing the security challenges. The work in [21] surveys the security challenges of integrating LPWAN technologies in 5G systems, and analyzes the security requirements of LPWAN-5G integration.

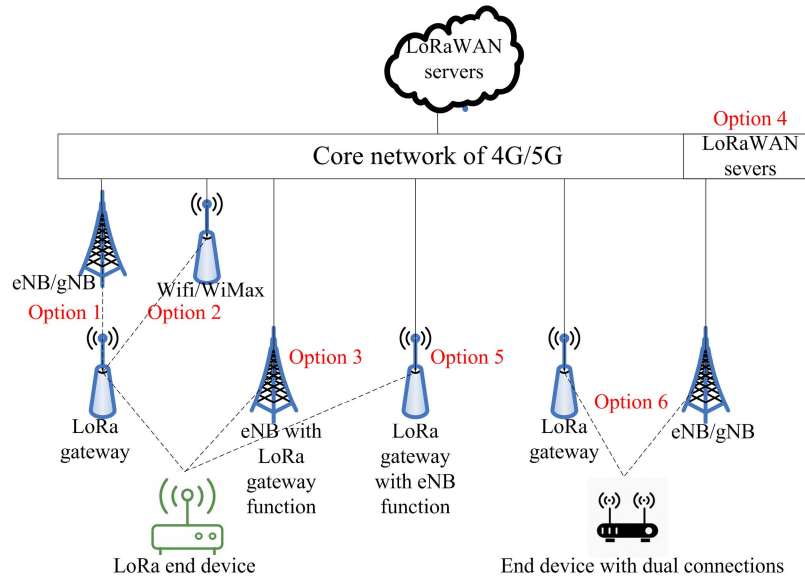


FIGURE 6. 6 LoRaWAN-5G hybrid architectures.

TABLE 4. Comparison of 6 hybrid architectures.

	Option 1	Option 2	Option 3	Option 4	Option 5	Option 6
Papers	[93], [94], [95]	[93]	[93]	[93]	[18], [96]	[92]
Architecture	3GPP access network	Non-3GPP untrusted access network	Part of eNodeB	Virtually as a part of core network	Incorporate eNodeB into LoRaWAN gateway	End device having dual connection
Applicable use cases	Most use cases	Most use cases	Most use cases	Most use cases	Most use cases	Roaming
Integration level	Access	Access	Access	Core	Access	Core
Deployment cost	Medium	Medium	High	Medium	Low	Low
Follow standard procedure	Many	Many	Almost all	Many	Almost all	Method A: little, Method B: Almost all

It can be seen from [21] that LPWAN-based security solutions need to be enhanced and adapted to meet the requirements of 5G. A secure LoRaWAN-cellular integration proposal is provided in [18], in which each LoRaWAN packet serves as the payload of a 4G message. In doing so, each LoRaWAN message ends up with two-layer encryption including AES-based encryption (LoRaWAN) and AKA-based encryption (4G). The security of both LoRaWAN and cellular networks can be ensured in this hybrid architecture. The solution proposed in [92] is to borrow 5G keys as the network session root key of LoRaWAN. Derived from the root key K , CK and IK are important 5G keys stored in both USIM and UDR to generate other derived keys. In this solution, IK is used as $NwkKey$, the network session root key of LoRaWAN, when authenticating roaming LoRaWAN end devices. In further messages after authentication, CK is used as $NwkKey$. This solution can improve the security of LoRaWAN and enhance the network efficiency as there is no need to store $NwkKey$ in LoRaWAN end devices or Join Server. However, in standard 5G systems, IK or CK is not allowed to leave UDM or UE. The key sharing proposed in [92] may have a negative impact on 5G security, which needs further analysis. Moreover, the importance of identity protection is also discussed in

this paper, but no potential solution is proposed to protect LoRaWAN identity in the integrated network.

Rather than designing a security method for a specific LPWAN technology, the authors in [114] and [113] propose a network-independent solution for access authentication of LPWAN end devices integrated into 5G. This solution is designed for constrained devices which is suitable for many LPWAN technologies, such as LoRaWAN, NB-IoT and LTE-M. But this solution is only for the secondary authentication of 5G. More research is expected to be carried out on the security aspect of LPWAN-5G integration.

C. MOBILITY AND ROAMING

Mobility and roaming of 5G has been comprehensively studied in [115] and [116], covering architecture, services, drivers, key challenges and solutions. Other surveys, including [22], [24], [117], [118], also analyze mobility and roaming of 5G. Moreover, distributed mobility management [119], [120] and blockchain-based mobility management [121], [122] are expected to bring great evolution to 5G. Compared with 5G, mobility is the weakness of LPWANs. Thus, some efforts have been undertaken to enhance the mobility of LPWANs [123]–[126].

In terms of LoRaWAN, roaming is the main research direction recognized by LoRa Alliance to enhance mobility [84] and some research, such as [127]–[129], has been carried out to enhance its roaming ability. However, we only find one paper focusing on addressing the roaming challenges of LPWAN-5G integrated networks [92]. In [92], two similar LoRaWAN-5G integration methods are proposed to enhance the mobility and roaming ability of LoRaWAN. By virtue of 5GC integrated with LoRaWAN, roaming end devices can be authenticated in a visited LoRaWAN network. In terms of interface designing, S1AP interface is used to connect Join Server with AUSF and S6a interface is used to connect Join Server with UDM. Borrowing standard interface can ensure security, but dedicated interfaces still need to be designed to improve the efficiency of data exchange. Although [92] provides the first roaming solution for LoRaWAN-5G integrated networks, the end devices in the methods are required to have dual connection ability which will significantly increase the cost of each end device. In most IoT use cases, a substantial number of end devices are needed to be deployed. It is obvious that including a 5G module in LoRaWAN end devices will significantly increase their cost. Instead of focusing on LPWAN-5G integrated network, the authors in [130] propose a media independent solution for mobility management in heterogeneous LPWANs. Although they do not consider 5G network, this IPv6-based solution can be potentially used for LPWAN-5G integrated network when multiple LPWAN technologies are integrated to a same 5G network.

D. INTEROPERABILITY BETWEEN DIFFERENT LPWAN TECHNOLOGIES

The interference between LPWANs has attracted attention from the research community. The authors in [91] measure and analyze the interference between LoRa and SigFox in the band of 863-870 MHz in Aalborg, Denmark. The results show that there is a 22-33% probability of interfering signals above -105 dBm in downtown Aalborg. Also focusing on interference measurement, the authors in [90] measure and analyze the interference between sub-Gigahertz technologies including LoRa, SigFox, Z-wave and IO Home Control. The results show that there is a non-negligible loss of 12-20% when the interferer starts during the preamble and header time. Although the interference between LPWANs has been measured and analyzed, to best of our knowledge, there is no effective solution having been proposed to eliminate the interference.

A single LPWAN technology has some limitations such as low reliability, high latency and low mobility. Adopting multi LPWANs simultaneously could enhance their capabilities. To enhance reliability, the interoperability between NB-IoT and LoRaWAN is studied in [131], and the interoperability between NB-IoT and SigFox is studied in [132]. The prototype of a multi-RAT LPWAN device in smart cities via integrating LoRaWAN into NB-IoT has been demonstrated in [131]. The result shows the feasibility of interoperability

between LoRaWAN and NB-IoT. Compared with a single LPWAN, the end devices with dual connections of both LoRaWAN and NB-IoT have higher flexibility, reliability, and dependability. To realize low cost and wide area coverage, most LPWAN technologies work in the sub-GHz band, suffering from high data loss rate mostly due to the channel effects [147], [148]. Besides, the quest to keep the network in the low power mode negatively affects data packet delivery. As a result, it is difficult for LPWAN to support critical use cases which need high reliability or low latency. In [132], redundant LPWAN technologies are used to provide improved resilience for critical use cases. Specifically, NB-IoT is implemented as the primary communication technology to send data while SigFox is chosen to be the secondary communication technology to provide a backhaul path. To enhance mobility, the handovers between LoRaWAN and NB-IoT is achieved in [130] by a IPv6-based solution. In conclusion, the works in [130], [131], and [132] demonstrate the benefits of interoperability between different LPWANs, but more solutions are needed to improve the efficiency of interoperability.

E. CO-EXISTENCE OF LPWAN WITH OTHER WIRELESS TECHNOLOGIES

In the era of the Internet of Everything, billions of devices will be connected and varieties of wireless access technologies will coexist in the same area or even in the same ecosystem. When designing the LPWAN-5G integrated network, the coexistence of LPWAN with other wireless technologies should also be considered. The work in [133] surveys the potentials of integrating Cognitive Radio (CR) into LPWAN for IoT-based applications. Given the heterogeneity and the requirements of IoT standardization, the authors in [134] propose an architecture of the integrated IoT application development platform which supports heterogeneous IoT end devices including both long-distance and short-distance communication devices such as LoRa, ZigBee and Bluetooth Low Energy. The options of the integration of LPWAN and Low Rate-Wireless Personal Area Networks (LR-WPAN) are investigated in [135], and two technologies: NB-IoT and IEEE 802.15.4.g, are selected to implement the integration. The authors in [136] analyze the coexistence of 5G NR, LTE-A and NB-IoT in the 700MHz band by an indoor experiment, showing an efficient spectrum sharing for the three wireless technologies.

Although NB-IoT is designed to comply with LTE and utilize the infrastructure of LTE, the interference and collision may still happen due to their operating frequency bands that are the same or close to cellular bands [138]. Oh and Song [33] demonstrates that NB-IoT may interfere with LTE which is likely to affect the coexistence of NB-IoT with LTE. The authors in [139] analyze the interference between NB-IoT and LTE signals, and propose a new algorithm for channel equalization to reduce the sampling rate mismatch between the NB-IoT user and LTE base station. To eliminate NB-IoT interference to LTE, machine

learning is a potential solution, e.g., the block sparse Bayesian learning-based approach proposed in [140] and the sparse machine learning-based approach proposed in [141]. Based on the interference prediction, the authors in [142] propose a novel framework for radio resource management in NB-IoT systems. In addition to the NB-IoT, LoRa may also interfere with LTE if the LoRa transceiver, like SX1281 released by Semtech, operates in the 2.4GHz frequency band [137].

VI. FUTURE WORKS

As shown in Table 3, many efforts have been undertaken to address the challenges of LPWAN-5G integration. However, most of the proposed solutions need to be further enhanced. In this section, we will identify and discuss two promising research directions that have potentials to address the challenges.

A. ARCHITECTURE DESIGNING FOR CORE-LEVEL INTEGRATION

As shown in Table 4, all current research works on LPWAN-5G integration are based on 4G or NSA 5G with EPC serving as the core network. The main reason is that 5G network deployments started in 2018 with non-standalone mode that employs EPC as the core network [149]. However, till March 2021, 68 operators in 38 countries globally have been investing in public 5G SA networks with 5GC according to Global mobile Suppliers Association (GSA) [150]. With the advent of Standalone (SA) 5G, 5GC is becoming available for both research and commercial deployments. Compared with EPC, 5GC can support more extensive and powerful functions by virtue of many enabling technologies like NFV, SDN and Network Slicing. Since the emergence of 5GC, Fixed-Mobile Convergence (FMC) [151], [152] has evolved gradually from access network level to core network level, which makes it possible to manage different access networks and UE by a converged 5GC. Similarly, it is expected that more research will be done at the core network level for LPWAN-5G integration. There are three motivations behind core-level integration in the SA 5G era. First, enabling technologies such as SDN and NFV can considerably reduce the cost and complexity when new functions (like servers of LPWAN) need to be implemented into the core mainly by reusing the same hardware [153]. Furthermore, Network Slicing enables many networks with different features to be able to coexist in a single core network [154]. For instance, LPWAN is characterized by low data rate and non-time-critical applications, while standard 5GC supports URLLC. By using NSF, the 5GC can be logically sliced into two distinct networks - one is characterized by a low data rate for LPWAN, while the other one is characterized by low latency for URLLC applications. Although logically separated, the two distinct networks still coexist in a converged 5GC, which is beneficial for optimization of network resource configuration and adoption of different security schemes.

Second, unified management and overall optimization can be achieved when integrating at the core level. If the

integration is considered only at access networks such as Options 1, 2, 3 and 5, the cellular network only serves as a backhaul network from the LPWAN perspective and there is no interworking between 5GC and the servers of LPWAN, which makes the cellular network transparent. Consequently, it is impossible to manage the 5G network and the LPWAN in a converged core and the overall optimization of the hybrid network is also unlikely to be achieved.

Third, for operators, especially cellular network operators, the core level integration can massively reduce the cost of deployment, operation, management and maintenance compared with operating two separate networks i.e. 5GC and LPWAN servers. To expand the scope of their customer base, operators have integrated NB-IoT into their cellular networks [155], [156]. Thus, it can be predicted that more LPWAN networks would be integrated into operators' cellular networks and more integrations would be implemented at the core level in the future. However, the integrated access network is still valuable which could considerably reduce the cost of gateway deployment by utilizing the 5G access network which has been already deployed. Therefore, rather than relying on a single option listed in Table 5, the prime integrated architecture is likely to be a hybrid of two options. For example, option 4 can be used to build a LPWAN-5G converged core network and then option 5 can be used to get access to the converged core network for LoRaWAN end devices.

B. UNIFIED DATA MANAGEMENT

As discussed in Section V, 5G and LPWANs employ different databases and data management methods, which has a negative impact on the efficiency, mobility and security of LPWAN-5G integrated networks. It is expected to use a unified database to store the subscription information of both 5G UE and LPWAN end devices, and to design a unified method to manage the unified database. Unlike Option 6 requiring dual connectivity, unified data management enables LPWAN end devices without a 5G module to be authenticated as if the LPWAN gateway receiving the join request is connected to a network server residing in the 5GC, which can retrieve the subscription information of the end device stored in the UDR. End devices roaming in a visited LPWAN network whose gateways have access to the same 5GC can also be authenticated without the need for a 5G module. Moreover, unified data management can enhance security of LPWAN-5G integrated network as it reduces the risk of data exposure when two independent data management entities interact with each other.

VII. CONCLUSION

In this paper, we provide a survey and tutorial on LPWAN-5G integration for hybrid networks, focusing on main integration challenges and potential solutions. We first compare the leading nine popular LPWAN technologies, which were classified into cellular LPWANs operating in licensed bands and non-cellular LPWANs operating in unlicensed bands.

We also introduce the 5G network architecture, which is a flexible, scalable, agile and programmable network platform to which other technologies can be integrated, and the enabling technologies. Then, the main challenges and potential solutions of LPWAN-5G integration are discussed in detail. Finally, we identify and discuss two future research directions that have great potential to enable hybrid LPWAN-5G networks. In conclusion, it is feasible to integrate LPWAN to 5G systems, but some key problems should be addressed including hybrid architectures, security, mobility, and interoperability between LPWANs, and coexistence with other wireless technologies. We predict that LoRaWAN will be given priority when integrating non-cellular LPWAN technologies to 5G given its popularity and open-source protocol. Moreover, unlike previous work mainly focusing on access-level integration, more efforts will be undertaken to design a converged core network for LPWAN-5G integration.

**APPENDIX
ABBREVIATIONS AND ACRONYMS**

As shown in Table 5, this appendix describes the abbreviations and acronyms in this paper, especially those that appear in Figure 3 and Figure 4, and have not yet been defined.

TABLE 5. Definition of all acronyms used in the paper.

Acronyms	Definition
5G NR	5G New Radio
5G-AKA	5G-Authentication and Key Agreement
5GC	5G Core Network
5G-EIR	5G-Equipment Identity Register
5GTN	5G Test Network
ADR	Adaptive Data Rate
AES	Advanced Encryption Standard
AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
BPSK	Binary Phase Shift Keying
CBCF	Cell Broadcast Center Function
CHF	Charging Function
CR	Cognitive Radio
CSS	Chirp Spread Spectrum
DBPSK	Differential Binary Phase Shift Keying
DevEUI	Devices Extended Unique Identifier
DN	Data Network
DoS	Denial-of-Service
DSSS	Direct Sequence Spread Spectrum
EAP-AKA	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EC-GSM-IoT	Extended Coverage Global System for Mobile Communication IoT
eDRX	extended Discontinuous Reception
eMBB	enhanced Mobile Broadband
eMTC	enhanced Machine Type Communication
EPC	Evolved Packet Core
ePDG	evolved Packet Data Gateway
FMC	Fixed Mobile Convergence
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
GMLC	Gateway Mobile Location Centre

TABLE 5. (Continued.) Definition of all acronyms used in the paper.

GMSK	Gaussian Filtered Minimum Shift Keying
gNB	5G base station
GSM	Global System for Mobile Communication
HSS	Home Subscriber Server
IoT	Internet of Things
IPSec	Internet Protocol Security
ISM	Industrial, Scientific and Medical
LMF	Location Management Function
JoinEUI	Join Extended Unique Identifier
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWA	Low Power Wide Area
LPWAN	Low Power Wide Area Network
LP-WPAN	Low Rate-Wireless Personal Area Networks
LTE	Long Term Evolution
LTE-M	LTE-Machine-to-Machine
LTN	Low Throughput Network
M2M	Machine-to-Machine
MAC	Medium Access Control
MBB	Mobile Broadband
MCC	Mobile Country Code
MIC	Message Integrity Code
mMTC	Massive Machine Type Communication
MNC	Mobile Network Code
MNOs	Mobile Network Operators
MSIN	Mobile Subscription Identification Number
MTC	Machine Type Communication
MVNOs	Mobile Virtual Network Operators
NB-IoT	Narrowband Internet of Things
NEF	Network Exposure Function
NFV	Network Function Virtualization
NRF	Network Repository Function
NSA	Non-standalone Architecture
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
PCF	Policy Control Function
RPMA	Random Phase Multiple Access
PSM	Power Savings Management
QPSK	Quadrature Phase Shift Keying
RFID	Radio-frequency Identification
SDN	Software Defined Network
SMF	Session Management Function
SMSF	Short Message Service Function
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UE	User Equipment
ueId	User Equipment Identifier
UNB	Ultra Narrow Bandwidth
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communications
USIM	Universal Mobile Telecommunications System Subscriber Identity Module
UWB	Ultra-wideband
Weightless SIG	Weightless Special Interest Group

REFERENCES

- [1] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN—Key technology enablers for 5G networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2468–2478, Nov. 2017.
- [2] A. Neumann, L. Wisniewski, T. Musiol, C. Mannweiler, B. Gajic, G. Borislava, S. Ganesan, and P. Rost, "Abstraction models for 5G mobile networks integration into industrial networks and their evaluation," in *Kommunikation Und Bildverarbeitung in der Automation*. Berlin, Germany: Springer, 2020, pp. 88–101.
- [3] A. Neumann, L. Wisniewski, R. S. Ganesan, P. Rost, and J. Jasperpeite, "Towards integration of industrial Ethernet with 5G mobile networks," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–4.

- [4] R. Davies, "Industry 4.0 digitalization for productivity and growth," in *Proc. Eur. Parliamentary Res. Service (EPRS), Briefing*, 2015, pp. 1–10.
- [5] M. Alam, R. H. Nielsen, and N. R. Prasad, "The evolution of M2M into IoT," in *Proc. 1st Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Jul. 2013, pp. 112–115.
- [6] A. Zaidi, Y. Hussain, M. Hogan, and C. Kuhfins, "Cellular IoT evolution for industry digitalization," Ericsson, Stockholm, Sweden, White Paper, GFMC-19, 2019, vol. 17.
- [7] *System Architecture for the 5G System*, Standard TS 23.501 v17.1.1, Release 17, 3GPP, 2021.
- [8] B. Martinez, F. Adelantado, A. Bartoli, and X. Vilajosana, "Exploring the performance boundaries of NB-IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5702–5712, Jun. 2019.
- [9] M. A. Ertürk, M. A. Aydin, M. T. Büyükkaktaşlar, and H. Evirgen, "A survey on LoRaWAN architecture, protocol and technologies," *Future Internet*, vol. 11, no. 10, p. 216, Oct. 2019.
- [10] J. C. Zuniga and B. Ponsard, "SigFox system description," in *Proc. LPWAN@ IETF*, Nov. 2016, p. 14.
- [11] D. M. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao, and C. Zubia, "Energy and coverage study of LPWAN schemes for industry 4.0," in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Their Appl. Mechatronics (ECMSM)*, May 2017, pp. 1–6.
- [12] K. Mekki, E. Bajica, F. Chaxela, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
- [13] S. Sinha. (Sep. 2021). *State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion*. [Online]. Available: <https://iot-analytics.com/number-connected-iot-devices/>
- [14] GSMA. *How Mobile IoT is Changing the Industrial Landscape*. Accessed: Mar. 17, 2022. [Online]. Available: https://www.gsma.com/IoT/wp-content/uploads/2018/09/201809_GSMA_Industrial_IoT_Feasibility_Study.pdf
- [15] IoT Analytics. (Oct. 2021). *LPWAN Market Report 2021–2026*. [Online]. Available: <https://iot-analytics.com/product/lpwan-market-report-2021-2026/>
- [16] A. Krishnan. (Feb. 2021). *LoRaWAN and Multi-RAN Architecture Connecting the Next Billion IoT Devices*. [Online]. Available: <https://info.semtech.com/abi-research-white-paper>
- [17] Q. Song, L. Nuaymi, and X. Lagrange, "Survey of radio resource management issues and proposals for energy-efficient cellular networks that will cover billions of machines," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 1–20, Dec. 2016.
- [18] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, Feb. 2018.
- [19] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77454–77473, 2018.
- [20] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
- [21] J. Sanchez-Gomez, D. G. Carrillo, R. Sanchez-Iborra, J. L. Hernandez-Ramos, J. Granjal, R. Marin-Perez, and M. A. Zamora-Izquierdo, "Integrating LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions," *IEEE Access*, vol. 8, pp. 216437–216460, 2020.
- [22] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.
- [23] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications," *Telecommun. Syst.*, vol. 71, no. 2, pp. 249–274, Jun. 2019.
- [24] D. D. Olatinwo, A. Abu-Mahfouz, and G. Hancke, "A survey on LPWAN technologies in WBAN for remote health-care monitoring," *Sensors*, vol. 19, no. 23, p. 5268, 2019.
- [25] B. S. Chaudhari, M. Zennaro, and S. Borkar, "LPWAN technologies: Emerging application characteristics, requirements, and design considerations," *Future Internet*, vol. 12, no. 3, p. 46, Mar. 2020.
- [26] J. Finnegan and S. Brown, "A comparative survey of LPWA networking," 2018, *arXiv:1802.04222*.
- [27] K. Mekkil, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, 2019.
- [28] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2018, pp. 197–202.
- [29] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–5.
- [30] *Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IoT; Technical Report for BS and UE Radio Transmission and Reception (Release 13)*, Standard TR 36.802, 3GPP, 2016.
- [31] A. Adhikary, X. Lin, and Y.-P.-E. Wang, "Performance evaluation of NB-IoT coverage," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.
- [32] S. Landström, J. Bergström, E. Westerberg, and D. Hammarwall, "NB-IoT: A sustainable technology for connecting billions of devices," *Ericsson Technol. Rev.*, vol. 4, pp. 2–11, Apr. 2016.
- [33] J. Oh and H. Song, "Study on the effect of LTE on the coexistence of NB-IoT," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 610–612.
- [34] R. Ratasuk, N. Mangalvedhe, A. Ghosh, and B. Vejlgaard, "Narrowband LTE-M system for M2M communication," in *Proc. IEEE 80th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2014, pp. 1–5.
- [35] R. Ratasuk, D. Bhatoolaul, N. Mangalvedhe, and A. Ghosh, "Performance analysis of voice over LTE using low-complexity eMTC devices," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
- [36] P. Jorke, R. Falkenberg, and C. Wietfeld, "Power consumption analysis of NB-IoT and eMTC in challenging smart city environments," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
- [37] K. Xu, J. Liu, and J. Lu, "Research and realization on smart city applications based on eMTC wireless communication technology," *J. Phys., Conf. Ser.*, vol. 1757, no. 1, Jan. 2021, Art. no. 012178.
- [38] S. Lippuner, B. Weber, M. Salomon, M. Korb, and Q. Huang, "EC-GSM-10T network synchronization with support for large frequency offsets," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
- [39] *LoRaWAN Specification 1.1*, LoRa Alliance, Fremont, CA, USA, 2017.
- [40] J. Haxhibeqiri, E. D. Poorter, I. Moerman, and J. Hoebeke, "A survey of LoRaWAN for IoT: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.
- [41] D. Bankov, E. Khorov, and A. Lyakhov, "On the limits of LoRaWAN channel access," in *Proc. Int. Conf. Eng. Telecommun. (EnT)*, Nov. 2016, pp. 10–14.
- [42] J. P. S. Sundaram, W. Du, and Z. Zhao, "A survey on LoRa networking: Research problems, current solutions, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 371–388, 1st Quart., 2020.
- [43] S. Bocker, C. Arendt, P. Jorke, and C. Wietfeld, "LPWAN in the context of 5G: Capability of LoRaWAN to contribute to mMTC," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 737–742.
- [44] Semtech. *LoRa Technology: Ecosystem, Applications and Benefits*. Accessed: Mar. 17, 2022. [Online]. Available: https://info.semtech.com/ecosystem_benefits_white_paper_download
- [45] *LoRaWAN 1.1 Regional Parameters*, LoRa Alliance, Fremont, CA, USA, 2017.
- [46] J. Petajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation model for Lora technology," in *Proc. 14th Int. Conf. ITS Telecommun. (ITST)*, Dec. 2015, pp. 55–59.
- [47] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the energy performance of LoRaWAN," *Sensors*, vol. 17, no. 10, p. 2364, 2017.
- [48] SigFox. *SigFox*. Accessed: Mar. 17, 2022. [Online]. Available: <http://www.sigfox.com>
- [49] (2002). *Low Throughput Networks (LTN) Functional Architecture*. [Online]. Available: <http://www.etsi.org>
- [50] A. Mathur, M. R. Bhatnagar, and B. K. Panigrahi, "On the performance of a PLC system assuming differential binary phase shift keying," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 668–671, Apr. 2016.
- [51] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of SigFox, LoRa, GPRS, and NB-IoT," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
- [52] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² area," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
- [53] C. Gomez, J. C. Veras, R. Vidal, L. Casals, and J. Paradells, "A sigfox energy consumption model," *Sensors*, vol. 19, no. 3, p. 681, Feb. 2019.

- [54] *RPMA Technology for the Internet of Things*, I. Tech, Burlington, VT, USA, 2017.
- [55] T. J. Myers, D. T. Werner, K. C. Sinsuan, J. R. Wilson, S. L. Reuland, P. M. Singler, and M. J. Huovila, "Light monitoring system using a random phase multiple access system," U.S. Patent 8 477 830, Jul. 2, 2013.
- [56] Q. Tang, L. Yang, G. B. Giannakis, and T. Qin, "Battery power efficiency of PPM and FSK in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 1308–1319, Apr. 2007.
- [57] W. Hassan, M. Føre, J. B. Ulvund, and J. A. Alfreðsen, "Internet of fish: Integration of acoustic telemetry with LPWAN for efficient real-time monitoring of fish in marine farms," *Comput. Electron. Agricult.*, vol. 163, Aug. 2019, Art. no. 104850.
- [58] H. Saleem, "Review of various aspects of radio frequency IDentification (RFID) technology," *IOSR J. Comput. Eng.*, vol. 8, no. 1, pp. 1–6, 2012.
- [59] DASH7. *Alliance Protocol Specification v1.2*. Accessed: Mar. 17, 2022. [Online]. Available: <https://www.dash7-alliance.org/product/dash7-alliance-protocol-specification-v1-2/>
- [60] M. Weyn, G. Ergeerts, L. Wante, C. Vercauteren, and P. Hellinckx, "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 12, Dec. 2013, Art. no. 870430.
- [61] X. Chen, A. Alghaihab, Y. Shi, D. S. Truesdell, B. H. Calhoun, and D. D. Wentzloff, "A crystal-less BLE transmitter with clock recovery from GFSK-modulated BLE packets," *IEEE J. Solid-State Circuits*, vol. 56, no. 7, pp. 1963–1974, Jul. 2021.
- [62] Weightless. *Weightless*. [Online]. Available: <http://www.weightless.org/>
- [63] *Weightless-N System Specification v1.0*, Weightless, Cambridge, U.K., 2015. Accessed: Mar. 17, 2022.
- [64] R. A. Abbas, A. Al-Sherbaz, A. Bennecer, and P. Picton, "A new channel selection algorithm for the weightless-n frequency hopping with lower collision probability," in *Proc. 8th Int. Conf. Netw. Future (NOF)*, Nov. 2019, pp. 171–175.
- [65] *Weightless-P System Specification v1.0*, Weightless, Cambridge, U.K., 2015.
- [66] Telensa. *Telensa*. Accessed: Mar. 17, 2022. [Online]. Available: <http://www.telensa.com/>
- [67] Telensa. *Global Smart Street Lighting Smart Cities: Market Forecast (2019–2028)*. Accessed: Mar. 17, 2022. [Online]. Available: <https://info.telensa.com/market-forecast-2019-2028>
- [68] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Apr. 2008.
- [69] *System; Principles and Guidelines for Service Definition*, Standard TS 29.501 v17.1.0 5G, Release 17, 3GPP, 2021.
- [70] *System; Unified Data Repository Services*, Standard TS 29.504 v17.2.0 5G, Release 17, 3GPP, 2021.
- [71] A. Pouttu, O. Liinamaa, and G. Destino, "Demo/poster abstract: 5G test network (5GTN)—Environment for demonstrating 5G and IoT convergence during 2018 Korean Olympics between Finland and Korea," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 1–2.
- [72] M. W. Kang and Y. W. Chung, "An efficient energy saving scheme for base stations in 5G networks with separated data and control planes using particle swarm optimization," *Energies*, vol. 10, no. 9, p. 1417, 2017.
- [73] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.
- [74] R. Fujdiak, K. Mikhaylov, M. Stusek, P. Masek, I. Ahmad, L. Malina, P. Porabage, M. Voznak, A. Pouttu, and P. Mlynek, "Security in low-power wide-area networks: State-of-the-art and development toward the 5G," in *LPWAN Technologies for IoT and M2M Applications*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 373–396.
- [75] S.-Y. Gao, X.-H. Li, and M.-D. Ma, "A malicious behavior awareness and defense countermeasure based on LoRaWAN protocol," *Sensors*, vol. 19, no. 23, p. 5122, Nov. 2019.
- [76] W.-J. Sung, H.-G. Ahn, J.-B. Kim, and S.-G. Choi, "Protecting end-device from replay attack on LoRaWAN," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 167–171.
- [77] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, p. 3, Dec. 2018.
- [78] *Security Architecture and Procedures for 5G System*, Standard TS 33.501 v15.5.0, Release 15, 3GPP, 2021.
- [79] V. L. J. Arkkio and P. Eronen. *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. [Online]. Available: <https://rfc-editor.org/rfc/rfc5448.txt>
- [80] R. H. D. Simon and D. B. D. A. D. Ph. *The EAP-TLS Authentication Protocol*. Accessed: Mar. 17, 2022. [Online]. Available: <https://rfc-editor.org/rfc/rfc5216.txt>
- [81] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal analysis of 5G EAP-TLS authentication protocol using proverif," *IEEE Access*, vol. 8, pp. 23674–23688, 2020.
- [82] S. Chacko and M. D. Job, "Security mechanisms and vulnerabilities in LPWAN," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 396, no. 1, 2018, Art. no. 012027.
- [83] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1561–1581, 2nd Quart., 2019.
- [84] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, Sep. 2017.
- [85] M. Lauridsen, L. C. Gimenez, I. Rodriguez, T. B. Sorensen, and P. Mogensen, "From LTE to 5G for connected mobility," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 156–162, Mar. 2017.
- [86] SEMTECH. (Jul. 2015). *LoRaWAN Network Server Demonstration: Gateway to Server Interface Definition*. [Online]. Available: <https://www.thingsnetwork.org/forum/uploads/default/original/1X/4fbd86583605f4aa24cedaab874ca5a1572825.pdf>
- [87] *5G System; Usage of the Unified Data Repository Services for Subscription Data (Release 17)*, Standard TR 29.505, 3GPP, 2021.
- [88] S. Wong, N. Sastry, O. Holland, V. Friderikos, M. Dohler, and H. Aghvami, "Virtualized authentication, authorization and accounting (V-AAA) in 5G networks," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Sep. 2017, pp. 175–180.
- [89] R. Törnkvist and C. Shan, "Charging and billing architecture for 5G network," *J. ICT Standardization*, vol. 7, pp. 185–194, May 2019.
- [90] J. Haxhibeqiri, A. Shahid, M. Saelens, J. Bauwens, B. Jooris, E. D. Poorter, and J. Hoebeke, "Sub-gigahertz inter-technology interference. How harmful is it for LoRa?" in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2018, pp. 1–7.
- [91] M. Lauridsen, B. Vejlgård, I. Z. Kovacs, H. Nguyen, and P. Mogensen, "Interference measurements in the European 868 MHz ISM band with focus on LoRa and SigFox," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.
- [92] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe, and A. Skarmeta, "Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN MEETS 5G," *IEEE Access*, vol. 8, pp. 103164–103180, 2020.
- [93] R. Yasmin, J. Petajajarvi, K. Mikhaylov, and A. Pouttu, "On the integration of LoRaWAN with the 5G test network," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.
- [94] D. Carrillo and J. Seki, "Rural area deployment of Internet of Things connectivity: LTE and LoRaWAN case study," in *Proc. IEEE 24th Int. Conf. Electron., Electr. Eng. Comput. (INTERCON)*, Aug. 2017, pp. 1–4.
- [95] M. Taneja, "LTE-LPWA networks for IoT applications," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2016, pp. 396–399.
- [96] C. C. Zhang, K. K. Nguyen, C. Pham, and M. Cheriet, "Routing and packet scheduling in LORAWANs-EPC integration network," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.
- [97] P. Schneider and G. Horn, "Towards 5G security," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1165–1170.
- [98] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards sCommun. Netw. (CSCN)*, Sep. 2017, pp. 193–199.
- [99] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
- [100] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, pp. 1–25, 2018.
- [101] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018.
- [102] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

- [103] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.
- [104] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
- [105] D. Schinianakis, "Alternative security options in the 5G and IoT era," *IEEE Circuits Syst. Mag.*, vol. 17, no. 4, pp. 6–28, 4th Quart., 2017.
- [106] H. Rahimi, A. Zibaenejad, P. Rajabzadeh, and A. A. Safavi, "On the security of the 5G-IoT architecture," in *Proc. Int. Conf. Smart Cities Internet Things (SCIoT)*, 2018, pp. 1–8.
- [107] V. Kumar, R. K. Jha, and S. Jain, "NB-IoT security: A survey," *Wireless Pers. Commun.*, vol. 113, pp. 2661–2708, Apr. 2020.
- [108] A. U. Mentsiev and T. R. Magomae, "Security threats of NB-IoT and countermeasures," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 862, no. 5, 2020, Art. no. 052033.
- [109] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Comput. Netw.*, vol. 148, pp. 328–339, Jan. 2019.
- [110] I. Butun, N. Pereira, and M. Gidlund, "Analysis of LoRaWAN v1. 1 security," in *Proc. ACM MobiHoc Workshop Exper. Design Implement. Smart Objects*, 2018, pp. 1–6.
- [111] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with end-to-end encryption," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–6.
- [112] L. Ferreira, "(In) security of the radio interface in Sigfox," *Cryptol. ePrint Arch.*, Tech. Rep. 2020/1575, 2020.
- [113] D. Garcia-Carrillo, J. Sanchez-Gomez, R. Marin-Perez, and A. Skarmeta, "EAP-based bootstrapping for secondary service authentication to integrate IoT into 5G networks," in *Proc. Int. Symp. Mobile Internet Secur.*, Cham, Switzerland: Springer, 2019, pp. 13–22.
- [114] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, Feb. 2020.
- [115] I. Shaya, M. Ergen, M. H. Azmi, S. A. Colak, R. Nordin, and Y. I. Daradkeh, "Key challenges, drivers and solutions for mobility management in 5G networks: A survey," *IEEE Access*, vol. 8, pp. 172534–172552, 2020.
- [116] N. Akkari and N. Dimitriou, "Mobility management solutions for 5G networks: Architecture and services," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107082.
- [117] H. Zhang, N. Liu, X. Chu, K. Long, A. Aghvami, and V. C. M. Leung, "Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 138–145, Aug. 2017.
- [118] P. Fan, J. Zhao, and I. Chih-Lin, "5G high mobility wireless communications: Challenges and solutions," *China Commun.*, vol. 13, no. 2, pp. 1–13, 2016.
- [119] F. Giust, L. Cominardi, and C. J. Bernardos, "Distributed mobility management for future 5G networks: Overview and analysis of existing approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 142–149, Jan. 2015.
- [120] T.-T. Nguyen, C. Bonnet, and J. Harri, "SDN-based distributed mobility management for 5G networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–7.
- [121] H. Lee and M. Ma, "Blockchain-based mobility management for 5G," *Future Gener. Comput. Syst.*, vol. 110, pp. 638–646, Sep. 2020.
- [122] N. Weerasinghe, T. Hewa, M. Dissanayake, M. Ylianttila, and M. Liyanage, "Blockchain-based roaming and offload service platform for local 5G operators," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–6.
- [123] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J.-C. Prévotet, "Mobility management with session continuity during handover in LPWAN," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6686–6703, Aug. 2020.
- [124] Y. Moon, S. Ha, M. Park, D. Lee, and J. Jeong, "A methodology of NB-IoT mobility optimization," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–5.
- [125] L. Oliveira, J. J. P. C. Rodrigues, S. A. Kozlov, R. A. L. Rabêlo, and V. Furtado, "Performance assessment of long-range and SigFox protocols with mobility support," *Int. J. Commun. Syst.*, vol. 32, no. 13, Sep. 2019, Art. no. e3956.
- [126] R. Brotzu, P. Aru, M. Fadda, and D. Giusto, "Urban SigFox-based mobility system," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Aug. 2021, pp. 1–4.
- [127] F. Flammini, A. Gaglione, D. Tokody, and D. Dohrilovic, "LoRa WAN roaming for intelligent shipment tracking," in *Proc. IEEE Global Conf. Artif. Intell. Internet Things (GCAIoT)*, Dec. 2020, pp. 1–2.
- [128] W. Ayoub, M. Mroue, A. E. Samhat, F. Nouvel, and J.-C. Prévotet, "SCHC-based solution for roaming in LoRaWAN," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Cham, Switzerland: Springer, 2019, pp. 162–172.
- [129] L. Vangelista and M. Centenaro, "Worldwide connectivity for the Internet of Things through LoRaWAN," *Future Internet*, vol. 11, no. 3, p. 57, Mar. 2019.
- [130] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, H. Jradi, and J.-C. Prévotet, "Media independent solution for mobility management in heterogeneous LPWAN technologies," *Comput. Netw.*, vol. 182, Dec. 2020, Art. no. 107423.
- [131] K. Mikhaylov, M. Stusek, P. Masek, V. Petrov, J. Petajajarvi, S. Andreev, J. Pokorny, J. Hosek, A. Pouttu, and Y. Koucheryavy, "Multi-RAT LPWAN in smart cities: Trial of LoRaWAN and NB-IoT integration," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
- [132] K. D. Ballal, L. Dittmann, S. Ruepp, and M. N. Petersen, "IoT devices reliability study: Multi-RAT communication," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–2.
- [133] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Low power wide area network, cognitive radio and the Internet of Things: Potentials for integration," *Sensors*, vol. 20, no. 23, p. 6837, Nov. 2020.
- [134] Y. Li, "An integrated platform for the Internet of Things based on an open source ecosystem," *Future Internet*, vol. 10, no. 11, p. 105, Oct. 2018.
- [135] J. P. Garcia-Martin and A. Torralba, "On the combination of LR-WPAN and LPWA technologies to provide a collaborative wireless solution for diverse IoT," in *Proc. Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2019, pp. 1–4.
- [136] L. C. Alexandre, A. L. De Souza Filho, and A. C. Sodre, "Indoor coexistence analysis among 5G new radio, LTE-A and NB-IoT in the 700 MHz band," *IEEE Access*, vol. 8, pp. 135000–135010, 2020.
- [137] L. Polak and J. Milos, "LTE and LoRa in the 2.4 GHz band: Adjacent channel interference issues," in *Proc. 30th Int. Conf. Radioelektronika (RADIOELEKTRONIKA)*, Apr. 2020, pp. 1–4.
- [138] R. Ratasuk, N. Mangalvedhe, and D. Bhatoolaul, "Coexistence analysis of LTE eMTC and 5G new radio," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.
- [139] L. Zhang, A. Ijaz, P. Xiao, and R. Tafazolli, "Channel equalization and interference analysis for uplink narrowband Internet of Things (NB-IoT)," *IEEE Commun. Lett.*, vol. 21, no. 10, pp. 2206–2209, Oct. 2017.
- [140] S. Liu, F. Yang, J. Song, and Z. Han, "Block sparse Bayesian learning-based NB-IoT interference elimination in LTE-advanced systems," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4559–4571, Oct. 2017.
- [141] S. Liu, L. Xiao, Z. Han, and Y. Tang, "Eliminating NB-IoT interference to LTE system: A sparse machine learning-based approach," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6919–6932, Aug. 2019.
- [142] H. Malik, M. M. Alam, H. Pervaiz, Y. L. Moullec, A. Al-Dulaimi, S. Parand, and L. Reggiani, "Radio resource management in NB-IoT systems: Empowered by interference prediction and flexible duplexing," *IEEE Netw.*, vol. 34, no. 1, pp. 144–151, Jan. 2020.
- [143] Kerlink. *Wired Ifemtocell-Evolution LoRaWAN Gateway*. Accessed: Mar. 17, 2022. [Online]. Available: <https://www.kerlink.com/product/wired-ifemtocell-evolution/>
- [144] CND. *Core Network Dynamics*. Accessed: Mar. 17, 2022. [Online]. Available: <http://www.corenetdynamics.com/products/openepc/>
- [145] Actility. Accessed: Mar. 17, 2022. [Online]. Available: <https://www.actility.com/>
- [146] Simfony. Accessed: Mar. 17, 2022. [Online]. Available: <https://www.simfony.com/>
- [147] P. Marcellis, N. Kouvelas, V. S. Rao, and V. Prasad, "Dare: Data recovery through application layer coding for LoRaWAN," *IEEE Trans. Mobile Comput.*, vol. 21, no. 3, pp. 895–910, Mar. 2020.
- [148] I. S. Ismail, N. A. A. Latiff, and N. A. A. Aziemah, "Performance analysis of data recovery via application layer for LPWAN," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.
- [149] G. Liu, Y. Huang, Z. Chen, L. Liu, Q. Wang, and N. Li, "5G deployment: Standalone vs. non-standalone from the operator perspective," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 83–89, Nov. 2020.
- [150] GSM. (Mar. 2021). *5G Standalone Global Market Status*. [Online]. Available: <https://gsacom.com/paper/5g-standalone-2021-summary/>

[151] J. Ha and N. Park, "Unified control architecture for 5G convergence network," in *Proc. Int. Conf. Circuits, Devices Syst. (ICCDs)*, Sep. 2017, pp. 226–230.

[152] M. Condoluci, S. H. Johnson, V. Ayadurai, M. A. Lema, M. A. Cuevas, M. Dohler, and T. Mahmoodi, "Fixed-mobile convergence in the 5G era: From hybrid access to converged core," *IEEE Netw.*, vol. 33, no. 2, pp. 138–145, Mar. 2019.

[153] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN architectures: A systematic literature review," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–39, 2018.

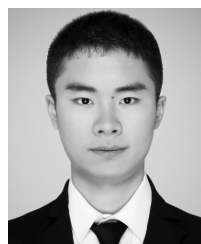
[154] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[155] B. Forum. *Tr-470, 5G Wireless Wireline Convergence Architecture*. Accessed: Mar. 17, 2022. [Online]. Available: <https://www.broadband-forum.org/technical/download/TR-470.pdf>

[156] T. Mamouni, J. A. T. Gijon, P. Olszki, and X. Lagrange, "Universal AAA for hybrid accesses," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2015, pp. 403–407.



OLUWAKAYODE ONIRETI (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in electronics engineering from the University of Surrey, Guildford, U.K. He is currently a Lecturer with the University of Glasgow. His research interests include self-organizing cellular networks, energy-efficient networks, blockchain networks, and cooperative communications.



YU CHEN (Student Member, IEEE) received the B.S. degree in measurement and control technology and instrumentation and the M.S. degree in instrument science and technology from the University of Electronic Science and Technology of China, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree with the University of Glasgow. His research interests include energy-efficient networks, hybrid network management, and compressive sampling.



YUSUF A. SAMBO (Member, IEEE) received the M.Sc. degree (Hons.) in mobile and satellite communications and the Ph.D. degree in electronic engineering from the Institute for Communication Systems (ICS) (formally known as CCSR), University of Surrey, in 2011 and 2016, respectively. He was a Postdoctoral Research Associate with the Communications, Sensing and Imaging (CSI) Research Group, University of Glasgow and has been a Lecturer with the James Watt School of

Engineering, University of Glasgow, since 2019, and the 5G Testbed Lead managing the Scotland 5G Centre testbed at the University of Glasgow. Prior to joining Glasgow, he was a Lecturer in telecommunications engineering at Baze University, Abuja, from 2016 to 2017. His research interests include self-organizing networks, cell-free massive MIMO, EMF exposure, and green communications.



MUHAMMAD A. IMRAN (Senior Member, IEEE) is currently a Professor of wireless communication systems with the University of Glasgow. He also heads the Communications, Sensing and Imaging CSI Research Group, University of Glasgow, and is the Dean of the University of Glasgow and UESTC. He is an Affiliate Professor with the University of Oklahoma, USA, and a Visiting Professor with the 5G Innovation Centre, University of Surrey, U.K. He has over 20 years

of combined academic and industry experience with several leading roles in multi-million pounds funded projects. He has filed 15 patents; has authored/coauthored over 400 journal and conference publications; was an editor of five books and author of more than 20 book chapters; and has successfully supervised over 40 postgraduate students at doctoral level. He has been a consultant to international projects and local companies in the area of self organized networks. He has been interviewed by BBC, Scottish television, and many radio channels on the topic of 5G technology. His research interests include self organized networks, wireless networked control systems, and the wireless sensor systems. He is a fellow of IET and a Senior Fellow of HEA.

...